# Citrix DaaS

# Contents



# Panoramica

November 21, 2023

## Introduzione

Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) offre soluzioni di virtualizzazione che offrono all'IT il controllo di macchine virtuali, applicazioni e sicurezza, fornendo al tempo stesso l'accesso ovunque per qualsiasi dispositivo. Gli utenti finali possono utilizzare applicazioni e desktop indipendentemente dal sistema operativo e dall'interfaccia del dispositivo.

Utilizzando Citrix DaaS, è possibile distribuire app e desktop virtuali sicuri su qualsiasi dispositivo, lasciando la maggior parte dell'installazione, della configurazione e degli aggiornamenti a Citrix. È possibile mantenere il controllo completo su applicazioni, criteri e utenti, offrendo al contempo la migliore esperienza utente su qualsiasi dispositivo.

Citrix DaaS consente di gestire i carichi di lavoro del centro dati on-premise e del cloud pubblico insieme in una distribuzione ibrida. È possibile connettersi a cloud pubblici Microsoft Azure, Amazon Web Services (AWS) e Google Cloud, oltre che ad hypervisor locali come Citrix Hypervisor, Microsoft Hyper-V, Nutanix AHV e VMware vSphere. L'approccio ibrido e multi-cloud offre la flessibilità necessaria per distribuire diverse applicazioni in diverse posizioni risorse in tutto il mondo.

Citrix DaaS offre diversi modi per distribuire app e desktop.

- I metodi di consegna descrivono i modi principali, con casi d'uso e pro/contro.
- I modelli di consegna offrono più scelte e offrono anche confronti tra modelli di VDI.

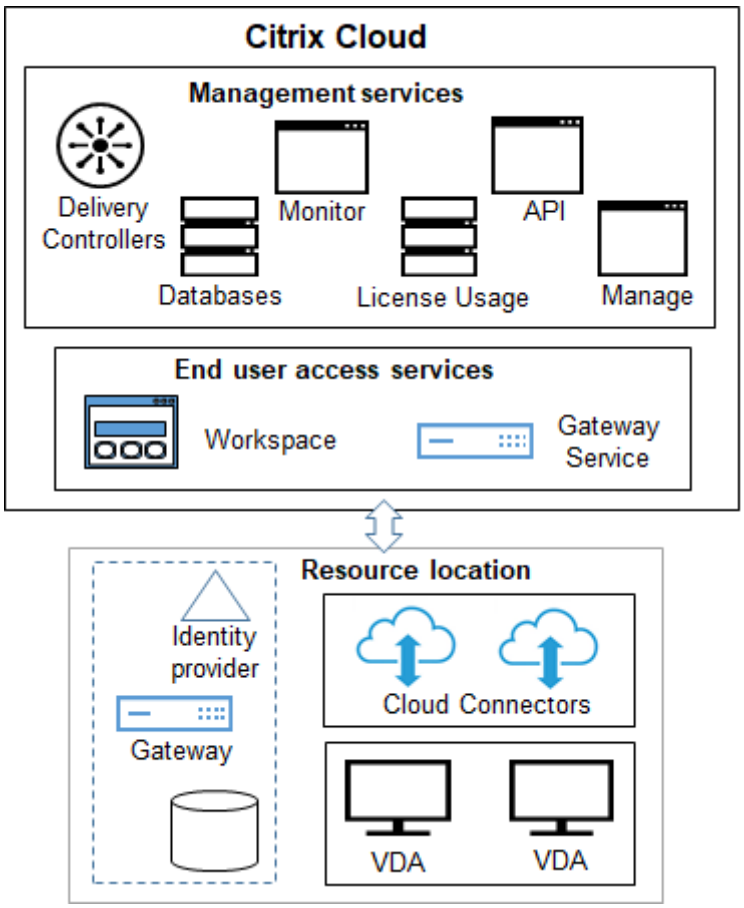
Citrix Managed Azure semplifica ulteriormente la distribuzione di app e desktop virtuali. Con Citrix Managed Azure, Citrix gestisce anche l'hosting dei carichi di lavoro di Azure.

Ulteriori informazioni sui vantaggi dell'utilizzo di questo servizio.

## Panoramica del sito

Il grafico seguente mostra i servizi e i componenti con cui lavorano gli amministratori Citrix in una distribuzione in produzione di Citrix DaaS (nota anche come sito).




Come mostrato nel grafico, Citrix gestisce i servizi e i componenti di accesso e gestione degli utenti in Citrix Cloud. Le applicazioni e i desktop distribuiti agli utenti risiedono su macchine in una o più posizioni risorse. In una distribuzione Citrix DaaS, una posizione risorsa contiene componenti del livello di accesso e dei livelli delle risorse. Ogni posizione risorse è considerata una zona.

Se di recente è stata eseguita la migrazione da Citrix Virtual Apps and Desktops, si noterà che Citrix DaaS elimina la maggior parte del lavoro di configurazione dei componenti richiesto in una distribuzione on-premise.

### Componenti e servizi gestiti da Citrix

- **Delivery Controller:** il servizio Citrix DaaS fornisce la funzionalità per bilanciare il carico di applicazioni e desktop, autenticare gli utenti e mediare o assegnare priorità alle connessioni direttamente dal cloud, senza la necessità di gestire i Delivery Controller, come avviene per Citrix Virtual Apps and Desktops.
- **Database:** i dati di configurazione, monitoraggio e registrazione della configurazione del sito vengono archiviati dal servizio cloud, eliminando la necessità di un database SQL per il prodotto Citrix Virtual Apps and Desktops locale.

- **Licensing:** gestisce le licenze e fornisce statistiche di utilizzo.
- **Interfacce di gestione:** vedere Interfacce di gestione. Molte attività sono disponibili anche nelle API di servizio.
- **Interfaccia Monitor:** l'interfaccia Monitor consente ai team di supporto IT e dell'helpdesk di monitorare un ambiente, risolvere i problemi prima che diventino critici ed eseguire attività di supporto per gli utenti finali. I display includono:
  - Dati di sessione in tempo reale dal servizio Broker nel Controller, che include i dati dell'agente broker nel Virtual Deliver Agent (VDA).
  - Dati passati del servizio di monitoraggio nel Controller.
  - Dati sul traffico HDX (noto anche come traffico ICA).
- **Cloud Connector:** un Cloud Connector è il canale di comunicazione tra i componenti di Citrix Cloud e i componenti nella posizione risorsa. Nella posizione risorsa, Cloud Connector funge da proxy per il Delivery Controller in Citrix Cloud.

  Ogni posizione risorsa contiene almeno un Cloud Connector. Per la ridondanza sono consigliati due o più Cloud Connector.
  - Quando si utilizza Full Configuration (configurazione completa) per il provisioning delle macchine, è innanzitutto necessario installare i Cloud Connector dalla console Citrix Cloud. Per ulteriori informazioni, vedere Cloud Connector.
  - Quando si utilizza Quick Deploy (Distribuzione rapida) per eseguire il provisioning delle macchine Azure, Citrix crea la posizione risorse e i Cloud Connector quando si crea un catalogo.

  Dopo aver installato i Cloud Connector, Citrix li gestisce e li aggiorna. Le uniche attività gestite dal cliente sono gli aggiornamenti e l'applicazione di patch Windows di Cloud Connector.

## Interfacce di gestione

Dalla scheda **Manage** (Gestisci) di Citrix DaaS, è possibile selezionare le seguenti interfacce.

### Full Configuration (Configurazione completa)

Dall'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa), è possibile:

- Ottenere una panoramica della distribuzione Citrix DaaS e delle funzionalità più recenti dalla home page.
- Creare e gestire connessioni agli host.

- Creare e gestire cataloghi di macchine che contengono app e desktop che vengono forniti agli utenti.
- Creare e gestire gruppi di consegna (e, facoltativamente, gruppi di applicazioni).
- Creare e gestire criteri Citrix che influenzano l'uso e il comportamento delle tecnologie e delle funzionalità HDX, oltre alla gestione a livello di sito. Sono incluse le impostazioni dei criteri per sessioni, trasporto adattivo, dispositivi, grafica, contenuti multimediali, reindirizzamento dei contenuti e VDA.
- Personalizzare l'amministrazione delegata per creare amministratori basati sui ruoli con ambiti di autorità specifici.
- Gestire la funzione Autoscale (Scalabilità automatica) per alimentare in modo proattivo le macchine che distribuiscono app e desktop.
- Bilanciare il carico delle macchine
- Eseguire controlli di integrità sui VDA per identificare potenziali problemi e suggerimenti per la risoluzione.
- Visualizzare il contenuto del log di configurazione per vedere quando sono state apportate modifiche alla configurazione e altre attività amministrative e chi le ha avviate.

#### Distribuzione rapida

Dall'interfaccia **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), è possibile distribuire e gestire facilmente i carichi di lavoro Microsoft Azure che utilizzano una sottoscrizione Citrix Managed Azure o la propria sottoscrizione Azure. Per ulteriori informazioni, vedere Quick Deploy (Distribuzione rapida) e Citrix Managed Azure. Da Quick Deploy (Distribuzione rapida) è possibile:

- Creare e gestire cataloghi.
- Creare e personalizzare immagini da varie immagini preparate da Citrix o da immagini importate dalla sottoscrizione Azure.

Per ulteriori informazioni, vedere Quick Deploy (Distribuzione rapida).

#### Environment Management (Gestione dell'ambiente)

Dall'interfaccia **Environment Management** (Gestione dell'ambiente), è possibile utilizzare le tecnologie intelligenti di gestione delle risorse e dei profili per offrire le migliori prestazioni possibili, l'accesso al desktop e i tempi di risposta delle applicazioni. Per ulteriori informazioni, vedere Workspace Environment Management.

### Componenti e tecnologie gestiti dal cliente

- **Citrix Gateway:** quando gli utenti si connettono dall'esterno del firewall aziendale, Citrix DaaS può utilizzare la tecnologia Citrix Gateway per proteggere queste connessioni con TLS. L'appliance virtuale Citrix Gateway o VPX è un'appliance VPN SSL distribuita nella zona demilitarizzata (DMZ). Fornisce un unico punto di accesso sicuro attraverso il firewall aziendale.

  Citrix installa e gestisce il servizio Citrix Gateway in Citrix Cloud. È inoltre possibile installare Citrix Gateway nelle posizioni risorse.

- **Active Directory:** Active Directory viene utilizzata per l'autenticazione e l'autorizzazione. Autentica gli utenti e garantisce che abbiano accesso alle risorse appropriate. L'identità di un abbonato definisce i servizi a cui ha accesso in Citrix Cloud. Questa identità proviene dagli account di dominio di Active Directory forniti dai domini all'interno della posizione risorsa.

- **Identity Provider (IdP):** l'IdP è l'autorità finale per l'identità dell'utente. Gli IdP supportati includono: Active Directory locale, Active Directory più token, Azure Active Directory, Citrix Gateway e Okta. Per ulteriori informazioni, vedere:

  - Identità dell'area di lavoro
  - Gestione delle identità e degli accessi

- **Virtual Delivery Agent (VDA):** su ogni macchina fisica o virtuale che distribuisce risorse (applicazioni e desktop) deve essere installato un VDA Citrix. I VDA stabiliscono e gestiscono la connessione tra la macchina su cui è installato e il dispositivo utente e applicano i criteri configurati per la sessione.

  Il VDA si registra con un Delivery Controller utilizzando un Cloud Connector nella posizione risorsa come proxy.

  Sono disponibili diversi tipi di VDA:

  - I VDA per sistemi operativi Windows multisessione consentono a più utenti di connettersi alla macchina contemporaneamente. Questo tipo di VDA viene solitamente installato su server Windows.
  - I VDA per i sistemi operativi Windows a sessione singola consentono a un solo utente di connettersi a una macchina alla volta. Questo tipo di VDA viene solitamente utilizzato per la VDI.

    Una versione di base di questo tipo di VDA è disponibile per l'uso con la funzione Remote PC Access (Accesso remoto PC). Contiene un sottoinsieme delle funzionalità del VDA a sessione singola completo.
  - I VDA Linux supportano app e desktop virtuali basati su una distribuzione RHEL, CentOS, SUSE o Ubuntu.

Nella documentazione di questo servizio, "VDA"spesso si riferisce all'agente e alla macchina su cui è installato.

- **Hypervisor e servizi cloud:** nella maggior parte dei siti di produzione, le istanze di app e desktop (carichi di lavoro) rese disponibili (pubblicate) agli utenti sono "ospitate"da un hypervisor o da un servizio cloud supportato (la funzione Remote PC Access [Accesso remoto PC] viene solitamente utilizzata con le macchine fisiche. Pertanto, non utilizza hypervisor o servizi cloud per il provisioning delle macchine).

  - Quando si utilizza l'interfaccia Full Configuration (Configurazione completa), si crea una connessione a un hypervisor host o a un servizio cloud supportato. Quindi, da Full Configuration (Configurazione completa), si utilizza un'immagine (creata tramite tale host) per creare un catalogo di macchine che contengono le istanze dell'app e del desktop. Successivamente si crea un gruppo di consegna. Citrix fornisce molti strumenti per semplificare e facilitare il modo in cui questi host di sessione vengono creati e gestiti.
  - Quando si utilizza Quick Deploy (Distribuzione rapida) per distribuire carichi di lavoro di Azure, occorre solo creare il catalogo. Sebbene sia possibile utilizzare la propria sottoscrizione Azure durante la creazione del catalogo, l'utilizzo di una sottoscrizione Citrix Managed Azure elimina anche la necessità di gestire l'host.

  Le istanze di app e desktop pubblicate possono essere locali, ospitate in cloud pubblici o in una combinazione ibrida di entrambi.

- **Citrix StoreFront:** Citrix StoreFront è il predecessore di Citrix Workspace ospitato nel cloud. Viene utilizzato come interfaccia web per l'accesso ad applicazioni e desktop.

  È possibile installare facoltativamente i server StoreFront nelle posizioni risorse. Avere store locali può aiutare a distribuire app e desktop durante le interruzioni della rete. La funzione Local Host Cache (Cache host locale) richiede uno StoreFront gestito dal cliente in ogni posizione risorse.

  Vedere User access (Accesso utente) per considerazioni sull'utilizzo di StoreFront in un ambiente di servizio.

### Oggetti configurati per la distribuzione di desktop e applicazioni

È possibile configurare i seguenti elementi per distribuire app e desktop in un ambiente di produzione.

- **Connessione host:** una connessione host (menzionata in precedenza) consente di abilitare la comunicazione tra i componenti nel piano di controllo (Citrix Cloud) e i VDA in una posizione risorse. Le specifiche di connessione includono:

  - L'indirizzo e le credenziali per accedere all'host

  - Il metodo di archiviazione da utilizzare e le macchine da utilizzare per l'archiviazione
  - Quale rete possono utilizzare le VM

  Da ricordare: quando si utilizza Quick Deploy (Distribuzione rapida), non è necessario creare una connessione. E se si utilizza Citrix Managed Azure, Citrix gestisce anche l'hosting.

- **Catalogo:** nelle interfacce Full Configuration (Configurazione completa) e Monitor, i cataloghi sono chiamati "cataloghi macchine".
  Un catalogo è una raccolta di macchine virtuali o fisiche che hanno lo stesso tipo di sistema operativo (ad esempio, Windows multisessione, Ubuntu a sessione singola).

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

  Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

  After the image is ready, you create the catalog.

  - For VMs, MCS creates the machines and the catalog.
  - For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

  For more information about MCS, see Image management.

- **Gruppo di consegna:** un gruppo di consegna specifica:

  - Una o più macchine di un catalogo.
  - Gli utenti a cui è consentito accedere a tali macchine.
  - Le applicazioni e i desktop a cui gli utenti possono accedere tramite Workspace.

  Quando si utilizza Quick Deploy (Distribuzione rapida), viene creato automaticamente un gruppo di consegna (viene visualizzato solo nell'interfaccia Full Configuration [Configurazione completa]).

- **Gruppo di applicazioni:** i gruppi di applicazioni consentono di gestire le raccolte di applicazioni. È possibile creare gruppi di applicazioni per applicazioni condivise tra gruppi di consegna diversi o utilizzate da un sottoinsieme di utenti all'interno di gruppi di consegna. I gruppi di applicazioni sono facoltativi.

## Citrix Managed Azure

Citrix Managed Azure è un'opzione disponibile in diverse edizioni di Citrix DaaS. L'utilizzo di Citrix Managed Azure semplifica la distribuzione di app e desktop virtuali da Azure. Citrix gestisce l'infrastruttura per l'hosting dei carichi di lavoro di Azure.

Con Citrix Managed Azure, si ottiene una sottoscrizione e una posizione risorse Azure dedicate gestite da Citrix. In tale sottoscrizione di Azure, si crea un catalogo di macchine virtuali. È possibile effettuare le seguenti operazioni:

- Distribuire macchine con sistema operativo Windows a sessione singola e multisessione o macchine con sistema operativo Linux da varie versioni supportate.
- Scegliere da un elenco curato di tipi di calcolo e opzioni di archiviazione in determinate regioni.
- Eseguire il provisioning di carichi di lavoro persistenti o non persistenti su tali macchine.
- Scegliere tra diverse immagini fornite da Citrix su cui è installata l'ultima versione di VDA. Quindi, dall'interfaccia Citrix, è possibile creare la propria immagine da quel modello e personalizzarla. È anche possibile importare e utilizzare immagini dalle sottoscrizioni di Azure.

Anche se Citrix gestisce la capacità di Azure, se si desidera comunicare con le risorse esistenti sulla propria sottoscrizione di Azure è possibile utilizzare il peering di Azure VNet per connettere le risorse. È inoltre possibile utilizzare Citrix SD-WAN per connettersi direttamente alle risorse locali.

Per informazioni sulla sicurezza e le responsabilità durante l'utilizzo di Citrix Managed Azure, vedere Panoramica tecnica della sicurezza per Citrix Managed Azure.

### Ordinare Citrix Managed Azure

Per ottenere una sottoscrizione a Citrix Managed Azure, è necessario sottoscrivere un'offerta di servizi Citrix supportata e quindi ordinare i Citrix Managed Azure Consumption Fund. È possibile ordinare Citrix DaaS e fondi di consumo tramite Citrix o da Azure Marketplace.
Citrix Managed Azure è supportato nelle seguenti offerte di servizi:

- Citrix Workspace Premium Plus
- Edizioni Citrix DaaS, Advanced, Advanced Plus e Premium
- Edizione Citrix DaaS Standard per Azure

Per i dettagli, consultare Iscriversi a Citrix DaaS.

### Riepilogo dei vantaggi Citrix Managed Azure

L'utilizzo di Citrix Managed Azure offre diversi vantaggi:

- Il percorso più rapido verso i vantaggi del cloud ibrido.

- Consente l'offload della gestione IT dell'infrastruttura. Offre un'esperienza di amministrazione che consente all'IT di avere il controllo, eliminando i problemi di gestione e manutenzione.
- Consente di scalare rapidamente le soluzioni di lavoro.
- Fornisce una sottoscrizione Azure separata gestita da Citrix. In questo modo si isola l'attività delle altre sottoscrizioni Azure.
- Si mantiene la flessibilità necessaria per creare e gestire carichi di lavoro utilizzando le sottoscrizioni Azure. La distribuzione può includere carichi di lavoro che utilizzano la sottoscrizione Citrix Managed Azure e carichi di lavoro che utilizzano sottoscrizioni Azure personalizzate (gestite dal cliente).
- Viene utilizzato un vero modello IaaS (Infrastructure as a Service) basato sul consumo.
- Sono disponibili diverse tecnologie per creare connessioni alle proprie reti locali (come il peering di Azure VNet e SD-WAN). Ciò consente agli utenti di accedere alle risorse della rete, ad esempio i file server.

La distribuzione e la gestione di Citrix Managed Azure da questo servizio utilizzano l'interfaccia di gestione Quick Deploy (Distribuzione rapida).

Per ulteriori informazioni, contattare il rappresentante Citrix.

## Fornitura di applicazioni e desktop agli utenti

### Citrix Workspace

Gli abbonati (utenti) accedono ai loro desktop e alle loro app tramite Citrix Workspace.

Dopo aver installato e configurato Citrix DaaS, viene fornito un collegamento all'URL dell'area di lavoro. L'URL dell'area di lavoro viene pubblicato in due posti:

- Dalla console di Citrix Cloud, selezionare **Workspace Configuration** (Configurazione dell'area di lavoro) dal menu nell'angolo in alto a sinistra. La scheda **Access** contiene l'URL di Workspace.
- Dalla pagina di **benvenuto** di Citrix DaaS, l'URL dell'area di lavoro viene visualizzato nella parte inferiore della pagina.

Eseguire il test e condividere il link dell'URL dell'area di lavoro con i propri abbonati (utenti) per consentire loro di accedere alle loro app e desktop. Gli abbonati possono accedere all'URL dell'area di lavoro senza alcuna configurazione aggiuntiva.

È possibile configurare aree di lavoro da Citrix Cloud.

- Specificare quali servizi sono integrati con Citrix Workspace.
- Personalizzare l'URL utilizzato dagli abbonati per accedere alla loro area di lavoro.
- Personalizzare l'aspetto delle aree di lavoro degli abbonati, come loghi, colori e preferenze.
- Specificare il modo in cui gli abbonati eseguono l'autenticazione nella propria area di lavoro, ad esempio utilizzando Active Directory o Azure Active Directory.

- Specificare la connettività esterna per le posizioni risorse utilizzate dagli abbonati.

Per ulteriori informazioni, vedere Citrix Workspace.

#### App Citrix Workspace

Dal lato utente, l'app Citrix Workspace viene installata sui dispositivi utente e su altri endpoint, come i desktop virtuali. L'app Citrix Workspace offre agli utenti un accesso sicuro e self-service a documenti, applicazioni e desktop da qualsiasi dispositivo, inclusi smartphone, tablet e PC. L'app Citrix Workspace consente l'accesso on-demand alle applicazioni Windows, Web e SaaS (Software as a Service).

Per i dispositivi sui quali non può essere installato il software dell'app Citrix Workspace, l'app Citrix Workspace per HTML5 fornisce una connessione tramite un browser Web compatibile con HTML5.

L'app Citrix Workspace è disponibile per diversi sistemi operativi. Per ulteriori informazioni, vedere l'app Citrix Workspace.

### Accordo sui livelli di servizio

Citrix DaaS è progettato utilizzando le procedure consigliate del settore per raggiungere la scalabilità del cloud e un alto grado di disponibilità del servizio.

Per i dettagli completi sull'impegno di Citrix per la disponibilità dei servizi Citrix Cloud, vedere l'Accordo sui livelli di servizio.

Le prestazioni relative a questo obiettivo possono essere monitorate su base continuativa alla pagina https://status.cloud.com.

#### Limiti

Il calcolo di questo obiettivo del livello di servizio non includerà la perdita di disponibilità dovuta alle seguenti cause:

- Mancato rispetto da parte del cliente dei requisiti di configurazione per Citrix DaaS indicati nella documentazione del prodotto alla pagina https://docs.citrix.com.
- Cause dovute a qualsiasi componente non gestito da Citrix, inclusi, a titolo esemplificativo ma non esaustivo, macchine fisiche e virtuali controllate dal cliente, sistemi operativi installati e gestiti dal cliente, apparecchiature di rete o altro hardware installati e controllati dal cliente; impostazioni di sicurezza definite e controllate dal cliente, criteri di gruppo e altri criteri di configurazione; errori del provider di cloud pubblico, errori del provider di servizi Internet o altri fattori esterni al controllo Citrix.

- Interruzione del servizio dovuta a motivi al di fuori del controllo di Citrix, tra cui calamità naturali, guerre o atti di terrorismo, azioni governative.

### Ulteriori informazioni

- Diagrammi Citrix DaaS
- Architettura di riferimento e metodi di distribuzione di Citrix DaaS
- Panoramica sulla sicurezza tecnica
- Porte di rete
- Avvisi di terze parti
- Requisiti di sistema
- Features
  - Un'introduzione alle tecnologie HDX, oltre a dettagli su dispositivi, grafica ed elementi multimediali.
  - Remote PC Access (Accesso remoto PC): consente agli utenti di accedere in remoto da qualsiasi luogo a un PC fisico dell'ufficio. È possibile configurare Remote PC Access (Accesso remoto PC) da Full Configuration (Configurazione completa) o Quick Deploy (Distribuzione rapida).
  - Publish content (Pubblica contenuto): pubblica un'applicazione che è semplicemente un percorso URL o UNC per una risorsa.
  - Server VDI (VDI server): fornisce un desktop da un sistema operativo server per un singolo utente.
- Per Citrix DaaS Standard per Azure, consultare la documentazione del prodotto dedicata.
- Per informazioni sulla disponibilità delle funzionalità nei prodotti e nelle edizioni Citrix DaaS, consultare la matrice delle funzionalità di Citrix DaaS.
- Citrix Cloud Learning Series offre corsi di formazione per spiegare agli utenti come usare Citrix Cloud e i relativi servizi. È possibile visualizzare in sequenza tutti i moduli, dalle presentazioni ai servizi di pianificazione e creazione. È inoltre possibile scegliere singoli moduli o segmenti specifici dell'attività all'interno di un modulo. Vedere Cloud Learning Series.

### Per iniziare

Per informazioni su come configurare la distribuzione, iniziare con Pianificare e creare una distribuzione. Questo riepilogo guida l'utente nei passaggi principali del processo e fornisce collegamenti a ulteriori informazioni e procedure dettagliate.

# Novità

December 18, 2023

Uno degli obiettivi di Citrix è fornire nuove funzionalità e aggiornamenti dei prodotti ai clienti Citrix DaaS quando sono disponibili. Le nuove versioni offrono più valore, quindi non c'è motivo di ritardare gli aggiornamenti. Vengono rilasciati aggiornamenti periodici di Citrix DaaS ogni tre settimane circa.

Questo processo è trasparente per l'utente. Gli aggiornamenti iniziali vengono applicati solo ai siti interni di Citrix e quindi gradualmente anche agli ambienti dei clienti. La distribuzione incrementale a ondate degli aggiornamenti aiuta a garantire la qualità del prodotto e a offrire la massima disponibilità.

Per dettagli sul Service Level Agreement per la scalabilità del cloud e la disponibilità del servizio, vedere Accordo sui livelli di servizio. Per monitorare le interruzioni del servizio e la manutenzione programmata, vedere Service Health Dashboard.

## Virtual Delivery Agent (VDA)

I VDA per macchine Windows vengono generalmente rilasciati contemporaneamente al prodotto Citrix Virtual Apps and Desktops.

- Per informazioni sulle nuove funzionalità VDA e HDX, vedere gli articoli Novità e Problemi noti della versione corrente di Citrix Virtual Apps and Desktops.
- Per informazioni sulle piattaforme e sulle funzionalità VDA non più supportate, vedere Deprecazione. Questo articolo include anche piattaforme e funzionalità per le quali è pianificata l'interruzione del supporto in una versione futura (ad esempio quali sistemi operativi supportano l'installazione di VDA).

> **Importante:**
>
> Se su un VDA era stato installato il componente Personal vDisk (PvD), tale VDA non può essere aggiornato alla versione 1912 LTSR o successiva. Per utilizzare il nuovo VDA, è necessario disinstallare il VDA corrente e quindi installare il nuovo VDA. Questa istruzione vale anche se si è installato PvD senza mai usarlo. Per i dettagli, vedere Se sui VDA è installato Personal vDisk.

## novembre 2023

### Funzionalità nuove e migliorate

**Limiti di configurazione modificati**. La tabella seguente descrive le modifiche apportate ai limiti di configurazione di DaaS per migliorare le prestazioni e garantire la convenienza.

| Risorsa | Limite precedente | Nuovo limite |
|---|---|---|
| Domini di Active Directory | 85 | 100 |
| Cataloghi | 1000 | 2000 |
| Gruppi di consegna | 1000 | 2000 |
| Posizione risorsa | 85 | 100 |
| Posizione delle risorse -> Sessioni totali | 20,000 | 25,000 |

Per maggiori informazioni, vedere Limiti.

**Un'unica opzione per conservare la macchina virtuale e il disco di sistema durante i cicli di alimentazione.** L'avvio di una macchina virtuale esistente in Azure è ora più rapido del lancio di una nuova macchina virtuale: una scelta più efficiente per conservare le macchine virtuali durante i cicli di alimentazione. In risposta a questa modifica, abbiamo combinato le opzioni **Retain VM across power cycles**(Conserva la VM per tutti i cicli di alimentazione) e **Retain system disk during power cycles** (Conserva il disco di sistema durante i cicli di alimentazione) in un'unica opzione **Retain VM and system disk during power cycles** (Conserva la VM e il disco di sistema durante i cicli di alimentazione). Ciò significa che quando si seleziona questa opzione per ridurre i tempi di riavvio delle VM conservando i dischi di sistema, vengono mantenute anche le macchine virtuali.

**Nuova funzionalità di Full Configuration per filtrare le dimensioni delle macchine in base alla *proprietà di crittografia sull'host* nei profili delle macchine (specifiche per le macchine virtuali di Azure).** Dopo aver scelto un profilo macchina con *Encryption at Host* abilitata durante la creazione o la gestione del catalogo delle macchine di Azure, vengono visualizzate solo le dimensioni delle macchine che supportano questa funzionalità.

**Limitare le azioni di backup e ripristino al ruolo di amministratore completo.** Abbiamo migliorato il controllo degli accessi per le azioni di backup e ripristino. Solo gli utenti con il ruolo di amministratore completo possono ora accedere al nodo **Backup + Restore**, impedendo azioni non autorizzate.

**Memorizzazione nella cache dei dati per il nodo di ricerca.** Abbiamo introdotto la memorizzazione nella cache dei dati per il nodo **Search** di Citrix DaaS. Questo potenziamento migliora le prestazioni della ricerca e di seguito sono elencati i casi d'uso che semplificano le attività regolari:

- Visualizzazione rapida dei risultati della ricerca dopo che sono stati richiamati per la prima volta.
- Vengono conservati i risultati dell'impaginazione dopo che si è usciti dalla pagina del nodo **Search** e vi si è tornati.

**Informazioni sulle immagini nella pagina Machine Catalogs**. È ora possibile visualizzare le seguenti informazioni sull'immagine tramite l'opzione **Template Properties** (Proprietà del modello) del catalogo di macchine:

- Sistema operativo
- Servizio di identità macchina
- Archiviazione di Machine Creation Service
- Percorso di file di `pagefile.sys` per le distribuzioni di Azure.

Questo miglioramento fornisce una maggiore chiarezza delle informazioni sull'immagine e garantisce che gli amministratori dispongano di tutte le informazioni sul catalogo delle macchine in un unico posto.

**Supporto del blocco dei filtri di ricerca**. Per fornire un'esperienza di ricerca rapida, Full Configuration consente di bloccare i filtri di ricerca. Le puntine di blocco dei filtri consentono di mantenere accessibili sulla pagina i filtri di ricerca utilizzati di frequente. Questo miglioramento è disponibile nei pannelli di ricerca dei seguenti nodi:

- **Cerca**
- **Cataloghi di macchine**
- **Gruppi di consegna**
- **Applicazioni**

Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Supporto dell'associazione di metadati con i log di configurazione**. Utilizzando questo miglioramento, ora è possibile allegare metadati ai log di configurazione associando una coppia `name-value` alle operazioni di alto livello. Per ulteriori informazioni, vedere Associare i metadati ai registri di configurazione.

**Ignorare le risorse orfane con un tag specifico**. Negli ambienti Azure, una risorsa gestita dal cliente contrassegnata con tutti i tag Citrix viene rilevata come risorsa orfana. Con questa funzinalità, se si aggiunge a quella risorsa un altro tag `CitrixDetectIgnore` con valore true, la risorsa viene ignorata durante il rilevamento delle risorse orfane.

**Soluzione per il problema del GUID duplicato SCCM**. Dopo aver creato più macchine virtuali utilizzando MCS, System Center Configuration Manager (SCCM) ha visualizzato solo una macchina virtuale sulla sua console a causa dei GUID duplicati. Questo problema viene ora risolto aggiungendo un passaggio nella preparazione dell'immagine. Questo passaggio elimina i certificati e le informazioni GUID esistenti all'interno dell'immagine master. Il passaggio è abilitato per impostazione predefinita.

**Ripristinare le informazioni sull'identità degli account computer attivi**. Con questa funzione, è possibile reimpostare le informazioni sull'identità degli account computer attivi che presentano problemi correlati all'identità. È possibile scegliere di reimpostare solo la password della macchina e le chiavi di attendibilità o ripristinare tutta la configurazione del disco di identità. Questa implementazione è applicabile ai cataloghi di macchine sia persistenti che non persistenti. Attualmente, la funzionalità è supportata solo per gli ambienti di virtualizzazione Azure e VMware. Per ulteriori informazioni, vedere Ripristinare le informazioni sull'identità degli account computer attivi.

**Ottenere la crittografia delle informazioni sull'host associate a un profilo macchina**. In ambienti Azure, con questa funzionalità ora è possibile sapere se la crittografia sull'host è abilitata per l'input di un profilo macchina (VM o specifiche di modello) utilizzando i comandi PowerShell. Per ulteriori informazioni, vedere Recuperare le informazioni sulla crittografia dell'host da un profilo macchina.

**Riparare i certificati utente delle identità ibride delle macchine aggiunte ad Azure AD**. Con questa funzionalità, è possibile utilizzare il comando PowerShell per riparare i certificati utente delle identità ibride delle macchine aggiunte ad Azure AD se sono danneggiate o scadute. Per ulteriori informazioni, vedere Creare cataloghi aggiunti ad Azure Active Directory ibrido.

È possibile eseguire il comando `Get-ProvScheme` per ottenere informazioni sulla data di scadenza del certificato utente di un catalogo di macchine aggiunto ad Azure AD ibrido.

**Supporto delle macchine virtuali riservate di Azure**. Le macchine virtuali di Azure con elaborazione riservata garantiscono che il desktop virtuale sia crittografato in memoria e protetto durante l'uso. Con questa funzionalità, ora è possibile usare MCS per creare un catalogo con macchine virtuali riservate di Azure. È necessario utilizzare il flusso di lavoro del profilo macchina per creare un catalogo di questo tipo. È possibile utilizzare una macchina virtuale e una specifica di modello ARM come input del profilo macchina. Per ulteriori informazioni, vedere VM riservate di Azure (anteprima).

**Supporto della conversione di un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina in ambiente AWS**. In un ambiente AWS è ora possibile utilizzare una VM o un modello di avvio come input per il profilo macchina per convertire un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina. Le nuove macchine virtuali aggiunte al catalogo prendono i valori delle proprietà dal profilo macchina. Per ulteriori informazioni, vedere Convertire un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina.

**Supporto del plug-in HPE Moonshot gestito da Citrix (anteprima)**. In precedenza, si utilizzava il plug-in Moonshot gestito da HPE (HPE Moonshot Machine Manager) gestito da Hewlett Packard Enterprise (HPE) per eseguire le azioni di gestione dell'alimentazione sullo chassis HPE Moonshot. Il plug-in era basato su API legacy che rendevano difficili i progetti su infrastruttura MCS. Con questa funzionalità, viene introdotto un plug-in HPE Moonshot (HPE Moonshot) gestito da Citrix. Con questo plug-in, è possibile creare connessioni allo chassis HPE Moonshot, creare cataloghi e gestire l'alimentazione delle macchine incluse nel catalogo utilizzando l'interfaccia Full Configuration e i comandi PowerShell. Per ulteriori informazioni, vedere:

- Ambienti di virtualizzazione HPE Moonshot (anteprima)
- Connessione a HPE Moonshot (anteprima)
- Creare un catalogo di macchine di HPE Moonshot (anteprima)
- Gestire un catalogo di HPE Moonshot (anteprima)

**Possibilità di modificare la dimensione della memoria e della cache del disco**. Con questa funzionalità, è ora possibile modificare la dimensione della memoria e della cache su disco della cache di write-back (quando MCSIO è abilitato) utilizzando un comando PowerShell senza creare un nuovo catalogo di macchine. Questa implementazione consente di avere la configurazione della cache ottimizzata adatta alle esigenze aziendali. Questa funzionalità è applicabile a:

- Ambienti GCP e Microsoft Azure e
- un catalogo non persistente con MCSIO abilitato

Per ulteriori informazioni, vedere Modificare la configurazione della cache su un catalogo di macchine esistente.

**Supporto della creazione di un catalogo abilitato alla chiave di crittografia gestita dal cliente**. Negli ambienti Azure, è ora possibile creare un catalogo Citrix Provisioning abilitato con chiave di crittografia gestita dal cliente (CMEK) utilizzando l'interfaccia Full Configuration e i comandi PowerShell. Per ulteriori informazioni, vedere Creare un catalogo abilitato per le chiavi di crittografia gestite dal cliente.

**Possibilità di copiare i tag su tutte le risorse in Azure**. Con questa funzionalità, in ambiente Azure è ora possibile copiare i tag specificati in un profilo macchina per tutte le risorse, ad esempio più NIC e dischi (disco del sistema operativo, disco di identità e disco della cache di write-back) di una nuova macchina virtuale o di una macchina virtuale esistente inclusa in un catalogo di macchine.

L'origine del profilo macchina può essere una VM o una specifica di modello ARM. Per ulteriori informazioni, vedere Copiare i tag su tutte le risorse.

**Stato della sessione aggiornato a disconnesso dopo la sospensione della macchina**. In precedenza, dopo aver sospeso una macchina virtuale, la sessione veniva ancora visualizzata come **attiva**. Con questo miglioramento, dopo aver sospeso una macchina virtuale, lo stato della sessione associata viene ora visualizzato come **Disconnessa**.

**Supporto della creazione di macchine virtuali AWS che supportano l'ibernazione**. Ora è possibile creare cataloghi di macchine che supportano l'ibernazione delle macchine virtuali negli ambienti AWS, migliorando l'economicità complessiva della distribuzione. È inoltre possibile modificare un catalogo perché includa le VM compatibili con l'ibernazione se il profilo macchina associato supporta questa funzionalità. Per ulteriori informazioni, veder Gestire l'alimentazione delle VM di AWS.

**Supporto della configurazione dei metodi di bilanciamento del carico a livello di gruppo di consegna (anteprima)**. Questa funzione consente di scegliere il metodo di **Vertical Load Balancing** (Bilanciamento del carico verticale) a livello di gruppo di consegna. Con questa funzione, ciascuna

macchina viene allineata all'indice di carico massimo prima dell'accensione della macchina successiva. Autoscale e l'opzione Vertical Load Balancing determinano quando viene accesa la macchina successiva. Questa funzionalità consente di ottenere il massimo utilizzo per ogni macchina e risparmi sui costi nei cloud pubblici. Questa funzionalità offre una maggiore flessibilità nella gestione delle strategie di bilanciamento del carico per le macchine.

È possibile configurare un gruppo di consegna in modo che erediti il metodo di bilanciamento del carico dalle impostazioni a livello di sito o ignorare il metodo di bilanciamento del carico a livello di sito, per scegliere invece il metodo di bilanciamento del carico verticale od orizzontale. Per ulteriori informazioni, vedere Passaggio 2. Bilanciamento del carico.

**Supporto delle macchine virtuali con funzionalità di ibernazione in Azure (anteprima)**. Negli ambienti Azure, è possibile creare un catalogo di macchine MCS che supporti l'ibernazione. Utilizzando questa funzionalità, è possibile sospendere una macchina virtuale e riconnettersi allo stato precedente della macchina virtuale quando un utente accede nuovamente. Per ulteriori informazioni, vedere Creare macchine virtuali compatibili con l'ibernazione (anteprima).

**Guida introduttiva di DaaS.** Abbiamo lanciato una nuova guida per snellire e semplificare l'implementazione e la configurazione di DaaS sia per gli amministratori nuovi che per quelli esperti. Offre i seguenti vantaggi chiave:

- **Iniziare è facile.** Mediante un approccio dettagliato basato su domande, questa guida aiuta i nuovi amministratori a configurare rapidamente le proprie implementazioni. Le informazioni di aiuto contestuali contenute nella guida aiutano a comprendere i concetti e la terminologia essenziali.
- **Semplifica le configurazioni complesse.** Questa guida include impostazioni preconfigurate, ove applicabile, e fornisce l'accesso all'interfaccia utente Full Configuration per la configurazione avanzata. Gli amministratori esperti possono utilizzarla come base per configurazioni più complesse.

Per ulteriori informazioni, vedere la guida Utilizzare la guida introduttiva di DaaS.

**È possibile assegnare le lettere di unità ai dischi della cache di write-back utilizzando Full Configuration.** In precedenza, era possibile assegnare una lettera di unità specifica al disco della cache di write-back solo utilizzando un cmdlet PowerShell. Ora è possibile eseguire la stessa operazione con Full Configuration. Per ulteriori informazioni, vedere Creare cataloghi delle macchine.

**Supporto per la modifica di varie proprietà delle macchine Azure utilizzando Full Configuration.** Per le macchine Azure il cui provisioning è effettuato da Machine Creation Services, ora è possibile modificare le seguenti impostazioni delle proprietà mediante Full Configuration:

- Tipo di archiviazione
- Gruppo host dedicato
- Impostazioni della Raccolta di calcolo di Azure

Quando si modifica una di queste impostazioni, Full Configuration identifica automaticamente le impostazioni pertinenti e fornisce la sincronizzazione automatica o messaggi di richiesta che richiedono di riselezionare le impostazioni pertinenti. Questa funzionalità garantisce modifiche coerenti tra le impostazioni associate, prevenendo potenziali errori di configurazione. Per ulteriori informazioni, vedere Modificare un catalogo.

**Utilizzare i pool di identità esistenti per creare identità per le macchine con provisioning effettuato da MCS.** Quando si creano cataloghi aggiunti ad AD o vi si aggiungono macchine utilizzando Full Configuration, è ora possibile utilizzare un pool di identità esistente per allocare le identità delle macchine. Questa funzionalità consente di applicare uno schema coerente di denominazione degli account delle macchine su più cataloghi. Per ulteriori informazioni, vedere Identità macchina.

**Topologia della sessione.** La vista Session Topology è il passo successivo verso il miglioramento dei flussi di lavoro di risoluzione problemi in Monitor. La vista Session Topology fornisce una rappresentazione visiva del percorso all'interno della sessione per le sessioni HDX connesse. È possibile accedere alla vista della topologia da **User Details > Session Performance** (Dettagli utente > Prestazioni della sessione).

La vista Session Topology di una sessione connessa HDX mostra i componenti coinvolti nel percorso della sessione con i relativi metadati, il collegamento tra i componenti e le applicazioni pubblicate sul VDA. Inoltre, le misurazioni ICA Latency e ICA RTT vengono visualizzate per la sessione quando è in uno stato connesso.

Utilizzare la vista Session Topology per comprendere attraverso quali componenti fluiscono i dati della sessione e per identificare l'hop specifico che potrebbe causare problemi di prestazioni. Per ulteriori informazioni, vedere Topologia della sessione.

## ottobre 2023

### Funzionalità nuove e migliorate

**Perfezionare le impostazioni di Autoscale utilizzando l'utilizzo cronologico.** Una nuova scheda delle impostazioni di Autoscale, denominata **Autoscale Insights**, offre un grafico completo che confronta visivamente le impostazioni di Autoscale e i dati di utilizzo della macchina della settimana precedente. Con questo grafico, è possibile ottenere informazioni sull'efficacia delle impostazioni di Autoscale:

- **Not cost-effective** (Non conveniente). Lo spreco finanziario è dovuto all'eccesso di provisioning della capacità.
- **Poor user experience** (Esperienza utente scadente). L'esperienza utente è influenzata negativamente a causa del provisioning insufficiente della capacità.
- **Good balance between user experience and cost** (Buon equilibrio tra esperienza utente e costi). La capacità offerta in provisioning è in linea con l'utilizzo storico.

Per ulteriori informazioni, vedere Analizzare l'efficacia delle impostazioni di Autoscale.

**Supporto di più NIC per macchine virtuali di Azure.** Con Full Configuration, ora è possibile creare macchine virtuali Azure con più NIC. Il numero massimo di NIC di una VM è determinato dall'impostazione delle dimensioni della macchina, mentre il numero effettivo di NIC consentito è definito dall'impostazione del profilo macchina. Per ulteriori informazioni, vedere Creare cataloghi delle macchine.

Per creare o aggiornare un catalogo con più NIC per VM utilizzando i comandi PowerShell, vedere Creare o aggiornare un catalogo con più NIC per macchina virtuale.

**Tendenze delle metriche delle prestazioni delle sessioni.** Monitor introduce una nuova scheda **User Details > Session Performance** (Dettagli utente > Prestazioni di sessione) con flussi di lavoro di risoluzione dei problemi migliorati, a partire dalla capacità di mettere in correlazione le metriche in tempo reale per l'identificazione dei problemi all'interno delle sessioni utente. Session Experience ora contiene tendenze di metriche di sessione come ICARTT, Latenza ICA, fotogrammi al secondo, larghezza di banda in uscita disponibile e larghezza di banda in entrata consumata. Questa funzionalità aiuta a ridurre il tempo medio di risoluzione consentendo di mettere in correlazione più metriche delle prestazioni in un'unica visualizzazione. Per ulteriori informazioni, vedere l'articolo Problemi degli utenti.

**Supporta la versione VDA nella pagina delle impostazioni del criterio di creazione/modifica.** Nell'ambito della creazione di un criterio, durante la configurazione delle impostazioni, il sistema offre un'opzione per visualizzare il tipo di impostazioni. È possibile visualizzare il seguente tipo di impostazioni:

- All settings: visualizza tutte le impostazioni per tutte le versioni di VDA
- Current settings only: visualizza le impostazioni solo per le versioni VDA correnti
- Legacy settings only: visualizza le impostazioni solo per le versioni VDA deprecate

Per ulteriori informazioni, vedere Creare criteri

**Limita la visibilità delle applicazioni supportata solo per gli account Active Directory.** La funzionalità per limitare la visibilità delle applicazioni è disponibile solo per gli account utente di Active Directory e non per gli account Azure Active Directory e Okta. Tenere presente che, per facilitare questa funzionalità, nel flusso di lavoro di impostazione dell'applicazione, nella pagina Select Users or Groups (Seleziona utenti o gruppi), le opzioni **Azure ActiveDirectory** e **Okta** nel campo **Select Identity type** (Seleziona il tipo di identità) sono disabilitate.

**Nuova opzione dell'interfaccia utente per eliminare i record delle macchine virtuali solo dal database del sito Citrix.** Quando l'eliminazione di un catalogo e di una macchina virtuale non riesce perché un hypervisor è irraggiungibile, ora è possibile scegliere di limitarsi a eliminare i record delle macchine virtuali dal database del sito Citrix, lasciando le VM intatte sull'host. Per ulteriori informazioni, vedere Eliminare un catalogo.

**Supporto della creazione di cataloghi di macchine di cui non è stato eseguito il provisioning con MCS.** La creazione di cataloghi di macchine vuoti ora si estende alle macchine di cui non è stato eseguito il provisioning con MCS, tra cui:

- Macchine virtuali o blade il cui provisioning utilizza tecnologie diverse dai Machine Creation Services.
- Macchine fisiche con alimentazione non gestita da Citrix DaaS
- Macchine con Accesso remoto al PC

Con questa funzionalità, è ora possibile creare un catalogo di macchine senza la necessità di aggiungervi macchine mentre lo si crea.

**Miglioramenti all'aggiornamento dell'immagine.** In precedenza, durante l'aggiornamento delle immagini, venivano aggiornate tutte le immagini presenti nell'albero delle immagini, indipendentemente dal fatto che fosse selezionato o meno un nodo specifico nell'albero. Con l'ultimo miglioramento, se si è selezionato un nodo, vengono aggiornate solo le immagini presenti in questo nodo. Questo miglioramento garantisce un processo di aggiornamento più mirato, migliorando significativamente la velocità di aggiornamento dell'immagine. Inoltre, è ora possibile cancellare un nodo selezionato nell'albero delle immagini tenendo premuto CTRL e facendo clic sul nodo. Per ulteriori informazioni, vedere Immagine master.

**Accensione assegnata ad Autoscale negli orari di punta.** Quando i desktop persistenti sono accesi, ma rimangono inutilizzati, oppure nessun utente effettua l'accesso, gli amministratori possono definire il tempo di attesa per intraprendere azioni come nessuna azione, sospensione o arresto.

Nel caso delle macchine assegnate accese ma a cui non è stata collegata una sessione entro l'ora impostata dopo l'inizio dell'ora di punta, è possibile aggiungere un criterio a livello di gruppo di consegna per arrestare la macchina.

Nel caso delle macchine assegnate in stato ripreso ma a cui non è stata collegata una sessione entro l'ora impostata dopo l'inizio dell'ora di punta, è possibile aggiungere un criterio a livello di gruppo di consegna per arrestare la macchina.

Questa funzionalità è utile se c'è un utente finale che è in ferie/permesso o che non ha effettuato l'accesso o se un'azienda ha un weekend lungo; è quindi possibile impostare il tempo di attesa e le azioni di disconnessione della macchina da intraprendere per contribuire a ridurre i costi di consumo di Azure. Per ulteriori informazioni, vedere Gruppi di consegna casuale di sistemi operativi a sessione singola e Gruppi di consegna statici di sistemi operativi a sessione singola

**Monitorare più istanze di Citrix DaaS (anteprima).** Ora è possibile utilizzare Citrix Monitor per monitorare e risolvere i problemi su più istanze Citrix DaaS. Citrix DaaS consente ai clienti di aggregare più istanze di servizio utilizzando un modello hub e spoke. Con questa configurazione, gli amministratori possono eseguire ricerche nell'helpdesk su tutte le istanze DaaS configurate da un'unica console Monitor. Per ulteriori informazioni sulla configurazione richiesta per aggregare

le istanze del servizio spoke in un hub, vedere Aggregate multiple Citrix Virtual Apps and Desktops service instances. Monitor supporta l'aggregazione di un massimo di quattro tenant DaaS (spoke) in un singolo tenant DaaS (hub).
Per disporre di un monitoraggio unificato su tutti i tenant DaaS, utilizzare l'enumerazione bidirezionale delle istanze hub e spoke. Per ulteriori informazioni, vedere Ricerca aggregata su più istanze DaaS (anteprima).

**Supporto di vSAN 8.0** È ora possibile utilizzare MCS per effettuare il provisioning delle macchine virtuali nell'ambiente vSAN 8.0.

**Conservare le impostazioni delle NIC sulle macchine virtuali di cui è stato effettuato il provisioning.** In precedenza, le impostazioni NIC dell'immagine master non venivano mantenute nelle macchine virtuali di cui è stato effettuato il provisioning. Ad esempio, se sono state configurate le impostazioni DNS sull'immagine master, le macchine virtuali predisposte non hanno mantenuto le impostazioni DNS configurate dell'immagine master. Grazie a questa funzionalità, le macchine virtuali predisposte possono ora mantenere le impostazioni delle NIC dell'immagine master. Le impostazioni vengono mantenute anche dopo un aggiornamento di Windows. Il driver del filtro viene installato automaticamente se si esegue una nuova installazione del VDA versione 2308 o successiva su una macchina distribuita con Hyper-V tramite le installazioni di immagini master MCS. Tuttavia, attualmente, se si esegue l'aggiornamento da una versione precedente del VDA (versione precedente alla 2308) e si desidera installare il driver del filtro, è necessario selezionare la casella di controllo **Citrix HyperV Filter Driver** nella pagina **Additional Components** (Componenti aggiuntivi) durante l'aggiornamento del VDA. Per ulteriori informazioni, vedere Installare i componenti aggiuntivi.

Questa funzionalità è applicabile a:

- VM Hyper-V (inclusi Azure e SCVMM)
- Cataloghi di macchine MCS persistenti e non persistenti
- Cataloghi di macchine MCS non persistenti con MCSIO
- Immagine master con più NIC

**Rilevare risorse di Azure orfane**. Con questa funzionalità, ora è possibile rilevare le risorse orfane nella propria distribuzione di Azure, abilitando una gestione efficiente delle risorse. Una volta identificate le risorse orfane, è possibile intraprendere ulteriori azioni per aumentare la produttività e ridurre i costi. Per ulteriori informazioni, vedere Rilevare le risorse di Azure orfane nella propria distribuzione.

**Nuovo stato di aggiornamento dell'immagine.** Quando si monitorano gli stati di aggiornamento delle immagini per i cataloghi in Full Configuration, ora è possibile visualizzare un nuovo stato **Preparing image** (Immagine in preparazione), oltre agli stati esistenti **Fully updated** (Completamente aggiornata), **Partially updated** (Parzialmente aggiornata) e **Pending update** (In attesa di aggiornamento). Per ulteriori informazioni, vedere Cambiare l'immagine master.

**Comandi PowerShell per creare tag automatici (anteprima).** Con questa funzionalità è ora

possibile creare tag automaticamente utilizzando il comando PowerShell. Per ulteriori informazioni, vedere Tag automatici.

**Viene mostrato un segno di notifica all'utente o al gruppo di consegna**. Durante la creazione o la modifica di un criterio e la configurazione delle impostazioni, se tutti i gruppi di consegna sono disabilitati, il sistema visualizza l'avviso "None of the elements in this filter is enabled"(Nessuno degli elementi di questo filtro è abilitato). Se è abilitato almeno un gruppo di consegna, il sistema non visualizza il segnale di avviso. Per ulteriori informazioni, vedere Impostazioni dei criteri.

## settembre 2023

### Funzionalità nuove e migliorate

**Comandi PowerShell per gestire la cache host locale (LHC).** È ora possibile utilizzare i comandi PowerShell per gestire la LHC su Citrix Cloud Connectors. Per ulteriori informazioni, vedere Comandi PowerShell della cache host locale.

**Supporto della creazione di cataloghi di macchine vuoti.** In Full Configuration, è ora possibile creare un catalogo di macchine senza la creazione immediata di VM. Con questa funzionalità, è possibile posticipare la creazione di macchine virtuali finché gli host di back-end non sono stati completamente preparati o il provisioning delle macchine virtuali è stato completato, ottenendo una maggiore flessibilità nella creazione di cataloghi. Attualmente, questa funzionalità si applica solo ai cataloghi il cui provisioning è effettuato da Machine Creation Services. Per ulteriori informazioni, vedere Creare cataloghi delle macchine.

**Memorizzazione nella cache dei dati per il nodo Home.** Abbiamo introdotto la memorizzazione nella cache dei dati per il nodo **Home** di Citrix DaaS. Questa nuova funzionalità migliora l'esperienza utente riducendo i tempi di caricamento della pagina quando si accede al nodo **Home**.

**Miglioramenti della ricerca di applicazioni.** Abbiamo rinnovato la funzionalità di ricerca nel nodo **Applications** per allinearla al nuovo design introdotto nel nodo **Search** (Ricerca). Questa nuova funzionalità migliora l'esperienza di ricerca delle applicazioni e mantiene un'esperienza di ricerca coerente in tutte le parti di DaaS. La parola chiave **Application Name** nell'espressione del filtro viene rinominata in **Name**, pur mantenendo il suo significato originale. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Gestione avanzata dell'ambito: visualizzazione degli oggetti nella visualizzazione in cartelle.** Nelle pagine di creazione e gestione degli ambiti, i cataloghi di macchine, i gruppi di consegna e i gruppi di applicazioni vengono ora visualizzati in strutture di cartelle per allinearsi alla loro gestione in DaaS. Questa visualizzazione in cartelle semplifica il processo di selezione degli oggetti per la creazione e la gestione degli ambiti, rendendo le scelte più intuitive e dirette. Per ulteriori informazioni, vedere Creare e gestire ambiti.

**Rimossa l'opzione Leave user management to Citrix Cloud (Lascia la gestione degli utenti a Citrix Cloud).** Quando si crea un gruppo di consegna in Manage > Full Configuration, nella pagina Users, il supporto di questa opzione è stato rimosso. Per quanto riguarda i gruppi di consegna in cui le assegnazioni degli utenti sono state gestite tramite Citrix Cloud, continuare a gestire le assegnazioni utenti all'interno della libreria Citrix Cloud.

**È stata rimossa l'opzione Azure Germany.** In linea con la chiusura di Microsoft Cloud Deutschland il 29 ottobre 2021, abbiamo rimosso l'opzione **Azure Germany** dalla pagina di creazione della connessione host.

**Avvisi di servizio proattivi in Full Configuration.** Gli avvisi sono a due livelli: avvisi a livello di sito visualizzati in Home (icona a forma di bandiera) e avvisi relativi alla zona visualizzati nella scheda Troubleshoot (Risoluzione dei problemi) di ciascuna area. Attualmente, questa funzionalità offre avvertenze e avvisi proattivi per garantire che la cache dell'host locale e le zone siano configurate correttamente in modo che, in caso di interruzione, la cache dell'host locale funzioni e gli utenti non ne risentano. Per ulteriori informazioni, vedere Avvisi sullo stato del servizio e Zone.

## agosto 2023

### Funzionalità nuove e migliorate

**Full Configuration: supporto del provisioning di macchine virtuali AWS e GCP utilizzando i profili macchina.** Quando si esegue il provisioning di macchine virtuali AWS o GCP utilizzando Machine Creation Services (MCS), è ora possibile selezionare una macchina virtuale esistente come profilo macchina, lasciando che le macchine virtuali all'interno del catalogo ereditino le impostazioni dalla macchina virtuale selezionata.

- Nel caso delle macchine virtuali GCP, le impostazioni ereditate includono l'ID del set di crittografia del disco, la dimensione della macchina, il tipo di archiviazione e la zona.
- Nelle macchine virtuali AWS, le impostazioni ereditate variano in base alla fase:
  - Durante la creazione del catalogo: dimensioni della macchina, tipo di locazione, gruppo di sicurezza e numero di NIC.
  - Durante la modifica del catalogo: dimensione della macchina e gruppo di sicurezza.

Per ulteriori informazioni, vedere Creare un catalogo di macchine.

**Presentazione della funzionalità di ricerca nei nodi Machine Catalogs e Delivery Groups.** È ora possibile cercare e individuare direttamente i cataloghi di macchine e i gruppi di consegna all'interno dei nodi **Machine Catalogs** e **Delivery Groups**. La funzionalità di ricerca in questi nodi fornisce la stessa interfaccia del nodo **Search**, offrendo un'esperienza di ricerca senza interruzioni in tutto DaaS. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Visualizzare lo stato del dispositivo endpoint in Session Launch Diagnostics utilizzando Device Posture.** La funzionalità Session Launch Diagnostics di Monitor aiuta a restringere l'ambito della ricerca al componente esatto e alla fase in cui si è verificato l'errore della sessione. Questo aiuta a identificare il motivo esatto dell'errore di avvio di una sessione e a intraprendere l'azione consigliata.

Come passaggio successivo per rendere questo controllo completo su tutti i componenti coinvolti nella sequenza di avvio della sessione, è ora possibile visualizzare i risultati della scansione del dispositivo endpoint. Facendo clic su **Endpoint Device** (Dispositivo endpoint) nell'elenco dei componenti, viene visualizzato lo stato di scansione di Device Posture. Il servizio Device Posture esegue la scansione del dispositivo endpoint per verificare la conformità in base ai criteri definiti dall'amministratore.

Assicurarsi che il servizio Device Posture sia configurato con DaaS come descritto nell'articolo su Device Posture. Gli errori registrati da Device Posture sono descritti in Device Posture Error Logs.

Per ulteriori informazioni, vedere Passaggi per diagnosticare un errore di avvio della sessione

**Nuove opzioni in Full Configuration per indirizzare le richieste API verso Azure e GCP tramite Citrix Cloud Connectors.** In precedenza, le richieste API verso Azure e GCP potevano essere instradate solo tramite endpoint pubblici. Con una nuova opzione disponibile in **Full Configuration > Add Connection and Resources** (Configurazione completa > Aggiungi connessione e risorse), ora sarà possibile optare per un approccio più sicuro instradandoli tramite Citrix Cloud Connectors. Per ulteriori informazioni, vedere Creare un'entità servizio e una connessione utilizzando Full Configuration.

**Miglioramenti della ricerca e del filtro.** Abbiamo apportato i seguenti miglioramenti all'esperienza di ricerca:

- **Ricerca semplificata**: l'esecuzione di una ricerca senza filtri ora rimuove i consigli di ricerca, offrendo un'esperienza di ricerca pulita e diretta.
- **Aggiornamento dell'operatore AND/OR**: le opzioni "Match all(AND operator)"[Abbina tutto (operatore AND)] e "Match any(OR operator)"[Corrispondi a qualsiasi (operatore OR)] sono ora disponibili nel pannello dei filtri, accessibile con un solo clic sull'icona dei filtri.
- **Configurazione semplificata dei filtri**: ora è possibile specificare e applicare più filtri senza problemi con il pannello dei filtri.
- **Interfaccia più pulita**: la funzionalità di "ancoraggio dei filtri"è stata rimossa, semplificando l'interfaccia utente e rendendo l'esperienza di ricerca più intuitiva.
- **Aggiunta rapida filtro**: dopo aver applicato i filtri, ora è possibile utilizzare il segno più per aggiungere rapidamente un altro filtro.
- **Eliminare i set di filtri salvati**: ora è possibile eliminare facilmente i set di filtri salvati direttamente dal menu di ricerca, senza passare a **Manage filter sets** (Gestisci i set di filtri).

Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Supporto dell'aggiornamento VDA per i cataloghi di macchine creati da Azure Quick Deploy.** Con Full Configuration, ora è possibile abilitare **VDA Upgrade** (Aggiornamento VDA) per i cataloghi di macchine creati tramite Azure Quick Deploy e quindi eseguire **Upgrade VDA** su di essi per aggiornamenti immediati o pianificati. Per ulteriori informazioni, vedere Upgrade VDAs using the Full Configuration interface.

**Possibilità di reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di computer creato da MCS in SCVMM**. È ora possibile utilizzare il comando PowerShell `Reset-ProvVMDisk` per reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di macchine creato da MCS. La funzione automatizza il processo di ripristino del disco del sistema operativo. Ad esempio, aiuta a ripristinare la VM allo stato iniziale di un catalogo desktop di sviluppo persistente creato con MCS. Attualmente, questa funzionalità è applicabile agli ambienti di virtualizzazione Azure, Citrix Hypervisor, SCVMM e VMware. Per ulteriori informazioni sull'utilizzo del comando PowerShell per reimpostare il disco del sistema operativo, vedere Reimpostare il disco del sistema operativo.

**Aggiornare le proprietà delle singole macchine virtuali**. È ora possibile aggiornare le proprietà delle singole macchine virtuali incluse in un catalogo di macchine MCS persistente utilizzando un comando PowerShell. Questa implementazione consente di gestire le singole macchine virtuali in modo efficiente senza aggiornare l'intero catalogo di macchine. Attualmente, questa funzionalità è applicabile solo all'ambiente Azure. Per ulteriori informazioni, vedere Aggiornare le proprietà delle singole macchine virtuali.

**Limitare il caricamento e il download dei dischi gestiti**. In base ai criteri di Azure, non è possibile caricare o scaricare più di cinque dischi o snapshot allo stesso tempo con lo stesso oggetto di accesso al disco. Con questa funzionalità, il limite di cinque caricamenti o download simultanei non viene applicato se:

- si configura `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` e
- non si configurano i criteri di Azure per creare automaticamente accessi al disco in modo che ciascun nuovo disco utilizzi endpoint privati.

**Supporto dell'assegnazione di una lettera di unità specifica al disco di cache write-back MCS I/O**. In precedenza, il sistema operativo Windows assegnava automaticamente una lettera di unità al disco cache di write-back MCS I/O. Con questa funzionalità, ora è possibile assegnare una lettera di unità specifica al disco cache di write-back MCS I/O. Questa implementazione consente di evitare conflitti tra la lettera di unità di qualsiasi applicazione utilizzata e la lettera di unità del disco di cache write-back I/O MCS. Questa funzionalità è applicabile solo al sistema operativo Windows. Per ulteriori informazioni, vedere Assegnare una lettera di unità specifica al disco di cache write-back MCS I/O.

**Supporto del profilo macchina in Citrix Hypervisor**. In Citrix Hypervisor, è ora possibile creare un catalogo di macchine MCS utilizzando un profilo macchina. L'origine dell'input del profilo macchina è una macchina virtuale. Il profilo della macchina acquisisce le proprietà hardware da un modello di

VM e le applica alle macchine virtuali di cui è appena stato effettuato il provisioning nel catalogo. Per ulteriori informazioni, vedere Creare un catalogo di macchine utilizzando un profilo macchina.

**Supporto della creazione di un catalogo di macchine virtuali abilitate con Amazon Elastic Graphics**. Utilizzando un flusso di lavoro basato sul profilo macchina, è ora possibile creare un catalogo di macchine virtuali abilitate con l'acceleratore Grafica elastica Amazon. È possibile utilizzare una macchina virtuale e un modello di avvio come input del profilo macchina. Per ulteriori informazioni, vedere Creare un catalogo di macchine virtuali abilitate con l'acceleratore Grafica elastica.

**Riprovare a creare il catalogo dopo l'errore**. Quando la creazione del catalogo non riesce, ora è possibile riprovare a creare il catalogo. Per garantire una creazione corretta, controllare le informazioni sulla risoluzione dei problemi e risolvere i problemi. Le informazioni descrivono i problemi rilevati e forniscono consigli per risolverli. I cataloghi non riusciti sono contrassegnati da un'icona di errore. Per visualizzare i dettagli, passare alla scheda **Troubleshoot** (Risoluzione problemi) di ogni catalogo. Per ulteriori informazioni, vedere Gestire i cataloghi delle macchine.

**Autorizzazione per la gestione dei set di configurazione**. Per consentire un controllo più preciso sulla gestione dei set di configurazione WEM, abbiamo introdotto una nuova autorizzazione denominata **Manage configuration sets** (Gestisci set di configurazione) al set di autorizzazioni **Machine catalogs** (Cataloghi di macchine). Questa autorizzazione concede l'accesso esclusivo agli utenti che possono eseguire attività come l'associazione o la dissociazione di un set di configurazione e il passaggio a un set di configurazione diverso per i cataloghi. Per ulteriori informazioni, vedere Gestire il set di configurazione per un catalogo.

**Nuova opzione di Full Configuration per abilitare la pulizia dei dispositivi aggiunti ad Azure AD obsoleti**. Abbiamo introdotto in Full Configuration un'opzione per semplificare la pulizia dei dispositivi obsoleti aggiunti ad Azure AD in Citrix DaaS. In precedenza, era necessario eseguire uno script PowerShell personalizzato per eseguire l'operazione. L'attivazione di questa opzione concede alle connessioni host l'autorizzazione a pulire automaticamente i dispositivi aggiunti ad Azure AD obsoleti. Per ulteriori informazioni, vedere Connessioni host di Azure.

**Monitorare lo stato di aggiornamento delle immagini per i cataloghi utilizzando Full Configuration.** È ora possibile monitorare gli stati di aggiornamento delle immagini per i cataloghi di macchine non persistenti utilizzando una nuova colonna: **Image Update**. Questa colonna indica se le immagini di un catalogo sono **Fully updated** (Completamente aggiornate), **Partially updated** (Parzialmente aggiornate) o **Pending update** (In attesa di aggiornamento).

Per visualizzare la colonna nella tabella **Machine Catalogs** (Cataloghi macchine), effettuare le seguenti operazioni:

1. Nel nodo **Machine Catalogs**, selezionare l'icona **Columns to Display** (Colonne da visualizzare) nella barra delle azioni.
2. Selezionare **Machine Catalog > Image Status** (Catalogo di macchine > Stato dell'immagine).
3. Fare clic su **Salva**.

La visualizzazione della colonna di **Image update** potrebbe ridurre le prestazioni della console. Se ne consiglia la visualizzazione solo quando necessario.

**Ambiente sicuro per il traffico gestito di GCP.** Con questa funzione, ora è possibile consentire l'accesso solo privato di Google ai propri progetti Google Cloud. Questa implementazione migliora la sicurezza per la gestione dei dati sensibili. A tale scopo, aggiungere `ProxyHypervisorTrafficThroughConne` a `CustomProperties` nel caso di un'implementazione di Citrix Cloud. Se si utilizza un pool di lavoratori privato, aggiungere `UsePrivateWorkerPool` in `CustomProperties`. Per ulteriori informazioni, vedere Creare un ambiente sicuro per il traffico gestito di GCP.

## luglio 2023

### Funzionalità nuove e migliorate

**Supporto dell'ottenimento di un elenco di risorse orfane in Azure.** Negli ambienti Azure, è ora possibile ottenere un elenco di risorse orfane create da MCS ma non più utilizzate da MCS. Questa funzionalità consente di evitare costi aggiuntivi. Per ulteriori informazioni, vedere Recuperare un elenco di risorse orfane.

**Supporto della creazione di macchine multisessione persistenti mediante Full Configuration.** Quando si crea un catalogo di macchine multisessione, è ora possibile specificare se renderle persistenti. Nel caso delle macchine multisessione persistenti, tenere presente che le modifiche apportate dagli utenti ai desktop vengono salvate e sono accessibili a tutti gli utenti autorizzati. Per ulteriori informazioni, vedere Creare cataloghi delle macchine.

**Nuova funzionalità di Full Configuration per filtrare l'inventario AMI AWS.** Quando si selezionano i modelli di macchina durante la creazione del catalogo AWS, è ora possibile filtrare l'inventario AMI AWS per un modello di destinazione utilizzando questi criteri di ricerca:

- Nome dell'immagine
- ID immagine
- Tag dell'immagine

L'elenco dei modelli di computer viene caricato dinamicamente mentre si scorre l'elenco verso il basso: inizialmente vengono caricati 25 elementi e se ne caricano altri mentre si scorre.

**Supporto dell'eliminazione dei dispositivi Azure AD.** Con questa funzionalità, i dispositivi Azure AD obsoleti possono essere eliminati in modo coerente assegnando il ruolo di amministratore dei dispositivi cloud all'entità servizio e modificando la proprietà personalizzata della connessione di hosting. Se non si eliminano i dispositivi AD di Azure non aggiornati, la macchina virtuale non persistente corrispondente rimane in stato di inizializzazione finché non viene rimossa manualmente dal portale di Azure AD. Per altre informazioni, vedere Creare cataloghi aggiunti ad Azure Active Directory.

**Supporto del profilo della macchina in ambiente AWS.** Quando si crea un catalogo per il provisioning delle macchine utilizzando Machine Creation Services (MCS) in AWS, è ora possibile utilizzare un profilo macchina per acquisire le proprietà hardware da un'istanza EC2 (VM) o da una versione del modello di avvio e applicarle alle macchine di cui è stato effettuato il provisioning. Le proprietà acquisite possono includere, ad esempio, le proprietà del volume EBS, il tipo di istanza, l'ottimizzazione EBS, la grafica elastica e altre configurazioni AWS supportate. Quando si modifica il catalogo, il profilo macchina delle macchine di cui è stato effettuato il provisioning può essere modificato fornendo una macchina virtuale o un modello di avvio diverso. Per ulteriori informazioni, vedere Creare un catalogo utilizzando un profilo macchina.

**Il limite di esportazione dei risultati di ricerca è stato esteso da 10.000 a 30.000**. Abbiamo esteso il limite di esportazione dei risultati di ricerca. In precedenza si limitava a 10.000 elementi, ma ora è possibile esportare fino a 30.000 elementi in un file CSV. Per ulteriori informazioni, vedere Esportare i risultati della ricerca in un file CSV.

**Opzione di aggiornamento dell'immagine.** Quando si selezionano le immagini master per i cataloghi di macchine, è ora possibile ottenere rapidamente l'elenco di immagini master più aggiornato utilizzando l'opzione **Refresh** in alto a destra. Tenere presente che l'opzione **Refresh** non è disponibile per i cataloghi AWS. È inoltre disponibile un'opzione **Refresh** per i profili di computer e i gruppi di host nei cataloghi di Azure.

## giugno 2023

### Funzionalità nuove e migliorate

**Supporto della possibilità di ottenere proprietà personalizzate dall'input del profilo della macchina in GCP.** In precedenza, negli ambienti GCP, durante la creazione di un catalogo di macchine MCS utilizzando un input di profilo macchina, era necessario specificare esplicitamente le proprietà personalizzate. L'azione ha richiesto uno sforzo supplementare. Con questa funzionalità, ora è possibile derivare le seguenti proprietà personalizzate senza definirle esplicitamente:

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

Quando si eseguono i comandi `New-ProvScheme` e `Set-ProvScheme` e non si specificano esplicitamente le proprietà personalizzate, i valori delle proprietà vengono derivati dall'input del profilo della macchina.

Ad esempio, `New-ProvScheme -MachineProfile` scrive il tipo di macchina del profilo macchina nella proprietà `ServiceOffering` dello schema di provisioning, a meno che non si speci-

fichi `ServiceOffering` nel comando `New-ProvScheme`. Se si esegue `Set-ProvVMScheme` due volte, ha effetto il comando più recente.

**Rimuovere i tag negli ambienti AWS.** In precedenza, i comandi `Remove-ProvVM` e `Remove-ProvScheme` di PowerShell con parametri `ForgetVM` rimuovevano le macchine virtuali e i cataloghi di macchine dal database Citrix. Tuttavia, i comandi non rimuovevano i tag. Era necessario gestire individualmente le macchine virtuali e i cataloghi di macchine che non erano stati rimossi completamente da tutte le risorse. Con questa funzionalità, è possibile utilizzare:

- `Remove-ProvVM` con il parametro `ForgetVM` per rimuovere macchine virtuali e tag da una singola macchina virtuale o un elenco di macchine virtuali da un catalogo di macchine.
- `Remove-ProvScheme` con il parametro `ForgetVM` per rimuovere un catalogo di macchine dal database Citrix e risorse da un catalogo di macchine.

Questa implementazione aiuta a:

- Identificare le risorse perse
- Eliminare i costi aggiuntivi di manutenzione delle risorse non necessarie

Questa funzionalità è applicabile solo alle macchine virtuali persistenti. Per ulteriori informazioni, vedere Rimuovere i tag.

**Capacità di ottenere la cronologia degli errori e degli avvisi associati a un catalogo di macchine MCS.** In precedenza, si ricevevano solo gli avvisi e gli errori più recenti associati a un catalogo di macchine. Con questa funzione, è ora possibile ottenere un elenco degli avvisi e degli errori storici di un catalogo di macchine MCS. Questo elenco consente di comprendere eventuali problemi relativi al catalogo delle macchine MCS e di risolverli.

Per ulteriori informazioni, vedere Recuperare gli avvisi e gli errori associati a un catalogo.

**Maggiore capacità con prestazioni migliorate per Citrix in Google Cloud.** Citrix può ora supportare cataloghi contenenti fino a 3.000 VDA in un singolo progetto Google Cloud. Questo aggiornamento apporta miglioramenti delle prestazioni in entrambe le operazioni di provisioning e di gestione dell'alimentazione.

**Possibilità di reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di computer creato da MCS in ambiente Google Cloud e AWS.** È ora possibile utilizzare il comando PowerShell `Reset-ProvVMDisk` per reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di macchine creato da MCS. La funzione automatizza il processo di ripristino del disco del sistema operativo. Ad esempio, aiuta a ripristinare la VM allo stato iniziale di un catalogo desktop di sviluppo persistente creato con MCS. Attualmente, questa funzionalità è applicabile agli ambienti di virtualizzazione AWS, Azure, Citrix Hypervisor, Google Cloud e VMware. Per ulteriori informazioni sull'utilizzo del comando PowerShell per reimpostare il disco del sistema operativo, vedere Reimpostare il disco del sistema operativo.

**Supporto della modifica delle proprietà personalizzate relative al disco di un catalogo esistente e delle VM esistenti in GCP.** In precedenza negli ambienti GCP era possibile aggiungere le proprietà personalizzate solo quando si creava il catalogo macchine MCS. Con questa funzionalità, è ora possibile modificare le seguenti proprietà personalizzate relative al disco di un catalogo esistente e delle VM esistenti del catalogo.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

Questa implementazione consente di selezionare diversi tipi di archiviazione per i diversi dischi anche dopo aver creato un catalogo e quindi di bilanciare i costi associati ai diversi tipi di archiviazione. Per ulteriori informazioni, vedere Modificare le proprietà personalizzate relative al disco di un catalogo esistente.

**Supporto del timeout dinamico della sessione esteso alla versione VDA 2203 LTSR CU3 o successiva.** Per i gruppi di consegna di sistemi operativi a sessione singola, questa funzionalità ora si applica ai VDA versione 2206 CR o successiva o 2203 LTSR CU3 o successiva. Per ulteriori informazioni, vedere Timeout dinamici delle sessioni.

**Esperienza di creazione della connessione host migliorata in Full Configuration.** Dopo aver selezionato una posizione di risorsa, l'elenco a discesa **Connection type** (Tipo di connessione) ora visualizza tutti gli hypervisor e i servizi cloud supportati da Citrix e la loro disponibilità dipende da:

- Per una posizione risorsa senza connettori cloud accessibili, sono disponibili solo hypervisor e servizi cloud che supportano le implementazioni senza connettori.
- Per una posizione risorsa con connettori cloud accessibili, sono disponibili solo gli hypervisor e i servizi cloud i cui plug-in sono installati correttamente su tali connettori.

Per ulteriori informazioni, vedere Creare e gestire le connessioni.

**Selezione di componenti aggiuntivi nell'aggiornamento del VDA**. È ora possibile selezionare quali componenti aggiuntivi aggiornare o installare durante l'aggiornamento di un VDA. Per ulteriori informazioni, vedere Configurare l'aggiornamento automatico per i VDA.

> **Importante:**
>
> Per utilizzare la funzionalità dei componenti aggiuntivi, assicurarsi che il proprio VDA Upgrade Agent sia la versione 7.34 o successiva, che inclusa nella versione 2206 o successiva del programma di installazione del VDA.

**Full Configuration ora preconfigura alcune impostazioni per le macchine Azure in base ai profili**

**delle macchine.** Quando si esegue il provisioning di macchine virtuali di Azure, Full Configuration ora preconfigura le seguenti impostazioni in base al profilo macchina selezionato:

- Gruppo host
- Set di crittografia disco
- Zona di disponibilità
- Tipo di licenza

**Supporto dell'ibernazione delle istanze AWS.** È ora possibile avviare le istanze AWS, impostarle come si desidera e ibernarle. Il processo di ibernazione memorizza lo stato in memoria dell'istanza, insieme ai relativi indirizzi IP privati ed elastici, consentendole di riprendere esattamente da dove era stata interrotta. Per ulteriori informazioni sulla creazione di macchine virtuali che supportano l'ibernazione, vedere Ibernazione delle istanze.

**Supporto dell'ottimizzazione della limitazione delle richieste di AWS Workspace.** Ora è possibile accendere e spegnere un numero elevato di macchine in un catalogo AWS senza riscontrare problemi di limitazione. I problemi di limitazione si verificano quando il numero di richieste inviate ad AWS supera il numero di richieste che il server è in grado di gestire. Questa funzionalità aumenta l'efficienza riducendo il numero di chiamate AWS di accensione e arresto di macchine in blocco. Inoltre, riduce significativamente il tempo necessario per accendere e arrestare le macchine nei cataloghi persistenti.

**Ambiente sicuro per il traffico gestito di Azure.** In precedenza, si faceva affidamento sulla rete Internet pubblica per consentire agli endpoint di Azure di interagire con le risorse del proprio ambiente. Di conseguenza, sono stati sollevati problemi di sicurezza legati all'accesso a Internet pubblico. Con questa funzionalità, MCS consente il routing del traffico di rete tramite Citrix Cloud Connectors nel proprio ambiente. Questo rende l'ambiente sicuro perché ora tutto il traffico gestito di Azure ha origine dal proprio ambiente. Per fare ciò, aggiungere `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`. Per ulteriori informazioni, vedere Creare un ambiente sicuro per il traffico gestito di Azure.

Dopo aver impostato le proprietà personalizzate, è possibile configurare i criteri di Azure per avere accesso privato ai dischi gestiti di Azure.

**Supporto del provisioning delle macchine virtuali del catalogo con l'agente di Monitoraggio di Azure.** L'agente di Monitoraggio di Azure (AMA) raccoglie i dati di monitoraggio e li fornisce all'agente di Monitoraggio di Azure. Con questa funzionalità, è possibile effettuare il provisioning delle VM del catalogo macchine MCS (persistenti e non persistenti) con AMA installato come estensione. Questa implementazione consente il monitoraggio identificando in modo univoco le VM nei dati di monitoraggio. Per ulteriori informazioni su AMA, vedere Panoramica dell'agente di Monitoraggio di Azure.

Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità. Per ulteriori informazioni sul provisioning delle VM del catalogo di macchine con AMA abilitato, vedere Effettuare il provisioning delle VM del catalogo con l'agente di Monitoraggio di Azure installato.

**Attivare la pianificazione del riavvio per un catalogo MCS.** In precedenza, era possibile pianificare gli aggiornamenti delle immagini attendendo il successivo riavvio o attivando un riavvio immediato di tutte le VM. Con questa funzionalità, è ora possibile creare una pianificazione di riavvio una tantum per l'attivazione di un catalogo nella data e nell'ora desiderate per facilitare gli aggiornamenti delle immagini MCS. Per creare una pianificazione di riavvio, utilizzare il comando `BrokerCatalogRebootSchedule`. Per ulteriori informazioni, vedere Cambiare l'immagine master.

**Gestire i segreti client scaduti in Azure Quick Deploy.** In Azure Quick Deploy, è ora possibile rimanere informati con avvisi quando scadono i segreti client e aggiornarli facilmente per garantire l'accesso continuo alle risorse di Azure. Per ulteriori informazioni, vedere Aggiornare i segreti del client scaduti.

## maggio 2023

### Funzionalità nuove e migliorate

**Miglioramenti della ricerca**. Questa funzionalità migliora la grafica e le interazioni per i filtri, offrendo un'esperienza di ricerca migliore. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Nuovo criterio di esclusione degli utenti in cui è possibile definire percorsi di directory che non vengono reindirizzati al livello utente.** Le esclusioni utente si applicano al livello di personalizzazione dell'utente (UPL), ma non all'host della sessione. Logoff.txt ora contiene tutte le esclusioni utente attive. Per ulteriori informazioni, vedere Livello di personalizzazione utente.

**Supporto dell'aggiornamento della versione hardware delle nuove VM aggiunte in un catalogo di macchine MCS.** Negli ambienti VMware, è ora possibile aggiornare la versione hardware delle macchine virtuali appena aggiunte a un catalogo di macchine MCS esistente utilizzando un'origine del profilo della macchina. Non è necessario creare un nuovo catalogo di macchine per aggiornare la versione hardware delle macchine virtuali aggiunte a un catalogo. È necessario utilizzare il flusso di lavoro del profilo macchina per utilizzare questa funzionalità.

**Supporto del filtraggio delle istanze di macchine virtuali AWS.** In precedenza, quando si utilizzava un'istanza di macchina virtuale AWS come input del profilo macchina per creare un catalogo di macchine MCS, il catalogo a volte non veniva creato o non funzionava correttamente a causa di un input di profilo macchina non valido. Con questa funzionalità, è ora possibile elencare le istanze di macchine virtuali AWS che possono essere utilizzate come macchine virtuali con profilo macchina valide. Per fare ciò, utilizzare il comando `Get-HypInventoryItem`. Per ulteriori informazioni, vedere Filtrare le istanze di macchine virtuali.

**Supporto della conversione di un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina in ambiente Azure.** Nell'ambiente Azure, è ora

possibile utilizzare una VM o una specifica di modello come input per il profilo della macchina per convertire un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina. Le VM esistenti e le nuove VM aggiunte al catalogo prendono i valori delle proprietà dal profilo della macchina, a meno che non vengano sovrascritti da proprietà personalizzate esplicite. Per ulteriori informazioni, vedere Convertire un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina.

**Supporto della doppia crittografia su disco gestito in ambiente Azure.** In ambiente Azure, è ora possibile creare un catalogo di macchine con doppia crittografia. La doppia crittografia è la crittografia lato piattaforma (impostazione predefinita) e la crittografia gestita dal cliente (CMEK). Pertanto, se si è un cliente altamente sensibile alla sicurezza e si nutre preoccupazione per il rischio associato a qualsiasi algoritmo di crittografia, implementazione o chiave compromessa, è possibile optare per questa doppia crittografia. Il sistema operativo persistente e i dischi di dati, le snapshot e le immagini sono tutti crittografati quando inattivi con doppia crittografia. Per ulteriori informazioni, vedere Doppia crittografia su disco gestito.

**Supporto del profilo della macchina in VMware.** Negli ambienti VMware, è ora possibile creare un catalogo di macchine MCS utilizzando un profilo macchina. L'origine dell'input del profilo della macchina è un modello VMware. Il profilo della macchina acquisisce le proprietà hardware da un modello VMware e le applica alle macchine virtuali di cui è appena stato effettuato il provisioning nel catalogo. Per ulteriori informazioni, vedere Creare un catalogo di macchine utilizzando un profilo macchina.

**Possibilità di reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di macchine creato da MCS in Azure e Citrix Hypervisor.** È ora possibile utilizzare il comando PowerShell `Reset-ProvVMDisk` per reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di macchine creato da MCS. La funzione automatizza il processo di ripristino del disco del sistema operativo. Ad esempio, aiuta a ripristinare la VM allo stato iniziale di un catalogo desktop di sviluppo persistente creato con MCS. Attualmente, questa funzionalità è applicabile agli ambienti di virtualizzazione Azure, Citrix Hypervisor e VMware. Per ulteriori informazioni sull'utilizzo del comando PowerShell per reimpostare il disco del sistema operativo, vedere Reimpostare il disco del sistema operativo.

**Esperienza di creazione della connessione host migliorata.** È ora possibile ottenere le seguenti informazioni durante la creazione di una connessione host:

- Elenco di tutti i plug-in hypervisor supportati da Citrix, inclusi i plug-in di terze parti
- Disponibilità del plugin hypervisor. Se lo stato di disponibilità è false, il possibile motivo potrebbe essere che Cloud Connector non è installato.

Questa funzione consente di configurare correttamente la posizione di una risorsa e quindi di creare una connessione host. Per ulteriori informazioni, vedere il Passaggio 1. Connessione.

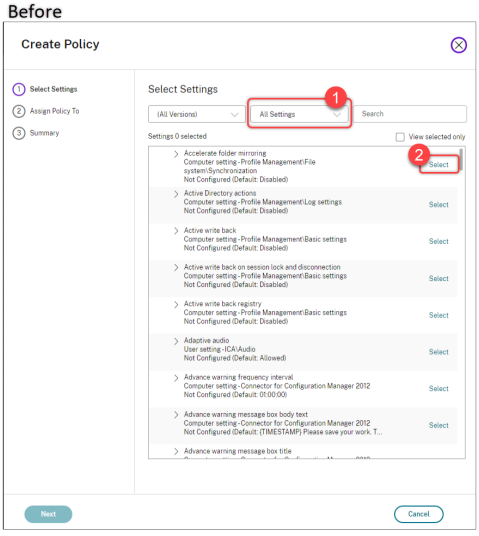
**Miglioramenti dell'esperienza utente per il nodo Policies (Criteri).** Per migliorare l'esperienza

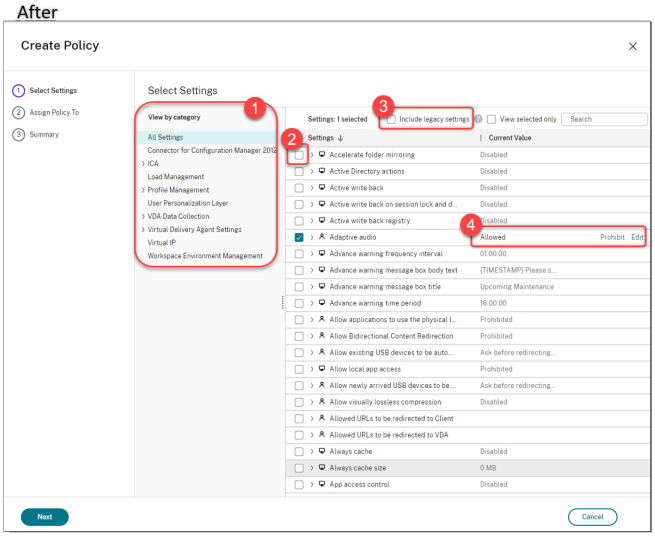
utente e rendere più efficiente la gestione dei criteri, abbiamo implementato i seguenti miglioramenti al nodo **Full Configuration > Policies**:

- Nuovo design dell'interfaccia utente per le azioni **Create Policy** (Crea criterio) e **Create Template** (Crea modello):
  - Visualizzazione delle cartelle espandibile per le impostazioni dei criteri. Nella pagina **Select Settings** (Seleziona impostazioni), tutte le impostazioni vengono visualizzate per categoria in una vista ad albero espandibile, che semplifica la ricerca di un'impostazione.
  - Per selezionare un'impostazione, è sufficiente fare clic su una casella di controllo anziché utilizzare il pulsante **Select**.
  - Le impostazioni precedenti sono state nascoste per impostazione predefinita in modo che vengano visualizzate solo le impostazioni più pertinenti. Se sono necessarie impostazioni precedenti, selezionare **Include legacy settings** (Includi impostazioni precedenti).
  - È stato aggiunto un pulsante di azione accanto a un'impostazione booleana, per consentire di modificarne il valore direttamente nell'elenco delle impostazioni.

Before

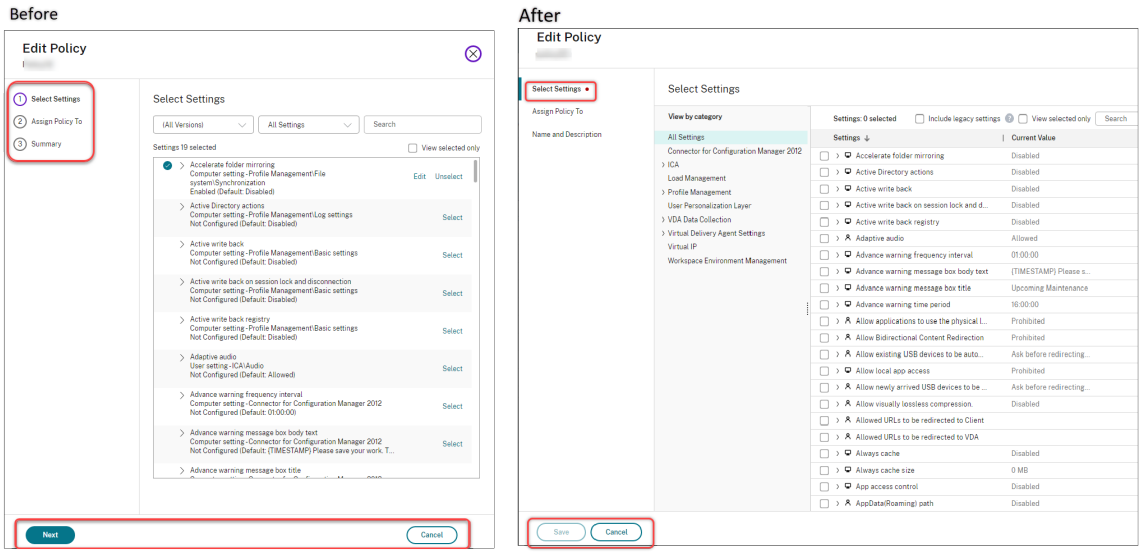



After




- Nuovo design dell'interfaccia utente per l'azione **Edit Policy** (Modifica criterio):
  - Il menu di navigazione è stato aggiornato in un elenco non ordinato. Ogni elemento dell'elenco ora include un pulsante **Save** nella relativa pagina. Con questo nuovo design, è possibile salvare le modifiche apportate a un elemento senza dover passare per tutti gli elementi del menu di navigazione. Questi miglioramenti rendono la gestione dei criteri più efficiente e semplice.
  - Accanto agli elementi di navigazione vengono visualizzati dei punti rossi per indicare gli errori di impostazione.




- Trascinare per riassegnare le priorità ai criteri. Nell'elenco delle priorità, è ora possibile modificare la priorità di un criterio trascinandolo nella posizione desiderata.

**Nuova opzione per disattivare lo scollegamento forzato dell'utente per AutoScale.** È ora disponibile la nuova opzione **Neither notify nor force user logoff** (Né notificare né forzare la disconnessione dell'utente) nella pagina **Manage Autoscale > User Logoff Notification** (Gestisci scala automatica > Notifica disconnessione utente). Quando l'opzione è selezionata, Autoscale non obbliga gli utenti a scollegarsi da macchine in stato di scarico né notifica agli utenti di scollegarsi e accedere a un altro computer. Per ulteriori informazioni, vedere Notifiche di scollegamento degli utenti.

**Possibilità di riavviare i PC cloud Windows 365.** È ora possibile utilizzare Citrix DaaS per riavviare i PC cloud Windows 365.

**More session details.** Quando si visualizza una sessione in **Full Configuration > Search > Sessions**, la vista della sessione (nel riquadro inferiore) ora include ulteriori dettagli sulla sessione per aiutare a risolvere e identificare i problemi dei client:

- **Reconnect time**. L'ora in cui una sessione si ricollega dopo essere stata disconnessa.
- **Client platform.** La piattaforma utilizzata per avviare la sessione.
- **Client version.** La versione della piattaforma client utilizzata per avviare la sessione.
- **Remote host IP.** L'indirizzo IP dell'host remoto in cui è ospitato Citrix Workspace.

**Supporto della ridenominazione dei gruppi di sicurezza di Azure AD per le macchine virtuali.** Per le macchine virtuali aggiunte a un gruppo di sicurezza di Azure AD tramite Citrix DaaS, è ora possibile rinominare il gruppo di sicurezza utilizzando **Full Configuration > Edit Machine Catalog**. La ridenominazione viene eseguita dopo il salvataggio della modifica.

**Selezione del dominio predefinito per gli account macchina.** Quando si crea un catalogo, il dominio in cui risiede la risorsa (connessione) viene selezionato per impostazione predefinita per gli account delle macchine.

**Possibilità di visualizzare i gruppi di sicurezza assegnati ad Azure AD a cui le VM possono aderire.** In Full Configuration, quando si creano macchine virtuali aggiunte ad Azure Active Directory, è ora disponibile un'opzione, **Join an assigned security group as a member** (Unisciti a un gruppo di sicurezza assegnato come membro), che consente di aggiungere il gruppo di sicurezza di Azure AD in cui risiedono le macchine virtuali a un gruppo di sicurezza assegnato. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

**Supporto del cambio di rete per le connessioni**. In Full Configuration, ora è possibile cambiare rete per una connessione. Non è possibile annullare l'associazione delle reti da una connessione se sono in uso. Per ulteriori informazioni, vedere Modificare la rete.

**Possibilità di rimuovere i tag negli ambienti Azure**. In precedenza, i comandi `Remove-ProvVM` e `Remove-ProvScheme` di PowerShell con parametri `ForgetVM` rimuovevano le macchine virtuali e i cataloghi di macchine dal database Citrix. Tuttavia, i comandi non hanno rimosso i tag dalle risorse. Era necessario gestire individualmente le macchine virtuali e i cataloghi di macchine che non erano stati eliminati completamente da tutte le risorse. Con questa funzionalità, è possibile utilizzare:

- `Remove-ProvVM` con il parametro `ForgetVM` per rimuovere macchine virtuali e tag creati sulle risorse da una singola macchina virtuale o un elenco di macchine virtuali da un catalogo di macchine.
- `Remove-ProvScheme` con il parametro `ForgetVM` per rimuovere un catalogo di macchine dal database Citrix e tag creati sulle risorse da un intero catalogo di macchine.

Questa implementazione aiuta a identificare le risorse orfane create da MCS ma non più utilizzate da MCS.

Questa funzionalità è applicabile solo alle macchine virtuali persistenti. Per ulteriori informazioni, vedere Rimuovere i tag.

**Avviso di macchine con errori**. La funzionalità Proactive Notification and Alerting di Director è stata migliorata per includere un nuovo avviso, Failed Machines (in%) basato sulla percentuale di computer con errori presenti in un gruppo di consegna. La nuova condizione di avviso consente di configurare le soglie di avviso in termini di percentuale di macchine con errori all'interno di un gruppo di consegna. Per ulteriori informazioni, vedere la sezione Failed Machines nell'articolo Avvisi.

## aprile 2023

### Funzionalità nuove e migliorate

**Pubblicare con piattaforme cloud specifiche utilizzando Citrix Provisioning in Image Portability Service.** Sono ora disponibili flussi di lavoro specifici per l'uso di Image Portability Service per la pubblicazione in AWS, Azure e Google Cloud. Inoltre, le autorizzazioni richieste per Azure e la rete sono state aggiornate. Per maggiori dettagli, vedere Migrare i carichi di lavoro sul cloud pubblico.

**Supporto dell'identificazione del motivo per cui una macchina è in modalità di manutenzione**. In precedenza, PowerShell era l'unica scelta per identificare il motivo per cui una macchina era in modalità di manutenzione. Ora è possibile farlo in Full Configuration:

1. Utilizzare Search per localizzare la macchina.
2. Controllare la voce **Maintenance Reason** (Motivo della manutenzione) nella scheda **Details** che si trova nel riquadro inferiore. Oppure passare il mouse sulla colonna **motivo della manutenzione** (Modalità di manutenzione). Possono essere visualizzate le seguenti informazioni:

- By Administrator (Dall'amministratore): messo in modalità di manutenzione dall'amministratore.
- Maximum Failed Registrations (Numero massimo di registrazioni non riuscite): messo in modalità di manutenzione quando la macchina ha superato il numero massimo di tentativi di registrazione consentiti.

Inoltre, è ora disponibile un filtro, **Maintenance Reason**. È possibile utilizzarlo per identificare i computer bersaglio.

Questa funzione è utile per gli amministratori quando devono risolvere i problemi delle macchine in modalità di manutenzione.

**Utilizzare le variabili per notificare agli utenti il tempo rimanente prima che vengano scollegati**. Quando si forza lo scollegamento dell'utente, è ora possibile utilizzare `%s%` o `%m%` come variabili per indicare il tempo specificato nel messaggio di notifica. Per esprimere il tempo in secondi, utilizzare `%s%`. Per esprimere il tempo in minuti, utilizzare `%m%`. Per ulteriori informazioni, vedere Notifiche di scollegamento degli utenti.

**Supporto della personalizzazione del comportamento di accensione in caso di errore di modifica del tipo di archiviazione**. All'accensione, il tipo di archiviazione di un disco gestito potrebbe non riuscire a passare al tipo desiderato a causa di un errore in Azure. In precedenza, in questi scenari, la VM rimaneva disattivata e veniva inviato un messaggio di errore. Con questa funzionalità, è possibile scegliere di accendere la VM anche quando l'archiviazione non può essere ripristinata al tipo configurato oppure scegliere di mantenere la VM spenta. Per ulteriori informazioni, vedere Personalizzare il comportamento di accensione in caso di mancata riuscita della modifica del tipo di archiviazione.

**Supporto dell'attivazione MAK**. È ora possibile effettuare il provisioning di cataloghi di macchine persistenti e non persistenti con macchine virtuali attivate tramite la chiave di attivazione multipla (MAK). Grazie a questa funzionalità, ora MCS può comunicare anche con le macchine virtuali di cui è stato effettuato il provisioning. Questa implementazione aiuta ad attivare il sistema Windows senza perdere il conteggio delle attivazioni. Per ulteriori informazioni, vedere Attivazione dei contratti multilicenza.

**Supporto della crittografia del disco di Azure sull'host**. Con questa funzionalità, è ora possibile creare un catalogo di macchine MCS con funzionalità di crittografia sull'host. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità. È possibile utilizzare una VM

o specifiche di modello come input per il profilo di una macchina. Per ulteriori informazioni, vedere Crittografia del disco di Azure sull'host.

In questo tipo di crittografia, il server che ospita la macchina virtuale crittografa i dati e quindi i dati crittografati fluiscono attraverso il server di archiviazione di Azure. Pertanto, questo metodo di crittografia crittografa i dati per tutto il loro percorso dall'inizio alla fine. Per ulteriori informazioni, vedere Crittografia nell'host - Crittografia end-to-end per i dati della macchina virtuale.

**Supporto del modello di istanza GCP come input per il profilo della macchina**. Con questa funzionalità, è ora possibile selezionare un modello di istanza GCP come input per il profilo della macchina. I modelli di istanza sono risorse leggere in GCP, quindi sono molto convenienti. Per fare ciò, utilizzare i comandi PowerShell. Per ulteriori informazioni sull'utilizzo dei comandi PowerShell per creare e aggiornare i cataloghi di macchine selezionando un modello di istanza GCP, vedere Creare un catalogo di macchine con il profilo della macchina come modello di istanza.

**Supporto della modifica del nome del gruppo di sicurezza dinamico di Azure AD**. È possibile modificare o eliminare il nome di un gruppo di sicurezza dinamico di Azure AD dal portale di Azure. Dopo questa azione il nome del gruppo di sicurezza dinamico di Azure AD potrebbe non essere sincronizzato con il gruppo di sicurezza dinamico associato a un catalogo di macchine. Con questa funzionalità, è ora possibile modificare il nome del gruppo di sicurezza dinamico di Azure AD associato a un catalogo di macchine.

Questa modifica consente di rendere le informazioni sul gruppo di sicurezza dinamico di Azure AD archiviate nell'oggetto del pool di identità di Azure AD coerenti con le informazioni archiviate nel portale di Azure. Per ulteriori informazioni, vedere Modificare il nome del gruppo di sicurezza dinamico di Azure AD.

**Sono state aggiunte le autorizzazioni richieste in GCP**. Sono state ora aggiunte le autorizzazioni necessarie per effettuare le seguenti operazioni:

- Creare una connessione host
- Effettuare la gestione dell'alimentazione delle macchine virtuali
- Cataloghi di provisioning

Per ulteriori informazioni, vedere Informazioni sulle autorizzazioni di Azure.

**Gestione delle credenziali**. Ai fini di una maggiore sicurezza, per impostazione predefinita, non vengono inoltrate al cloud le credenziali degli utenti che non si trovano nello stesso dominio dei loro VDA. I tentativi di accesso non riescono quando vengono soddisfatte tutte le seguenti condizioni:

- L'utente si trova in un dominio diverso dal VDA
- Non esiste un rapporto di attendibilità tra i domini
- StoreFront è installato nello stesso dominio del VDA

In precedenza, quando si verificavano queste condizioni, l'utente non poteva essere autenticato su StoreFront. Quindi, Cloud Connector inoltrava le credenziali dell'utente al cloud per indirizzare

la richiesta di autenticazione alla destinazione corretta per quell'utente. Questo comportamento può ancora essere configurato se necessario. Per ulteriori informazioni, vedere il parametro `CredentialForwardingToCloudAllowed` di Set-Brokersite nell'SDK PowerShell di DaaS.

### marzo 2023

#### Funzionalità nuove e migliorate

**Supporto della configurazione del ruolo e dell'ambito per gli amministratori**. Citrix Cloud ora supporta un livello più elevato di flessibilità e personalizzazione nella configurazione dell'accesso per un amministratore. In precedenza, era possibile selezionare solo coppie predefinite di ruoli e ambiti. Con questo miglioramento, è possibile selezionare un ruolo e poi abbinarlo all'ambito che si preferisce.

Per ulteriori informazioni, consultare Configurare l'accesso personalizzato per un amministratore.

**Supporto per la creazione di gruppi di sicurezza dinamici all'interno del gruppo di sicurezza assegnato esistente**. In precedenza, era possibile creare gruppi di sicurezza dinamici di Azure AD per un catalogo di macchine. Con questa funzionalità, è anche possibile aggiungere un gruppo di sicurezza dinamico di Azure AD all'interno di un gruppo di sicurezza assegnato ad Azure AD esistente. È possibile procedere come segue:

- Ottenere informazioni sui gruppi di sicurezza.
- Ottenere tutti i gruppi di sicurezza assegnati ad Azure AD che sono sincronizzati dal server AD locale o i gruppi di sicurezza assegnati a cui è possibile assegnare i ruoli di Azure AD.
- Ottenere tutti i gruppi di sicurezza dinamici di Azure AD.
- Aggiungere il gruppo di sicurezza dinamico di Azure AD come membro del gruppo assegnato ad Azure AD.
- Rimuovere l'appartenenza tra il gruppo di sicurezza dinamico di Azure AD e il gruppo di sicurezza assegnato ad Azure AD quando il gruppo di sicurezza dinamico di Azure AD viene eliminato insieme al catalogo macchine.

Per ulteriori informazioni, vedere Creare un gruppo di sicurezza dinamico di Azure AD in un gruppo di sicurezza assegnato ad Azure AD esistente.

**Supporto dei gruppi di sicurezza dinamici di Azure AD per le macchine virtuali aggiunte ad Azure AD**. Citrix ora supporta i gruppi di sicurezza dinamici per un catalogo durante la creazione di un catalogo di macchine MCS. Le regole dei gruppi di sicurezza dinamici collocano le VM del catalogo in un gruppo di sicurezza dinamico basato sullo schema di denominazione del catalogo delle macchine. Ciò è utile quando si desidera gestire le macchine virtuali tramite Azure Active Directory (Azure AD). È utile anche quando si desidera applicare i criteri di accesso condizionale o distribuire app da Intune filtrando le macchine virtuali con il gruppo di sicurezza dinamico di Azure AD. Quando si elimina un

catalogo, viene eliminato anche il gruppo di sicurezza dinamico. Per ulteriori informazioni, vedere Gruppo di sicurezza dinamico di Azure Active Directory.

Per altre informazioni sui requisiti di licenza per l'uso dei gruppi di sicurezza dinamici, vedere il documento Microsoft Creare o aggiornare un gruppo dinamico in Azure Active Directory.

**Supporto dell'aggiunta di macchine virtuali ai gruppi di sicurezza di Azure AD tramite Full Configuration.** È ora disponibile l'opzione **Azure AD security group** (Gruppo di sicurezza di Azure AD) quando si creano macchine virtuali aggiunte ad Azure AD. L'opzione consente di aggiungere le macchine virtuali a un gruppo di sicurezza di Azure AD in base al loro schema di denominazione. Per altre informazioni, vedere Creare un catalogo Microsoft Azure.

**Supporto della modifica del tipo di archiviazione delle macchine virtuali esistenti a un livello inferiore al momento dell'arresto in ambienti Azure.** Negli ambienti Azure, è ora possibile risparmiare sui costi di archiviazione modificando il tipo di archiviazione delle macchine virtuali esistenti portandolo a un livello inferiore quando le macchine virtuali vengono arrestate. A tale scopo, utilizzare la proprietà personalizzata StorageTypeAtShutdown. Per ulteriori informazioni, vedere Cambiare il tipo di archiviazione delle VM esistenti a un livello inferiore al momento dell'arresto.

**Supporto della possibilità di accettare gli identificatori di sicurezza durante la creazione di macchine virtuali.** In precedenza, durante la creazione di nuove macchine virtuali con la configurazione specificata da uno schema di provisioning, non era possibile aggiungere un identificatore di sicurezza (`ADAccountSid`) al comando `NewProvVM`. Con questa funzionalità, ora è possibile aggiungere il parametro `ADAccountSid` per identificare in modo univoco le macchine durante la creazione di nuove macchine virtuali. Per ulteriori informazioni, vedere Aggiungere i SID durante la creazione di macchine virtuali.

**Possibilità di ricevere avvisi associati ai cataloghi MCS.** In precedenza, non si riceveva alcuna informazione che indicasse la presenza di problemi nel catalogo delle macchine. Con questa funzione, è ora possibile ricevere avvisi per comprendere i problemi dei cataloghi MCS e risolverli.

Gli avvisi, a differenza degli errori, non determinano la non riuscita di un'attività di provisioning avviata.

Per ricevere avvisi, utilizzare i comandi PowerShell. Per ulteriori informazioni, vedere Recuperare gli avvisi associati a un catalogo.

**Tenant condivisi per le connessioni**. Ora è possibile aggiungere tenant e sottoscrizioni che condividono la Raccolta di calcolo di Azure con la sottoscrizione della connessione. Di conseguenza, quando si creano o si aggiornano i cataloghi, è possibile selezionare immagini condivise da questi tenant e sottoscrizioni. Per ulteriori informazioni, consultare Modificare le impostazioni di connessione.

**È stato rimosso il supporto per la modifica del tipo di sistema operativo per i cataloghi di Azure**. Quando si modificano le immagini del catalogo, vengono visualizzate solo le immagini con lo stesso tipo di sistema operativo dell'immagine in uso. Con questo miglioramento, Citrix DaaS non supporta

più la modifica del tipo di sistema operativo per i cataloghi di Azure dopo la creazione del catalogo, ad esempio il passaggio dal tipo di sistema operativo Windows a Linux e viceversa.

## febbraio 2023

### Funzionalità nuove e migliorate

**Supporto della condivisione di immagini tra diversi tenant di Azure.** In precedenza, negli ambienti Azure, era possibile condividere immagini solo con sottoscrizioni condivise mediante Azure Compute Gallery. Con questa funzionalità, ora è possibile selezionare un'immagine in Raccolta di calcolo di Azure che appartiene a una sottoscrizione condivisa diversa in un tenant diverso per creare e aggiornare un catalogo MCS. Per ulteriori informazioni, vedere Condivisione di immagini tra tenant di Azure.

**Modellazione dei criteri**. La funzionalità di modellazione dei criteri è ora disponibile a livello generale. È possibile simulare i criteri per scopi di pianificazione e test. Per ulteriori informazioni, vedere Utilizzare la procedura guidata per la modellazione dei criteri.

**Possibilità di attivare o disattivare le funzionalità di anteprima**. In Full Configuration > Home, in qualità di amministratore di Citrix Cloud con accesso completo, ora è possibile attivare o disattivare le funzionalità di anteprima senza contattare Citrix. Per ulteriori informazioni, vedere Home page per l'interfaccia Full Configuration.

**Cercare in Session Diagnostics con il nome utente**. Questa funzionalità consente l'uso di Session Launch Diagnostics a partire dal nome utente se non si dispone dell'ID della transazione. Questa funzionalità è particolarmente utile per gli amministratori dell'helpdesk per valutare una sessione non riuscita se l'utente finale non ha acquisito l'ID della transazione.
È possibile cercare un nome utente e selezionare una sessione da esaminare da un elenco di sessioni non riuscite che l'utente ha tentato di avviare nelle ultime 48 ore. La pagina Session Launch Diagnostics (Diagnostica dell'avvio della sessione) mostra i dettagli della sessione non riuscita. Elenca il componente esatto e la fase in cui si è verificato l'errore. Per ulteriori informazioni, vedere l'articolo Diagnostica di avvio della sessione.

**Distribuire app Web e SaaS sicure con Secure Private Access**. Nella scheda **Full Configuration > Applications > Applications** è ora disponibile una nuova opzione, **Add Web/SaaS Applications** (Aggiungi applicazioni Web/SaaS), nella barra delle azioni. L'opzione consente di distribuire app Web e SaaS sicure con Secure Private Access. Citrix Secure Private Access offre agli utenti remoti un modo semplice e flessibile di accedere alle app basate su Web, SaaS e client-server utilizzando un approccio Zero-Trust. Consente l'accesso Single Sign-on alle app Web e SaaS, insieme a controlli di sicurezza granulari quali i controlli di filigrana e di copia/incolla, tra le altre funzionalità di sicurezza. Con Citrix Secure Private Access, è possibile combinare tutte le proprie app virtualizzate e non virtualizzate in

un unica posizione e migliorare l'esperienza utente per i propri utenti. Vedere Citrix Secure Private Access.

**Filtrare il contenuto del registro per un periodo di tempo specifico**. È ora disponibile una nuova opzione, **Custom** (Personalizzato), nell'elenco della durata temporale disponibile in **Full Configuration > Logging > Events**. Si usa per specificare un periodo degli eventi da utilizzare come filtro per la ricerca. Per ulteriori informazioni, vedere Registrazione della configurazione.

**Aggiornamenti di Autoscale**. Abbiamo aggiornato l'opzione **Control when Autoscale starts powering on tagged machines** (Controlla quando Autoscale inizia ad accendere le macchine etichettate) per facilitarne la comprensione. L'opzione controlla quando Autoscale inizia ad accendere le macchine con tag in base alla percentuale di capacità residua delle macchine senza tag. Quando la percentuale scende al di sotto della soglia (impostazione predefinita 10%), Autoscale inizia ad accendere i computer con tag. Quando la percentuale supera la soglia, Autoscale passa alla modalità di spegnimento. Per ulteriori informazioni, vedere Scalabilità automatica delle macchine con tag (cloud burst).

**Criteri di protezione delle app**. Ora è possibile abilitare la protezione delle app quando si crea o si modifica un gruppo di consegna. La funzione fornisce funzionalità anti-keylogging e anti-screen-capturing per le sessioni client. Per ulteriori informazioni, vedere Creare gruppi di consegna e Gestire i gruppi di consegna.

**Utilizzo della GPU in tempo reale disponibile per le GPU AMD.** Ora è possibile visualizzare l'utilizzo della GPU delle GPU AMD Radeon Instinct MI25 e delle CPU AMD EPYC 7V12(Rome) su Monitor. Monitor supporta già le GPU NVIDIA Tesla M60. GPU Utilization (Utilizzo della GPU) visualizza grafici in tempo reale della percentuale di utilizzo della GPU, della memoria della GPU, del codificatore e del decodificatore per risolvere i problemi relativi alla GPU sui VDA con sistema operativo multisessione o a sessione singola. I grafici di utilizzo della GPU AMD sono disponibili solo per i VDA che eseguono Windows a 64 bit e Citrix Virtual Apps and Desktops 7 2212 o versioni successive. Per ulteriori informazioni, vedere Utilizzo della GPU.

**Supporto della pianificazione degli aggiornamenti della configurazione in Azure**. Negli ambienti di Azure, è ora possibile pianificare una fascia oraria per gli aggiornamenti della configurazione delle macchine MCS esistenti dotate di provisioning utilizzando il comando PowerShell `Schedule-ProvVMUpdate`. Eventuali accensioni o riavvii durante la fascia oraria pianificata applicano un aggiornamento pianificato dello schema di provisioning a una macchina. È inoltre possibile annullare l'aggiornamento della configurazione prima dell'ora pianificata utilizzando `Cancel-ProvVMUpdate`.

È possibile pianificare e annullare l'aggiornamento della configurazione di:

- Una o più macchine virtuali
- Un intero catalogo

Per ulteriori informazioni, vedere Pianificare gli aggiornamenti della configurazione.

**Supporto dell'uso di immagini pronte per Citrix direttamente da Google Cloud Marketplace**. È ora possibile sfogliare e selezionare le immagini offerte da Citrix su Google Cloud Marketplace per creare cataloghi MCS. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità. Per ulteriori informazioni, vedere Google Cloud Marketplace.

**Limitare l'ambito dei gruppi di host in SCVMM Host Connection**. In precedenza, la connessione host a SCVMM richiedeva che l'amministratore configurasse un unico gruppo di host di primo livello. Ciò implicava dare all'amministratore visibilità su tutti i gruppi di host, i cluster o gli host all'interno del singolo gruppo di host di primo livello. Con questa funzionalità, nelle implementazioni di grandi dimensioni in cui un singolo SCVMM gestisce più cluster in diversi data center è ora possibile limitare l'ambito degli amministratori dei gruppi host. A tale scopo, è possibile utilizzare il ruolo di amministratore delegato nella console Microsoft System Center Virtual Machine Manager (VMM) per selezionare i gruppi di host a cui un amministratore deve avere accesso. Per ulteriori informazioni, vedere Installare e configurare un hypervisor.

**Supporto dell'archiviazione con ridondanza della zona in Azure**. In precedenza, MCS offriva solo archiviazione ridondante a livello locale. Con questa funzionalità, l'archiviazione con ridondanza della zona è ora possibile in Azure e consente di selezionare un tipo di archiviazione in base al tipo di ridondanza che si desidera utilizzare. L'archiviazione con ridondanza della zona replica il disco gestito di Azure in più zone di disponibilità, il che consente di ripristinare un guasto in una zona utilizzando la ridondanza in altre. Per ulteriori informazioni, vedere Abilitare l'archiviazione con ridondanza della zona.

## gennaio 2023

### Funzionalità nuove e migliorate

**Opzione per il downgrade del disco di archiviazione a HDD standard all'arresto delle VM**. Una nuova opzione, **Enable storage cost saving** (Abilitare i risparmi sui costi di archiviazione), è ora disponibile nella pagina **Disk Settings** (Impostazioni disco) quando si creano o si aggiornano i cataloghi di Azure. L'opzione consente di risparmiare sui costi di archiviazione eseguendo il downgrade all'HDD standard per il disco di archiviazione e il disco cache di write-back all'arresto della VM. La VM torna alle impostazioni originali al momento del riavvio. Per altre informazioni, vedere Creare un catalogo Microsoft Azure.

**Supporto della configurazione del roaming della sessione in Full Configuration**. In precedenza, PowerShell era l'unica scelta per configurare il roaming delle sessioni per applicazioni e desktop. Ora è possibile farlo in **Full Configuration**. Per ulteriori informazioni, vedere Gestire i gruppi di consegna.

**Alcune azioni sono state rinominate per allinearle meglio ai loro significati effettivi.** Abbiamo

rinominato le seguenti azioni in **Full Configuration > Machine Catalogs** e **Full Configuration > Delivery Groups**. I flussi di lavoro per eseguire tali azioni rimangono invariati.

- **Update Machines** è stato rinominato in **Change Master Image** (Modifica immagine master)
- **Rollback Machine Update** è stato rinominato **Roll Back Master Image** (Esegui il rollback dell'aggiornamento della macchina)
- **Upgrade Catalog** è stato rinominato in **Change Functional Level** (Cambia il livello funzionale)
- **Upgrade Delivery Group** è stato rinominato in **Change Functional Level** (Cambia il livello funzionale)
- **Undo Upgrade Catalog** è stato rinominato in **Undo Functional Level Change** (Annulla modifica del livello funzionale)
- **Undo Upgrade Delivery Group** è stato rinominato in **Undo Functional Level Change** (Annulla modifica del livello funzionale)

**Supporto dell'organizzazione di gruppi di applicazioni tramite cartelle.**Ora è possibile creare cartelle per organizzare i gruppi di applicazioni per un facile accesso. Per ulteriori informazioni, vedere Organizzare i gruppi di applicazioni utilizzando le cartelle.

**Miglioramenti delle restrizioni per i gruppi di consegna**. In precedenza, quando si limitava l'uso di app o desktop per un gruppo di consegna, era possibile specificare solo gli utenti e i gruppi di utenti autorizzati a utilizzarli in un gruppo di consegna. Ora è anche possibile aggiungere utenti e gruppi di utenti che si desidera bloccare. Questo miglioramento è utile quando si aggiunge un gruppo di utenti a un elenco di utenti consentiti e allo stesso tempo si desidera bloccare un sottoinsieme di utenti inclusi nell'elenco degli utenti consentiti. Per ulteriori informazioni, vedere Creare gruppi di consegna.

**Accedere a Citrix Analytics for Performance - Dettagli della sessione da Monitor.** La pagina Session Details (Dettagli della sessione) di Citrix Analytics for Performance è ora integrata in Monitor. Fare clic su **View Session Timeline** (Visualizza cronologia della sessione) nella pagina Sessions di Monitor per visualizzare la pagina dei dettagli delle sessioni di Citrix Analytics for Performance all'interno di Monitor. Ciò richiede una licenza valida per Citrix Analytics for Performance. I dettagli della sessione sono disponibili per le sessioni classificate da Citrix Analytics for Performance come eccellenti, accettabili o scadenti.

È possibile visualizzare l'andamento dell'esperienza di sessione per un massimo di tre giorni insieme ai fattori che contribuiscono all'esperienza. Queste informazioni integrano i dati in tempo reale disponibili in Monitor, utilizzati dall'amministratore dell'helpdesk per la risoluzione dei problemi relativi all'esperienza di sessione.

Per ulteriori informazioni, vedere l'articolo Analisi del sito.

**Le macchine virtuali non persistenti vengono eliminate dagli hypervisor o dai servizi cloud quando l'utente le elimina o elimina i relativi cataloghi di macchine in Full Configuration.** L'opzione di conservare le VM negli hypervisor o nei servizi cloud è ora disponibile solo per le VM persistenti. Per ulteriori informazioni, vedere Gestire i cataloghi delle macchine.

## dicembre 2022

### Funzionalità nuove e migliorate

**Supporto della creazione di cataloghi compatibili con Azure AD, Hybrid Azure AD e Microsoft Intune con macchine virtuali master aggiunte ad Azure AD.** È ora possibile creare cataloghi compatibili con Azure AD, Hybrid Azure AD e Microsoft Intune con macchine virtuali master aggiunte ad Azure AD, aggiunte a Hybrid Azure AD e non aggiunte a dominio. Se si desidera gestire una macchina virtuale master tramite Microsoft Intune, utilizzare VDA versione 2212 o successiva e non saltare la preparazione delle immagini durante la creazione o l'aggiornamento dei cataloghi di macchine.

Per altre informazioni sulle identità delle macchine, vedere Aggiunte ad Azure Active DirectoryMicrosoft Intune e Agigunte ad Hybrid Azure Active Directory.

**Supporto in MCS dell'eliminazione di oggetti VM senza accedere all'hypervisor**. È ora possibile eliminare gli oggetti VM in MCS senza avere accesso all'hypervisor. Quando si elimina una macchina virtuale o uno schema di provisioning, MCS deve rimuovere i tag in modo che le risorse non vengano più tracciate o identificate. In precedenza, se non era possibile accedere all'hypervisor, gli errori di rimozione dei tag venivano ignorati. Con questa funzionalità, se l'hypervisor non è accessibile quando si utilizza il comando `Remove-ProvVM`, la rimozione del tag non riuscirà, ma utilizzando l'opzione `PurgeDBOnly` è comunque possibile eliminare l'oggetto della risorsa VM dal database. Per ulteriori informazioni, vedere Eliminare i computer senza accesso all'hypervisor.

## novembre 2022

### Funzionalità nuove e migliorate

**Supporto della fornitura di app MSIX e MSIX App Attach.** In **Full Configuration > App Packages** è ora possibile caricare le app in pacchetti MSIX e MSIX App Attach in Citrix Cloud, per poi distribuirle agli utenti. Per ulteriori informazioni, vedere Pacchetti di app.

**Richiesta di versioni VDA e livelli funzionali non supportati.** L'interfaccia Full Configuration ora avvisa l'utente delle versioni e dei livelli funzionali dei VDA non supportati. Per evitare potenziali problemi:

- Se una macchina esegue una versione VDA non supportata, viene richiesto di eseguire l'aggiornamento a una versione supportata.
- Se il livello funzionale di un catalogo o di un gruppo di consegna non è supportato, viene richiesto di impostarlo su un livello superiore.

> **Suggerimento:**
>
> I VDA sono coperti dai cicli di vita CR e LTSR di Citrix Virtual Apps and Desktops.

**Capacità di annotare le immagini master estesa alla creazione del catalogo.** Quando si crea un catalogo MCS in **Full Configuration**, è ora possibile annotarne l'immagine master. Per ulteriori informazioni, vedere Immagine master.

**Supporto dell'esportazione dei dati di assegnazione del desktop tramite Full Configuration.** Quando si visualizzano le assegnazioni desktop per un gruppo di consegna di sistemi operativi a sessione singola, è ora possibile esportare i dati delle assegnazioni in un file CSV per scopi di controllo. A tal fine, selezionare il gruppo di consegna in **Full Configuration > Delivery Groups**, passare alla scheda **Desktop** e quindi fare clic su **Export** nell'angolo in alto a sinistra della scheda.

**Tutte le schede delle applicazioni e le cartelle di applicazioni sono riunite in un'unica scheda.** In **Full Configuration > Applications**, le schede **All Applications** e **Application Folders** sono state consolidate in un'unica scheda, **Applications** (Applicazioni). Questa modifica unifica l'esperienza utente della gestione della visualizzazione delle cartelle tra i nodi di Full Configuration.

**Supporto della modifica del tipo di archiviazione in un livello inferiore quando una macchina virtuale viene arrestata in ambienti Azure**. Negli ambienti Azure, è ora possibile risparmiare sui costi di archiviazione cambiando il tipo di archiviazione di un disco gestito portandolo a un livello inferiore quando si arresta una VM. Per fare ciò, utilizzare la proprietà personalizzata `StorageTypeAtShutdown`. Il tipo di archiviazione del disco passa a un livello inferiore (come specificato nella proprietà personalizzata `StorageTypeAtShutdown`) quando si arresta la macchina virtuale. Dopo aver acceso la VM, il tipo di archiviazione torna al tipo originale (come specificato nella proprietà personalizzata`StorageType` o `WBCDiskStorageType`). Per ulteriori informazioni, vedere Portare il tipo di archiviazione a un livello inferiore quando una VM viene arrestata.

**Aggiornamenti nella vista Filters.** La pagina Filters di Monitor viene aggiornata per includere elenchi separati di filtri salvati e predefiniti per una migliore visualizzazione e accessibilità ai filtri. È possibile selezionare una vista tra macchine, sessioni, connessioni o istanze di applicazioni. È quindi possibile selezionare un filtro dall'elenco dei filtri salvati o dei filtri predefiniti per visualizzare l'elenco di dati filtrato. È possibile utilizzare gli elenchi a discesa per affinare i criteri di filtro o modificare i criteri esistenti. È possibile salvare un filtro creato nell'elenco dei filtri salvati. Per ulteriori informazioni, vedere l'articolo Filtri.

**Possibilità di reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di computer creato da MCS.** Negli ambienti di virtualizzazione VMware, ora è possibile utilizzare il comando PowerShell `Reset-ProvVMDisk` per reimpostare il disco del sistema operativo di una VM persistente in un catalogo di macchine creato da MCS. La funzione automatizza il processo di ripristino del disco del sistema operativo. Ad esempio, aiuta a ripristinare la VM allo stato iniziale di un catalogo desktop di sviluppo persistente creato con MCS.

Per ulteriori informazioni sull'utilizzo del comando PowerShell per reimpostare il disco del sistema operativo, vedere Reimpostare il disco del sistema operativo.

**Supporto dell'aggiornamento del profilo della macchina e delle proprietà personalizzate aggiuntive delle macchine di cui è stato eseguito il provisioning con MCS in ambienti Azure.** In precedenza, negli ambienti Azure, era possibile utilizzare `Request-ProvVMUpdate` per aggiornare la proprietà personalizzata `ServiceOffering` di una macchina di cui è stato eseguito il provisioning con MCS. È ora anche possibile aggiornare il profilo della macchina e le seguenti proprietà personalizzate:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

Per ulteriori informazioni, vedere Aggiornare le macchine di cui è stato eseguito il provisioning allo stato corrente dello schema di provisioning.

**Supporto del profilo della macchina in GCP**. Quando si crea un catalogo per il provisioning delle macchine utilizzando Machine Creation Services (MCS) negli ambienti Google Cloud Platform (GCP), è ora possibile utilizzare un profilo macchina per acquisire le proprietà hardware da una macchina virtuale e applicarle alle macchine virtuali di cui è stato appena effettuato il provisioning nel catalogo. Quando il parametro `MachineProfile` non viene utilizzato, le proprietà hardware vengono acquisite dalla VM o dalla snapshot dell'immagine master.

I profili macchina funzionano con entrambi i sistemi operativi Linux e Windows.

Per informazioni sulla creazione di un catalogo di macchine con un profilo macchina, vedere Creare un catalogo di macchine utilizzando un profilo macchina.

**Supporto dell'aggiornamento di macchine di cui è stato eseguito il provisioning con MCS in ambienti GCP**. Negli ambienti GCP `Set-ProvScheme` modifica il modello (schema di provisioning) e non influisce sulle macchine esistenti. Utilizzando il comando PowerShell `Request-ProvVMUpdate`, è ora possibile applicare lo schema di provisioning corrente a una macchina (o a un insieme di macchine) esistente. Attualmente, in GCP, l'aggiornamento delle proprietà supportato da questa funzionalità è il profilo del computer. Per ulteriori informazioni, vedere Aggiornare i computer sottoposti a provisioning utilizzando PowerShell.

## ottobre 2022

### Funzionalità nuove e migliorate

**Supporto dell'utilizzo simultaneo dei profili delle macchine e dei gruppi di host**. Quando si crea un catalogo usando un'immagine master di Azure Resource Manager, ora è possibile usare un profilo macchina e un gruppo host allo stesso tempo. Ciò è utile negli scenari in cui si desidera utilizzare l'avvio attendibile per una maggiore sicurezza e allo stesso tempo eseguire le macchine su host dedicati. Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft Azure Resource Manager.

**Supporto dell'organizzazione di gruppi di consegna tramite cartelle.** È ora possibile creare un albero di cartelle per organizzare i gruppi di consegna per un facile accesso. Per ulteriori informazioni, vedere Organizzare i gruppi di consegna tramite cartelle.

**Supporto della pianificazione di un riavvio una tantum per i computer tramite Full Configuration.** Una nuova opzione, **Once** (Una volta), è ora disponibile quando si creano piani di riavvio per i gruppi di consegna. Con questa opzione, è possibile pianificare il riavvio delle macchine di un gruppo di consegna una volta, a una data e a un'ora specificate. Per ulteriori informazioni, vedere Creare una pianificazione di riavvio.

**Pianificazione avanzata del probe.** È ora possibile eseguire una migliore pianificazione dei probe per applicazioni e desktop da Monitor. Utilizzando questa funzione, Citrix Probe Agent può essere configurato per eseguire le attività di probe in giorni specifici della settimana e ripeterle a intervalli specifici durante il giorno. Ciò consente di pianificare una singola operazione di probe da ripetere in orari specifici del giorno e della settimana. È ora possibile controllare in modo proattivo lo stato del proprio sito con probe impostati per funzionare regolarmente in orari appropriati. Questa funzionalità semplifica la configurazione e la gestione delle sonde in Monitor. Per ulteriori informazioni, vedere Probe delle applicazioni e dei desktop.

## settembre 2022

### Funzionalità nuove e migliorate

**Le versioni precedenti dell'SDK Remote PowerShell sono ora deprecate.** Se si utilizza una versione deprecata, l'SDK smette di funzionare e viene visualizzato un messaggio di errore in cui si richiede di scaricare la versione corrente. In tal caso, scaricare l'ultima versione dell'SDK Remote PowerShell dal sito Web di Citrix.

**Cataloghi di macchine con avvio attendibile in Azure**. Negli ambienti Azure, è possibile creare cataloghi di macchine abilitati con Trusted Launch e usare la proprietà `SupportsTrustedLaunch` dell'inventario delle VM per determinare le dimensioni delle VM che supportano Trusted Launch.

L'avvio attendibile (Trusted Launch) è un modo semplice per migliorare la sicurezza delle macchine virtuali di seconda generazione. L'avvio attendibile protegge da tecniche di attacco avanzate e persistenti. Per ulteriori informazioni, vedere Cataloghi di macchine con avvio attendibile.

**Supporto dell'identificazione delle risorse di Microsoft System Center Virtual Machine Manager create da MCS**. È ora possibile identificare le risorse di Microsoft System Center Virtual Machine Manager (SCVMM) create da MCS utilizzando i tag. Per ulteriori informazioni sui tag che MCS aggiunge alle risorse, vedere Identificare le risorse create da MCS.

**Supporto dell'identificazione delle risorse VMware create da MCS**. È ora possibile identificare le risorse VMware create da MCS utilizzando i tag. Per ulteriori informazioni sui tag che MCS aggiunge alle risorse, vedere Identificare le risorse create da MCS.

**Supporto dell'ottimizzazione della limitazione di AWS Workspace**. Ora è possibile accendere e spegnere un numero elevato di macchine in AWS Workspace senza riscontrare problemi di limitazione. I problemi di limitazione si verificano quando il numero di richieste inviate ad AWS Workspace supera il numero di richieste che il server è in grado di gestire. Pertanto, Citrix ora raggruppa più richieste in un'unica richiesta prima dell'invio all'SDK AWS Workspace.

**Capacità di controllare i dettagli della macchina durante la visualizzazione del numero di macchine in Home.** Quando si visualizza il numero di macchine in base allo stato di disponibilità in **Home**, ora è possibile fare clic su uno stato per visualizzare i dettagli delle macchine che si trovano in quello stato. Per ulteriori informazioni, vedere Home page per l'interfaccia Full Configuration.

**Supporto della creazione di cataloghi di macchine utilizzando un'immagine tratta da una sottoscrizione diversa nello stesso tenant di Azure**. In precedenza, negli ambienti Azure, era possibile solo selezionare un'immagine all'interno della sottoscrizione per creare un catalogo di macchine. Con questa funzionalità, ora è possibile selezionare un'immagine in Raccolta di calcolo di Azure (precedentemente Raccolta immagini condivise) che appartiene a una diversa sottoscrizione condivisa per creare e aggiornare i cataloghi MCS.

Per ulteriori informazioni sulla creazione di un catalogo, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

Per informazioni sulla condivisione dell'immagine con un altra entità servizio all'interno dello stesso tenant, vedere Condivisione di immagini con un'altra entità servizio nello stesso tenant.

Per informazioni sui comandi PowerShell per selezionare un'immagine da una sottoscrizione diversa, vedere Usare PowerShell per selezionare un'immagine da una sottoscrizione diversa.

Per ulteriori informazioni su Raccolta di calcolo di Azure, vedere Raccolta immagini condivise di Azure.

## agosto 2022

### Funzionalità nuove e migliorate

**Supporto dell'identificazione delle risorse Citrix Hypervisor create da MCS**. Ora è possibile identificare le risorse hypervisor Citrix create da MCS utilizzando i tag. Per ulteriori informazioni sui tag che MCS aggiunge alle risorse, vedere Identificare le risorse create da MCS.

**Supporto dell'utilizzo simultaneo di gruppi di host e zone di disponibilità di Azure**. Negli ambienti Azure è ora disponibile un controllo preliminare per valutare se la creazione di un catalogo di macchine avrà esito positivo in base alla zona di disponibilità di Azure specificata nella proprietà personalizzata e alla zona del gruppo host. La creazione del catalogo non riesce se la proprietà personalizzata della zona di disponibilità non corrisponde alla zona del gruppo host.

Un gruppo di host è una risorsa che rappresenta una raccolta di host dedicati. Un host dedicato è un servizio che fornisce server fisici che ospitano una o più macchine virtuali.
Le zone di disponibilità di Azure sono posizioni fisicamente separate all'interno di ogni area di Azure che sono tolleranti agli errori locali.

Per ulteriori informazioni sulle varie combinazioni di zona di disponibilità e zona di gruppo host che determinano l'esito positivo o negativo della creazione del catalogo di macchine, vedere Usare gruppi di host e zone di disponibilità di Azure allo stesso tempo.

**Supporto dell'aggiornamento dell'ID della cartella di un catalogo di macchine in VMware**. Negli ambienti di virtualizzazione VMware, è ora possibile aggiornare l'ID della cartella di un catalogo di macchine MCS utilizzando la proprietà personalizzata `FolderID` in `Set-ProvScheme`. Le macchine virtuali create dopo l'aggiornamento dell'ID della cartella vengono create con questo nuovo ID della cartella. Se questa proprietà non è specificata in `CustomProperties`, le macchine virtuali vengono create nella cartella in cui si trova l'immagine master. Per ulteriori informazioni sull'aggiornamento dell'ID della cartella, vedere Aggiornare l'ID della cartella di un catalogo di macchine.

**Impostazione del fuso orario**. Ora è possibile configurare il formato di data e ora dell'interfaccia in base alle proprie preferenze utilizzando l'impostazione **Date and time** (Data e ora). Per ulteriori informazioni, vedere Impostazione del fuso orario.

**Image Portability Service (IPS) ora supporta Amazon Web Services (AWS).** Configurando le autorizzazioni e i componenti richiesti per AWS, i flussi di lavoro IPS possono essere utilizzati con un account AWS. Per maggiori dettagli, vedere Migrare i carichi di lavoro sul cloud pubblico .

**Impostazione del file di paging durante la preparazione delle immagini in ambienti Azure**. Negli ambienti Azure, è ora possibile evitare la potenziale confusione sul percorso del file di paging. A tal fine, MCS ora determina la posizione del file di paging quando si crea lo schema di provisioning durante la preparazione dell'immagine. Questo calcolo si basa su determinate regole. Funzionalità quali il disco del sistema operativo effimero (EOS) e MCS I/O hanno la propria posizione prevista del file di

paging e si escludono a vicenda. Inoltre, se la preparazione dell'immagine viene disaccoppiata dalla creazione dello schema di provisioning, MCS determina correttamente la posizione del file di paging. Per ulteriori informazioni sulla posizione del file di paging, vedere Posizione del file di paging.

**Supporto dell'aggiornamento delle impostazioni dei file di paging negli ambienti Azure**. Durante la creazione di un catalogo in un ambiente Azure, è ora possibile specificare l'impostazione del file di paging, inclusa la posizione e la dimensione, utilizzando i comandi di PowerShell. Ciò sostituisce l'impostazione del file di paging determinata da MCS. È possibile farlo eseguendo il comando `New-ProvScheme` con le seguenti proprietà personalizzate:

- `PageFileDiskDriveLetterOverride`: lettera dell'unità disco del percorso del file di paging
- `InitialPageFileSizeInMB`: dimensione iniziale del file di paging in MB
- `MaxPageFileSizeInMB`: dimensione massima del file di paging in MB

Per ulteriori informazioni sull'aggiornamento delle impostazioni del file di paging, vedere Aggiornare l'impostazione del file di paging

**Aggiornamenti della home page**. Il widget Get Started ora ha un nuovo aspetto. Altri aggiornamenti alla home page includono:

- Le nuove icone Aggiorna e Guida, aggiunte nell'angolo in alto a destra.
- Conteggi delle risorse cliccabili, per dare accesso rapido alle pagine delle risorse pertinenti.
- Miglioramento dell'icona Non mi piace. Se una raccomandazione non ti piace, la raccomandazione scompare. Se il widget dei consigli non ti piace, il widget scompare.

Per ulteriori informazioni, vedere Home page.

**Supporto dell'abilitazione delle estensioni di macchine virtuali di Azure**. Quando si utilizza una specifica di modello ARM come profilo macchina per creare un catalogo di macchine, ora è possibile aggiungere estensioni di macchine virtuali di Azure alle macchine virtuali del catalogo, visualizzare l'elenco delle estensioni supportate e rimuovere le estensioni aggiunte. Le estensioni delle macchine virtuali di Azure sono piccole applicazioni che forniscono attività di automazione e configurazione post-distribuzione nelle macchine virtuali di Azure. Ad esempio, se una macchina virtuale richiede l'installazione di software, la protezione antivirus o la possibilità di eseguire uno script al suo interno, è possibile utilizzare un'estensione di VM. Per altre informazioni su come abilitare le estensioni di macchine virtuali di Azure, vedere Utilizzare PowerShell per abilitare le estensioni delle macchine virtuali di Azure.

**Supporto dell'avvio attendibile per il disco del sistema operativo temporaneo**. È ora possibile creare schemi di provisioning utilizzando il disco del sistema operativo temporaneo su Windows con avvio attendibile. L'avvio attendibile è un modo semplice per migliorare la sicurezza delle macchine virtuali di seconda generazione. Protegge da tecniche di attacco avanzate e persistenti combinando tecnologie che possono essere abilitate in modo indipendente come l'avvio sicuro e la versione virtu-

alizzata del Trusted Platform Module (vTPM). Per ulteriori informazioni sulla creazione di un catalogo di macchine, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

## luglio 2022

### Funzionalità nuove e migliorate

**Timeout di sessione dinamici per macchine con sistema operativo a sessione singola**. I timeout di sessione dinamici ora supportano le macchine con sistema operativo a sessione singola. È richiesto un gruppo di consegna con almeno un VDA versione 2206 o successiva. Verificare che i VDA siano stati registrati su Citrix Cloud almeno una volta. Per ulteriori informazioni, vedere Timeout dinamici delle sessioni.

**Inviare promemoria di scollegamento senza forzare lo scollegamento dell'utente in Autoscale**. Una nuova funzionalità è ora disponibile in **User Logoff Notifications** (Notifiche di scollegamento utente) (precedentemente **Force User Logoff** [Forza scollegamento utente]) in Autoscale. La funzione consente di inviare promemoria di scollegamento agli utenti senza costringerli a scollegarsi. In questo modo si evitano potenziali perdite di dati causate forzando gli utenti a scollegarsi dalle proprie sessioni. Vedere Notifiche di scollegamento degli utenti per i dettagli.

**Possibilità di impostare il tipo di licenza del sistema operativo Linux durante la creazione di cataloghi di macchine virtuali Linux in Azure**. Utilizzando l'interfaccia Full Configuration, è ora possibile scegliere il tipo di licenza del sistema operativo Linux durante la creazione di cataloghi di macchine virtuali Linux in Azure. Sono disponibili due opzioni per le licenze Linux personalizzate: Red Hat Enterprise Linux e SUSE Linux Enterprise Server. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

**Esperienza di ricerca migliorata in Full Configuration**. Il nodo Ricerca offre le seguenti nuove funzionalità e miglioramenti:

- **Capacità di esportare i risultati della ricerca**. Ora è possibile esportare i risultati della ricerca. Per farlo, fare clic sull'icona di esportazione nell'angolo in alto a destra.
- **Disponibile nuovo filtro**. È ora disponibile per l'uso il filtro Pending Power Action (Azione relativa all'alimentazione in sospeso). Usare il filtro per affinare la ricerca.
- **Supporto della ricerca "Does not contain"per determinati elementi**. Elementi come i nomi delle macchine e i tag ora supportano il criterio di ricerca "Does not contain"(Non contiene).
- **Supporto della ricerca di oggetti quando si aggiungono filtri**. Quando si aggiungono filtri per i seguenti oggetti, è ora possibile cercarli: connessioni, cataloghi di macchine, gruppi di consegna, gruppi di applicazioni e tag.

Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Supporto dei profili di archiviazione VMware.** Quando si crea un catalogo di macchine utilizzando un'immagine master su un datastore vSAN, è ora possibile copiare criteri di archiviazione come le informazioni RAID-1 o RAID-5 dall'immagine master ai dispositivi di destinazione creati. Per i cataloghi esistenti, il criterio di archiviazione rimane invariato anche se si aggiorna il catalogo.

**Supporto della registrazione SPN RestrictedKrbHost.** Tutti gli account computer creati da Citrix MCS sono ora registrati con i Service Principal Names (SPN) `RestrictedKrbHost`. In questo modo si evita la necessità di eseguire il comando `setspn` per registrare l'SPN per gli account computer dopo la creazione da parte di MCS.

**Pacchetti di app in Full Configuration per la distribuzione di applicazioni in pacchetto Microsoft.** Il nodo App-V viene rinominato in App Packages e riprogettato per adattarsi a più tipi di app in pacchetto Microsoft. In precedenza, era necessario utilizzare il modulo di individuazione per aggiungere app in pacchetto App-V al proprio ambiente per la distribuzione. Ora è possibile aggiungere e distribuire le app in un unica posizione utilizzando il nodo App Packages. Per ulteriori informazioni, vedere Pacchetti di app.

**Supporto dell'utilizzo delle specifiche di modello ARM come profili macchina.** In precedenza, era possibile solo utilizzare macchine virtuali come profili macchina. Ora è possibile utilizzare anche le specifiche di modello ARM come profili macchina durante la creazione di cataloghi di macchine di Azure. Questa funzionalità consente di sfruttare le funzionalità dei modelli ARM di Azure come controllo delle versioni. Per garantire che la specifica selezionata sia configurata correttamente e contenga le configurazioni richieste, eseguiamo la convalida su di essa. Se la convalida non riesce, viene richiesto di selezionare un profilo macchina diverso. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

**Supporto della convalida delle specifiche di modello ARM**. È ora possibile convalidare la specifica di modello ARM per assicurarsi che possa essere utilizzata come profilo macchina per creare un catalogo di macchine. Esistono due modi per convalidare la specifica di modello ARM:

- Utilizzando l'interfaccia di gestione Full Configuration.
- Utilizzando il comando di PowerShell.

Per ulteriori informazioni sulla convalida della specifica di modello ARM, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

## giugno 2022

### Funzionalità nuove e migliorate

**Supporto della pianificazione del riavvio per i computer con sistema operativo a sessione singola**. In precedenza, la funzione di pianificazione del riavvio era disponibile solo per le macchine con sistemi operativi multisessione. Ora è disponibile anche per le macchine con sistema operativo

a sessione singola. È ora possibile creare pianificazioni di riavvio per i gruppi di consegna contenenti computer con sistema operativo a sessione singola. Per ulteriori informazioni, vedere Creare e gestire pianificazioni di riavvio per le macchine di un gruppo di consegna.

**Opzione per eseguire i controlli preliminari del nome utente**. È ora disponibile l'opzione **Check name** (Controlla nome), quando si immettono le credenziali del dominio. Con questa opzione, è possibile verificare se il nome utente è valido o univoco. L'opzione è utile, ad esempio, quando:

- Lo stesso nome utente esiste in più domini. Viene richiesto di selezionare l'utente desiderato.
- Non si ricorda il nome del dominio. È possibile immettere il nome utente senza specificare il nome del dominio. Se il controllo viene superato, il nome del dominio viene popolato automaticamente.

Per ulteriori informazioni, vedere Credenziali di dominio.

**Possibilità di modificare le impostazioni di rete per uno schema di provisioning esistente.** È ora possibile modificare l'impostazione di rete per uno schema di provisioning esistente in modo che le nuove macchine virtuali vengano create nella nuova sottorete. Utilizzare il parametro `-NetworkMapping` nel comando `Set-ProvScheme` per modificare l'impostazione di rete. Solo le nuove macchine virtuali di cui è stato eseguito il provisioning in quello schema avranno le nuove impostazioni della sottorete. È inoltre necessario assicurarsi che le sottoreti si trovino nella stessa unità di hosting. Per ulteriori informazioni, vedere Modificare le impostazioni di rete per uno schema di provisioning esistente.

**Recupero delle informazioni sui nomi delle aree per macchine virtuali di Azure, dischi gestiti, snapshot, Azure VHD e modello ARM.** Ora è possibile visualizzare le informazioni sul nome della regione per una macchina virtuale di Azure, per i dischi gestiti, le snapshot, il VHD di Azure e il modello ARM. Queste informazioni vengono visualizzate per le risorse sull'immagine master quando viene assegnato un catalogo delle macchine. Per ulteriori informazioni, vedere Recuperare informazioni sui nomi delle regioni per macchine virtuali di Azure, dischi gestiti, snapshot, Azure VHD e modelli ARM.

**Possibilità di utilizzare i valori delle proprietà del profilo macchina in ambiente Azure.** Quando si crea un catalogo di Azure con un profilo macchina, è ora possibile impostare i valori delle proprietà dalla specifica di modello ARM o dalla VM, a seconda di quale sia utilizzata come profilo macchina, se i valori non sono definiti in modo esplicito nelle proprietà personalizzate. Le proprietà interessate da questa funzione sono:

- Zona di disponibilità
- ID gruppo host dedicato
- ID set crittografia disco
- Tipo di sistema operativo
- Tipo di licenza
- Offerta di servizi
- Tipo di archiviazione

Se alcune delle proprietà non sono presenti nel profilo macchina e non sono definite nelle proprietà personalizzate, il valore predefinito delle proprietà ha luogo laddove applicabile. Per ulteriori informazioni, vedere Utilizzare i valori delle proprietà del profilo macchina.

**Supporto esteso per l'aggiornamento dei VDA**. Utilizzando l'interfaccia Full Configuration, è ora possibile aggiornare le macchine persistenti di cui è stato eseguito il provisioning con MCS. È possibile aggiornarle per catalogo o per macchina. Per ulteriori informazioni, vedere Upgrade VDAs using the Full Configuration interface.

**Citrix Probe Agent nei piani di controllo Citrix Cloud Japan e Citrix Cloud Government.** Citrix Probe Agent ora supporta i siti in hosting sui piani di controllo Citrix Cloud Japan e Citrix Cloud Government. Per utilizzare questi piani, impostare il valore del Registro di sistema nel percorso "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region"su 2 per il Giappone e su 3 per la regione Government. Citrix Probe Agent automatizza il processo di verifica di integrità delle app e dei desktop virtuali pubblicati in un sito. Per ulteriori informazioni, vedere Probe delle applicazioni e dei desktop.

**Personalizzare la porta utilizzata per la comunicazione tra i VDA e i Cloud Connector**. È ora possibile personalizzare la porta utilizzata dal VDA per comunicare con i Cloud Connector in base ai propri requisiti di sicurezza specifici. Questa funzione è utile se il team di sicurezza non consente l'apertura della porta predefinita (porta 80) o se la porta predefinita è già in uso. Per ulteriori informazioni, vedere Customize the port for communicating with Cloud Connectors.

**Supporto dell'organizzazione dei cataloghi di macchine utilizzando le cartelle.** Ora è possibile creare cartelle nidificate in cui organizzare i cataloghi delle macchine per facilità di accesso. Per ulteriori informazioni, vedere Organize catalogs using folders.

**Supporto di SCVMM 2022**. Citrix DaaS ora supporta System Center Virtual Machine Manager (SCVMM) 2022 di Microsoft. SCVMM fornisce una gamma di servizi che includono la manutenzione delle risorse necessarie per l'implementazione delle VM. Per ulteriori informazioni sulle nuove funzionalità supportate in SCVMM 2022, vedere Novità di System Center Virtual Machine Manager.

**Supporto della configurazione del parametro massimo delle operazioni di provisioning simultaneo su AWS**. Citrix DaaS ora supporta `MaximumConcurrentProvisioningOperations` come proprietà personalizzata configurabile per MCS su AWS. `MaximumConcurrentProvisioningOperations` è la proprietà che determina il numero di macchine virtuali che è possibile creare o eliminare contemporaneamente. Anche se MCS supporta 100 operazioni di provisioning simultanee massime per impostazione predefinita, ora è possibile immettere i comandi PowerShell per personalizzare questo valore. È possibile inserire un intervallo compreso tra 1 e 1000. L'impostazione di questa proprietà sul valore preferito consente di controllare il numero di attività parallele che è possibile eseguire durante la creazione o l'eliminazione delle VM. Per informazioni dettagliate sulla configurazione del numero massimo di operazioni di provisioning simultanee, vedere Valori predefiniti della connessione host.

## maggio 2022

### Funzionalità nuove e migliorate

**Diagnostica avanzata di avvio della sessione.** Citrix DaaS ora supporta la diagnostica dettagliata degli errori di avvio della sessione. Ora è possibile visualizzare i componenti coinvolti nella sequenza di avvio della sessione. Sono evidenziati i componenti che hanno riportato errori con gli ultimi codici di errore generati. Questo aiuta a identificare il motivo esatto dell'errore di avvio di una sessione e a intraprendere l'azione consigliata.

La pagina Transaction viene estesa con il pannello Transaction Details (Dettagli transazione) che contiene un elenco di componenti che indicano il verificarsi dell'errore. Facendo clic sul nome del componente vengono visualizzati i dettagli dello stesso e i dettagli dell'ultimo errore noto. Vengono visualizzati il motivo dell'errore e il codice di errore. Facendo clic sul collegamento Learn more (Ulteriori informazioni) si accede al codice specifico in Error codes (Codici di errore) contenente una descrizione dettagliata e l'azione consigliata. Per ulteriori informazioni, vedere Session Diagnostics (Diagnostica della sessione).

**Supporto dell'utilizzo di Set-ProvServiceConfigurationData nell'SDK Remote PowerShell.** Ora è possibile eseguire `Set-ProvServiceConfigurationData` utilizzando l'SDK Remote PowerShell per impostare tutti i parametri applicabili. È anche possibile saltare l'abilitazione di DHCP durante la preparazione dell'immagine utilizzando questo comando. Di seguito è riportato l'elenco delle impostazioni supportate da `Set-ProvServiceConfigurationData`:

- Timeout di preparazione della modifica immagine: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout"-value 60`
- Salta Abilita DHCP: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Ex -Value EnableDHCP`
- Ignora la riattivazione del servizio di gestione delle chiavi (KMS) di Microsoft Windows: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Ignora la riattivazione di Microsoft Office KMS: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm`
- Disabilita la preparazione dello spegnimento automatico della macchina virtuale `Set-ProvServiceConfigurationData –Name ImageManagementPrep_NoAutoShutdown –Value true`
- Disabilita l'inserimento del dominio `Set-ProvServiceConfigurationData –Name DisableDomainInjection –Value true`

**Possibilità di impostare il tipo di licenza Linux durante la creazione di cataloghi di macchine**

**Linux utilizzando i comandi PowerShell.** Utilizzando i comandi PowerShell, è possibile impostare il tipo di licenza Linux durante la creazione di cataloghi di macchine Linux. Sono disponibili due opzioni per le licenze Linux "bring your own": RHEL_BYOS e SLES_BYOS. L'impostazione predefinita è la licenza Azure Linux. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

**Supporto dell'identificazione di tutte le risorse di Azure create da MCS.** È ora possibile identificare tutte le risorse di Azure create da MCS come Immagine, Disco ID, Disco sistema operativo, NIC, VM e così via, che sono associate a un ProvScheme utilizzando un tag chiamato `provschemeID`. Per ulteriori informazioni sui tag che MCS aggiunge alle risorse, vedere Identificare le risorse create da MCS.

**Supporto del provisioning di Azure Stack HCI tramite SCVMM.** MCS ora supporta il provisioning di Azure Stack HCI tramite Microsoft System Center Virtual Machine Manager (SCVMM). È possibile gestire il cluster HCI dello stack di Azure con i propri strumenti esistenti, incluso SCVMM. Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.

**Supporto dell'aggiunta manuale di utenti non Active Directory**. Utilizzando l'interfaccia di gestione Full Configuration, è ora possibile immettere un elenco di nomi utente separati da punto e virgola quando si aggiungono utenti non Active Directory per un catalogo. Tenere presente il formato quando si aggiungono utenti che risiedono in directory diverse. Ad esempio, se gli utenti si trovano in Active Directory, immettere direttamente i nomi. In caso contrario, inserire i nomi in questo formato: `<identity provider>:<user name>`. Esempio: `AzureAD:username`. Per ulteriori informazioni, vedere Creare cataloghi di macchine.

## aprile 2022

### Funzionalità nuove e migliorate

**Home page per l'interfaccia Full Configuration**. Full Configuration ha ora una home page, che fornisce una panoramica della distribuzione e dei carichi di lavoro di Citrix DaaS insieme a informazioni che consentono di ottenere il massimo dalla propria sottoscrizione. La pagina comprende le seguenti parti:

- **Panoramica del servizio**. Fornisce una panoramica della distribuzione e dei carichi di lavoro di Citrix DaaS.
- **Raccomandazioni**. Raccomanda le funzionalità disponibili con la propria sottoscrizione e raccoglie commenti e suggerimenti.
- **Novità**. Mostra le funzionalità più recenti.
- **Funzionalità di anteprima**. Mostra le funzionalità attualmente in anteprima.
- **Per iniziare**. Mostra i passaggi della configurazione iniziale.

Per ulteriori informazioni, vedere Home page.

**Mostrare lo stato di avanzamento della creazione e degli aggiornamenti del catalogo**. Full Configuration ora mantiene aggiornati sulla creazione e sugli aggiornamenti del catalogo. È possibile ottenere una panoramica del processo di creazione e aggiornamento, visualizzare la cronologia dei passaggi eseguiti e monitorare lo stato di avanzamento e il tempo di esecuzione del passaggio corrente. Per ulteriori informazioni, vedere Iniziare a creare il catalogo.

**Visualizzare gli hypervisor e i servizi cloud disponibili in base alla zona selezionata**. In Full Configuration, quando si creano connessioni di hosting, è necessario selezionare una zona prima di selezionare un tipo di connessione. L'elenco a discesa Connection type (Tipo di connessione) contiene gli hypervisor e i servizi cloud disponibili con la zona. In precedenza, per garantire che l'elenco Connection type contenesse un hypervisor o un servizio cloud richiesto, era necessario installare il relativo plug-in in ogni zona. Con questa nuova sequenza di configurazione, ora è possibile installare il plug-in solo nella zona richiesta.

È inoltre possibile utilizzare il comando PowerShell per ottenere l'elenco dei plug-in hypervisor disponibili con la zona selezionata. Per ulteriori informazioni, vedere Creare una connessione e risorse.

**Supporto degli utenti non locali iscritti ad AD in Full Configuration**. È disponibile un nuovo campo, **Select identity type** (Seleziona tipo di identità), nelle interfacce in cui si assegnano gli utenti a desktop o app di cui è stato eseguito il provisioning, gruppi di consegna o gruppi di applicazioni. Con il campo, ora è possibile selezionare gli account utente da uno dei seguenti provider di identità a cui è connesso Citrix Cloud:

- Active Directory
- Azure Active Directory
- Okta

**Possibilità di rifiutare le proprietà personalizzate non valide negli ambienti Google Cloud Platform (GCP) e Azure**. Ora è possibile evitare una potenziale confusione se le proprietà personalizzate impostate su `New-ProvScheme` e `Set-ProvScheme` non hanno effetto. Se si specificano proprietà personalizzate non esistenti, viene visualizzato un messaggio di errore. Per ulteriori informazioni, vedere Important consideration about setting custom properties.

**Supporto della creazione di macchine aggiunte ad Azure Active Directory**. In **Full Configuration**, quando si crea un catalogo, un tipo di identità **aggiunto ad Azure Active Directory** è ora disponibile in **Machine Identities**. Con quel tipo di identità, è possibile utilizzare MCS per creare macchine aggiunte ad Azure Active Directory. È inoltre disponibile un'opzione aggiuntiva, **Enroll the machines in Microsoft Intune**, per registrare le macchine in Microsoft Intune per la gestione.

Per informazioni sulla creazione di cataloghi aggiunti ad Azure Active Directory, vedere Creare cataloghi di macchine. Per informazioni sui requisiti e le considerazioni relative all'aggiunta ad Azure Active Directory, vedere Azure Active Directory joined.

**Supporto della creazione di macchine aggiunte ad Azure Active Directory ibride**. In **Full Configuration**, quando si crea un catalogo, è ora disponibile un tipo di identità **aggiunto ad Azure Active Directory ibrido** in **Identità macchina**. Con quel tipo di identità, è possibile utilizzare MCS per creare macchine aggiunte ad Azure Active Directory ibrido. Tali macchine sono di proprietà di un'organizzazione e hanno effettuato l'accesso con un account Active Directory Domain Services appartenente a tale organizzazione.

Per informazioni sulla creazione di cataloghi aggiunti ad Azure Active Directory ibridi, vedere Creare cataloghi di macchine. Per informazioni sui requisiti e le considerazioni relative all'aggiunta ibrida ad Azure Active Directory, vedere Aggiunto ad Azure Active Directory ibrido.

**Supporto dell'avvio attendibile di Azure per le snapshot.** Oltre alle immagini, l'avvio attendibile di Azure è ora disponibile anche per le snapshot. Se si seleziona una snapshot con avvio attendibile abilitato, l'utilizzo di un profilo macchina è obbligatorio. Inoltre, è necessario selezionare un profilo macchina con l'avvio attendibile abilitato. Per ulteriori informazioni, vedere Ambienti cloud Microsoft Azure Resource Manager.

**Macchine per l'esportazione.** È ora possibile esportare le macchine elencate nella pagina **Machines** della procedura guidata **Machine Catalog Setup** (Configurazione catalogo macchine) in un file CSV, da utilizzare come modello quando si aggiungono macchine a un catalogo in blocco. Per ulteriori informazioni, vedere Export machines from a catalog.

**Opzione per accedere alla console Web Workspace Environment Management**. Un'opzione, Environment Management (Web), è ora disponibile nel menu della scheda **Manage**. L'opzione offre l'accesso alla nuova console di Workspace Environment Management basata sul Web. Per accedere alla console precedente, utilizzare **Environment Management** (Gestione dell'ambiente). Stiamo migrando l'intero set di funzionalità dalla console legacy alla console Web. La console Web generalmente risponde più velocemente rispetto alla console legacy. Per ulteriori informazioni, vedere Servizio WEM (Workspace Environment Management).

**Capacità di gestire i parametri ProvScheme.** Quando si utilizza MCS per creare un catalogo, ora viene visualizzato un errore se si impostano i parametri `New-ProvScheme` in hypervisor non supportati durante la creazione del catalogo macchine o si aggiornano i `Set-ProvScheme` parametri dopo la creazione del catalogo macchine. Per ulteriori informazioni, vedere Creare cataloghi delle macchine.

**Limiti delle posizioni di risorse aumentati.** I limiti delle posizioni di risorse per VDA a sessione singola e VDA multisessione sono ora aumentati rispettivamente a 10000 e 1000. Per maggiori informazioni, vedere Limiti.

**Supporto del riavvio di macchine ad alimentazione non gestita dopo aver svuotato tutte le sessioni.** Citrix DaaS ora consente di creare pianificazioni di riavvio per macchine con alimentazione non gestita dopo che tutte le sessioni sono state esaurite dalle macchine. Nell'interfaccia Full Configuration, selezionare **Restart all machines after draining all sessions** (Riavvia tutte le macchine dopo

aver esaurito tutte le sessioni) in **Restart duration** (Durata del riavvio). Per ulteriori informazioni, vedere Creare una pianificazione di riavvio.

**Supporto dell'aggiornamento delle macchine VDA (anteprima).** Utilizzando l'interfaccia Full Configuration, è ora possibile aggiornare le macchine VDA per la distribuzione Citrix DaaS. È possibile aggiornarle per catalogo o per macchina. La funzione si applica alle macchine che non sono state create utilizzando MCS (ad esempio, macchine fisiche). Per ulteriori informazioni, vedere Upgrade VDAs using the Full Configuration interface.

**Le macchine non vengono spente durante le interruzioni.** Citrix DaaS ora impedisce che le macchine virtuali vengano chiuse dal broker quando la zona in cui si trovano subisce un'interruzione. Le macchine diventano automaticamente disponibili per i collegamenti al termine dell'interruzione. Non è necessario intraprendere alcuna azione per rendere disponibili le macchine dopo l'interruzione.

**Diagnostica di avvio della sessione**. Citrix DaaS ora supporta la diagnostica avianzata degli errori di avvio delle sessioni. Utilizzare l'ID transazione a 32 cifre (8-4-4-4-12) generato dall'app Citrix Workspace dall'interno di Citrix Monitor (ovvero il servizio Citrix Director) per restringere il campo al componente e alla fase esatti in cui si è verificato il problema e applicare quindi le azioni consigliate per risolverlo. Per ulteriori informazioni, vedere Diagnostica di avvio della sessione.

**Opzione per accedere al servizio di registrazione della sessione**. Un'opzione, Session Recording (Registrazione sessione), è ora disponibile nel menu della scheda **Manage**. L'introduzione del servizio di registrazione delle sessioni fornisce una gestione centralizzata dei criteri, della riproduzione e delle configurazioni del server. Allevia il carico degli amministratori IT fornendo un punto di ingresso unificato per gestire e osservare gli oggetti distribuiti in tutta l'organizzazione. Per ulteriori informazioni, vedere Session Recording service (preview).

**Rebranding del servizio Citrix Virtual Apps and Desktops**. Il **servizio Citrix Virtual Apps and Desktops** è stato rinominato **Citrix DaaS**. Ulteriori informazioni sul cambio di nome nel nostro annuncio sul nostro blog.

Le seguenti offerte del servizio Citrix Virtual Apps and Desktops sono state rinominate.

- Il **servizio Citrix Virtual Apps Advanced** è stato rinominato **Citrix DaaS Advanced**.
- Il **servizio Citrix Virtual Apps Premium** è stato rinominato **Citrix DaaS Premium**.
- Il **servizio Citrix Virtual Desktops** è stato rinominato **Citrix DaaS Advanced Plus**.
- Il **servizio Citrix Virtual Apps and Desktops Advanced** è stato rinominato **Citrix DaaS Advanced Plus**.
- Il **servizio Citrix Virtual Apps and Desktops Premium** è ora disponibile come **Citrix DaaS Premium e Citrix DaaS Premium Plus**.
- **Citrix Virtual Apps and Desktops Standard per Azure** è stato rinominato **Citrix DaaS Standard per Azure**.

- **Citrix Virtual Apps and Desktops Standard per Google Cloud** è stato rinominato **Citrix DaaS Standard per Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium per Google Cloud** è stato rinominato **Citrix DaaS Premium per Google Cloud**.

L'implementazione di questa transizione nei nostri prodotti e nella relativa documentazione è un processo continuo. La pazienza dimostrata durante questa transizione è apprezzata.

- L'interfaccia utente del prodotto, il contenuto interno del prodotto e le immagini e le istruzioni nella relativa documentazione verranno aggiornati nelle prossime settimane.
- È possibile che alcuni elementi (come comandi e MSI) continuino a mantenere i nomi precedenti per evitare che gli script esistenti dei clienti smettano di funzionare.
- La documentazione relativa al prodotto e altre risorse (come video e post dei blog) accessibili tramite collegamenti presenti nella documentazione di questo prodotto potrebbero ancora contenere i nomi precedenti.

> **Nota:**
>
> Il nome del prodotto **Citrix Virtual Apps and Desktops** in locale rimane lo stesso.

**Supporto dei tenant in Full Configuration** È ora possibile creare partizioni di configurazione all'interno di una singola istanza di Citrix DaaS. È possibile ottenere questo risultato creando ambiti tenant in **Administrators > Scopes** (Amministratori > Ambiti) e associando gli oggetti di configurazione correlati, ad esempio cataloghi macchine e gruppi di consegna, a tali tenant. Di conseguenza, gli amministratori con accesso a un tenant possono gestire solo gli oggetti associati al tenant. Questa funzione è utile, ad esempio, se la propria organizzazione:

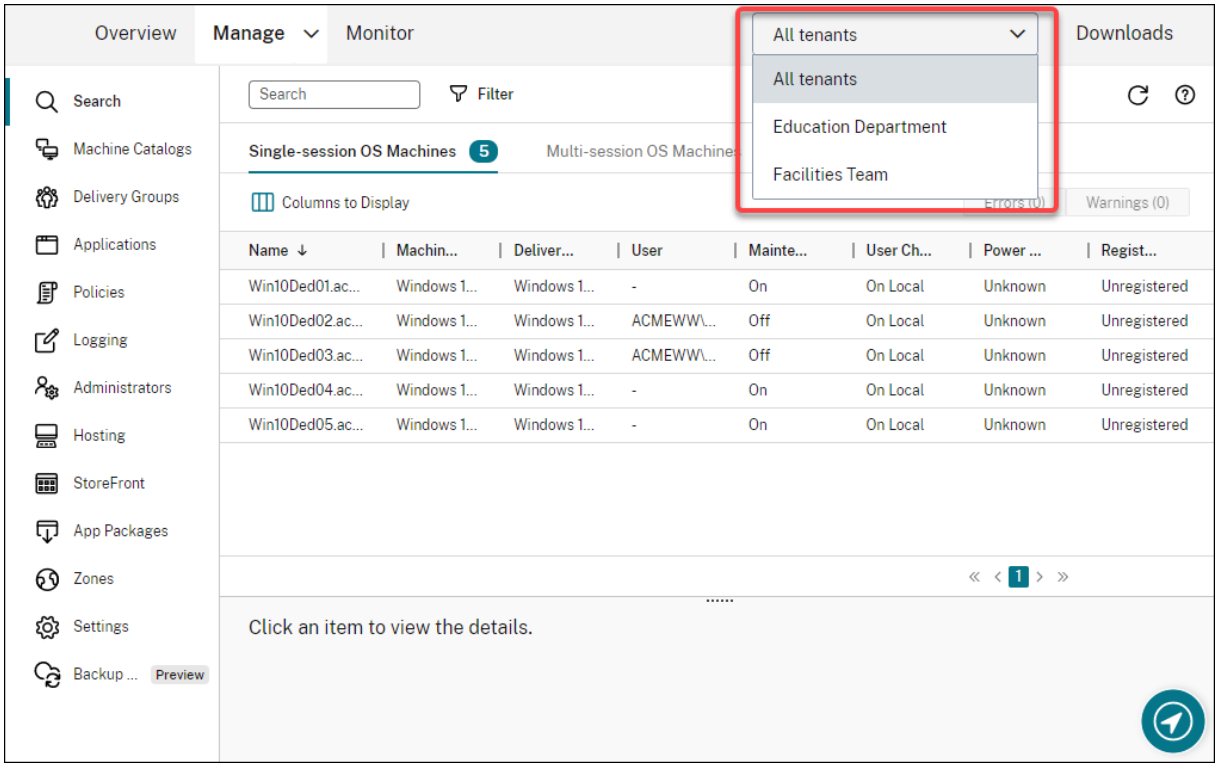
- Dispone di silos aziendali diversi (divisioni indipendenti o team di gestione IT separati) o
- Dispone di più siti locali e desidera mantenere la stessa configurazione in una singola istanza di Citrix DaaS.

Inoltre, l'interfaccia Full Configuration consente di filtrare i clienti tenant per nome. Per impostazione predefinita, l'interfaccia visualizza informazioni su tutti i tenant.

La funzione è disponibile sia per i Citrix Service Provider (CSP) che per i non-CSP. L'interfaccia di un ambiente CSP è essenzialmente la stessa di quella di un ambiente non CSP, a eccezione del metodo utilizzato per creare i tenant.

- I CSP inseriscono i clienti tenant su Citrix DaaS e quindi configurano l'accesso amministratore a Citrix DaaS. Per ulteriori informazioni, vedere Citrix DaaS for Citrix Service Providers.
- I non-CSP creano clienti tenant creando prima gli ambiti e quindi configurando l'accesso personalizzato per i rispettivi amministratori. Per ulteriori informazioni, vedere Creare e gestire ambiti.




**Aggiornamenti di Autoscale**. Abbiamo aggiornato Autoscale in stile a pannelli per offrire una migliore esperienza utente. I flussi di lavoro per la configurazione delle impostazioni rimangono gli stessi. Altri aggiornamenti di Autoscale includono:

- Rinominato **Restrict Autoscale** (Limita Autoscale) in **Autoscaling Tagged Machines** (Autoscale delle macchine con tag) per facilitarne la comprensione.
- Aggiunta una nuova opzione: **Control when Autoscale starts powering on tagged machines** (Controlla quando Autoscale inizia ad accendere le macchine etichettate). L'opzione consente di controllare quando Autoscale inizia ad alimentare le macchine con tag in base all'utilizzo di macchine senza tag.

Per ulteriori informazioni sull'Autoscale delle macchine con tag, vedere Autoscale tagged machines (Autoscale delle macchine con tag).

**Controlli di validità della licenza**. L'interfaccia Full Configuration ora controlla automaticamente la validità delle licenze utilizzate dalle connessioni host. Una connessione host viene messa in modalità di manutenzione se la licenza non è valida. Di conseguenza, non è possibile eseguire determinate operazioni, come la modifica della connessione e la disattivazione della modalità di manutenzione. Una licenza diventa non valida, ad esempio, quando:

- La licenza è scaduta. In questo caso, rivolgersi al rappresentante di vendita Citrix per rinnovarla o acquistare nuove licenze.
- La licenza è stata eliminata dal License Server.

**Stile a pannelli applicato ai nodi Machine Catalogs (Cataloghi macchine) e Policies (Criteri)**. Lo stile a pannelli viene ora applicato a tutti i nodi di Full Configuration.

**Supporto dell'aggiornamento di macchine di cui è stato eseguito il provisioning con MCS in ambienti Azure**. `Set-ProvScheme` modifica il modello (schema di provisioning) e non influisce sulle macchine esistenti. Utilizzando il comando Request-ProvVMUpdate, è ora possibile applicare lo schema di provisioning corrente a una macchina (o set di macchine) esistente. Attualmente, l'aggiornamento delle proprietà supportato da questa funzionalità è `ServiceOffering`. Per ulteriori informazioni, vedere Aggiornare le macchine di cui è stato eseguito il provisioning allo stato corrente dello schema di provisioning.

## marzo 2022

### Funzionalità nuove e migliorate

**Citrix Virtual Apps and Desktops per Google Cloud è ora disponibile in Google Cloud Marketplace.** Citrix Virtual Apps and Desktops Premium per Google Cloud è ora disponibile per l'acquisto su Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium per Google Cloud esegue il piano di controllo del servizio Citrix Virtual Apps and Desktops su Google Cloud.

**Supporto dell'avvio attendibile di Azure**. L'avvio attendibile di Azure è ora disponibile per l'interfaccia di gestione Full Configuration. Se si sceglie di selezionare un'immagine con l'avvio attendibile abilitato, l'uso di un profilo macchina è obbligatorio. Inoltre, è necessario selezionare un profilo macchina con l'avvio attendibile abilitato. Per ulteriori informazioni, vedere Ambienti cloud Microsoft Azure Resource Manager.

**È stato applicato lo stile a pannelli alle procedure guidate in altri tre nodi di Full Configuration.** I nodi sono **Search** (Ricerca), **Delivery Groups** (Gruppi di consegna) e **Applications** (Applicazioni).

**Image Portability Service (IPS) è stato rilasciato per la disponibilità generale.** IPS semplifica la gestione delle immagini su più piattaforme. Questa funzione è utile per la gestione delle immagini tra una posizione risorsa locale e il cloud pubblico. Le API REST di Citrix Virtual Apps and Desktops possono essere utilizzate per automatizzare l'amministrazione delle risorse all'interno di un sito Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere Migrare i carichi di lavoro nel cloud pubblico.

## febbraio 2022

### Funzionalità nuove e migliorate

**Autorizzazioni di Azure**. Sono necessarie due serie di autorizzazioni per i requisiti di sicurezza e per ridurre al minimo i rischi.

- Autorizzazioni minime: questa serie di autorizzazioni offre un migliore controllo di sicurezza. Tuttavia, le nuove funzionalità che richiedono autorizzazioni aggiuntive non funzioneranno se si utilizzano le autorizzazioni minime.
- Autorizzazioni generali: questo insieme di autorizzazioni non impedisce di ottenere nuovi vantaggi di miglioramento.

Per ulteriori informazioni, vedere Informazioni sulle autorizzazioni di Azure.

**Supporto dell'utilizzo del disco temporaneo della macchina virtuale per ospitare il disco della cache write-back negli ambienti Azure**. È stata aggiunta un'opzione, **Use non-persistent write-back cache disk** (Usa disco cache write-back non persistente), alla pagina **Machine Catalog Setup > Disk Settings** (Configurazione catalogo macchine > Impostazioni disco) dell'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa). Selezionare questa opzione se non si desidera che il disco della cache write-back rimanga persistente per le macchine virtuali di cui è stato eseguito il provisioning. Con l'opzione selezionata, usiamo il disco temporaneo della macchina virtuale per ospitare il disco cache write-back se il disco temporaneo ha spazio sufficiente. In questo modo si riducono i costi. Per ulteriori informazioni, vedere Ambienti cloud Microsoft Azure Resource Manager.

**Aggiornamenti delle impostazioni predefinite della connessione host AWS.** I valori delle impostazioni predefinite della connessione host AWS vengono aggiornati a valori più alti e molto probabilmente uguali per tutte le configurazioni della piattaforma cloud AWS. Questo aiuta a creare connessioni host in ambienti cloud AWS, senza valutare e configurare i valori di impostazione predefiniti in base alla configurazione individuale. Per ulteriori informazioni, vedere Valori predefiniti della connessione host.

**È stato aggiunto il supporto di diversi livelli di archiviazione negli ambienti GCP.** È ora possibile fornire le seguenti proprietà personalizzate negli ambienti GCP per impostare il tipo di archiviazione dei dischi collegati alla macchina virtuale appena creata:

- Tipo di archiviazione
- IdentityDiskStorageType
- WBCDiskStorageType

Per ulteriori informazioni, vedere Citrix Virtual Apps and Desktops Service SDK.

**Modificare determinate impostazioni della macchina virtuale dopo aver creato i cataloghi di macchine virtuali Azure**. Utilizzando l'interfaccia di gestione Full Configuration, è ora possibile modificare le seguenti impostazioni dopo aver creato un catalogo:

- Dimensioni macchina
- Zone di disponibilità
- Profilo macchina
- Licenze Windows

A tale scopo, nel nodo **Full Configuration**, selezionare il catalogo e quindi selezionare **Edit Machine Catalog** (Modifica catalogo macchine) nella barra delle azioni. Per ulteriori informazioni, vedere Modificare un catalogo.

**Supporto dell'archiviazione del disco del sistema operativo temporaneo di Azure sul disco della cache o sul disco temporaneo.** Il servizio Citrix Virtual Apps and Desktops ora consente di archiviare il disco del sistema operativo temporaneo di Azure su un disco di cache o su un disco temporaneo per una macchina virtuale abilitata per Azure. Questa funzionalità è utile per gli ambienti Azure che richiedono un disco SSD a prestazioni più elevate rispetto a un disco rigido standard. Per ulteriori informazioni, vedere Ambienti cloud Microsoft Azure Resource Manager.

**Supporto dei cluster Nutanix su AWS**. Il servizio Citrix Virtual Apps and Desktops supporta i Nutanix Clusters su AWS. Nutanix Clusters semplifica il modo in cui le applicazioni vengono eseguite su cloud privati o su più cloud pubblici. Per ulteriori informazioni, vedere Nutanix clusters on AWS.

**Supporto del cloud VMware su Amazon Web Services (AWS)**. Il cloud VMware su Amazon Web Services (AWS) consente di migrare i carichi di lavoro Citrix locali basati su VMware nel cloud AWS e l'ambiente principale Citrix Virtual Apps and Desktops nel servizio Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere VMware Cloud on Amazon Web Services (AWS).

**Supporto della configurazione del disco cache write-back per macchine in esecuzione su Google Cloud Platform (GCP)**. Nell'interfaccia di gestione Full Configuration, quando si esegue il provisioning di macchine su GCP, è ora possibile configurare le seguenti impostazioni del disco della cache write-back:

- Dimensioni del disco
- Memoria allocata alla cache
- Tipo di archiviazione su disco
- Persistenza del disco

Per ulteriori informazioni, vedere Creare un catalogo macchine nell'articolo Ambienti di virtualizzazione Google Cloud Platform .

## gennaio 2022

### Funzionalità nuove e migliorate

**Supporto dei cluster Nutanix su AWS**. Il servizio Citrix Virtual Apps and Desktops ora supporta Nutanix Clusters su AWS. Questo supporto offre le stesse funzionalità di un cluster locale Nutanix. È supportato solo un singolo cluster, *Prism Element*. Per ulteriori informazioni, vedere Ambienti di virtualizzazione Nutanix.

**Nuove funzionalità disponibili in Cloud Health Check.** Cloud Health Check è stato aggiornato a una nuova versione con funzionalità tra cui:

- **Correzione automatica.** Cloud Health Check ora supporta il rilevamento e la risoluzione automatici di determinati problemi identificati sulle macchine in cui è in esecuzione. Ora è disponibile un rapporto sui risultati per evidenziare quali azioni specifiche sono state intraprese. Per ulteriori informazioni, vedere Correzione automatica.
- **Supporto della riga di comando.** Cloud Health Check può ora essere eseguito dalla riga di comando. Per ulteriori informazioni, vedere Esecuzione di Cloud Health Check dalla riga di comando.
- **Stato di Citrix Universal Injection Driver.** Cloud Health Check ora mostra lo stato del driver Citrix UVI e ha un controllo del registro eventi correlato per i driver Citrix UVI.
- **Controllo del registro di avvio della sessione.** Cloud Health check ora controlla le impostazioni del registro di avvio della sessione.
- **Aggiornamenti del rapporto di controllo.** Per gli elementi selezionati che hanno diversi punti di controllo, il rapporto di controllo finale ora elenca tutti i controlli che sono stati verificati per mostrare quali azioni sono state eseguite durante il controllo dello stato.

Per ulteriori informazioni, vedere Cloud Health Check.

**Risolvere i problemi di registrazione e avvio della sessione VDA utilizzando Full Configuration**. Utilizzando l'interfaccia di gestione Full Configuration, è ora possibile eseguire controlli che misurano l'integrità dei VDA. I controlli di integrità dei VDA identificano le possibili cause di problemi comuni di registrazione e avvio della sessione dei VDA. È possibile eseguire controlli di integrità singolarmente e in batch. Per ulteriori informazioni, vedere Controlli di integrità dei VDA.

**Possibilità di specificare la data di scadenza segreta di Azure per le connessioni esistenti**. Utilizzando l'interfaccia di gestione Full Configuration, è ora possibile specificare la data dopo la quale scade il segreto dell'applicazione. Per linee guida su come visualizzare la data di scadenza del segreto, vedere Ambienti cloud Microsoft Azure Resource Manager. Quando viene utilizzata, considerare le seguenti differenze:

- Per le entità servizio create manualmente in Azure, è possibile modificare direttamente la data di scadenza nella pagina **Edit Connection > Connection Properties** (Modifica connessione > Proprietà connessione).
- Per le prime modifiche della data di scadenza per le entità servizio create tramite Full Configuration per l'utente, passare a **Edit Connection > Edit settings > Use existing** (Modifica connessione > Modifica impostazioni > Usa esistente). Le modifiche successive potranno essere apportate nella pagina **Edit Connection > Connection Properties** (Modifica connessione > Proprietà connessione).

**Un pulsante per aggiungere amministratori**. Abbiamo aggiunto un pulsante, **Add Administrator** (Aggiungi amministratore), alla scheda **Full Configuration > Administrators > Administrators** (Configurazione completa > Amministratori > Amministratori). Il pulsante costituisce un modo rapido per

accedere a **Identity and Access Management > Administrators** (Gestione identità e accessi > Amministratori), dove è possibile aggiungere (invitare) amministratori. Per ulteriori informazioni, vedere Aggiungere un amministratore.

**Nuovo aspetto delle procedure guidate in Full Configuration**. Abbiamo aggiornato le procedure guidate nei seguenti nodi dando loro un nuovo stile, inclusi colori, caratteri e altre modifiche di formattazione, per offrire un'esperienza utente migliore: **Administrators**, **Hosting**, **StoreFront**, **App Packages**, **Zones** e **Settings**. Le nuove procedure guidate vengono visualizzate nelle viste in pannello con riquadri di visualizzazione più ampi, in modo da visualizzare una quantità maggiore di contenuti. I flussi di lavoro per la configurazione delle impostazioni rimangono gli stessi.

**Supporto della conservazione del disco di sistema quando l'I/O MCS è abilitato per le macchine in esecuzione su Google Cloud Platform (GCP)**. Nell'interfaccia di gestione Full Configuration, quando si esegue il provisioning di macchine su GCP, è ora possibile conservare il disco di sistema durante i cicli di alimentazione quando è abilitata l'ottimizzazione dell'archiviazione MCS (MCS I/O). Per ulteriori informazioni, vedere Abilitazione degli aggiornamenti per l'ottimizzazione dell'archiviazione MCS.

**Supporto del caricamento o il download diretto da EBS su Amazon Web Services (AWS)**. AWS ora fornisce API per consentire la creazione diretta di volumi EBS con il contenuto desiderato. È ora possibile utilizzare l'API per eliminare i requisiti di volume worker per la creazione di cataloghi e l'aggiunta di macchine virtuali. Per informazioni sulle autorizzazioni AWS richieste per questa funzionalità, vedere Amazon Web Services cloud environments.

**Capacità di identificare le risorse Amazon Web Services (AWS) create da MCS**. Abbiamo aggiunto un nuovo tag denominato `CitrixProvisioningSchemeID` per identificare le risorse AWS create da MCS. Per ulteriori informazioni, vedere Identificare le risorse create da MCS.

**Capacità di configurare l'accesso a Manage e Monitor**. L'interfaccia di gestione Full Configuration offre ora opzioni aggiuntive per controllare se concedere l'accesso ai ruoli personalizzati a **Manage** e **Monitor**. Per ulteriori informazioni, vedere Creare e gestire ruoli.

## dicembre 2021

### Funzionalità nuove e migliorate

**Supporto di Google Cloud VMware Engine**. La piattaforma ora consente di migrare i carichi di lavoro Citrix locali basati su VMware a Google Cloud e il proprio ambiente Citrix Virtual Apps and Desktops di base al servizio Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere Supporto di Google Cloud Platform (GCP) VMware Engine.

**Capacità di specificare come iniziano i nomi di account quando si specifica uno schema di denominazione**. Questa versione introduce un'opzione nella pagina **Machine Catalog Setup > Machine Identities** dell'interfaccia di gestione Full Configuration. L'opzione consente di specificare i

numeri o le lettere con cui iniziano i nomi degli account, offrendo un maggiore controllo sul modo in cui gli account delle macchine vengono denominati durante la creazione del catalogo. Per ulteriori informazioni, vedere Identità macchina.

**Supporto della creazione di connessioni Nutanix AHV XI e Nutanix AHV Prism Central (PC)**. Nell'interfaccia di gestione Full Configuration, ora è possibile creare connessioni PC Nutanix AHV XI e Nutanix AHV. Per ulteriori informazioni, vedere Ambienti di virtualizzazione Nutanix.

**Supporto della selezione del tipo di archiviazione per i dischi del sistema operativo durante il provisioning delle VM su GCP**. Nell'interfaccia di gestione Full Configuration, quando si esegue il provisioning di macchine virtuali su GCP, è ora possibile selezionare il tipo di archiviazione per il disco del sistema operativo. Le opzioni di archiviazione disponibili nella pagina **Machine Catalog Setup > Storage** (Configurazione catalogo computer > Archiviazione) includono **Standard persistent disk** (Disco persistente standard), **Balanced persistent disk** (Disco persistente bilanciato) e **SSD persistent disk** (Disco persistente SSD). Per ulteriori informazioni, vedere Creare un catalogo di macchine.

**L'interfaccia di gestione Full Configuration ora supporta il disco temporaneo di Azure**. In precedenza, PowerShell era l'unica scelta disponibile per creare macchine che utilizzavano dischi del sistema operativo effimeri. Ora abbiamo aggiunto un'opzione, **Azure ephemeral OS disk** (Disco del sistema operativo temporaneo di Azure), alla pagina **Machine Catalog Setup > Storage and License Types** (Configurazione catalogo macchine > Archiviazione e tipi di licenza). Selezionare l'opzione se si desidera utilizzare il disco locale della macchina virtuale per ospitare il disco del sistema operativo. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

**Proteggere le risorse gestite da Machine Creation Services (MCS) dall'eliminazione accidentale**. È ora possibile proteggere le risorse gestite da MCS su Google Cloud Platform (GCP) applicando il contrassegno `deletionProtection` di GCP abilitato per le macchine virtuali. Utilizzando l'autorizzazione `compute.instances.setDeletionProtection` o il ruolo IAM Compute Admin, è possibile reimpostare il contrassegno per consentire l'eliminazione della risorsa. Questa funzionalità è applicabile sia ai cataloghi persistenti che a quelli non persistenti. Per ulteriori informazioni, vedere Proteggersi dall'eliminazione accidentale di macchine.

## novembre 2021

### Funzionalità nuove e migliorate

**Annotare un'immagine durante l'aggiornamento delle macchine**. Nell'interfaccia di gestione Full Configuration, è ora possibile annotare un'immagine aggiungendo una nota apposita quando si aggiorna un catalogo creato da MCS. Ogni volta che si aggiorna il catalogo, viene creata una voce correlata alla nota se si aggiunge una nota. Se si aggiorna il catalogo senza aggiungere una nota, la voce viene visualizzata come null (-). Per visualizzare la cronologia delle note per l'immagine, selezionare

il catalogo, fare clic su **Template Properties** (Proprietà modello) nel riquadro inferiore e quindi fare clic su **View note history** (Visualizza cronologia note). Per ulteriori informazioni, vedere Aggiornare un catalogo.

**Supporto delle licenze multi-tipo**. L'interfaccia di gestione Full Configuration ora supporta le licenze multi-tipo, consentendo di specificare quale autorizzazione di licenza si desidera che sia utilizzata dal proprio sito (la distribuzione di un prodotto di servizio Citrix Virtual Apps and Desktops) o da un gruppo di consegna.

- A livello di sito, si determina quale licenza utilizzare in tutto il sito quando gli utenti avviano un'app o un desktop sui propri dispositivi. La licenza selezionata si applica a tutti i gruppi di consegna, ma non a quelli configurati con una licenza diversa.
- A livello di gruppo di consegna, si determina quale licenza si desidera che il gruppo di consegna utilizzi, godendo della flessibilità e dei vantaggi delle licenze multi-tipo.

Per ulteriori informazioni, vedere Licenze multi-tipo.

**Supporto della visualizzazione delle informazioni sul piano di acquisto di Azure Marketplace** Nell'interfaccia di gestione Full Configuration, quando si crea un catalogo macchine, è ora possibile visualizzare le informazioni sul piano di acquisto per le immagini master originate da immagini di Azure Marketplace.

## ottobre 2021

### Funzionalità nuove e migliorate

**Possibilità di aggiornare i cataloghi MCS persistenti**. Abbiamo introdotto l'opzione **Update Machines** (Aggiorna macchine) per i cataloghi MCS persistenti nell'interfaccia di gestione Full Configuration. L'opzione consente di gestire l'immagine o il modello utilizzato dal catalogo. Quando si aggiorna un catalogo persistente, tenere presente quanto segue: solo le macchine aggiunte al catalogo in un secondo momento vengono create utilizzando la nuova immagine o il nuovo modello. Non implementiamo l'aggiornamento alle macchine esistenti nel catalogo. Per ulteriori informazioni, vedere Aggiornare un catalogo.

**Opzione per il provisioning di macchine virtuali su un host dedicato di Azure**. È stata aggiunta un'opzione, **Use a host group** (Usa un gruppo host), alla pagina **Machine Catalog Setup > Master Image** (Configurazione catalogo macchine > Immagine master) dell'interfaccia di gestione Full Configuration. L'opzione consente di specificare quale gruppo host si desidera utilizzare per il provisioning di macchine virtuali in ambienti Azure. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

**Migliorare le prestazioni conservando una macchina virtuale di cui è stato effettuato il provisioning durante un ciclo di alimentazione**. È stata aggiunta un'impostazione, **Retain VMs across**

**power cycles** (Conserva le macchine virtuali attraverso i cicli di alimentazione), alla pagina **Machine Catalog Setup > Disk Settings** (Configurazione catalogo macchine > Impostazioni disco) dell'interfaccia di gestione Full Configuration. L'impostazione consente di conservare una macchina virtuale di cui è stato effettuato il provisioning durante un ciclo di alimentazione in ambienti Azure. Per ulteriori informazioni, vedere Ottimizzazione dell'archiviazione MCS. In alternativa, è possibile configurare la funzionalità utilizzando PowerShell. Per ulteriori informazioni, vedere Conservazione di una macchina virtuale di cui è stato eseguito il provisioning durante il ciclo di alimentazione.

**Associare un catalogo macchine a un set di configurazione Workspace Environment Management**. Quando si crea un catalogo di macchine, è ora possibile associarlo a un set di configurazione di Workspace Environment Management. In questo modo è possibile utilizzare il servizio Workspace Environment Management per offrire agli utenti la migliore esperienza di spazio di lavoro possibile. È inoltre possibile scegliere di associare il catalogo dopo averlo creato. Per ulteriori informazioni, vedere Creare cataloghi di macchine e Gestire i cataloghi delle macchine.

## settembre 2021

### Funzionalità nuove e migliorate

**Aggiungere una descrizione informativa per gli aggiornamenti delle immagini**. È ora possibile aggiungere descrizioni informative sulle modifiche correlate agli aggiornamenti delle immagini per i cataloghi delle macchine. Questa funzionalità è utile per gli amministratori che desiderano aggiungere etichette descrittive durante l'aggiornamento di un'immagine utilizzata da un catalogo, ad esempio *Office 365 installato*. Utilizzando i comandi di PowerShell, è possibile creare e visualizzare questi messaggi. Per informazioni dettagliate, vedere Aggiungere descrizioni a un'immagine.

**Integrazione con la soluzione Azure VMware (AVS)**. Il servizio Citrix Virtual Apps and Desktops supporta AVS, la soluzione Azure VMware. AVS fornisce un'infrastruttura cloud contenente cluster vSphere creati da Azure. Sfruttare il servizio Citrix Virtual Apps and Desktops per utilizzare AVS per il provisioning del carico di lavoro VDA nello stesso modo in cui si utilizzerebbe vSphere negli ambienti on-premise. Per ulteriori informazioni, vedere Integrazione con la soluzione Azure VMware.

**Stesso gruppo di risorse per più cataloghi**. Ora è possibile utilizzare lo stesso gruppo di risorse per l'aggiornamento e la creazione di cataloghi nel servizio Citrix Virtual Apps and Desktops. Questo processo:

- si applica a qualsiasi gruppo di risorse che contenga uno o più cataloghi di macchine.
- supporta i gruppi di risorse non creati da Machine Creation Services.
- crea la macchina virtuale e le risorse associate.
- elimina le risorse dal gruppo di risorse quando la macchina virtuale o il catalogo vengono rimossi.

Per ulteriori informazioni, vedere Gruppi di risorse di Azure.

**Recuperare informazioni per le macchine virtuali di Azure, le snapshot, il disco del sistema operativo e la definizione delle immagini della raccolta**. È possibile visualizzare informazioni su una macchina virtuale di Azure, sul disco del sistema operativo, la snapshot e la definizione delle immagini della raccolta. Queste informazioni vengono visualizzate per le risorse sull'immagine master quando viene assegnato un catalogo delle macchine. Utilizzare questa funzionalità per visualizzare e selezionare un'immagine Linux o Windows. Per ulteriori informazioni, vedere Recuperare informazioni per le macchine virtuali di Azure, le snapshot, il disco del sistema operativo e la definizione delle immagini della raccolta.

**Nuovo aggiornamento di Automated Configuration.** Automated Configuration è stato aggiornato a una nuova versione con funzionalità tra cui:

- Supporto Machines Creation Services (MCS): la configurazione automatizzata ora supporta i cataloghi MCS. Per ulteriori informazioni su MCS, vedere Informazioni sulla migrazione dei cataloghi con provisioning di Machine Creation Services.

Altri aggiornamenti di Automated Configuration includono:

- Supporto avanzato per le zone mediante la precompilazione del file ZoneMapping.yml con i nomi delle zone locali durante l'esportazione e le posizioni delle risorse cloud durante il backup.
- StoreFront è diventato un componente gestibile di alto livello. In precedenza StoreFront era gestito come parte di Delivery Groups. Questa separazione facilita meglio la fusione dei siti.
- `AddMachinesOnly` è diventato `MergeMachines` per corrispondere al modello per le opzioni di unione correnti e nuove.
- È stato aggiunto l'utilizzo del file SecurityClient.csv per importare ClientID e Secret durante la creazione e l'aggiornamento di CustomerInfo.yml quando si utilizzano i cmdlet di supporto.
- Aggiunta la migrazione delle preferenze della zona utente.
- Supporto fisso per il Control Plane giapponese.
- Altre correzioni e miglioramenti.

Scaricare Automated Configuration da Citrix Downloads. Per ulteriori informazioni su Automated Configuration, vedere Migrazione della configurazione a Citrix Cloud.

**Altre opzioni di pianificazione disponibili con le pianificazioni di riavvio**. L'interfaccia di gestione Full Configuration ora fornisce opzioni aggiuntive per controllare quando si verificano i riavvii pianificati. Oltre alle pianificazioni di riavvio ricorrenti giornaliere, ora è possibile impostare modelli di ricorrenza settimanali e mensili. Per ulteriori informazioni, vedere Creare una pianificazione di riavvio.

**Conservare le colonne personalizzate che degradano le prestazioni**. In precedenza, nel nodo **Search** dell'interfaccia di gestione Full Configuration, le colonne personalizzate che riducevano le prestazioni scomparivano dopo l'aggiornamento della finestra del browser o lo scollegamento dalla

console seguito dall'accesso. Ora è possibile decidere di conservare quelle colonne personalizzate. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Utilizzare lo strumento Automated Configuration per eseguire il backup e il ripristino**. Abbiamo aggiunto un nodo, **Backup and Restore**, all'interfaccia di gestione Full Configuration. Tale nodo raduna tutte le risorse correlate allo strumento Automated Configuration, comprese informazioni su:

- Pianificazione dei backup automatici della configurazione di Citrix Virtual Apps and Desktops utilizzando un unico comando
- Ripristino da un backup precedente, se necessario
- Esecuzione di backup e ripristino in modo granulare
- Altri casi d'uso supportati

Per ulteriori informazioni, vedere la documentazione relativa di Automated Configuration.

**Supporto dei cataloghi non aggiunti a un dominio**. È stato aggiunto un tipo di identità, **Non-domain-joined** (Non appartenente a un dominio), alla pagina **Machine Catalog Setup > Machine Identities** (Configurazione catalogo macchine > Identità macchina) dell'interfaccia di gestione Full Configuration. Con questo tipo di identità, è possibile utilizzare MCS per creare macchine che non sono state aggiunta ad alcun dominio. Per ulteriori informazioni, vedere Creare cataloghi delle macchine.

**Supporto dell'utilizzo di un profilo macchina**. È stata aggiunta un'opzione, **Use a machine profile** (Usa un profilo macchina), alla pagina **Machine Catalog Setup > Master Image** (Configurazione catalogo macchine > Immagine master) dell'interfaccia di gestione Full Configuration. L'opzione consente di specificare da quale profilo macchina si desidera che le macchine virtuali ereditino le configurazioni durante la creazione di macchine virtuali in ambienti Azure. Le macchine virtuali incluse nel catalogo possono ereditare la configurazione dal profilo macchina selezionato. Esempi di configurazioni includono:

- Networking accelerato
- Diagnostica di avvio
- Memorizzazione nella cache del disco host (relativa ai dischi del sistema operativo e MCSIO)
- Dimensioni della macchina (se non diversamente specificato)
- Tag posizionati sulla macchina virtuale

Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

**Supporto di Windows Server 2022.** Richiede come minimo un VDA 2106.

## agosto 2021

### Funzionalità nuove e migliorate

**Aumento del numero di elementi ordinabili da 500 a 5.000**. Nel nodo **Search** dell'interfaccia di gestione Full Configuration, è ora possibile ordinare fino a 5.000 elementi in base all'intestazione di qualsiasi colonna. Quando il numero di elementi supera 5.000, utilizzare i filtri per ridurre il numero di elementi a 5.000 o meno in modo da abilitare l'ordinamento. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

**Supporto di tipi di archiviazione di Azure aggiuntivi**. È ora possibile selezionare diversi tipi di archiviazione per le macchine virtuali in ambienti Azure utilizzando MCS. Per i dettagli, vedere Tipologie di archiviazione.

**Supporto della selezione del tipo di archiviazione per i dischi cache write-back**. Nell'interfaccia di gestione Full Configuration, quando si crea un catalogo MCS, è ora possibile selezionare il tipo di archiviazione per il disco cache write-back. I tipi di archiviazione disponibili includono: SSD Premium, SSD standard e HDD standard. Per ulteriori informazioni, vedere Creare cataloghi delle macchine.

**Spegnere le macchine in sospensione**. Nell'interfaccia **Manage > Full Configuration** (Gestione > Configurazione completa), è stata aggiunta un'opzione, **When no reconnection in (minutes)** (Quando non vi è riconnessione dopo (minuti)), alla pagina **Load-based Settings** (Impostazioni basate sul carico) dell'interfaccia utente Manage Autoscale per i gruppi di consegna di sistemi operativi a sessione singola. L'opzione diventa disponibile dopo aver selezionato **Suspend** (Sospensione), che consente di specificare quando arrestare le macchine in modalità di sospensione. Le macchine sospese rimangono disponibili per gli utenti disconnessi quando questi si riconnettono, ma non sono disponibili per i nuovi utenti. Lo spegnimento delle macchine le rende nuovamente disponibili per gestire tutti i carichi di lavoro. Per ulteriori informazioni, vedere Scalabilità automatica.

**Ampliato il supporto dell'utilizzo di file CSV per aggiungere macchine a un catalogo in blocco**. Nell'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa), ora è possibile utilizzare un file CSV per aggiungere in blocco le macchine già presenti nel data center a un catalogo in cui tali macchine hanno l'alimentazione gestita. Per ulteriori informazioni, vedere Creare cataloghi di macchine e Gestire i cataloghi delle macchine.

## luglio 2021

### Funzionalità nuove e migliorate

**Registrazione della configurazione**. L'interfaccia utente **Logging** (Registrazione) è diventata **Manage > Full Configuration**(Gestisci > Configurazione completa). Le seguenti tre schede comprendono l'interfaccia:

- **Eventi** (in precedenza, Configuration Logging). Questa scheda consente di tenere traccia delle modifiche alla configurazione e delle attività amministrative.
- **Tasks**. Questa scheda consente di visualizzare le attività relative al catalogo macchine.
- **API**. Questa scheda consente di visualizzare le richieste API REST effettuate durante un determinato periodo di tempo.

Per ulteriori informazioni, vedere Registrazione della configurazione.

**Autoscale ora fornisce opzioni di timeout dinamico della sessione**. È possibile configurare timeout di sessione disconnessa e inattiva per le ore di utilizzo di punta e non di punta per ottenere uno svuotamento della macchina più rapido e risparmi sui costi. Per ulteriori informazioni, vedere Timeout dinamici delle sessioni.

**Supporto delle chiavi di crittografia gestite dal cliente (CMEK) di Google Cloud Platform (GCP)**. È ora possibile utilizzare le CMEK di Google con i cataloghi MCS. Le CMEK offrono un maggiore controllo delle chiavi utilizzate per crittografare i dati all'interno di un progetto Google Cloud. Per ulteriori informazioni, vedere Customer-managed encryption keys (CMEK). Per configurare questa funzione, vedere Using Customer Managed Encryption Keys (CMEK). La funzione è disponibile nella pagina **Machine Catalog Setup > Disk Settings** (Configurazione catalogo macchine > Impostazioni disco) dell'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa).

> **Nota:**
>
> Questa funzionalità è disponibile come anteprima.

**Aggiornamenti della scheda Manage**. Abbiamo aggiornato le opzioni nel menu della scheda **Manage**:

- **Full Configuration**: in precedenza, questa opzione portava alla console legacy. Ora porta alla nuova console basata sul Web (Web Studio). La console basata sul Web è pienamente compatibile con la console legacy e include diversi miglioramenti. Consigliamo di iniziare a usarla subito.
- **Legacy Configuration** (Configurazione legacy): questa opzione consente di accedere alla console legacy, la cui rimozione è prevista per settembre 2021. Successivamente, **Full Configuration** sarà l'unica interfaccia che offre l'accesso all'intera gamma di azioni di configurazione e gestione.

**Web Studio ora supporta la scelta di una connessione di gestione dell'alimentazione per un catalogo di accesso remoto al PC**. In precedenza, era possibile utilizzare Studio per creare una connessione host con riattivazione su LAN alla posizione della risorsa (selezionando **Remote PC Wake on LAN** come tipo di connessione). Tuttavia, PowerShell era l'unica scelta per associare quella connessione a un catalogo di accesso remoto al PC. Ora è possibile usare Studio per raggiungere questo obiettivo. Per ulteriori informazioni, vedere Configurare la riattivazione LAN nell'interfaccia Full Configuration.

## giugno 2021

### Funzionalità nuove e migliorate

**Accedere alle immagini della raccolta immagini condivise di Azure**. Quando si crea un catalogo di macchine, è ora possibile accedere alle immagini dalla Raccolta immagini condivise di Azure nella schermata Master Image. Per informazioni dettagliate, vedere Accedere alle immagini dalla Raccolta immagini condivise di Azure.

**Supporto delle macchine virtuali schermate su Google Cloud Platform (GCP)**. È possibile effettuare il provisioning di macchine virtuali schermate su GCP. Una macchina virtuale schermata è rafforzata da una serie di controlli di sicurezza che forniscono l'integrità verificabile delle istanze di Compute Engine, utilizzando funzionalità avanzate di sicurezza della piattaforma quali l'avvio sicuro, un modulo di piattaforma attendibile virtuale, firmware UEFI e monitoraggio dell'integrità. Per ulteriori informazioni, vedere Shield VMs.

**Applicare HTTPS o HTTP**. Utilizzare le impostazioni del Registro di sistema per applicare il traffico HTTPS o HTTP attraverso il servizio XML.

**Usare sempre SSD standard per un disco di identità in modo da ridurre i costi negli ambienti Azure**. I cataloghi di macchine utilizzano il tipo di archiviazione SSD standard per i dischi di identità. Le unità SSD standard di Azure sono un'opzione di archiviazione conveniente e ottimizzata per i carichi di lavoro che richiedono prestazioni costanti a livelli di IOPS inferiori. Per ulteriori informazioni sui tipi di archiviazione, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

> **Nota:**
>
> Per ulteriori informazioni sui prezzi dei dischi gestiti di Azure, vedere Prezzi dei dischi gestiti.

**Nuova funzionalità disponibile in Web Studio**. Le seguenti funzionalità sono ora disponibili nella console basata sul Web:

- **Studio ora supporta l'autenticazione in Azure per creare un'entità di servizio**. È ora possibile stabilire una connessione host ad Azure autenticandosi in Azure per creare un'entità servizio. In questo modo si elimina la necessità di creare manualmente un'entità servizio nella sottoscrizione di Azure prima di creare una connessione in Studio. Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft Azure Resource Manager.
- **Studio ora supporta la clonazione di cataloghi di macchine esistenti**. Questa funzione consente di clonare un catalogo macchine esistente da utilizzare come modello per uno nuovo, eliminando la necessità di creare un catalogo simile da zero. Quando si clona un catalogo, non è possibile modificare le impostazioni associate al sistema operativo e alla gestione della macchina. Il catalogo clonato eredita tali impostazioni dall'originale. Per ulteriori informazioni, vedere Clonare un catalogo.

- **Un nuovo nodo chiamato Settings è ora disponibile nel pannello di navigazione di Studio**. Il nodo **Settings** (Impostazioni) consente di configurare le impostazioni che si applicano all'intero sito (la distribuzione di un prodotto di servizio Citrix Virtual Apps and Desktops). Sono disponibili le seguenti impostazioni:

  - **Load balance multi-session catalogs** (Cataloghi multisessione per il bilanciamento del carico). Selezionare l'opzione di bilanciamento del carico che soddisfa le proprie esigenze. Questa impostazione si applica a tutti i propri cataloghi. In precedenza, si accedeva a questa funzione facendo clic sull'icona a forma di ingranaggio nell'angolo in alto a destra della console. Per ulteriori informazioni, vedere Macchine di bilanciamento del carico.

- **Esperienza di ricerca migliorata in Studio**. In questa versione l'esperienza di ricerca in Studio è potenziata. Quando si utilizzano i filtri per eseguire una ricerca avanzata, la finestra Add filters (Aggiungi filtri) viene visualizzata in primo piano, lasciando invariata la vista di sfondo. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

- **Possibilità di sospendere e riprendere le macchine virtuali di Google Cloud in MCS**. È ora possibile sospendere e riprendere le macchine virtuali di Google Cloud in MCS come si farebbe con qualsiasi macchina virtuale. Per ulteriori informazioni, vedere Gestire i gruppi di consegna. Per abilitare questa funzionalità, impostare le autorizzazioni `compute.instances.suspend` e `compute.instances.resume` nell'account del servizio Google Cloud. Il ruolo Compute Admin è già dotato di queste autorizzazioni.

  In Citrix Virtual Apps and Desktops, è anche possibile utilizzare il comando `New-BrokerHostingPowerAc` di PowerShell per sospendere e riprendere le macchine virtuali. Per i dettagli, vedere New-Brokerhostingpoweraction.

  Google Cloud impone alcune limitazioni al tipo e alla configurazione delle istanze che possono essere sospese. Per ulteriori informazioni, vedere Sospendere e ripristinare una VM sul sito di Google Cloud.

## maggio 2021

### Funzionalità nuove e migliorate

**Riconnessione della sessione dopo la disconnessione da una macchina in modalità di manutenzione**. In precedenza, quando gli utenti del desktop a sessione singola (VDI) in pool (casuale) venivano disconnessi da una macchina in modalità di manutenzione, non era consentita la riconnessione della sessione a nessuna macchina del pool. Le macchine multisessione e le macchine statiche a sessione singola consentivano sempre la riconnessione della sessione in quella circostanza.

Ora, utilizzando PowerShell, è possibile controllare a livello di gruppo di consegna se è consentita la riconnessione della sessione dopo che si verifica una disconnessione su una macchina in modalità di

manutenzione. Questo vale per tutti i VDA del gruppo (a sessione singola e multisessione).

Per ulteriori dettagli, vedere Controllare la riconnessione della sessione quando è disconnessa dalla macchina in modalità di manutenzione.

**Supporto del probe delle applicazioni e dei desktop in tutte le edizioni di Citrix Virtual Apps and Desktops Service**. Oltre al supporto dell'edizione **Premium** esistente, il probe delle applicazioni e dei desktop è ora disponibile nelle edizioni **Citrix Virtual Apps Advanced Service** e **Citrix Virtual Apps and Desktops Advanced Service**.

**Nuova funzionalità disponibile in Web Studio**. La seguente funzionalità è ora disponibile nella console basata sul Web:

- **Studio ora supporta la selezione delle zone di disponibilità di Azure**. In precedenza, PowerShell era l'unica scelta per il provisioning di macchine in una zona di disponibilità specifica in ambienti Azure. Quando si utilizza Studio per creare un catalogo di macchine, è ora possibile selezionare una o più zone di disponibilità in cui si desidera eseguire il provisioning delle macchine. Se non viene specificata alcuna zona, Machine Creation Services (MCS) consente ad Azure di posizionare le macchine all'interno della regione. Se viene specificata più di una zona, MCS distribuisce in modo casuale le macchine nelle zone. Per maggiori informazioni, vedere Eseguire il provisioning delle macchine in zone di disponibilità specificate.

**Disco temporaneo di Azure**. Il servizio Citrix Virtual Apps and Desktops supporta il disco temporaneo di Azure. Un disco temporaneo consente di riutilizzare il disco della cache per archiviare il disco del sistema operativo per una macchina virtuale abilitata per Azure. Questa funzionalità è utile per gli ambienti Azure che richiedono un disco SSD a prestazioni più elevate rispetto a un disco rigido standard.

> **Nota:**
>
> I cataloghi persistenti non supportano i dischi del sistema operativo temporanei. Inoltre, quando si utilizza questa funzione, considerare che il disco ad alte prestazioni comporta un costo aggiuntivo. È utile riutilizzare il disco della cache per archiviare il disco del sistema operativo invece di sostenere il costo di un disco gestito aggiuntivo.

I dischi del sistema operativo temporanei richiedono che lo schema di provisioning utilizzi dischi gestiti e una Raccolta immagini condivise. Per ulteriori informazioni, vedere Dischi temporanei di Azure.

**Prestazioni migliorate per i VDA gestiti da MCS in Azure**. Il servizio Citrix Virtual Apps and Desktops migliora le prestazioni per i VDA gestiti con Machine Creation Services (MCS) in Azure. Questo miglioramento modifica i valori predefiniti per *le azioni simultanee assolute* per la connessione di hosting a 500 e il *numero massimo di nuove azioni al minuto* per la connessione di hosting a 2.000. Non sono necessarie attività di configurazione manuale per sfruttare questo miglioramento. Per informazioni dettagliate, vedere Limitazione delle richieste di Azure.

**Nuove funzionalità disponibili in Cloud Health Check**. Cloud Health Check è stato aggiornato a una nuova versione con funzionalità tra cui:

- **Rilevamento automatico delle macchine VDA**. Cloud Health Check è in grado di rilevare e recuperare automaticamente i VDA dalle distribuzioni del servizio Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere Recuperare macchine VDA.
- **Programmare i controlli di integrità**. Cloud Health Check ora consente di impostare pianificazioni per l'esecuzione di controlli di integrità periodici. Per ulteriori informazioni, vedere Utilità di pianificazione di Cloud Health Check.
- **Informazioni sulla versione di Cloud Health Check**. È ora possibile verificare quale versione di Cloud Health Check si sta utilizzando. Per visualizzare le informazioni sulla versione, fare clic sull'icona a forma di ingranaggio nell'angolo in alto a destra della finestra principale di Cloud Health Check.
- **Correzione automatica**. Cloud Health Check ora supporta il rilevamento e la risoluzione automatici di determinati problemi identificati sulle macchine in cui è in esecuzione. Per ulteriori informazioni, vedere Correzione automatica.

  > **Nota:**
  >
  > La correzione automatica è disponibile come anteprima.

## aprile 2021

### Funzionalità nuove e migliorate

**Recuperare le istanze dinamiche utilizzando l'API AWS**. Il servizio Citrix Virtual Apps and Desktops ora interroga AWS per recuperare i tipi di istanza in modo dinamico. Questa funzionalità elimina la necessità di creare un file `InstanceTypes.xml` personalizzato per quei clienti che desiderano utilizzare macchine di dimensioni superiori a quelle definite nel servizio Citrix Virtual Apps and Desktops. Queste informazioni in precedenza erano fornite dal file `InstanceTypes.xml`. Per facilitare questo accesso dinamico ai tipi di istanze AWS disponibili, gli utenti devono aggiornare le autorizzazioni sulle loro entità servizio in modo che includano le autorizzazioni `ec2:DescribeInstanceTypes`. Per supportare la compatibilità con le versioni precedenti per i clienti che scelgono di non aggiornare le proprie autorizzazioni delle entità servizio, vengono utilizzati i tipi di istanza AWS inclusi in `InstanceTypes.xml`. Questo processo genera un messaggio di avviso per il registro CDF MCS.

> **Nota:**
>
> Citrix Studio non visualizza il messaggio di avviso contenuto nel registro CDF.

Per ulteriori informazioni sulle autorizzazioni, vedere Definizione delle autorizzazioni IAM e Informazioni sulle autorizzazioni AWS.

**Nuova funzionalità disponibile in Web Studio**. La seguente funzionalità è ora disponibile nella console basata sul Web:

- **Studio ora visualizza la data e l'ora nel fuso orario in cui ci si trova**. In precedenza, Studio visualizzava solo la data e ora in base all'orologio e al fuso orario di sistema. Studio ora supporta la visualizzazione di data e ora locali del fuso orario dell'utente quando si passa il puntatore del mouse su un elemento evento. L'ora è espressa in UTC.

**Supporto I/O MCS per macchine virtuali di Azure senza archiviazione temporanea**. MCS I/O ora supporta la creazione di cataloghi di macchine per le macchine virtuali che non dispongono di dischi temporanei o di archiviazione collegata. Con questo supporto:

- La snapshot (disco gestito) viene recuperata dalla macchina virtuale di origine *senza* archiviazione temporanea. Le macchine virtuali incluse nel catalogo macchine non dispongono di archiviazione temporanea.
- La snapshot (disco gestito) viene recuperata dalla macchina virtuale di origine *con* archiviazione temporanea. Le macchine virtuali incluse nel catalogo macchine dispongono di archiviazione temporanea.

Per ulteriori informazioni, vedere Ottimizzazione dell'archiviazione MCS (Machine Creation Services)

**Nuova funzionalità disponibile in Web Studio**. La seguente funzionalità è ora disponibile nella console basata sul Web:

- **Force log off**. Autoscale ora consente di scollegare forzatamente le sessioni esistenti sulle macchine quando viene raggiunto il periodo di tolleranza stabilito, rendendo la macchina idonea allo spegnimento. Ciò consente ad Autoscale di spegnere le macchine molto più velocemente, riducendo così i costi. È possibile inviare notifiche agli utenti prima che vengano scollegati. Per ulteriori informazioni, vedere Scalabilità automatica.

**Nuovo aggiornamento di Automated Configuration.** Automated Configuration è stato aggiornato a una nuova versione con funzionalità tra cui:

- **Unione di più siti**: è possibile unire più siti in un sito unico evitando i conflitti di nomi mediante prefissi e suffissi. Per ulteriori informazioni, vedere Unire più siti in un unico sito.
- **Attivazione del sito**: è possibile scegliere se la propria distribuzione locale o sul cloud controlla risorse quali pianificazioni di riavvio e schemi di alimentazione. Per ulteriori informazioni, vedere Attivare i siti.

Altri aggiornamenti di Automated Configuration includono:

- La capacità di migrare ruoli e ambiti di amministratore.
- Un parametro `Quiet` per i cmdlet selezionati per eliminare la registrazione della console.
- Un parametro `SecurityFileFolder` per consentire il posizionamento del file CvadAcSecurity.yml in una condivisione di file di rete sicura che richiede l'autenticazione.
- Possibilità di filtrare in base al nome della macchina nei cataloghi di macchine e nei gruppi di consegna.
- Miglioramenti dei parametri di selezione dei componenti per utilizzare il metodo dei parametri switch, eliminando la necessità di aggiungere un `$true` dopo il nome del componente.
- Un nuovo cmdlet (`New-CvadAcZipInfoForSupport`) per comprimere tutti i file di registro da inviare a Citrix per assistenza.

Scaricare Automated Configuration da Citrix Downloads. Per ulteriori informazioni su Automated Configuration, vedere Migrazione al cloud.

**Conservare le istanze GCP durante i cicli di alimentazione.** Le istanze non persistenti di Google Cloud Platform (GCP) non vengono più eliminate allo spegnimento. Al contrario, le istanze vengono preservate attraverso i cicli di alimentazione. Quando un'istanza non persistente viene spenta, il disco del sistema operativo viene scollegato ed eliminato. Quando l'istanza è accesa, il disco del sistema operativo viene ricreato dal disco di base e collegato all'istanza esistente.

**Supporto delle immagini di Azure Gen2**. È ora possibile effettuare il provisioning di un catalogo di VM Gen2 utilizzando uno snapshot Gen2 o un disco gestito Gen 2 per migliorare le prestazioni in fase di avvio. Per ulteriori informazioni, vedere Creare cataloghi delle macchine. I seguenti sistemi operativi sono supportati per le immagini di Azure Gen2:

- Windows Server 2019, 2016, 2012 e 2012 R2
- Windows 10

> **Nota:**
>
> La creazione di un catalogo di macchine Gen2 utilizzando una snapshot Gen1 o un disco gestito non è supportata. Analogamente, non è supportata nemmeno la creazione di un catalogo macchine Gen1 utilizzando uno snapshot Gen2 o un disco gestito. Per ulteriori informazioni, vedere Supporto delle macchine virtuali di seconda generazione in Azure.

**Disabilitare gli account di archiviazione delle tabelle**. Machine Creation Services (MCS) non crea più account di archiviazione tabelle per i cataloghi che utilizzano dischi gestiti durante il provisioning di VDA in Azure. Per ulteriori informazioni, vedere Che cos'è l'archiviazione tabelle di Azure.

**Eliminazione dei blocchi negli account di archiviazione**. Quando si crea un catalogo in Azure utilizzando un disco gestito, non viene più creato un account di archiviazione. Gli account di archiviazione creati per i cataloghi esistenti rimangono invariati. Questa modifica è applicabile solo ai dischi gestiti.

Per i dischi non gestiti, non vi è alcuna variazione del comportamento esistente. Machine Creation Services (MCS) continua a creare account e blocchi di archiviazione.

**Nuove funzionalità disponibili in Web Studio**. Le seguenti funzionalità sono ora disponibili nella console basata sul Web:

- **Utilizzare una chiave di crittografia gestita dal cliente per crittografare i dati sulle macchine**. Studio ora aggiunge un'impostazione denominata **Customer-managed encryption key** (Chiave di crittografia gestita dal cliente) alla pagina **Machine Catalog Setup > Disk Settings** (Configurazione catalogo macchine > Impostazioni disco). L'impostazione consente di scegliere se crittografare i dati sulle macchine del catalogo di cui si intende eseguire il provisioning. Per ulteriori informazioni, vedere Chiave di crittografia gestita dal cliente.
- **Studio ora supporta la limitazione di Autoscale alle macchine etichettate**. In precedenza, era necessario utilizzare PowerShell per limitare la scalabilità automatica a determinate macchine di un gruppo di consegna. È ora possibile usare anche Studio. Per ulteriori informazioni, vedere Limitare Autoscale a determinate macchine di un gruppo di consegna.

## marzo 2021

### Funzionalità nuove e migliorate

**Host dedicati di Azure**. Gli host dedicati di Azure consentono di effettuare il provisioning di macchine virtuali su hardware dedicato a un singolo cliente. Durante l'utilizzo di un host dedicato, Azure garantisce che le macchine virtuali siano le uniche macchine in esecuzione su quell'host. Ciò fornisce maggiore controllo e visibilità ai clienti, garantendo così la soddisfazione dei loro requisiti di sicurezza interni o normativi. Quando si utilizza il parametro `HostGroupId`, è necessario un gruppo host di Azure preconfigurato nella regione dell'unità di hosting. È inoltre necessario il posizionamento automatico di Azure. Per ulteriori informazioni, vedere Host dedicati di Azure.

> **Suggerimento:**
>
> Quando si utilizzano host dedicati di Azure, la selezione della **zona di disponibilità di Azure** non ha alcun effetto. La macchina virtuale viene posizionata dal processo di posizionamento automatico di Azure.

**Supporto della crittografia lato server di Azure**. Il servizio Citrix Virtual Apps and Desktops supporta le chiavi di crittografia gestite dal cliente per i dischi gestiti di Azure. Con questo supporto è possibile gestire i requisiti organizzativi e di conformità crittografando i dischi gestiti del catalogo delle macchine utilizzando la propria chiave di crittografia. Per ulteriori informazioni, vedere Crittografia lato server di Azure.

**Eseguire il provisioning delle macchine in zone di disponibilità specificate in Azure**. È possibile effettuare il provisioning delle macchine in zone di disponibilità specifiche negli ambienti Azure. Con questa funzionalità:

- È possibile specificare una o più zone di disponibilità in Azure. Le macchine sono nominalmente distribuite equamente in tutte le zone fornite se è prevista più di una zona.
- La macchina virtuale e il disco corrispondente vengono posizionati nella zona specificata (o nelle zone specificate).
- È possibile esplorare le zone di disponibilità per verificare la presenza di una determinata offerta di servizi o regione. Le zone di disponibilità valide vengono visualizzate utilizzando i comandi PowerShell Visualizzare gli elementi di inventario che offrono servizi utilizzando `Get-Item`.

Per ulteriori informazioni, vedere Eseguire il provisioning delle macchine in zone di disponibilità specificate in Azure.

**Nuove funzionalità disponibili in Web Studio**. Le seguenti funzionalità sono ora disponibili nella console basata sul Web:

- **Studio ora supporta l'associazione di app a icone personalizzate**. In precedenza, era necessario utilizzare PowerShell per aggiungere icone personalizzate da utilizzare con le applicazioni pubblicate. Ora è anche possibile utilizzare Studio per farlo. Per ulteriori informazioni, vedere Gestire i gruppi di applicazioni.
- **Studio ora supporta l'applicazione di tag ai cataloghi di macchine**. In precedenza, era possibile utilizzare Studio per creare o eliminare tag da utilizzare con un catalogo. Tuttavia, era necessario utilizzare PowerShell per applicare i tag al catalogo. Ora è anche possibile utilizzare Studio per applicare tag a un catalogo o rimuoverle da esso come si fa con i gruppi di consegna. Per ulteriori informazioni, vedere Applicare i tag ai cataloghi di macchine.
- **Studio ora supporta la commutazione tra le modalità "bilanciamento del carico orizzontale"e "bilanciamento del carico verticale"**. In precedenza, PowerShell era l'unica scelta per passare dalla modalità di bilanciamento del carico orizzontale a quella verticale e viceversa. Studio ora offre maggiore flessibilità per controllare come bilanciare il carico di macchine con sistema operativo multisessione. Per ulteriori informazioni, vedere Macchine di bilanciamento del carico.
- **Studio ora supporta l'inclusione di macchine in modalità di manutenzione nelle pianificazioni di riavvio**. In precedenza, PowerShell era l'unica scelta per configurare i riavvii pianificati per le macchine in modalità di manutenzione. Ora è anche possibile utilizzare Studio per controllare se includere tali macchine in una pianificazione di riavvio. Per ulteriori informazioni, vedere Creare una pianificazione di riavvio.
- **Studio ora supporta la configurazione di Wake on LAN per Accesso remoto PC**. In precedenza, era necessario utilizzare PowerShell per configurare la riattivazione LAN per Accesso re-

moto PC. È ora possibile anche usare Studio per configurare quella funzionalità. Per ulteriori informazioni, vedere Configurare la riattivazione su LAN.

- **Studio ora supporta l'applicazione delle proprietà delle istanze AWS e l'assegnazione di tag alle risorse operative**. Quando si crea un catalogo per il provisioning delle macchine in AWS utilizzando MCS, è possibile specificare se applicare il ruolo IAM e le proprietà dei tag a tali macchine. È inoltre possibile specificare se applicare tag delle macchine alle risorse operative. Sono disponibili le due opzioni seguenti:

  - **Apply machine template properties to virtual machines** (Applica le proprietà dei modelli di macchine alle macchine virtuali)
  - **Apply machine tags to operational resources** (Applica i tag delle macchine alle risorse operative)

  Per ulteriori informazioni, vedere Applicare le proprietà delle istanze AWS e assegnare tag alle risorse operative.

**Raccolta immagini condivise di Azure**. Il servizio Citrix Virtual Apps and Desktops supporta la Raccolta immagini condivise di Azure come repository di immagini pubblicate per macchine di cui è stato eseguito il provisioning con MCS in Azure. Gli amministratori hanno la possibilità di archiviare un'immagine nella raccolta per accelerare la creazione e l'attivazione dei dischi del sistema operativo. Questo processo migliora i tempi di avvio del computer e delle applicazioni per le macchine virtuali non persistenti. Per i dettagli su questa funzionalità, vedere Raccolta immagini condivise di Azure.

> **Nota:**
>
> La funzionalità della Raccolta immagini condivise è compatibile con i dischi gestiti. Non è disponibile per i cataloghi delle macchine legacy.

**Bucket di archiviazione creati nella stessa regione di Google Cloud Platform del catalogo macchine**. Nelle release precedenti, MCS creava bucket di archiviazione temporanei durante il provisioning come parte del processo di caricamento del disco. Questi bucket si estendevano su più regioni, che Google definisce come una grande area geografica contenente due o più luoghi geografici. Questi bucket temporanei risiedevano nella posizione geografica degli Stati Uniti, indipendentemente dal luogo in cui era stato effettuato il provisioning del catalogo. MCS ora crea bucket di archiviazione nella stessa regione in cui si effettua il provisioning dei cataloghi. I bucket di archiviazione non sono più temporanei; rimangono nel proprio progetto Google Cloud Platform dopo aver completato il processo di provisioning. Le future operazioni di provisioning utilizzano il bucket di archiviazione esistente, se presente in quella regione. Viene creato un nuovo bucket di archiviazione se non esiste nella regione specificata.

## febbraio 2021

### Funzionalità nuove e migliorate

**Supporto delle immagini di Azure Gen2**. È ora possibile effettuare il provisioning di dischi gestiti utilizzando VM Gen2 in ambienti Azure per migliorare le prestazioni in fase di avvio. Sono supportati i seguenti sistemi operativi:

- Windows Server 2019, 2016, 2012 e 2012 R2
- Windows 10

> **Nota:**
>
> Con questo supporto, è supportato solo un sottoinsieme di macchine virtuali. Ad esempio, alcune macchine virtuali possono essere sia di tipo Gen1 che Gen2, mentre altre possono essere solo Gen1. Per ulteriori informazioni, vedere Supporto delle macchine virtuali di seconda generazione in Azure.

**Programmi di riavvio delle macchine**. Citrix Studio ora aggiunge l'opzione **Restart all machines after draining sessions** (Riavvia tutte le macchine dopo aver esaurito le sessioni) al menu **Restart duration** (Durata riavvio). L'opzione consente di scegliere se riavviare tutte le macchine dopo aver esaurito tutte le sessioni. Quando viene raggiunto l'orario del riavvio, le macchine vengono messe in stato di svuotamento e quindi riavviate quando tutte le sessioni sono scollegate. Per ulteriori informazioni, vedere Creare una pianificazione di riavvio.

**Nuove funzionalità disponibili in Web Studio**. Le seguenti funzionalità sono ora disponibili nella console basata sul Web:

- **Studio ora supporta l'utilizzo di file CSV per aggiungere macchine a un catalogo in blocco**. Questa funzione consente di utilizzare un file CSV per:
  - Aggiungere in blocco a un catalogo macchine con sistema operativo multisessione o a sessione singola nei casi in cui l'alimentazione delle macchine non è gestita mediante Studio.
  - Aggiungere le macchine a un catalogo di accesso remoto al PC in blocco. In precedenza, era necessario scegliere delle unità organizzative per aggiungere le macchine a un catalogo di accesso remoto al PC in blocco. Ciò, tuttavia, non è semplice in scenari con limitazioni della struttura delle unità organizzative. Questa funzionalità offre una maggiore flessibilità per l'aggiunta di macchine in blocco. È possibile aggiungere solo macchine (da utilizzare con assegnazioni automatiche degli utenti) o aggiungere macchine insieme alle assegnazioni utente.

  Per ulteriori informazioni, vedere Creare cataloghi di macchine e Gestire i cataloghi delle macchine.

- **Supporto esteso di Citrix Managed Azure.** Citrix Managed Azure è ora disponibile nelle seguenti edizioni del servizio Citrix Virtual Apps and Desktops: Standard per Azure, Advanced, Premium e Workspace Premium Plus.
- **Supporto del posizionamento di immagini master nella Raccolta immagini condivise di Azure**. Studio ora offre un'opzione che consente di inserire immagini master nella Raccolta immagini condivise di Azure (SIG). SIG è un repository per la gestione e la condivisione di immagini. Consente di rendere disponibili le immagini in tutta l'organizzazione. Si consiglia di memorizzare un'immagine in SIG quando si creano cataloghi macchine di grandi dimensioni non persistenti, perché in questo modo è possibile reimpostare più velocemente i dischi del sistema operativo del VDA. Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft Azure Resource Manager.
- **Conservare il disco di sistema per i cataloghi di macchine MCS in Azure**. Studio ora consente di controllare se conservare i dischi di sistema per i VDA durante i cicli di alimentazione. Normalmente, il disco di sistema viene eliminato all'arresto e ricreato all'avvio. Ciò garantisce che il disco sia sempre in uno stato pulito, ma comporta tempi di riavvio delle macchine virtuali più lunghi. Se le scritture di sistema vengono reindirizzate alla cache e riscritte sul disco della cache, il disco di sistema rimane invariato. Per evitare inutili operazioni di ricreazione del disco, utilizzare l'opzione **Retain system disk during power cycles** (Mantieni disco di sistema durante i cicli di alimentazione), disponibile nella pagina **Machine Catalog Setup > Disk Settings** (Configurazione catalogo macchine > Impostazioni disco). L'abilitazione di questa opzione riduce i tempi di riavvio delle macchine virtuali, ma aumenta i costi di archiviazione. Questa opzione può essere utile in scenari in cui un ambiente contiene carichi di lavoro con tempi di riavvio sensibili. Per ulteriori informazioni, vedere Ottimizzazione dell'archiviazione MCS.
- **Studio ora supporta la creazione di cataloghi di macchine MCS con disco cache write-back persistente**. In precedenza, PowerShell era l'unica scelta per creare un catalogo con disco cache write-back persistente. È ora possibile utilizzare Studio per controllare se il disco della cache write-back persiste per le macchine virtuali di cui è stato eseguito il provisioning in Azure durante la creazione di un catalogo. Se disabilitato, il disco della cache write-back viene eliminato durante ogni ciclo di alimentazione per risparmiare sui costi di archiviazione, causando la perdita di eventuali dati reindirizzati al disco. Per conservare i dati, abilitare l'opzione **Use persistent write-back cache disk** (Usa disco cache write-back persistente), disponibile nella pagina **Machine Catalog Setup > Disk Settings** (Configurazione catalogo computer > Impostazioni disco). Per ulteriori informazioni, vedere Ottimizzazione dell'archiviazione MCS.

**Supporto della protezione delle app per Citrix Virtual Apps and Desktops Service con StoreFront**. Per ulteriori informazioni, vedere Protezione delle app.

### gennaio 2021

**Nuove funzionalità disponibili in Web Studio**. Le seguenti funzionalità sono ora disponibili nella console basata sul Web:

- **Studio ora supporta l'associazione di app a icone personalizzate**. In precedenza, era necessario utilizzare PowerShell per aggiungere icone personalizzate da utilizzare con le applicazioni pubblicate. Ora è anche possibile utilizzare Studio per farlo. Per ulteriori informazioni, vedere Gestire i gruppi di applicazioni.
- **Studio ora supporta l'applicazione di tag ai cataloghi di macchine**. In precedenza, era possibile utilizzare Studio per creare o eliminare tag da utilizzare con un catalogo. Tuttavia, era necessario utilizzare PowerShell per applicare i tag al catalogo. Ora è anche possibile utilizzare Studio per applicare tag a un catalogo o rimuoverle da esso come si fa con i gruppi di consegna. Per ulteriori informazioni, vedere Applicare i tag ai cataloghi di macchine.
- **Studio ora supporta la commutazione tra le modalità "bilanciamento del carico orizzontale"e "bilanciamento del carico verticale"**. In precedenza, PowerShell era l'unica scelta per passare dalla modalità di bilanciamento del carico orizzontale a quella verticale e viceversa. Studio ora offre maggiore flessibilità per controllare come bilanciare il carico di macchine con sistema operativo multisessione. Per ulteriori informazioni, vedere Macchine di bilanciamento del carico.
- **Studio ora supporta l'inclusione di macchine in modalità di manutenzione nelle pianificazioni di riavvio**. In precedenza, PowerShell era l'unica scelta per configurare i riavvii pianificati per le macchine in modalità di manutenzione. Ora è anche possibile utilizzare Studio per controllare se includere tali macchine in una pianificazione di riavvio. Per ulteriori informazioni, vedere Creare una pianificazione di riavvio.
- **Studio ora supporta la configurazione di Wake on LAN per Accesso remoto PC**. In precedenza, era necessario utilizzare PowerShell per configurare la riattivazione LAN per Accesso remoto PC. È ora possibile anche usare Studio per configurare quella funzionalità. Per ulteriori informazioni, vedere Configurare la riattivazione su LAN.
- **Studio ora supporta l'applicazione delle proprietà delle istanze AWS e l'assegnazione di tag alle risorse operative**. Quando si crea un catalogo per il provisioning delle macchine in AWS utilizzando MCS, è possibile specificare se applicare il ruolo IAM e le proprietà dei tag a tali macchine. È inoltre possibile specificare se applicare tag delle macchine alle risorse operative. Sono disponibili le due opzioni seguenti:
  - **Apply machine template properties to virtual machines** (Applica le proprietà dei modelli di macchine alle macchine virtuali)
  - **Apply machine tags to operational resources** (Applica i tag delle macchine alle risorse operative)

Per ulteriori informazioni, vedere Applicare le proprietà delle istanze AWS e assegnare tag alle risorse operative.

- **Host dedicato per AWS**. Citrix Studio ora contiene un'opzione denominata **Use dedicated host** (Usa host dedicato) nella pagina **Machine Catalog Setup > Security** (Configurazione catalogo macchine > Sicurezza). Questa impostazione è adatta per le distribuzioni con restrizioni di licenza o requisiti di sicurezza che richiedono l'uso di un host dedicato. Con un host dedicato, si possiede un intero host fisico e l'addebito viene effettuato su base oraria. La proprietà di tale host consente di avviare tante istanze EC2 quante ne consente l'host, senza costi aggiuntivi. Per ulteriori informazioni, vedere Tenancy di AWS.
- **Studio ora supporta l'esecuzione immediata di una pianificazione di riavvio**. Studio ora consente di eseguire immediatamente una pianificazione di riavvio per riavviare tutte le macchine pertinenti della pianificazione. Per ulteriori informazioni, vedere Eseguire immediatamente un programma di riavvio.
- **Autoscale**. Autoscale offre le seguenti nuove funzionalità e miglioramenti:
  - **Studio ora supporta la visualizzazione di macchine in stato di svuotamento**. In precedenza, PowerShell era l'unica scelta per identificare le macchine in stato di svuotamento. Ora è possibile utilizzare Studio per identificare le macchine che si trovano in stato di svuotamento. Per ulteriori informazioni, vedere Visualizzare le macchine in stato di svuotamento.
  - **Studio ora supporta la definizione delle ore di punta a un livello granulare di 30 minuti per i gruppi di consegna VDI**. In precedenza, era necessario utilizzare PowerShell per definire le ore di punta per i giorni inclusi in una pianificazione a un livello granulare di 30 minuti per i gruppi di consegna VDI. Ora è anche possibile utilizzare Studio per farlo. Questo supporto consente di impostare il numero minimo di macchine in esecuzione in un gruppo di consegna VDI separatamente per ogni mezz'ora del giorno.

**Raccolta immagini condivise di Azure**. Il servizio Citrix Virtual Apps and Desktops supporta la Raccolta immagini condivise di Azure come repository di immagini pubblicate per macchine di cui è stato eseguito il provisioning con MCS in Azure. Gli amministratori hanno la possibilità di memorizzare un'immagine nella raccolta per accelerare la creazione e l'attivazione dei dischi del sistema operativo dall'immagine master. Questo processo migliora i tempi di avvio del computer e delle applicazioni per le macchine virtuali non persistenti.

La raccolta contiene i seguenti tre elementi:

- Raccolta. Le immagini sono memorizzate qui. MCS crea una raccolta per ogni catalogo delle macchine.
- Definizione dell'immagine della raccolta. Questa definizione include informazioni (tipo e stato del sistema operativo, regione di Azure) sull'immagine master. MCS crea una definizione di immagine per ogni immagine master creata per il catalogo.

- Versione dell'immagine della raccolta. Ogni immagine in una Raccolta immagini condivise può avere più versioni e ogni versione può avere più repliche in regioni diverse. Ogni replica è una copia completa dell'immagine master. Il servizio Citrix Virtual Apps and Desktops crea sempre una versione dell'immagine Standard_LRS (versione 1.0.0) per ogni immagine con il numero appropriato di repliche nella regione del catalogo. Questa configurazione si basa sul numero di macchine incluse nel catalogo, sul rapporto di replica configurato e sul numero massimo di repliche configurate.

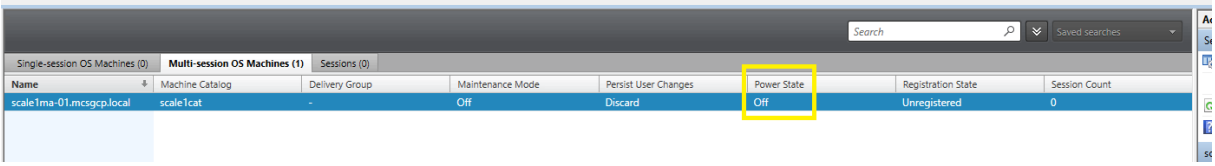
> **Nota:**
>
> La funzionalità Raccolta immagini condivise funziona solo con i dischi gestiti. Non è disponibile per i cataloghi delle macchine legacy.

Per dettagli su questa funzione, vedere Configurare la Raccolta immagini condivise.

**Bucket di archiviazione creati nella stessa regione di Google Cloud Platform del catalogo macchine**. Nelle release precedenti, MCS creava bucket di archiviazione temporanei durante il provisioning come parte del processo di caricamento del disco. Questi bucket si estendevano su più regioni, che Google definisce come una grande area geografica contenente due o più luoghi geografici. Questi bucket temporanei risiedevano nella posizione geografica degli Stati Uniti, indipendentemente dal luogo in cui era stato effettuato il provisioning del catalogo. MCS ora crea bucket di archiviazione nella stessa regione in cui si effettua il provisioning dei cataloghi. I bucket di archiviazione non sono più temporanei; rimangono nel proprio progetto Google Cloud Platform dopo aver completato il processo di provisioning. Le future operazioni di provisioning utilizzano il bucket di archiviazione esistente, se ne esiste uno in quella regione, oppure viene creato un nuovo bucket di archiviazione se non esiste nella regione specificata.

**Opzione PowerShell che imposta il valore predefinito per il riutilizzo di VDA in pool durante un'interruzione.** Una nuova opzione di comando di PowerShell (`-DefaultReuseMachinesWithoutShutdown`) estende la possibilità di riutilizzare i VDA desktop in pool che non sono stati arrestati durante un'interruzione, per impostazione predefinita. Vedere Supporto di applicazioni e desktop.

**Provisioning on demand di Google Cloud Platform**. Il servizio Citrix Virtual Apps and Desktops aggiorna il modo in cui Google Cloud Platform (GCP) effettua il provisioning dei cataloghi delle macchine. Quando si crea un catalogo di macchine, l'istanza di macchina corrispondente non viene creata in GCP e lo stato di alimentazione è impostato su **OFF**. Il provisioning delle macchine non avviene al momento della creazione del catalogo, ma alla prima accensione delle macchine. Ad esempio, dopo aver creato un catalogo, lo stato di alimentazione della macchina virtuale è impostato su **Off**:



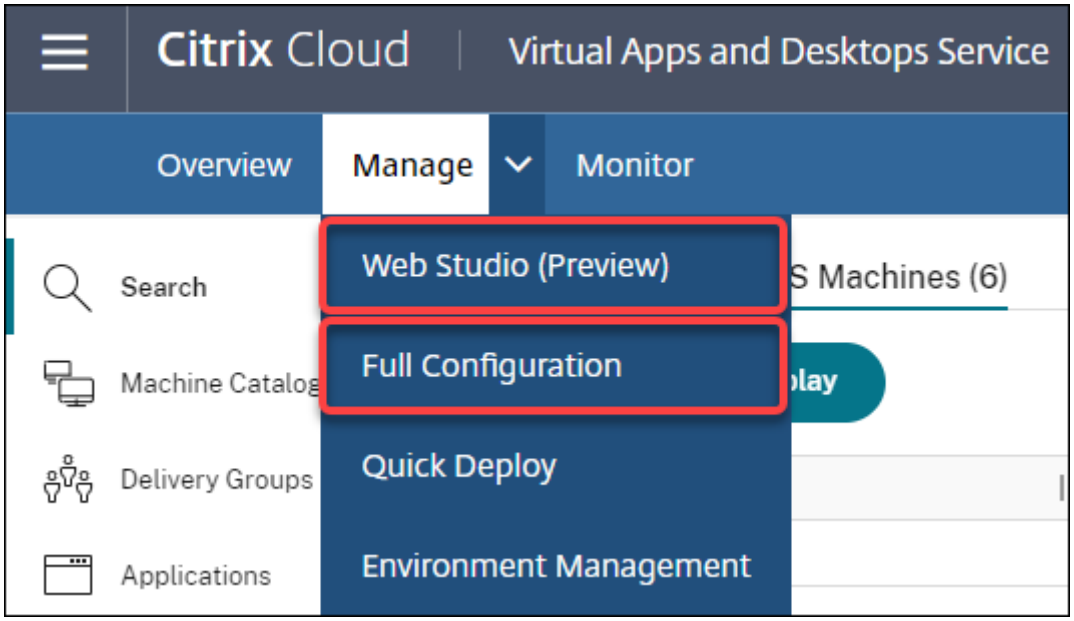

 

## dicembre 2020

### Funzionalità nuove e migliorate

**Web Studio è disponibile come anteprima**. È ora disponibile una nuova console Web. Stiamo migrando l'intero set di funzionalità di Studio dalla console legacy alla nuova console Web. La console Web generalmente risponde più velocemente rispetto alla console legacy. Per impostazione predefinita, si accede automaticamente alla console Web. È possibile passare facilmente dalla console Web alla console legacy dalla scheda **Manage** per eseguire le attività di configurazione o gestione del sito. Fare clic sulla freccia verso il basso accanto a **Manage** e selezionare un'opzione:

- **Web Studio (Preview)** [Web Studio (Anteprima)]. Porta alla nuova console Web.
- **Full Configuration** (Configurazione completa). Porta alla console legacy.




Le seguenti funzionalità sono disponibili solo nella console Web:

- **Supporto del tipo di disco SSD standard per Azure**. Studio ora aggiunge il supporto del tipo di disco SSD standard. Le unità SSD standard di Azure sono un'opzione di archiviazione conveniente e ottimizzata per i carichi di lavoro che richiedono prestazioni costanti a livelli di IOPS inferiori. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.
- **Studio ora supporta la configurazione del ritardo di spegnimento per i gruppi di consegna VDI statici**. In precedenza, era possibile configurare il ritardo di spegnimento per i gruppi di consegna VDI statici solo tramite PowerShell SDK. Studio ora consente di configurare il ritardo di spegnimento nell'interfaccia utente Autoscale per i gruppi di consegna VDI statici. Per ulteriori informazioni, vedere Scalabilità automatica.

## ottobre 2020

### Funzionalità nuove e migliorate

**Dismiss multiple hypervisor alerts** (Ignora più avvisi degli hypervisor). Citrix Monitor ora supporta l'eliminazione automatica degli avvisi degli hypervisor più vecchi di un giorno. Per ulteriori informazioni, vedere Monitoraggio degli avvisi di Hypervisor.

**Remove external IP address** (Rimuovi l'indirizzo IP esterno). Non è più necessario un indirizzo IP esterno su una macchina virtuale temporanea utilizzata per preparare un'immagine di cui è stato eseguito il provisioning in Google Cloud Platform (GCP). Questo indirizzo IP esterno consente alla macchina virtuale temporanea di accedere all'API pubblica di Google per completare il processo di provisioning.

Abilitare l'accesso privato a Google per consentire alla macchina virtuale di accedere all'API pubblica di Google direttamente dalla sottorete. Per maggiori informazioni, vedere Abilitare l'accesso privato a Google.

**Il nuovo modello affronta il modo in cui vengono gestite le identità delle macchine**. Le identità delle macchine utilizzate nei cataloghi macchine sono state gestite e mantenute utilizzando Active Directory. Tutte le macchine create da MCS entreranno ora in Active Directory. Il nuovo modello del servizio Citrix Virtual Apps and Desktops affronta il modo in cui vengono gestite le identità delle macchine. Questo modello consente la creazione di cataloghi di macchine utilizzando macchine collegate a *gruppi di lavoro*o non a dominio.

> **Suggerimento:**
>
> Questa funzionalità supporta un nuovo servizio di identità, *FMA trust*, aggiunto a Citrix Cloud per le macchine non associate a domini.

MCS comunica con il nuovo servizio fiduciario FMA per la gestione delle identità. Le informazioni sull'identità vengono archiviate nel disco di identità come coppia di GUID e coppie di chiavi private, invece del SID di dominio e del paradigma della password dell'account computer utilizzato da Active Directory. I VDA che utilizzano macchine non appartenenti a domini utilizzano questa combinazione di GUID e chiavi private per la registrazione del broker. Per maggiori informazioni, vedere Configurare il supporto per cataloghi non aggiunti al dominio.

**Usare il caricamento diretto per i dischi gestiti di Azure**. Questa versione consente di utilizzare il caricamento diretto durante la creazione di dischi gestiti in un ambiente Azure. Questa funzionalità riduce i costi associati agli account di archiviazione aggiuntivi. Non è più necessario lo staging del disco rigido virtuale in un account di archiviazione prima di convertirlo in un disco gestito. Inoltre, il caricamento diretto elimina la necessità di collegare un disco gestito vuoto a una macchina virtuale. Il caricamento diretto su un disco gestito di Azure semplifica il flusso di lavoro consentendo di copiare

direttamente un disco rigido virtuale locale per l'utilizzo come disco gestito. I dischi gestiti supportati includono HDD standard, SSD standard e SSD Premium.

Per ulteriori informazioni su questa funzionalità, vedere il blogdi Microsoft Azure.

Per ulteriori informazioni sui dischi gestiti di Azure, vedere la pagina della documentazione.

**Gruppo di risorse singolo in Azure**. Ora è possibile creare e utilizzare un singolo gruppo di risorse di Azure per l'aggiornamento e la creazione di cataloghi in Citrix Virtual Apps and Desktops. Questo miglioramento si applica sia alle entità servizio a tutto campo che a quelle ad ambito ristretto.
Il precedente limite di 240 macchine virtuali per 800 dischi gestiti per ciascun gruppo di risorse di Azure è stato rimosso. Non ci sono più limiti al numero di macchine virtuali, dischi gestiti, snapshot e immagini per ciascun gruppo di risorse di Azure.

Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft Azure Resource Manager.

## settembre 2020

### Funzionalità nuove e migliorate

**Quick Deploy**. La nuova funzionalità Quick Deploy sostituisce la precedente Azure Quick Deploy. La nuova funzionalità costituisce un modo rapido per iniziare a utilizzare il servizio Citrix Virtual Apps and Desktops utilizzando Microsoft Azure. È possibile utilizzare Quick Deploy per distribuire desktop e app e configurare l'accesso remoto al PC.

**Amministratore di sessione (ruolo integrato)**. È stato aggiunto a Citrix Studio un nuovo ruolo integrato chiamato **Session Administrator**. Il ruolo consente a un amministratore di visualizzare i gruppi di consegna e gestire le sessioni e le macchine associate nella pagina **Filters** della scheda **Monitor**. Con questa funzione è possibile definire le autorizzazioni di accesso degli amministratori esistenti o degli amministratori che si invitano in modo appropriato al loro ruolo nell'organizzazione. Per ulteriori informazioni sul ruolo integrato, vedere Ruoli e ambiti integrati. Per informazioni su come assegnare il ruolo integrato a un amministratore, vedere Amministrazione e monitoraggio delegati.

Per un livello più granulare di controllo dell'accesso alla pagina **Filters** relativa a sessioni e macchine, creare un ruolo personalizzato e selezionare una delle seguenti opzioni per l'oggetto Director: **View Filters page - Machines only** (Pagina Visualizza filtri - Solo macchine), **View Filters page - Sessions only**(Pagina Visualizza filtri - Solo sessioni). Per informazioni sulla creazione di un ruolo personalizzato, vedere Creare e gestire ruoli.

**Supporto di un nuovo tipo di macchina**. In questa versione è stato aggiunto il supporto delle serie NV v4 e DA v4 di macchine AMD, durante la configurazione di dischi Premium per un catalogo macchine. Per ulteriori informazioni, vedere Creare gruppi di consegna.

## agosto 2020

### Funzionalità nuove e migliorate

**Accesso limitato all'SDK Remote PowerShell durante un'interruzione**. In precedenza, non era possibile utilizzare i comandi di PowerShell durante un'interruzione. Ora, Local Host Cache consente l'accesso limitato all'SDK PowerShell remoto durante un'interruzione. Vedere Cosa non è disponibile durante un'interruzione.

**Supporto di due nuove edizioni del servizio Citrix Virtual Apps and Desktops**. Citrix Monitor ora supporta due nuove edizioni del servizio Citrix Virtual Apps and Desktops, vale a dire **il servizio Citrix Virtual Apps Advanced** e **il servizio Citrix Virtual Apps and Desktops Advanced**. Per ulteriori informazioni, vedere la Matrice di compatibilità delle funzionalità di Citrix Monitor.

**Supporto di Virtual Private Cloud (VPC) condiviso in Google Cloud Platform**. Il servizio Citrix Virtual Apps and Desktops supporta il cloud privato virtuale condiviso su Google Cloud Platform come risorsa host. È possibile utilizzare Machine Creation Services (MCS) per effettuare il provisioning delle macchine in un cloud privato virtuale condiviso (Shared VPC) e gestirle utilizzando Citrix Studio. Per informazioni su Shared VPC, vedere Cloud privato virtuale condiviso.

**Supporto della selezione delle zone per Google Cloud Platform**. Il servizio Citrix Virtual Apps and Desktops supporta la selezione delle zone su Google Cloud Platform. Questa funzione consente agli amministratori di specificare una o più zone all'interno di una regione per la creazione del catalogo.

Per le macchine virtuali di tipo single-tenant, la selezione delle zone offre agli amministratori la possibilità di posizionare nodi single-tenant nelle zone che scelgono. Per le macchine virtuali non single-tenant, la selezione delle zone offre la possibilità di posizionare le macchine virtuali in modo deterministico nelle zone che scelgono, fornendo così flessibilità nella progettazione della distribuzione. Per informazioni sulla configurazione, vedere Abilitare la selezione delle zone.

Inoltre:

- La single-tenancy fornisce l'accesso esclusivo a un nodo single-tenant, che è un server del motore di calcolo fisico dedicato all'hosting solo delle macchine virtuali del proprio progetto. Questi nodi consentono di raggruppare le macchine virtuali sullo stesso hardware o di separare le macchine virtuali da quelle di altri progetti.
- I nodi single-tenant consentono di soddisfare i requisiti hardware dedicati per gli scenari Bring Your Own License (BYOL). Consentono inoltre di rispettare il criterio di controllo degli accessi alla rete, la sicurezza e i requisiti di privacy come HIPAA.

> **Nota:**
>
> La single-tenancy è l'unico percorso per utilizzare le distribuzioni VDI di Windows 10 su Google Cloud. Anche Server VDI supporta questo metodo. Una descrizione dettagliata della single-

> tenancy è disponibile sul sito della documentazione di Google.

**Prestazioni di avvio migliorate per i dischi di sistema Azure**. Questa versione supporta prestazioni di avvio migliorate per le implementazioni di Citrix Cloud che utilizzano Azure, quando MCSIO è abilitato. Con questo supporto, è possibile mantenere il disco di sistema. Ciò offre i seguenti vantaggi:

- Le macchine virtuali e le applicazioni ora si avviano e si avviano con prestazioni simili a quelle dell'immagine golden.
- Riduzione del consumo di quote API, eliminazione e creazione del disco di sistema e ritardo di transizione dello stato causato dall'eliminazione di una macchina virtuale.

Utilizzare ad esempio la `PersistOSDisk`proprietà personalizzata di PowerShell nel comando `New -ProvScheme` per configurare questa funzionalità.

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>'
<!--NeedCopy-->
```

Per maggiori informazioni sulla configurazione, vedere Migliorare le prestazioni di avvio.

## luglio 2020

### Funzionalità nuove e migliorate

**Supporto dell'accesso granulare e basato sui ruoli alla pagina Filters**. Citrix Studio offre ora un controllo più granulare sull'accesso alla pagina **Monitor > Filters** quando si crea un ruolo personalizzato. In particolare, è possibile assegnare autorizzazioni per visualizzare qualsiasi combinazione di macchine, sessioni, connessioni e istanze di applicazioni a un ruolo personalizzato scegliendo rispettivamente **Machines**, **Sessions**, **Connections** o **Application Instances**. Di seguito sono riportate altre quattro opzioni per l'oggetto **Director** nella finestra **Create role** (Crea ruolo):

- Pagina View Filters - Solo istanze di applicazione
- Pagina View Filters - Solo connessioni
- Pagina View Filters - Solo macchine
- Pagina View Filters - Solo sessioni

Per informazioni sulla creazione di ruoli, vedere Creare e gestire ruoli.

**Supporto del ritardo di spegnimento per le macchine VDI assegnate (solo PowerShell)**. Nelle versioni precedenti, il ritardo di spegnimento si applicava solo alle macchine non assegnate. A partire da questa versione, il ritardo di spegnimento si applica sia alle macchine assegnate che a quelle non assegnate. Per ulteriori informazioni, vedere Come Autoscale gestisce l'alimentazione delle macchine.

**Supporto delle licenze client Windows.** Il servizio Citrix Virtual Apps and Desktops ora supporta l'utilizzo di licenze client Windows per il provisioning di macchine virtuali in Azure. Per eseguire VM Windows 10 in Azure, verificare che il contratto multilicenza con Microsoft sia idoneo per questo utilizzo. Per ulteriori informazioni, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

## maggio 2020

### Funzionalità nuove e migliorate

**Programmi di riavvio delle macchine.** Ora è possibile indicare se una pianificazione di riavvio riguarda le macchine in modalità di manutenzione. Questa funzionalità è disponibile solo in PowerShell. Per i dettagli, vedere Riavvii pianificati per le macchine in modalità di manutenzione.

**Disponibilità delle risorse.** È ora possibile garantire la disponibilità delle risorse durante un'interruzione senza dover pubblicare risorse in ogni zona (posizione delle risorse). Per i dettagli, vedere Disponibilità delle risorse.

## aprile 2020

### Funzionalità nuove e migliorate

**Granularità di pianificazione migliorata per i gruppi di consegna VDI (solo PowerShell).** Autoscale ora supporta la definizione delle ore di punta per i giorni inclusi in una pianificazione a un livello granulare di 30 minuti. È possibile impostare il numero minimo di macchine in esecuzione in un gruppo di consegna VDI separatamente per ogni mezz'ora del giorno. Inoltre, Autoscale ora può aumentare o diminuire il numero di macchine accese nei gruppi di consegna VDI di mezzora in mezzora anziché di ora in ora. Per ulteriori informazioni, vedere Comandi dell'SDK Broker PowerShell.

**MTU Discovery (Rilevamento MTU).** Il protocollo Citrix Enlightened Data Transport (EDT) ora dispone di funzionalità MTU Discovery. MTU Discovery consente a EDT di determinare e impostare automaticamente le dimensioni del payload per la sessione. Questa funzione consente alla sessione ICA di adattarsi alle reti con requisiti non standard di Maximum Transmission Unit (MTU) o Maximum

Segment Size (MSS). La capacità di regolazione evita la frammentazione dei pacchetti, che potrebbe comportare un peggioramento delle prestazioni o l'impossibilità di stabilire una sessione ICA. Questo aggiornamento richiede almeno l'app Citrix Workspace 1911 per Windows. Se si utilizza Citrix Gateway, la versione minima del firmware Citrix ADC richiesta è 13.0.52.24 o 12.1.56.22. Per ulteriori informazioni, vedere EDT MTU Discovery.

## marzo 2020

### Funzionalità nuove e migliorate

**Metriche del dispositivo di destinazione PVS.** Citrix Monitor ora fornisce un pannello delle metriche del dispositivo target PVS nella pagina Dettagli macchina. Utilizzare il pannello per visualizzare lo stato del Provisioning dei dispositivi di destinazione per macchine con sistema operativo a sessione singola e multisessione. In questo pannello sono disponibili diverse metriche per Rete, Avvio e Cache. Queste metriche aiutano a monitorare i dispositivi di destinazione PVS e a risolverne i problemi per assicurarsi che siano attivi e funzionanti. Per maggiori informazioni, vedere Metriche del dispositivo di destinazione PVS.

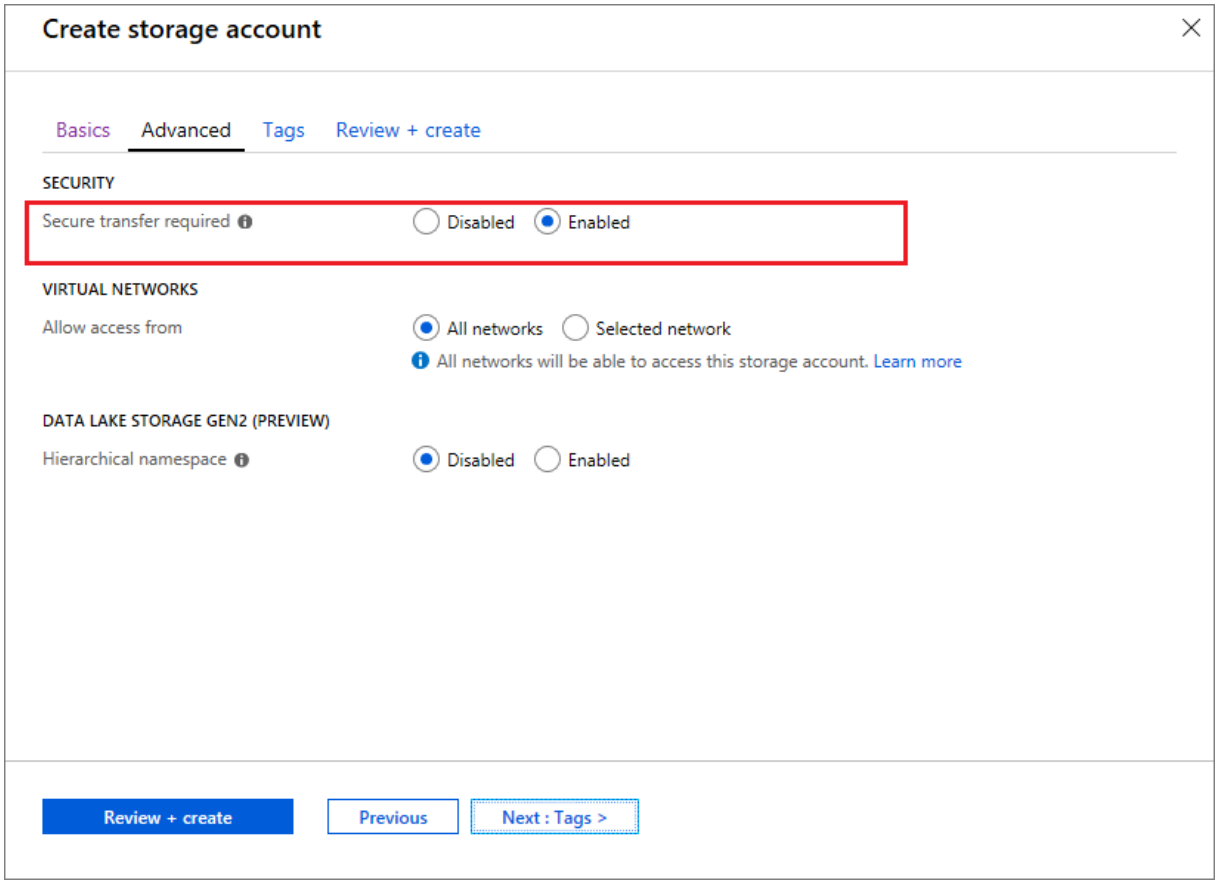
**Acquisizione delle proprietà delle istanze AWS.** MCS ora legge le proprietà dall'istanza da cui è stata presa l'AMI e applica il ruolo di IAM e i tag della macchina alle macchine di cui è stato eseguito il provisioning per un determinato catalogo. Quando si utilizza questa funzione facoltativa, il processo di creazione del catalogo trova l'istanza dell'origine AMI selezionata che legge un insieme limitato di proprietà. Queste proprietà vengono quindi archiviate in un modello di avvio AWS, utilizzato per il provisioning di macchine per quel catalogo. Qualsiasi macchina nel catalogo eredita le proprietà dell'istanza acquisita. Per ulteriori informazioni, vedere Acquisizione delle proprietà delle istanze AWS.

**Etichettatura delle risorse operative AWS.** Questa release introduce un'opzione per applicare tag alle risorse create dai componenti Citrix durante il provisioning. Ogni tag rappresenta un'etichetta composta da una chiave definita dal cliente e da un valore opzionale che migliorano la capacità di gestire, cercare e filtrare le risorse. Per ulteriori informazioni, vedere Etichettatura delle risorse operative di AWS.

**Trasferimento sicuro nell'archiviazione di Azure.** Machine Creation Services (MCS) offre un miglioramento per gli account di archiviazione creati dai cataloghi con provisioning MCS negli ambienti di Azure Resource Manager. Questo miglioramento consente automaticamente il trasferimento sicuro della proprietà richiesta. Questa opzione migliora la sicurezza dell'account di archiviazione consentendo solo le richieste inviate all'account da connessioni sicure. Per ulteriori informazioni, vedere Richiedere il trasferimento sicuro per garantire connessioni sicure nel sito Microsoft.

Abilitare la proprietà **Secure transfer required** (Trasferimento sicuro obbligatorio) quando si crea un account di archiviazione in Azure:




**Supporto dei dischi gestiti SSD di Azure.** Machine Creation Services (MCS) supporta i dischi gestiti SSD standard per le macchine virtuali di Azure. Questo tipo di disco offre prestazioni costanti e offre una maggiore disponibilità rispetto ai dischi HDD. Per ulteriori informazioni, vedere Dischi SSD standard per carichi di lavoro di macchine virtuali di Azure.

Utilizzare la proprietà personalizzata di PowerShell `StorageAccountType` nel comando `New-ProvScheme` o nel comando `Set-ProvScheme` per configurare questa funzionalità:

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property xsi:type=`"StringProperty`" Value=`"Windows_Server`" />
<!--NeedCopy-->
```

> **Nota:**
>
> Questa funzionalità è disponibile solo quando si utilizzano dischi gestiti, ovvero la proprietà personalizzata `UseManagedDisks` è impostata su **true**. Per quanto riguarda i dischi non gestiti, sono supportati solo HDD standard e SSD Premium.

## gennaio 2020

### Funzionalità nuove e migliorate

**Barra della lingua in Citrix Studio.** A partire da questa versione, Citrix Studio fornisce una barra della lingua per facilitare la corretta mappatura della tastiera.

- Se la lingua di Citrix Cloud o la lingua di visualizzazione del browser è impostata su **English** o **Japanese**, la barra della lingua non viene visualizzata.
- Se la lingua di Citrix Cloud o la lingua di visualizzazione del browser è impostata su **German**, **Spanish**o **French**, la barra della lingua viene visualizzata dopo l'accesso a Citrix Studio. Ci sono due opzioni di lingua nell'elenco della barra delle lingue. Selezionare un'opzione che corrisponda alla lingua in cima all'elenco del proprio browser.

  > **Suggerimento:**
  >
  > ```
  > - Settings that you configure for the language bar might not take effect. In this case, log out and log back on.
  > - You might fail to input certain symbols and localized characters by using the language bar. To resolve the issue, you need to configure the language of Citrix Cloud, the display language of your browser, and the local keyboard layout. For more information, see Knowledge Center article [CTX310743](https://support.citrix.com/article/CTX310743).
  > ```

**Timer di ritardo massimo del programma di riavvio (solo PowerShell).** Se un riavvio pianificato dei computer in un gruppo di consegna non inizia a causa di un'interruzione del database del sito, è possibile specificare il tempo di attesa oltre l'ora di inizio pianificata. Se la connessione al database viene ripristinata durante tale intervallo, i riavvii iniziano. Se la connessione non viene ripristinata durante tale intervallo, i riavvii non iniziano. Per i dettagli, vedere Riavvii pianificati ritardati a causa di un'interruzione del database.

**Bilanciamento del carico verticale (solo PowerShell).** In precedenza, per tutti gli avvii RDS il servizio utilizzava il bilanciamento del carico orizzontale, che assegnava il carico in entrata alla macchina RDS meno caricata. Questa rimane l'impostazione predefinita. Ora è possibile utilizzare PowerShell per abilitare il bilanciamento del carico verticale come impostazione a livello di sito.

Quando il bilanciamento del carico verticale è abilitato, il broker assegna il carico in entrata alla macchina più caricata che non ha raggiunto una filigrana elevata. Questo processo satura le macchine esistenti prima di passare a nuove macchine. Man mano che gli utenti si disconnettono e liberano le macchine esistenti, a tali macchine viene assegnato un nuovo carico.

Per impostazione predefinita, il bilanciamento del carico orizzontale è abilitato. Per visualizzare, abilitare o disabilitare il bilanciamento del carico verticale, i cmdlet `Get-BrokerSite` e `Set-`

`BrokerSite` ora supportano l'impostazione `UseVerticalScalingForRdsLaunches`. Per maggiori informazioni, vedere Caricare macchine gestite nei gruppi di consegna.

## dicembre 2019

### Funzionalità nuove e migliorate

**Servizio per i Citrix Service Provider (CSP).** I CSP possono ora integrare i clienti tenant al servizio Virtual Apps and Desktops, configurare l'accesso dell'amministratore del cliente al servizio e fornire spazi di lavoro condivisi o dedicati agli utenti dei clienti che utilizzano domini federati. Per ulteriori informazioni, vedere Servizio Citrix Virtual Apps and Desktops per i fornitori di servizi Citrix.

**Supporto dell'individuazione del motivo per cui una macchina è in modalità di manutenzione (solo PowerShell).** Utilizzando PowerShell, è ora possibile determinare il motivo per cui una macchina è in modalità di manutenzione. A tale scopo, utilizzare il parametro `-MaintenanceModeReason`. Questa funzione è utile per gli amministratori quando devono risolvere i problemi delle macchine in modalità di manutenzione. Per i dettagli, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/.

**Autoscale.** Autoscale ora offre la possibilità di creare macchine ed eliminarle dinamicamente. È possibile utilizzare questa funzionalità mediante uno script PowerShell. Lo script consente di aumentare o diminuire dinamicamente il numero di macchine incluse nel gruppo di consegna in base alle condizioni di carico correnti. Per ulteriori informazioni, vedere Provisioning dinamico delle macchine con Autoscale.

## novembre 2019

### Funzionalità nuove e migliorate

**GroomStartHour.** Monitor ora supporta **GroomStartHour**, una nuova configurazione che aiuta gli amministratori a determinare l'ora del giorno in cui deve iniziare la pulizia. Per ulteriori informazioni, vedere la documentazione di Citrix Virtual Apps and Desktops SDK .

**Impaginazione OData.** Monitor ora supporta l'**impaginazione OData**. Tutti gli endpoint OData v4 restituiscono un massimo di 100 record per pagina con un collegamento ai 100 record successivi nella risposta. Per ulteriori informazioni, vedere Accesso ai dati del servizio di monitoraggio mediante l'endpoint OData v4 in Citrix Cloud.

## ottobre 2019

### Funzionalità nuove e migliorate

**App-V.** La funzionalità App-V è ora disponibile in Citrix Cloud. È possibile aggiungere pacchetti App-V al Delivery Controller nella configurazione Citrix Cloud, in modalità amministratore singolo o doppio. Il *modulo di rilevamento dei pacchetti App-V del servizio Virtual Apps and Desktops*, disponibile in Citrix Downloads, consente di importare pacchetti App-V e registrare server Microsoft App-V. Le app che contengono sono quindi disponibili per i propri utenti. Questo modulo PowerShell consente di registrare i server di gestione e pubblicazione di Microsoft App-V utilizzando URL DNS, evitando la necessità che i server soggetti a meccanismi di bilanciamento del carico vengano registrati utilizzando il loro URL macchina effettivo. Per ulteriori informazioni, vedere Modulo di rilevamento dei servizi Citrix Virtual Apps and Desktops per pacchetti e server App-V.

**Google Cloud Platform.** Il servizio Citrix Virtual Apps and Desktops ora aggiunge il supporto dell'utilizzo di Machine Creation Services (MCS) per il provisioning di macchine su Google Cloud Platform (GCP). Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Google Cloud Platform.

## settembre 2019

### Funzionalità nuove e migliorate

**Supporto VDA per Azure Virtual Desktop.** Per i sistemi operativi e le versioni VDA supportati, vedere VDA in un ambiente desktop virtuale Azure.

**Criteri di alimentazione migliorati**. Nelle versioni precedenti, una macchina VDI che passava a un periodo di tempo in cui era necessaria un'azione (azione di disconnessione= "**Suspend**"o "**Shutdown**" ) rimaneva alimentata. Questo scenario si verificava se la macchina si disconnetteva durante un periodo di tempo (di punta o non di punta) in cui non era richiesta alcuna azione (azione di disconnessione = "**Nothing**").

A partire da questa versione, Autoscale mette in sospensione o arresta la macchina al termine del tempo di disconnessione specificato, a seconda dell'azione di disconnessione configurata per il periodo di tempo di destinazione. Per i ulteriori informazioni, vedere Gestire l'alimentazione di macchine VDI che passano a un periodo di tempo diverso con sessioni disconnesse.

**Cataloghi di macchine: Tag.** Ora è possibile utilizzare PowerShell per applicare tag ai cataloghi di macchine. Per ulteriori informazioni, vedere Applicare i tag ai cataloghi di macchine.

**Durata dell'avvio della sessione.** Monitor ora visualizza la durata di avvio della sessione suddivisa in periodi di avvio sessione app Workspace e Avvio sessione VDA. Questi dati aiutano a comprendere e risolvere i problemi di durata elevata dell'avvio delle sessioni. Inoltre, la durata di ogni fase coinvolta nell'avvio della sessione aiuta a risolvere i problemi associati alle singole fasi. Ad esempio, se il

tempo di mappatura dell'unità è elevato, è possibile verificare se tutte le unità valide sono mappate adeguatamente nell'oggetto Criteri di gruppo o nello script. Questa funzione è disponibile sui VDA 1903 o versioni successive. Per ulteriori informazioni, vedere Diagnosticare i problemi di avvio della sessione.

## agosto 2019

### Funzionalità nuove e migliorate

**Riconnessione automatica della sessione.** La pagina Sessions nella scheda Trends ora include informazioni sul numero di riconnessioni automatiche. Viene tentata la riconnessione automatica quando sono in vigore i criteri Session Reliability (Affidabilità della sessione) o Auto Client Reconnect (Riconnessione automatica client). Le informazioni di riconnessione automatica consentono di visualizzare le connessioni di rete che presentano interruzioni e risolverne i problemi, nonché di analizzare le reti che presentano un'esperienza senza problemi.

Il drill down fornisce informazioni aggiuntive come l'affidabilità della sessione o la riconnessione automatica del client, i timestamp, l'IP dell'endpoint e il nome dell'endpoint della macchina su cui è installata l'app Workspace. Questa funzionalità è disponibile per l'app Citrix Workspace per Windows, l'app Citrix Workspace per Mac, Citrix Receiver per Windows e Citrix Receiver per Mac. Questa funzionalità richiede VDA 1906 o versioni successive. Per ulteriori informazioni, vedere:

- Sessioni
- Impostazioni dei criteri di riconnessione automatica client
- Impostazioni dei criteri di affidabilità della sessione
- Riconnessione automatica della sessione

## luglio 2019

### Funzionalità nuove e migliorate

**Registrazione della configurazione.** È ora possibile utilizzare l'SDK Remote PowerShell per eliminare periodicamente il contenuto del database di registrazione della configurazione. Per i dettagli, vedere Pianificare l'eliminazione dati periodica

**Autoscale.** Autoscale ora offre la flessibilità necessaria per gestire solo un sottoinsieme di macchine di un gruppo di consegna. Questa funzione può essere utile nei casi d'uso del cloud bursting, in cui si desidera utilizzare risorse locali per gestire i carichi di lavoro prima che le risorse basate sul cloud soddisfino altre esigenze (ovvero carichi di lavoro burst). Per maggiori informazioni, vedere Limitare Autoscale a determinate macchine di un gruppo di consegna.

**Accesso alle app locali e reindirizzamento URL.** Citrix Studio ora consente di aggiungere l'opzione Add Local App Access Application (Aggiungi applicazione di accesso alle app locali) all'interfaccia utente di Studio per il sito utilizzando PowerShell SDK. Per ulteriori informazioni, vedere Fornire l'accesso solo alle applicazioni pubblicate.

**Modifica del nome del sistema operativo**. I nomi dei sistemi operativi nelle pagine **Create Machine Catalog > Machine Catalog Setup > Operating System** (Creare cataloghi delle macchine > Configurazione del catalogo delle macchine > Sistema operativo) e **Monitor** sono cambiati:

- Sistema operativo multisessione (in precedenza sistema operativo server): il catalogo delle macchine con sistema operativo multisessione fornisce desktop condivisi ospitati per una distribuzione su larga scala di macchine con sistema operativo Windows multisessione o Linux standardizzate.
- Sistema operativo a sessione singola (in precedenza sistema operativo desktop): il catalogo delle macchine con sistema operativo a sessione singola fornisce desktop VDI ideali per vari utenti.

**Durata di Profile Management Citrix nel caricamento del profilo**. Monitor ora include la durata dell'elaborazione del profilo nella barra di caricamento del profilo del grafico della durata dell'accesso. Si tratta del tempo impiegato da Citrix Profile Management per elaborare i profili utente. Queste informazioni aiutano gli amministratori a risolvere i problemi relativi alle durate di carico elevato del profilo con maggiore precisione. Questo miglioramento è disponibile sui VDA 1903 e versioni successive. Per ulteriori informazioni, vedere Profile load (Caricamento del profilo).

**Probe dei desktop**. Il probe dei desktop è una funzionalità del servizio Citrix Virtual Apps and Desktops. Automatizza i controlli di integrità dei desktop virtuali pubblicati su un sito, migliorando l'esperienza dell'utente. Per avviare il probe dei desktop, installare e configurare Citrix Probe Agent su uno o più endpoint. Il probe dei desktop è disponibile per i siti con licenza Premium. Questa funzionalità richiede Citrix Probe Agent 1903 o versione successiva. Per ulteriori informazioni, vedere Probe delle applicazioni e dei desktop.

> **Nota:**
>
> Citrix Probe Agent ora supporta TLS 1.2.

## giugno 2019

### Funzionalità nuove e migliorate

**Limitare mediante tag.** I tag sono stringhe che identificano elementi come macchine, applicazioni, desktop, gruppi di applicazioni e criteri. Dopo aver creato un tag e averlo aggiunto a un elemento, è possibile personalizzare determinate operazioni per applicarle solo agli elementi che hanno un tag specificato. Per ulteriori informazioni, vedere Gruppi di applicazioni e Tag.

**Notifiche tramite e-mail.** Il servizio Citrix Virtual Apps and Desktops invia direttamente le notifiche e-mail relative agli avvisi e al probe. Ciò elimina la necessità di configurare il server di posta elettronica SMTP. La casella **Notification Preferences** (Preferenze di notifica) è abilitata per impostazione predefinita e Citrix Cloud invia notifiche di avviso agli indirizzi e-mail forniti nella sezione **Notification Preferences** . Assicurarsi che l'indirizzo e-mail `donotreplynotifications@citrix.com` sia inserito nella whitelist nella propria configurazione e-mail.

## maggio 2019

### Funzionalità nuove e migliorate

**Autoscale.** Autoscale è una funzionalità esclusiva del servizio Citrix Virtual Apps and Desktops che offre una soluzione coerente e ad alte prestazioni per gestire l'alimentazione delle macchine in modo proattivo. Punta a raggiungere un equilibrio fra i costi e l'esperienza dell'utente. Autoscale incorpora la tecnologia Smart Scale deprecata nella soluzione di gestione dell'alimentazione di Studio. Per ulteriori informazioni, vedere Scalabilità automatica. È possibile monitorare le metriche delle macchine gestite da Autoscale dalle pagine Trends nella scheda **Monitor**. Per ulteriori informazioni, vedere Monitorare macchine gestite dalla scalabilità automatica.

## febbraio 2019

### Funzionalità nuove e migliorate

**Monitoraggio degli avvisi di Hypervisor.** Gli avvisi provenienti da Citrix Hypervisor e VMware vSphere sono ora visualizzati nella scheda **Monitor** > **Alerts** (Avvisi) per aiutare a monitorare i seguenti stati/parametri di integrità dell'hypervisor:

- CPU usage (Utilizzo della CPU)
- Memory usage (Utilizzo della memoria)
- Network usage (Utilizzo della rete)
- Hypervisor connection unavailable (Connessione all'Hypervisor non disponibile)
- Utilizzo del disco (solo vSphere)
- Connessione host o stato di alimentazione (solo vSphere)

Per ulteriori informazioni, vedere la sezione sul monitoraggio degli avvisi di Hypervisor in Avvisi e notifiche.

**Comunicazioni su versioni TLS precedenti.** Per migliorare la sicurezza del servizio, Citrix bloccherà qualsiasi comunicazione su Transport Layer Security (TLS) 1.0 e 1.1 a partire dal 15 marzo 2019, consentendo solo le comunicazioni TLS 1.2. Per ulteriori informazioni, vedere Versioni TLS. Per indicazioni esaustive, vedere CTX247067.

**Gruppi di applicazioni.** I gruppi di applicazioni consentono di gestire raccolte di applicazioni. È possibile creare gruppi di applicazioni per applicazioni condivise tra gruppi di consegna diversi o utilizzate da un sottoinsieme di utenti all'interno di gruppi di consegna. Per ulteriori informazioni, vedere Creare gruppi di applicazioni.

**Prestazioni di accesso: drilldown del profilo.** Il pannello **Logon Duration** (Durata accesso) nella pagina **User Details** (Dettagli utente) all'interno di **Monitor** ora include informazioni sul drilldown di **Profile load phase** (Fase di caricamento del profilo) del processo di accesso. Il drilldown dei profili fornisce informazioni utili sui profili utente per la sessione corrente che possono aiutare gli amministratori a risolvere i problemi di carico elevato del profilo. Viene visualizzata una descrizione comando con le seguenti informazioni sui profili utente:

- Numero di file
- Dimensione del profilo
- Numero di file di grandi dimensioni

Un drilldown dettagliato fornisce informazioni sulle singole cartelle, le loro dimensioni e il numero di file. Questa funzionalità è disponibile sui VDA 1811 e versioni successive. Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti.

**Stato della licenza Servizi Desktop remoto Microsoft.** Monitorare lo stato della licenza di Microsoft RDS (Remote Desktop Services) nel pannello **Machine Details** (Dettagli macchina) delle pagine Machine Details e User Details (Dettagli utente) per i computer con sistema operativo server. Viene visualizzato un messaggio appropriato per lo stato della licenza. È possibile passare il mouse sull'icona delle informazioni per visualizzare ulteriori dettagli. Per ulteriori informazioni, vedere la sezione relativa allo stato della licenza Microsoft RDS in Troubleshooting Machines(Risoluzione dei problemi delle macchine).

**Probe delle applicazioni.** Questa funzione automatizza la valutazione dell'integrità delle app virtuali pubblicate in un sito.

Per avviare il probe dell'applicazione:

- Su una o più macchine endpoint, installare Citrix Application Probe Agent
- Configurare Citrix Application Probe Agent con le credenziali di Citrix Workspace e del servizio Citrix Virtual Apps and Desktops.
- Configurare i desktop da sottoporre a probe, le macchine endpoint su cui eseguire il probe e l'ora del probe in **Monitor** > **Configuration** del servizio Citrix Virtual Apps and Desktops.

L'agente verifica l'avvio di applicazioni selezionate tramite Citrix Workspace e riporta i risultati del probe nella scheda **Monitor** del servizio Citrix Virtual Apps and Desktops in:

- la pagina Applications: i dati delle ultime 24 ore e la pagina **Trends** > **Application Probe Results**

- i dati storici di probe insieme alla fase in cui si è verificato l'errore di probe: Workspace Reachability, WorkspaceAuthentication, WorkspaceEnumeration, download ICA o avvio dell'applicazione

Il report degli errori viene inviato per e-mail agli indirizzi configurati. È possibile pianificare l'esecuzione dei probe delle applicazioni durante le ore di minor utilizzo in più posizioni geografiche. In questo modo, è possibile utilizzare i risultati per risolvere in modo proattivo i problemi delle applicazioni sottoposte a provisioning, alle macchine di hosting o alle connessioni prima che gli utenti li sperimentino. Per ulteriori informazioni, vedere Probe delle applicazioni e dei desktop.

## gennaio 2019

### Funzionalità nuove e migliorate

**Amministrazione delegata con ambito personalizzato.** Il monitoraggio ora supporta l'ambito personalizzato per i ruoli di amministratore delegato incorporati. Per ulteriori informazioni sui ruoli predefiniti disponibili per il monitoraggio e su come assegnarli, vedere Delegated administrator roles.

## dicembre 2018

### Funzionalità nuove e migliorate

La data dopo la quale Citrix bloccherà la comunicazione su Transport Layer Security (TLS) 1.0 e 1.1 è stata spostata dal 31 dicembre 2018 al 31 gennaio 2019. Per i dettagli, vedere Deprecazione delle versioni TLS.

## novembre 2018

### Funzionalità nuove e migliorate

**Dati cronologici delle macchine disponibili tramite l'API OData:** i dati cronologici contenenti l'analisi delle macchine sono ora disponibili tramite l'API OData. Questi dati vengono raccolti su base oraria e aggregati per la giornata.

- Numero di macchine accese (per le macchine con gestione dell'alimentazione)
- Numero di macchine registrate
- Numero di macchine in modalità di manutenzione
- Numero totale di macchine

I dati vengono aggregati per il periodo di tempo durante il quale il servizio di monitoraggio è in esecuzione. Per ulteriori informazioni sull'utilizzo dell'API OData ed esempi, vedere Citrix Monitor Service 7 1808. Lo schema del database è disponibile in Monitor Service Schema.

**Prestazioni di accesso - Drilldown interattivo della sessione:** il pannello **Logon Duration** (Durata accesso) nella vista **User and Session Details** (Dettagli utente e sessione) include informazioni sulla fase **Interactive Session** (Sessione interattiva) del processo di accesso. Il tempo impiegato per ciascuna delle tre sottofasi (**Pre-userinit**, **Userinit**e **Shell**) viene visualizzato nella barra **Interactive Session** come descrizione comando. Ciò fornisce una risoluzione dei problemi e una correzione più granulari per questa fase dell'accesso. Viene inoltre fornito il tempo di ritardo cumulativo tra le sottofasi e un collegamento alla documentazione. Questa funzionalità è disponibile in Delivery Controller versione 7 1808 e successive. La barra di drilldown **Interactive Session** mostra la durata solo per la sessione corrente. Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti.

**Prestazioni di accesso - Drilldown oggetto Criteri di gruppo:** il pannello **Logon Duration** (Durata accesso) nella vista **User and Session** (Dettagli utente e sessione) contiene la durata del GPO (Oggetti Criteri di gruppo). Si tratta del tempo totale impiegato per applicare gli oggetti Criteri di gruppo sulla macchina virtuale durante il processo di accesso. Ora è possibile visualizzare il drilldown di ogni criterio applicato secondo la CSE (Clients-Side Extension) come descrizione comando sulla barra degli oggetti Criteri di gruppo. Per ogni applicazione dei criteri, il drilldown visualizza lo stato e il tempo impiegato. Queste informazioni aggiuntive facilitano la risoluzione e la correzione dei problemi che comportano una durata elevata degli oggetti Criteri di gruppo. Le durate temporali nel drill-down rappresentano solo il tempo di elaborazione delle CSE e non si sommano al tempo totale dell'oggetto Criteri di gruppo. Questa funzionalità è disponibile in Delivery Controller versione 7 1808 e successive. Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti.

#### Correzioni

Le query di report personalizzate salvate durante il monitoraggio non sono disponibili dopo un aggiornamento del cloud. [DNA-23420]

### ottobre 2018

#### Funzionalità nuove e migliorate

**Applicazioni: limite per macchina.** È ora possibile limitare il numero di istanze dell'applicazione per computer. Questo limite si applica a tutte le macchine presenti nel Sito. Questo limite è un'aggiunta al limite di applicazioni esistente per tutti gli utenti del gruppo di consegna e al limite per utente. Questa funzionalità è disponibile solo tramite PowerShell, non in Studio. Per i dettagli, vedere Configurare i limiti delle applicazioni.

**Windows Server 2019.** È ora possibile installare VDA per sistemi operativi multisessione (in precedenza VDA per il sistema operativo server) su macchine Windows Server 2019, come indicato in Requisiti di sistema.

### settembre 2018

#### Funzionalità nuove e migliorate

**Amministrazione delegata.** Con l'amministrazione delegata in Citrix Cloud, è possibile configurare le autorizzazioni di accesso di cui tutti gli amministratori hanno bisogno, in base al loro ruolo nell'organizzazione. Per i dettagli, vedere Amministrazione delegata. Il monitoraggio supporta l'assegnazione di ruoli predefiniti. I ruoli incorporati sono disponibili con un ambito completo. Per ulteriori informazioni sui ruoli predefiniti per il monitoraggio e su come assegnarli, vedere Ruoli di amministratore delegato.

**Registrazione della configurazione.** La registrazione della configurazione consente agli amministratori di tenere traccia delle modifiche apportate alla configurazione e delle attività amministrative. Per i dettagli, vedere Registrazione della configurazione.

Diversi cmdlet PowerShell dell'SDK Remote PowerShell che erano in precedenza disabilitati sono ora abilitati, per l'utilizzo con la registrazione di configurazione:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

**Cache host locale.** La cache host locale è ora completamente disponibile. La cache host locale consente di continuare le operazioni di intermediazione delle connessioni quando un Cloud Connector che si trova nella posizione di una risorsa non può comunicare con Citrix Cloud. Per i dettagli, vedere Cache host locale.

**Citrix Provisioning.** Per effettuare il provisioning dei VDA, è ora possibile utilizzare Citrix Provisioning o i Machine Creation Services esistenti. Per informazioni su Citrix Provisioning specifiche per l'ambiente cloud, vedere Citrix Provisioning gestito da Citrix Cloud.

#### Correzioni

Nelle versioni precedenti, quando si utilizzava il provisioning su richiesta di Azure, tutte le macchine virtuali venivano eliminate allo spegnimento. Ora, solo le macchine virtuali in pool vengono eliminate. Le macchine virtuali persistenti (dedicate) non vengono eliminate allo spegnimento.

### agosto 2018

- **Nuovi nomi di prodotti**

  Se l'utente è un cliente o un partner di Citrix da un certo periodo di tempo, noterà nuovi nomi nei nostri prodotti e in questa documentazione del prodotto. Se per l'utente questo prodotto Citrix è nuovo, potrebbe notare nomi diversi per un prodotto o un componente.

  I nuovi nomi di prodotti e componenti derivano dal portafoglio e dalla strategia cloud Citrix in espansione. Gli articoli di questa documentazione del prodotto utilizzano i seguenti nomi.

  - **Citrix Virtual Apps and Desktops**: Citrix Virtual Apps and Desktops offre una soluzione per app e desktop virtuali, fornita come servizio cloud e come prodotto locale, che offre ai dipendenti la libertà di lavorare ovunque su qualsiasi dispositivo, riducendo i costi IT. Consente di fornire applicazioni Windows, Linux, Web e SaaS o desktop virtuali completi da qualsiasi cloud: pubblico, locale o ibrido. Virtual Apps and Desktops era in precedenza chiamato XenApp e XenDesktop.
  - **App Citrix Workspace**: l'app Citrix Workspace incorpora la tecnologia Citrix Receiver esistente e le altre tecnologie client Citrix Workspace. È stata migliorata per offrire più funzionalità che forniscono agli utenti finali un'esperienza contestuale unificata in cui possono interagire con tutte le app, i file e i dispositivi di lavoro di cui hanno bisogno per svolgere al meglio le loro mansioni. Per ulteriori informazioni, vedere questo post del blog.
  - **Citrix SD-WAN**: NetScaler SD-WAN, una tecnologia cruciale per i nostri clienti e partner che trasforma le reti delle filiali e le WAN con la tecnologia cloud, è ora chiamato Citrix SD-WAN.
  - **Citrix Secure Web Gateway**: con l'espansione del portafoglio Citrix Networking, siamo orgogliosi di offrire il nostro solido servizio Citrix Secure Web Gateway, in precedenza noto come NetScaler Secure Web Gateway.
  - **Citrix Gateway**: il nostro solido NetScaler Unified Gateway, che consente un accesso sicuro e contestuale alle app e ai dati necessari per lavorare al meglio, ora si chiama Citrix Gateway.
  - **Citrix Content Collaboration e Citrix Files for Windows**: le funzionalità avanzate di accesso, collaborazione, flussi di lavoro, gestione dei diritti e integrazione di ShareFile sono ora disponibili nel set di componenti Citrix Content Collaboration nel nostro Citrix Workspace protetto, contestuale e integrato. Citrix Files for Windows consente di accedere ai file di Content Collaboration direttamente tramite un'unità mappata, fornendo un'esperienza nativa di Windows Explorer.
  - **Citrix Hypervisor**: la tecnologia di XenServer per l'infrastruttura di virtualizzazione, basata sull'hypervisor XenProject, ora si chiama Citrix Hypervisor.

  Ecco un riepilogo rapido:

| È | Era |
| --- | --- |
| Citrix Virtual Apps and Desktops | XenApp e XenDesktop |
| App Citrix Workspace | Incorpora Citrix Receiver e miglioramenti estesi |
| Citrix SD-WAN | NetScaler SD-WAN |
| Citrix Secure Web Gateway | NetScaler Secure Web Gateway |
| Citrix Gateway | Unified Gateway NetScaler |
| Citrix Content Collaboration | ShareFile |
| Citrix Files per Windows | ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper |
| Citrix Hypervisor | XenServer |
| Citrix Provisioning | Citrix Provisioning Services |

L'implementazione di questa transizione nei nostri prodotti e nella relativa documentazione è un processo continuo.

- I contenuti all'interno del prodotto potrebbero ancora riportare i nomi precedenti. Ad esempio, è possibile che vengano visualizzate istanze di nomi precedenti nel testo della console, nei messaggi e nei nomi di directory e file.
- È possibile che alcuni elementi (come comandi e MSI) continuino a mantenere i nomi precedenti per evitare che gli script esistenti dei clienti smettano di funzionare.
- La documentazione relativa al prodotto e altre risorse (come video e post dei blog) collegate dalla documentazione di questo prodotto potrebbero ancora contenere nomi precedenti.
- Per Citrix Hypervisor: il nuovo nome viene utilizzato sul sito Web Citrix e nei materiali informativi dei prodotti a partire da settembre 2018. Il nuovo nome verrà inoltre visualizzato nelle console degli amministratori di alcuni prodotti Citrix, come Citrix Virtual Apps and Desktops. Il rilascio del prodotto XenServer e i materiali di documentazione tecnica continuano a utilizzare XenServer 7.x fino all'inizio del 2019.

La pazienza dimostrata durante questa transizione è apprezzata.

Per maggiori dettagli sui nostri nuovi nomi, vedere https://www.citrix.com/about/citrix-product-guide/.

- **Modifiche dei numeri di versione dei prodotti e dei componenti**

  Citrix installa e gestisce la maggior parte dei componenti di Citrix Virtual Apps and Desktops, quindi non sarà necessario preoccuparsi dei numeri di versione di questi. Tuttavia, potrebbero

comparire i numeri di versione durante l'installazione dei Cloud Connector e durante l'installazione o l'aggiornamento dei VDA nelle posizioni delle risorse.

I numeri di versione dei prodotti e dei componenti di Citrix Virtual Apps and Desktops sono visualizzati nel formato: **AAMM.*c.m. b***

- AAMM = anno e mese in cui il prodotto o il componente è stato rilasciato. Ad esempio, una versione di settembre 2018 appare come 1809.
- c = numero di release di Citrix Cloud per il mese.
- m = versione di manutenzione (se applicabile).
- b = numero di build. Questo campo viene visualizzato solo nella pagina About (Informazioni su) del componente e nella funzionalità del sistema operativo per la rimozione o la modifica dei programmi.

Ad esempio, **Citrix Virtual Apps and Desktops 1809.1.0** indica che il componente è stato rilasciato nel settembre 2018. È associato a Citrix Cloud release 1 di quel mese e non è una versione di manutenzione. In alcuni casi vengono visualizzati solo l'anno e il mese della versione, ad esempio **Citrix Virtual Apps and Desktops 1809**.

Nelle versioni precedenti (7.18 e versioni precedenti), i numeri di versione erano visualizzati nel formato: 7.*versione*, dove il valore della versione veniva incrementato di uno per ogni versione. Ad esempio, la versione di VDA successiva a XenApp e XenDesktop 7.17 era la 7.18. Le versioni precedenti (7.18 e precedenti) non verranno aggiornate al nuovo formato di numerazione.

- **Deprecazione delle versioni TLS.** Per migliorare la sicurezza del servizio Citrix Virtual Apps and Desktops, Citrix bloccherà qualsiasi comunicazione su Transport Layer Security (TLS) 1.0 e 1.1, a partire dal 31 dicembre 2018. Per i dettagli, vedere Deprecazione delle versioni TLS.
- **Ambienti di virtualizzazione Google Cloud Platform.** Il servizio Citrix Virtual Apps and Desktops supporta la possibilità di spegnere e riaccendere manualmente le macchine virtuali Virtual Apps and Desktops su Google Cloud Platform (GCP). Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Google Cloud Platform.

### luglio 2018

- **Esportazione dei dati dei filtri.** Ora è possibile esportare i dati di monitoraggio in tempo reale contenuti nella scheda **Monitor** > **Filters** in file formato CSV. La funzione di esportazione è disponibile nelle pagine Machines, Sessions, Connections e Application Instances Filters. È possibile selezionare un filtro personalizzato predefinito o criteri di filtro adatti, scegliere le colonne richieste nella tabella ed esportare i dati. È possibile esportare fino a 100.000 record di dati. I file CSV esportati offrono una visione completa dei dati in tempo reale e aiutano a facilitare l'analisi di set di dati di grandi dimensioni.

### giugno 2018

- **Connessioni ad Azure Resource Manager.** Nella procedura guidata per la creazione della connessione a Studio, la selezione dell'ambiente Azure nella pagina **Connection** include tutti i Cloud di Azure validi per la sottoscrizione di Azure. La disponibilità generale per Azure US Government Cloud e Azure Germany Cloud sostituisce le versioni di anteprima di questi due ambienti nelle versioni precedenti.

### maggio 2018

- **Azure Quick Deploy.** Quando la posizione delle risorse utilizza macchine di Azure Resource Manager per distribuire applicazioni e desktop, è ora possibile scegliere un metodo di distribuzione:
  - Full Configuration: questo metodo esistente utilizza la console di gestione di Studio, che guida l'utente nella creazione di un catalogo di macchine e nella successiva creazione di un gruppo di consegna.
  - Distribuzione rapida di Azure: questa nuova opzione offre un'interfaccia più semplice che consente una distribuzione più rapida di app e desktop.
- **Collegamento a Citrix Health Assistant.** La pagina Machine Details di una macchina non registrata nella console di monitoraggio ora contiene un pulsante **Health Assistant**. Attualmente, il pulsante si collega all'articolo Risolvere i problemi relativi alle macchine e all'articolo del Knowledge Center Citrix Health Assistant - Risoluzione dei problemi relativi alla registrazione VDA e all'avvio della sessione in cui è possibile scaricare lo strumento. Citrix Health Assistant è uno strumento per risolvere i problemi di configurazione nei VDA non registrati. Lo strumento automatizza diversi controlli di integrità per identificare le possibili cause principali dei comuni per i problemi comuni di registrazione dei VDA e relativi all'avvio della sessione e alla configurazione del reindirizzamento del fuso orario.
- **Drill-down interattivo della sessione** Nella console di monitoraggio, Nella console di monitoraggio, il pannello **User Details view > Logon Duration** (vista Dettagli utente > Durata accesso) ora include informazioni sulla fase **Interactive Session** (Sessione interattiva) del processo di accesso. Per fornire una risoluzione dei problemi e una correzione più granulari di questa fase dell'accesso, **Interactive Session** ha ora tre sottofasi: **Pre-userinit**, **Userinit** e **Shell**. In questa versione, passando il mouse su **Interactive Session** viene visualizzata una descrizione comando che mostra le sottofasi e un collegamento alla documentazione. Per una descrizione delle sottofasi e come migliorare le prestazioni di ciascuna fase, vedere Diagnosticare i problemi di accesso utente.

### marzo 2018

- **Previsione dell'istanza dell'applicazione (funzione di anteprima).** Questa è la prima funzionalità di monitoraggio basata sull'analisi predittiva. La previsione dei modelli di utilizzo delle risorse è importante per gli amministratori al fine di organizzare le risorse e il numero di licenze richieste su ciascuna risorsa. La funzione di previsione delle istanze dell'applicazione indica il numero di istanze di applicazione ospitate che possono essere avviate per sito o gruppo di consegna nel tempo. Per fare la previsione vengono utilizzati algoritmi di apprendimento automatico basati su modelli di dati creati con dati storici esistenti. Il livello di tolleranza indica la qualità della previsione.

  Per ulteriori informazioni, vedere Previsione delle istanze dell'applicazione in Director. Inviare commenti sull'utilità e l'usabilità di questa funzione nel forum di discussione di Citrix Cloud.

- **API dei gruppi di consegna - Anteprima**

  L'anteprima delle API dei gruppi di consegna fornisce una serie di API REST utilizzabili per automatizzare la gestione dei gruppi di consegna. Il set completo di API disponibili può essere visualizzato e provato nella documentazione delle API di Citrix Cloud all'indirizzo https://developer.cloud.com/.

- **Autenticazione Web Studio**

  La console di gestione dei servizi su Citrix Cloud ora utilizza un token al portatore per autenticare i clienti. Il token al portatore è necessario per autenticare l'accesso all'API REST dei gruppi di consegna.

- **Accedere ai dati del servizio di monitoraggio utilizzando l'API OData versione 4 (funzione di anteprima)**

  È possibile creare dashboard di monitoraggio e reporting personalizzate in base ai dati del servizio di monitoraggio utilizzando l'endpoint OData V.4. OData V.4 si basa sull'API Web ASP.NET e supporta le query di aggregazione. Utilizzare il proprio nome utente Citrix Cloud e il token al portatore per accedere ai dati con l'endpoint V4. Per ulteriori informazioni ed esempi, vedere Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

  Condividere commenti sull'utilità di questa funzione nel forum di discussione Citrix Cloud.

#### Correzioni

- È possibile rinominare, spostare ed eliminare le cartelle delle applicazioni. [#STUD -2376]

## gennaio 2018

- **Controllo licenza Servizi Desktop remoto.** La creazione di un catalogo delle macchine contenente macchine con sistema operativo Windows Server ora include un controllo automatico delle licenze RDS. Vengono visualizzati tutti i problemi di licenza RDS rilevati, consentendo di adottare le misure appropriate per evitare interruzioni del servizio. Per ulteriori informazioni, vedere Creare cataloghi di macchine.
- **Accedere alla console della macchina da Monitor.** Il pannello Machine Details di Monitor ora fornisce l'accesso alle console delle macchine ospitate sull'hypervisor XenServer versione 7.3. Ora è possibile risolvere i problemi dei VDA direttamente da Monitor. Per ulteriori informazioni, vedere Accesso alla console della macchina in Risoluzione dei problemi relativi alle macchine.

## dicembre 2017

### Funzionalità nuove e migliorate

- **Citrix Workspace.** Citrix Workspace è ora disponibile per i **nuovi** clienti di XenApp e XenDesktop Service. Per ulteriori informazioni, vedere Configurazione dell'area di lavoro.
- **Analisi delle applicazioni.** Ora è possibile analizzare e monitorare le prestazioni delle applicazioni in modo efficiente con la nuova pagina Application Analytics disponibile dalla scheda **Monitor** > **Applications** . La pagina fornisce una visione consolidata dello stato e dell'utilizzo di tutte le applicazioni pubblicate sul Sito. Questa scheda mostra metriche come il numero di istanze per applicazione e gli errori e i guasti associati alle applicazioni pubblicate. Questa funzionalità richiede i VDA versione 7.15 o successiva.

  Per ulteriori informazioni, vedere la sezione Application Analytics (Analisi delle applicazioni) in Monitor.

## novembre 2017

### Funzionalità nuove e migliorate

- **Cache host locale.** La cache host locale consente di continuare le operazioni di intermediazione delle connessioni quando un Cloud Connector che si trova nella posizione di una risorsa non può comunicare con Citrix Cloud. Per i dettagli, vedere Cache host locale.
- **Dischi gestiti di Azure.** I dischi gestiti di Azure sono ora utilizzati per impostazione predefinita per le macchine virtuali con provisioning MCS negli ambienti di Azure Resource Manager. Facoltativamente, è possibile utilizzare account di archiviazione convenzionali. Per i dettagli, vedere Ambienti di virtualizzazione Microsoft Azure Resource Manager.

- **Amministratore dell'helpdesk.** Quando si gestiscono gli amministratori del servizio per un account cliente di Citrix Cloud, ora è disponibile una nuova scelta: helpdesk Administrator. Un amministratore di helpdesk può accedere alle funzioni Monitor sul servizio. Per i dettagli, vedere Gestione.

### Correzioni

- È ora possibile utilizzare la procedura guidata della console di gestione dei servizi per creare un catalogo di macchine Accesso remoto al PC. Nelle versioni precedenti, era necessario utilizzare un cmdlet PowerShell per creare un catalogo (come documentato in CTX220737). In esse era necessario tornare alla console di gestione per creare un gruppo di consegna. Ora, è possibile creare il catalogo e il gruppo di consegna in sequenza sulla console di gestione.
- I cataloghi creati da MCS possono utilizzare gli account macchina Active Directory esistenti. [#DNA -24566]
- Quando si effettua il monitoraggio di una distribuzione e si fa scorrere una tabella **Trends > Sessions** (Tendenze > Sessioni) ordinata vengono visualizzati risultati accurati. [DNA-51257]

### Ulteriori informazioni

- Problemi noti.
- Per informazioni sul software di terze parti incluso nel servizio, vedere Notifiche di terze parti.

## Problemi noti

October 30, 2023

Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops) presenta i seguenti problemi noti:

- Il disco di identità di preparazione AWS è disponibile anche dopo che il processo di creazione della macchina ha eliminato la macchina virtuale di preparazione. Questo problema è stato risolto. Tuttavia, è possibile eliminare qualsiasi disco di identità di preparazione disponibile se non è in corso alcuna attività di creazione del catalogo o aggiornamento delle immagini. [PMCS-34500]
- In un ambiente VMware ospitato su AWS, la creazione del catalogo macchine MCS non riesce se l'immagine master è abilitata per vTPM. Per il supporto di VMware, vedere Ricevere assistenza. [PMCS-37603]

- Le schermate del monitor potrebbero non essere caricate se l'URL di Pendo, `https://citrix-cloud-content.customer.pendo.io/`, è bloccato.
  [DIR-18482]
- Viene visualizzato un errore se si esegue un comando con `XDHyp:\` nell'SDK Remote PowerShell. Per risolvere questo problema:

  1. Eseguire un comando con `Hyp`. Ad esempio: `Get-HypServiceStatus`
  2. Eseguire un comando con `XDHyp:\`. Ad esempio: `Get-ChildItem XDHyp:\Connections\`

  [BRK-13723]
- La creazione del catalogo delle macchine MCS non riesce se si utilizza il disco del sistema operativo temporaneo per creare un catalogo utilizzando un'immagine proveniente da una sottoscrizione diversa in ambiente Azure. [CCVADHELP-2600]
- Dopo le modifiche dell'architettura Citrix DaaS nella versione 2209, le icone predefinite per i desktop Windows e per le applicazioni distribuite prima di questa versione sono state sostituite da icone desktop PC generiche. Questa modifica è applicabile solo ai desktop e alle applicazioni che puntano all'icona predefinita. Se si desidera riportare le icone all'icona predefinita dell'applicazione Windows, eseguire il seguente script utilizzando l'SDK Remote PowerShell:
  `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- In **Manage > Full Configuration** i tentativi di modificare il tipo di sistema operativo per i cataloghi di Azure falliscono e viene visualizzato un messaggio di errore. La modifica del tipo di sistema operativo per i cataloghi di Azure non è più supportata anche se si utilizza PowerShell. [STUD-19819]
- Se non si esegue l'aggiornamento alla versione più recente di Remote SDK prima di introdurre i VDA Citrix Virtual Apps and Desktops versione 2206 nell'ambiente DaaS, viene visualizzato il seguente errore durante l'esecuzione dei cmdlet: **Invalid enum value *L7_34* cannot be deserialized into *Citrix.Broker.Admin.SDK.FunctionalLevel*** (Il valore enum non valido L7_34 non può essere deserializzato in Citrix.Broker.Admin.SDK.FunctionalLevel). [PMCS-27248]
- Quando si crea un catalogo di macchine, la macchina virtuale in cui viene eseguito il programma di avvio automatico di Volume Worker (XenDesktop Temp) non viene terminata correttamente. Di conseguenza, si verifica un errore e la macchina virtuale subisce una perdita. Ciò si verifica quando Machine Creation Services (MCS) non riesce a riconoscere un nome di dispositivo associato al programma di avvio automatico di HVM Linux. Per risolvere questo problema, eliminare manualmente il programma di avvio automatico del Volume Worker (XenDesktop Temp) e l'interfaccia di rete a esso associata. [PMCS-20277]

- Negli ambienti Microsoft Azure, l'abilitazione simultanea del disco del sistema operativo temporaneo di Azure e dell'I/O MCS non riesce a creare un catalogo di macchine. Tuttavia, per i cataloghi di macchine esistenti, è comunque possibile aggiornare un catalogo di macchine, aggiungere o eliminare macchine virtuali ed eliminare un catalogo di macchine. [PMCS-21698]
- L'attuale implementazione della comunicazione con hypervisor, *Remote HCL*, potrebbe generare eccezioni da parte della piattaforma hypervisor di destinazione. Di conseguenza, la connessione tra il controller cloud e il connettore cloud non riesce e viene quindi ricreata. Se sono in corso altre operazioni di Remote HCL che utilizzano la stessa connessione, anche queste connessioni possono fallire. Ciò fa sì che gli stati di alimentazione e registrazione della macchina non siano sincronizzati. Di conseguenza possono sorgere altri problemi perché il problema riguarda tutti i tipi di operazioni di Remote HCL, non solo gli stati di alimentazione. Gli hypervisor di Azure e GCP che ospitano le connessioni non sono interessati. Queste connessioni non utilizzano Remote HCL. [CCVADHELP-483]
- Le macchine VMware non si riavviano e non possono essere riavviate forzatamente. Questo problema si applica a tutte le versioni di VMware, incluso VMC su AWS. Il problema si verifica nei cataloghi di macchine che dispongono di macchine virtuali persistenti (dedicate) o di macchine virtuali ad alimentazione gestita. Per risolvere questo problema, utilizzare il cmdlet `New-Brokerhostingpoweraction` per riavviare o forzare il riavvio delle macchine. [PMCS-15797]
- L'icona a forma di freccia dell'elena discesa per i pulsanti Average IOPS (IOPS medio), Session Control (Controllo sessione) e Power Control (Controllo alimentazione) potrebbe non essere visualizzata nelle pagine **User Details** (Dettagli utente) e **Machine Details** (Dettagli macchina). Tuttavia, la funzionalità funziona come previsto. Per visualizzare tutte le voci del menu, fare clic in un punto qualsiasi del pulsante. [DIR-11875]
- Se si utilizza Azure AD Domain Services: gli UPN di accesso a Workspace (o StoreFront) devono contenere il nome di dominio specificato durante l'abilitazione di Azure AD Domain Services. Gli accessi non possono utilizzare gli UPN per un dominio personalizzato creato dall'utente, anche se tale dominio personalizzato è designato come primario.
- Quando si esegue la distribuzione in Azure e si crea un catalogo MCS versione 7.9 o successiva con la cache write-back abilitata e la versione del VDA installato nell'immagine master è 1811 o precedente, si verifica un errore. Inoltre, non è possibile creare nulla che sia correlato a Personal vDisk per Microsoft Azure. Come soluzione alternativa, selezionare una versione del catalogo diversa da distribuire in Azure o disabilitare la cache write-back. Per disabilitare la cache write-back quando si crea un catalogo, deselezionare le caselle di controllo **Memory allocated to cache** (Memoria allocata alla cache) e **Disk cache size** (Dimensione cache disco) nella pagina **Machines**.
- Il collegamento **Console** in **Monitor > Machine Details** (Monitor > Dettagli macchina) non avvia la console della macchina nei browser Microsoft Edge 44 e Firefox 68 ESR. [DIR-8160]

- La modifica del nome di un Virtual Private Cloud (VPC) AWS nella console AWS danneggia l'unità di hosting esistente in Citrix Cloud. Quando l'unità di hosting è danneggiata, non è possibile creare cataloghi o aggiungere macchine ai cataloghi esistenti. [PMCS-7701]
- Quando si tenta di utilizzare l'opzione "Restart"nell'app Workspace Web o desktop, la finestra di dialogo "Restarting"non si chiude mai e non segnala mai l'esito positivo. L'hypervisor mostra che il computer è stato arrestato ma non è stato avviato. Come soluzione alternativa, dopo un po'di tempo l'utente può chiudere la finestra di dialogo "Restarting"e avviare il desktop; il desktop dovrebbe avviarsi. [BRK-5564]
- Quando si distribuiscono macchine in un catalogo MCS, l'attività di provisioning può non riuscire e viene visualizzato il seguente messaggio di errore: "Terminating Error: Desktop Studio closed."(Errore di interruzione: Desktop Studio chiuso). I dettagli dell'errore potrebbero indicare che non sono stati creati account AD. Il catalogo potrebbe completarsi correttamente in seguito senza intervento. Il problema viene riscontrato nelle distribuzioni grandi e complesse. [PMCS-8869]
- Cloud Library non può essere utilizzata per assegnare risorse nelle distribuzioni che includono StoreFront locale. [CCVADHELP-625]

Per i problemi relativi agli attuali VDA, vedere Problemi noti.

## Deprecazione

December 18, 2023

Questo articolo fornisce un avviso anticipato sulle funzionalità di Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) che vengono gradualmente eliminate, in modo da poter prendere decisioni aziendali tempestive. Citrix monitora l'utilizzo da parte dei clienti e il loro feedback per determinare quando procedere al ritiro di funzioni. Gli annunci possono cambiare nelle versioni successive e potrebbero non includere tutte le funzionalità deprecate. Per informazioni dettagliate sul supporto del ciclo di vita del prodotto, vedere l'articolo Criteri di supporto del ciclo di vita del prodotto.

> **Nota:**
>
> Le deprecazioni e le rimozioni di Citrix Virtual Apps and Desktops sono descritte nei relativi articoli sulla deprecazione.

### Deprecazioni e rimozioni

L'elenco seguente mostra le funzionalità Citrix DaaS che sono state deprecate o rimosse.

Gli elementi *deprecati* non vengono rimossi immediatamente. Citrix continua a supportarli, ma verranno rimossi in una versione futura.

Gli elementi *rimossi* vengono rimossi o non sono più supportati in Citrix DaaS. Le date in **grassetto** indicano gli ultimi aggiornamenti.

| Elemento | Deprecazione annunciata nella versione | Rimosso nella versione | Alternativa |
|---|---|---|---|
| Supporto di AWS volume worker | novembre 2023 | | Utilizzare il caricamento e il download diretti del disco. Vedere Caricamento e download diretti del disco. |
| Supporto di `Leave user management to Citrix Cloud` utilizzato nella creazione di gruppi di consegna | settembre 2023 | settembre 2023 | |
| Supporto dell'uso di `AwsCaptureInstanceProperties` in ambienti AWS | agosto 2023 | | Usare un profilo macchina. Vedere Creare un catalogo utilizzando un profilo macchina. |
| Supporto per VMware vSphere 6.7 | | giugno 2023 | Utilizzare versioni superiori per VMware vSphere. |
| Comando PowerShell `Schedule-ProvVMUpdate` | aprile 2023 | | Utilizzare il comando `Set-ProvVMUpdateTimeWindow`. |

| Elemento | Deprecazione annunciata nella versione | Rimosso nella versione | Alternativa |
|---|---|---|---|
| Comando PowerShell `Request-ProvVMUpdate` | aprile 2023 | | Usare i comandi `Set-ProvVMUpdateTimeWindow` con i parametri `-StartsNow` e `-DurationInMinutes -1`. |
| Comando PowerShell `Cancel-ProvVMUpdate` | aprile 2023 | | Utilizzare il comando `Clear-ProvVMUpdateTimeWindow`. |
| Parametro `DedicatedTenancy` usato nel comando `New-ProvScheme` | marzo 2023 | | Utilizzare il parametro `TenancyType`. |
| Disco non gestito per il provisioning di macchine virtuali in ambienti Azure | giugno 2022 | | |
| Supporto di quattro comandi specifici di AWS: `Revoke-HypSecurityGroupIngress` `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` e `Grant-HypSecurityGroupIngress` | maggio 2022 | | |
| Parametro `StorageAccountType` utilizzato negli ambienti Azure | aprile 2022 | | Utilizzare `StorageType`. |

| Elemento | Deprecazione annunciata nella versione | Rimosso nella versione | Alternativa |
|---|---|---|---|
| Console legacy (console basata su MMC) | luglio 2021 | novembre 2021 | Utilizzare **Manage > Full Configuration** (Gestisci > Configurazione completa) per accedere all'intera serie di azioni di configurazione e gestione. |
| Azure Quick Deploy | settembre 2020 | | Utilizzare Quick Deploy. |
| Possibilità di importare dispositivi di destinazione Citrix Provisioning per creare cataloghi in Citrix Studio. | agosto 2020 | febbraio 2021 | Utilizzare la procedura guidata Citrix Provisioning Export Devices Wizard per eseguire il push delle macchine virtuali di Citrix Provisioning nei controller di consegna/MCS per la creazione del catalogo. Vedere la procedura guidata Export Devices. |

## Requisiti di sistema

October 30, 2023

### Introduzione

I requisiti di sistema per i componenti non descritti in questa sezione (ad esempio l'app Citrix Workspace e Citrix Provisioning) sono descritti nella rispettiva documentazione.

Non è possibile fornire raccomandazioni specifiche per il dimensionamento di macchine virtuali che forniscono desktop e applicazioni a causa della natura complessa e dinamica delle offerte hardware. Ogni distribuzione ha esigenze specifiche. Generalmente, il dimensionamento di una VM si basa sull'hardware e non sui carichi di lavoro dell'utente (ad eccezione della RAM; è necessaria più RAM per le applicazioni che consumano di più). Citrix Tech Zone contiene le linee guida più recenti sul dimensionamento dei VDA.

> **Importante:**
>
> Le versioni VDA citate in questo articolo sono soggette al ciclo di vita del prodotto Citrix. Per ulteriori informazioni, vedere la Product Matrix sul sito Web di Citrix.
>
> Per ulteriori informazioni sull'uso dei VDA LTSR con Citrix DaaS, vedere CTX205549.

**Da ricordare:** in una distribuzione Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops), non è necessario installare o gestire i componenti principali (Delivery Controller, database del sito o console di gestione e monitoraggio). Per la guida all'installazione di Virtual Delivery Agent (VDA), vedere:

- Installare i VDA
- Installare i VDA utilizzando la riga di comando

### Cloud Connector

Per ulteriori informazioni, vedere Dettagli tecnici di Cloud Connector.

### VDA in un ambiente Azure

Sistemi operativi supportati:

- Windows 11 multisessione
- Windows 11 a sessione singola
- Windows 10 multisessione
- Windows 10 a sessione singola
- Windows Server 2022 (versione minima: VDA 2106)
- Windows Server 2019
- Windows Server 2016

Tutti i VDA che non hanno raggiunto la fine del ciclo di vita sono supportati per l'uso con Citrix DaaS. Per i vDA LTSR, si consiglia di utilizzarli con l'aggiornamento cumulativo più recente. Per ulteriori informazioni sul ciclo di vita dei VDA, vedere la matrice dei prodotti Citrix..

Windows Server 2012 R2 è supportato solo con VDA 1912 (e CU successive).

Windows Server richiede la licenza Microsoft RDS.

Per informazioni su Desktop virtuale Azure, vedere la documentazione di Microsoft.

### VDA per sistema operativo a sessione singola

Le seguenti informazioni sono valide per l'ultima versione di VDA.

Sistemi operativi supportati:

- Windows 11
- Windows 10
  - Per il supporto della versione, vedere CTX224843. Questo articolo contiene anche collegamenti a problemi noti Citrix con le versioni di Windows supportate.
  - Il reindirizzamento della composizione del desktop e la modalità grafica legacy non sono supportati in Windows 10.

Requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se è installata una versione successiva).
- Microsoft Visual C++ 2015-2019 Redistributable.
  - Se la macchina contiene una versione precedente di quel runtime (ad esempio 2015-2017), il programma di installazione di Citrix la aggiorna.
  - Se la macchina contiene una versione precedente al 2015, Citrix installa la versione più recente in parallelo.

Accesso remoto PC utilizza questo VDA, che viene installato sui PC fisici dell'ufficio. Questo VDA supporta Secure Boot per Remote PC Access (Accesso remoto PC) di Citrix Virtual Desktops.

Diverse funzionalità di accelerazione multimediale (ad esempio HDX MediaStream Windows Media Redirection) richiedono l'installazione di Microsoft Media Foundation nel computer in cui si installa il VDA. Se nel computer non è installato Media Foundation, le funzionalità di accelerazione multimediale non vengono installate e non funzionano. Non rimuovere Media Foundation dal computer dopo l'installazione del software Citrix. In caso contrario, gli utenti non possono accedere al computer. Nella maggior parte delle versioni del sistema operativo Windows desktop supportate, il supporto di Media Foundation è già installato e non può essere rimosso. Tuttavia, le versioni N non includono alcune tecnologie relative ai supporti multimediali. È possibile ottenere tale software da Microsoft o da terze parti.

Ulteriori informazioni:

- Per informazioni sui VDA Linux, vedere la documentazione del prodotto Linux Virtual Delivery Agent.
- Per utilizzare la funzionalità VDI del server, è possibile utilizzare l'interfaccia della riga di comando per installare un VDA a sessione singola su un computer Windows Server supportato. Per ulteriori informazioni, vedere VDI del server.
- Per informazioni sull'installazione di un VDA su una macchina meno recente, vedere Sistemi operativi precedenti.
- Vedere anche VDA in un ambiente desktop virtuale Azure.

### VDA per sistema operativo multisessione

Le seguenti informazioni sono valide per l'ultima versione di VDA.

Sistemi operativi supportati:

- Windows Server 2022 (versione minima: VDA 2106)
- Windows Server 2019 edizioni Standard e Datacenter
- Windows Server 2016, edizioni standard e Datacenter
- Windows 11
- Windows 10 (64 bit) tutte le versioni supportate

Il programma di installazione implementa automaticamente i seguenti requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se è installata una versione successiva).
- Microsoft Visual C++ 2015-2019 Redistributable.
  - Se la macchina contiene una versione precedente di quel runtime (ad esempio 2015-2017), il programma di installazione di Citrix la aggiorna.
  - Se la macchina contiene una versione precedente al 2015, Citrix installa la versione più recente in parallelo.

Il programma di installazione installa automaticamente e abilita i servizi ruolo Servizi Desktop remoto, se non sono già installati e abilitati. In questo modo viene attivato un riavvio.

Diverse funzionalità di accelerazione multimediale (ad esempio HDX MediaStream Windows Media Redirection) richiedono l'installazione di Microsoft Media Foundation nel computer in cui si installa il VDA. Se nel computer non è installato Media Foundation, le funzionalità di accelerazione multimediale non vengono installate e non funzionano. Non rimuovere Media Foundation dal computer dopo l'installazione del software Citrix. In caso contrario, gli utenti non possono accedere al computer.

Nella maggior parte delle versioni di Windows Server, la funzionalità Media Foundation viene installata tramite Server Manager. Tuttavia, le versioni N non includono alcune tecnologie relative ai supporti multimediali. È possibile ottenere tale software da Microsoft o da terze parti.

Se Media Foundation non è presente sul VDA, queste funzionalità multimediali non funzionano:

- Reindirizzamento flash
- Reindirizzamento di Windows Media
- Reindirizzamento video HTML5
- Reindirizzamento webcam HDX RealTime

Ulteriori informazioni:

- Per informazioni sui VDA Linux, vedere gli articoli su Linux Virtual Delivery Agent.
- Per informazioni sull'installazione di un VDA su un sistema operativo Windows non più supportato, vedere Sistemi operativi precedenti.
- Vedere anche VDA in un ambiente desktop virtuale Azure.

### Host/risorse di virtualizzazione

Sono supportati gli host/le risorse di virtualizzazione seguenti (in ordine alfabetico). Ove applicabile, sono supportate le versioni *major.minor*, inclusi gli aggiornamenti di tali versioni. CTX131239 contiene le informazioni più aggiornate sulla versione dell'hypervisor, oltre a collegamenti a problemi noti.

- **Amazon Web Services (AWS)**
  - È possibile eseguire il provisioning di applicazioni e desktop sui sistemi operativi server Windows supportati.
  - Amazon Relational Database Service (RDS) non è supportato.

  Per ulteriori informazioni, consultare Ambienti cloud AWS.
- **Citrix Hypervisor (in precedenza XenServer)**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Citrix Hypervisor.
- **Google Cloud Platform**

  Per ulteriori informazioni, vedere Ambienti Google Cloud e Getting Started with Citrix DaaS on Google Cloud.
- **Microsoft Azure Resource Manager**

  Per ulteriori informazioni, vedere Ambienti cloud Microsoft Azure Resource Manager.

- **Microsoft System Center Virtual Machine Manager**

  Include qualsiasi versione di Hyper-V registrabile con le versioni supportate di System Center Virtual Machine Manager.

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.

- **Nutanix Acropolis**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione Nutanix.

- **VMware Cloud on AWS**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere VMware Cloud on Amazon Web Services (AWS).

- **Soluzione Azure VMware (AVS)**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Integrazione con la soluzione Azure VMware (AVS).

- **Google Cloud VMware Engine**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Google Cloud VMware Engine.

- **VMware vSphere(vCenter + ESXi)**

  Non viene fornito alcun supporto del funzionamento della modalità collegata vSphere vCenter.

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione VMware.

> **Nota:**
>
> Non è necessario installare il software VDA su alcun server Citrix DDC o StoreFront. Il VDA deve essere un sistema autonomo. L'installazione di più componenti su una singola macchina virtuale è consentita solo quando si sviluppa un proof-of-concept o quando si pubblica la console di amministrazione di Studio solo per gli amministratori. In questo caso è necessario assicurarsi che gli utenti non amministratori non abbiano accesso alle VM DDC/StoreFront.

### Livelli funzionali di Active Directory

Sono supportati i seguenti livelli di funzionalità per la foresta e il dominio di Active Directory:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2

Per ulteriori informazioni su Active Directory, vedere Aggiunto ad Active Directory.

### Tecnologie HDX

Per il supporto e i requisiti specifici della funzionalità HDX, vedere HDX.

### Universal Print Server

Universal Print Server comprende componenti client e server. Il componente UpsClient è incluso nell'installazione VDA. Installare il componente UpsServer su ogni server di stampa in cui risiedono stampanti condivise di cui si desidera eseguire il provisioning con Citrix Universal Print Driver nelle sessioni utente.

Il componente UpsServer è supportato in:

- Windows Server 2019
- Windows Server 2016

Requisiti:

- Microsoft .NET Framework 4.8 (minimo)
- Microsoft Visual C++ 2015-2022 ridistribuibile.
  - Se la macchina contiene una versione precedente di quel runtime (ad esempio 2015-2017), il programma di installazione di Citrix la aggiorna.
  - Se la macchina contiene una versione precedente al 2015, Citrix installa la versione più recente in parallelo.

Per i VDA multisessione, l'autenticazione utente durante le operazioni di stampa richiede che Universal Print Server venga aggiunto allo stesso dominio del VDA.

I pacchetti di componenti client e server autonomi sono disponibili anche per il download.

Per ulteriori informazioni, vedere Eseguire il provisioning delle stampanti.

### Connettività del servizio

Per informazioni sulla connessione a Internet, vedere Requisiti di sistema e connettività. Tali informazioni includono i requisiti comuni alla maggior parte dei servizi Citrix Cloud, oltre ai requisiti specifici di Citrix DaaS.

### Altro

- La Console Gestione Criteri di gruppo Microsoft (GPMC) è necessaria se si memorizzano le informazioni sui criteri Citrix in Active Directory anziché nel database di configurazione del sito. Sulla macchina su cui si installa `CitrixGroupPolicyManagement_x64.msi` deve essere installato il runtime di Visual Studio 2015. Per ulteriori informazioni, vedere la documentazione Microsoft.
- Questo prodotto supporta le versioni di PowerShell dalla 3 alla 5.
- Per i componenti e le funzionalità di prodotto che possono essere installati su server Windows, le installazioni Server Core e Nano Server non sono supportate, a meno che non sia specificato.
- Per informazioni dettagliate sui limiti delle risorse in una distribuzione, vedere Limiti.
- Per le versioni StoreFront supportate, vedere i requisiti di sistema di StoreFront.
- Per informazioni sulla globalizzazione, vedere CTX119253.
- Per informazioni sulle porte utilizzate da Citrix DaaS, vedere Porte di comunicazione utilizzate da Citrix Technologies.
- Per informazioni sui requisiti per l'utilizzo dell'interfaccia di gestione Quick Deploy (Distribuzione rapida), vedere Requisiti.

## Limiti

December 18, 2023

I valori contenuti in questo articolo indicano i limiti di una singola istanza di Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops). Questi limiti sono stati ampiamente testati da Citrix e sono consigliati per la migliore esperienza utente e amministratore. Si tratta di limiti non vincolanti e non imposti tecnicamente (a eccezione del numero totale di VDA per posizione risorse). Quando il numero di utenti simultanei supera 125,000, Citrix può scalare e combinare più istanze di Citrix DaaS, per offrire un'esperienza unificata su qualsiasi scala.

Le informazioni contenute in questo articolo sono dinamiche. Controllare frequentemente gli aggiornamenti. Se i requisiti attuali non sono soddisfatti dai limiti pubblicati, contattare il proprio rappresentante Citrix per assistenza al più presto possibile.

### Limiti di configurazione

Se i criteri superano il limite, Citrix consiglia di utilizzare il servizio Workspace Environment Management o gli oggetti Criteri di gruppo (GPO) di Active Directory.

| Risorsa | Limite |
| --- | --- |
| Domini di Active Directory | 100 |
| Cartelle delle applicazioni | 1,000 |
| Gruppi di applicazioni | 250 |
| Applicazioni | 5,000 |
| Cataloghi | 2,000 |
| Gruppi di consegna | 2,000 |
| Connessioni host | 200 |
| Posizioni delle risorse | 100 |
| Gestire i criteri della console (Full Configuration [Configurazione completa]) | 200 |
| Tag | 10,000 |
| VDA | 100,000 |

### Limiti di posizione delle risorse

Nella tabella seguente sono elencati i limiti per ciascuna posizione di risorsa.

Se le vostre esigenze superano questi limiti, Citrix consiglia di utilizzare ulteriori posizioni di risorse.

| Risorsa | Limite |
| --- | --- |
| VDA totali (limite rigido) | 10,000 |
| Sessioni totali | 25,000 |
| Domini di Active Directory | 1 |
| Connessioni host | 40 |

I Citrix Cloud Connector sono assegnati alle posizioni delle risorse e collegano i carichi di lavoro a Citrix DaaS. Per informazioni sui limiti di Cloud Connector, vedere Considerazioni su dimensioni e scalabilità per i Cloud Connector.

### Limiti di provisioning

I limiti di provisioning contenuti nella tabella seguente sono i massimi consigliati da Citrix per una singola sottoscrizione a un provider pubblico.

È probabile che si raggiungano i limiti di quota del proprio fornitore di cloud pubblico a livelli inferiori. In questi casi, contattare il fornitore per aumentare la quota di sottoscrizione. Per implementazioni su larga scala, Citrix consiglia un modello hub e spoke, in cui i VDA sono distribuiti su più abbonamenti e connessioni host.

Per ulteriori informazioni, vedere le seguenti architetture di riferimento:

- Citrix DaaS su AWS
- Virtualizzazione Citrix su Google Cloud
- Citrix DaaS su Azure

| Risorsa | Limite |
|---|---|
| VDA per account Amazon Web Services per regione | 1,500 |
| VDA per progetto Google Cloud Platform | 3,000 |
| VDA come da abbonamento a Microsoft Azure per regione | 5,000 |

> **Nota:**
>
> I limiti sono consigliati da Citrix.

### Limiti di utilizzo

Per informazioni sui ruoli dell'amministratore e sulle differenze tra di essi, vedere:

- Gestire gli amministratori (Full Configuration [Configurazione completa])
- Amministratori di monitoraggio (Director)

| Risorsa | Limite |
|---|---|
| Amministratori completi di Concurrent Monitor (Director) | 40 |
| Amministratori dell'helpdesk di Concurrent Monitor (Director) | 200 |
| Amministratori di sessione Concurrent Monitor (Director) | 50 |
| Gestione simultanea degli amministratori cloud (Full Configuration [Configurazione completa]) | 100 |

| Risorsa | Limite |
| --- | --- |
| Gestione simultanea degli amministratori dell'helpdesk (Full Configuration [Configurazione completa]) | 60 |
| Utenti finali simultanei | 125,000 |
| Risorse pubblicate per un singolo utente | 250 |
| Avvio di sessioni al minuto | 3,000 |

- Monitor (Director) supporta l'aggregazione di un massimo di quattro tenant (spoke) Citrix DaaS sotto un singolo tenant (hub).
- Un amministratore dell'helpdesk sull'istanza dell'hub può monitorare e risolvere i problemi di utenti, macchine, endpoint e transazioni da tutte le istanze aggregate (hub e spoke) secondo la configurazione di Delegated Administration sull'istanza specifica.
- Il numero di amministratori simultanei per istanza di Citrix DaaS è indicato nella tabella Limiti di utilizzo.

### Limita il registro delle modifiche

La tabella seguente tiene traccia della modifica del limite di configurazione:

| Data | Risorsa | Descrizione |
| --- | --- | --- |
| 22 Nov 2023 | Domini di Active Directory | Limite aumentato da 85 a 100. |
| | Cataloghi | Limite aumentato da 1000 a 2000. |
| | Gruppi di consegna | Limite aumentato da 1000 a 2000. |
| | Posizioni delle risorse | Limite aumentato da 85 a 100. |
| | Posizione delle risorse -> Sessioni totali | Limite aumentato da 20.000 a 25.000. |
| 07 Dec 2023 | Limiti di provisioning -> VDA come da abbonamento a Microsoft Azure per regione | Limite aumentato da 2.500 a 5.000. |

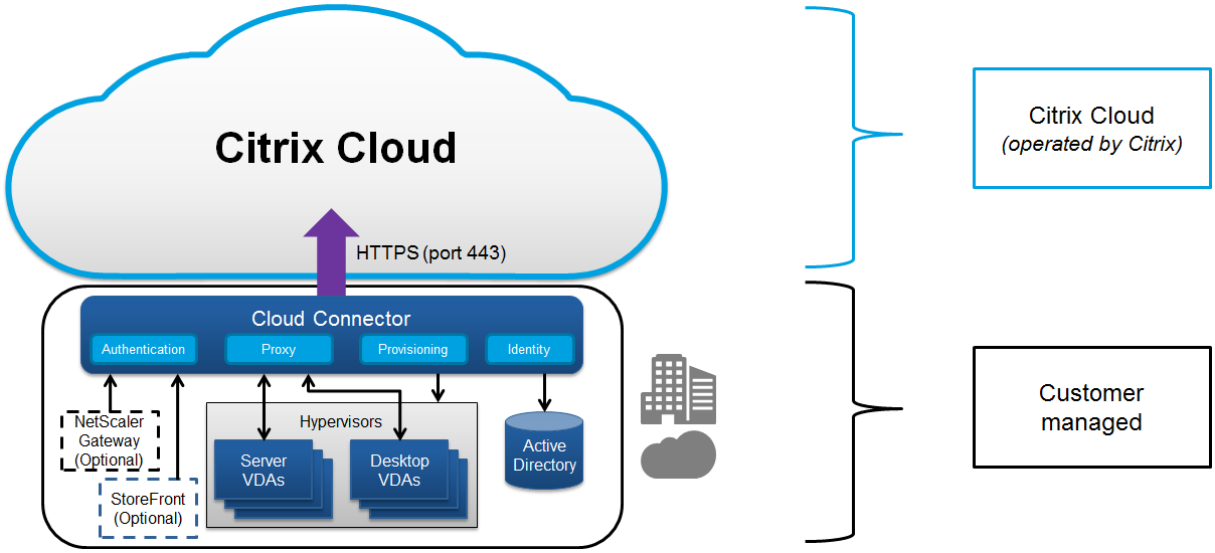
# Panoramica sulla sicurezza tecnica

June 8, 2023

## Panoramica sulla sicurezza

Questo documento si applica a Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) ospitato in Citrix Cloud. Queste informazioni includono Citrix Virtual Apps Essentials e Citrix Virtual Desktops Essentials.

Citrix Cloud gestisce il funzionamento del piano di controllo per gli ambienti Citrix DaaS. Il piano di controllo include i Delivery Controller, le console di gestione, il database SQL, il server delle licenze e, facoltativamente, StoreFront e Citrix Gateway (in precedenza chiamato NetScaler Gateway). I Virtual Delivery Agent (VDA) che ospitano le app e i desktop rimangono sotto il controllo del cliente nel data center di sua scelta, cloud o locale. Questi componenti sono collegati al servizio cloud tramite un agente chiamato Citrix Cloud Connector. Se i clienti scelgono di utilizzare Citrix Workspace, possono anche scegliere di utilizzare il servizio Citrix Gateway invece di eseguire Citrix Gateway all'interno del proprio data center. Il seguente diagramma illustra Citrix DaaS e i suoi limiti di sicurezza.




## Conformità basata su cloud Citrix

A partire da gennaio 2021, l'utilizzo di Citrix Managed Azure Capacity con varie edizioni di Citrix DaaS e Workspace Premium Plus non è stato valutato per Citrix SOC 2 (Tipo 1 o 2), ISO 27001, HIPAA o altri requisiti di conformità cloud. Visitare il Citrix Trust Center per ulteriori informazioni sulle certificazioni Citrix Cloud e controllare frequentemente gli aggiornamenti.

### Flusso di dati

Citrix DaaS non ospita i VDA, pertanto i dati e le immagini delle applicazioni del cliente richiesti per il provisioning sono sempre ospitati nella configurazione del cliente. Il piano di controllo ha accesso ai metadati, come nomi utente, nomi di macchine e collegamenti alle applicazioni, limitando l'accesso alla proprietà intellettuale del cliente dal piano di controllo.

Il flusso di dati tra il cloud e la sede del cliente utilizza connessioni TLS sicure sulla porta 443.

### Isolamento dei dati

Citrix DaaS memorizza solo i metadati necessari per l'intermediazione e il monitoraggio delle applicazioni e dei desktop del cliente. Le informazioni sensibili, tra cui immagini, profili utente e altri dati delle applicazioni, rimangono nella sede del cliente o nella sottoscrizione con un fornitore di cloud pubblico.

### Versioni del servizio

Le funzionalità di Citrix DaaS variano a seconda dell'edizione. Ad esempio, Citrix Virtual Apps Essentials supporta solo il servizio Citrix Gateway e Citrix Workspace. Consulta la documentazione del prodotto per ulteriori informazioni sulle funzionalità supportate.

### Sicurezza ICA

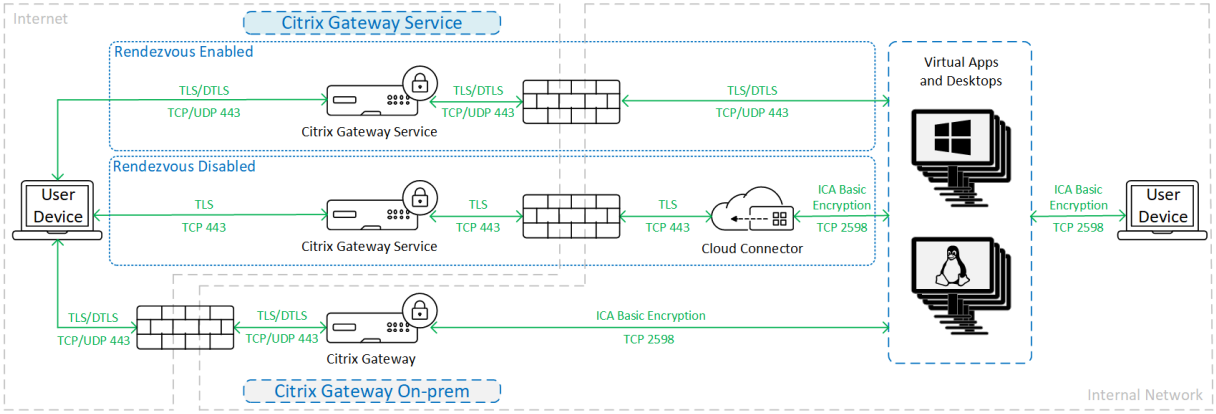
Citrix DaaS offre diverse opzioni per proteggere il traffico ICA in transito. Di seguito sono riportate le opzioni disponibili:

- **Crittografia di base:** impostazione predefinita.
- **SecureICA:** consente di crittografare i dati delle sessioni utilizzando la crittografia RC5 (128 bit).
- **VDA TLS/DTLS:** consente di utilizzare la crittografia a livello di rete utilizzando TLS/DTLS.
- **Protocollo Rendezvous:** disponibile solo quando si utilizza il servizio Citrix Gateway. Quando si utilizza il protocollo Rendezvous, le sessioni ICA vengono crittografate end-to-end utilizzando TLS/DTLS.

#### Crittografia di base

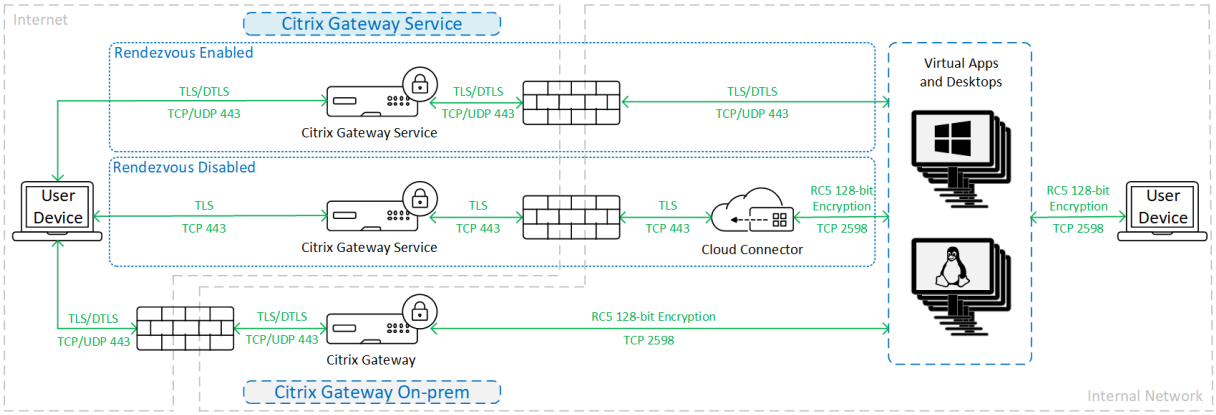
Quando si utilizza la crittografia di base, il traffico viene crittografato come illustrato nella figura seguente.




## SecureICA

Quando si utilizza SecureICA, il traffico viene crittografato come illustrato nella figura seguente.

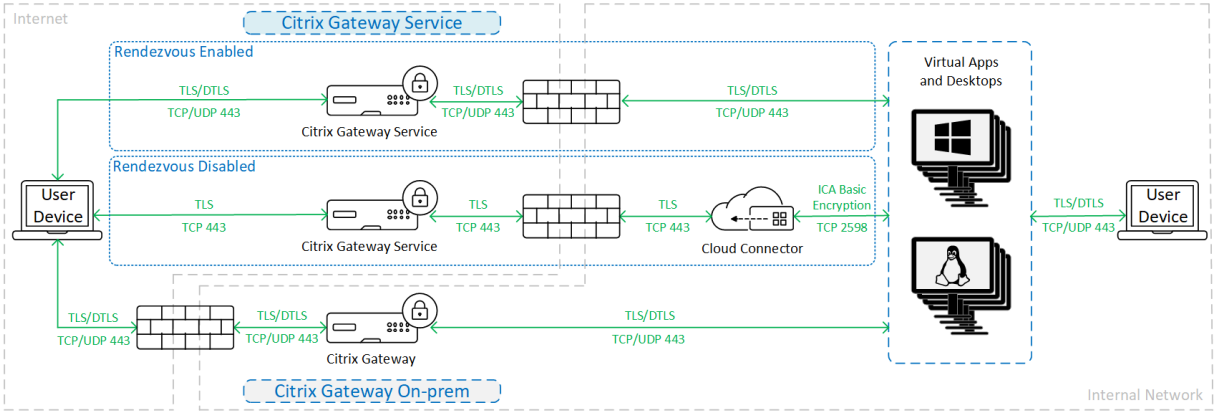



> **Nota:**
>
> SecureICA non è supportato quando si utilizza l'app Workspace per HTML5.

## VDA TLS/DTLS

Quando si utilizza la crittografia VDA TLS/DTLS, il traffico viene crittografato come illustrato nella figura seguente.




> **Nota:**
>
> Quando si utilizza il servizio Gateway senza Rendezvous, il traffico tra VDA e Cloud Connector non è crittografato tramite TLS, poiché il Cloud Connector non supporta la connessione al VDA con crittografia a livello di rete.

### Altre risorse

Per ulteriori informazioni sulle opzioni di sicurezza ICA e su come configurarle, vedere:

- SecureICA: impostazioni dei criteri di sicurezza
- VDA TLS/DTLS: sicurezza a livello di trasporto
- Protocollo Rendezvous: protocollo Rendezvous

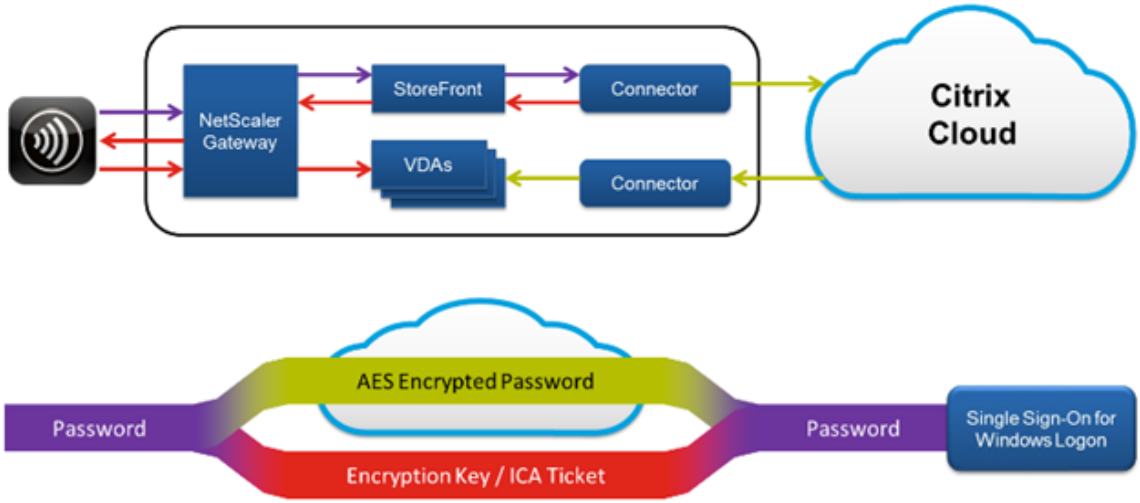
## Gestione delle credenziali

Citrix DaaS gestisce quattro tipi di credenziali:

- Credenziali utente: quando si utilizza uno StoreFront gestito dal cliente, Cloud Connector crittografa le credenziali utente utilizzando la crittografia AES-256 e una chiave casuale monouso generata per ogni avvio. La chiave non viene mai trasferita al cloud e viene restituita solo all'app Citrix Workspace. L'app Citrix Workspace trasferisce quindi questa chiave al VDA per decrittografare la password utente durante l'avvio della sessione per un'esperienza Single Sign-On. Il flusso è illustrato nella figura riportata di seguito.

  Per impostazione predefinita, le credenziali utente non vengono inoltrate attraverso confini di domini non attendibili. Se un VDA e StoreFront sono installati in un dominio e un utente che si trova in un dominio diverso tenta di connettersi al VDA, il tentativo di accesso fallisce a meno che non venga stabilita l'attendibilità tra i domini. È possibile disabilitare questo comportamento e consentire l'inoltro delle credenziali tra domini non attendibili utilizzando l'SDK PowerShell per DaaS. Per ulteriori informazioni, vedere Set-Brokersite.




- Credenziali dell'amministratore: gli amministratori si autenticano con Citrix Cloud. L'autenticazione genera un JSON Web Token (JWT) firmato una tantum che fornisce all'amministratore l'accesso a Citrix DaaS.
- Password dell'hypervisor: gli hypervisor on-premise che richiedono una password per l'autenticazione dispongono di una password generata dall'amministratore che è direttamente archiviata e crittografata nel database SQL nel cloud. Citrix gestisce le chiavi peer per garantire che le credenziali dell'hypervisor siano disponibili solo per i processi autenticati.
- Credenziali di Active Directory (AD): Machine Creation Services utilizza Cloud Connector per la creazione di account delle macchine nell'AD di un cliente. Poiché l'account della macchina di Cloud Connector dispone solo dell'accesso in lettura ad AD, all'amministratore vengono richieste le credenziali per ogni operazione di creazione o eliminazione di macchine. Queste credenziali vengono archiviate solo nella memoria e vengono conservate solo per un singolo evento di provisioning.

### Considerazioni sulla distribuzione

Citrix consiglia agli utenti di consultare la documentazione sulle procedure consigliate pubblicata per la distribuzione di applicazioni Citrix Gateway e VDA nei propri ambienti.

### Requisiti di accesso alla rete di Citrix Cloud Connector

I Citrix Cloud Connector richiedono solo il traffico in uscita della porta 443 verso Internet e possono essere ospitati dietro un proxy HTTP.

- La comunicazione utilizzata in Citrix Cloud per HTTPS è TLS (vedere Deprecazione delle versioni TLS).

- Nell'ambito della rete interna, il Cloud Connector deve accedere a quanto segue per Citrix DaaS:
  - VDA: porta 80, sia in entrata che in uscita, oltre alle porte 1494 e 2598 in entrata se si utilizza il servizio Citrix Gateway
  - Server StoreFront: porta 80 in entrata.
  - Citrix Gateway, se configurati come STA: porta 80 in entrata.
  - Controller di dominio di Active Directory
  - Hypervisor: solo in uscita. Vedere Porte di comunicazione utilizzate da Citrix Technologies per le porte specifiche.

Il traffico tra i VDA e i Cloud Connector viene crittografato utilizzando la sicurezza Kerberos a livello di messaggio.

### StoreFront gestito dal cliente

Uno StoreFront gestito dal cliente offre maggiori opzioni di configurazione di sicurezza e flessibilità per l'architettura di distribuzione, inclusa la possibilità di mantenere le credenziali utente in locale. Lo StoreFront può essere ospitato dietro Citrix Gateway per fornire un accesso remoto sicuro, applicare l'autenticazione a più fattori e aggiungere altre funzionalità di sicurezza.

### Servizio Citrix Gateway

L'utilizzo del servizio Citrix Gateway evita la necessità di implementare Citrix Gateway nei data center dei clienti.

Per ulteriori informazioni, vedere Servizio Citrix Gateway.

Tutte le connessioni TLS tra Cloud Connector e Citrix Cloud vengono avviate da Cloud Connector a Citrix Cloud. Non è richiesta la mappatura delle porte del firewall in entrata.

### Attendibilità XML

Questa impostazione è disponibile in **Full Configuration > Settings > Enable XML trust** (Configurazione completa > Impostazioni > Abilita attendibilità XML) ed è disattivata per impostazione predefinita. In alternativa, è possibile utilizzare Citrix DaaS Remote PowerShell SDK per gestire l'attendibilità XML.

L'attendibilità XML si applica alle distribuzioni che utilizzano:

- StoreFront locale.
- Tecnologia di autenticazione degli abbonati (utenti) che non richiede password. Esempi di tali tecnologie sono le soluzioni mediante pass-through di dominio, smart card, SAML e Veridium.

L'abilitazione dell'impostazione di attendibilità XML consente agli utenti di autenticare e quindi avviare correttamente le applicazioni. Cloud Connector considera attendibili le credenziali inviate da StoreFront. Attivare l'attendibilità XML solo quando sono state protette le comunicazioni tra i Citrix Cloud Connector e StoreFront (utilizzando firewall, IPsec o altri sistemi di protezione consigliati).

Questa impostazione è disabilitata per impostazione predefinita.

Utilizzare l'SDK Remote PowerShell Citrix DaaS per gestire l'attendibilità XML.

- Per verificare il valore corrente dell'attendibilità XML, eseguire `Get-BrokerSite` ed esaminare il valore di `TrustRequestsSentToTheXMLServicePort`.
- Per abilitare l'attendibilità XML, eseguire `Set-BrokerSite -TrustRequestsSentToTheXmlServi $true`
- Per disattivare l'attendibilità XML, eseguire `Set-BrokerSite -TrustRequestsSentToTheXmlServ $false`

### Applicare il traffico HTTPS o HTTP

Per applicare il traffico HTTPS o HTTP tramite il servizio XML, configurare uno dei seguenti set di valori del Registro di sistema su ciascuno dei Cloud Connector.

Dopo aver configurato le impostazioni, riavviare il servizio Remote Broker Provider su ciascun Cloud Connector.

In `HKLM\Software\Citrix\DesktopServer\`:

- Per applicare il traffico HTTPS (ignorare HTTP): impostare `XmlServicesEnableSsl` su `1` e `XmlServicesEnableNonSsl` su `0`.
- Per applicare il traffico HTTP (ignorare HTTPS): impostare `XmlServicesEnableNonSsl` su `1` e `XmlServicesEnableSsl` su `0`.

### Deprecazione delle versioni TLS

Per migliorare la sicurezza di Citrix DaaS, Citrix ha iniziato a bloccare qualsiasi comunicazione su Transport Layer Security (TLS) 1.0 e 1.1 a partire dal 15 marzo 2019.

Tutte le connessioni ai servizi Citrix Cloud da Citrix Cloud Connector richiedono TLS 1.2.

Per garantire la corretta connessione a Citrix Workspace dai dispositivi degli utenti, la versione installata di Citrix Receiver deve essere uguale o più recente rispetto alle versioni successive.

| Receiver | Versione |
| --- | --- |
| Windows | 4.2.1000 |
| Mac | 12.0 |
| Linux | 13.2 |
| Android | 3.7 |
| iOS | 7.0 |
| Chrome/HTML5 | Più recente (il browser deve supportare TLS 1.2) |

Per eseguire l'aggiornamento alla versione più recente di Citrix Receiver, andare alla pagina https://www.citrix.com/products/receiver/.

In alternativa, eseguire l'aggiornamento all'app Citrix Workspace, che utilizza TLS 1.2. Per scaricare l'app Citrix Workspace, andare alla pagina https://www.citrix.com/downloads/workspace-app/.

Se è necessario continuare a utilizzare TLS 1.0 o 1.1 (ad esempio, con un thin client basato su una versione precedente di Receiver per Linux), installare uno StoreFront nella posizione risorsa. Quindi, fare in modo che tutti i Citrix Receiver puntino a esso.

### Ulteriori informazioni

Le seguenti risorse contengono informazioni sulla sicurezza:

- Panoramica tecnica sulla sicurezza per Citrix Managed Azure.
- Sito di sicurezza Citrix.
- Informazioni su sicurezza e conformità: il centro sicurezza e conformità contiene bollettini sulla sicurezza che possono aiutare a rimanere informati. Il centro dispone inoltre di documentazione su standard e certificazioni importanti per mantenere un ambiente IT sicuro e conforme.
- Guida alla distribuzione sicura per la piattaforma Citrix Cloud: questa guida fornisce una panoramica delle procedure consigliate di sicurezza quando si utilizza Citrix Cloud e descrive le informazioni raccolte e gestite da Citrix Cloud. Contiene anche collegamenti a informazioni complete su Citrix Cloud Connector.
- Requisiti di sistema e connettività.
- Considerazioni sulla sicurezza e procedure consigliate.
- Smart card.
- Transport Layer Security (TLS).

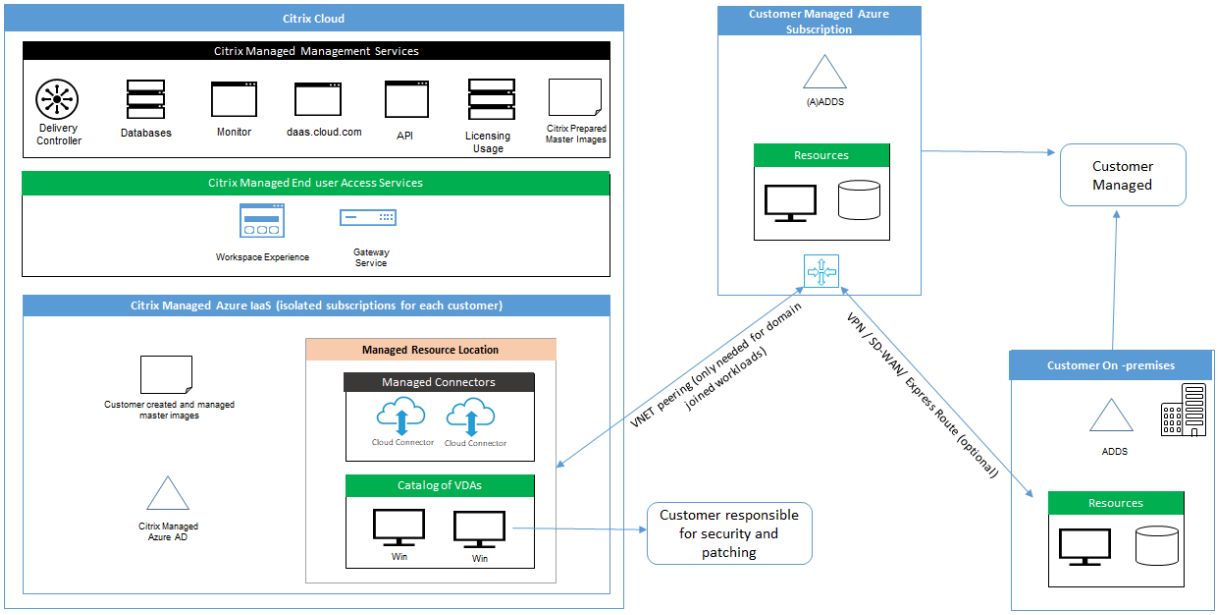
 

> **Nota:**
>
> Questo documento ha lo scopo di fornire al lettore un'introduzione e una panoramica delle funzionalità di sicurezza di Citrix Cloud e di definire la divisione di responsabilità tra Citrix e i clienti per quanto riguarda la sicurezza della distribuzione di Citrix Cloud. Non è destinato a fungere da manuale con linee guida per la configurazione e amministrazione per Citrix Cloud o per uno qualsiasi dei relativi componenti o servizi.

## Panoramica tecnica sulla sicurezza per Citrix Managed Azured

October 6, 2022

Il diagramma seguente mostra i componenti di una distribuzione di Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops) che utilizza Citrix Managed Azure. In questo esempio viene utilizzata una connessione di peering VNet.




Con Citrix Managed Azure, i Virtual Delivery Agent (VDA) del cliente che distribuiscono desktop e app, oltre ai Citrix Cloud Connector, vengono distribuiti in una sottoscrizione di Azure e un tenant gestito da Citrix.

### Conformità basata su cloud Citrix

A partire da gennaio 2021, l'utilizzo di Citrix Managed Azure Capacity con varie edizioni di Citrix DaaS e Workspace Premium Plus non è stato valutato per Citrix SOC 2 (Tipo 1 o 2), ISO 27001, HIPAA o altri

requisiti di conformità cloud. Visitare il Citrix Trust Center per ulteriori informazioni sulle certificazioni Citrix Cloud e controllare frequentemente gli aggiornamenti.

## Responsabilità di Citrix

### Citrix Cloud Connector per cataloghi non aggiunti a un dominio

Quando si utilizza una sottoscrizione Citrix Managed Azure, Citrix DaaS distribuisce almeno due Cloud Connector in ogni posizione di risorse. Alcuni cataloghi possono condividere una posizione risorsa se si trovano nella stessa area geografica di altri cataloghi per lo stesso cliente.

Citrix è responsabile delle seguenti operazioni di sicurezza su Cloud Connector di cataloghi non aggiunti a un dominio:

- Applicazione di aggiornamenti del sistema operativo e patch di sicurezza
- Installazione e manutenzione di software antivirus
- Applicazione degli aggiornamenti software di Cloud Connector

I clienti non hanno accesso ai Cloud Connettor. Pertanto, Citrix è interamente responsabile delle prestazioni dei Cloud Connector dei cataloghi non aggiunti a un dominio.

### Sottoscrizione di Azure e Azure Active Directory

Citrix è responsabile della sicurezza della sottoscrizione di Azure e di Azure Active Directory (AAD) create per il cliente. Citrix garantisce l'isolamento dei tenant, in modo che ogni cliente abbia la propria sottoscrizione di Azure e la propria AAD, evitando così il cross-talk tra tenant diversi. Citrix limita inoltre l'accesso all'AAD solo al personale operativo Citrix DaaS e Citrix. L'accesso di Citrix alla sottoscrizione di Azure di ogni cliente viene verificato.

I clienti che utilizzano cataloghi non aggiunti a un dominio possono utilizzare l'AAD gestita da Citrix come mezzo di autenticazione per Citrix Workspace. Per questi clienti, Citrix crea account utente con privilegi limitati nell'AAD gestita da Citrix. Tuttavia, né gli utenti né gli amministratori dei clienti possono eseguire alcuna azione sull'AAD gestita da Citrix. Se questi clienti scelgono di utilizzare la propria AAD, sono interamente responsabili della sicurezza.

### Reti e infrastruttura virtuali

Nell'ambito della sottoscrizione Citrix Managed Azure del cliente, Citrix crea reti virtuali per isolare le posizioni risorse. All'interno di tali reti, Citrix crea macchine virtuali per VDA, Cloud Connector e macchine per la creazione di immagini, oltre agli account di archiviazione, agli insiemi di credenziali

delle chiavi e ad altre risorse di Azure. Citrix, in collaborazione con Microsoft, è responsabile della sicurezza delle reti virtuali, inclusi i firewall delle reti virtuali.

Citrix garantisce che il criterio firewall di Azure predefinito (gruppi di sicurezza di rete) sia configurato per limitare l'accesso alle interfacce di rete nel peering VNet e nelle connessioni SD-WAN. In genere, controlla il traffico in entrata verso VDA e Cloud Connector. Per ulteriori informazioni, vedere:

- Criteri firewall per le connessioni di peering di Azure VNet
- Criteri firewall per le connessioni SD-WAN

I clienti non possono modificare questo criterio firewall predefinito, ma possono implementare regole firewall aggiuntive sulle macchine VDA create da Citrix, ad esempio per limitare parzialmente il traffico in uscita. I clienti che installano client di reti private virtuali o altro software in grado di aggirare le regole del firewall su macchine VDA create da Citrix sono responsabili di eventuali rischi per la sicurezza che potrebbero insorgere.

Quando si utilizza il generatore di immagini in Citrix DaaS per creare e personalizzare una nuova immagine della macchina, le porte 3389-3390 vengono aperte temporaneamente nella VNet gestita da Citrix, in modo che il cliente possa eseguire RDP sulla macchina contenente la nuova immagine per personalizzarla.

#### Responsabilità di Citrix nell'utilizzo delle connessioni di peering di Azure VNet

Perché i VDA di Citrix DaaS contattino i controller di dominio, le condivisioni di file o altre risorse intranet locali, Citrix DaaS fornisce un flusso di lavoro di peering VNet come opzione di connettività. La rete virtuale gestita da Citrix del cliente viene sottoposta a peering con una rete virtuale di Azure gestita dal cliente. La rete virtuale gestita dal cliente può abilitare la connettività con le risorse locali del cliente utilizzando la soluzione di connettività dal cloud all'ambiente locale scelta dal cliente, ad esempio Azure ExpressRoute o i tunnel IPSec.

La responsabilità di Citrix per il peering VNet è limitata al supporto del flusso di lavoro e della relativa configurazione delle risorse di Azure per stabilire relazioni di peering tra Citrix e le VNet gestite dal cliente.

**Criteri firewall per le connessioni di peering di Azure VNet** Citrix apre o chiude le seguenti porte per il traffico in entrata e in uscita che utilizza una connessione di peering VNet.

#### VNet gestita da Citrix con macchine non aggiunte a un dominio

- Regole in entrata
  - Porte in ingresso 80, 443, 1494 e 2598 consentite dai VDA ai Cloud Connector e dai Cloud Connector ai VDA.

  - Porte 49152-65535 in ingresso consentite per i VDA di un intervallo di indirizzi IP utilizzato dalla funzionalità di monitoraggio dello shadowing. Vedere Porte di comunicazione utilizzate da Citrix Technologies.
  - Tutto l'altro traffico in entrata viene negato. Ciò include il traffico intra-VNet da VDA a VDA e da VDA a Cloud Connector.

- Regole in uscita
  - Tutto il traffico in uscita è consentito.

**VNet gestita da Citrix con macchine aggiunte a un dominio**

- Regole in entrata:
  - Porte 80, 443, 1494 e 2598 in ingresso consentite dai VDA ai Cloud Connector e dai Cloud Connector ai VDA.
  - Porte 49152-65535 in ingresso consentite per i VDA di un intervallo di indirizzi IP utilizzato dalla funzionalità di monitoraggio dello shadowing. Vedere Porte di comunicazione utilizzate da Citrix Technologies.
  - Tutto l'altro traffico in entrata viene negato. Ciò include il traffico intra-VNet da VDA a VDA e da VDA a Cloud Connector.
- Regole in uscita
  - Tutto il traffico in uscita è consentito.

**VNet gestita dal cliente con macchine aggiunte a un dominio**

- È responsabilità del cliente configurare correttamente la VNet. Ciò include l'apertura delle seguenti porte per l'aggiunta al dominio.
- Regole in entrata:
  - Ingresso consentito sulle porte 443, 1494, 2598 dagli IP client per i lanci interni.
  - Ingresso consentito sulle porte 53, 88, 123, 135-139, 389, 445, 636 da Citrix VNet (intervallo di indirizzi IP specificato dal cliente).
  - Ingresso consentito sulle porte aperte con una configurazione proxy.
  - Altre regole create dal cliente.
- Regole in uscita:
  - Uscita consentita sulle porte 443, 1494, 2598 verso Citrix VNet (intervallo di indirizzi IP specificato dal cliente) per i lanci interni.
  - Altre regole create dal cliente.

### Responsabilità di Citrix per l'utilizzo della connettività SD-WAN

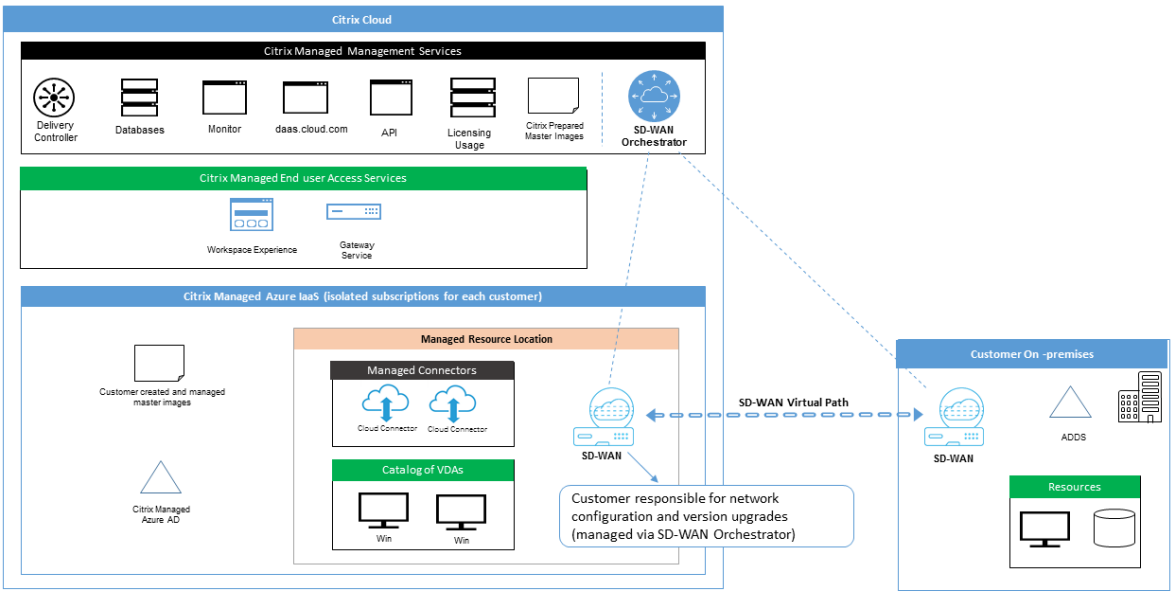
Citrix supporta un modo completamente automatizzato di distribuire istanze Citrix SD-WAN virtuali per abilitare la connettività tra Citrix DaaS e le risorse locali. La connettività Citrix SD-WAN presenta diversi vantaggi rispetto al peering VNet, tra cui:

Elevata affidabilità e sicurezza delle connessioni dal VDA al centro dati e dal VDA alla filiale (ICA).

- La migliore esperienza utente finale per chi lavora in ufficio, con funzionalità QoS avanzate e ottimizzazioni VoIP.
- Capacità integrata di ispezionare, assegnare priorità e creare report sul traffico di rete Citrix HDX e sull'utilizzo di altre applicazioni.

Citrix richiede ai clienti che desiderano sfruttare la connettività SD-WAN per Citrix DaaS di utilizzare SD-WAN Orchestrator per la gestione delle loro reti Citrix SD-WAN.

Il diagramma seguente mostra i componenti aggiunti in una distribuzione di Citrix DaaS utilizzando una sottoscrizione Citrix Managed Azure e la connettività SD-WAN.




La distribuzione Citrix SD-WAN per Citrix DaaS è simile alla configurazione di distribuzione standard di Azure per Citrix SD-WAN. Per ulteriori informazioni, vedere Distribuire l'istanza Citrix SD-WAN Standard Edition su Azure. In una configurazione ad alta disponibilità, una coppia attiva/standby di istanze SD-WAN con sistemi di bilanciamento del carico di Azure viene distribuita come gateway tra la subnet contenente i VDA e i Cloud Connector e Internet. In una configurazione non HA, come gateway viene distribuita solo una singola istanza SD-WAN. Alle interfacce di rete delle appliance SD-WAN virtuali vengono assegnati indirizzi da un intervallo di indirizzi ridotto separato suddiviso in due subnet.

Quando si configura la connettività SD-WAN, Citrix apporta alcune modifiche alla configurazione di rete dei desktop gestiti descritta sopra. In particolare, tutto il traffico in uscita dalla VNet, incluso il traffico verso destinazioni Internet, viene instradato attraverso l'istanza cloud SD-WAN. L'istanza SD-WAN è inoltre configurata per essere il server DNS per la VNet gestita da Citrix.

L'accesso in gestione alle istanze SD-WAN virtuali richiede un login e una password amministratore. A ogni istanza di SD-WAN viene assegnata una password sicura univoca e casuale che può essere utilizzata dagli amministratori SD-WAN per l'accesso remoto e la risoluzione dei problemi tramite l'interfaccia utente di SD-WAN Orchestrator, l'interfaccia utente di gestione dell'appliance virtuale e l'interfaccia della riga di comando.

Proprio come altre risorse specifiche del tenant, le istanze SD-WAN virtuali distribuite in una VNet specifica del cliente sono completamente isolate da tutte le altre VNet.

Quando il cliente abilita la connettività Citrix SD-WAN, Citrix automatizza la distribuzione iniziale delle istanze SD-WAN virtuali utilizzate con Citrix DaaS, mantiene le risorse Azure sottostanti (macchine virtuali, bilanciatori del carico e così via), fornisce impostazioni predefinite sicure ed efficienti pronte all'uso per la configurazione iniziale delle istanze SD-WAN virtuali e consente la manutenzione continua e la risoluzione dei problemi tramite SD-WAN Orchestrator. Citrix adotta inoltre misure ragionevoli per eseguire la convalida automatica della configurazione di rete SD-WAN, verificare la presenza di rischi noti per la sicurezza e visualizzare gli avvisi corrispondenti tramite SD-WAN Orchestrator.

**Criteri firewall per le connessioni SD-WAN** Citrix utilizza i criteri firewall di Azure (gruppi di sicurezza di rete) e l'assegnazione di indirizzi IP pubblici per limitare l'accesso alle interfacce di rete delle appliance SD-WAN virtuali:

- Solo alle interfacce WAN e di gestione vengono assegnati indirizzi IP pubblici e tali interfacce consentono la connettività in uscita a Internet.
- Le interfacce LAN, che fungono da gateway per la VNet gestita da Citrix, possono scambiare traffico di rete solo con macchine virtuali sulla stessa VNet.
- Le interfacce WAN limitano il traffico in ingresso alla porta UDP 4980 (utilizzata da Citrix SD-WAN per la connettività dei percorsi virtuali) e negano il traffico in uscita verso la VNet.
- Le porte di gestione consentono il traffico in entrata verso le porte 443 (HTTPS) e 22 (SSH).
- Le interfacce HA sono consentite solo per lo scambio reciproco del traffico di controllo.

#### Accesso all'infrastruttura

Citrix può accedere all'infrastruttura gestita da Citrix del cliente (Cloud Connector) per eseguire determinate attività amministrative come la raccolta di registri (incluso il Visualizzatore eventi di Windows) e il riavvio dei servizi senza avvisare il cliente. Citrix è responsabile dell'esecuzione di queste attività in modo sicuro e con un impatto minimo per il cliente. Citrix è inoltre responsabile di garantire che

tutti i file di registro vengano recuperati, trasportati e gestiti in modo sicuro e protetto. Non è possibile accedere ai VDA dei clienti in questo modo.

#### Backup per cataloghi non aggiunti a un dominio

Citrix non è responsabile dell'esecuzione di backup di cataloghi non aggiunti a un dominio.

#### Backup per immagini delle macchine

Citrix è responsabile del backup di tutte le immagini delle macchine caricate in Citrix DaaS, comprese le immagini create con il generatore di immagini. Citrix utilizza l'archiviazione ridondante locale per queste immagini.

#### Bastioni per cataloghi non aggiunti a un dominio

Il personale operativo di Citrix ha la possibilità di creare un bastione, se necessario, per accedere alla sottoscrizione di Azure del cliente gestita da Citrix per diagnosticare e risolvere i problemi del cliente, potenzialmente prima che il cliente li riscontri. Citrix non richiede il consenso del cliente per creare un bastione. Quando crea il bastione, Citrix crea una password complessa generata casualmente per il bastione e limita l'accesso RDP agli indirizzi IP NAT di Citrix. Quando il bastione non è più necessario, Citrix lo elimina e la password non è più valida. Il bastione e le relative regole di accesso RDP vengono eliminati al termine dell'operazione. Citrix può accedere solo ai Cloud Connector non aggiunti a un dominio del cliente con il bastione. Citrix non dispone della password per accedere ai VDA non aggiunti a un dominio o ai Cloud Connector e ai VDA aggiunti a un dominio.

#### Criteri firewall quando si utilizzano strumenti per la risoluzione dei problemi

Quando un cliente richiede la creazione di una macchina bastione per la risoluzione dei problemi, vengono apportate le seguenti modifiche al gruppo di sicurezza nella VNet gestita da Citrix:

- Viene consentita temporaneamente la porta 3389 in entrata dall'intervallo di indirizzi IP specificato dal cliente verso il bastione.
- Viene consentita temporaneamente la porta 3389 in entrata dall'indirizzo IP del bastione a qualsiasi indirizzo nella VNet (VDA e Cloud Connector).
- Si continua a bloccare l'accesso RDP tra i Cloud Connector, i VDA e altri VDA.

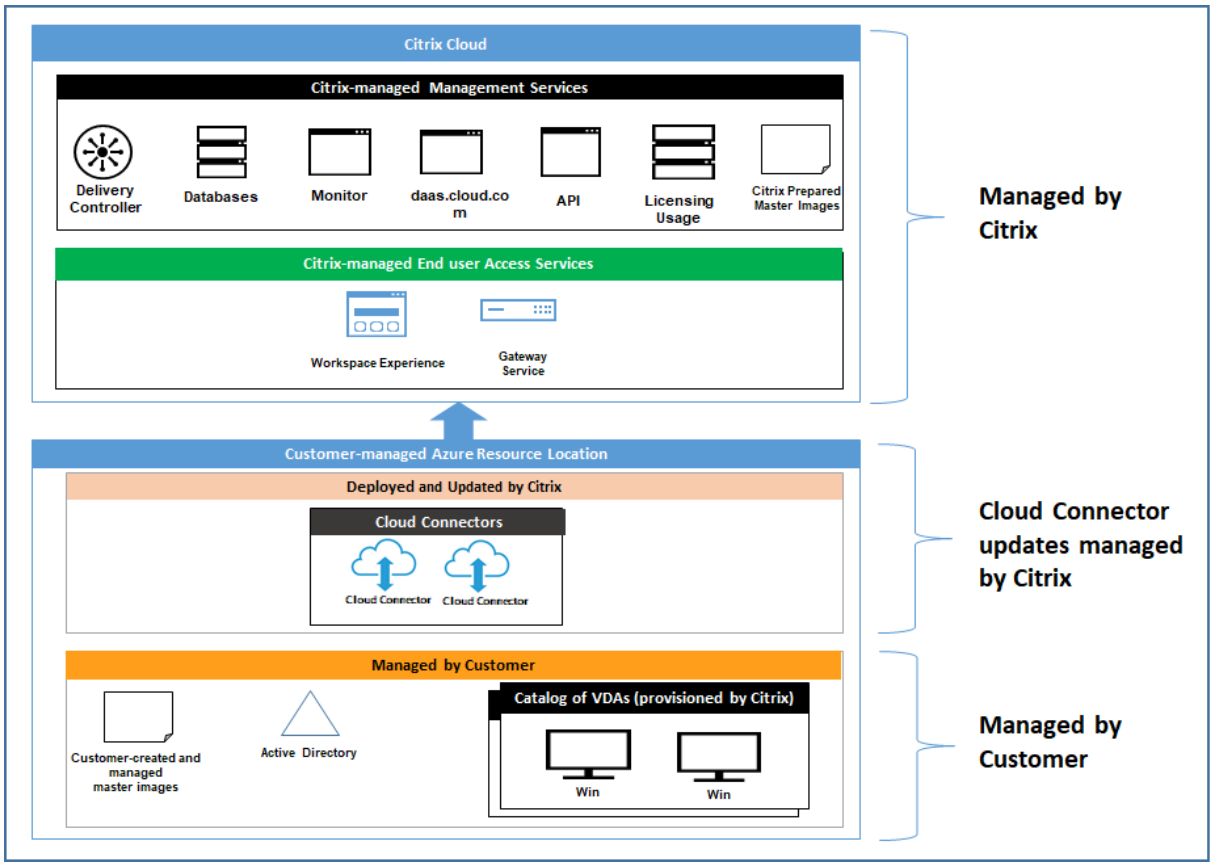
Quando un cliente abilita l'accesso RDP per la risoluzione dei problemi, vengono apportate le seguenti modifiche al gruppo di sicurezza nella VNet gestita da Citrix:

- Viene consentita temporaneamente la porta 3389 in entrata dall'intervallo di indirizzi IP specificato dal cliente a qualsiasi indirizzo nella VNet (VDA e Cloud Connector).
- Si continua a bloccare l'accesso RDP tra i Cloud Connector, i VDA e altri VDA.

### Sottoscrizioni gestite dal cliente

Per le sottoscrizioni gestite dal cliente, Citrix aderisce alle responsabilità di cui sopra durante la distribuzione delle risorse di Azure. Dopo la distribuzione, tutto quanto indicato sopra è di responsabilità del cliente, in quanto è il proprietario della sottoscrizione di Azure.




## Responsabilità del cliente

### VDA e immagini delle macchine

Il cliente è responsabile di tutti gli aspetti del software installato sulle macchine VDA, tra cui:

- Aggiornamenti del sistema operativo e patch di sicurezza
- Antivirus e antimalware
- Aggiornamenti e patch di sicurezza del software del VDA

- Regole firewall software aggiuntive (in particolare per il traffico in uscita)
- Attenersi alle considerazioni sulla sicurezza e alle procedure consigliate di Citrix

Citrix fornisce un'immagine preparata che funge da punto di partenza. I clienti possono utilizzare questa immagine a scopo dimostrativo o come Proof of Concept (POC), oppure come base per creare la propria immagine della macchina. Citrix non garantisce la sicurezza di questa immagine preparata. Citrix tenterà di mantenere aggiornati il sistema operativo e il software del VDA sull'immagine preparata e abiliterà Windows Defender su queste immagini.

#### Responsabilità del cliente nell'utilizzo del peering VNet

Il cliente deve aprire tutte le porte specificate nella VNet gestita dal cliente con macchine aggiunte a un dominio.

Quando viene configurato il peering VNet, il cliente è responsabile della sicurezza della propria rete virtuale e della connettività alle risorse locali. Il cliente è inoltre responsabile della sicurezza del traffico in entrata dalla rete virtuale con peering gestita da Citrix. Citrix non intraprende alcuna azione per bloccare il traffico dalla rete virtuale gestita da Citrix alle risorse locali del cliente.

I clienti hanno a disposizione le seguenti opzioni per limitare il traffico in entrata:

- Fornire alla rete virtuale gestita da Citrix un blocco IP che non è utilizzato altrove nella rete locale del cliente o nella rete virtuale connessa gestita dal cliente. Questa operazione è necessaria per il peering VNet.
- Aggiungere i gruppi di sicurezza e i firewall della rete di Azure nella rete virtuale del cliente e nella rete locale per bloccare o limitare il traffico proveniente dal blocco IP gestito da Citrix.
- Implementare misure come sistemi di prevenzione delle intrusioni, firewall del software e motori di analisi comportamentale nella rete virtuale del cliente e nella rete locale, mirando al blocco IP gestito da Citrix.

#### Responsabilità del cliente nell'utilizzo della connettività SD-WAN

Quando la connettività SD-WAN è configurata, i clienti hanno la piena flessibilità di configurare le istanze SD-WAN virtuali utilizzate con Citrix DaaS in base ai loro requisiti di rete, ad eccezione di alcuni elementi necessari per garantire il corretto funzionamento della SD-WAN nella VNet gestita dal cliente. Le responsabilità del cliente includono:

- Progettazione e configurazione di regole di routing e firewall, incluse le regole per il DNS e il breakout del traffico Internet.
- Manutenzione della configurazione della rete SD-WAN.
- Monitoraggio dello stato operativo della rete.

- Implementazione tempestiva di aggiornamenti software o correzioni di sicurezza di Citrix SD-WAN. Poiché tutte le istanze di Citrix SD-WAN su una rete del cliente devono eseguire la stessa versione del software SD-WAN, le distribuzioni di versioni software aggiornate alle istanze SD-WAN di Citrix DaaS devono essere gestite dai clienti in base ai programmi e ai vincoli di manutenzione della rete.

Una configurazione errata delle regole di routing e firewall SD-WAN o una cattiva gestione delle password di gestione SD-WAN possono comportare rischi per la sicurezza sia per le risorse virtuali in Citrix DaaS, sia per le risorse locali raggiungibili attraverso i percorsi virtuali Citrix SD-WAN. Un altro possibile rischio per la sicurezza deriva dal mancato aggiornamento del software Citrix SD-WAN all'ultima versione di patch disponibile. Mentre SD-WAN Orchestrator e altri servizi Citrix Cloud forniscono i mezzi per affrontare tali rischi, i clienti sono in ultima analisi responsabili di garantire che le istanze SD-WAN virtuali siano configurate in modo appropriato.

#### Proxy

Il cliente può scegliere se utilizzare un proxy per il traffico in uscita dal VDA. Se viene utilizzato un proxy, il cliente è responsabile di quanto segue:

- Configurazione delle impostazioni proxy sull'immagine della macchina VDA o, se il VDA è aggiunto a un dominio, utilizzando Criteri di gruppo di Active Directory.
- Manutenzione e sicurezza del proxy.

Non è consentito utilizzare proxy con Citrix Cloud Connector o altre infrastrutture gestite da Citrix.

#### Resilienza del catalogo

Citrix offre tre tipi di cataloghi con diversi livelli di resilienza:

- **Statico:** ogni utente è assegnato a un singolo VDA. Questo tipo di catalogo non garantisce un'elevata disponibilità. Se il VDA di un utente non funziona, ne occorrerà uno nuovo per il ripristino. Azure offre un contratto di servizio del 99,5% per le macchine virtuali a istanza singola. Il cliente può comunque eseguire il backup del profilo utente, ma tutte le personalizzazioni apportate al VDA (ad esempio l'installazione di programmi o la configurazione di Windows) andranno perse.
- **Casuale:** ogni utente viene assegnato casualmente a un server VDA al momento dell'avvio. Questo tipo di catalogo offre un'elevata disponibilità grazie alla ridondanza. Se un VDA non funziona, nessuna informazione viene persa perché il profilo dell'utente risiede altrove.
- **Multisessione di Windows 10:** questo tipo di catalogo funziona allo stesso modo del tipo casuale ma utilizza VDA di workstation Windows 10 anziché VDA del server.

#### Backup per cataloghi aggiunti a un dominio

Se il cliente utilizza cataloghi aggiunti a un dominio con un peering VNet, è responsabile del backup dei propri profili utente. Citrix consiglia ai clienti di configurare le condivisioni di file locali e di impostare criteri sulla propria Active Directory o sui propri VDA per estrarre i profili utente da queste condivisioni di file. Il cliente è responsabile del backup e della disponibilità di queste condivisioni di file.

#### Disaster recovery

In caso di perdita di dati di Azure, Citrix recupererà quante più risorse possibili nella sottoscrizione Azure gestita da Citrix. Citrix tenterà di ripristinare i Cloud Connector e i VDA. Se Citrix non riesce a recuperare questi elementi, i clienti sono responsabili della creazione di un nuovo catalogo. Citrix presuppone che venga eseguito il backup delle immagini delle macchine e che i clienti abbiano eseguito il backup dei loro profili utente, consentendo la ricostruzione del catalogo.

In caso di perdita di un'intera area geografica di Azure, il cliente è responsabile della ricostruzione della propria rete virtuale gestita dal cliente in una nuova area geografica e della creazione di un nuovo peering VNet o di una nuova istanza SD-WAN all'interno di Citrix DaaS.

### Citrix e le responsabilità condivise con i clienti

#### Citrix Cloud Connector per cataloghi aggiunti a un dominio

Citrix DaaS implementa almeno due Cloud Connector in ogni posizione di risorse. Alcuni cataloghi possono condividere una posizione risorsa se si trovano nella stessa area geografica, nello stesso peering VNet e nello stesso dominio di altri cataloghi per lo stesso cliente. Citrix configura i Cloud Connector aggiunti a un dominio del cliente per le seguenti impostazioni di sicurezza predefinite nell'immagine:

- Aggiornamenti del sistema operativo e patch di sicurezza
- Software antivirus
- Aggiornamenti software di Cloud Connector

Normalmente i clienti non hanno accesso ai Cloud Connector. Tuttavia, possono acquisire l'accesso utilizzando la procedura di risoluzione dei problemi del catalogo e accedendo con le credenziali di dominio. Il cliente è responsabile di eventuali modifiche apportate al momento dell'accesso tramite il bastione.

I clienti hanno anche il controllo sui Cloud Connector aggiunti a un dominio tramite i Criteri di gruppo di Active Directory. Il cliente è responsabile di garantire che i criteri di gruppo applicabili a Cloud Connector siano sicuri e ragionevoli. Ad esempio, se il cliente sceglie di disabilitare gli aggiornamenti

del sistema operativo utilizzando Criteri di gruppo, è responsabile dell'esecuzione degli aggiornamenti del sistema operativo sui Cloud Connector. Il cliente può anche scegliere di utilizzare Criteri di gruppo per applicare una protezione più rigorosa rispetto alle impostazioni predefinite di Cloud Connector, ad esempio installando un software antivirus diverso. In generale, Citrix consiglia ai clienti di posizionare i Cloud Connector nella propria unità organizzativa di Active Directory senza criteri, in quanto ciò garantirà che le impostazioni predefinite utilizzate da Citrix possano essere applicate senza problemi.

### Risoluzione dei problemi

Nel caso in cui il cliente riscontri problemi con il catalogo in Citrix DaaS, ci sono due opzioni per la risoluzione dei problemi: utilizzare i bastioni e abilitare l'accesso RDP. Entrambe le opzioni comportano rischi per la sicurezza per il cliente. Il cliente deve comprendere questi rischi e acconsentirvi prima di utilizzare queste opzioni.

Citrix è responsabile dell'apertura e della chiusura delle porte necessarie per eseguire le operazioni di risoluzione dei problemi e della limitazione delle macchine a cui è possibile accedere durante queste operazioni.

Con i bastioni o l'accesso RDP, l'utente attivo che esegue l'operazione è responsabile della sicurezza delle macchine a cui viene effettuato l'accesso. Se il cliente accede a VDA o Cloud Connector tramite RDP e contrae accidentalmente un virus, la responsabilità è sua. Se il personale di supporto Citrix accede a queste macchine, ha la responsabilità di eseguire le operazioni in sicurezza. La responsabilità per eventuali vulnerabilità esposte da qualsiasi persona che accede al bastione o ad altre macchine nella distribuzione (ad esempio, la responsabilità del cliente di aggiungere intervalli di indirizzi IP per all'elenco di elementi consentiti, la responsabilità di Citrix di implementare correttamente gli intervalli di indirizzi IP) è trattata altrove in questo documento.

In entrambi gli scenari, Citrix è responsabile della corretta creazione di eccezioni firewall per consentire il traffico RDP. Citrix è inoltre responsabile della revoca di queste eccezioni dopo che il cliente ha eliminato il bastione o ha terminato l'accesso RDP tramite Citrix DaaS.

**Bastioni** Citrix può creare bastioni nella rete virtuale gestita da Citrix del cliente all'interno della sottoscrizione gestita da Citrix del cliente per diagnosticare e risolvere i problemi in modo proattivo (senza notificare il cliente) o in risposta a un problema sollevato dal cliente. Il bastione è una macchina a cui il cliente può accedere tramite RDP e quindi utilizzare per accedere ai VDA e (per i cataloghi aggiunti a un dominio) ai Cloud Connector tramite RDP per raccogliere registri, riavviare servizi o eseguire altre attività amministrative. Per impostazione predefinita, la creazione di un bastione apre una regola del firewall esterno per consentire il traffico RDP da un intervallo di indirizzi IP specificato dal cliente alla macchina bastione. Apre inoltre una regola firewall interna per consentire l'accesso ai

Cloud Connector e ai VDA tramite RDP. L'apertura di queste regole comporta un notevole rischio per la sicurezza.

Il cliente ha la responsabilità di fornire una password complessa utilizzata per l'account Windows locale. Il cliente ha inoltre la responsabilità di fornire un intervallo di indirizzi IP esterno che consente l'accesso RDP al bastione. Se il cliente sceglie di non fornire un intervallo di indirizzi IP (consentendo a chiunque di tentare l'accesso RDP), è responsabile di qualsiasi tentativo di accesso tentato da indirizzi IP dannosi.

Il cliente è inoltre responsabile dell'eliminazione del bastione al termine della risoluzione dei problemi. L'host del bastione espone una superficie di attacco aggiuntiva, quindi Citrix spegne automaticamente la macchina otto (8) ore dopo l'accensione. Tuttavia, Citrix non elimina mai automaticamente un bastione. Se il cliente sceglie di utilizzare il bastione per un lungo periodo di tempo, è responsabile dell'applicazione delle patch e dell'aggiornamento. Citrix consiglia di utilizzare un bastione solo per alcuni giorni prima di eliminarlo. Se il cliente desidera un bastione aggiornato, può eliminare quello attuale e quindi crearne uno nuovo, che fornirà una nuova macchina con le ultime patch di sicurezza.

**Accesso RDP** Per i cataloghi aggiunti a un dominio, se il peering VNet del cliente è funzionale, il cliente può abilitare l'accesso RDP dalla propria VNet con peering alla VNet gestita da Citrix. Se il cliente utilizza questa opzione, è responsabile dell'accesso ai VDA e ai Cloud Connector tramite il peering VNet. È possibile specificare intervalli di indirizzi IP di origine in modo che l'accesso RDP possa essere ulteriormente limitato, anche nell'ambito della rete interna del cliente. Il cliente dovrà utilizzare le credenziali di dominio per accedere a questi computer. Se il cliente sta collaborando con il supporto Citrix per risolvere un problema, potrebbe dover condividere queste credenziali con il personale di supporto. Dopo aver risolto il problema, il cliente è responsabile della disabilitazione dell'accesso RDP. Mantenere aperto l'accesso RDP dalla rete con peering o on-premise del cliente rappresenta un rischio per la sicurezza.

#### Credenziali di dominio

Se il cliente sceglie di utilizzare un catalogo aggiunto a un dominio, ha la responsabilità di fornire a Citrix DaaS un account di dominio (nome utente e password) con le autorizzazioni per aggiungere macchine al dominio. Quando fornisce le credenziali di dominio, il cliente è responsabile del rispetto dei seguenti principi di sicurezza:

- **Possibilità di verifica:** l'account deve essere creato appositamente per l'utilizzo di Citrix DaaS in modo che sia facile controllare per cosa viene utilizzato.
- **Limitazione dell'ambito:** l'account richiede solo le autorizzazioni per aggiungere macchine a un dominio. Non deve essere un amministratore di dominio completo.
- **Sicurezza:** è necessario proteggere l'account con una password complessa.

Citrix è responsabile dell'archiviazione sicura di questo account di dominio in un Azure Key Vault nella sottoscrizione di Azure gestita da Citrix del cliente. L'account viene recuperato solo se un'operazione richiede la password dell'account di dominio.

### Ulteriori informazioni

Per informazioni correlate, vedere:

- Guida alla distribuzione sicura della piattaforma Citrix Cloud: informazioni sulla sicurezza per la piattaforma Citrix Cloud.
- Panoramica tecnica sulla sicurezza: informazioni sulla sicurezza per Citrix DaaS.
- Notifiche di terze parti

## Metodi di consegna

October 6, 2022

Un singolo metodo di consegna probabilmente non soddisferà tutte le proprie esigenze.

Si possono prendere in considerazione diversi metodi di consegna delle applicazioni. La scelta del metodo appropriato consente di migliorare la scalabilità, la gestione e l'esperienza utente.

- **App installata:** l'applicazione fa parte dell'immagine desktop di base. Il processo di installazione comporta la copia di file dll, exe e di altro tipo nell'unità immagine, oltre a modifiche del Registro di sistema. Per ulteriori informazioni, vedere Creare cataloghi di macchine.
- **App in streaming (Microsoft App-V):** l'applicazione viene profilata e consegnata ai desktop mediante la rete su richiesta. I file dell'applicazione e le impostazioni del Registro di sistema vengono collocati in un contenitore sul desktop virtuale, isolati dal sistema operativo di base e tra loro. Questo intervento aiuta a risolvere i problemi di compatibilità. Per ulteriori informazioni, vedere App-V.
- **App a più livelli (Citrix App Layering):** ogni livello contiene una singola applicazione, un singolo agente o un singolo sistema operativo. Integrando un livello del sistema operativo, un unico livello di piattaforma (for esempio il VDA) e molti livelli applicativi, un amministratore può facilmente creare nuove immagini distribuibili. La stratificazione semplifica la manutenzione continua, poiché un sistema operativo, un agente e un'applicazione esistono in un unico livello. Quando si aggiorna il livello, tutte le immagini distribuite che contengono tale livello vengono aggiornate. Consultare Citrix App Layering.
- **App Windows ospitata:** applicazione installata su un host Citrix Virtual Apps multi-utente e distribuita come applicazione e non come desktop. Un utente accede all'app Windows ospitata

senza soluzione di continuità dal desktop o dal dispositivo endpoint VDI, nascondendo il fatto che l'app è in esecuzione in modalità remota. Per ulteriori informazioni, vedere Creare gruppi di consegna.

- **App locale:** applicazione distribuita sul dispositivo endpoint. L'interfaccia dell'applicazione viene visualizzata all'interno della sessione VDI ospitata dell'utente, anche se viene eseguita sull'endpoint. Per ulteriori informazioni, vedere Accesso alle app locali e reindirizzamento URL.

Per i desktop, si possono prendere in considerazione i desktop pubblicati da Citrix Virtual Apps o i desktop VDI.

### App e desktop pubblicati da Citrix Virtual Apps

Utilizzare computer con sistema operativo multisessione per distribuire Citrix Virtual Apps e desktop pubblicati.

**Caso d'uso:**

- Desiderate una distribuzione economica basata su server per ridurre al minimo i costi di distribuzione delle applicazioni a molti utenti, offrendo al contempo un'esperienza utente sicura e ad alta definizione.
- Gli utenti eseguono attività ben definite e non richiedono personalizzazione né accesso offline alle applicazioni. Gli utenti possono includere task worker, ad esempio operatori del call center e addetti al dettaglio, oppure utenti che condividono le workstation.
- Tipi di applicazione: qualsiasi applicazione.

**Vantaggi e considerazioni:**

- Soluzione gestibile e scalabile all'interno del data center.
- La soluzione più conveniente per la distribuzione delle applicazioni.
- Le applicazioni ospitate sono gestite centralmente e gli utenti non possono modificare l'applicazione, offrendo un'esperienza utente coerente, sicura e affidabile.
- Gli utenti devono essere online per accedere alle loro applicazioni.

**Esperienza utente:**

- L'utente richiede una o più applicazioni da StoreFront, dal menu Start o dall'URL che gli è stato fornito dall'amministratore.
- Le applicazioni vengono distribuite virtualmente e vengono visualizzate perfettamente in alta definizione sui dispositivi utente.
- A seconda delle impostazioni del profilo, le modifiche dell'utente vengono salvate al termine della sessione dell'applicazione dell'utente. Altrimenti, le modifiche vengono eliminate.

**Elaborare, ospitare e distribuire le applicazioni:**

- L'elaborazione delle applicazioni avviene su macchine di hosting, piuttosto che sui dispositivi dell'utente. La macchina di hosting può essere una macchina fisica o virtuale.
- Applicazioni e desktop risiedono su una macchina con sistema operativo multisessione.
- Le macchine si rendono disponibili attraverso i cataloghi di macchine.
- Le macchine dei cataloghi macchine sono organizzate in gruppi di consegna che forniscono lo stesso set di applicazioni a gruppi di utenti.
- Le macchine del sistema operativo multisessione supportano gruppi di consegna che ospitano desktop o applicazioni o entrambi.

**Gestione e assegnazione delle sessioni:**

- I sistemi operativi multisessione eseguono più sessioni su un'unica macchina per distribuire più applicazioni e desktop a più utenti connessi contemporaneamente. Ogni utente richiede una singola sessione da cui eseguire tutte le sue applicazioni ospitate.

  Ad esempio, un utente accede e richiede un'applicazione. Una sessione di quella macchina diventa non disponibile per gli altri utenti. Un secondo utente accede e richiede un'applicazione ospitata su quella macchina. Una seconda sessione attiva sulla stessa macchina ora non è disponibile. Se entrambi gli utenti richiedono più applicazioni, non sono necessarie sessioni aggiuntive perché un utente può eseguire più applicazioni utilizzando la stessa sessione. Se altri due utenti eseguono l'accesso richiedendo desktop e sono disponibili due sessioni su quella macchina, quella singola macchina ora utilizza quattro sessioni per ospitare quattro utenti diversi.

- All'interno del gruppo di consegna a cui è assegnato un utente, viene selezionata una macchina sul server meno caricato. Una macchina con disponibilità di sessione viene assegnata in modo casuale alla consegna di applicazioni a un utente quando questi esegue l'accesso.

### App ospitate nella VM

Utilizzare macchine del sistema operativo a sessione singola per distribuire applicazioni ospitate nella VM

**Caso d'uso:**

- Si desidera una soluzione di distribuzione delle applicazioni basata su client che sia sicura, che fornisca una gestione centralizzata e che supporti molti utenti per server host. Si desidera fornire a quegli utenti applicazioni che vengono visualizzate senza soluzione di continuità in alta definizione.
- Gli utenti sono collaboratori interni, esterni su contratto, di terze parti e altri membri del team provvisorio. Gli utenti non necessitano di accesso offline alle applicazioni ospitate.

- Tipi di applicazione: applicazioni che potrebbero non funzionare correttamente con altre applicazioni o potrebbero interagire con il sistema operativo, ad esempio Microsoft .NET Framework. Questi tipi di applicazioni sono ideali per l'hosting su macchine virtuali.

**Vantaggi e considerazioni:**

- Le applicazioni e i desktop dell'immagine sono gestiti, ospitati ed eseguiti in modo sicuro su macchine all'interno del data center, offrendo una soluzione di distribuzione delle applicazioni più conveniente.
- All'accesso, gli utenti possono essere assegnati casualmente a un computer all'interno di un gruppo di consegna configurato per ospitare la stessa applicazione. È inoltre possibile assegnare staticamente una singola macchina alla distribuzione di un'applicazione a un singolo utente ogni volta che l'utente esegue l'accesso. Le macchine assegnate staticamente consentono agli utenti di installare e gestire le proprie applicazioni nella macchina virtuale.
- L'esecuzione di più sessioni non è supportata sui computer con sistema operativo a sessione singola. Pertanto, ogni utente utilizza una singola macchina all'interno di un gruppo di consegna al momento dell'accesso e gli utenti devono essere online per accedere alle proprie applicazioni.
- Questo metodo può aumentare la quantità di risorse server per l'elaborazione delle applicazioni e aumentare la quantità di spazio di archiviazione per i vDisk personali degli utenti.

**Esperienza utente:**

- La stessa esperienza applicativa senza soluzione di continuità dell'hosting di applicazioni condivise su sistemi operativi multisessione.

**Elaborare, ospitare e distribuire le applicazioni:**

- Come nelle macchine con sistema operativo multi-sessione, tranne per il fatto che sono macchine con sistema operativo virtuale a sessione singola.

**Gestione e assegnazione delle sessioni:**

- Le macchine del sistema operativo a sessione singola eseguono una singola sessione desktop da una singola macchina. Quando si accede solo alle applicazioni, un solo utente può utilizzare più applicazioni (e non deve limitarsi a una singola applicazione). Il sistema operativo considera ogni applicazione una nuova sessione.
- All'interno di un gruppo di consegna, gli utenti che hanno effettuato l'accesso possono accedere a una macchina assegnata staticamente (ogni volta che l'utente accede allo stesso computer) o a una macchina assegnata in modo casuale selezionata in base alla disponibilità di sessioni.

### Desktop VDI

Utilizzaa le macchine del sistema operativo a sessione singola per distribuire i desktop VDI di Citrix Virtual Desktops.

I desktop VDI sono ospitati su macchine virtuali e forniscono a ciascun utente un sistema operativo desktop.

I desktop VDI richiedono più risorse rispetto ai desktop pubblicati di Citrix Virtual Apps, ma non richiedono che le applicazioni installate supportino sistemi operativi basati su server. Inoltre, a seconda del tipo di desktop VDI scelto, questi desktop possono essere assegnati a singoli utenti. Ciò consente agli utenti un alto livello di personalizzazione.

Quando si crea un catalogo di macchine per desktop VDI, si crea uno dei seguenti tipi di desktop:

- **Desktop casuale non persistente, noto anche come desktop VDI in pool:** ogni volta che un utente accede a uno di questi desktop, tale utente si connette a un desktop selezionato in un pool di desktop. Quel pool è basato su una singola immagine. Tutte le modifiche apportate al desktop vengono perse al riavvio del computer.
- **Desktop statico non persistente:** durante il primo accesso, a un utente viene assegnato un desktop tratto da un pool di desktop. Ogni macchina del pool è basata su una singola immagine. Dopo il primo utilizzo, ogni volta che un utente accede per utilizzare uno di quersti desktop, tale utente si connette allo stesso desktop assegnato al primo utilizzo. Tutte le modifiche apportate al desktop vengono perse al riavvio del computer.
- **Desktop statico persistente:** a differenza di altri tipi di desktop VDI, questi desktop possono essere personalizzati completamente dagli utenti. Durante il primo accesso, a un utente viene assegnato un desktop tratto da un pool di desktop. Gli accessi successivi di tale utente si connettono allo stesso desktop assegnato al primo utilizzo. Le modifiche apportate al desktop vengono mantenute al riavvio del computer.

### Accesso remoto al PC

Remote PC Access (Accesso remoto PC) è una funzionalità di Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) che consente alle organizzazioni di permettere facilmente ai dipendenti di accedere alle risorse aziendali da remoto in modo sicuro. La piattaforma Citrix rende possibile questo accesso sicuro offrendo agli utenti l'accesso ai PC fisici dell'ufficio. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Accesso remoto PC elimina la necessità di introdurre e fornire altri strumenti per il telelavoro. Ad esempio, desktop o applicazioni virtuali e la relativa infrastruttura associata.

Remote PC Access (Accesso remoto PC) utilizza gli stessi componenti Citrix DaaS che forniscono desktop e applicazioni virtuali. Di conseguenza, i requisiti e il processo di distribuzione e configurazione di Remote PC Access (Accesso remoto PC) sono gli stessi richiesti per la distribuzione di Citrix DaaS per

distribuire risorse virtuali. Questa uniformità offre un'esperienza amministrativa coerente e unificata. Gli utenti ricevono la migliore esperienza utente utilizzando Citrix HDX per offrire la propria sessione PC da ufficio.

Per ulteriori informazioni, vedere Accesso remoto al PC.

## Per iniziare: pianificare e creare una distribuzione

June 8, 2023

Se non si ha familiarità con i componenti, la terminologia e gli oggetti utilizzati con Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops), consultare Citrix DaaS.

Per la prospettiva di percorso dei clienti, andare al Citrix Success Center. Il Success Center fornisce una guida per le cinque fasi chiave del percorso Citrix: pianificare, costruire, implementare, gestire e ottimizzare.

- Le informazioni fornite nel Success Center sono un partner essenziale per questa documentazione prodotto.
- Gli articoli e le guide del Success Center offrono un'ampia prospettiva basata sulle soluzioni. Contengono inoltre collegamenti a dettagli specifici del servizio di questa documentazione prodotto.

Se si sta eseguendo la migrazione da una distribuzione di Citrix Virtual Apps and Desktops, vedere Migrazione al cloud.

> **Importante:**
>
> Per assicurarsi di ottenere importanti informazioni su Citrix Cloud e sui servizi Citrix a cui si è abbonati, assicurarsi di poter ricevere tutte le notifiche e-mail.
>
> Nell'angolo in alto a destra della console Citrix Cloud, espandere il menu a destra del nome del cliente e dei campi OrgID. Selezionare **Impostazioni account**. Nella scheda **Il mio profilo**, selezionare tutte le voci nella sezione **Notifiche tramite e-mail**.

### Come utilizzare questo articolo

Per configurare la distribuzione Citrix DaaS, completate le attività riassunte di seguito. Vengono forniti collegamenti ai dettagli di ogni attività.

Esaminare l'intero processo prima di iniziare la distribuzione, in modo da sapere cosa aspettarsi. In questo articolo si rimanda anche ad altre fonti di informazione utili.

> **Nota:**
>
> Se si prevede di utilizzare l'interfaccia Quick Deploy per eseguire il provisioning di macchine Microsoft Azure, seguire le istruzioni per l'installazione in Get started with Quick Deploy.

### Pianificare e preparare

Utilizzare le linee guida contenute in Plan nel Success Center per stabilire obiettivi, definire casi d'uso e obiettivi aziendali, identificare i rischi potenziali e creare un piano di progetto.

Nella documentazione di Citrix Tech Zone, vedere una guida proof of concept dettagliata di questo servizio.

### Iscrizione

Registrarsi per un account Citrix e richiedere una demo Citrix DaaS.

### Impostare un'ubicazione per le risorse

Una posizione risorsa contiene le risorse necessarie per distribuire applicazioni e desktop agli utenti. La creazione di posizioni risorsa consente a DaaS di utilizzare tali risorse. Per ulteriori informazioni sulle posizioni risorsa, vedere Connettersi a Citrix Cloud.

Prima di creare macchine, è necessario connettere una posizione risorsa a DaaS:

- Le macchine aggiunte al dominio richiedono l'installazione di Cloud Connector nella posizione risorsa. In questo caso, è possibile:
  - Creare cataloghi aggiunti ad Active Directory locali
  - Creare cataloghi aggiunti ad Azure Active Directory
  - Creare cataloghi aggiunti ad Azure Active Directory ibridi

  Per un'elevata disponibilità, consigliamo di installare due Cloud Connector in ciascuna posizione risorsa. Vedere Installazione di Cloud Connector.

  Ulteriori informazioni:

  - Quali sono le posizioni delle risorse e i connettori cloud?
  - Video sull'installazione dei Cloud Connector:

- Le macchine non aggiunte al dominio non richiedono Cloud Connector, ma richiedono che Rendezvous V2 sia abilitato. Il protocollo Rendezvous consente ai VDA di aggirare i Cloud Connector per connettersi direttamente e in modo sicuro a DaaS. Vedere Rendezvous V2. In questo caso, è possibile:
  - Creare cataloghi non aggiunti a un dominio

Se si utilizza l'interfaccia Quick Deploy per eseguire il provisioning delle macchine virtuali di Azure, Citrix crea la posizione delle risorse e i Cloud Connector.

### Creare una connessione alla posizione della risorsa

Dopo aver aggiunto una posizione risorsa e i Cloud Connector, creare una connessione alla posizione risorsa utilizzando l'interfaccia Full Configuration (Configurazione completa) di Citrix DaaS.

Questo passaggio non è necessario nei seguenti casi:

- Si sta realizzando una semplice implementazione proof of concept
- Si sta utilizzando l'interfaccia Quick Deploy per eseguire il provisioning delle macchine virtuali di Azure.

Ulteriori informazioni:

- Cosa sono gli host?
- Cosa sono le connessioni host?

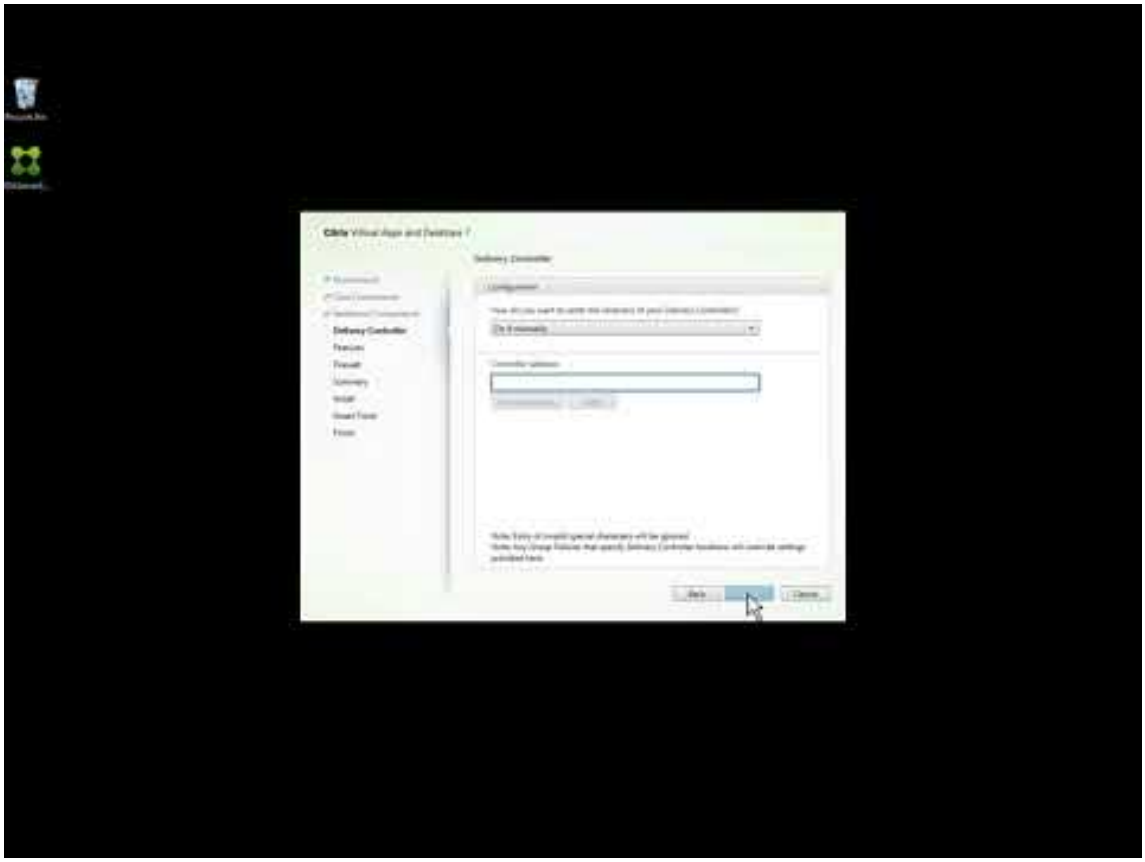
### Install VDAs

Ogni macchina che distribuisce applicazioni e desktop agli utenti deve disporre di un Citrix Virtual Delivery Agent (VDA) installato su di essa.

- Per una semplice installazione proof of concept, scaricare e installare un VDA su una macchina.
- Se si utilizza un'immagine per eseguire il provisioning di macchine virtuali, installare un VDA sull'immagine.
- Per una distribuzione di Accesso remoto al PC, installare la versione principale del VDA per sistema operativo a sessione singola su ogni PC fisico dell'ufficio.

Istruzioni e ulteriori informazioni:

- Cosa sono i VDA?
- Preparazione e istruzioni per l'installazione
- Installazione di VDA dalla riga di comando
- Video sul download e l'installazione di un VDA:



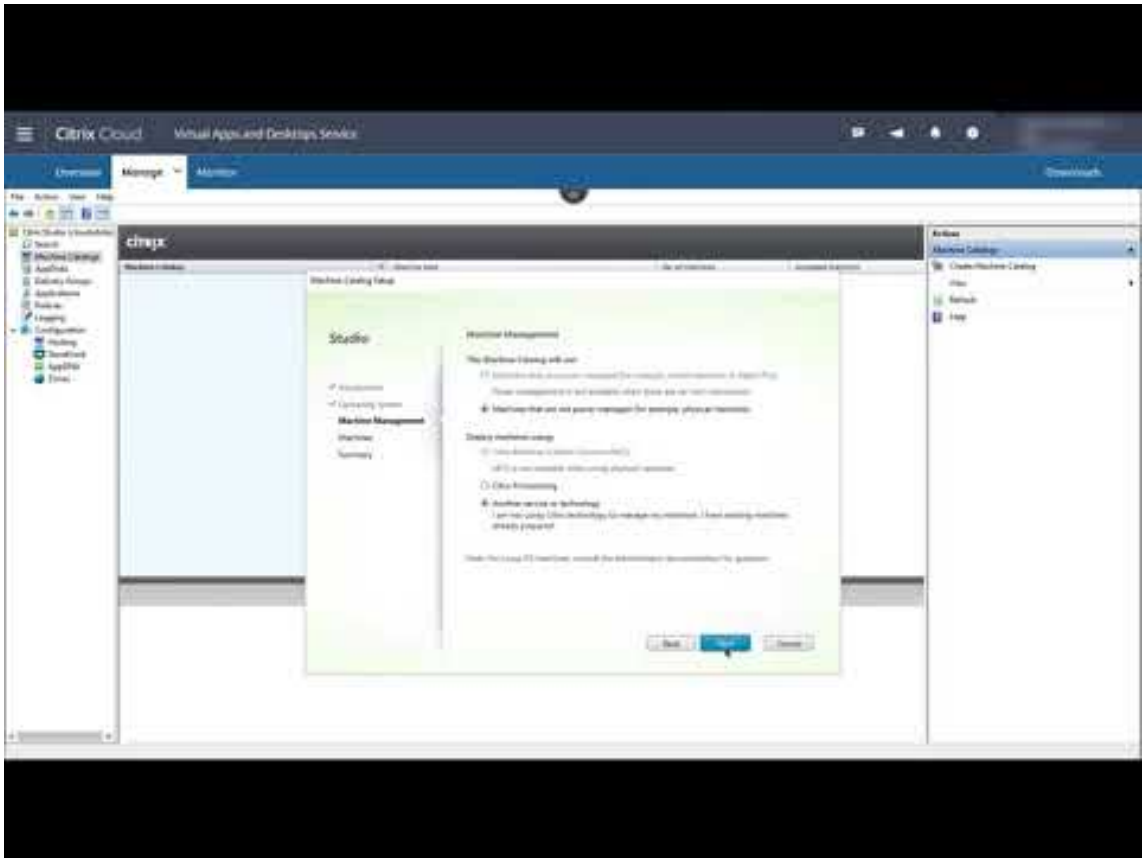
 

### Creare un catalogo

Dopo aver creato una connessione alla posizione della risorsa (se necessario), si crea un catalogo. Se si utilizza l'interfaccia Full Configuration (Configurazione completa), il flusso di lavoro guida automaticamente a questo passaggio.

Istruzioni e ulteriori informazioni:

- Cosa sono i cataloghi?
- Creare un catalogo
- Usare l'interfaccia Quick Deploy per distribuire un catalogo contenente macchine virtuali di Azure.
- Video sulla creazione di un catalogo utilizzando l'interfaccia di gestione della configurazione completa:




### Creare un gruppo di consegna

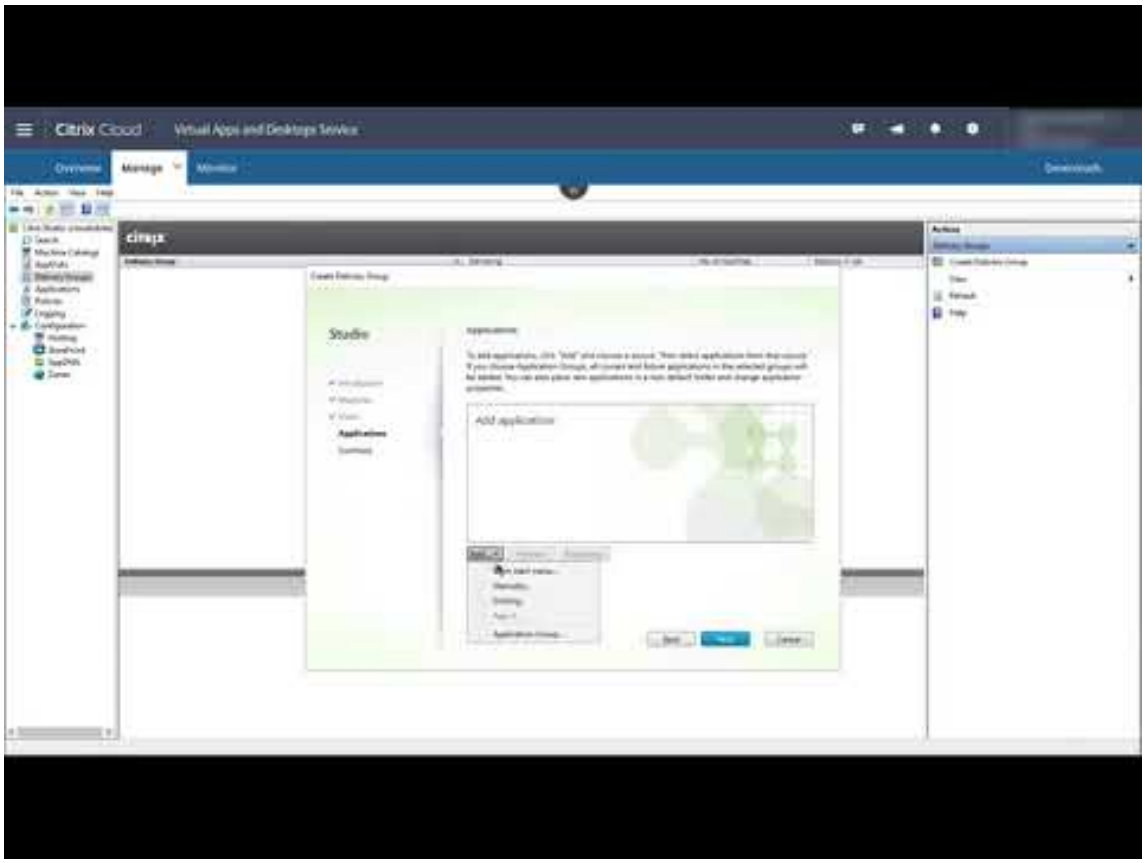
Dopo aver creato il primo catalogo, il flusso di lavoro **Manage** guida l'utente nella creazione di un gruppo di consegna.

Questo passaggio non è necessario quando si utilizza l'interfaccia Quick Deploy per eseguire il provisioning delle macchine virtuali di Azure.

Istruzioni e ulteriori informazioni:

- Cosa sono i gruppi di consegna?
- Creare un gruppo di consegna
- Video su come creare un gruppo di consegna:




### Implementare altri componenti e tecnologie

Dopo aver completato le attività di cui sopra per configurare la distribuzione di Citrix DaaS, seguire le indicazioni fornite nell'area Build del Citrix Success Center. Sono disponibili informazioni sul provisioning e la configurazione di altri componenti e tecnologie disponibili nella soluzione Citrix, ad esempio:

- Criteri Citrix
- StoreFront
- App Layering
- Servizio WEM (Workspace Environment Management)

- Servizio Citrix Gateway
- Zone
- Federated Authentication Service (FAS)

Completare altre attività pertinenti per la configurazione. Ad esempio, se si prevede di distribuire carichi di lavoro di Windows Server, configurare un server di licenze Microsoft RDS.

### Avviare applicazioni e desktop

Dopo che è stata configurata la distribuzione, la pubblicazione avviene automaticamente. Le applicazioni e i desktop configurati sono disponibili per gli utenti nel loro Citrix Workspace. Un utente accede semplicemente all'URL dell'area di lavoro e seleziona un'applicazione o un desktop, che si avvia immediatamente.

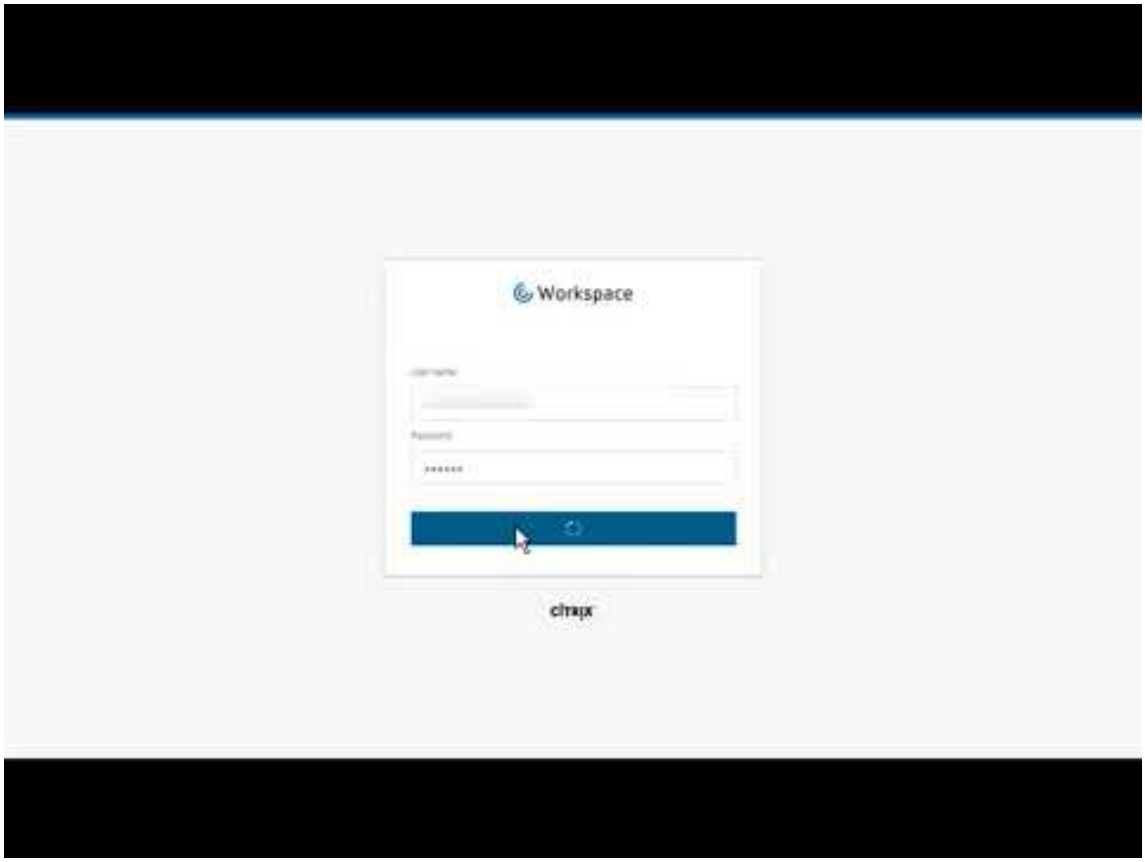
Inviare l'URL dell'area di lavoro ai propri utenti. L'URL dell'area di lavoro è reperibile in due posizioni:

- Dalla console di Citrix Cloud, selezionare **Workspace Configuration** (Configurazione dell'area di lavoro) dal menu nell'angolo in alto a sinistra. La scheda **Access** contiene l'URL di Workspace.
- Dalla pagina **Overview** (Panoramica) di Citrix DaaS, l'URL dell'area di lavoro viene visualizzato nella parte inferiore della pagina.

Ulteriori informazioni:

- Video di utenti che avviano applicazioni e desktop dal proprio Workspace:




### Ulteriori informazioni

La serie Citrix Cloud Learning offre corsi di formazione organizzati in base al percorso:

- Se non si conosce Citrix DaaS, consultare Nozioni di base del percorso di apprendimento di Citrix DaaS.
- Se si sta eseguendo la migrazione da una distribuzione Citrix Virtual Apps and Desktops, vedere Percorso di apprendimento per la migrazione da Citrix DaaS a Citrix Cloud.

## Iscriversi a Citrix DaaS

October 6, 2022

### Introduzione

È possibile abbonarsi a Citrix DaaS tramite Citrix o tramite Azure Marketplace.

Se si prevede di utilizzare Citrix Managed Azure, è anche possibile ordinare Citrix Azure Consumption Fund tramite Citrix o tramite Azure Marketplace.

- Quando si effettua l'ordine tramite Citrix, è possibile ordinare contemporaneamente Citrix DaaS e Citrix Azure Consumption Fund.
- Quando si effettua l'ordine tramite Azure Marketplace, ordinare prima Citrix DaaS. Quindi, è possibile effettuare un altro ordine per Citrix Azure Consumption Fund.

Se si ordina solo il servizio Citrix DaaS, è possibile ordinare Citrix Azure Consumption Fund in un secondo momento, tramite Azure Marketplace o il rappresentante dell'account Citrix.

### Demo e periodi di prova

È possibile valutare Citrix DaaS su richiesta tramite Citrix. Dopo un periodo di prova è possibile passare a un abbonamento al servizio a pagamento.

Durante un periodo di prova è possibile utilizzare facoltativamente una sottoscrizione di Citrix Managed Azure per cataloghi, immagini e connessioni di rete. Se si dispone di risorse gestite da Citrix al momento della conversione in un abbonamento a pagamento, è necessario acquistare i consumi o eliminare tali risorse gestite da Citrix. Se non si acquistano i consumi, tali risorse vengono eliminate automaticamente, il che potrebbe influire sugli utenti.

### Se si è attualmente abbonati a un servizio Citrix DaaS

In generale, un account Citrix Cloud consente di abbonarsi solo a uno dei servizi (o un'edizione) Citrix DaaS alla volta per ciascun Citrix OrgID. Ad esempio, è possibile abbonarsi a Citrix DaaS Premium edition OPPURE a Citrix DaaS per Azure, ma non entrambi.

Se attualmente si è abbonati a un servizio Citrix DaaS e si desidera abbonarsi a questo servizio, vi sono due possibilità:

- Abbonarsi a questo servizio utilizzando un altro account Citrix Cloud (OrgID).
- Ritirare il servizio Citrix DaaS già in uso e ordinare questo servizio. Per istruzioni sul ritiro, vedere CTX239027.

### Ordinare tramite Citrix

È possibile ordinare questo servizio (e Citrix Azure Consumption Fund) tramite Citrix Cloud o tramite il rappresentante dell'account Citrix.

Tramite Citrix Cloud:

- Seguire le indicazioni riportate in Abbonarsi a Citrix Cloud per ottenere un account Citrix Cloud e un ID organizzazione.
- È possibile richiedere una demo di Citrix DaaS. Nel riquadro Citrix DaaS, fare clic su **Request Demo** (Richiedi demo). Fornire le informazioni richieste.

  Un rappresentante Citrix si metterà in contatto per discutere le esigenze, l'ambiente e i piani. A seconda della valutazione del nostro rappresentante, si verrà autorizzati a partecipare a una demo per amministratori o a una prova Proof of Concept (PoC). Per ulteriori informazioni, vedere Versioni di prova del servizio Citrix Cloud.

Quando si è autorizzati per una versione di prova, il testo nel riquadro Citrix DaaS nella console Citrix Cloud viene modificato in **Manage** (Gestisci).

## Ordinare tramite Azure Marketplace

È possibile ordinare i seguenti prodotti Citrix tramite Azure Marketplace:

- Citrix DaaS per Azure
- Citrix DaaS Advanced edition
- Citrix DaaS Premium edition
- Workspace Premium Plus

Se si prevede di ospitare i carichi di lavoro Citrix Virtual Apps and Desktops in Microsoft Azure e si desidera utilizzare una sottoscrizione a Citrix Managed Azure, ordinare Citrix Azure Consumption Fund dopo aver ordinato Citrix DaaS o Workspace Premium Plus.

Con Citrix Azure Consumption Fund viene addebitato il consumo ogni mese, che può variare a seconda delle risorse di hosting scelte e delle ore di utilizzo. È possibile controllare l'utilizzo del consumo tramite Citrix Cloud.

Da Azure Marketplace:

- Non è possibile combinare Citrix DaaS e un fondo di consumo in un unico ordine.
- Il processo di ordinazione per Citrix Azure Consumption Fund è essenzialmente lo stesso dell'ordinazione di Citrix DaaS, ma è necessario aver precedentemente ordinato Citrix DaaS.

### Requisiti per ordinare tramite Azure Marketplace

- L'OrgID del tuo account Citrix Cloud.
  - Se si dispone di un account Citrix Cloud, ma non si conosce l'OrgID, guardare nell'angolo in alto a destra della console Citrix Cloud. Oppure, controllare l'e-mail ricevuta quando è stato creato l'account.

  - Se non si dispone di un account Citrix Cloud, seguire le indicazioni riportate in Abbonarsi a Citrix Cloud.

- Un account di Azure e almeno una sottoscrizione di Azure in tale account.

#### Procedura per ordinare tramite Azure Marketplace

Seguire questa procedura per ordinare Citrix DaaS o Workspace Premium Plus tramite Azure Marketplace (se si desidera utilizzare Citrix Managed Azure, effettuare un altro ordine per Citrix Azure Consumption Fund dopo aver ordinato Citrix DaaS).

1. Accedere ad Azure Marketplace utilizzando le credenziali dell'account Azure.
2. Cercare il prodotto Citrix che si desidera ordinare e selezionarlo.
3. Selezionare **Get it now** (Ottieni ora).
4. Nel messaggio **One more thing** (Ancora una cosa), inserire le informazioni richieste, abilitare la casella di controllo per il consenso e quindi selezionare **Continue** (Continua).
5. Consultare le schede contenenti informazioni sul prodotto, i piani, i prezzi e l'utilizzo. Quando si è pronti, selezionare un piano (se ne sono disponibili più di uno), quindi selezionare **Set up + subscribe** (Configura + abbonati).
6. Nella scheda **Basics** (Elementi di base):
   - **Subscription** (Abbonamento): indica il piano selezionato.
   - **Resource group** (Gruppo di risorse): selezionare o creare un gruppo di risorse.
   - **Name** (Nome): inserire un nome per l'ordine di abbonamento in modo da poterlo identificare facilmente in un secondo momento.
   - Le informazioni su **Plan** (Piano) mostrano il prezzo per il piano selezionato, in base al periodo di fatturazione. Per modificare la durata del piano, selezionare **Change plan** (Modifica piano). Selezionare la durata desiderata e selezionare **Change plan**(Modifica piano).
7. Nella scheda **Review + subscribe** (Esamina + abbonati), esaminare le informazioni di contatto e aggiornarle, se necessario. Esaminare le informazioni di base sull'abbonamento. Selezionare **Subscribe** (Abbonati).
8. Nella pagina **Subscription in progress** (Abbonamento in corso), selezionare **Configure account now** (Configura account ora) (se il pulsante è disabilitato, attendere qualche istante). Si viene reindirizzati a una pagina di attivazione di Citrix.
9. Nella pagina di attivazione:
   - Utilizzare il link **Sign in** (Accedi) per accedere a Citrix Cloud. Se l'accesso riesce, viene compilato automaticamente il campo **Organization ID** (ID organizzazione).

- **Quantity** (Quantità): immettere il numero di utenti (un ordine iniziale deve essere di almeno 25). Viene visualizzato un prezzo stimato.
- Accettare i termini e le condizioni, quindi selezionare **Activate Order** (Attiva ordine).

#### Dopo aver ordinato tramite Azure Marketplace

Citrix invia un'e-mail quando viene eseguito il provisioning del servizio. Il provisioning può richiedere un po'di tempo. Se non si riceve l'e-mail entro il giorno successivo, contattare il supporto Citrix. Quando si riceve l'e-mail da Citrix, è possibile iniziare a utilizzare Citrix DaaS.

L'evasione di un ordine Citrix Azure Consumption Fund non richiede molto tempo. Quando Citrix riceve una notifica dell'ordine, viene visualizzato un banner nella console di Citrix DaaS, che indica che verrà preparata una sottoscrizione di Citrix Managed Azure.

Non eliminare la risorsa Citrix DaaS in Azure. L'eliminazione di tale risorsa annulla l'abbonamento.

### Ordinare tramite Google Cloud Marketplace

È possibile ordinare i seguenti prodotti Citrix tramite Google Cloud Marketplace:

- Citrix DaaS Standard per Google Cloud
- Citrix DaaS Premium per Google Cloud

Per ordinare tramite Google Cloud Marketplace, è necessario quanto segue:

- L'OrgID del tuo account Citrix Cloud.
  - Se si dispone di un account Citrix Cloud, ma non si conosce l'OrgID, guardare nell'angolo in alto a destra della console Citrix Cloud. Oppure, controllare l'e-mail ricevuta quando è stato creato l'account.
  - Se non si dispone di un account Citrix Cloud, seguire le indicazioni riportate in Abbonarsi a Citrix Cloud.
- Un account Google Cloud e almeno una sottoscrizione Google Cloud in quell'account.

Per effettuare l'ordine:

1. Accedere a Google Cloud Marketplace
2. Seguire le istruzioni sulla pagina Citrix DaaS per Google Cloud per effettuare l'acquisto.

Citrix invia un'e-mail quando viene eseguito il provisioning del servizio. Il provisioning può richiedere un po'di tempo. Se non si riceve l'e-mail entro il giorno successivo, contattare il supporto Citrix. Quando si riceve l'e-mail da Citrix, è possibile iniziare a utilizzare Citrix DaaS.

Non eliminare la risorsa Citrix DaaS in Google Cloud. L'eliminazione di tale risorsa annulla l'abbonamento.

### Passaggi successivi

Dopo aver evaso l'ordine, continuare con i passaggi successivi in Plan and build a deployment (Pianifica e crea una distribuzione).

Ad esempio:

- Se l'hypervisor o il servizio cloud o Active Directory non sono già stati configurati, consultare Configurare una posizione per le risorse.
- Se l'ambiente host e Active Directory sono già configurati, vedere Creare una connessione.

## Citrix HDX Plus per Windows 365

November 9, 2022

Citrix HDX Plus per Windows 365 consente di integrare Citrix Cloud con Windows 365 per utilizzare le tecnologie Citrix HDX per un'esperienza Windows 365 Cloud PC migliorata e più sicura in aggiunta ad altri servizi Citrix Cloud per una migliore gestibilità.

Per ulteriori informazioni, vedere Citrix HDX Plus per Windows 365

## Citrix DaaS per Google Cloud

November 16, 2022

Citrix DaaS per Google Cloud consente di distribuire desktop e app Google Cloud utilizzando l'interfaccia di gestione Full Configuration (Configurazione completa) di Citrix DaaS. Citrix DaaS per Google Cloud è disponibile nelle edizioni Standard e Premium.

Per informazioni sulle funzionalità supportate, consultare la matrice delle funzionalità di Citrix Virtual Apps and Desktops.

È possibile ordinare Citrix DaaS per Google Cloud da Google Cloud Marketplace.

Dopo aver ordinato Citrix DaaS, accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).

Seguire le istruzioni per la configurazione in questa documentazione del prodotto. Utilizzando l'interfaccia Full Configuration (Configurazione completa), è possibile creare connessioni, cataloghi e gruppi di consegna, proprio come si farebbe quando si utilizza tale interfaccia con altre edizioni del prodotto (queste edizioni attualmente non dispongono di un'interfaccia di gestione Quick Deploy).

Alcuni display nell'interfaccia Full Configuration (Configurazione completa) potrebbero differire da quelli della documentazione. Ad esempio, quando si crea una connessione in un'edizione Citrix Virtual Apps and Desktops per Google Cloud, i tipi di connessione disponibili includono gli hypervisor supportati e Google Cloud. Non sono disponibili altri servizi cloud.

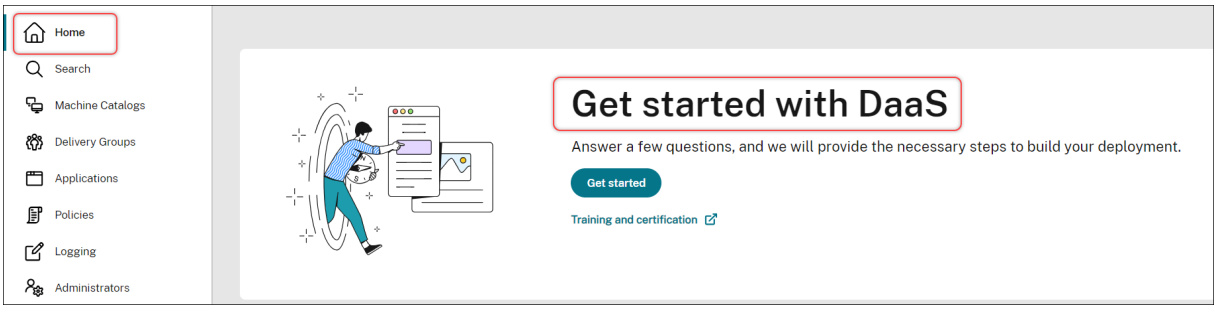
Allo stesso modo, utilizzare le informazioni contenute nella documentazione del prodotto che si applicano agli hypervisor supportati e a Google Cloud.

Per istruzioni dettagliate sull'implementazione e la configurazione di Citrix DaaS su Google Cloud, consultare questo articolo di Citrix Tech Zone: Virtualizzazione Citrix su Google Cloud. Questo articolo tratta la definizione dell'architettura di distribuzione, la preparazione del progetto Google Cloud, la configurazione dei servizi di rete e la distribuzione di Active Directory.

## Utilizzare la guida introduttiva di DaaS (anteprima)

December 5, 2023

La guida introduttiva di DaaS snellisce e semplifica il processo di distribuzione di DaaS sia per gli amministratori nuovi che per quelli esperti. Utilizzando la guida, è possibile configurare rapidamente le distribuzioni DaaS rispondendo a una serie di domande.




Questo articolo illustra i processi di configurazione di cinque scenari tipici di distribuzione con DaaS.

### Vantaggi

I vantaggi dell'uso di questa guida includono:

- **Iniziare è facile**. Questa guida collega i passaggi essenziali della distribuzione tramite un flusso di lavoro dettagliato basato su questionari. Un nuovo amministratore può configurare rapidamente la sua distribuzione mentre impara concetti e terminologia grazie alla guida contestuale.
- **Semplificare le configurazioni complesse.** Questa guida fornisce impostazioni preconfigurate dove occorre e dà l'accesso all'interfaccia utente Full Configuration per le configurazioni

avanzate. Un amministratore esperto può utilizzare la guida come punto di partenza per le configurazioni complesse.

### Scenari di distribuzione supportati

Questa guida fornisce distribuzioni rapide per questi scenari:

| Cosa consegnare? | Le macchine esistono già? | Tipo di macchina | Osservazione |
|---|---|---|---|
| App e desktop virtuali | No | Macchine virtuali (con provisioning da parte di DaaS) | Alimentazione gestita |
| App e desktop virtuali | Sì | Macchine virtuali o PC blade | Alimentazione gestita |
| App e desktop virtuali | Sì | Macchine fisiche o virtuali | Alimentazione non gestita |
| PC da ufficio | Sì | Macchine fisiche | Alimentazione gestita |
| PC da ufficio | Sì | Macchine fisiche | Alimentazione non gestita |

Per istruzioni dettagliate, vedere le seguenti sezioni:

- Distribuire app e desktop da zero (con alimentazione gestita)
- Distribuire le app e i desktop utilizzando macchine esistenti (con alimentazione gestita)
- Distribuire le app e i desktop utilizzando macchine esistenti (con alimentazione non gestita)
- Distribuire PC da ufficio (con alimentazione gestita)
- Consegnare PC da ufficio (con alimentazione non gestita)

### Terminologia

I seguenti sono termini specifici di DaaS:

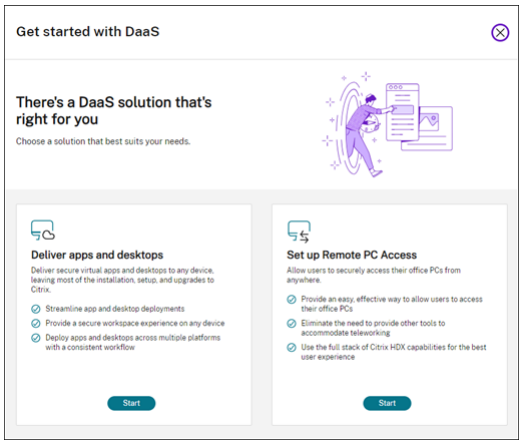
- **Resource location (Posizione risorsa).** Contiene le risorse necessarie per distribuire app e desktop agli utenti.
- **Host connection (Connessione host).** Connette DaaS a un host (hypervisor o servizio cloud) in una posizione risorsa. La creazione di connessioni host è necessaria per creare e gestire macchine sugli host o per gestire l'alimentazione delle macchine esistenti.
- **Master image (Immagine master).** Funge da modello per replicare le macchine virtuali sull'host. Include il sistema operativo, le applicazioni, il Virtual Delivery Agent (VDA) e altro software.

- **Machine Catalog (Catalogo di macchine)**. Raccolta di macchine identiche. Possono essere virtuali o fisiche a seconda delle esigenze. È possibile creare un catalogo di macchine per creare macchine configurate in modo identico su un host o importare macchine in DaaS per la gestione.
- **Delivery group (Gruppo di consegna).** Contiene le macchine dei cataloghi di macchine. Inoltre, specifica quali utenti possono utilizzare tali macchine e quali applicazioni e desktop sono disponibili per tali utenti.
- **Machine Profile (Profilo macchina).** Specifica le proprietà delle macchine virtuali. Le macchine virtuali di un catalogo possono ereditare le proprietà da un profilo macchina.

## Accedere alla guida

1. Andare alla pagina **DaaS > Home**.
2. Localizzare **Get started with DaaS** (Inizia a usare DaaS).
3. Fare clic su **Get Started** (Inizia) per avviare il processo di distribuzione.




> **Nota:**
>
> È possibile uscire dal processo in qualsiasi momento facendo clic su **Close** (Chiudi) e la guida salva automaticamente le impostazioni. Per continuare la configurazione, fare clic su **Continue** (Continua). Per ricominciare da capo, fare clic su **Start over** (Ricomincia).

## Distribuire app e desktop da zero (con alimentazione gestita)

Questa sezione guida l'utente nel processo di distribuzione riguardante la creazione di macchine virtuali e la distribuzione di app e desktop che le utilizzano.

### Prerequisiti

Prima di iniziare, sono necessari gli elementi seguenti:

- Connettività da Citrix Cloud al provider di identità di destinazione

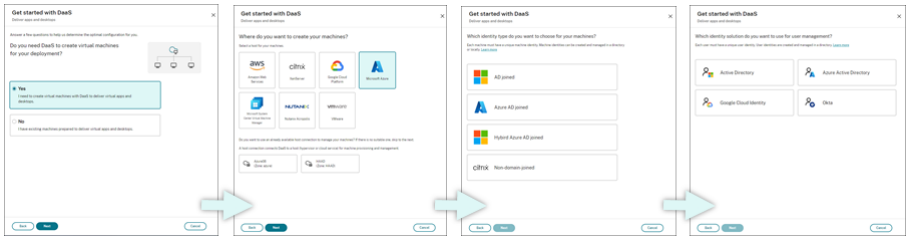
  Per ulteriori informazioni, vedere la sezione corrispondente in [Provider di identità](/en-us/citrix-cloud/citrix-cloud-management/identity-access-management#identity-providers.

- Ruolo: Full Administrator (Amministratore completo) o Cloud Administrator (Amministratore del cloud)
- Autorizzazioni richieste sull'hypervisor o sul servizio cloud di destinazione.

  Per ulteriori informazioni, vedere le sezioni corrispondenti in Creare e gestire le connessioni
- Credenziali di amministratore per la creazione di account per VM

### Preparazione

Rispondere alle domande sullo schermo per completare le seguenti impostazioni a livello di infrastruttura. Per ulteriori informazioni, vedere la tabella seguente.



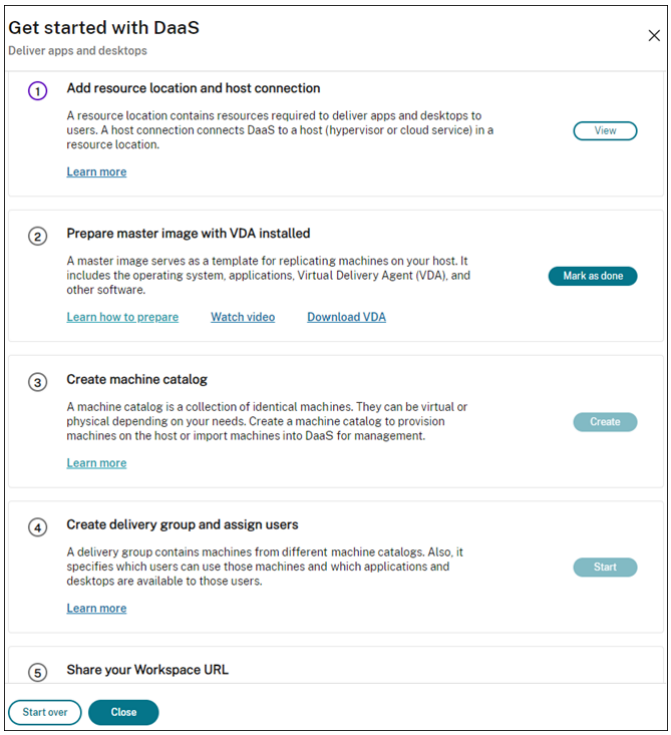
| # | Impostazione | Descrizione |
|---|---|---|
| 1 | Specificare se è necessaria la creazione di VM | Selezionare **Yes**. |
| 2 | Selezionare il tipo di host | Selezionare un tipo di host per la distribuzione.<br>Opzioni: AWS, XenServer (precedentemente Citrix Hypervisor), Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis e VMware |
| 3 | Selezionare il tipo di identità della macchina | Selezionare un tipo di identità per la gestione della macchina. |

| # | Impostazione | Descrizione |
|---|---|---|
| 4 | Selezionare il tipo di identità dell'utente | Opzioni: aggiunta ad AD, aggiunta ad Azure AD, aggiunta ad Azure AD ibrido e non aggiunta a dominio<br>Selezionare un tipo di identità per la gestione degli utenti.<br>Opzioni: Active Directory, Azure Active Directory, Google Cloud Identity e Okta |

### Procedura di distribuzione

Dopo aver completato le impostazioni a livello di infrastruttura, i passaggi specifici di questo scenario di distribuzione vengono visualizzati come segue.




Seguire le istruzioni sullo schermo per completare le impostazioni.

**Passaggio 1: aggiungere una posizione risorsa e le connessioni host** Configurare la posizione risorsa installando i Cloud Connector e configurare le connessioni agli hypervisor o ai servizi cloud presenti nella posizione.

1. Assegnare un nome alla posizione risorsa.
2. Scaricare e installare i Cloud Connector su almeno due macchine Windows Server.
3. Rilevare i Cloud Connector installati.
4. Aggiungere e configurare le connessioni host per la posizione risorsa. Le impostazioni dettagliate di una connessione includono:
   - Dettagli di connessione, come indirizzo di connessione, nome utente e password.
   - Risorse di archiviazione
   - Risorse di rete

   > **Nota:**
   >
   > DaaS crea e gestisce le VM sugli host tramite tali connessioni. È necessario specificare le connessioni quando si creano cataloghi di macchine.

**Passaggio 2: preparare le immagini master per le macchine** Preparare le immagini master sulle macchine virtuali nella posizione risorsa. Per ulteriori informazioni, vedere Preparare un'immagine master sull'hypervisor o sul servizio cloud.

**Passaggio 3: creare un catalogo di macchine** Creare un catalogo di macchine per creare un gruppo di macchine configurate in modo identico su un host. I passaggi dettagliati sono i seguenti:

1. Assegnare un nome al catalogo.
2. Selezionare il tipo di macchina.

   Opzioni: multisessione, statica a sessione singola (desktop personali) e casuale a sessione singola (desktop in pool).
3. Selezionare una connessione host.

   Le opzioni provengono da tutte le connessioni host configurate per le posizioni risorsa nel Passaggio 1.
4. Selezionare un'immagine master.
5. Selezionare un profilo macchina.

   > **Nota:**
   >
   > Il supporto dei profili macchina è attualmente disponibile per i servizi cloud Azure, GCP e AWS e l'uso del profilo macchina è facoltativo per GCP.

6. Impostare quante macchine si desidera creare.

7. Impostare le identità delle macchine.

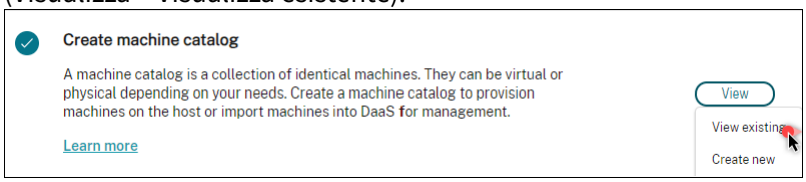
   Per impostazione predefinita, viene visualizzato il tipo di identità della macchina selezionato nella fase di preparazione. Fornire le impostazioni di identità richieste per le macchine virtuali, quali dominio, unità organizzativa e schema di denominazione.

8. Inserire le credenziali di amministratore richieste per la creazione della macchina.

9. Fare clic su **Create**.

   > **Suggerimento:**
   >
   > Il pulsante **Create** (Crea) è disponibile solo dopo che sono state fornite tutte le impostazioni richieste.

   Per visualizzare l'avanzamento della creazione del catalogo, selezionare **View > View existing** (Visualizza > Visualizza esistente).




### Passaggio 4: Creare gruppi di consegna e assegnare utenti

> **Suggerimento:**
>
> Prima di creare i gruppi di consegna, visualizzare i cataloghi esistenti per assicurarsi che almeno un catalogo sia stato creato correttamente. Altrimenti, non sarà possibile creare i gruppi di consegna.

La creazione di un gruppo di consegna include le seguenti sottoattività:

- Aggiungere macchine virtuali al gruppo
- Assegnare utenti al gruppo
- Specificare quali app e desktop rendere disponibili agli utenti assegnati

1. Assegnare un nome al gruppo.
2. Aggiungere macchine al gruppo selezionando un catalogo di macchine e specificando quante macchine virtuali sono disponibili per il gruppo.
3. Specificare le applicazioni e i desktop disponibili per questo gruppo:

   - Per aggiungere applicazioni da una macchina in esecuzione inclusa nel catalogo selezionato, fare clic su **Add new > From start menu**Aggiungi nuova > Dal menu Start.
   - Per aggiungere applicazioni distribuite su condivisioni di rete, fare clic su **Add new > Manually**(Aggiungi nuova > Manualmente), quindi inserire le impostazioni richieste quali percorso, directory di lavoro e altro.

- (Visibile solo con macchine con sistema operativo multisessione) Per la distribuzione di desktop, mantenere selezionata l'opzione **Enable desktop delivery** (Abilita distribuzione desktop).

4. Aggiungere gli utenti che possono accedere alle app e ai desktop di questo gruppo.

**Passaggio 5: condividere l'URL di Workspace con gli utenti** In Workspace, passare a **Configuration > Access** (Configurazione > Accesso), quindi condividere l'URL di Workspace con gli utenti

## Distribuire le app e i desktop utilizzando macchine esistenti (con alimentazione gestita)

Questa sezione guida l'utente nel processo di distribuzione di app e desktop utilizzando macchine esistenti (con alimentazione gestita).

### Prerequisiti

Prima di iniziare, sono necessari gli elementi seguenti:

- Connettività da Citrix Cloud al provider di identità di destinazione

  Per ulteriori informazioni, vedere la sezione corrispondente in Identity providers (Provider di identità).

- Ruolo: Full Administrator (Amministratore completo) o Cloud Administrator (Amministratore del cloud)

### Preparazione

Rispondere alle domande sullo schermo per completare le seguenti impostazioni a livello di infrastruttura.

| # | Impostazione | Descrizione |
|---|---|---|
| 1 | Specificare se è necessaria la creazione di VM | Selezionare **No**. |

| # | Impostazione | Descrizione |
|---|---|---|
| 2 | Selezionare se è richiesta la gestione dell'alimentazione | Selezionare **Machines that are power managed (for example, virtual machines or blade PCs)** [Macchine con alimentazione gestita (ad esempio, macchine virtuali o PC blade)]. |
| 3 | Selezionare la piattaforma host | Selezionare la piattaforma host in cui risiedono le macchine esistenti.<br>Opzioni: AWS, Citrix, Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis e VMware |
| 4 | Selezionare il tipo di identità dell'utente | Selezionare un tipo di identità per la gestione degli utenti.<br>Opzioni: Active Directory, Azure Active Directory, Google Cloud Identity e Okta |

**Procedura di distribuzione**

Dopo che sono state completate le impostazioni a livello di infrastruttura, vengono visualizzati i passaggi specifici per questo scenario di distribuzione. Seguire le istruzioni sullo schermo per completare le impostazioni.

**Passaggio 1: aggiungere una posizione risorsa e le connessioni host** Configurare la posizione delle risorse installando i Cloud Connector e configurare le connessioni agli hypervisor o ai servizi cloud nella propria posizione.

1. Assegnare un nome alla posizione risorsa.
2. Scaricare e installare i Cloud Connector su almeno due macchine Windows Server.
3. Rilevare i Cloud Connector installati.
4. Aggiungere e configurare le connessioni host per la posizione risorsa. Esempi di impostazioni di connessione sono l'indirizzo di connessione, il nome utente e la password.

> **Nota:**
>
> DaaS gestisce l'alimentazione delle macchine nelle posizioni risorsa tramite le connessioni. È necessario specificare una connessione quando si importano le macchine in un catalogo.

**Passaggio 2: Creare cataloghi di macchine** Creare un catalogo di macchine e importare le proprie macchine in esso.

1. Assegnare un nome al catalogo
2. Selezionare il tipo di macchina.

   Opzioni: multisessione, statica a sessione singola (desktop personali) e casuale a sessione singola (desktop in pool).
3. Selezionare una posizione risorsa.
4. Importare delle macchine nel catalogo.
   Le macchine sono organizzate per connessione host. Scegliere una connessione host per importare le macchine associate.
5. Fare clic su **Create**.

**Passaggio 3: Creare gruppi di consegna e assegnare utenti** Per creare un gruppo di consegna, è necessario:

- Aggiungere macchine virtuali al gruppo
- Assegnare utenti al gruppo
- Specificare quali app e desktop rendere disponibili agli utenti assegnati

1. Assegnare un nome al gruppo.
2. Selezionare un catalogo di macchine in base alle esigenze, quindi specificare quante macchine sono disponibili per il gruppo di consegna.
3. Specificare le applicazioni e i desktop disponibili per questo gruppo:
   - Per aggiungere applicazioni da una macchina in esecuzione inclusa nel catalogo selezionato, fare clic su **Add new > From start menu**Aggiungi nuova > Dal menu Start.
   - Per aggiungere applicazioni distribuite su condivisioni di rete, fare clic su **Add new > Manually**(Aggiungi nuova > Manualmente), quindi inserire le impostazioni richieste quali percorso, directory di lavoro e altro.
   - (Visibile solo con macchine con sistema operativo multisessione) Per la distribuzione di desktop, mantenere selezionata l'opzione **Enable desktop delivery** (Abilita distribuzione desktop).
4. Aggiungere utenti al gruppo.

**Passaggio 4: condividere l'URL dell'area di lavoro con i propri utenti** Passare a **Workspace Configuration > Access** (Configurazione di Workspace > Accesso), quindi condividere l'URL di Workspace con gli utenti.

## Distribuire le app e i desktop utilizzando macchine esistenti (con alimentazione non gestita)

Questa sezione guida l'utente nel processo di distribuzione di app e desktop utilizzando macchine esistenti (con alimentazione non gestita).

### Prerequisiti

Prima di iniziare, sono necessari gli elementi seguenti:

- Connettività da Citrix Cloud al provider di identità di destinazione

  Per ulteriori informazioni, vedere la sezione corrispondente in Provider di identità
- Ruolo: Full Administrator (Amministratore completo) o Cloud Administrator (Amministratore del cloud)

### Preparazione

Rispondere alle domande sullo schermo per completare le seguenti impostazioni a livello di infrastruttura.

| # | Impostazione | Descrizione |
|---|---|---|
| 1 | Specificare se è necessaria la creazione di VM | Selezionare **No**. |
| 2 | Selezionare se è richiesta la gestione dell'alimentazione | Selezionare **Machines that are not power managed (for example, physical machines)** [Macchine con alimentazione non gestita (ad esempio, macchine fisiche)]. |
| 3 | Selezionare il tipo di identità dell'utente | Selezionare un tipo di identità per la gestione degli utenti. Opzioni: Active Directory, Azure Active Directory, Google Cloud Identity e Okta |

**Procedura di distribuzione**

Dopo che sono state completate le impostazioni a livello di infrastruttura, vengono visualizzati i passaggi specifici per questo scenario di distribuzione. Seguire le istruzioni sullo schermo per completare le impostazioni.

**Passaggio 1: Aggiungere una posizione risorsa** Configurare la posizione risorsa installando i Cloud Connector.

1. Assegnare un nome alla posizione risorsa.
2. Scaricare e installare i Cloud Connector su almeno due macchine Windows Server.
3. Rilevare i Cloud Connector installati.

> **Nota:**
>
> La creazione di connessioni host è necessaria solo se si desidera gestire l'alimentazione delle macchine esistenti.

**Passaggio 2: Creare un catalogo macchine** Creare un catalogo di macchine e importare le proprie macchine in esso.

1. Assegnare un nome al catalogo
2. Selezionare il tipo di macchina.

   Opzioni: multisessione, statica a sessione singola (desktop personali) e casuale a sessione singola (desktop in pool).
3. Selezionare una posizione risorsa.
4. Importare delle macchine nel catalogo.

   Per facilitare la ricerca automatica, utilizzare i nomi parziali dei computer e la selezione delle directory.
5. Fare clic su **Create**.

**Passaggio 3: Creare gruppi di consegna e assegnare utenti** Per creare un gruppo di consegna, è necessario:

- Aggiungere macchine virtuali al gruppo
- Assegnare utenti al gruppo
- Specificare quali app e desktop rendere disponibili agli utenti assegnati

1. Assegnare un nome al gruppo.

2. Selezionare un catalogo di macchine in base alle esigenze, quindi specificare quante macchine sono disponibili per il gruppo di consegna.
3. Specificare le applicazioni e i desktop disponibili per questo gruppo:
    - Per aggiungere applicazioni da una macchina in esecuzione inclusa nel catalogo selezionato, fare clic su **Add new > From start menu**Aggiungi nuova > Dal menu Start.
    - Per aggiungere applicazioni distribuite su condivisioni di rete, fare clic su **Add new > Manually**(Aggiungi nuova > Manualmente), quindi inserire le impostazioni richieste quali percorso, directory di lavoro e altro.
    - (Visibile solo con macchine con sistema operativo multisessione) Per la distribuzione di desktop, mantenere selezionata l'opzione **Enable desktop delivery** (Abilita distribuzione desktop).
4. Aggiungere utenti al gruppo.

**Passaggio 4: condividere l'URL dell'area di lavoro con i propri utenti** Passare a **Workspace Configuration > Access** (Configurazione di Workspace > Accesso), quindi condividere l'URL di Workspace con gli utenti.

## Distribuire PC da ufficio (con alimentazione gestita)

Questa sezione guida l'utente attraverso il processo di distribuzione dei PC da ufficio (con alimentazione gestita).

### Prerequisiti

Prima di iniziare, sono necessari gli elementi seguenti:

- Nomi macchina dei PC.
- Citrix Virtual Delivery Agent (VDA) installato su ogni PC. (Questo passaggio può essere eseguito dopo la creazione del catalogo.)

  Per ulteriori informazioni, vedere Scaricare VDA.

### Preparazione

Rispondere alle domande sullo schermo per completare le seguenti impostazioni a livello di infrastruttura.

| # | Passaggio | Descrizione |
|---|---|---|
| 1 | Selezionare il tipo di allocazione della macchina. | Selezionare la modalità di assegnazione delle macchine. Opzioni: Static auto-assigned (assegnata automaticamente in modo statico), Static preassigned (preassegnata in modo statico) e Random pool unassigned (in pool casuale non assegnata) |
| 2 | Determinare se consentire agli utenti di accendere le macchine | Selezionare **I want remote users to power on machines by themselves** (Desidero che gli utenti remoti accendano le macchine da soli). |
| 3 | Selezionare il tipo di identità dell'utente | Selezionare un tipo di identità per la gestione degli utenti. Opzioni: Active Directory, Azure Active Directory, Google Cloud Identity e Okta |

**Procedura di distribuzione**

Dopo che sono state completate le impostazioni a livello di infrastruttura, vengono visualizzati i passaggi specifici per questo scenario di distribuzione. Seguire le istruzioni sullo schermo per completare le impostazioni.

**Passaggio 1: aggiungere una posizione risorsa e le connessioni host** Configurare la posizione risorsa installando i Cloud Connector e aggiungere una connessione di tipo **Remote PC Wake on LAN** (Riattivazione LAN PC remoto).

1. Assegnare un nome alla posizione risorsa.
2. Scaricare e installare i Cloud Connector su almeno due macchine Windows Server.
3. Rilevare i Cloud Connector installati.
4. Fare clic su **Add new** (Aggiungi nuova) per aggiungere una connessione:
    a) Selezionare una posizione (zona) risorsa.
    b) Selezionare **Remote PC Wake on LAN** (Riattivazione LAN PC remoto) in **Connection type** (Tipo di connessione).

c) Inserire un nome per la connessione.

> **Nota:**
>
> L'alimentazione DaaS gestisce l'alimentazione delle macchine tramite le connessioni configurate. È necessario configurare connessioni di tipo **Remote PC Wake on LAN** quando si creano cataloghi Remote PC Access per macchine con gestione dell'alimentazione.

**Passaggio 2: Creare un catalogo Remote PC Access** Creare un catalogo di macchine e importare i propri PC da ufficio in esso.

1. Assegnare un nome al catalogo
2. Selezionare una posizione risorsa.
3. Selezionare un tipo di allocazione della macchina. Per impostazione predefinita, viene visualizzato il tipo selezionato nella fase di preparazione.
4. Selezionare la **Wake on LAN connection** (Connessione di riattivazione LAN). Le opzioni sono le connessioni di tipo **Remote PC Wake on LAN** configurate per la posizione selezionata.
5. Importare le proprie macchine.
6. Fare clic su **Create**.

**Passaggio 3: Creare gruppi di consegna e assegnare utenti** Creare un gruppo di consegna per raggruppare le macchine da consegnare e specificare chi può accedervi.

1. Assegnare un nome al gruppo.
2. Selezionare un catalogo di macchine in base alle esigenze. Vengono visualizzati solo i cataloghi di tipo **Remote PC Access** .
3. Assegnare utenti al gruppo.

**Passaggio 4: condividere l'URL dell'area di lavoro con i propri utenti** Passare a **Workspace Configuration > Access** (Configurazione di Workspace > Accesso), quindi condividere l'URL di Workspace con gli utenti.

## Consegnare PC da ufficio (con alimentazione non gestita)

Questa sezione guida l'utente nel processo di distribuzione dei PC da ufficio (con alimentazione non gestita).

### Prerequisiti

Prima di iniziare, sono necessari gli elementi seguenti:

- Nomi macchina dei PC.
- Citrix Virtual Delivery Agent (VDA) installato su ogni PC. (Questo passaggio può essere eseguito dopo la creazione del catalogo.)

  Per ulteriori informazioni, vedere Scaricare VDA.

### Preparazione

Rispondere alle domande sullo schermo per completare le seguenti impostazioni a livello di infrastruttura.

| # | Impostazione | Descrizione |
|---|---|---|
| 1 | Selezionare il tipo di allocazione della macchina. | Selezionare la modalità di assegnazione delle macchine. Opzioni: Static auto-assigned (assegnata automaticamente in modo statico), Static preassigned (preassegnata in modo statico) e Random pool unassigned (in pool casuale non assegnata) |
| 2 | Determinare se consentire agli utenti di accendere le macchine | Mantenere l'opzione **Keep I want remote users to accende le macchine da soli è stata** non selezionata. |
| 3 | Selezionare il tipo di identità dell'utente | Selezionare un tipo di identità per la gestione degli utenti. Opzioni: Active Directory, Azure Active Directory, Google Cloud Identity e Okta |

### Procedura di distribuzione

Dopo che sono state completate le impostazioni a livello di infrastruttura, vengono visualizzati i passaggi specifici per questo scenario di distribuzione. Seguire le istruzioni sullo schermo per completare le impostazioni.

**Passaggio 1: Aggiungere una posizione risorsa** Configurare la posizione risorsa installando i Cloud Connector.

1. Assegnare un nome alla posizione risorsa.
2. Scaricare e installare i Cloud Connector su almeno due macchine Windows Server.
3. Rilevare i Cloud Connector installati.

> **Nota:**
>
> La creazione di connessioni host è necessaria solo se si desidera gestire l'alimentazione delle macchine esistenti.

**Passaggio 2: Creare un catalogo Remote PC Access** Creare un catalogo e importare i propri PC da ufficio in esso.

1. Assegnare un nome al catalogo
2. Selezionare una posizione risorsa.
3. Selezionare un tipo di allocazione. Per impostazione predefinita, viene visualizzato il tipo selezionato nella fase di preparazione.
4. Importare le proprie macchine.
5. Fare clic su **Create**.

**Passaggio 3: Creare gruppi di consegna e assegnare utenti** Creare un gruppo di consegna per le macchine da consegnare e specificare chi può accedervi.

1. Assegnare un nome al gruppo.
2. Selezionare un catalogo di macchine in base alle esigenze. Vengono visualizzati solo i cataloghi di tipo **Remote PC Access** .
3. Assegnare utenti al gruppo.

**Passaggio 4: condividere l'URL dell'area di lavoro con i propri utenti** Passare a **Workspace Configuration > Access** (Configurazione di Workspace > Accesso), quindi condividere l'URL di Workspace con gli utenti.

## Identità macchina

October 30, 2023

Ciascuna macchina deve avere un'identità macchina univoca, nota anche come account computer. Le identità delle macchine possono essere create e gestite nelle macchine localmente o in una directory,

ad esempio Active Directory (AD) on-premise o Azure AD. Citrix supporta l'hosting di applicazioni e desktop virtuali su macchine aggiunte ad Active Directory, ad Azure Active Directory, ad Azure Active Directory ibrido o non aggiunte a un dominio.

### Tipi di identità delle macchine

Sono supportati i seguenti tipi di identità delle macchine.

| Tipo di identità della macchina | Descrizione |
| --- | --- |
| Aggiunte ad AD | Le identità vengono create e gestite in Active Directory on-premise. Le macchine sottoposte a provisioning vengono aggiunte ad Active Directory on-premise utilizzando le identità delle macchine assegnate. |
| Aggiunte ad Azure AD | Le identità vengono create e gestite in Azure AD. Le macchine sottoposte a provisioning vengono aggiunte ad Azure AD utilizzando le identità delle macchine assegnate. L'importazione di macchine virtuali in Citrix DaaS non è supportata. |
| Aggiunto ad Azure AD ibrido | Le identità vengono create in Active Directory on-premise e vengono sincronizzate con Azure AD tramite Azure AD Connect. Le macchine sottoposte a provisioning vengono aggiunte ad Active Directory e Azure AD on-premise. Le macchine vengono quindi aggiunte ad Azure AD ibrido. Per l'importazione di una macchina virtuale aggiunta ad Azure AD ibrida, la macchina virtuale viene trattata da Citrix DaaS come se fosse aggiunta ad Active Directory. |
| Non aggiunto a un dominio | Le identità vengono create e gestite nelle macchine localmente. L'importazione di macchine virtuali in Citrix DaaS non è supportata. |

### Configurazioni supportate

Di seguito sono riportati i dettagli delle configurazioni supportate per ciascuno scenario.

**Infrastruttura supportata**

| Identità della macchina | Citrix DaaS | Citrix Workspace | Citrix StoreFront | Citrix Gateway Service | Citrix Gateway |
|---|---|---|---|---|---|
| Aggiunte ad AD | Sì | Sì | Sì | Sì | Sì |
| Aggiunte ad Azure AD | Sì | Sì | No | Sì | No |
| Aggiunto ad Azure AD ibrido | Sì | Sì | Sì | Sì | Sì |
| Non aggiunte al dominio | Sì | Sì | Sì | Sì | Sì |

> **Nota**
>
> Quando si utilizza Storefront non sono disponibili né Local Host Cache né Service Continuity per gli host di sessioni non aggiunte al dominio.

**Provider di autenticazione dell'identità per l'area di lavoro supportati**

| Identità della macchina | Azure Active Directory | Active Directory | Active Directory e token | Okta | SAML | Citrix Gateway | Autenticazione adattiva |
|---|---|---|---|---|---|---|---|
| Aggiunte ad AD | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| Aggiunte ad Azure AD | Sì | No | No | No | No | No | No |
| Aggiunto ad Azure AD ibrido | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| Non aggiunte al dominio | Sì | Sì | Sì | Sì | Sì | Sì | Sì |

## Aggiunto a Active Directory

July 6, 2023

Le identità vengono create e gestite in Active Directory on-premise. Le macchine sottoposte a provisioning vengono aggiunte ad Active Directory on-premise utilizzando le identità delle macchine assegnate. Per ulteriori informazioni sui livelli di funzionalità supportati per la foresta e il dominio, vedere Livelli funzionali di Active Directory.

Per informazioni su come creare cataloghi aggiunti ad Active Directory (AD) utilizzando Citrix DaaS, vedere Creare cataloghi di macchine.

## Aggiunte ad Azure Active Directory

August 17, 2023

Questo articolo descrive i requisiti per creare cataloghi aggiunti ad Azure Active Directory (AAD) utilizzando Citrix DaaS oltre ai requisiti descritti nella sezione dei requisiti di sistema Citrix DaaS.

### Requisiti

- Piano di controllo: vedere Supported Configurations (Configurazioni supportate)
- Tipo VDA: a sessione singola (solo desktop) o multisessione (app e desktop)
- Versione VDA: 2203 o successiva
- Tipo di provisioning: Machine Creation Services (MCS) persistente e non persistente utilizzando il flusso di lavoro Machine Profile (Profilo macchina)
- Tipo di assegnazione: dedicato e in pool
- Piattaforma di hosting: solo Azure
- Rendezvous V2 deve essere abilitato

### Limiti

- La continuità del servizio non è supportata.
- Il Single Sign-On ai desktop virtuali non è supportato. Gli utenti devono inserire manualmente le credenziali quando accedono ai propri desktop.
- L'accesso con Windows Hello nel desktop virtuale non è supportato. Al momento sono supportati solo nome utente e password. Se gli utenti tentano di accedere con qualsiasi metodo di

Windows Hello, ricevono un messaggio di errore che indica che non sono l'utente negoziato e la sessione viene disconnessa. I metodi associati includono PIN, chiave FIDO2, MFA e così via.
- Supporta solo ambienti cloud Microsoft Azure Resource Manager.
- La prima volta che viene avviata una sessione di desktop virtuale, nella schermata di accesso di Windows potrebbe essere visualizzata la richiesta di accesso per l'ultimo utente connesso senza l'opzione di passare a un altro utente. L'utente deve attendere il timeout dell'accesso e viene visualizzata la schermata di blocco del desktop, quindi deve fare clic sulla schermata di blocco per visualizzare nuovamente la schermata di accesso. A questo punto, l'utente è in grado di selezionare **Other Users** (Altri utenti) e di inserire le proprie credenziali. Questo è il comportamento di ogni nuova sessione quando i computer non sono persistenti.

## Considerazioni

### Configurazione dell'immagine

- Prendere in considerazione l'ottimizzazione dell'immagine Windows utilizzando lo strumento Citrix Optimizer.

### Aggiunte ad Azure AD

- Valutare la possibilità di disattivare Windows Hello in modo che agli utenti non venga richiesto di configurarlo quando accedono al desktop virtuale. Se si utilizza VDA 2209 o versione successiva, questa operazione viene eseguita automaticamente. Nelle versioni precedenti, vi sono due modi di farlo:
  - Criterio di gruppo o criterio locale
    - Accedere a **Configurazione computer > Modelli amministrativi > Componenti di Windows > Windows Hello for Business**.
    - Impostare **Usa Windows Hello for Business** su:
      - **Disabilitato** o
      - **Abilitato** e selezionare **Do not start Windows Hello provisioning after sign-in** (Non avviare il provisioning di Windows Hello dopo l'accesso).
  - Microsoft Intune
    - Creare un profilo di dispositivo che disabiliti Windows Hello for Business. Per i dettagli, consultare la documentazione Microsoft.
    - Attualmente, Microsoft supporta la registrazione a Intune solo di macchine persistenti, il che significa che non è possibile gestire macchine non persistenti con Intune.

- Agli utenti deve essere concesso l'accesso esplicito in Azure per accedere alle macchine utilizzando le proprie credenziali AAD. Questo può essere facilitato aggiungendo l'assegnazione del ruolo a livello di gruppo di risorse:

  1. Accedere al portale di Azure.
  2. Selezionare **Gruppi di risorse**.
  3. Fare clic sul gruppo di risorse in cui risiedono i carichi di lavoro del desktop virtuale.
  4. Selezionare **Access control (IAM)** (Controllo dell'accesso [IAM]).
  5. Fare clic su **Add role assignment** (Aggiungi assegnazione ruolo).
  6. Cercare **Virtual Machine User Login** (Accesso utente macchina virtuale), selezionarlo nell'elenco e fare clic su **Next** (Avanti).
  7. Selezionare **User, group, or service principal** (Utente, gruppo o entità servizio).
  8. Fare clic su **Select members** (Seleziona membri) e selezionare gli utenti e i gruppi a cui si desidera fornire l'accesso ai desktop virtuali.
  9. Fare clic su **Select** (Seleziona).
  10. Fare clic su **Review + assign** (Rivedi + assegna).
  11. Fare di nuovo clic su **Review + assign** (Rivedi + assegna).

> **Nota:**
>
> Se si sceglie di consentire a MCS di creare il gruppo di risorse per i desktop virtuali, si aggiunge questa assegnazione di ruolo dopo la creazione del catalogo delle macchine.

- Le macchine virtuali master possono essere aggiunte ad Azure AD o non aggiunte al dominio. Questa funzionalità richiede VDA versione 2212 o successiva.

### Installazione e configurazione del VDA

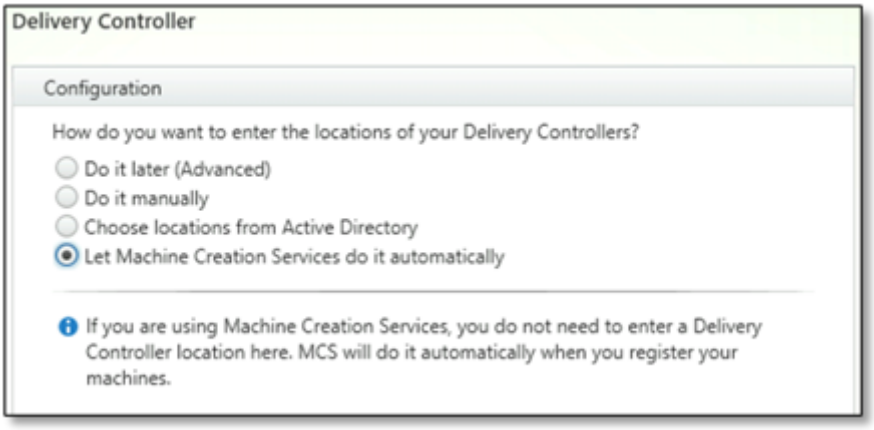
Seguire i passaggi per l'installazione del VDA:

1. Assicurarsi di selezionare le seguenti opzioni nella procedura guidata di installazione:

   - Nella pagina Environment (Ambiente), selezionare **Create a master MCS image** (Crea un'immagine MCS master).


- Nella pagina Delivery Controller, selezionare **Let Machine Creation Services do it automatically** (Consenti a Machine Creation Services di eseguire l'operazione automaticamente).




2. Dopo l'installazione del VDA, aggiungere il seguente valore di registro:

   - Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Tipo di valore: DWORD
   - Nome valore: GctRegistration
   - Dati del valore: 1

3. Per la macchina virtuale master basata su Windows 11 22H2, creare un'attività pianificata nella macchina virtuale master che esegua il seguente comando all'avvio del sistema utilizzando l'account SYSTEM. Questa attività di pianificazione di un'attività nella macchina virtuale master è richiesta solo per la versione VDA 2212 o precedente.

```
reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
    /d Citrix /f
<!--NeedCopy-->
```

4. Se si unisce la macchina virtuale master ad Azure AD e quindi si rimuove manualmente l'unione tramite l'utilità `dsregcmd`, assicurarsi che il valore di `AADLoginForWindowsExtensionJoined` in HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension sia zero.

### Passaggi successivi

Una volta si siano rese disponibili la posizione della risorsa e la connessione all'hosting, procedere alla creazione del catalogo della macchina. Per ulteriori informazioni sulla creazione di cataloghi di macchine aggiunti ad Azure Active Directory, vedere Creare cataloghi aggiunti ad Azure Active Directory.

## Microsoft Intune

July 6, 2023

Questo articolo descrive i requisiti per creare cataloghi compatibili con Microsoft Intune utilizzando Citrix DaaS oltre ai requisiti descritti nella sezione dei requisiti di sistema Citrix DaaS.

Microsoft Intune è un servizio basato su cloud incentrato sulla gestione dei dispositivi mobili (MDM) e sulla gestione delle applicazioni mobili (MAM). L'utente controlla il modo in cui vengono utilizzati i dispositivi dell'organizzazione, inclusi telefoni cellulari, tablet e laptop. Per ulteriori informazioni, vedere Microsoft Intune. I dispositivi devono soddisfare i requisiti minimi di sistema. Per ulteriori informazioni, vedere Sistemi operativi e browser supportati in Intune nella documentazione Microsoft.

Microsoft Intune funziona utilizzando la funzionalità di Azure AD.

> **Importante:**
>
> Prima di abilitare questa funzionalità, verificare che l'ambiente Azure soddisfi i requisiti di licenza per utilizzare Microsoft Intune. Per ulteriori informazioni, vedere la documentazione Microsoft: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses. Non abilitare la funzionalità se non si dispone della licenza Intune appropriata.

### Requisiti

- Piano di controllo: Citrix DaaS
- Tipo di VDA: sistema operativo VDA a sessione singola
- Versione VDA: 2203 o successiva

- Tipo di provisioning: Machine Creation Services (MCS) persistente utilizzando solo il flusso di lavoro Machine Profile (Profilo macchina)
- Tipo di assegnazione: dedicato
- Piattaforma di hosting: solo Azure

### Limiti

- Supporta solo macchine virtuali persistenti a sessione singola collegate ad Azure AD.
- Supporta solo macchine virtuali persistenti aggiunte ad Azure AD ibride a sessione singola utilizzando credenziali utente o credenziali di dispositivo con funzionalità di co-gestione. Per ulteriori informazioni, vedere Registrare automaticamente un dispositivo Windows usando Criteri di gruppo.
- Non saltare la preparazione delle immagini durante la creazione o l'aggiornamento dei cataloghi di macchine.

### Considerazioni

- Creare un profilo di dispositivo che disabiliti Windows Hello for Business.
- Utilizzare un VDA versione 2212 o successiva se Microsoft Intune deve gestire una macchina virtuale master.

### Passaggi successivi

Per informazioni sulla creazione di cataloghi compatibili con Microsoft Intune, vedere Creare cataloghi compatibili con Microsoft Intune.

## Hybrid Azure Active Directory joined (Aggiunta ad Azure Active Directory ibrida)

April 14, 2023

Questo articolo descrive i requisiti per creare cataloghi aggiunti ad Hybrid Azure Active Directory (HAAD) utilizzando Citrix DaaS oltre ai requisiti descritti nella sezione dei requisiti di sistema di Citrix DaaS.

Le macchine aggiunte ad Azure AD ibrida utilizzano AD on-premise come provider di autenticazione. È possibile assegnarle a utenti o gruppi di dominio in AD on-premise. Per abilitare l'esperienza SSO

senza soluzione di continuità di Azure AD, è necessario sincronizzare gli utenti del dominio con Azure AD.

> **Nota:**
>
> Le VM ibride aggiunte ad Azure AD sono supportate nelle infrastrutture di identità sia federate che gestite.

### Requisiti

- Piano di controllo: vedere Supported Configurations (Configurazioni supportate)
- Tipo VDA: a sessione singola (solo desktop) o multisessione (app e desktop)
- Versione VDA: 2212 o successiva
- Tipo di provisioning: Machine Creation Services (MCS), persistente e non persistente
- Tipo di assegnazione: dedicato e in pool
- Piattaforma di hosting: qualsiasi hypervisor o servizio cloud

### Limiti

- Se si utilizza Citrix Federated Authentication Service (FAS), il Single Sign-On viene indirizzato ad AD in locale anziché ad Azure AD. In questo caso, si consiglia di configurare l'autenticazione basata sul certificato di Azure AD in modo che il token di aggiornamento primario (PRT) venga generato all'accesso dell'utente, in modo da facilitare il single sign-on alle risorse di Azure AD all'interno della sessione. Altrimenti, il PRT non sarà presente e l'accesso SSO alle risorse di Azure AD non funzionerà. Per informazioni su come ottenere l'accesso singolo (SSO) da Azure AD a VDA uniti ibridi utilizzando Citrix Federated Authentication Service ( FAS), vedere Hybrid-joined VDAs.
- Non saltare la preparazione delle immagini durante la creazione o l'aggiornamento dei cataloghi di macchine. Se si desidera saltare la preparazione delle immagini, assicurarsi che le macchine virtuali master non siano aggiunte ad Azure AD o a Hybrid Azure AD.

### Considerazioni

- La creazione di macchine aggiunte ad Azure Active Directory ibrida richiede l'autorizzazione `Write userCertificate` nel dominio di destinazione. Assicurarsi di immettere le credenziali di un amministratore con tale autorizzazione durante la creazione del catalogo.
- Il processo di join di Azure AD ibrida è gestito da Citrix. È necessario disabilitare `autoWorkplaceJoin` controllato da Windows nelle macchine virtuali master come segue: L'operazione di disattivazione manuale `autoWorkplaceJoin` è richiesta solo per la versione VDA 2212 o precedente.

1. Eseguire `gpedit.msc`.
2. Accedere a **Configurazione computer > Modelli amministrativi > Componenti di Windows > Registrazione dispositivo**.
3. Impostare **Registra i computer aggiunti a un dominio come dispositivi** su **Disabilitato**.

- Selezionare l'unità organizzativa (OU) configurata per la sincronizzazione con Azure AD quando si creano le identità delle macchine.
- Per la macchina virtuale master basata su Windows 11 22H2, creare un'attività pianificata nella macchina virtuale master che esegua i seguenti comandi all'avvio del sistema utilizzando l'account SYSTEM. Questa attività di pianificazione di un'attività nella macchina virtuale master è richiesta solo per la versione VDA 2212 o precedente.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
   Windows\WorkplaceJoin'
$MaxCount = 60

for ($count = 1; $count -le $MaxCount; $count++)
{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
  {

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
       "Provider", $null)
    if ($provider -eq 'Citrix')
    {

        break;
     }


    if ($provider -eq 1)
    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
           Provider" -Value "Citrix" -Force
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
           autoWorkplaceJoin" -Value 1 -Force
        Start-Sleep 5
        dsregcmd /join
        break
     }

   }


  Start-Sleep 1
 }

```

```
<!--NeedCopy-->
```

### Passaggi successivi

Per ulteriori informazioni sulla creazione di cataloghi aggiunti ad Azure Active Directory ibridi, vedere Creare cataloghi aggiunti ad Azure Active Directory ibridi.

## Non aggiunte al dominio

November 21, 2023

Questo articolo descrive i requisiti per creare cataloghi non aggiunti a domini utilizzando Citrix DaaS oltre ai requisiti descritti nella sezione dei requisiti di sistema di Citrix DaaS.

### Requisiti

- Piano di controllo: vedere Supported Configurations (Configurazioni supportate)
- Tipo VDA: a sessione singola (solo desktop) o multisessione (app e desktop)
- Versione VDA: 2203 o successiva
- Tipo di provisioning: Machine Creation Services (MCS), persistente e non persistente
- Tipo di assegnazione: dedicato e in pool
- Piattaforma di hosting: tutte le piattaforme supportate da MCS
- Rendezvous V2 deve essere abilitato
- Cloud Connectors: richiesti solo se si prevede di effettuare il provisioning di macchine su hypervisor locali o se si desidera utilizzare Active Directory come provider di identità in Workspace.

### Limiti

- La continuità del servizio non è supportata.
- Ogni volta che utilizziamo un VDA multisessione non collegato a un dominio, i dati del profilo dell'utente locale non vengono conservati e vengono eliminati al momento dello scollegamento.

### Installazione e configurazione del VDA

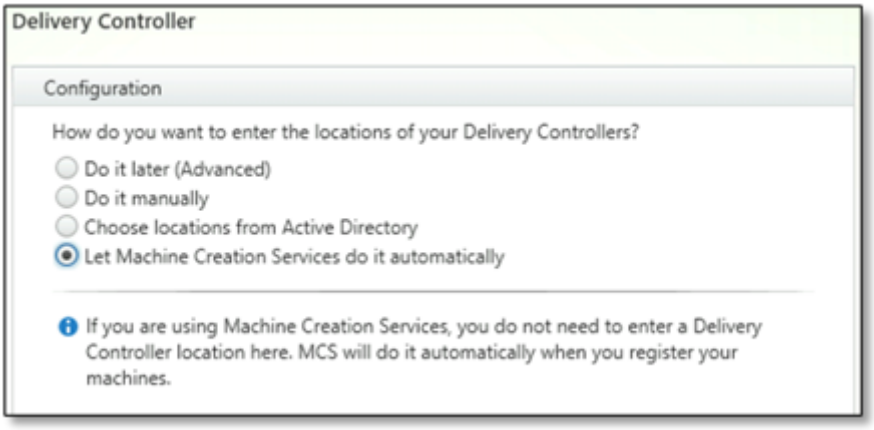
Seguire i passaggi per l'installazione del VDA:

1. Assicurarsi di selezionare le seguenti opzioni nella procedura guidata di installazione:

   - Nella pagina Environment (Ambiente), selezionare **Create a master MCS image** (Crea un' immagine MCS master).


   - Nella pagina Delivery Controller, selezionare **Let Machine Creation Services do it automatically** (Consenti a Machine Creation Services di eseguire l'operazione automaticamente).




2. Dopo l'installazione del VDA, aggiungere il seguente valore di registro:

   - Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Tipo di valore: DWORD
   - Nome valore: GctRegistration
   - Dati del valore: 1

### Passaggi successivi

Una volta si siano rese disponibili la posizione della risorsa e la connessione all'hosting, procedere alla creazione del catalogo della macchina. Per ulteriori informazioni sulla creazione di cataloghi di macchine non aggiunti a un dominio, vedere Creare cataloghi non aggiunti a un dominio.

## Configurare le posizioni risorsa

January 3, 2023

Le posizioni risorsa contengono le risorse necessarie per distribuire applicazioni e desktop agli utenti. Vengono gestite le risorse provenienti da Citrix Cloud. In genere, le risorse includono:

- Controller di dominio di Active Directory.
- Hypervisor o servizi cloud, noti come *host*.
- Virtual Delivery Agent (VDA). I VDA sono le macchine che contengono le app o il desktop. Su ogni macchina è installato anche un Citrix VDA. Il termine *VDA* si riferisce spesso al software VDA e alla macchina su cui è installato.
- Citrix Gateway (opzionale): per consentire un accesso esterno sicuro alle applicazioni e ai desktop offerti agli utenti, aggiungere un'appliance Citrix Gateway VPX alla posizione risorsa, quindi configurare Citrix Gateway.
- Server Citrix StoreFront (gestiti dal cliente).
- Per comunicare con Citrix Cloud, ogni posizione risorsa deve contenere un Citrix Cloud Connector. Per la disponibilità è consigliabile un minimo di due Cloud Connector per ciascuna posizione risorsa.

Una posizione risorsa è considerata una zona in un ambiente Citrix DaaS. Per ulteriori informazioni, vedere Zone.

Per ulteriori informazioni sui tipi di risorse, vedere Connettersi a Citrix Cloud.

### Requisiti host

L'hypervisor o il servizio cloud in cui si effettua il provisioning di macchine virtuali che distribuiscono app o desktop agli utenti potrebbe disporre di autorizzazioni o requisiti di configurazione univoci.

- Se l'hypervisor o il servizio cloud richiedono reti virtuali o altri elementi, attenersi alle linee guida nella relativa documentazione.
- Creare il cloud privato virtuale (VPC) o le reti virtuali appropriate per le macchine che verranno aggiunte alla posizione risorsa, se necessario. Ad esempio, quando si utilizza AWS, configurare un VPC con subnet pubbliche e private.

- Creare le regole appropriate per proteggere il traffico Internet in entrata e in uscita e il traffico tra le macchine nella rete virtuale. Ad esempio, quando si utilizza AWS, assicurarsi che il gruppo di sicurezza del VPC disponga delle regole appropriate configurate in modo che le macchine nel VPC siano accessibili solo agli indirizzi IP specificati.

Sono supportati i seguenti tipi di host:

- Ambienti di virtualizzazione Amazon Web Services (AWS)
- Ambienti di virtualizzazione Citrix Hypervisor
- Ambienti di virtualizzazione Google Cloud Platform
- Ambienti di virtualizzazione Microsoft Azure Resource Manager
- Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager
- Ambienti di virtualizzazione Nutanix
- Soluzioni Nutanix Cloud e dei partner
- Ambienti di virtualizzazione VMware
- Soluzioni VMware Cloud e dei partner

### Active Directory

Eseguire il provisioning di un server Windows, installare Active Directory Domain Services e promuoverlo a un controller di dominio. Per ulteriori informazioni, vedere la documentazione di Microsoft Active Directory.

- È necessario disporre di almeno un controller di dominio che esegua Servizi di dominio Active Directory.
- Non installare alcun componente Citrix su un controller di dominio.
- Non utilizzare una barra (/) quando si specificano i nomi delle unità organizzative nell'interfaccia di gestione Full Configuration (Configurazione completa).

Per ulteriori informazioni, vedere:

- Livelli funzionali di Active Directory
- Gestione delle identità e degli accessi in Citrix Cloud.

### Cloud Connector

Cloud Connector è un gruppo di servizi di Citrix Cloud che consente la comunicazione tra VDA, StoreFront gestito dal cliente e Delivery Controller basato su cloud. È possibile installare i Cloud Connector in modo interattivo o dalla riga di comando.

Per informazioni complete su Cloud Connector, vedere:

- Citrix Cloud Connector

- Dettagli tecnici, che includono i requisiti di sistema
- Configurazione di proxy e firewall
- Installazione
- Aggiornamenti del connettore

#### Considerazioni su dimensioni e scala

Quando si valuta Citrix DaaS per il dimensionamento e la scalabilità, prendere in considerazione tutti i componenti. Esaminare e verificare la configurazione dei Cloud Connector e dello StoreFront gestito dal cliente in base alle proprie esigenze specifiche. Il sottodimensionamento delle macchine può influire negativamente sulle prestazioni del sistema.

Il seguente articolo contiene informazioni sui test relativi a dimensioni e scala. Questo articolo fornisce dettagli sulle capacità massime testate, oltre a consigli sulle procedure consigliate per la configurazione della macchina Cloud Connector.

- Considerazioni su dimensioni e scalabilità per i Cloud Connector

### Aggiungere un tipo di risorsa o attivare un dominio inutilizzato in Citrix Cloud

Per aggiungere un tipo di risorsa:

1. Accedere a Citrix Cloud.
2. Nel menu in alto a sinistra, selezionare **Resource Locations** (Posizioni risorsa).
3. Selezionare **+ Resource Locations** (+ Posizioni risorse) per aggiungere una nuova posizione risorsa.
4. Immettere un nome per la posizione risorsa e fare clic su **Save** (Salva). Per informazioni sulle considerazioni relative ai nomi, vedere Restrizioni relative ai nomi.
5. Nella nuova posizione risorse, selezionare **Cloud Connectors**.
6. Scaricare e installare il software Cloud Connector su almeno due server nel dominio in cui risiedono le risorse Citrix DaaS.
    - Durante l'installazione, selezionare la posizione risorsa creata nei passaggi 3 e 4.
    - Dopo l'installazione, Citrix Cloud aggiunge i server alla posizione risorsa e registra i domini in cui sono stati installati i Cloud Connector.
7. Verificare che i domini registrati siano attivi:
    - Dal menu Citrix Cloud, selezionare **Identity Access Management**.

- Selezionare **Domains** (Domini). Viene visualizzato un elenco di domini in cui sono stati distribuiti Cloud Connector.
- Individuare i domini che si utilizzano con Citrix DaaS. I domini attivi vengono visualizzati con una barra verde sul lato sinistro della voce del dominio.

Se il proprio dominio non ha l'indicatore visivo descritto nel passaggio 7, si trova in stato "inutilizzato". Se si specifica un dominio inutilizzato durante la configurazione del catalogo delle macchine, la creazione del catalogo non riesce. Per assicurarsi che la configurazione del catalogo macchine avvenga senza errori, seguire i passaggi descritti in "Attivare un dominio inutilizzato"in questo articolo.

Per ulteriori informazioni, vedere CTX473009: Procedura guidata per la creazione del catalogo DaaS: "Errore interno del server"durante la creazione dell'aggiunta di nuovi account macchina.

Attivare un dominio non utilizzato:

1. Nella scheda **Domain**, in **Identity and Access Management** (Gestione delle identità e degli accessi), selezionare **Show Unused Domains** (Mostra domini inutilizzati). Dopo aver selezionato questa opzione, l'etichetta cambia in **Hide Unused Domains** (Nascondi domini inutilizzati).
2. Individuare il dominio non utilizzato nell'elenco. I domini non utilizzati sono dotati di una barra grigia sul lato sinistro della voce di dominio e di un menu con puntini di sospensione a singola opzione sul lato destro.
3. Selezionare il menu con i puntini di sospensione, quindi selezionare **Use domain** (Usa dominio). La barra grigia diventa verde e il menu con i puntini di sospensione diventa **Disable** (Disabilita).

## Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per impostare le posizioni risorsa per tipi di host specifici:
  - Ambienti cloud AWS
  - Ambienti di virtualizzazione Citrix Hypervisor
  - Ambienti Google Cloud
  - Ambienti cloud Microsoft Azure Resource Manager
  - Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager
  - Ambienti di virtualizzazione Nutanix
  - Soluzioni Nutanix Cloud e dei partner
  - Ambienti di virtualizzazione VMware
  - Soluzioni VMware Cloud e dei partner
- Per una distribuzione completa, creare una connessione a una posizione risorsa.

- Esaminare tutti i passaggi del processo di installazione e configurazione

## Ambienti cloud AWS

January 18, 2023

Questo articolo illustra la configurazione dell'account Amazon Web Services (AWS) come posizione risorsa che è possibile utilizzare con Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). La posizione risorsa include un set di componenti di base, ideale per una Proof of Concept o un'altra distribuzione che non richiede risorse distribuite in più zone di disponibilità. Dopo aver completato queste attività, è possibile installare VDA, eseguire il provisioning delle macchine, creare cataloghi delle macchine e creare gruppi di consegna.

Una volta completate le attività descritte in questo articolo, la posizione risorsa include i seguenti componenti:

- Un cloud privato virtuale (VPC) con subnet pubbliche e private all'interno di un'unica zona di disponibilità.
- Un'istanza che viene eseguita sia come controller di dominio Active Directory che come server DNS, situata nella subnet privata del VPC.
- Due istanze aggiunte al dominio su cui è installato Citrix Cloud Connector, situate nella subnet privata del VPC.
- Un'istanza che funge da host bastion, situata nella subnet pubblica del VPC. Questa istanza viene utilizzata per avviare connessioni RDP alle istanze nella subnet privata per scopi amministrativi. Dopo aver completato la configurazione della posizione risorsa, è possibile chiudere questa istanza in modo che non sia più facilmente accessibile. Quando è necessario gestire altre istanze nella subnet privata, come le istanze VDA, è possibile riavviare l'istanza host bastion.

### Panoramica delle attività

**Configurare un cloud privato virtuale (VPC) con subnet pubbliche e private.** Una volta completata questa attività, AWS distribuisce il/i gateway NAT con un indirizzo IP elastico nella subnet pubblica. Ciò consente alle istanze nella subnet privata di accedere a Internet. Le istanze nella subnet pubblica sono accessibili al traffico pubblico in entrata, mentre le istanze nella subnet privata non lo sono.

**Configurare i gruppi di sicurezza**. I gruppi di sicurezza agiscono come firewall virtuali che controllano il traffico per le istanze nel VPC. È possibile aggiungere regole ai gruppi di sicurezza che consentono alle istanze nella subnet pubblica di comunicare con le istanze nella subnet privata. Inoltre, questi gruppi di sicurezza verranno associati a ogni istanza nel VPC.

**Creare un set di opzioni DHCP**. Con un VPC Amazon, i servizi DHCP e DNS sono forniti per impostazione predefinita, il che influisce sulla configurazione del DNS sul controller di dominio Active Directory. Il DHCP di Amazon non può essere disabilitato e il DNS di Amazon può essere utilizzato solo per la risoluzione DNS pubblica, non per la risoluzione dei nomi di Active Directory. Per specificare i server di dominio e dei nomi trasferiti alle istanze tramite DHCP, creare un set di opzioni DHCP. Il set assegna il suffisso di dominio Active Directory e specifica il server DNS per tutte le istanze nel VPC. Per garantire che i record Host (A) e Ricerca inversa (PTR) vengano registrati automaticamente quando le istanze entrano a far parte del dominio, è necessario configurare le proprietà dell'adattatore di rete per ogni istanza aggiunta alla subnet privata.

**Aggiungere un host bastion, un controller di dominio e Citrix Cloud Connector a VPC**. Tramite l'host bastion, è possibile accedere alle istanze nella subnet privata per configurare il dominio, unire le istanze al dominio e installare Citrix Cloud Connector.

### Attività 1: Configurare il VPC

1. Dalla console di gestione AWS, selezionare **VPC**.
2. Dalla dashboard VPC, selezionare **Create VPC**.
3. Selezionare **VPC and more** (VPC e altro).
4. In NAT gateways ($) selezionare **In 1 AZ** o **1 per AZ**.
5. Per l'istanza NAT, specificate il tipo di istanza e la coppia di chiavi che si desidera utilizzare. La coppia di chiavi consente di connettersi in modo sicuro all'istanza in un secondo momento.
6. In DNS options (Opzioni DNS), lasciare selezionata l'opzione **Enable DNS hostnames** (Abilita nomi host DNS).
7. Selezionare **Create VPC** (Crea VPC). AWS crea le subnet pubbliche e private, il gateway Internet, le tabelle di instradamento e il gruppo di sicurezza predefinito.

> **Nota:**
>
> la modifica del nome di un Virtual Private Cloud (VPC) AWS nella console AWS danneggia l'unità di hosting esistente in Citrix Cloud. Quando l'unità di hosting è danneggiata, non è possibile creare cataloghi o aggiungere macchine ai cataloghi esistenti. Dal problema noto: PMCS-7701

### Attività 2: Configurare i gruppi di sicurezza

Questa attività crea e configura i seguenti gruppi di sicurezza per il VPC:

- Un gruppo di sicurezza pubblico, a cui verranno associate le istanze della subnet pubblica.
- Un gruppo di sicurezza privato, a cui verranno associate le istanze della subnet privata.

Per creare i gruppi di sicurezza

1. Dalla dashboard del VPC, selezionare **Security Groups** (Gruppi di sicurezza).
2. Creare un gruppo di sicurezza per il gruppo di sicurezza pubblico. Selezionare **Create Security Group** (Crea gruppo di sicurezza) e immettere un nome e una descrizione per il gruppo. Nel VPC, selezionare il VPC creato in precedenza. Selezionare **Yes, Create** (Sì, crea).

**Configurare il gruppo di sicurezza pubblico**

1. Dall'elenco dei gruppi di sicurezza, selezionare il gruppo di sicurezza pubblico.
2. Selezionare la scheda **Inbound Rules** (Regole in entrata) e selezionare Edit (Modifica) per creare le seguenti regole:

| Tipo | Origine |
|---|---|
| TUTTO il traffico | Selezionare il gruppo di sicurezza privato. |
| TUTTO il traffico | Selezionare il gruppo di sicurezza pubblico. |
| ICMP | 0.0.0.0/0 |
| 22 (SSH) | 0.0.0.0/0 |
| 80 (HTTP) | 0.0.0.0/0 |
| 443 (HTTPS) | 0.0.0.0/0 |
| 1494 (ICA/HDX) | 0.0.0.0/0 |
| 2598 (affidabilità della sessione) | 0.0.0.0/0 |
| 3389 (RDP) | 0.0.0.0/0 |

3. Al termine, selezionare **Save** (Salva).
4. Selezionare la scheda **Outbound Rules** (Regole in uscita) e selezionare **Edit** (Modifica) per creare le seguenti regole:

| Tipo | Destinazione |
|---|---|
| TUTTO il traffico | Selezionare il gruppo di sicurezza privato. |
| TUTTO il traffico | 0.0.0.0/0 |
| ICMP | 0.0.0.0/0 |

5. Al termine, selezionare **Save** (Salva).

**Configurare il gruppo di sicurezza privato**

1. Dall'elenco dei gruppi di sicurezza, selezionare il gruppo di sicurezza privato.
2. Se non è stato ancora impostato il traffico dal gruppo di sicurezza pubblico, è necessario impostare le porte TCP da includere; selezionare la scheda **Inbound Rules** (Regole in entrata) e selezionare **Edit** (Modifica) per creare le seguenti regole:

| Tipo | Origine |
|---|---|
| TUTTO il traffico | Selezionare il gruppo di sicurezza NAT. |
| TUTTO il traffico | Selezionare il gruppo di sicurezza privato. |
| TUTTO il traffico | Selezionare il gruppo di sicurezza pubblico. |
| ICMP | Selezionare il gruppo di sicurezza pubblico. |
| TCP 53 (DNS) | Selezionare il gruppo di sicurezza pubblico. |
| UDP 53 (DNS) | Selezionare il gruppo di sicurezza pubblico. |
| 80 (HTTP) | Selezionare il gruppo di sicurezza pubblico. |
| TCP 135 | Selezionare il gruppo di sicurezza pubblico. |
| TCP 389 | Selezionare il gruppo di sicurezza pubblico. |
| UDP 389 | Selezionare il gruppo di sicurezza pubblico. |
| 443 (HTTPS) | Selezionare il gruppo di sicurezza pubblico. |
| TCP 1494 (ICA/HDX) | Selezionare il gruppo di sicurezza pubblico. |
| TCP 2598 (affidabilità della sessione) | Selezionare il gruppo di sicurezza pubblico. |
| 3389 (RDP) | Selezionare il gruppo di sicurezza pubblico. |
| TCP 49152-65535 | Selezionare il gruppo di sicurezza pubblico. |

3. Al termine, selezionare **Save** (Salva).
4. Selezionare la scheda **Outbound Rules** (Regole in uscita) e selezionare **Edit** (Modifica) per creare le seguenti regole:

| Tipo | Destinazione |
|---|---|
| TUTTO il traffico | Selezionare il gruppo di sicurezza privato. |
| TUTTO il traffico | 0.0.0.0/0 |
| ICMP | 0.0.0.0/0 |

| Tipo | Destinazione |
| --- | --- |
| UDP 53 (DNS) | 0.0.0.0/0 |

5. Al termine, selezionare **Save** (Salva).

### Attività 3: Avviare le istanze

I seguenti passaggi creano quattro istanze EC2 e decrittografano la password dell'amministratore predefinita generata da Amazon.

1. Dalla Console di gestione AWS, selezionare **EC2**.
2. Dalla dashboard di EC2, selezionare **Launch Instance** (Avvia istanza).
3. Selezionare un'immagine e un tipo di istanza della macchina Windows Server.
4. Nella pagina Configure Instance Details (Configura dettagli istanza), inserire un nome per l'istanza e selezionare il VPC configurato in precedenza.
5. In **Subnet**, effettuare le seguenti selezioni per ogni istanza:
   - Host bastion: selezionare la subnet pubblica.
   - Controller di dominio e connettori: selezionare la subnet privata.
6. In **Auto-assign Public IP address** (Assegna automaticamente l'indirizzo IP pubblico), effettuare le seguenti selezioni per ogni istanza:
   - Host bastion: selezionare **Enable** (Abilita).
   - Controller di dominio e connettori: selezionare **Use default setting** (Usa impostazione predefinita) o **Disable** (Disabilita).
7. In **Network Interfaces** (Interfacce di rete), immettere un indirizzo IP primario all'interno dell'intervallo IP della subnet privata per il controller di dominio e le istanze di Cloud Connector.
8. Nella pagina Add Storage (Aggiungi spazio di archiviazione), modificare le dimensioni del disco, se necessario.
9. Nella pagina Tag Instance (Istanza tag), inserire un nome descrittivo per ogni istanza.
10. Nella pagina Configure Security Groups (Configura gruppi di sicurezza), selezionare **Select an existing security group** (Seleziona un gruppo di sicurezza esistente) e quindi effettuare le seguenti selezioni per ogni istanza:
    - Host bastion: selezionare il gruppo di sicurezza pubblico.
    - Controller di dominio e connettori cloud: selezionare il gruppo di sicurezza privato.

11. Controllare le selezioni e quindi selezionare **Launch** (Avvia).
12. Creare una nuova coppia di chiavi o selezionarne una esistente. Se si crea una nuova coppia di chiavi, scaricare il file della chiave privata (.pem) e conservalo in un luogo sicuro. È necessario fornire la chiave privata quando si acquisisce la password di amministratore predefinita per l'istanza.
13. Selezionare **Launch Instances** (Avvia istanze). Selezionare **View Instances** (Visualizza istanze) per visualizzare un elenco delle istanze. Attendere che l'istanza appena avviata abbia superato tutti i controlli di stato prima di accedervi.
14. Acquisire la password di amministratore predefinita per ogni istanza:
    a) Dall'elenco delle istanze, selezionare l'istanza e quindi selezionare **Connect** (Connetti).
    b) Selezionare **Get Password** (Ottieni password) e inserire il file della chiave privata (.pem) quando richiesto.
    c) Selezionare **Decrypt Password** (Decrittografa password). AWS visualizza la password predefinita.
15. Ripetere i passaggi da 2 a 14 fino a quando non sono state create quattro istanze: un'istanza host bastion nella subnet pubblica e tre istanze nella subnet privata da utilizzare come controller di dominio e due Cloud Connector.

### Attività 4: Creare un set di opzioni DHCP

1. Dalla dashboard del VPC, selezionare **DHCP Options Sets** (Set di opzioni DHCP).
2. Inserire le seguenti informazioni:
    - Nome: inserire un nome descrittivo per il set.
    - Nome di dominio: immettere il nome di dominio completo utilizzato quando si configura l'istanza del controller di dominio.
    - Server del nome di dominio: immettere l'indirizzo IP privato assegnato all'istanza del controller di dominio e la stringa **AmazonProvidedDNS**, separati da virgole.
    - Server NTP: lasciare vuoto questo campo.
    - Server dei nomi NetBIOS: immettere l'indirizzo IP privato dell'istanza del controller di dominio.
    - Tipo di nodo NetBIOS: immettere **2**.
3. Selezionare **Yes, Create** (Sì, crea).
4. Associare il nuovo set al VPC:
    a) Dalla dashboard del VPC, selezionare **Your VPCs** (VPC disponibili), quindi selezionare il VPC configurato in precedenza.

b) Selezionare **Actions > Edit DHCP Options Set** (Azioni > Modifica set di opzioni DHCP).
c) Quando richiesto, selezionare il nuovo set che hai creato e quindi selezionare **Save** (Salva).

### Attività 5: Configurare le istanze

1. Utilizzando un client RDP, connettersi all'indirizzo IP pubblico dell'istanza host bastion. Quando richiesto, inserire le credenziali per l'account amministratore.
2. Dall'istanza host bastion, avviare Connessione Desktop remoto e connettersi all'indirizzo IP privato dell'istanza che si desidera configurare. Quando richiesto, inserire le credenziali dell'amministratore per l'istanza.
3. Per tutte le istanze nella subnet privata, configurare le impostazioni DNS:

    a) Selezionare **Start > Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione > Modifica impostazioni scheda**. Fare doppio clic sulla connessione di rete visualizzata.

    b) Selezionare **Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties** (Proprietà > Protocollo Internet versione 4 (TCP/IPv4) > Proprietà).

    c) Selezionare **Advanced > DNS**. Assicurarsi che le seguenti impostazioni siano abilitate e selezionare **OK**:

        - Registra nel DNS gli indirizzi di questa connessione
        - Utilizza il suffisso DNS di questa connessione nella registrazione DNS

4. Per configurare il controller di dominio:

    a) Utilizzando Server Manager, aggiungere il ruolo Servizi di dominio Active Directory con tutte le funzionalità predefinite.
    b) Promuovere l'istanza a un controller di dominio. Durante la promozione, abilitare il DNS e utilizzare il nome di dominio specificato al momento della creazione del set di opzioni DHCP. Riavviare l'istanza quando richiesto.

5. Per configurare il primo Cloud Connector:

    a) Aggiungere l'istanza al dominio e riavviare quando richiesto. Dall'istanza host bastion, riconnettersi all'istanza utilizzando RDP.
    b) Accedere a Citrix Cloud. Selezionare **Resource Locations** (Posizioni delle risorse) dal menu in alto a sinistra.
    c) Scaricare il Cloud Connector.
    d) Quando richiesto, eseguire il file `cwcconnector.exe` e fornire le credenziali Citrix Cloud. Seguire la procedura guidata.

e) Al termine, selezionare **Refresh** (Aggiorna) per visualizzare la pagina Resource Locations (Posizioni delle risorse). Quando il Cloud Connector è registrato, l'istanza viene visualizzata nella pagina.

6. Ripetere il passaggio 5 per configurare il secondo Cloud Connector.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione ad AWS.
- Esaminare tutti i passaggi del processo di installazione e configurazione

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

## Ambienti di virtualizzazione Citrix Hypervisor

December 21, 2022

Citrix Hypervisor semplifica la gestione operativa, garantendo un'esperienza utente ad alta definizione per carichi di lavoro intensivi.

Per configurare l'hypervisor Citrix, vedere Configurare il tipo di risorsa.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione a Citrix Hypervisor.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

# Ambienti Google Cloud

May 9, 2023

Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) consente di effettuare il provisioning delle macchine su Google Cloud e gestirle.

## Requisiti

- Account Citrix Cloud. La funzionalità descritta in questo articolo è disponibile solo in Citrix Cloud.
- Sottoscrizione a Citrix DaaS. Per ulteriori informazioni, consultare Per iniziare.
- Un progetto Google Cloud. Il progetto memorizza tutte le risorse di elaborazione associate al catalogo delle macchine. Può essere un progetto esistente o nuovo.
- Abilitare quattro API nel progetto Google Cloud. Per i dettagli, consultare Abilitare le API di Google Cloud.
- Account del servizio Google Cloud. L'account del servizio si autentica su Google Cloud per consentire l'accesso al progetto. Per informazioni dettagliate, vedere Configurare e aggiornare gli account di servizio.
- Abilitare l'accesso privato di Google. Per i dettagli, consultare Abilitare l'accesso privato di Google.

## Abilitare le API di Google Cloud

Per utilizzare la funzionalità Google Cloud tramite l'interfaccia Full Configuration (Configurazione completa) di Citrix Virtual Apps and Desktops, abilitare queste API nel progetto Google Cloud:

- API di Compute Engine
- API di Cloud Resource Manager
- API di Gestione delle identità e degli accessi (IAM)
- API Cloud Build

Dalla console di Google Cloud, completare questi passaggi:

1. Nel menu in alto a sinistra, selezionare **API e servizi > Dashboard**.
2. Nella schermata **Dashboard**, assicurarsi che l'API Compute Engine sia abilitata. In caso contrario, attenersi alla seguente procedura:
    a) Andare ad **API e servizi > Libreria**.
    b) Nella casella di ricerca, digitare *Compute Engine*.

c) Dai risultati della ricerca, selezionare **Compute Engine API** (API Compute Engine).

d) Nella pagina **Compute Engine API** (API Compute Engine), selezionare **Abilita**.

3. Abilitare l'API Cloud Resource Manager.

a) Andare ad **API e servizi > Libreria**.

b) Nella casella di ricerca, digitare *Cloud Resource Manager*.

c) Dai risultati della ricerca, selezionare **Cloud Resource Manager API** (API Cloud Resource Manager).

d) Nella pagina **Cloud Resource Manager API** (API Cloud Resource Manager), selezionare **Abilita**. Viene visualizzato lo stato dell'API.

4. Allo stesso modo, abilitare **Identity and Access Management (IAM) API** (API Gestione dell'identità e degli accessi [IAM]) e **Cloud Build API** (API Cloud Build).

È anche possibile utilizzare Google Cloud Shell per abilitare le API. A questo scopo:

1. Aprire la Google Console e caricare Cloud Shell.
2. Eseguire i seguenti quattro comandi in Cloud Shell:

   - gcloud services enable compute.googleapis.com
   - gcloud services enable cloudresourcemanager.googleapis.com
   - gcloud services enable iam.googleapis.com
   - gcloud services enable cloudbuild.googleapis.com

3. Fare clic su **Authorize** se richiesto da Cloud Shell.

### Configurare e aggiornare gli account di servizio

Citrix Cloud utilizza tre account di servizio separati all'interno del progetto Google Cloud:

- *Account di servizio Citrix Cloud*: questo account di servizio consente a Citrix Cloud di accedere al progetto Google, di effettuare il provisioning e di gestire le macchine. L'account Google Cloud esegue l'autenticazione su Citrix Cloud utilizzando una chiave generata da Google Cloud.

  È necessario creare questo account di servizio manualmente.

  È possibile identificare questo account di servizio con un indirizzo e-mail. Ad esempio, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

  Ogni account (personale o di servizio) ha diversi ruoli che definiscono la gestione del progetto. Assegnare i seguenti ruoli a questo account di servizio:

  – Amministratore Compute

  - Amministratore Storage
  - Editor Cloud Build
  - Utente account di servizio
  - Utente di Cloud Datastore

- *Account del servizio Cloud Build*: questo account di servizio viene fornito automaticamente dopo aver abilitato tutte le API menzionate in Enable Google Cloud APIs (Abilita le API di Google Cloud).

  È possibile identificare questo account di servizio tramite un indirizzo e-mail che inizia con l'**ID del progetto** e la parola **cloudbuild**. Ad esempio, `<project-id>@cloudbuild.gserviceaccount.com`

  Assegnare i seguenti ruoli a questo account di servizio:

  - Account del servizio Cloud Build
  - Amministratore istanze Compute
  - Utente account di servizio

- *Account del servizio Cloud Compute*: questo account di servizio viene aggiunto da Google Cloud alle istanze create in Google Cloud una volta attivata l'API Compute. Questo account ha il ruolo di editor di base IAM per eseguire le operazioni. Tuttavia, se si elimina l'autorizzazione predefinita per avere un controllo più granulare, è necessario aggiungere il ruolo **Storage Admin** che richiede le seguenti autorizzazioni:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

È possibile identificare questo account di servizio tramite un indirizzo e-mail che inizia con l'**ID del progetto** e la parola **compute**. Ad esempio, `<project-id>-compute@developer.gserviceaccount.com`.

#### Creare un account Citrix Cloud Service

Per creare un account Citrix Cloud Service, effettuare le seguenti operazioni:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > Account di servizio**.
2. Nella pagina **Account di servizio**, selezionare **CREA ACCOUNT DI SERVIZIO**.
3. Nella pagina **Create service account** (Crea account di servizio), immettere le informazioni richieste e quindi selezionare **CREATE AND CONTINUE** (CREA E CONTINUA).

4. Nella pagina **Grant this service account access to project** (Concedi a questo account di servizio l'accesso al progetto), fare clic sul menu a discesa **Select a role** (Seleziona un ruolo) e selezionare i ruoli richiesti. Fare clic su **+ADD ANOTHER ROLE** (+AGGIUNGI UN ALTRO RUOLO) se si desidera aggiungere altri ruoli.

   > **Nota:**
   >
   > Abilitare tutte le API per ottenere l'elenco completo dei ruoli disponibili durante la creazione di un nuovo account di servizio.

5. Fare clic su **CONTINUE** (Continua).
6. Nella pagina **Grant users access to this service account** (Concedi agli utenti l'accesso a questo account di servizio), aggiungere utenti o gruppi per concedere loro l'accesso necessario per eseguire azioni in questo account di servizio.
7. Fare clic su **DONE** (Fine).
8. Accedere alla console principale di IAM.
9. Identificare l'account di servizio creato.
10. Confermare che i ruoli sono stati assegnati correttamente.

**Considerazioni:**

Quando si crea l'account di servizio, tendere in considerazione quanto segue:

- I passaggi **Grant this service account access to project** (Concedi a questo account di servizio l'accesso al progetto) e **Grant users access to this service account** (Consenti agli utenti l'accesso a questo account di servizio) sono facoltativi. Se si sceglie di saltare questi passaggi di configurazione facoltativi, l'account di servizio appena creato non viene visualizzato nella pagina **IAM e amministrazione > IAM**.
- Per visualizzare i ruoli associati a un account di servizio, aggiungere i ruoli senza saltare i passaggi facoltativi. Questo processo garantisce la visualizzazione dei ruoli per l'account di servizio configurato.

**Chiave dell'account Citrix Cloud Service** Quando si crea un account di servizio, è disponibile un'opzione per creare una chiave per l'account. Questa chiave è necessaria per creare una connessione in Citrix DaaS. La chiave è contenuta in un file di credenziali (.json). Il file viene scaricato e salvato automaticamente nella cartella **Download** dopo aver creato la chiave. Quando si crea la chiave, assicurarsi di impostare il tipo di chiave su JSON. In caso contrario, l'interfaccia Full Configuration (Configurazione completa) di Citrix non può analizzarla.

> **Suggerimento:**
>
> Creare chiavi utilizzando la pagina **Account di servizio** nella console di Google Cloud. Si consiglia di cambiare le chiavi regolarmente per motivi di sicurezza. È possibile fornire nuove chiavi all'applicazione Citrix Virtual Apps and Desktops modificando una connessione Google Cloud esistente.

#### Aggiungere ruoli all'account Citrix Cloud Service

Per aggiungere ruoli all'account Citrix Cloud Service:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > IAM**.
2. Nella pagina **IAM > PERMISSIONS** (AUTORIZZAZIONI), individuare l'account di servizio creato, identificabile con un indirizzo e-mail.

   Ad esempio, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selezionare l'icona a forma di matita per modificare l'accesso al principale dell'account del servizio.
4. Nella pagina **Edit access to "project-id"** (Modifica accesso a "project-id") per l'opzione principale selezionata, selezionare **ADD ANOTHER ROLE** (AGGIUNGI UN ALTRO RUOLO) per aggiungere i ruoli richiesti al proprio account di servizio uno per uno, quindi selezionare **SAVE** (SALVA).

#### Aggiungere ruoli all'account di servizio Cloud Build

Per aggiungere ruoli all'account di servizio Cloud Build:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > IAM**.
2. Nella pagina **IAM**, individuare l'account di servizio Cloud Build, identificabile con un indirizzo e-mail che inizia con l'**ID del progetto** e la parola **cloudbuild**.

   Ad esempio, `<project-id>@cloudbuild.gserviceaccount.com`
3. Selezionare l'icona a forma di matita per modificare i ruoli dell'account Cloud Build.
4. Nella pagina **Edit access to "project-id"** (Modifica accesso a "project-id") per l'opzione principale selezionata, selezionare **ADD ANOTHER ROLE** (AGGIUNGI UN ALTRO RUOLO) per aggiungere i ruoli richiesti al proprio account di servizio Cloud Build uno per uno, quindi selezionare **SAVE** (SALVA).

> **Nota:**
>
> Abilitare tutte le API per ottenere l'elenco completo dei ruoli.

#### Permessi di archiviazione e gestione dei bucket

Citrix DaaS migliora il processo di segnalazione degli errori di compilazione del cloud per il servizio Google Cloud. Questo servizio esegue le compilazioni su Google Cloud. Citrix DaaS crea un bucket di archiviazione denominato `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` in cui i servizi Google Cloud acquisiscono le informazioni dei log di compilazione. In questo bucket è impostata un'opzione che elimina i contenuti dopo un periodo di 30 giorni. Questo processo richiede che l'account di servizio utilizzato per la connessione abbia le autorizzazioni di Google Cloud impostate su `storage.buckets.update`. Se l'account del servizio non dispone di questa autorizzazione, Citrix DaaS ignora gli errori e procede con il processo di creazione del catalogo. Senza questa autorizzazione, la dimensione dei log di compilazione aumenta e richiede una pulizia manuale.

### Abilitare l'accesso privato a Google

Quando una macchina virtuale non ha un indirizzo IP esterno assegnato alla relativa interfaccia di rete, i pacchetti vengono inviati solo ad altre destinazioni di indirizzi IP interni. Quando si abilita l'accesso privato, la macchina virtuale si connette all'insieme di indirizzi IP esterni utilizzati dall'API Google e dai servizi associati.

> **Nota:**
>
> Se l'accesso privato a Google è abilitato, tutte le macchine virtuali con e senza indirizzi IP pubblici devono essere in grado di accedere alle API pubbliche di Google, soprattutto se nell'ambiente sono stati installati dispositivi di rete di terze parti.

Per assicurare che una macchina virtuale nella subnet possa accedere alle API Google senza un indirizzo IP pubblico per il provisioning MCS:

1. In Google Cloud, accedere alla **configurazione della rete VPC**.
2. Nella schermata dei dettagli della subnet, attivare **Private Google access** (Accesso privato a Google).

Per ulteriori informazioni, consultare Configurazione dell'accesso privato a Google.

> **Importante:**
>
> Se la rete è configurata per impedire l'accesso delle macchine virtuali a Internet, assicurarsi che l'organizzazione si assuma i rischi associati all'abilitazione dell'accesso privato a Google per la

> subnet a cui è connessa la macchina virtuale.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione agli ambienti cloud di Google.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

## Ambienti di virtualizzazione HPE Moonshot (anteprima)

December 5, 2023

Citrix DaaS gestisce i carichi di lavoro di HPE Moonshot tramite un plug-in HPE Moonshot gestito da Citrix presente nel piano di controllo DaaS. Con questo plug-in, è possibile creare connessioni allo chassis HPE Moonshot, creare cataloghi e gestire l'alimentazione delle macchine incluse nel catalogo.

### Requisito

Abilitare l'attivazione/disattivazione della funzionalità **moonshotpluginenabled** in **DaaS > Home > Preview features** (Funzioni di anteprima).

### Passaggi chiave

1. Configurare i propri ambienti HPE.
2. Creare una connessione allo chassis HPE Moonshot.

> **Nota:**
>
> Dopo che è stata abilitata l'opzione di attivazione/disattivazione della funzionalità, il plug-in HPE Moonshot gestito da Citrix viene installato automaticamente. È quindi possibile

> continuare a utilizzare il catalogo di macchine esistente utilizzando il plug-in Moonshot gestito da Citrix anziché il plug-in HPE Moonshot gestito da HPE.

3. Creare un catalogo di macchine.

   > **Nota:**
   >
   > Prima di creare un catalogo, assicurarsi di disporre di uno o più nodi di cartucce HPE Moonshot e installare i VDA su tali nodi. È possibile considerare lo chassis HPE Moonshot come hypervisor e i nodi di cartucce come macchine virtuali.

4. Creare un gruppo di consegna.
5. Eseguire la migrazione del resto dei nodi HPE Moonshot non gestiti al catalogo o al gruppo di consegna gestito.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connection to HPE Moonshot.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Creare e gestire le connessioni
- Creare cataloghi di macchine

## Ambienti cloud Microsoft Azure Resource Manager

December 21, 2022

Quando si utilizza Microsoft Azure Resource Manager per eseguire il provisioning di macchine virtuali nella distribuzione del servizio Citrix Virtual Apps o Citrix Virtual Desktops, prendere dimestichezza con quanto segue:

- Azure Active Directory: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/

- Framework di consenso: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Entità servizio: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Per configurare Microsoft Azure Resource Manager, vedere Configurare le posizioni risorsa.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione a Microsoft Azure.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine
- CTX219211: Configurare un account Microsoft Azure Active Directory
- CTX219243: Concedere a XenApp e XenDesktop l'accesso alla sottoscrizione di Azure
- CTX219271: Distribuire il cloud ibrido utilizzando una VPN da sito a sito

## Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager

February 24, 2023

Seguire queste indicazioni se si utilizza Hyper-V con Microsoft System Center Virtual Machine Manager (VMM) per fornire macchine virtuali.

Per un elenco delle versioni di VMM supportate, vedere Requisiti di sistema.

È possibile utilizzare Machine Creation Services o Citrix Provisioning (in precedenza Provisioning Services) per eseguire il provisioning di quanto segue:

- Macchine virtuali con sistema operativo desktop o server di prima generazione
- Macchine virtuali Windows Server 2012 R2, Windows Server 2016 e Windows 10 di seconda generazione (con o senza Avvio protetto)

### Installare e configurare un hypervisor

Installare il server Microsoft Hyper-V e VMM sui server.

Verificare le seguenti informazioni sull'account:

In **Manage > Full Configuration** (Gestisci > Configurazione completa), l'account specificato durante la creazione di una connessione deve essere un amministratore VMM o un amministratore delegato VMM per le macchine Hyper-V pertinenti. Se questo account ha solo il ruolo di amministratore delegato in VMM, i dati di archiviazione non vengono elencati nell'interfaccia **Full Configuration** (Configurazione completa) durante il processo di creazione della connessione.

L'account utente deve inoltre essere membro del gruppo di sicurezza locale dell'amministratore su ciascun server Hyper-V per supportare la gestione del ciclo di vita delle macchine virtuali (ad esempio creazione, aggiornamento ed eliminazione delle macchine virtuali).

Nelle implementazioni di grandi dimensioni in cui un singolo SCVMM gestisce più cluster in diversi data center, è possibile limitare l'ambito degli amministratori dei gruppi host.

Per limitare l'ambito dei gruppi di host, utilizzare il ruolo di amministratore delegato nella console di Microsoft System Center Virtual Machine Manager (VMM):

1. In **Create User Roles Wizard** (Creazione guidata di creazione ruoli utente), selezionare **Fabric Administrator** (amministratore delegato) come ruolo utente.
2. In **Members**, aggiungere l'account utente in Active Directory che si desidera utilizzare come amministratore delegato.
3. In **Scope**, selezionare i gruppi host a cui si desidera che l'amministratore delegato abbia accesso.
4. Creare un nuovo **account Esegui come** utilizzando le credenziali utente dell'amministratore delegato. Utilizzare queste credenziali per creare una connessione hypervisor in un secondo momento. Non utilizzare gli account con ruolo di amministratore principale.

### Installare la console VMM

Installare una console di System Center Virtual Machine Manager su ogni server con un Citrix Cloud Connector.

La versione della console deve corrispondere alla versione del server di gestione. Sebbene una console precedente possa connettersi al server di gestione, il provisioning dei VDA non riesce se le versioni sono diverse.

## Provisioning di Azure Stack HCI tramite SCVMM

Azure Stack HCI è una soluzione cluster di infrastruttura iperconvergente (HCI) che ospita i carichi di lavoro Windows e Linux virtualizzati e la relativa archiviazione in un ambiente ibrido locale.

I servizi ibridi di Azure migliorano il cluster dotandolo di funzionalità come il monitoraggio basato su cloud, il ripristino del sito e i backup delle macchine virtuali. È anche possibile ottenere una visione centrale di tutte le distribuzioni di Azure Stack HCI nel portale di Azure.

### Integrazione di Azure Stack HCI con SCVMM

Per integrare Azure Stack HCI con SCVMM, è prima necessario creare un cluster HCI di Azure Stack e quindi integrare quel cluster con SCVMM.

1. Per creare il cluster HCI di Azure Stack, vedere il documento Microsoft Connettersi e gestire la registrazione di Azure Stack HCI.
2. Per integrare il cluster HCI di Azure Stack con SCVMM, effettuare le seguenti operazioni:

   a) Accedere alla macchina preparata per ospitare il server SCVMM e installare SCVMM 2019 UR3 o versione successiva.

   > **Nota:**
   >
   > Installare la Administrator Console di SCVMM 2019 UR3 o versione successiva nella macchina virtuale del Cloud Connector.

   b) Nella pagina **Settings** (Impostazioni) della console VMM, creare un account Esegui come.

   c) Eseguire i seguenti comandi PowerShell con autorizzazioni amministrative nel server SCVMM per aggiungere il cluster HCI di Azure Stack come host:

   ```
   $runAsAccountName = 'Admin'
   $runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
   $hostGroupName = 'All Hosts'
   $hostGroup = Get-SCVMHostGroup -Name $hostGroupName
   $hostCluster = 'FQDN of Azure Stack HCI cluster'
   Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
       VMHostGroup
   $hostGroup -Credential $runAsAccount -RemoteConnectEnabled
       $true
   <!--NeedCopy-->
   ```

   d) È ora possibile visualizzare il cluster HCI di Azure Stack insieme ai nodi nella console VMM.

   e) Creare la connessione di hosting SCVMM nell'interfaccia **Full Configuration**.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione a Microsoft System Center Virtual Machine Manager.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

## Ambienti di virtualizzazione Nutanix

December 21, 2022

Seguire queste indicazioni quando si utilizza Nutanix Acropolis per fornire macchine virtuali nella distribuzione di Citrix Virtual Apps and Desktops. Il processo di configurazione include l'installazione e la registrazione del plug-in Nutanix nell'ambiente Citrix Virtual Apps and Desktops.

Per ulteriori informazioni, vedere la Guida all'installazione del plug-in Nutanix Acropolis MCS, disponibile presso il Portale di supporto Nutanix.

> **Importante:**
>
> Installare il plug-in Nutanix su tutti i Cloud Connector in cui Citrix DaaS deve creare una connessione host alla posizione risorsa che dispone di un hypervisor Nutanix.

### Installare e registrare il plug-in Nutanix

Completare la seguente procedura per installare e registrare il plug-in Nutanix su tutti i Cloud Connector. Utilizzare le funzioni **Manage > Full Configuration** (Gestisci > Configurazione completa) in Citrix Cloud per creare una connessione a Nutanix. Quindi creare un catalogo di macchine che utilizzi un'istantanea di un'immagine master creata nell'ambiente Nutanix.

> **Suggerimento:**
>
> Consigliamo di arrestare, quindi riavviare Citrix Host Service, Citrix Broker Service e Machine Creation Services quando si installa o si aggiorna il plug-in Nutanix.

Per informazioni sull'installazione del plug-in Nutanix, vedere il sito della documentazione di Nutanix.

Per ulteriori informazioni su come configurare gli ambienti di virtualizzazione Nutanix, vedere Configurare le posizioni risorsa.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione a Nutanix.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

## Soluzioni Nutanix Cloud e dei partner

April 14, 2023

Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) supporta la seguente soluzione Nutanix Cloud e dei partner:

- Nutanix Cloud Clusters su AWS

### Nutanix Cloud Clusters su AWS

Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) supporta Nutanix Cloud Clusters su AWS. I cluster Nutanix semplificano il modo in cui le applicazioni vengono eseguite su cloud privati o su più cloud pubblici. Per ulteriori informazioni su Nutanix Cloud Clusters su AWS, vedere Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Suggerimento:**
>
> Questo supporto offre le stesse funzionalità di un cluster locale Nutanix. È supportato solo un singolo cluster, *Prism Element*. Per ulteriori informazioni, vedere questa pagina.

### Requisiti

Per utilizzare Nutanix Clusters on AWS sono necessari i seguenti elementi:

- Un account Nutanix.
- Un account AWS con le seguenti autorizzazioni:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

### Creare un cluster Nutanix

Per creare un cluster Nutanix:

1. Accedere all'account Nutanix.
2. Individuare l'opzione **Nutanix cluster** (Cluster Nutanix) e fare clic su **Launch** (Avvia). Si apre la **console Nutanix**. Per ulteriori informazioni, consultare Introduzione a Nutanix Clusters on AWS.
3. Scegliere di creare un **nuovo VPC**.

Il processo di creazione del cluster potrebbe non riuscire con i seguenti errori:

- Il cluster non è stato creato in un determinato periodo di tempo. Eliminazione del cluster.
- Host Nutanix Cluster - Nodo `XXXXXXXXXX: Instance i-xxxxxxxxxxxx: disable network interface source/dest check error.`
- Host Nutanix Cluster - Nodo `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`

Se la creazione del cluster non è riuscita:

- Provare a ricrearne uno in un'altra regione.
- Assicurarsi di eliminare Nutanix CloudFormation Stack (CFS) prima di riprovare.

Oltre ad altre risorse, Nutanix CFS crea:

- 1 VPC denominato *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 subnet 10.0.128.0/24 e 10.0.129.0/24
- 1 gateway Internet
- 1 gateway NAT

Una volta creato il cluster, recuperare l'indirizzo del **Nutanix Prism**:

1. Andare alla **console Nutanix**.
2. In alto a destra nella console, passare il mouse sul link **Launch Prism Element** (Avvia Prism Element) e copiare l'URL.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione alle soluzioni Nutanix Cloud e dei partner.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

## Ambienti di virtualizzazione VMware

December 21, 2022

Seguire queste indicazioni se si utilizza VMware per fornire macchine virtuali.

Installare vCenter Server e gli strumenti di gestione appropriati. Non viene fornito alcun supporto per il funzionamento della modalità collegata vSphere vCenter.

Se si prevede di utilizzare Machine Creation Services (MCS), non disattivare la funzionalità Datastore Browser in vCenter Server (descritta in questo articolo di VMware). Se si disattiva questa funzionalità, MCS non funziona correttamente.

Per configurare gli ambienti di virtualizzazione VMware, vedere Configurare il tipo di risorsa.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.
- Per informazioni su come creare e gestire una connessione, vedere Connessione a VMware.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine
- Soluzione Azure VMware

# Soluzioni VMware Cloud e dei partner

October 30, 2023

Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) supporta le seguenti soluzioni VMware Cloud e dei partner:

- Soluzione Azure VMware (AVS)
- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

Utilizzare Citrix DaaS per migrare i carichi di lavoro Citrix locali basati su VMware alle rispettive soluzioni dei partner VMware.

## Integrazione con la soluzione Azure VMware (AVS)

Il servizio Citrix Virtual Apps and Desktops supporta AVS. AVS fornisce un'infrastruttura cloud contenente cluster vSphere creati dall'infrastruttura Azure. Sfruttare il servizio Citrix Virtual Apps and Desktops per utilizzare AVS per il provisioning del carico di lavoro VDA nello stesso modo in cui si utilizzerebbe vSphere negli ambienti on-premise.

### Configurazione del cluster AVS

Per abilitare il servizio Citrix Virtual Apps and Desktops per l'utilizzo di AVS, eseguire i seguenti passaggi in Azure:

- Richiedere una quota host
- Registrare il provider di risorse Microsoft.AVS
- Elenco di controllo di rete
- Creare un cloud privato della soluzione Azure VMware
- Accedere a un cloud privato della soluzione Azure VMware
- Configurare la rete per il cloud privato VMware in Azure
- Configurare DHCP per la soluzione Azure VMware
- Aggiungere un segmento di rete nella soluzione Azure VMware
- Verificare l'ambiente della soluzione Azure VMware

**Richiedere una quota host per i clienti del contratto Azure Enterprise** Nella pagina **Guida e supporto** del portale di Azure, selezionare **Nuova richiesta di supporto**e includere le seguenti informazioni:

- Tipo di problema: tecnico
- Sottoscrizione: selezionare la propria sottoscrizione
- Servizio: Tutti i servizi > Soluzione Azure VMware
- Risorsa: domanda generale
- Riepilogo: è necessaria capacità
- Tipo di problema: problemi di gestione della capacità
- Sottotipo di problema: richiesta del cliente per quota/capacità host aggiuntiva

Nel campo **Description** (Descrizione) del ticket di supporto, includere le seguenti informazioni nella scheda **Details** (Dettagli):

- POC o implementazione in produzione
- Nome regione
- Numero di host
- Eventuali altri dettagli

> **Nota:**
>
> AVS richiede un minimo di tre host e consiglia di utilizzare una ridondanza di N+1 host.

Dopo aver specificato i dettagli per il ticket di supporto, selezionare **Controlla e crea** per inviare la richiesta ad Azure.

**Registrare il provider di risorse Microsoft.AVS** Dopo aver richiesto la quota host, registrare il provider di risorse:

1. Accedere al portale di Azure.
2. Nel menu del portale di Azure, selezionare **Tutti i servizi**.
3. Nel menu **Tutti i servizi**, inserire la sottoscrizione e selezionare **Sottoscrizioni**.
4. Selezionare la sottoscrizione dall'elenco delle sottoscrizioni.
5. Selezionare **Provider di risorse** e inserire **Microsoft.AVS** nella barra di ricerca.
6. Se il provider di risorse non è registrato, selezionare **Registra**.

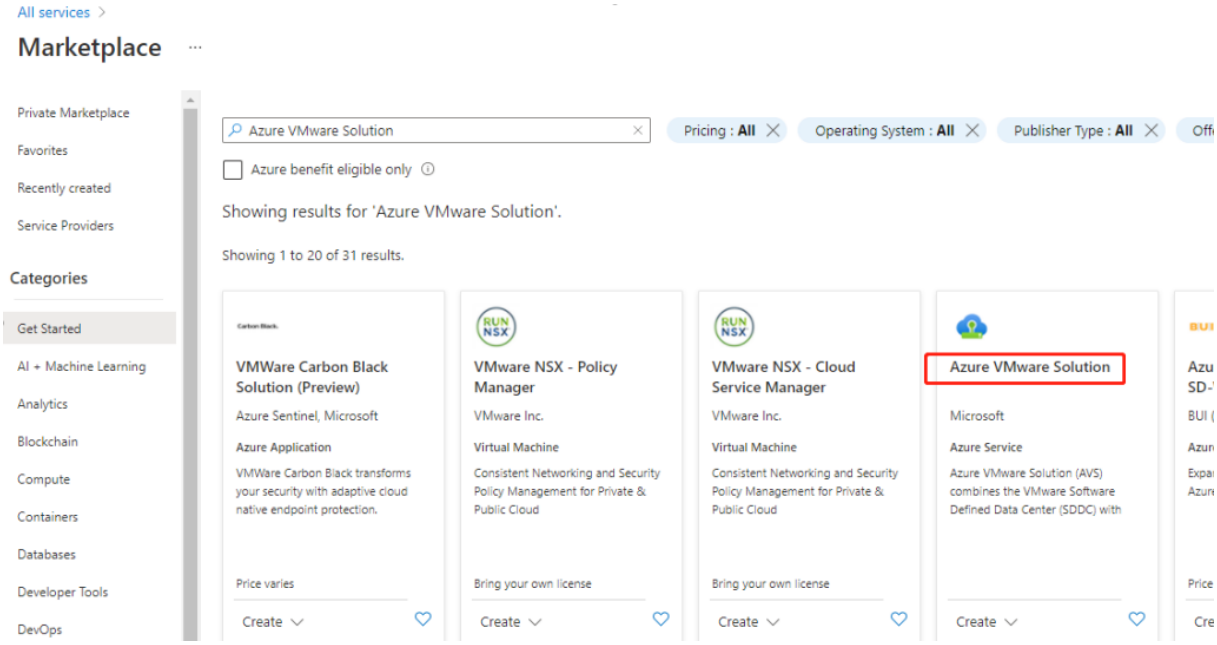
**Considerazioni sul networking** AVS offre servizi di networking che richiedono specifici intervalli di indirizzi di rete e porte firewall. Vedere Elenco di controllo per la pianificazione della rete per la soluzione Azure VMware per ulteriori informazioni.

**Creare un cloud privato della soluzione Azure VMware** Dopo aver considerato i requisiti di rete per l'ambiente, creare un cloud privato ASV:

1. Accedere al portale di Azure.

2. Selezionare **Crea una nuova risorsa**.
3. Nella casella di testo **Cerca nel Marketplace**, digitare *Soluzione Azure VMware* e selezionare **Soluzione Azure VMware** dall'elenco.




Immagine

Nella finestra della **soluzione Azure VMware**:

1. Selezionare **Create**.
2. Fare clic sulla scheda **Informazioni di base**.
3. Immettere i valori per i campi, utilizzando le informazioni nella tabella seguente:

| Campo | Valore |
|---|---|
| Sottoscrizione | Selezionare la sottoscrizione che si prevede di utilizzare per la distribuzione. Tutte le risorse in una sottoscrizione di Azure vengono fatturate insieme. |
| Gruppo di risorse | Selezionare il gruppo di risorse per il cloud privato. Un gruppo di risorse di Azure è un contenitore logico in cui vengono distribuite e gestite le risorse di Azure. In alternativa, è possibile creare un nuovo gruppo di risorse per il cloud privato. |
| Posizione | Selezionare una posizione, ad esempio "east us" (Stati Uniti orientali). Questa è la regione definita durante la fase di pianificazione. |

| Campo | Valore |
| --- | --- |
| Nome della risorsa | Fornire il nome del cloud privato della soluzione Azure VMware. |
| SKU | Selezionare AV36. |
| Host | Mostra il numero di host allocati per il cluster del cloud privato. Il valore predefinito è 3, che può essere aumentato o abbassato dopo la distribuzione. |
| Blocco di indirizzi | Fornire un blocco di indirizzi IP per il cloud privato. La notazione CIDR rappresenta la rete di gestione del cloud privato e verrà utilizzata per i servizi di gestione del cluster, come vCenter Server e NSX-T Manager. Utilizzare lo spazio degli indirizzi /22, ad esempio 10.175.0.0/22. L'indirizzo deve essere univoco e non sovrapporsi ad altre reti virtuali di Azure, oltre che alle reti on-premise. |
| Rete virtuale | Lasciare vuoto questo campo perché il circuito ExpressRoute della soluzione Azure VMware viene definito come passaggio successivo alla distribuzione. |

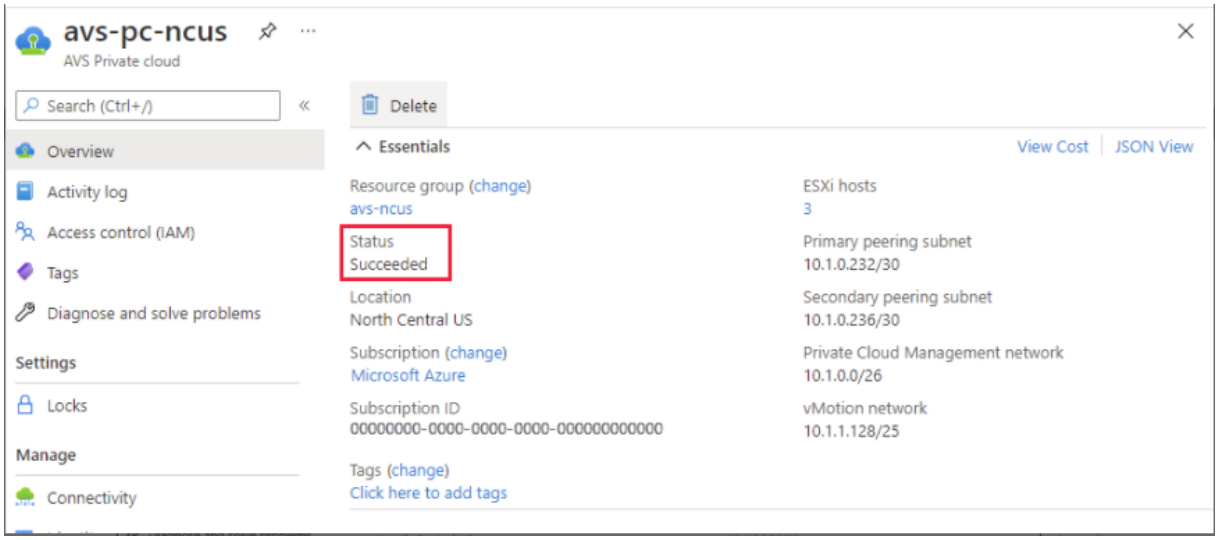
Nella schermata **Crea un cloud privato**:

1. Nel campo **Posizione**, selezionare la regione in cui si trova AVS; la regione del gruppo di risorse è la stessa della regione AVS.
2. Nel campo **SKU**, selezionare **Nodo AV36**.
3. Specificare un indirizzo IP nel campo **Blocco di indirizzi**. Ad esempio, 10.15.0.0/22.
4. Selezionare **Controlla e crea**.
5. Dopo aver esaminato le informazioni, fare clic su **Crea**.

> **Suggerimento:**
>
> La creazione di un cloud privato può richiedere 3-4 ore. L'aggiunta di un singolo host al cluster può richiedere 30-45 minuti.

Verificare che la distribuzione sia andata a buon fine. Andare al gruppo di risorse creato e selezionare il cloud privato. Quando lo **Stato** è **Operazione completata**, la distribuzione è completata.




**Accedere a un cloud privato della soluzione Azure VMware** Dopo aver creato un cloud privato, creare una macchina virtuale Windows e connettersi al vCenter locale del cloud privato.

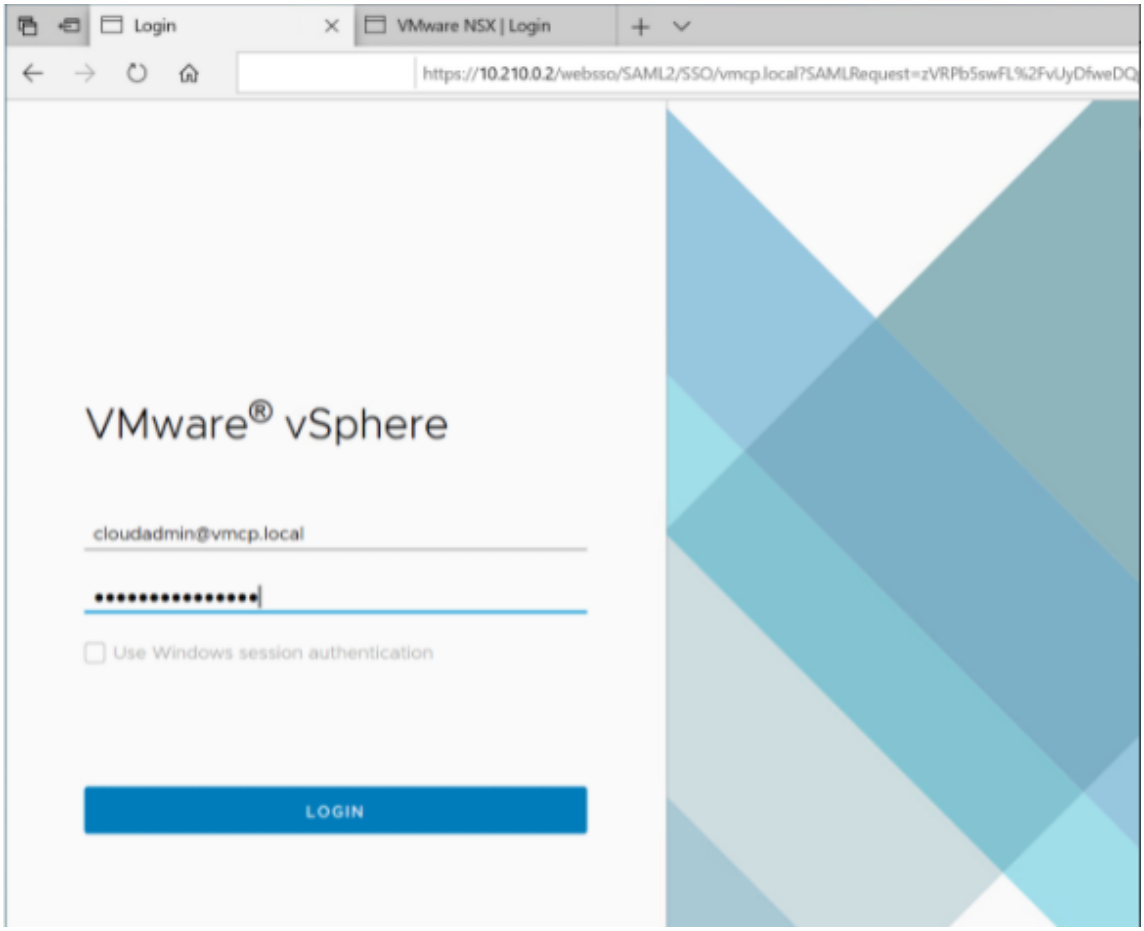
### Creare una nuova macchina virtuale Windows

1. Nel gruppo di risorse, selezionare **+ Aggiungi**, quindi cercare e selezionare **Microsoft Windows 10/2016/2019**.
2. Fare clic su **Create**.
3. Inserire le informazioni richieste, quindi selezionare **Controlla e crea**.
4. Una volta superata la convalida, selezionare **Crea** per avviare il processo di creazione delle macchine virtuali.

### Connettersi al vCenter locale del cloud privato

1. Accedere a **vSphere Client con VMware vCenter SSO** come amministratore cloud.

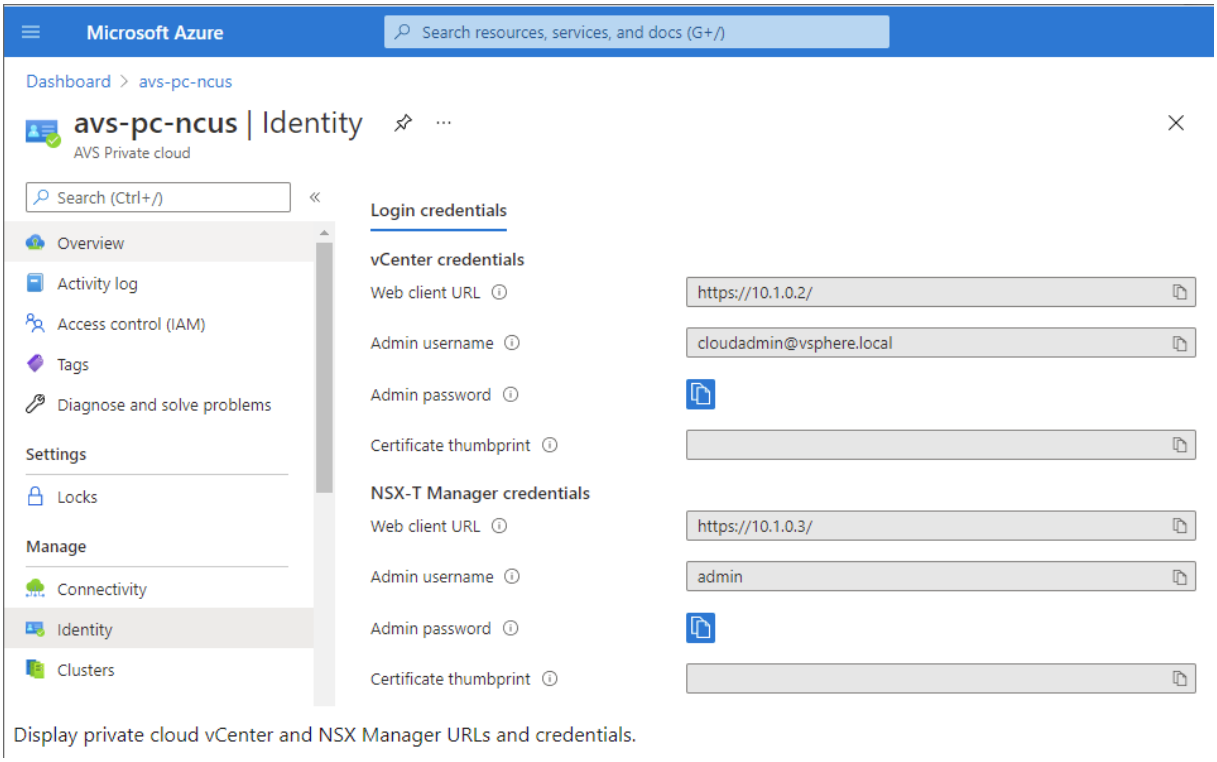
 




2. Nel portale di Azure, selezionare il cloud privato, quindi **Gestisci > Identità**.

Vengono visualizzati gli URL e le credenziali utente per il cloud privato vCenter e NSX-T Manager:



Display private cloud vCenter and NSX Manager URLs and credentials.

Dopo aver confermato gli URL e le credenziali utente:

1. Accedere alla macchina virtuale creata nel passaggio precedente e connettersi alla macchina virtuale.
2. Nella macchina virtuale Windows, aprire un browser e accedere agli URL vCenter e NSX-T Manager in due schede del browser. Nella scheda vCenter, inserire le credenziali utente *cloudadmin@vmcp.local* dal passaggio precedente.

**Configurare la rete per il cloud privato VMware in Azure** Dopo aver effettuato l'accesso a un cloud privato ASV, configurare la rete creando una rete virtuale e un gateway.

### Creare una rete virtuale

1. Accedere al portale di Azure.
2. Passare al gruppo di risorse creato in precedenza.
3. Selezionare **+ Aggiungi** per definire una nuova risorsa.
4. Nella casella di testo **Cerca nel Marketplace**, digitare *rete virtuale*. Trovare la risorsa di rete virtuale e selezionarla.
5. Nella pagina **Rete virtuale**, selezionare **Crea** per configurare la rete virtuale per il cloud privato.
6. Nella pagina **Crea rete virtuale**, inserire i dettagli della rete virtuale.
7. Nella scheda **Informazioni di base**, immettere un nome per la rete virtuale, selezionare la regione appropriata e fare clic su **Avanti: Indirizzi IP.**

8. Nella scheda **Indirizzi IP**, in Spazio indirizzi IPv4, immettere l'indirizzo creato in precedenza.

> **Importante:**
>
> Utilizzare un indirizzo che non si sovrapponga allo spazio degli indirizzi usato durante la creazione del cloud privato.

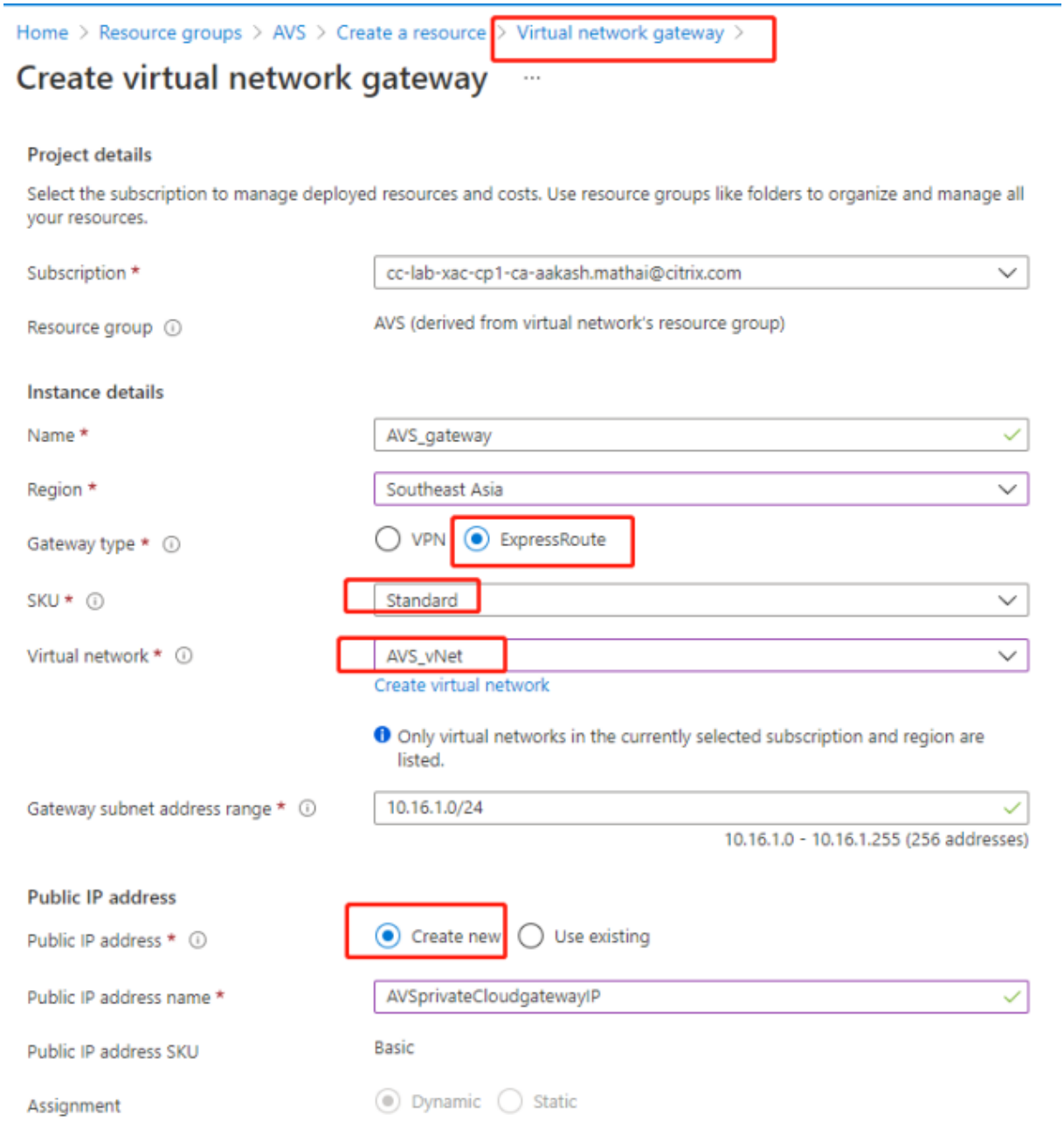
Dopo aver inserito lo spazio degli indirizzi:

1. Selezionare **+ Aggiungi subnet**.
2. Nella pagina **Aggiungi subnet**, assegnare alla subnet un nome e un intervallo di indirizzi appropriato.
3. Fare clic su **Aggiungi**.
4. Selezionare **Controlla e crea**.
5. Verificare le informazioni e fare clic su **Crea**. Una volta completata la distribuzione, la rete virtuale viene visualizzata nel gruppo di risorse.

**Creare un gateway di rete virtuale** Dopo aver creato una rete virtuale, creare un gateway di rete virtuale.

1. Nel gruppo di risorse, selezionare **+ Aggiungi** per aggiungere una nuova risorsa.
2. Nella casella di testo **Cerca nel Marketplace**, digitare *gateway di rete virtuale*. Trovare la risorsa di rete virtuale e selezionarla.
3. Nella pagina **Gateway di rete virtuale**, fare clic su **Crea**.
4. Nella scheda **Informazioni di base** della pagina **Crea gateway di rete virtuale**, fornire i valori per i campi.
5. Fare clic su **Controlla e crea**.



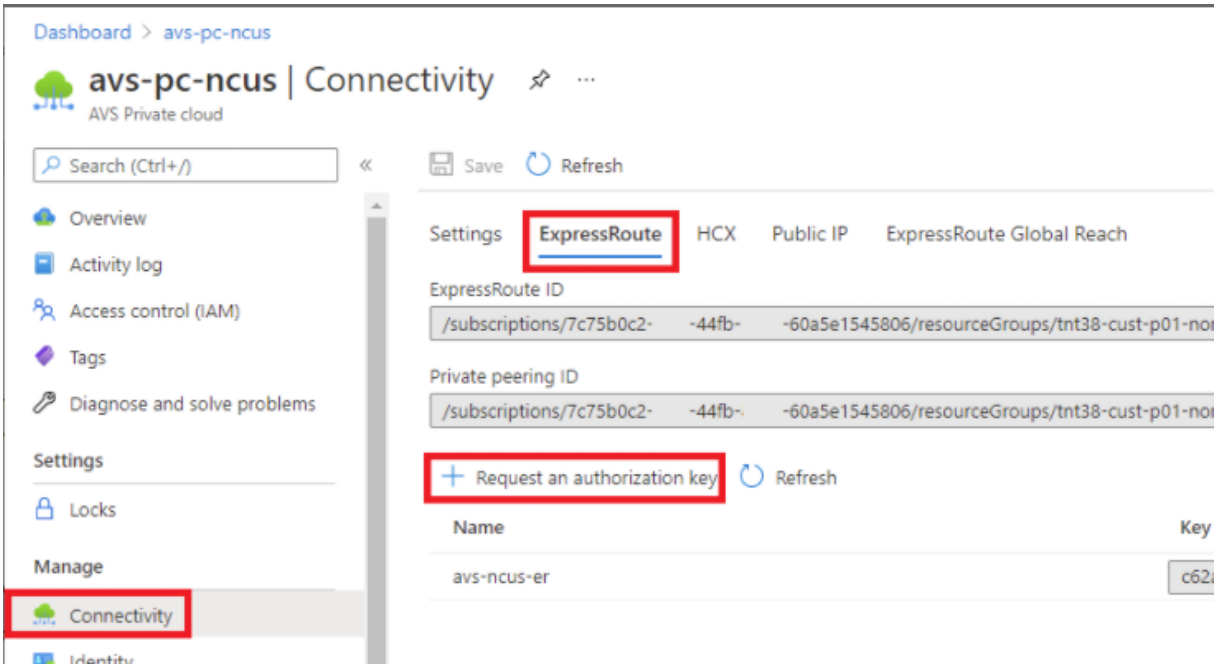

Dopo aver esaminato la configurazione del gateway di rete virtuale, fare clic su **Crea** per distribuire il gateway di rete virtuale.
Una volta completata la distribuzione, connettere la connessione **ExpressRoute** al gateway di rete virtuale contenente il cloud privato di Azure AVS.

**Connettere ExpressRoute al gateway di rete virtuale** Dopo aver distribuito un gateway di rete virtuale, aggiungere una connessione tra il gateway e il cloud privato di Azure AVS:

1. Richiedere una chiave di autorizzazione ExpressRoute.

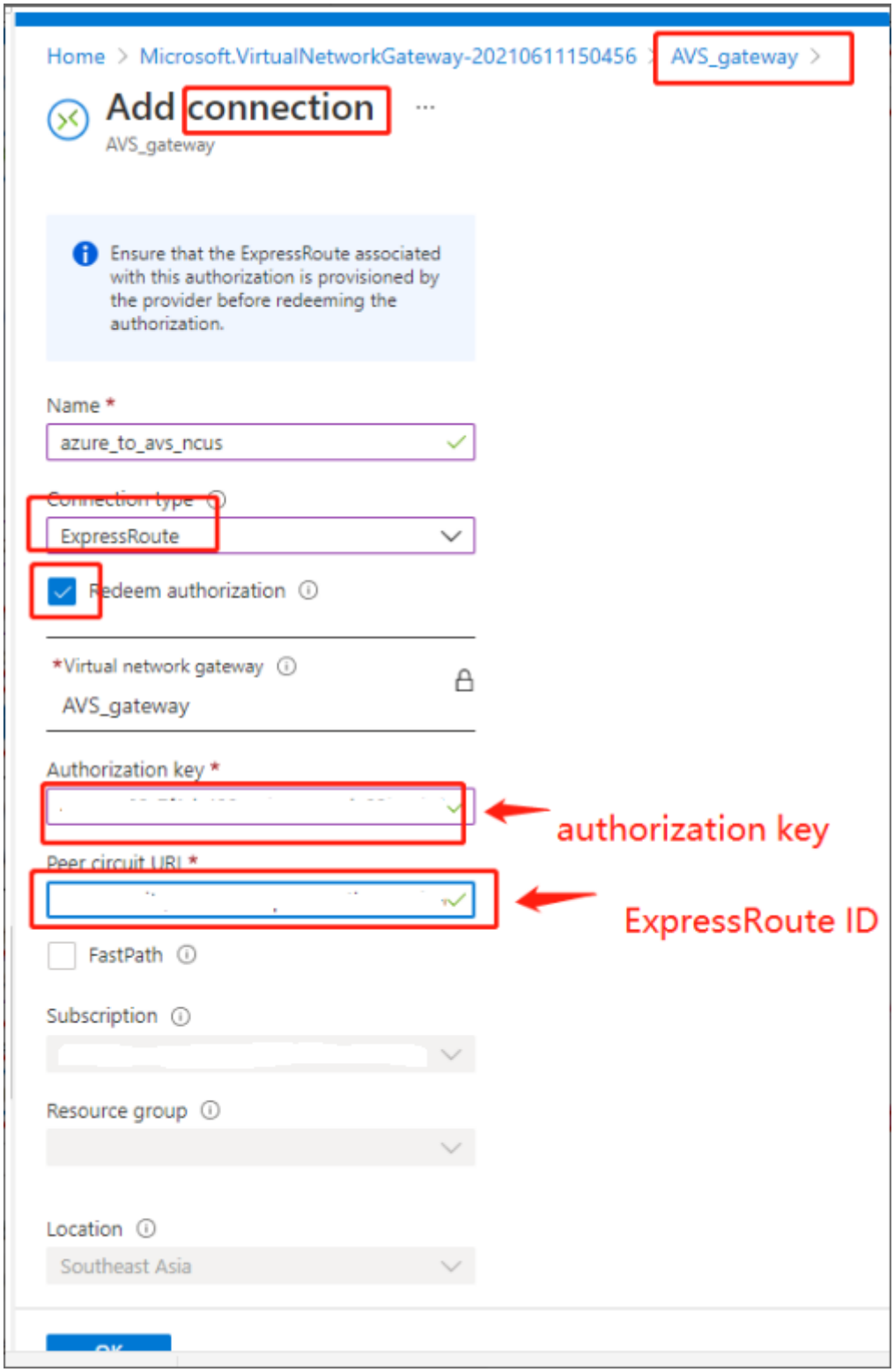
2. Nel portale di Azure, accedere al **cloud privato della soluzione Azure VMware**. Selezionare **Gestisci > Connettività > ExpressRoute** e quindi selezionare **+ Richiedi una chiave di autorizzazione**.




Dopo aver richiesto una chiave di autorizzazione:

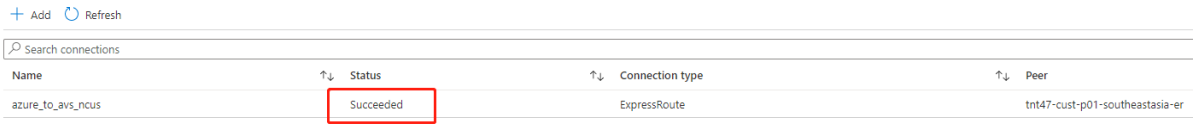
1. Inserire un nome per la chiave e fare clic su **Crea**. Potrebbero essere necessari circa 30 secondi per creare la chiave. Una volta creata, la nuova chiave viene visualizzata nell'elenco delle chiavi di autorizzazione per il cloud privato.
2. Copiare la **chiave di autorizzazione** e l'**ID ExpressRoute**. Saranno necessari per completare il processo di peering. La chiave di autorizzazione scompare dopo un po'di tempo, quindi copiarla non appena viene visualizzata.
3. Accedere al **gateway di rete virtuale** che si intende utilizzare e selezionare **Connessioni > + Aggiungi**.
4. Nella pagina **Aggiungi connessione**, fornire i valori per i campi e selezionare **OK**.




La connessione viene stabilita tra il circuito ExpressRoute e la rete virtuale:

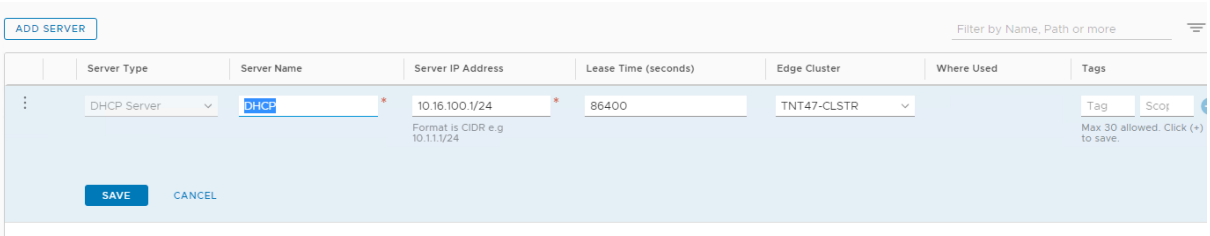
 




**Configurare DHCP per la soluzione Azure VMware** Dopo aver connesso ExpressRoute al gateway virtuale, configurare DHCP.

**Utilizzare NSX-T per ospitare il server DHCP** In NSX-T Manager:

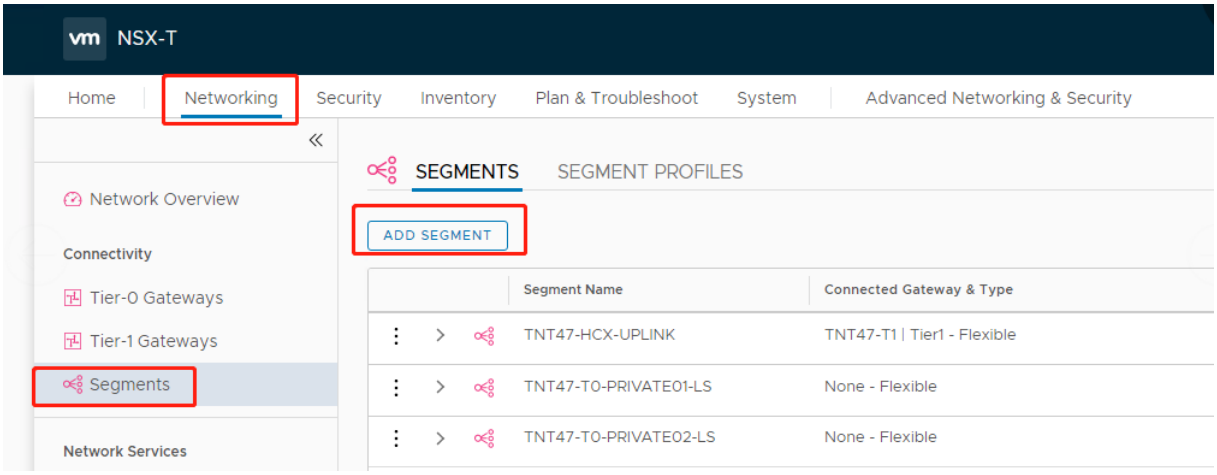
1. Selezionare **Networking > DHCP** (Rete > DHCP), quindi selezionare **Add Server** (Aggiungi server).
2. Selezionare **DHCP** come **Server Type** (Tipo di server), fornire il nome del server e l'indirizzo IP.
3. Fare clic su **Salva**.
4. Selezionare **Tier 1 Gateways** (Gateway di livello 1), selezionare i puntini di sospensione verticali sul gateway di livello 1, quindi selezionare **Edit** (Modifica).
5. Selezionare **No IP Allocation Set** (Nessun set di allocazione IP) per aggiungere una subnet.
6. Selezionare **DHCP Local Server** (Server locale DHCP) per **Type** (Tipo).
7. Per **DHCP Server** (Server DHCP), selezionare **Default DHCP** (DHCP predefinito), quindi fare clic su **Save** (Salva).
8. Fare di nuovo clic su **Save** (Salva) e quindi selezionare **Close Editing** (Chiudi modifica).




**Aggiungere un segmento di rete nella soluzione Azure VMware** Dopo aver configurato DHCP, aggiungere un segmento di rete.

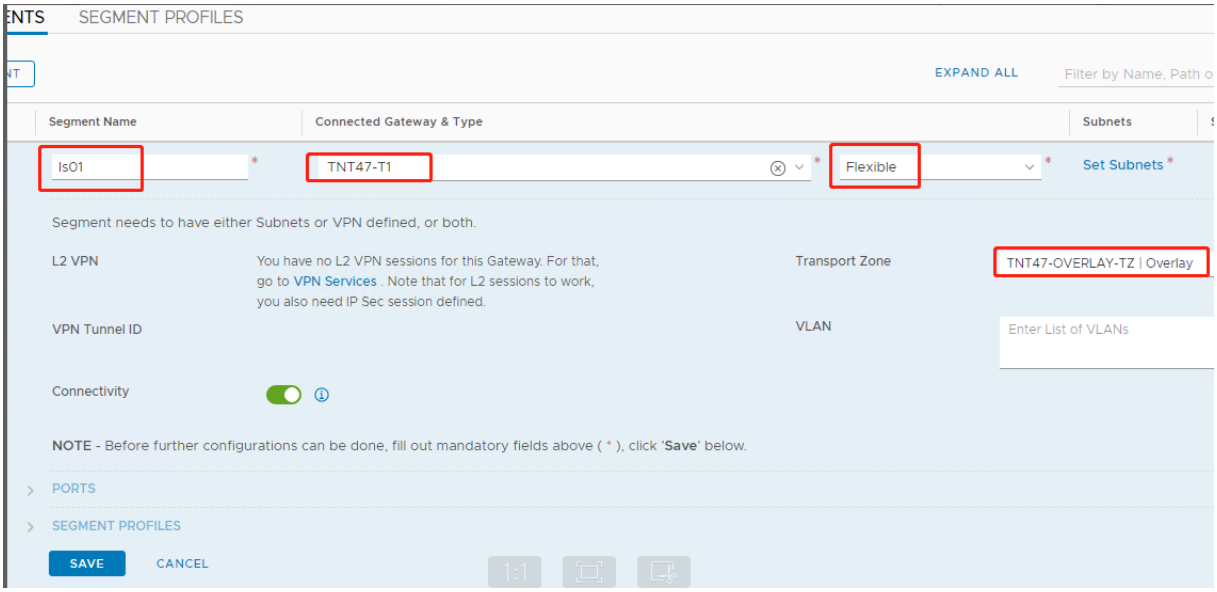
Per aggiungere un segmento di rete, in NSX-T Manager selezionare **Networking > Segments** (Rete > Segmenti), quindi fare clic su **Add Segment** (Aggiungi segmento).




Nella schermata **Segments profile** (Profilo segmenti):

1. Immettere un **nome** per il segmento.
2. Selezionare **Tier-1 Gateway (TNTxx-T1)** (Gateway di livello 1 [TNTxx-T1]) come **Connected Gateway (Gateway connesso)** e lasciare **Type** (Tipo) impostato su **Flexible** (Flessibile).
3. Selezionare la sovrapposizione preconfigurata **Transport Zone(TNTxx-OVERLAY-TZ)** (Zona di trasporto [TNTxx-OVERLAY-TZ]).
4. Fare clic su **Set Subnets** (Imposta subnet).



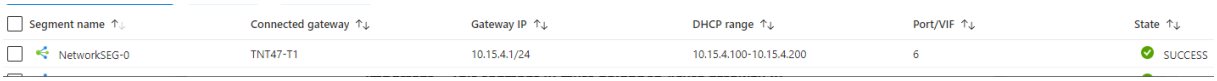

Nella sezione **Subnets** (Subnet):

1. Immettere l'indirizzo IP del gateway.
2. Selezionare **Add** (Aggiungi).

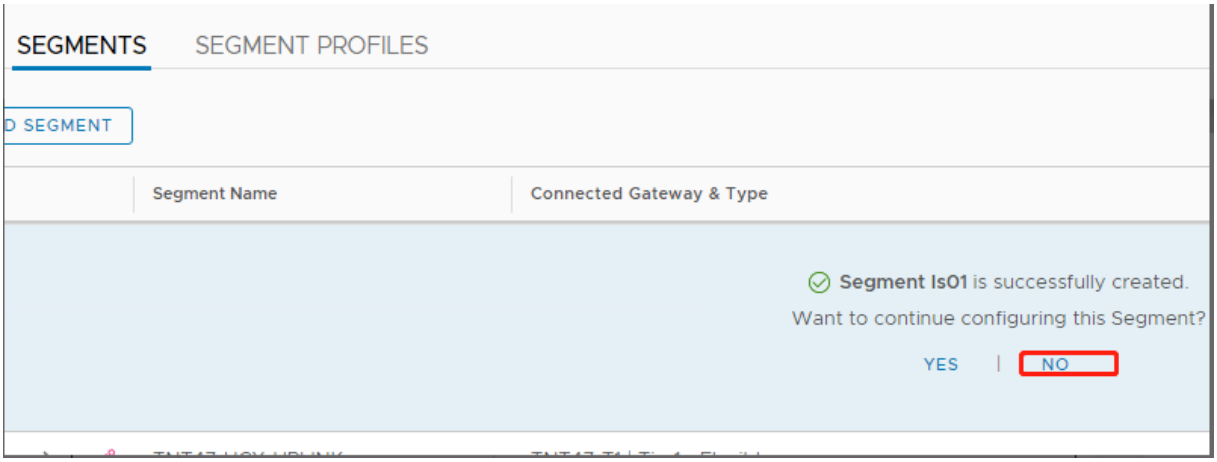
 

> **Importante:**
>
> Questo indirizzo IP del segmento deve appartenere all'indirizzo IP del gateway Azure, 10.15.0.0/22.

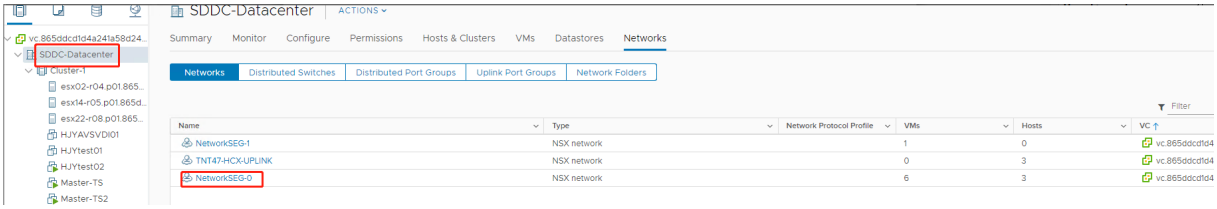
L'intervallo DHCP deve appartenere all'indirizzo IP del segmento:




Selezionare **No** per rifiutare l'opzione per continuare a configurare il segmento:




In vCenter, selezionare **Networking > SDDC-Datacenter** (Rete > SDDC-Datacenter):




**Verificare l'ambiente Azure AVS** Configurare una connessione diretta e un connettore nel gruppo di risorse di Azure:

Verificare la connessione con le credenziali vCenter:

## Google Cloud VMware Engine

Citrix DaaS consente di migrare i carichi di lavoro Citrix locali basati su VMware a Google Cloud VMware Engine.

### Configurazione di Google Cloud VMware Engine

La seguente procedura descrive come acquisire e configurare un cluster su Google Cloud VMware Engine.

#### Accedere al portale di VMware Engine

1. In **Google Cloud Console**, fare clic sul menu di navigazione.
2. Nella sezione **Computing**, fare clic su **VMware Engine** per aprire VMware Engine in una nuova scheda del browser.

**Requisiti per creare il primo cloud privato** È necessario avere accesso a Google Cloud VMware Engine, alla quota di nodi VMware Engine disponibile e a un ruolo IAM appropriato. Preparare i seguenti requisiti prima di continuare a creare il cloud privato:

1. Richiedere l'accesso all'API e la quota dei nodi. Per ulteriori informazioni, consultare Richiedere l'accesso all'API e la quota.
2. Annotare gli intervalli di indirizzi che si desidera utilizzare per le appliance di gestione VMware e la rete di distribuzione HCX. Per ulteriori informazioni, vedere Requisiti di rete.
3. Ottenere il ruolo IAM Amministratore servizio VMware Engine.

#### Creare il primo cloud privato

1. Accedere al portale di VMware Engine.
2. Nella home page di VMware Engine, fare clic su **Create a private cloud** (Crea un cloud privato). Sono elencati la posizione di hosting e i tipi di nodi hardware.
3. Selezionare il numero di nodi per il cloud privato. Sono necessari almeno tre nodi.
4. Immettere un intervallo CIDR (Classless Inter-Domain Routing) per la rete di gestione VMware.
5. Immettere un intervallo CIDR per la rete di distribuzione HCX.

   > **Importante:**
   >
   > L'intervallo CIDR non deve sovrapporsi a nessuna delle subnet on-premise o cloud. L'intervallo CIDR deve essere pari o superiore a /27.

6. Selezionare **Review and create** (Rivedi e crea).
7. Controllare le impostazioni. Per modificare le impostazioni, fare clic su **Back** (Indietro).
8. Fare clic su **Create** (Crea) per iniziare a creare il cloud privato.

Man mano che VMware Engine crea il nuovo cloud privato, distribuisce diversi componenti VMware e imposta i criteri iniziali di scalabilità automatica per i cluster nel cloud privato. La creazione di un cloud privato può richiedere da 30 minuti a 2 ore. Una volta completato il provisioning, si riceverà un' e-mail.

**Configurare il gateway VPN di Google Cloud VMware Engine** Per stabilire una connettività iniziale a Google Cloud VMware Engine, è possibile utilizzare un gateway VPN. Si tratta di una VPN client basata su OpenVPN che consente di connettersi al Software Defined Data Center (SDDC) VMware vCenter ed eseguire qualsiasi configurazione iniziale richiesta.

Prima di distribuire il gateway VPN, configurare l'intervallo di **servizi Edge** per l'area geografica in cui viene distribuito l'SDDC. A questo scopo:

1. Accedere al portale **Google Cloud VMware Engine** e andare a **Rete > Impostazioni regionali**. Fare clic su **Aggiungi area geografica**.
2. Scegliere l'area geografica in cui viene distribuito l'SDDC e abilitare l'**accesso a Internet** e il **servizio IP pubblico**.
3. Indicare l'intervallo dei servizi Edge di cui si è preso nota durante la pianificazione e fare clic su **Invia**. L'abilitazione di questi servizi richiede 10-15 minuti.

   Al completamento della procedura, i servizi Edge vengono visualizzati come **Abilitati** nella pagina Impostazioni regionali. L'abilitazione di queste impostazioni consente di allocare gli IP pubblici all'SDDC, che è un requisito per la distribuzione di un gateway VPN.

Per distribuire un gateway VPN:

1. Nel portale **Google Cloud VMware Engine**, andare a **Rete > Gateway VPN**. Fare clic su **Create New VPN Gateway** (Crea nuovo gateway VPN).
2. Fornire il nome per il gateway VPN e la subnet client riservati durante la pianificazione. Fare clic su **Next** (Avanti).
3. Selezionare gli utenti a cui concedere l'accesso alla VPN. Fare clic su **Next** (Avanti).
4. Specificare le reti che devono essere accessibili tramite VPN. Fare clic su **Next** (Avanti).
5. Viene visualizzata una schermata di riepilogo. Verificare le selezioni e fare clic su **Submit** (Invia) per creare il gateway VPN. La pagina VPN Gateways (Gateway VPN) viene visualizzata con lo stato del nuovo gateway VPN **Creating** (Creazione in corso).
6. Dopo che lo stato viene modificato in **Operational** (Operativo), fare clic sul nuovo gateway VPN.
7. Fare clic su **Download my VPN configuration** (Scarica la mia configurazione VPN) per scaricare un file ZIP contenente profili OpenVPN preconfigurati per il gateway VPN. Sono disponibili profili per la connessione tramite UDP/1194 e TCP/443. Scegliere la propria preferenza e importala in Open VPN, quindi connettersi.
8. Andare a **Resources** (Risorse) e seleziona il proprio SDDC.

#### Connettere la VPN

1. Stabilire una connessione da punto a sito tra la propria rete locale e il cloud privato tramite la configurazione VPN Gateway. Vedere Configurare il gateway VPN di Google Cloud VMware Engine.
2. Caricare la configurazione della VPN scaricata in Configurare il gateway VPN di Google Cloud VMware Engine.
3. Importarla nel proprio client VPN, ad esempio OpenVPN Connect.

Per ulteriori informazioni, vedere Connessione tramite VPN.

#### Creare la prima subnet

**Accedere a NSX-T Manager dal portale VMware Engine** Il processo di creazione di una subnet avviene in NSX-T, a cui si accede tramite VMware Engine. Effettuare le seguenti operazioni per accedere a NSX-T Manager.

1. Accedere al portale **Google Cloud VMware Engine**.
2. Dalla navigazione principale, andare a **Resources** (Risorse).
3. Fare clic sul **nome del cloud privato** corrispondente al cloud privato in cui si desidera creare la subnet.
4. Nella pagina dei dettagli del cloud privato, fare clic sulla scheda **vSphere Management Network** (Rete di gestione di vSphere).
5. Fare clic sul **nome di dominio completo** corrispondente a NSX-T Manager.
6. Quando richiesto, inserire le proprie credenziali di accesso. Se si è configurato vIDM e lo si è connesso a un'origine identità, ad esempio Active Directory, utilizzare invece le credenziali dell'origine identità.

   > **Promemoria:**
   >
   > È possibile recuperare le credenziali generate dalla pagina dei dettagli del cloud privato.

**Configurare il servizio DHCP per la subnet** Prima di poter creare una subnet, configurare un servizio DHCP:

In NSX-T Manager:

1. Andare a **Networking > DHCP**. La dashboard di rete mostra che il servizio DHCP crea un gateway Tier-0 e uno Tier-1.
2. Per iniziare il provisioning di un server DHCP, fare clic su **Add Server** (Aggiungi server).

3. Selezionare **DHCP** come **Server Type** (Tipo di server), fornire il nome del server e l'indirizzo IP.
4. Fare clic su **Save** (Salva) per creare il servizio DHCP.

Effettuare le seguenti operazioni per collegare questo servizio DHCP al gateway Tier-1 pertinente. Un gateway Tier-1 predefinito è già fornito dal servizio DHCP:

1. Selezionare **Tier 1 Gateways** (Gateway di livello 1), selezionare i puntini di sospensione verticali sul gateway di livello 1, quindi selezionare **Edit** (Modifica).
2. Nel campo **IP Address Management** (Gestione indirizzi IP), selezionare **No IP Allocation Set** (Nessuna allocazione IP impostata).
3. Selezionare **DHCP Local Server** (Server locale DHCP) per **Type** (Tipo).
4. Selezionare il server DHCP creato per il **server DHCP**.
5. Fare clic su **Salva**.
6. Fare clic su **Close Editing** (Chiudi modifica).

È ora possibile creare un segmento di rete in NSX-T. Per ulteriori informazioni sul DHCP in NSX-T, vedere la documentazione di VMware per DHCP.

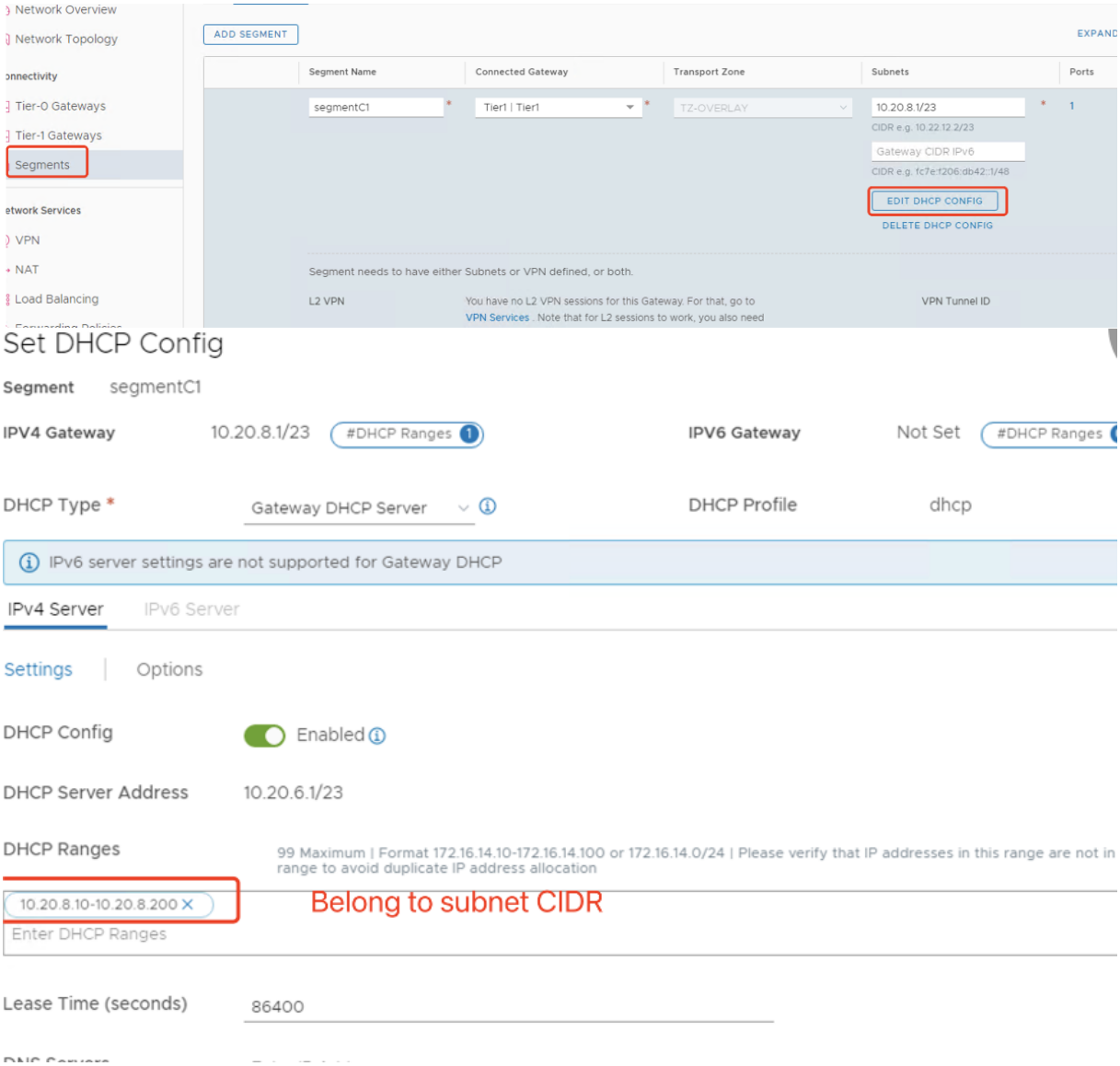
**Creare un segmento di rete in NSX-T** Per le macchine virtuali dei carichi di lavoro si creano subnet come segmenti di rete NSX-T per il cloud privato:

1. In NSX-T Manager, andare a **Networking > Segments** (Networking > Segmenti).
2. Fare clic su **Add Segment** (Aggiungi segmento).
3. Immettere un nome per il segmento.
4. Selezionare **Tier-1** come **Connected Gateway** (Gateway connesso) e lasciare Type (Tipo) impostato su **Flexible** (Flessibile).
5. Fare clic su **Set Subnets** (Imposta subnet).
6. Fare clic su **Add Subnets** (Aggiungi subnet).
7. Immettere l'intervallo di subnet nel campo **Gateway IP/Prefix Length** (Lunghezza del prefisso/IP gateway). Specificare l'intervallo di subnet con **.1** come ultimo ottetto. Ad esempio, **10.12.2.1/24**.
8. Specificare gli intervalli DHCP e fare clic su **ADD** (AGGIUNGI).
9. In **Transport Zone** (Zona di trasporto), selezionare **TZ-OVERLAY** dall'elenco a discesa.
10. Fare clic su **Salva**. Ora è possibile selezionare questo segmento di rete in vCenter quando si crea una macchina virtuale.

In una determinata area geografica, è possibile impostare al massimo 100 route uniche da VMware Engine alla rete VPC utilizzando l'accesso ai servizi privati. Ciò include, ad esempio, gli intervalli di indirizzi IP per la gestione del cloud privato, i segmenti di rete del carico di lavoro NSX-T e gli intervalli di indirizzi IP di rete HCX. Questo limite include tutti i cloud privati nella regione.

> **Nota:**
>
> A causa di un problema di configurazione di Google Cloud, è necessario configurare più volte l'impostazione dell'intervallo DHCP. Pertanto, assicurarsi di configurare l'impostazione dell'intervallo DHCP dopo la configurazione di Google Cloud. Fare clic su **EDIT DHCP CONFIG** (MODIFICA CONFIGURAZIONE DHCP) per configurare gli intervalli DHCP.

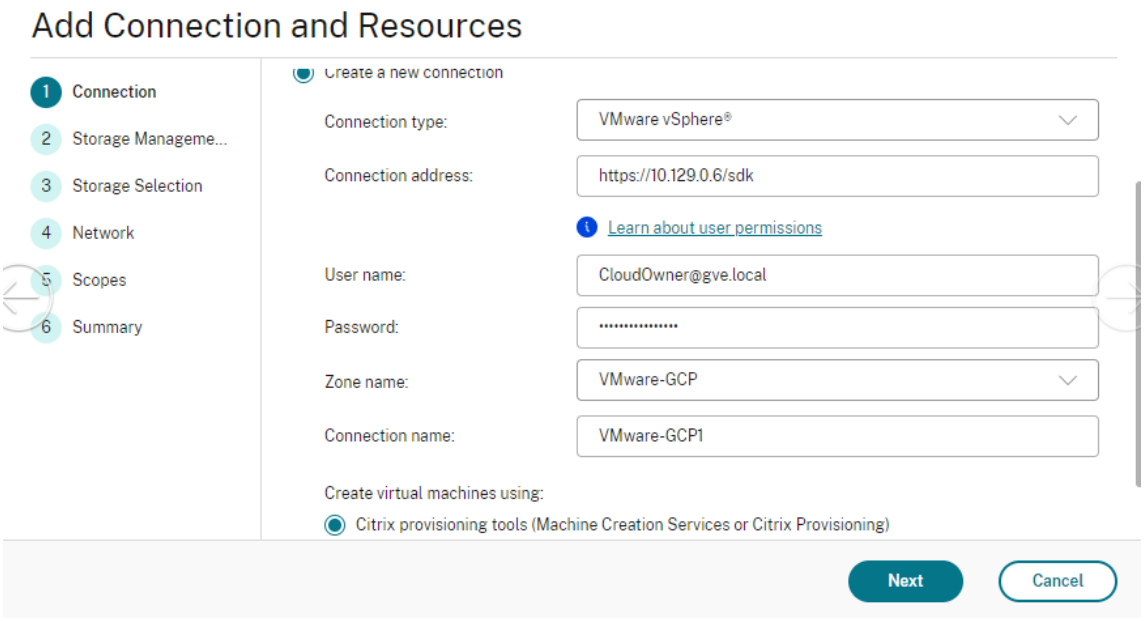



### Creare la connessione VMware a Google Cloud in Citrix Studio

1. Creare una macchina in vCenter e installare il Cloud Connector nella macchina.
2. Avviare Citrix Studio.

3. Selezionare il nodo di hosting e fare clic su **Add Connection and Resources** (Aggiungi connessione e risorse).
4. Nella schermata **Connessione**, selezionare **Create a new Connection** (Crea una nuova connessione) e i seguenti dettagli:




   a) Selezionare **VMware vSphere** come **Connection type** (Tipo di connessione).
   b) In **Connection address** (Indirizzo di connessione), inserire l'indirizzo IP privato di vCenter.
   c) Inserire le credenziali di vCenter.
   d) Immettere un nome per la connessione.
   e) Scegliere lo strumento per creare macchine virtuali.

5. Nella schermata **Network** (Rete), selezionare la subnet creata nel server NSX-T.
6. Completare la procedura guidata.

## VMware Cloud on Amazon Web Services (AWS)

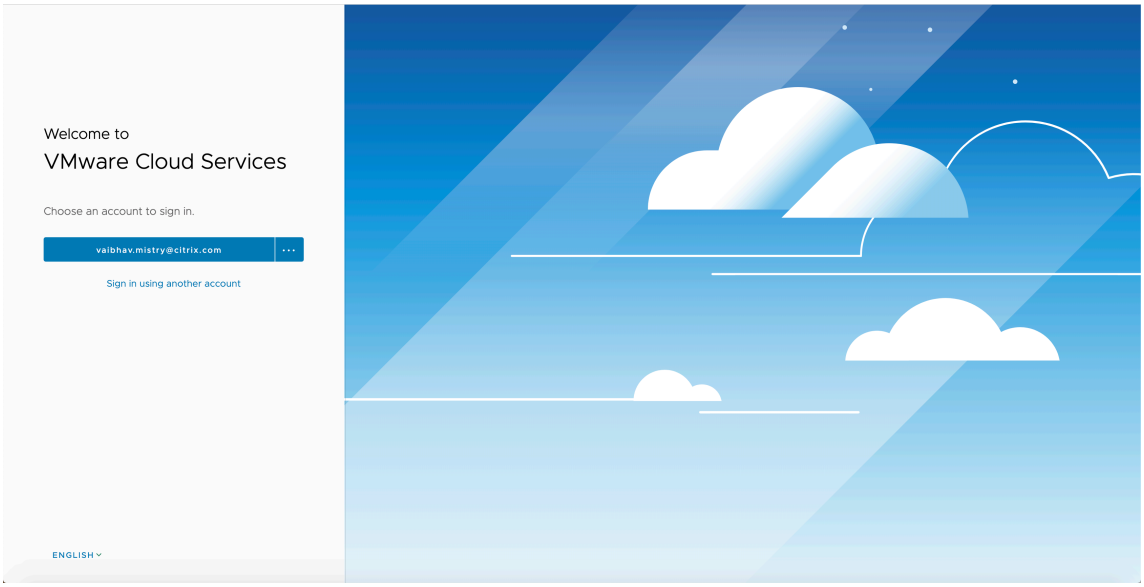
VMware Cloud on Amazon Web Services (AWS) consente di migrare i carichi di lavoro Citrix on-premise basati su VMware nel cloud AWS e l'ambiente principale Citrix Virtual Apps and Desktops in Citrix DaaS.

Questo articolo descrive la procedura per configurare VMware Cloud on AWS.

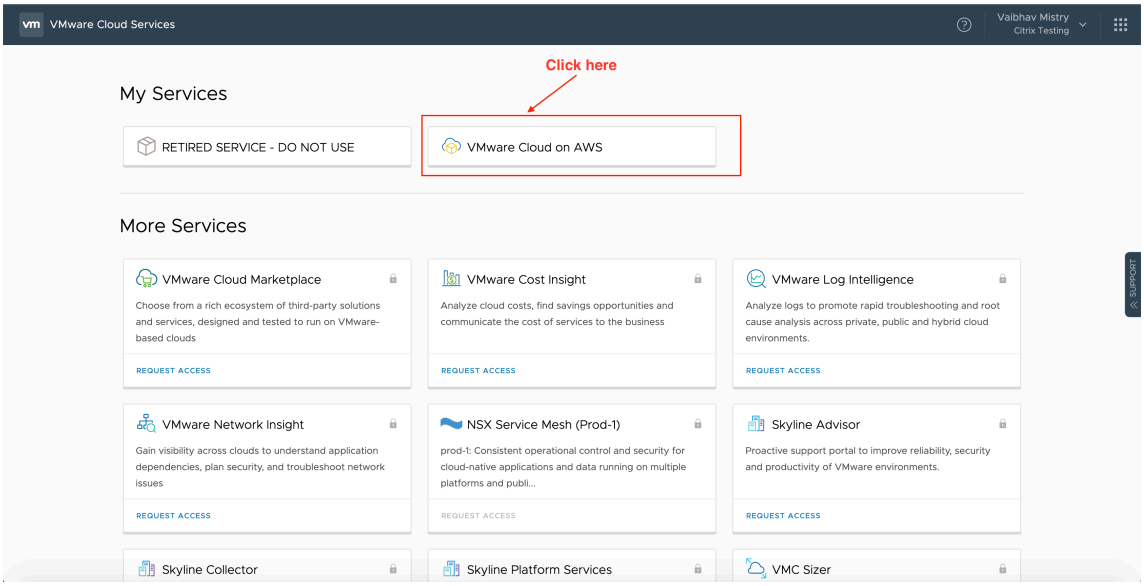
### Accedere all'ambiente VMware Cloud

1. Accedere ai servizi VMware Cloud utilizzando l'URL https://console.cloud.vmware.com/.

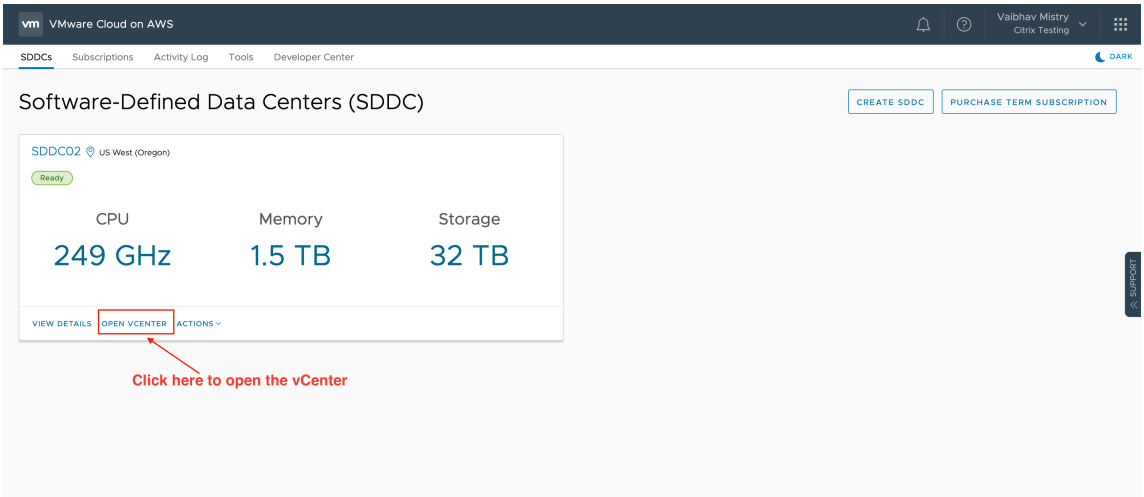



2. Fare clic su **VMware Cloud on AWS**. Viene visualizzata la pagina Software-Defined Data Centers (SDDC) (Software-Defined Data Center [SDDC]).

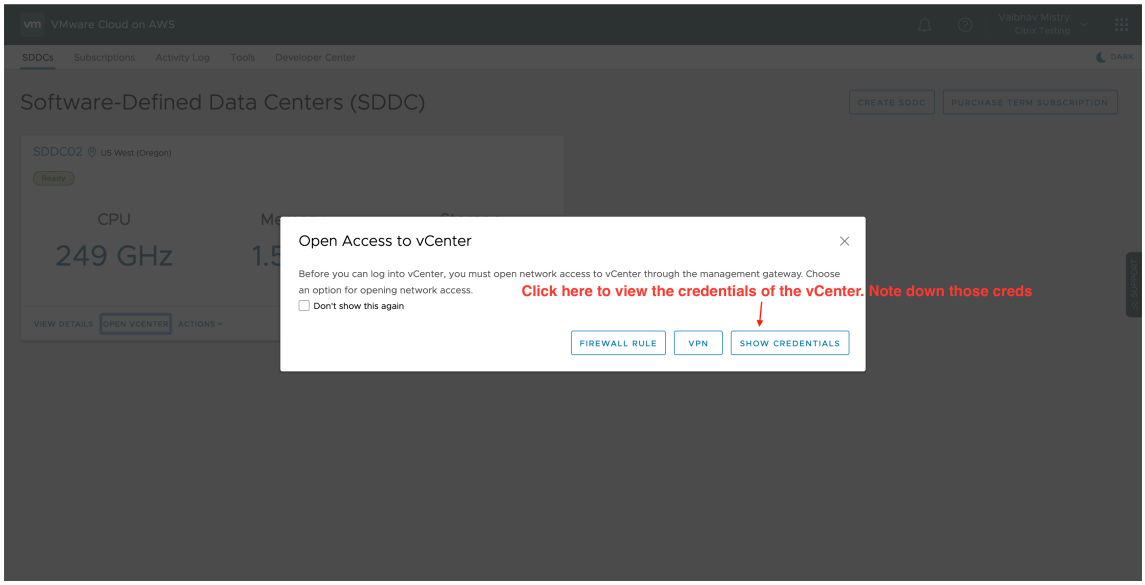



3. Fare clic su **OPEN VCENTER** (APRI VCENTER) e quindi fare clic su **SHOW CREDENTIALS** (MOSTRA CREDENZIALI). Prendere nota delle credenziali per usarle in seguito.



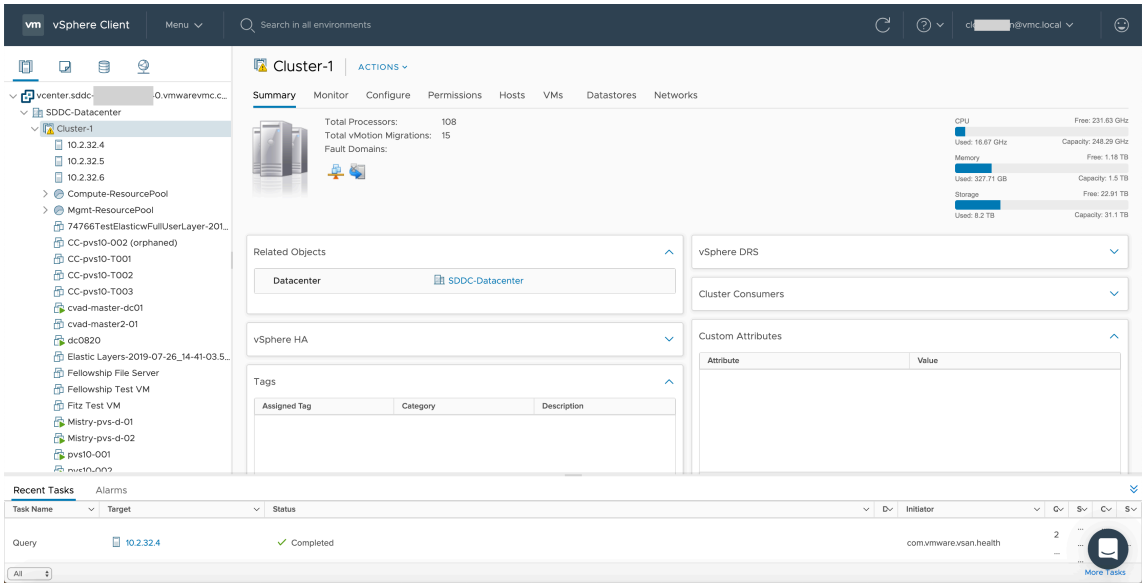

(Apri vCenter)




(Mostra credenziali)

4. Aprire un browser Web e immettere l'URL del Web Client vSphere.
5. Inserire le credenziali come indicato e fare clic su **Login** (Accedi). La pagina Web del client vSphere è simile all'ambiente on-premise.

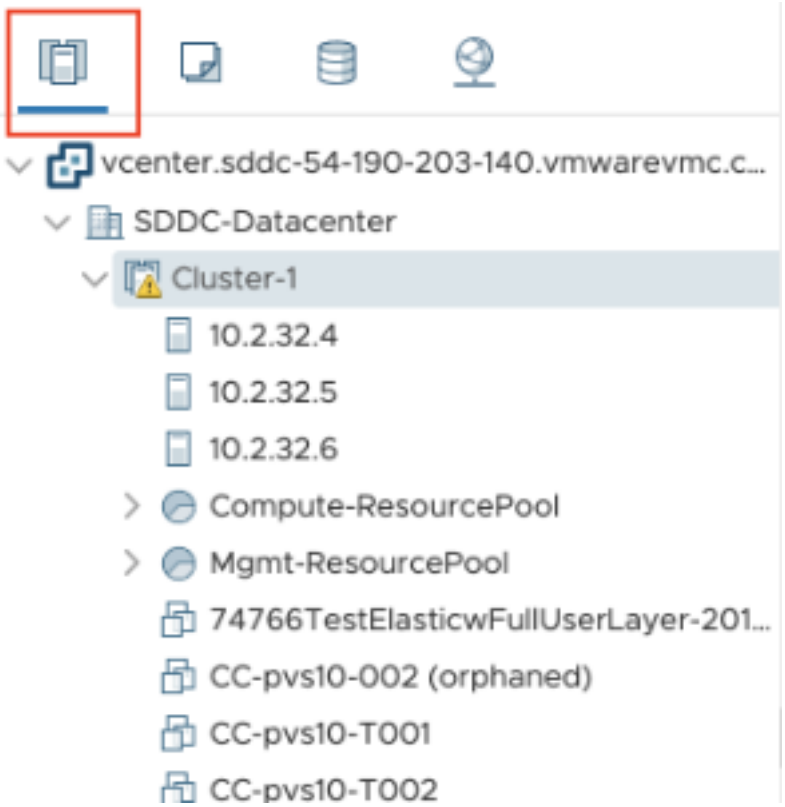
 




### Informazioni sull'ambiente VMware Cloud

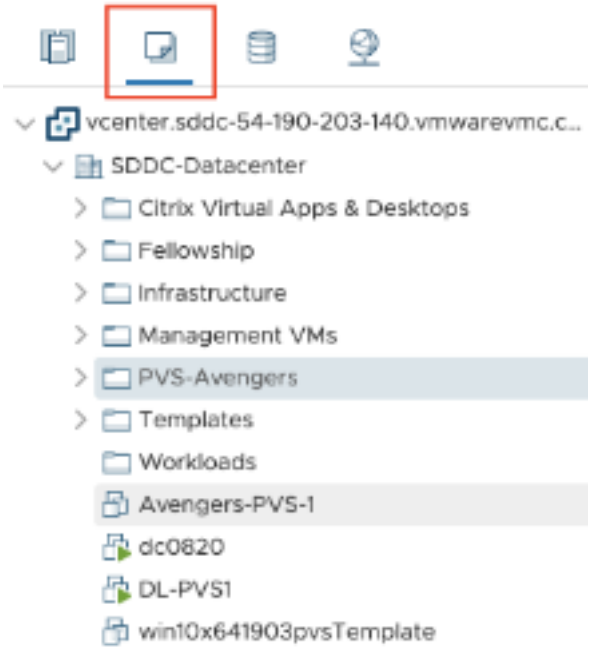
Sono disponibili quattro visualizzazioni sulla pagina Web del client vSphere.

- Visualizzazione host e cluster: non è possibile creare un nuovo cluster, ma l'amministratore del cloud può creare più pool di risorse.



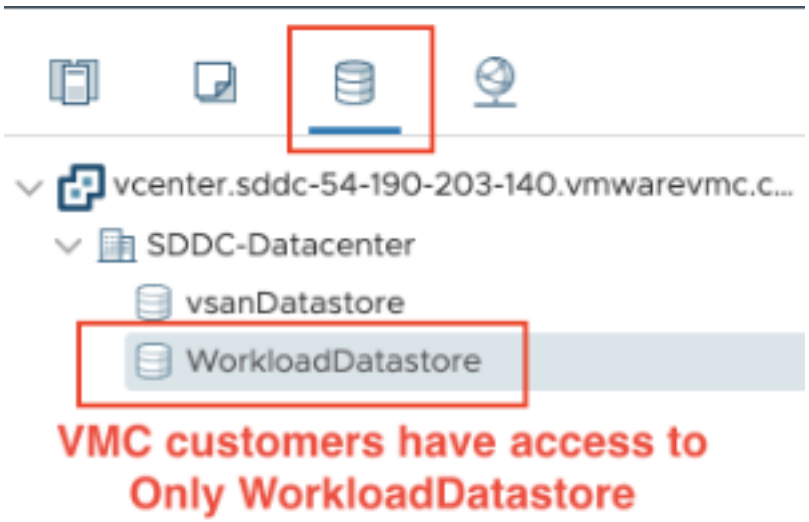

 

- Visualizzazione macchine virtuali e modelli: l'amministratore del cloud può creare molte cartelle.

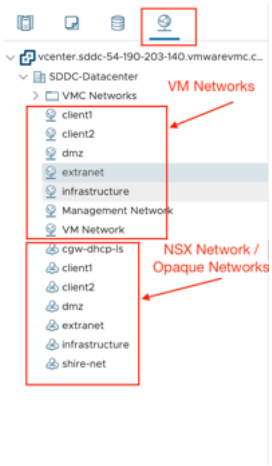



- Visualizzazione archiviazione: selezionare l'archiviazione **WorkloadDatastore** quando si aggiunge un'unità di hosting in Citrix Studio, perché si ha accesso solo all'archivio dati dei carichi di lavoro.




- Visualizzazione rete: le icone sono diverse per le reti VMware Cloud e le reti opache.




Dopo aver configurato il cluster, fare riferimento agli ambienti di virtualizzazione VMware per l'aggiunta di connessioni e risorse.

### Passaggi successivi

- Per una semplice distribuzione Proof of Concept (POC), installare un VDA su una macchina che distribuirà app o desktop agli utenti.

- Per informazioni su come creare e gestire una connessione, vedi Connessione a soluzioni cloud e partner VMware.
- Esaminare tutti i passaggi del processo di installazione e configurazione.

### Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

## Considerazioni su dimensioni e scalabilità per i Cloud Connector

March 3, 2023

Quando si valuta il servizio Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) in termini di dimensionamento e scalabilità, prendere in considerazione tutti i componenti. Esaminare e verificare la configurazione dei Citrix Cloud Connector e dello StoreFront in base alle proprie esigenze specifiche. Fornire risorse insufficienti per il dimensionamento e la scalabilità influisce negativamente sulle prestazioni della distribuzione.

> **Nota:**
>
> Queste raccomandazioni si applicano a Citrix DaaS Standard per Azure oltre che a Citrix DaaS.

Questo articolo fornisce dettagli sulle capacità massime testate, oltre a consigli sulle procedure consigliate per la configurazione della macchina Cloud Connector. I test sono stati eseguiti su distribuzioni configurate con StoreFront e Local Host Cache (LHC).

Le informazioni fornite si applicano alle distribuzioni in cui ogni posizione risorsa contiene carichi di lavoro VDI o carichi di lavoro RDS. Per le posizioni risorsa che contengono carichi di lavoro misti di VDI e RDS insieme, contattare Citrix Consulting Services.

Cloud Connector collega i carichi di lavoro a Citrix DaaS nei seguenti modi:

- Fornisce un proxy per la comunicazione tra i VDA e Citrix DaaS
- Fornisce un proxy per la comunicazione tra Citrix DaaS e Active Directory (AD) e gli hypervisor
- Nelle distribuzioni che includono server StoreFront, Cloud Connector funge da broker di sessione temporaneo durante le interruzioni del cloud, fornendo agli utenti un accesso continuato alle risorse

È importante che i Cloud Connector siano dimensionati e configurati correttamente per soddisfare le proprie esigenze specifiche.

Ogni set di Cloud Connector viene assegnato a una posizione risorsa (nota anche come zona). Una posizione risorsa è una separazione logica che specifica quali risorse comunicano con il set specifico di Cloud Connector. È richiesta almeno una posizione risorsa per dominio per comunicare con Active Directory (AD).

Ogni catalogo di macchine e ogni connessione di hosting vengono assegnati a una posizione risorsa.

Per le distribuzioni con più di una posizione risorsa, assegnare i cataloghi delle macchine e i VDA alle posizioni risorsa per ottimizzare la capacità della cache host locale (LHC) di mediare le connessioni durante le interruzioni. Per ulteriori informazioni sulla creazione e la gestione delle posizioni risorsa, consultare Connettersi a Citrix Cloud. Per prestazioni ottimali, configurare i Cloud Connector su connessioni a bassa latenza a VDA, server AD e hypervisor.

### Processori e archiviazione consigliati

Per prestazioni simili a quelle osservate in questi test, utilizzare processori moderni che supportano le estensioni SHA. Le estensioni SHA riducono il carico crittografico sulla CPU. I processori consigliati includono:

- Advanced Micro Devices (AMD) Zen e processori più recenti
- Intel Ice Lake e processori più recenti

I processori consigliati funzionano in modo efficiente. È possibile utilizzare processori meno recenti; tuttavia ciò potrebbe comportare un maggiore carico della CPU. Consigliamo di aumentare il numero di vCPU per compensare questo problema.

I test descritti in questo articolo sono stati eseguiti con processori AMD EPYC e Intel Cascade Lake.

I Cloud Connector hanno un carico crittografico elevato durante la comunicazione con il cloud. I Cloud Connector che utilizzano processori con estensioni SHA presentano un carico inferiore sulla CPU, espresso da un minore utilizzo della CPU da parte del Local Security Authority Subsystem Service (LSASS) di Windows.

Citrix consiglia di utilizzare archiviazione moderna con adeguate operazioni I/O al secondo (IOPS), in particolare per le implementazioni che utilizzano LHC. Le unità a stato solido (SSD) sono consigliate, ma non sono necessari livelli di archiviazione cloud premium. Sono necessari IOPS più elevate per gli scenari LHC in cui il Cloud Connector esegue una piccola copia del database. Questo database viene aggiornato regolarmente con le modifiche alla configurazione del sito e fornisce funzionalità di intermediazione alla posizione risorsa in caso di interruzioni di Citrix Cloud.

### Configurazione di elaborazione consigliata per Local Host Cache

La cache host locale (LHC) fornisce l'alta disponibilità consentendo la continuazione delle operazioni di intermediazione delle connessioni in una distribuzione quando un Cloud Connector non è in grado

di comunicare con Citrix Cloud.

I Cloud Connector eseguono Microsoft SQL Express Server LocalDB, che viene installato automaticamente quando si installa il Cloud Connector. La configurazione della CPU di Cloud Connector, in particolare il numero di core disponibili per SQL Express Server LocalDB, influisce direttamente sulle prestazioni LHC. Il numero di core della CPU disponibili per SQL Server Express Server LocalDB influisce sulle prestazioni LHC ancora di più rispetto all'allocazione della memoria. Questo sovraccarico della CPU viene osservato solo in modalità LHC quando Citrix DaaS non è raggiungibile e il broker LHC è attivo. Per qualsiasi implementazione che utilizza LHC, Citrix consiglia quattro core per socket, con un minimo di quattro core della CPU per Cloud Connector. Per informazioni sulla configurazione delle risorse di elaborazione per SQL Express Server LocalDB, vedere Limiti della capacità di elaborazione in base alla versione di SQL Server.

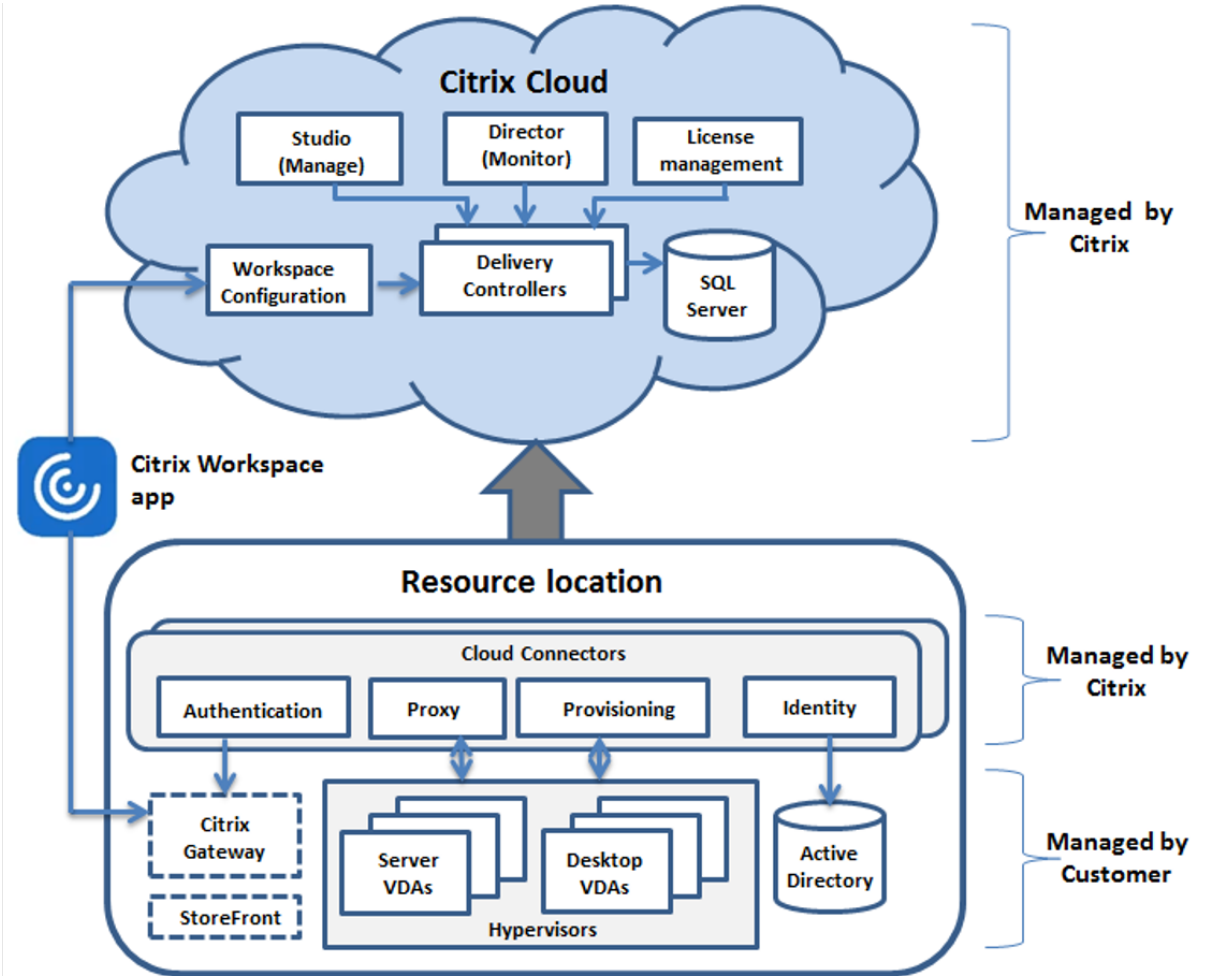
Se le risorse di calcolo disponibili per SQL Express Server LocalDB sono configurate in modo errato, i tempi di sincronizzazione della configurazione potrebbero essere aumentati e le prestazioni durante le interruzioni potrebbero essere ridotte. In alcuni ambienti virtualizzati, la capacità di elaborazione potrebbe dipendere dal numero di processori logici e non dai core della CPU.

### Riepilogo dei risultati dei test

Tutti i risultati di questo riepilogo si basano sui risultati di un ambiente di test configurato come indicato nelle sezioni dettagliate di questo articolo. I risultati illustrati qui si riferiscono a una singola posizione di risorsa. Configurazioni di sistema diverse potrebbero produrre risultati diversi.

Questa illustrazione fornisce una panoramica grafica della configurazione testata.




Questa tabella fornisce una guida rapida al dimensionamento della posizione risorsa. 10k è il massimo per una singola posizione risorsa. Vedi Limiti per informazioni sui limiti di localizzazione delle risorse.

> **Nota:**
>
> Il superamento del limite può causare problemi di connettività e prestazioni durante un'interruzione. Pertanto, non superare il limite consigliato in quanto ciò può portare a VDA non registrati.

I risultati si basano su test interni di Citrix. Le configurazioni descritte sono state testate con carichi di lavoro diversi, inclusi test di lancio delle sessioni ad alto tasso e tempeste di registrazioni.

| | Medio | Grande | Massimo |
|---|---|---|---|
| VDA | 1000 VDI o 250 RDS | 5000 VDI o 500 RDS | 10.000 VDI o 1000 RDS |
| Connessioni hosting | 20 | 40 | 40 |

| | Medio | Grande | Massimo |
|---|---|---|---|
| **CPU per i Connector** | 4 vCPU | 4 vCPU | 8 vCPU |
| **Memoria per i Connector** | 6 GB | 8 GB | 10 GB |

### Metodologia dei test

Sono stati condotti test per aggiungere carico e misurare le prestazioni dei componenti dell'ambiente. I componenti sono stati monitorati raccogliendo dati sulle prestazioni e sulle tempistiche delle procedure, come tempo di accesso e tempo di registrazione. In alcuni casi, sono stati utilizzati strumenti di simulazione proprietari di Citrix per simulare VDA e sessioni. Questi strumenti sono progettati per far funzionare i componenti Citrix allo stesso modo dei VDA e delle sessioni tradizionali, senza gli stessi requisiti di risorse necessari per ospitare sessioni e VDA reali. I test sono stati condotti sia in modalità cloud brokering che in modalità LHC per scenari con Citrix StoreFront.

I consigli per il dimensionamento dei Cloud Connector in questo articolo si basano sui dati raccolti da questi test.

Sono stati eseguiti i seguenti test:

- **Tempesta di avvio della sessione/accesso alla sessione:** un test che simula periodi di accesso ad alto volume.
- **Tempesta di registrazioni VDA:** un test che simula periodi con un elevato volume di registrazioni VDA. Ad esempio, dopo un ciclo di aggiornamento o la transizione tra la modalità cloud brokering e la modalità cache host locale.
- **Tempesta di azione alimentazione VDA:** un test che simula un elevato volume di azioni di alimentazione dei VDA.

### Scenari e condizioni di test

Questi test sono stati eseguiti con LHC configurato. Per ulteriori informazioni sull'utilizzo di LHC, vedere l'articolo Cache host locale. LHC richiede un server StoreFront on-premise. Per informazioni dettagliate su StoreFront, consultare la documentazione del prodotto StoreFront.

Consigli per le configurazioni StoreFront:

- Se si dispone di più posizioni risorsa con un singolo server o gruppo di server StoreFront, abilitare l'opzione di controllo dello stato avanzata per lo store StoreFront. Consultare i requisiti di StoreFront nell'articolo Cache host locale.

- Per velocità di avvio delle sessioni più elevate, utilizzare un gruppo di server StoreFront. Consultare Configurare i gruppi di server nella documentazione del prodotto StoreFront.

Condizioni del test:

- I requisiti di CPU e memoria sono solo per il sistema operativo di base e i servizi Citrix. Le app e i servizi di terze parti potrebbero richiedere risorse aggiuntive.
- I VDA sono macchine virtuali o fisiche che eseguono Citrix Virtual Delivery Agent.
- Per tutti i VDA testati è stata impostata la gestione dell'alimentazione utilizzando Citrix DaaS.
- Sono stati testati carichi di lavoro da 1000 a 10.000 VDI e 250-1000 server RDS con 1000-20000 sessioni.
- Le sessioni RDS sono state testate fino a 20.000 per posizione risorsa.
- I test sono stati eseguiti utilizzando un solo Cloud Connector sia durante le normali operazioni che durante le interruzioni. Citrix consiglia di utilizzare almeno due Cloud Connector per un'elevata disponibilità. In modalità di interruzione, viene utilizzato solo uno dei connettori per le registrazioni e l'intermediazione dei VDA.
- I test sono stati eseguiti con Cloud Connector configurato con processori Intel Cascade Lake.
- Le sessioni sono state avviate tramite un singolo server Citrix StoreFront.
- I test di avvio delle sessioni con interruzione LHC sono stati condotti dopo la nuova registrazione delle macchine.

I conteggi delle sessioni RDS sono una raccomandazione e non un limite. Verificare il limite di sessioni RDS nel proprio ambiente.

> **Nota:**
>
> Il numero di sessioni e la frequenza di avvio sono più importanti per RDS del conteggio dei VDA.

#### Carichi di lavoro medi

Questi carichi di lavoro sono stati testati con 4 vCPU e 6 GB di memoria.

| Carichi di lavoro di prova | Condizioni del sito | Ora di registrazione del VDA | Utilizzo di CPU e memoria alla registrazione | Durata del test di avvio | Utilizzo di CPU e memoria all'avvio della sessione | Velocità di avvio |
|---|---|---|---|---|---|---|
| 1000 VDI | Online | 5 minuti | CPU massima = 36%, CPU media = 33%, memoria massima = 5,3 GB | 2 minuti | CPU massima = 29%, CPU media = 27%, memoria massima = 3,7 GB | 500 al minuto |
| 1000 VDI | Interruzione | 4 minuti | CPU massima = 11%, CPU media = 10%, memoria massima = 4,5 GB | 2 minuti | CPU massima = 42%, CPU media = 28%, memoria massima = 4,0 GB | 500 al minuto |
| 250 RDS, 5000 sessioni | Online | 3 minuti | CPU massima = 14%, CPU media = 4%, memoria massima = 3,5 GB | 9 minuti | CPU massima = 46%, CPU media = 21%, memoria massima = 3,7 GB | 555 al minuto |
| 250 RDS, 5000 sessioni | Interruzione | 3 minuti | CPU massima = 15%, CPU media = 5%, memoria massima = 3,7 | 9 minuti | CPU massima = 51%, CPU media = 32%, memoria massima = 4,2 GB | 555 al minuto |

**Carichi di lavoro grandi**

Questi carichi di lavoro sono stati testati con 4 vCPU e 8 GB di memoria.

| Carichi di lavoro di prova | Condizioni del sito | Ora di registrazione del VDA | Utilizzo di CPU e memoria alla registrazione | Durata del test di avvio | Utilizzo di CPU e memoria all'avvio della sessione | Velocità di avvio |
|---|---|---|---|---|---|---|
| 5000 VDI | Online | 3-4 minuti | CPU massima = 45%, CPU media = 25%, memoria massima = 7,0 GB | 5 minuti | CPU massima = 75%, CPU media = 55%, memoria massima = 7,0 GB | 1000 al minuto |
| 5000 VDI | Interruzione | 4-6 minuti | CPU massima = 15%, CPU media = 5%, memoria massima = 7,5 GB | 5 minuti | CPU massima = 45%, CPU media = 40%, memoria massima = 7,5 GB | 1000 al minuto |
| 500 RDS, 10.000 sessioni | Online | 3 minuti | CPU massima = 45%, CPU media = 25%, memoria massima = 7,0 GB | 10 minuti | CPU massima = 75%, CPU media = 55%, memoria massima = 7,0 GB | 1000 al minuto |

| Carichi di lavoro di prova | Condizioni del sito | Ora di registrazione del VDA | Utilizzo di CPU e memoria alla registrazione | Durata del test di avvio | Utilizzo di CPU e memoria all'avvio della sessione | Velocità di avvio |
|---|---|---|---|---|---|---|
| 500 RDS, 10.000 sessioni | Interruzione | 3 minuti | CPU massima = 15%, CPU media = 5%, memoria massima = 7,5 | 10 minuti | CPU massima = 45%, CPU media = 40%, memoria massima = 7,5 GB | 1000 al minuto |

**Carichi di lavoro massimi**

Questi carichi di lavoro sono stati testati con 8 vCPU e 10 GB di memoria.

| Carichi di lavoro di prova | Condizioni del sito | Ora di registrazione del VDA | Utilizzo di CPU e memoria alla registrazione | Durata del test di avvio | Utilizzo di CPU e memoria all'avvio della sessione | Velocità di avvio |
|---|---|---|---|---|---|---|
| 10.000 VDI | Online | 3-4 minuti | CPU massima = 85%, CPU media = 10%, memoria massima = 8,5 GB | 7 minuti | CPU massima = 66%, CPU media = 28%, memoria massima = 7,0 GB | 1400 al minuto |

| Carichi di lavoro di prova | Condizioni del sito | Ora di registrazione del VDA | Utilizzo di CPU e memoria alla registrazione | Durata del test di avvio | Utilizzo di CPU e memoria all'avvio della sessione | Velocità di avvio |
|---|---|---|---|---|---|---|
| 10.000 VDI | Interruzione | 4-5 minuti | CPU massima = 90%, CPU media = 17%, memoria massima = 8,2 GB | 5 minuti | CPU massima = 90%, CPU media = 45%, memoria massima = 8,5 GB | 2000 al minuto |
| 1000 RDS, 20.000 sessioni | Online | 1-2 minuti | CPU massima = 60%, CPU media = 20%, memoria massima = 8,6 GB | 17 minuti | CPU massima = 66%, CPU media = 25%, memoria massima = 6,8 GB | 1200 al minuto |
| 1000 RDS, 20.000 sessioni | Interruzione | 3-4 minuti | CPU massima = 22%, CPU media = 10%, memoria massima = 8,5 | 21 minuti | CPU massima = 90%, CPU media = 50%, memoria massima = 7,5 GB | 1000 al minuto |

> **Nota:**
>
> I carichi di lavoro mostrati di seguito sono i carichi di lavoro massimi consigliati per una posizione risorsa. Per supportare carichi di lavoro più grandi, aggiungere altre posizioni risorsa.

**Utilizzi delle risorse di sincronizzazione della configurazione**

Il processo di sincronizzazione della configurazione mantiene i Cloud Connector aggiornati con Citrix DaaS. Gli aggiornamenti vengono inviati automaticamente ai Cloud Connector per assicurare che i Cloud Connector siano pronti a subentrare nell'intermediazione in caso di interruzione. La sincronizzazione della configurazione aggiorna il database LHC, SQL Express Server LocalDB. Il processo importa i dati in un database temporaneo, quindi passa a quel database una volta completata l'importazione. Ciò garantisce che ci sia sempre un database LHC pronto a subentrare.

L'utilizzo di CPU, memoria e disco viene temporaneamente aumentato durante l'importazione dei dati nel database temporaneo.

Risultati dei test:

- **Tempo di importazione dei dati:** 7-10 minuti
- **Utilizzo della CPU:**
  - massimo = 25%
  - medio = 15%
- **Utilizzo della memoria:**
  - massimo = 9 GB
  - aumento di circa 2-3 GB
- **Utilizzo del disco:**
  - Picco di lettura del disco di 4 MB/s
  - Picco di scrittura su disco di 18 MB/s
  - Picco di scrittura su disco di 70 MB/s durante il download e la scrittura di file di configurazione xml
  - Picco di lettura del disco di 4 MB/s al completamento dell'importazione
- **Dimensioni del database LHC:**
  - File del database di 400-500 MB
  - Database dei log di 200-300 MB

Condizioni del test:

- Test eseguito su un processore AMD EPYC con 8 vCPU
- Il database di configurazione del sito importato era destinato a un ambiente con un totale di 80.000 VDA e 300.000 utenti (tre turni di 100.000 utenti) per tutto il sito
- Il tempo di importazione dei dati è stato testato in una posizione risorsa con 10.000 VDI

Considerazioni aggiuntive sull'utilizzo delle risorse:

- Durante l'importazione vengono scaricati i dati completi di configurazione del sito. Questo download potrebbe causare un picco di memoria, a seconda delle dimensioni del sito.
- Il sito testato ha utilizzato circa 800 MB per il database e i file di log del database combinati. Durante una sincronizzazione della configurazione, questi file vengono duplicati con una dimensione massima combinata di circa 1600 MB. Assicurarsi che Cloud Connector disponga di spazio su disco sufficiente per i file duplicati. Il processo di sincronizzazione della configurazione non riesce se il disco è pieno.

# Installare i VDA

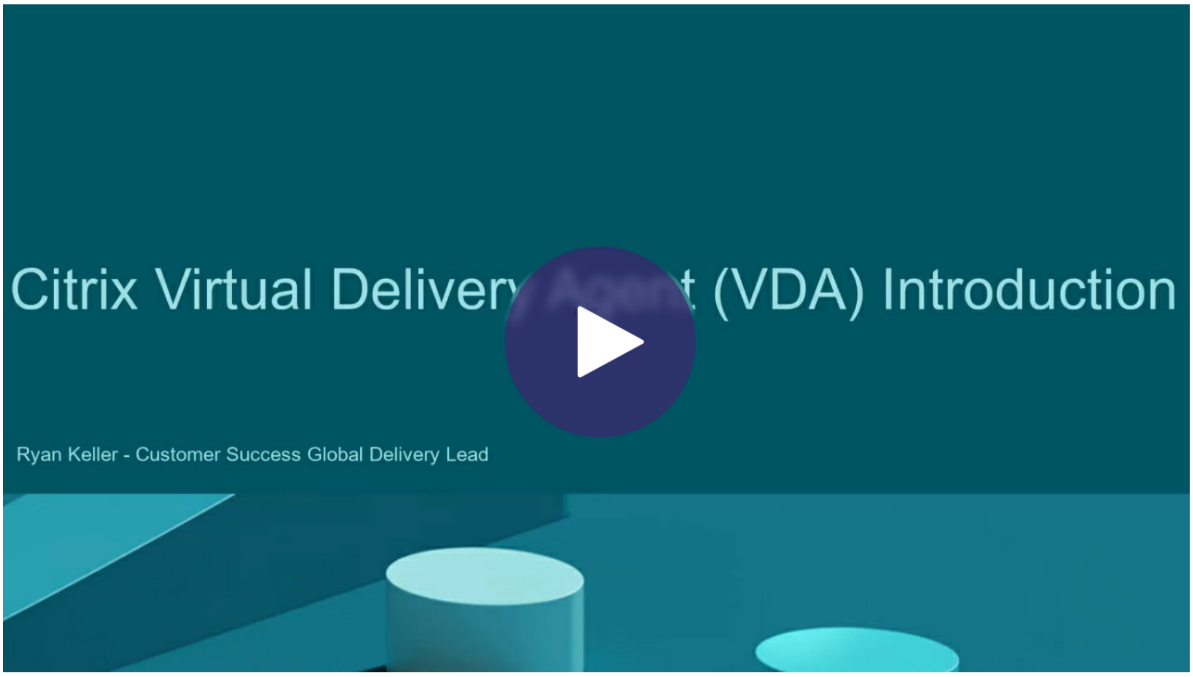
October 30, 2023

## Introduzione

Questo articolo inizia con una descrizione dei VDA Windows e dei programmi di installazione VDA disponibili. Il resto dell'articolo descrive i passaggi della procedura guidata di installazione dei VDA. Vengono forniti equivalenti della riga di comando. Per ulteriori informazioni, vedere Installare i VDA utilizzando la riga di comando.

Per informazioni sui VDA Linux, vedere Linux Virtual Delivery Agent.

Visualizzare un'introduzione ai VDA.



### Considerazioni sull'installazione

L'articolo Citrix DaaS descrive cosa sono e cosa fanno i VDA. Ecco ulteriori informazioni.

- **Raccolta di analisi**: le analisi vengono raccolte automaticamente quando si installano o si aggiornano i componenti. Per impostazione predefinita, tali dati vengono caricati automaticamente su Citrix al termine dell'installazione. Inoltre, quando si installano i componenti, si viene automaticamente registrati nel CEIP (Citrix Customer Experience Improvement Program), che carica dati anonimi. Inoltre, durante un'installazione o un aggiornamento, viene offerta l'opportunità di iscriversi a Call Home.

  Se un'installazione VDA non riesce, un analizzatore MSI analizza il registro MSI in errore, visualizzando il codice di errore esatto. L'analizzatore suggerisce un articolo CTX, se si tratta di un problema noto. L'analizzatore raccoglie anche dati anonimi sul codice di errore. Questi dati sono inclusi con altri dati raccolti dal CEIP. Se si termina la registrazione in CEIP, i dati dell'analizzatore MSI raccolti non vengono più inviati a Citrix.

  Per informazioni su questi programmi, vedere Citrix Insight Services.

- **App Citrix Workspace**: l'app Citrix Workspace per Windows non è installata per impostazione predefinita quando si installa un VDA. È possibile scaricare e installare o aggiornare l'app Citrix Workspace per Windows e altre app Citrix Workspace dal sito Web Citrix. In alternativa, è possibile rendere disponibili tali app Citrix Workspace dal server Workspace o StoreFront.

- **Servizio spooler di stampa:** il servizio Spooler di stampa Microsoft deve essere abilitato. Non è possibile installare correttamente un VDA se tale servizio è disabilitato.

- **Microsoft Media Foundation:** la maggior parte delle edizioni Windows supportate viene fornita con Media Foundation già installato. Se la macchina su cui si sta installando un VDA non dispone di Microsoft Media Foundation (come le edizioni N), diverse funzionalità multimediali non sono installate e non funzionano.

  - Reindirizzamento flash
  - Reindirizzamento di Windows Media
  - Reindirizzamento video HTML5
  - Reindirizzamento webcam HDX RealTime

  È possibile riconoscere la limitazione o terminare l'installazione di VDA e riavviarla in un secondo momento, dopo aver installato Media Foundation. Nell'interfaccia grafica, questa scelta è presentata in un messaggio. Nella riga di comando, è possibile utilizzare l'opzione `/no_mediafoundation_ack` per riconoscere la limitazione.

- **Gruppo utenti locale:** quando si installa il VDA, viene creato automaticamente un nuovo gruppo di utenti locale denominato Direct Access Users (Utenti con accesso diretto). In un VDA con sistema operativo a sessione singola, questo gruppo si applica solo alle connessioni RDP.

In un VDA con sistema operativo multisessione, questo gruppo si applica alle connessioni ICA e RDP.

- **Requisito dell'indirizzo di Cloud Connector:** il VDA deve avere almeno un indirizzo Cloud Connector valido (nella stessa posizione della risorsa) con cui comunicare. In caso contrario, non è possibile stabilire sessioni. È possibile specificare gli indirizzi di Cloud Connector quando si installa il VDA. Per informazioni su altri modi per specificare gli indirizzi di Cloud Connector in cui i VDA possono registrarsi, vedere Registrazione VDA.
- **Considerazioni sul sistema operativo:**
  - Rivedere i requisiti di sistema per conoscere le piattaforme, i sistemi operativi e le versioni supportate.
  - Assicurarsi che ciascun sistema operativo disponga degli aggiornamenti più recenti.
  - Verificare che i VDA dispongano di orologi di sistema sincronizzati. L'infrastruttura Kerberos che protegge la comunicazione tra le macchine richiede la sincronizzazione.
  - Le linee guida sull'ottimizzazione per le macchine Windows 10 sono disponibili in CTX216252.
  - Se si tenta di installare (o eseguire l'aggiornamento a) un VDA Windows su un sistema operativo non supportato per quella versione di VDA, viene visualizzato un messaggio che descrive le opzioni disponibili. Ad esempio, se si tenta di installare il VDA più recente su una macchina con sistema operativo Windows meno recente, un messaggio indirizza l'utente a CTX139030. Per ulteriori informazioni, vedere Sistemi operativi precedenti.
- **MSI installati:** quando si installa un VDA, vengono installati automaticamente diversi MSI. È possibile impedire l'installazione di alcuni MSI nella pagina **Additional Components** (Componenti aggiuntivi) dell'interfaccia grafica o con l'opzione `/exclude` nell'interfaccia della riga di comando. Per altri, l'unico modo per impedirne l'installazione è con l'opzione `/exclude` della CLI.
- **Domain-joined** (Aggiunta al dominio): assicurarsi che la macchina sia aggiunta al dominio prima di installare il software VDA.

#### Strumenti di supportabilità dei VDA

Ogni programma di installazione di VDA include un MSI di supportabilità che contiene strumenti Citrix per il controllo delle prestazioni del VDA, come l'integrità generale e la qualità delle connessioni. Attivare o disattivare l'installazione di questo MSI nella pagina **Componenti aggiuntivi** dell'interfaccia grafica del programma di installazione del VDA. Dalla riga di comando, è possibile disabilitare l'installazione con l'opzione `/exclude "Citrix Supportability Tools"`.

Per impostazione predefinita, l'MSI di supportabilità è installato in `C:\Program Files (x86)\Citrix\Supportability Tools\`. È possibile modificare questo percorso nella pagina

**Componenti** dell'interfaccia grafica del programma di installazione VDA o con l'opzione della `/installdir` riga di comando. Tenere presente che la modifica della posizione interessa tutti i componenti VDA installati, non solo gli strumenti di supportabilità.

Strumenti attualmente presenti nell'MSI di supportabilità:

- Citrix Health Assistant: per i dettagli, vedere CTX207624.
- VDA Cleanup Utility: per i dettagli, vedere CTX209255.

Se non si installano gli strumenti quando si installa il VDA, l'articolo CTX contiene un collegamento al pacchetto di download corrente.

### Riavvii durante l'installazione del VDA

Al termine dell'installazione del VDA è necessario riavviare. Tale riavvio avviene automaticamente per impostazione predefinita.

Per ridurre al minimo il numero di riavvii necessari durante l'installazione del VDA:

- Assicurarsi che sia installata una versione di Microsoft .NET Framework supportata prima di iniziare l'installazione del VDA.
- Per le macchine con sistema operativo multisessione Windows, installare e abilitare i servizi ruolo di Servizi Desktop remoto prima di installare il VDA.

Se non si installano tali prerequisiti prima di installare il VDA:

- Se si utilizza l'interfaccia grafica o l'interfaccia della riga di comando senza l'opzione `/noreboot`, la macchina si riavvia automaticamente dopo aver installato il prerequisito.
- Se si utilizza l'interfaccia della riga di comando con l'opzione `/noreboot`, è necessario effettuare personalmente il riavvio.

Dopo ogni riavvio, l'installazione del VDA continua. Se si sta installando dalla riga di comando, è possibile impedire la ripresa automatica con l'opzione `/noresume`.

Quando si esegue l'aggiornamento di un VDA alla versione 7.17 o a una versione successiva supportata, si verifica un riavvio durante l'aggiornamento. Questo riavvio non può essere evitato.

### Ripristino in caso di errore di installazione o aggiornamento

> **Nota:**
>
> Questa funzionalità è disponibile solo per i VDA a sessione singola.

Se un'installazione o un aggiornamento di un VDA a sessione singola non va a buon fine e la funzionalità Restore on failure (Ripristina in caso di errore) è abilitata, la macchina viene riportata a un punto di ripristino impostato prima dell'inizio dell'installazione o dell'aggiornamento.

Quando un'installazione o un aggiornamento di un VDA a sessione singola inizia con questa funzionalità abilitata, il programma di installazione crea un punto di ripristino del sistema prima di iniziare l'installazione o l'aggiornamento effettivi. Se l'installazione o l'aggiornamento del VDA non riesce, la macchina viene riportata allo stato del punto di ripristino. La cartella `%temp%/Citrix` contiene log di distribuzione e altre informazioni sul ripristino.

Per impostazione predefinita, questa funzionalità è disabilitata.

Se si prevede di abilitare questa funzionalità, assicurarsi che il ripristino del sistema non sia disabilitato tramite un'impostazione dell'oggetto Criteri di gruppo (`Computer Configuration > Administrative Templates > System > System Restore`).

Per abilitare questa funzionalità durante l'installazione o l'aggiornamento di un VDA a sessione singola:

- Quando si utilizza l'interfaccia grafica di un programma di installazione VDA (ad esempio si utilizza **Autostart** o il comando `XenDesktopVDASetup.exe` senza alcuna opzione di ripristino o non interattiva), selezionare la casella di controllo **Enable automatic restore if update fails** (Abilita ripristino automatico in caso di errore dell'aggiornamento) nella pagina **Summary** (Riepilogo).

  Se l'installazione/aggiornamento viene completato correttamente, il punto di ripristino non viene utilizzato, ma viene mantenuto.

- Eseguire un programma di installazione VDA con l'opzione `/enablerestore` o `/enablerestoreclean`.

  - Se si utilizza l'opzione `/enablerestorecleanup` e l'installazione/aggiornamento viene completato correttamente, il punto di ripristino viene rimosso automaticamente.
  - Se si utilizza l'opzione `/enablerestore` e l'installazione/aggiornamento viene completato correttamente, il punto di ripristino non viene utilizzato, ma viene mantenuto.

### Programmi di installazione dei VDA

I programmi di installazione VDA possono essere scaricati direttamente dalla console Citrix Cloud.

Per impostazione predefinita, i file nei programmi di installazione autoestraenti vengono estratti nella cartella `Temp`. I file estratti nella cartella `Temp` vengono eliminati automaticamente al termine dell'installazione. In alternativa, è possibile utilizzare il comando `/extract` con un percorso assoluto.

Sono disponibili per il download tre programmi di installazione VDA autonomi.

**VDAServerSetup.exe** Installa un VDA con sistema operativo multisessione.

**VDAWorkstationSetup.exe** Installa un VDA con sistema operativo a sessione singola.

**VDAWorkstationCoreSetup.exe** Installa un VDA con sistema operativo a sessione singola ottimizzato per le distribuzioni di Accesso remoto PC o per le installazioni VDI di base. Accesso remoto PC utilizza macchine fisiche. Le installazioni VDI principali sono macchine virtuali che non vengono utilizzate come immagine. Questo programma di installazione distribuisce solo i servizi di base necessari per le connessioni VDA. Pertanto, supporta solo un sottoinsieme delle opzioni valide con il programma di installazione di VDAWorkstationSetup.

Questo programma di installazione per la versione corrente non installa o non contiene i componenti utilizzati per:

- App-V.
- Profile Management. L'esclusione di Citrix Profile Management dall'installazione influisce sui display Monitor.
- Servizio di identità macchina.
- App Citrix Workspace per Windows.
- Strumenti di supportabilità Citrix.
- Citrix Files per Windows.
- Citrix Files per Outlook.
- Cache di scrittura MCSIO per l'ottimizzazione dell'archiviazione.

Il programma di installazione non installa e non contiene un'app Citrix Workspace per Windows.

Il programma di installazione installa automaticamente l'MSI di reindirizzamento del contenuto del browser. L'installazione automatica si applica a VDA versione 2003 e successive supportate.

L'utilizzo di `VDAWorkstationCoreSetup.exe` equivale a utilizzare il programma di installazione `VDAWorkstationSetup.exe` per installare un VDA con sistema operativo a sessione singola e a una delle seguenti azioni:

- Nell'interfaccia grafica: selezionare l'opzione **Remote PC Access** (Accesso remoto PC) nella pagina **Environment** (Ambiente).
- Nell'interfaccia della riga di comando: specificare l'opzione `/remotepc`.
- Nell'interfaccia della riga di comando: specificare `/components vda` e `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix Profile Management""Citrix Profile Management WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix Files for Outlook""Citrix MCS IODriver"`.

Se si installa un VDA con il programma di installazione `VDAWorkstationCoreSetup.exe` e successivamente si aggiorna il VDA utilizzando il programma di installazione `VDAWorkstationSetup.exe`, è possibile installare facoltativamente i componenti e le funzionalità omessi.

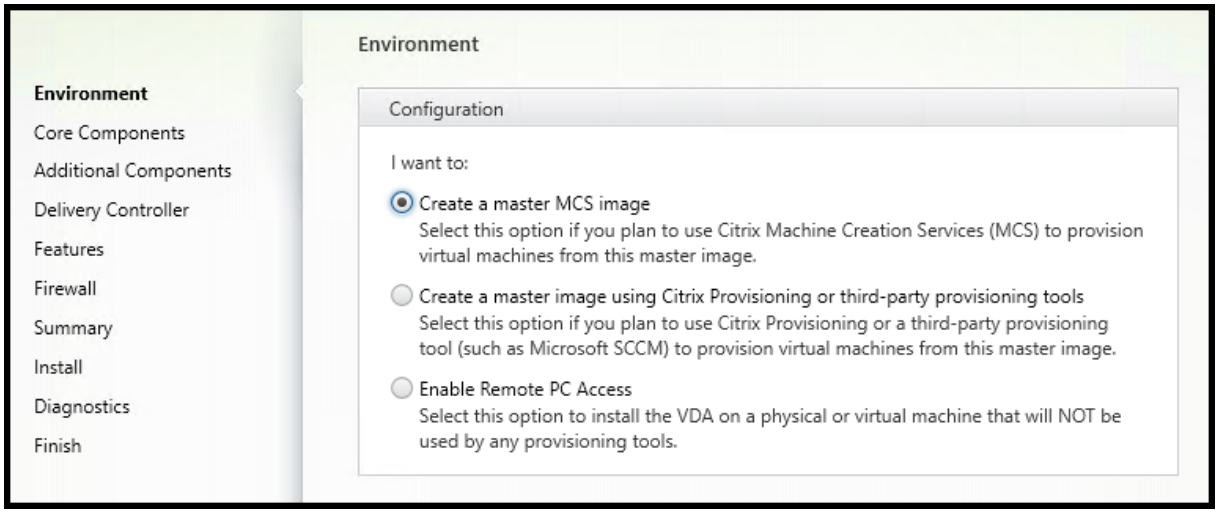
 

### Passaggio 1. Scaricare il software del prodotto e avviare la procedura guidata

1. Sulla macchina su cui si sta installando il VDA, accedere a Citrix Cloud.
2. Nel menu in alto a sinistra, selezionare Citrix DaaS nell'elenco **My Services** (I miei servizi).
3. Sul lato destro, fare clic su **Downloads** (Download) e selezionare **Download VDA** (Scarica VDA). Si viene reindirizzati alla pagina di download VDA. Trovare il programma di installazione VDA desiderato e quindi selezionare **Download File** (Scarica file).
4. Al termine del download, fare clic con il pulsante destro del mouse sul file e selezionare **Run as administrator** (Esegui come amministratore). Viene avviata l'installazione guidata.

In alternativa ai passaggi 1-3, è possibile scaricare il VDA direttamente dalla pagina di download di Citrix.

### Passaggio 2. Specificare come verrà utilizzato il VDA




Nella pagina **Environment** (Ambiente), specificare la modalità di utilizzo del VDA, indicando se si utilizzerà questa macchina come immagine per eseguire il provisioning delle macchine. L'opzione scelta influisce sugli strumenti di provisioning Citrix che verranno installati automaticamente (se presenti) e sui valori predefiniti nella pagina **Additional Components** (Componenti aggiuntivi) del programma di installazione dei VDA.

Scegliere una delle seguenti opzioni:

- **Create a master MCS image (Crea un'immagine MCS master):** selezionare questa opzione per installare un VDA in un'immagine di macchina virtuale, se si prevede di utilizzare Machine Creation Services per eseguire il provisioning delle macchine virtuali. Questa opzione installa Machine Identity Service. Questa è l'opzione predefinita.

  Opzione della riga di comando: `/mastermcsimage` o `/masterimage`

- **Create a master image using Citrix Provisioning or third-party provisioning tools:** (Crea un'immagine master utilizzando Citrix Provisioning o strumenti di provisioning di terze parti): selezionare questa opzione per installare un VDA su un'immagine VM, se si prevede di utilizzare Citrix Provisioning o strumenti di provisioning di terze parti (ad esempio Microsoft System Center Configuration Manager). Utilizzare questa opzione per le macchine virtuali precedentemente sottoposte a provisioning avviate da un disco di lettura/scrittura Citrix Provisioning.

  Opzione della riga di comando: `/masterpvsimage`

- (viene visualizzata solo su macchine con sistema operativo multisessione) **Enable brokered connections to a server** (Abilita connessioni negoziate a un server): selezionare questa opzione per installare un VDA su una macchina fisica o virtuale che non verrà utilizzata come immagine.

  Opzione della riga di comando: `/remotepc`

- (viene visualizzata solo su macchine con sistema operativo a sessione singola) **Enable Remote PC Access** (Abilita accesso remoto PC): selezionare questa opzione per installare un VDA su una macchina fisica da utilizzare con Remote PC Access (Accesso remoto PC).

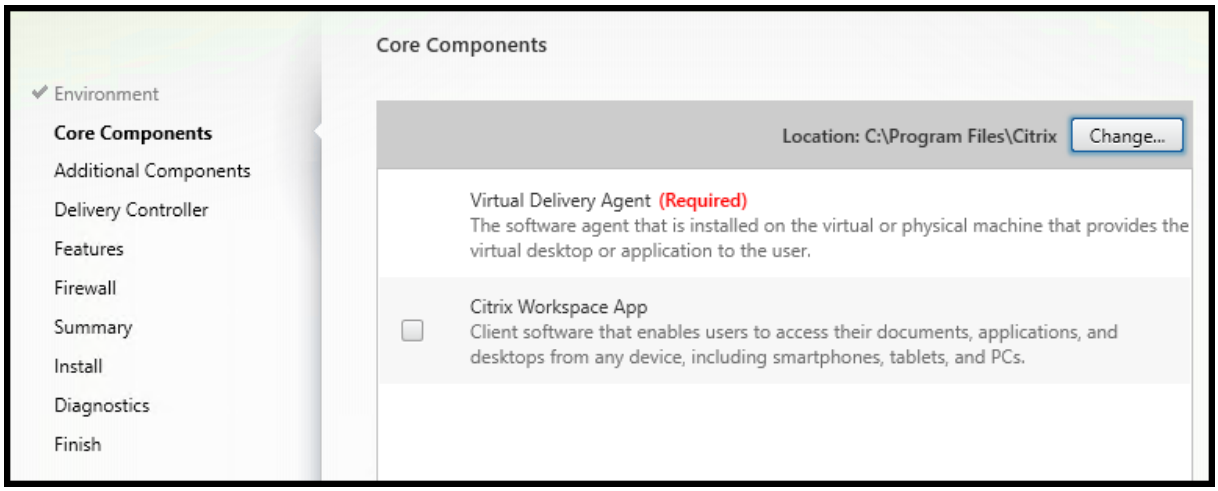
  Opzione della riga di comando: `/remotepc`

Selezionare **Next** (Avanti).

Questa pagina non viene visualizzata:

- Quando si aggiorna un VDA.
- Quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`.

### Passaggio 3. Selezionare i componenti da installare e il percorso di installazione




Nella pagina **Core components**:

- **Location (Percorso):** per impostazione predefinita, i componenti sono installati in `C:\Program Files\Citrix`. Questa impostazione predefinita va bene per la maggior parte delle distribuzioni. Se si specifica un percorso diverso, tale percorso deve disporre delle autorizzazioni di esecuzione per il servizio di rete.

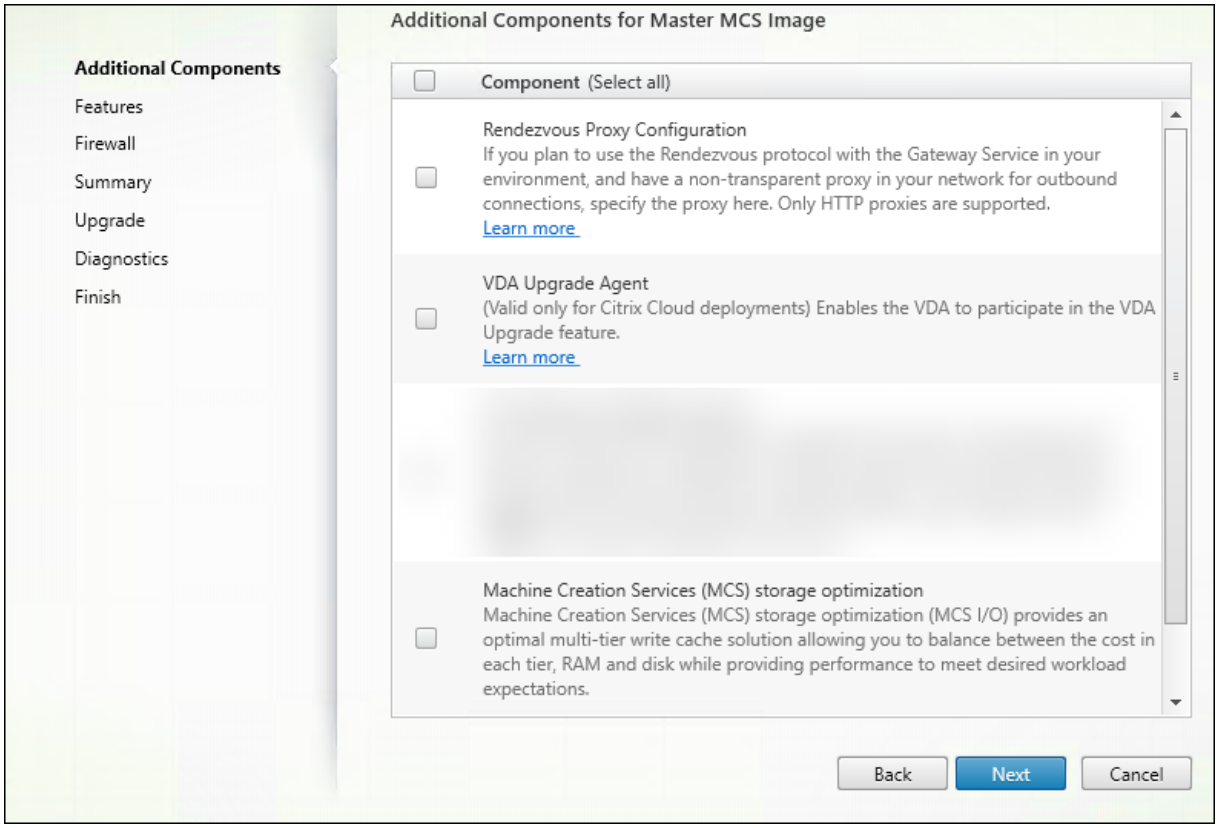
  Opzione della riga di comando: `/installdir`

- **Componenti:** per impostazione predefinita, l'app Citrix Workspace per Windows non è installata con il VDA. Se si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`, l'app Citrix Workspace per Windows non viene mai installata, quindi questa casella di controllo non viene visualizzata.

  Opzione della riga di comando: `/components vda,plugin` per installare il VDA e l'app Citrix Workspace per Windows

Selezionare **Next** (Avanti).

### Passaggio 4. Installare componenti aggiuntivi




La pagina **Additional Components** (Componenti aggiuntivi) contiene caselle di controllo che consentono di abilitare o disabilitare l'installazione di altre funzionalità e tecnologie con il VDA. In un'installazione mediante riga di comando, è possibile utilizzare l'opzione `/exclude` o `/includeadditional` per omettere o includere uno o più componenti disponibili.

Nella tabella seguente è indicata l'impostazione predefinita degli elementi presenti in questa pagina. L'impostazione predefinita dipende dall'opzione selezionata nella pagina **Environment**.

| Pagina Additional Components | Pagina Environment (Ambiente): opzione "Master image with MCS"(Immagine master con MCS) o "Master image with Citrix Provisioning" (Immagine master con Citrix Provisioning) selezionata | Pagina Environment: opzione "Enable brokered connections to server"(Abilita connessioni negoziate al server) (per sistema operativo multisessione) o "Remote PC Access"(Accesso remoto PC) (per sistema operativo a sessione singola) selezionata |
|---|---|---|
| Personalizzazione Citrix per App-V | Non selezionato | Non selezionato |
| Livello di personalizzazione utente | Non selezionato | Non visualizzato perché non valido per questo caso d'uso |
| Strumenti di supportabilità Citrix | Selezionato | Non selezionato |
| Citrix Profile Management | Selezionato | Non selezionato |
| Plug-in WMI Citrix Profile Management | Selezionato | Non selezionato |
| Agente di aggiornamento Citrix VDA | Non selezionato | Non selezionato |
| Citrix Backup and Restore | Non selezionato | Non selezionato |
| Citrix Files per Windows | Non selezionato | Non selezionato |
| Citrix Files per Outlook | Non selezionato | Non selezionato |
| Ottimizzazione dell' archiviazione MCS (Machine Creation Services) | Non selezionato | Non selezionato |
| Configurazione del protocollo Rendezvous | Non selezionato | Non selezionato |

Questa pagina non viene visualizzata quando:

- Si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Inoltre, le opzioni della riga di comando per i componenti aggiuntivi non sono valide con tale programma di installazione.
- Si sta aggiornando un VDA e tutti i componenti aggiuntivi sono già installati. Se alcuni dei componenti aggiuntivi sono già installati, nella pagina vengono elencati solo i componenti non in-

stallati.

L'elenco dei componenti può includere:

- **Citrix Personalization for App-V (Personalizzazione Citrix per App-V):** installare questo componente se si utilizzano applicazioni provenienti da pacchetti Microsoft App-V. Per ulteriori informazioni, vedere App-V.

  Opzione della riga di comando: `/includeadditional "Citrix Personalization for App-V – VDA"` per abilitare l'installazione dei componenti, `/exclude "Citrix Personalization for App-V – VDA"` per impedire l'installazione dei componenti

- **Livello di personalizzazione utente Citrix:** installa MSI per il livello di personalizzazione utente. Per ulteriori informazioni, vedere Livello di personalizzazione utente.

  Questo componente viene visualizzato solo quando si installa un VDA su una macchina Windows 10 a sessione singola.

  Opzione della riga di comando: `/includeadditional "User Personalization Layer"` per abilitare l'installazione dei componenti, `/exclude "User Personalization Layer"` per impedire l'installazione dei componenti

- **Strumenti di supportabilità Citrix:** installa l'MSI che contiene gli strumenti di supportabilità Citrix.

  Opzione della riga di comando: `/includeadditional "Citrix Supportability Tools"` per abilitare l'installazione dei componenti, `/exclude "Citrix Supportability Tools"` per impedire l'installazione dei componenti.

- **Citrix Profile Management:** questo componente gestisce le impostazioni di personalizzazione degli utenti nei profili utente. Per ulteriori informazioni, vedere Profile Management.

  L'esclusione di Citrix Profile Management dall'installazione influisce sul monitoraggio e la risoluzione dei problemi dei VDA in Citrix Cloud.

  - Nelle pagine **User details** (Dettagli utente) ed **EndPoint** della scheda **Monitor** (Monitoraggio), i riquadri **Personalization** (Personalizzazione) e **Logon Duration** (Durata dell'accesso) riportano errori.
  - Nelle pagine **Dashboard** e **Trends**, il pannello **Average Logon Duration** (Durata media dell'accesso) visualizza i dati solo per le macchine su cui è installato Profile Management.

  Anche se si utilizza una soluzione di gestione dei profili utente di terze parti, Citrix consiglia di installare ed eseguire Citrix Profile Management Service. L'attivazione del servizio Citrix Profile Management non è necessaria.

  Opzione della riga di comando: `/includeadditional "Citrix Profile Management "` per abilitare l'installazione dei componenti, `/exclude "Citrix Profile Management "` per impedire l'installazione dei componenti.

- **Plug-in WMI Citrix Profile Management:** questo plug-in fornisce informazioni di runtime Profile Management negli oggetti WMI (Windows Management Instrumentation) (ad esempio provider di profili, tipo di profilo, dimensioni e utilizzo del disco). Gli oggetti WMI forniscono informazioni sulla sessione a Director.

  Opzione della riga di comando: `/includeadditional "Citrix Profile Management WMI Plugin"` per abilitare l'installazione dei componenti, `/exclude "Citrix Profile Management WMI Plugin"` per impedire l'installazione dei componenti.

- **VDA Upgrade Agent** (Agente di aggiornamento VDA): valido solo per le distribuzioni Citrix DaaS. Consente al VDA di partecipare alla funzionalità di aggiornamento VDA. È possibile utilizzare questa funzione per aggiornare i VDA di un catalogo dalla console di gestione, immediatamente o in un orario pianificato. Se questo agente non è installato, è possibile aggiornare un VDA eseguendo il programma di installazione VDA sulla macchina.

  Opzioni della riga di comando: `/includeadditional "Citrix VDA Upgrade Agent"` per abilitare l'installazione dei componenti, `/exclude "Citrix VDA Upgrade Agent"` per impedire l'installazione dei componenti

- **Citrix Files per Windows:** questo componente consente agli utenti di connettersi al proprio account Citrix Files. Gli utenti possono quindi interagire con Citrix Files tramite un'unità mappata nel file system Windows (senza richiedere una sincronizzazione completa del relativo contenuto).

  Opzioni della riga di comando: `/includeadditional "Citrix Files for Windows"` per abilitare l'installazione dei componenti, `/exclude "Citrix Files for Windows"` per impedire l'installazione dei componenti

- **Citrix Files per Outlook:** questo componente consente di ignorare le restrizioni sulle dimensioni dei file e di aggiungere sicurezza agli allegati o alle e-mail inviandoli attraverso Citrix Files. È possibile fornire una richiesta di caricamento sicuro dei file direttamente nella propria e-mail. Per ulteriori informazioni, vedere Citrix Files for Outlook.

  Opzioni della riga di comando: `/includeadditional "Citrix Files for Outlook"` per abilitare l'installazione dei componenti, `/exclude "Citrix Files for Outlook"` per impedire l'installazione dei componenti

- **Ottimizzazione dell'archiviazione Machine Creation Services (MCS):** installa il driver Citrix MCS IO. Per ulteriori informazioni, vedere Archiviazione condivisa dagli hypervisor e Configurare la cache per i dati temporanei.

  Opzioni della riga di comando: `/includeadditional "Citrix MCS IODriver"` per abilitare l'installazione dei componenti, `/exclude "Citrix MCS IODriver"` per impedire l'installazione dei componenti

- **Configurazione del proxy Rendezvous:** installare questo componente se si intende utilizzare

il protocollo Rendezvous con il servizio Citrix Gateway nel proprio ambiente e si dispone di un proxy non trasparente nella rete per le connessioni in uscita. Sono supportati solo i proxy HTTP.

Se si installa questo componente, specificare l'indirizzo del proxy o il percorso del file PAC nella pagina **Rendezvous Proxy Configuration** (Configurazione del proxy Rendezvous). Per dettagli delle funzionalità, vedere Protocollo Rendezvous.

Opzione della riga di comando: `/includeadditional "Citrix Rendezvous V2"` per abilitare l'installazione dei componenti, `/exclude "Citrix Rendezvous V2"` per impedire l'installazione dei componenti

- **Citrix Backup and Restore:** se l'installazione o l'aggiornamento di un VDA falliscono, questo componente può riportare la macchina a un backup eseguito prima dell'installazione o dell'aggiornamento.

  Opzione della riga di comando: `/includeadditional "Citrix Backup and Restore"` per abilitare l'installazione dei componenti, `/exclude "Citrix Backup and Restore"` per impedire l'installazione dei componenti.

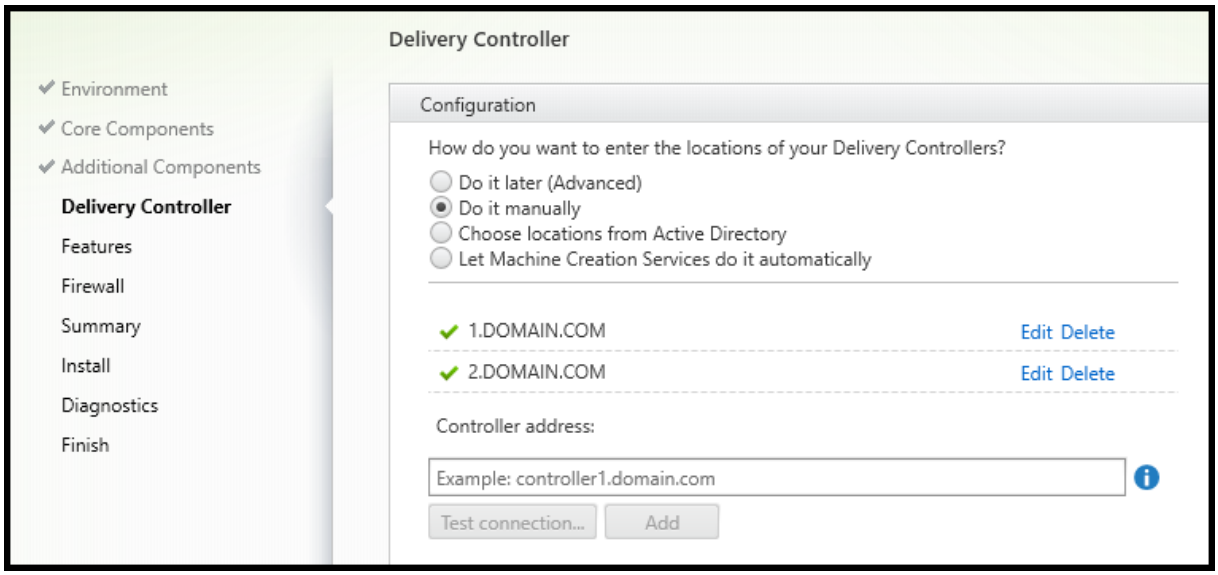
- **Citrix HyperV Filter Driver** (Driver di filtro Citrix HyperV): questo componente deve essere abilitato utilizzando la casella di controllo solo se si esegue l'aggiornamento da una versione precedente del VDA (precedente alla 2308). Il componente mantiene le impostazioni relative alla NIC dell'immagine master nelle macchine virtuali di cui effettua il provisioning. Le impostazioni vengono mantenute anche dopo l'aggiornamento di Windows.

  Opzione della riga di comando: `/includeadditional "Citrix HyperV Filter Driver"` per abilitare l'installazione dei componenti, `/exclude "Citrix HyperV Filter Driver"` per impedire l'installazione dei componenti.

  > **Nota:**
  >
  > Questo componente viene installato automaticamente se si esegue una nuova installazione del VDA versione 2308 o successiva su una macchina distribuita con Hyper-V (inclusi Azure e SCVMM) tramite le installazioni di immagini master MCS.

### Passaggio 5. Indirizzi Cloud Connector




Nella pagina **Delivery Controller**, selezionare **Do it manually** (Esegui l'operazione manualmente). Immettere il nome DNS di un Cloud Connector installato e quindi selezionare **Aggiungi**. Se sono stati installati altri Cloud Connector nella posizione della risorsa, aggiungere i relativi nomi DNS.

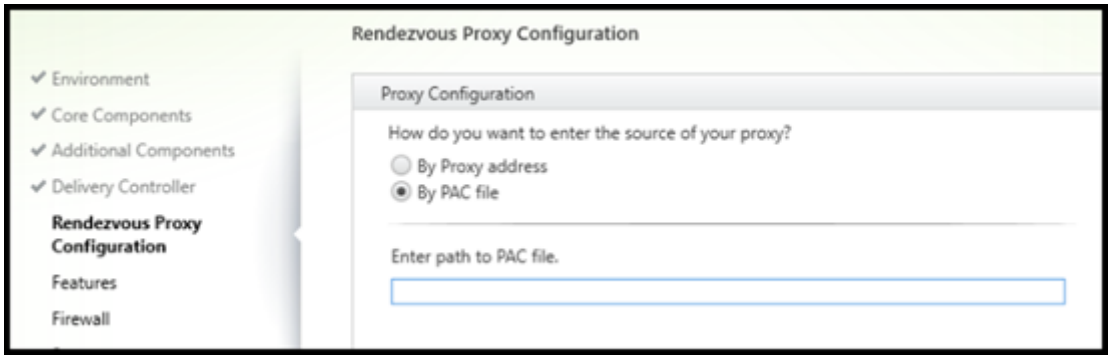
Selezionare **Next** (Avanti).

Considerazioni:

- L'indirizzo può contenere solo caratteri alfanumerici.
- La corretta registrazione del VDA richiede che le porte firewall utilizzate per comunicare con Cloud Connector siano aperte. Tale azione è abilitata per impostazione predefinita nella pagina **Firewall** della procedura guidata.

Opzione della riga di comando: `/controllers`

### Passaggio 6. Configurazione del proxy Rendezvous



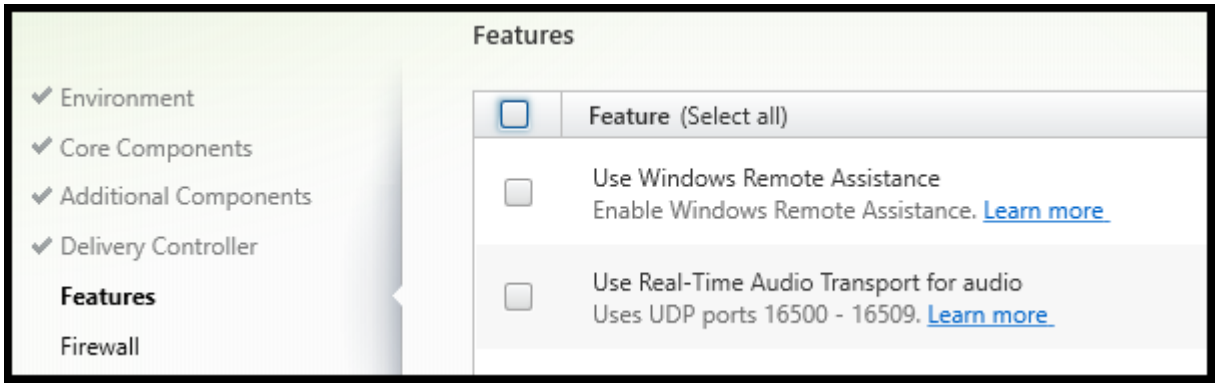
La pagina **Configurazione proxy Rendezvous** viene visualizzata solo se è stata abilitata la casella di controllo **Configurazione proxy Rendezvous** nella pagina **Componenti aggiuntivi** .

1. Selezionare se si dovrà specificare l'origine del proxy mediante l'indirizzo proxy o il percorso del file PAC.
2. Specificare l'indirizzo del proxy o il percorso del file PAC.
   - Formato dell'indirizzo proxy: `http://<url-or-ip>:<port>`
   - Formato del file PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

Il firewall per la porta proxy deve essere aperto affinché il test di connessione abbia esito positivo. Se non è possibile stabilire una connessione al proxy, è possibile scegliere se continuare l'installazione di VDA.

Opzione della riga di comando: `/proxyconfig`

### Passaggio 7. Attivare o disattivare funzionalità




Nella pagina **Features** utilizzare le caselle di controllo per attivare o disattivare le funzionalità che si desidera utilizzare.

- **Use Windows Remote Assistance** (Utilizza Assistenza remota di Windows): quando questa funzionalità è abilitata, Assistenza remota di Windows viene utilizzata con la funzionalità di shadowing utente del componente Director in Citrix Cloud. Assistenza remota di Windows apre le porte dinamiche nel firewall. (Impostazione predefinita= disabilitato)

  Opzione della riga di comando: `/enable_remote_assistance`

- **Use Real-Time Audio Transport for audio** (Utilizza il trasporto audio in tempo reale per l'audio): abilitare questa funzione se la funzionalità voice-over-IP è ampiamente utilizzata nella rete. La funzione riduce la latenza e migliora la resilienza audio sulle reti con perdita di dati. Consente di trasmettere i dati audio utilizzando RTP su trasporto UDP. (Impostazione predefinita= disabilitato)

  Opzione della riga di comando: `/enable_real_time_transport`

- **Use screen sharing (Usa la condivisione dello schermo):** se abilitata, le porte utilizzate dalla condivisione dello schermo vengono aperte nel firewall di Windows. (Impostazione predefinita= disabilitato)

  Opzione della riga di comando: `/enable_ss_ports`

- **Is this VDA installed on a VM in a cloud (Questo VDA è installato su una macchina virtuale in un cloud?)** Questa impostazione aiuta Citrix a identificare correttamente le posizioni delle risorse per le distribuzioni VDA on-premise e come servizio (Citrix Cloud) a scopi di telemetria. Questa funzionalità non ha alcuna ripercussione sull'utilizzo da parte del cliente. Abilitare questa impostazione se la distribuzione utilizza Citrix DaaS. (Impostazione predefinita= disabilitato)

  Opzione della riga di comando: `/xendesktopcloud`

Selezionare **Next** (Avanti).

Se questa pagina contiene una funzionalità denominata **MCS I/O**, non utilizzarla. La funzionalità MCS IO è configurata nella pagina **Additional Components** (Componenti aggiuntivi).

### Passaggio 8. Porte del firewall


La pagina **Firewall** indica le porte utilizzate dal VDA e dai Cloud Connector per comunicare tra loro. Per impostazione predefinita, queste porte vengono aperte automaticamente se il servizio Windows

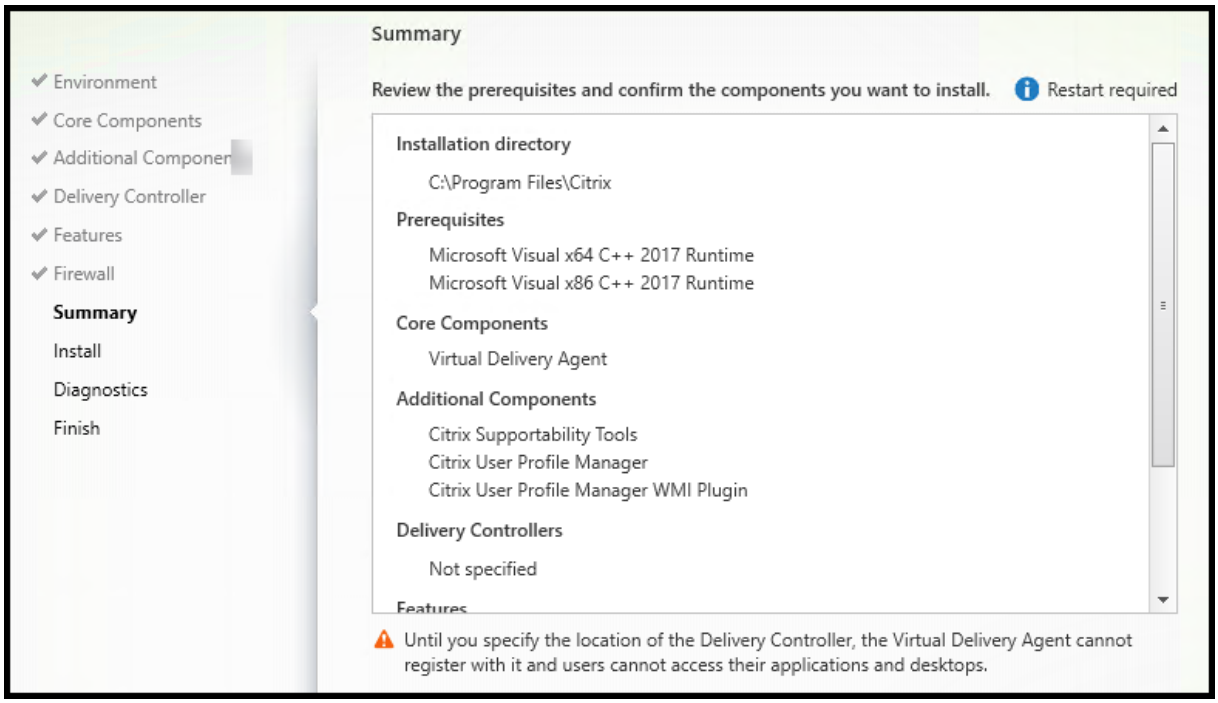
Firewall è in esecuzione, anche se il firewall non è abilitato. Questa impostazione predefinita è adatta alla maggior parte delle distribuzioni.

Per informazioni sulle porte, vedere Porte di rete.

Selezionare **Next** (Avanti).

Opzione della riga di comando: `/enable_hdx_ports`

### Passaggio 9 Esaminare i prerequisiti e confermare l'installazione



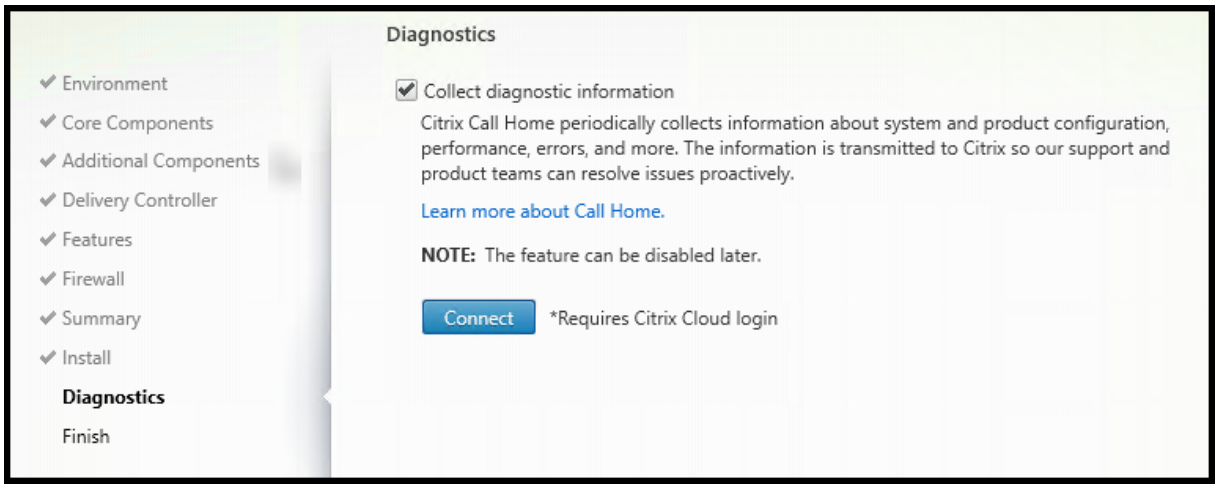

Nella pagina **Summary** sono elencati gli elementi che verranno installati. È possibile tornare alle pagine precedenti della procedura guidata e modificare le selezioni, se necessario.

(Solo VDA a sessione singola) Selezionare la casella di controllo **Enable automatic restore if update fails** (Abilita ripristino automatico in caso di errore dell'aggiornamento) per abilitare la funzionalità di ripristino in caso di errore. Per ulteriori informazioni, vedere Ripristino in caso di errore di installazione o aggiornamento.

Quando si è pronti, selezionare **Install** (Installa).

### Passaggio 10. Diagnostica

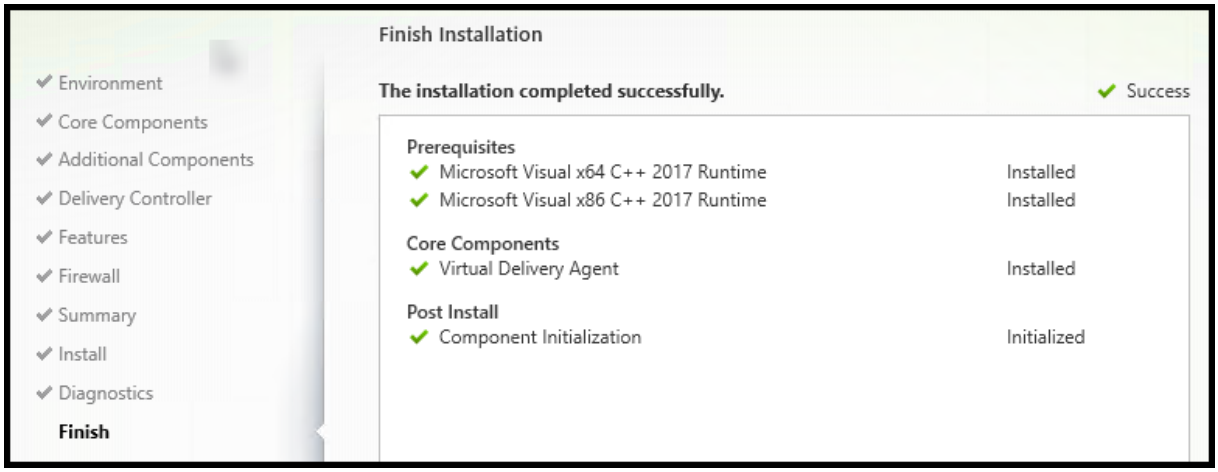



Nella pagina **Diagnostics** (Diagnostics), scegliere se partecipare a Citrix Call Home. Se si sceglie di partecipare (impostazione predefinita), selezionare **Connect** (Connetti). Quando richiesto, immettere le credenziali dell'account Citrix.

Dopo aver convalidato le credenziali (o se si sceglie di non partecipare), selezionare **Next** (Avanti).

Per ulteriori informazioni, vedere Call Home.

### Passaggio 11. Completare questa installazione




La pagina **Finish** contiene segni di spunta verdi per tutti i prerequisiti e i componenti installati e inizializzati correttamente.

Selezionare **Finish** (Fine). Per impostazione predefinita, la macchina si riavvia automaticamente. Sebbene sia possibile disattivare questo riavvio automatico, il VDA non può essere utilizzato fino al completamento del riavvio della macchina.

Se si sta installando un VDA su macchine singole (anziché su un'immagine), ripetere i passaggi precedenti per installare un VDA su altre macchine, se necessario.

### Risoluzione dei problemi

Nella visualizzazione **Manage > Full Configuration** (Gestisci > Configurazione completa) per un gruppo di consegna, la voce **Installed VDA version** (Versione VDA installata) nel riquadro Details (Dettagli) potrebbe non essere la versione installata sulle macchine. La visualizzazione Programmi e funzionalità di Windows della macchina mostra la versione VDA effettiva.

### Citrix Optimizer

Citrix Optimizer è uno strumento per il sistema operativo Windows che aiuta gli amministratori Citrix a ottimizzare i VDA rimuovendo e ottimizzando vari componenti.

Dopo aver installato un VDA e completato il riavvio finale, scaricare e installare Citrix Optimizer. Vedere CTX224676. L'articolo CTX contiene il pacchetto di download, oltre a istruzioni sull'installazione e l'utilizzo di Citrix Optimizer.

### Personalizzare un VDA

Successivamente, per personalizzare (modificare le informazioni per) un VDA installato:

1. Dalla funzione Windows per la rimozione o la modifica dei programmi, selezionare **Citrix Virtual Delivery Agent** o **Citrix Remote PC Access/VDI Core Services VDA**. Quindi fare clic con il pulsante destro del mouse e selezionare **Modifica**.
2. Selezionare **Customize Virtual Delivery Agent Settings** (Personalizza impostazioni del Virtual Delivery Agent).

All'avvio del programma di installazione, modificare le impostazioni disponibili.

### Personalizzare la porta per la comunicazione con i Cloud Connector

È possibile personalizzare la porta utilizzata dai VDA per comunicare con i Cloud Connector in base ai propri requisiti di sicurezza specifici. Questa funzione è utile se il team di sicurezza non consente l'apertura della porta predefinita (porta 80) o se la porta predefinita è già in uso.

Per personalizzare la porta, completare i seguenti passaggi:

1. Aggiungere il numero di porta del controller ai Citrix Cloud Connector.
2. Aggiungere il numero di porta del VDA ai VDA.

#### Aggiungere il numero di porta del controller ai Citrix Cloud Connector

Accedere a Citrix Cloud Connector ed eseguire i due comandi PowerShell seguenti:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort <port number> -ConfigureFirewall`

Esempio:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort 18000 -ConfigureFirewall`

Quando si personalizza la porta, considerare quanto segue:

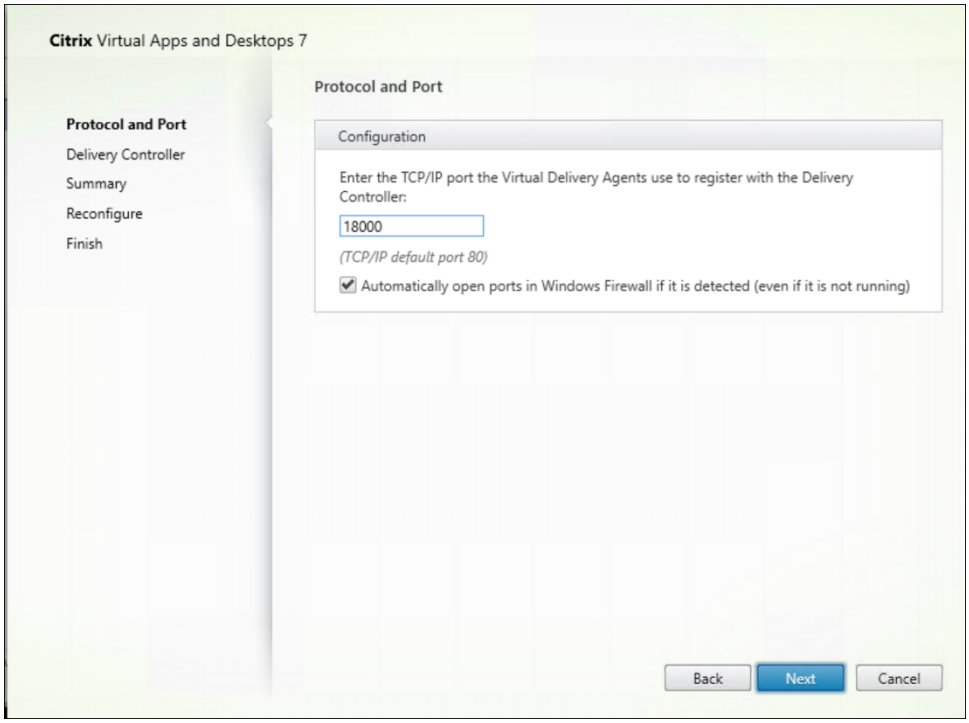
- È necessario utilizzare lo stesso numero di porta in entrambi i comandi.
- È necessario eseguire entrambi i comandi *su tutti i Cloud Connector*.
- Per comunicare correttamente con i Cloud Connector, assicurarsi che tutti i VDA utilizzino lo stesso numero di porta.
- La porta configurata persiste tra gli aggiornamenti dei Connector.

#### Aggiungere il numero di porta del VDA ai VDA

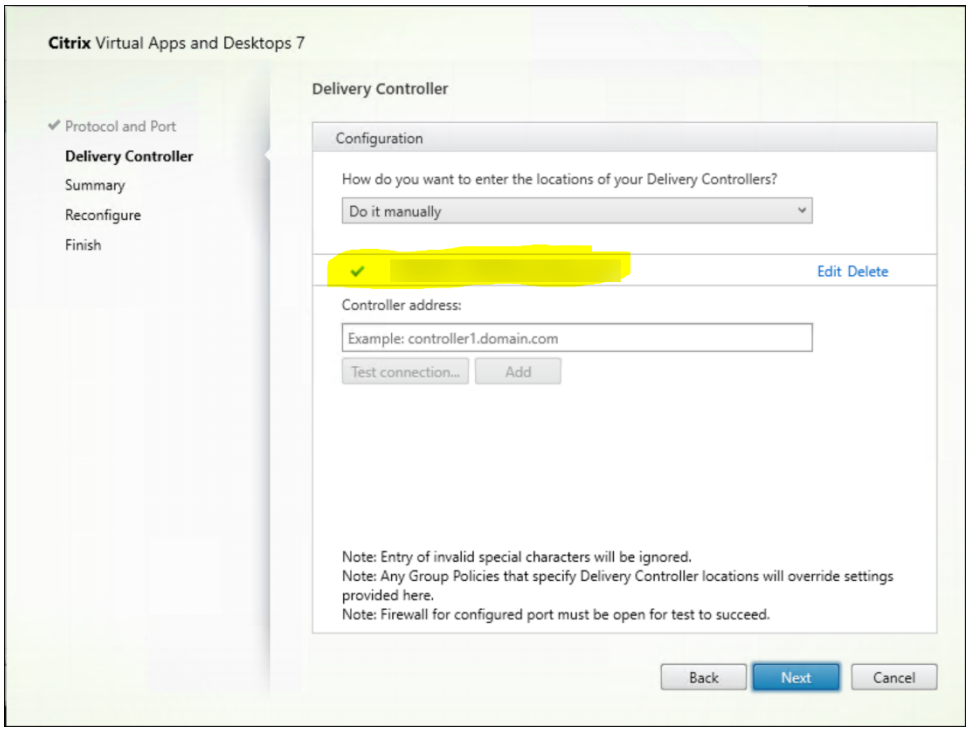
Installare il VDA con le impostazioni predefinite e configurarlo come segue. Se il VDA è già installato, continuare con i passaggi riportati di seguito.

1. Sul VDA, aprire **XenDesktopVdaSetup.exe**, che si trova in `C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe`.
2. Nella pagina **Protocol and Port** (Protocollo e porta), aggiungere il numero di porta personalizzato.




3. Nella pagina **Delivery Controller**, immettere il nome di dominio completo del controller.




4. Fare clic su **Next** (Avanti) per eseguire la procedura guidata e completare la configurazione.

I numeri di porta vengono quindi riconfigurati correttamente.

> **Nota:**
>
> È possibile che venga visualizzato il seguente messaggio di errore quando si verifica una connessione del controller: No running instance of a Controller found on < the Controller address you entered (Nessuna istanza in esecuzione di un controller trovata in < indirizzo del controller inserito>). Se l'indirizzo è corretto, è possibile ignorare il messaggio.

**Risoluzione dei problemi**

Per verificare se le porte personalizzate sono configurate correttamente, andare al Cloud Connector ed eseguire i seguenti passaggi per la risoluzione dei problemi:

1. Verificare che siano presenti le due chiavi del Registro di sistema seguenti.

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Name: CustomVDAPortNumber
   Type: REG_DWORD
   Data: 18000

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Name: CustomVDAPortNumberHA
   Type: REG_DWORD
   Data: 18000

2. Eseguire il seguente comando per creare un file .txt.

   - `netsh http show urlacl > <filepath>.txt`

   Esempio:

   - `netsh http show urlacl > c:\reservations.txt`

3. Aprire il file .txt e controllare i quattro URL seguenti per verificare che venga utilizzata la porta corretta.

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. Verificare che le due regole firewall seguenti siano state create e che le porte richieste siano aperte.

   - Citrix XaXdProxy
   - Citrix Broker Service (TCP-In)

### Altre informazioni

- Dopo aver installato un VDA, è possibile verificare lo stato e la disponibilità del sito e dei suoi componenti con un controllo di integrità del cloud.

### Passaggi successivi

Creare cataloghi di macchine.

Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.

## Installare i VDA utilizzando la riga di comando

June 8, 2023

### Introduzione

Questo articolo si applica all'installazione, all'aggiornamento e alla personalizzazione di Virtual Delivery Agent (VDA) su macchine con sistemi operativi Windows.

In questo articolo viene descritto come emettere i comandi di installazione VDA. Prima di iniziare un'installazione, consultare Installare i VDA per considerazioni sull'installazione, i programmi di installazione e le informazioni da specificare durante l'installazione.

### Installare un VDA dalla riga di comando

Per installare un VDA (e vedere l'avanzamento dell'esecuzione dei comandi e i valori restituiti), è necessario disporre di autorizzazioni amministrative elevate o utilizzare **Run as administrator** (Esegui come amministratore).

1. Sulla macchina su cui si sta installando il VDA, accedere a Citrix Cloud.
2. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
3. In alto a destra, fare clic su **Downloads** (Download) e selezionare **Download VDA** (Scarica VDA). Si viene reindirizzati alla pagina di download VDA. Trovare il programma di installazione VDA desiderato e fare clic su **Download File** (Scarica file).
4. Al termine del download, eseguirlo. Utilizzare le opzioni descritte in questo articolo.

- Per Virtual Delivery Agent con sistema operativo multisessione, eseguire `VDAServerSetup.exe`
- Per Virtual Delivery Agent con sistema operativo a sessione singola, eseguire `VDAWorkstationSetup.exe`
- Per Core Services Virtual Delivery Agent per sistema operativo a sessione singola, eseguire `VDAWorkstationCoreSetup.exe`

Per estrarre i file prima di installarli, utilizzare `/extract` con il percorso assoluto, ad esempio `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia` (la directory deve esistere. In caso contrario, l'estrazione non andrà a buon fine). Quindi, in un comando separato, eseguire il comando appropriato, utilizzando le opzioni valide elencate in questo articolo.

- Per `VDAServerSetup_XXXX.exe`, eseguire `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- Per `VDAWorkstationCoreSetup_XXXX.exe`, eseguire `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- Per `VDAWorkstationSetup_XXXX.exe`, eseguire `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

### Opzioni della riga di comando per installare un VDA

Le seguenti opzioni sono valide con uno o più comandi: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` e `VDAWorkstationCoreSetup.exe`.

- **/componenti** *componente*[,*componente*]

  Elenco separato da virgole di componenti da installare o rimuovere. I valori validi sono:

  - **VDA:** Virtual Delivery Agent
  - **PLUGINS:** app Citrix Workspace per Windows

  Per installare il VDA e l'app Citrix Workspace, specificare `/components vda,plugins`.

  Se l'opzione `plugins` viene omessa, viene installato solo il VDA (non l'app Citrix Workspace).

  Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Tale programma di installazione non può installare l'app Citrix Workspace.

- **/controllers** "*controller* [*controller*]…"

  Nomi di dominio completi separati da spazi dei connettori Citrix Cloud con cui il VDA può comunicare, racchiusi tra virgolette diritte. Non specificare entrambe le opzioni `/site_guid` e `/controllers`.

- **/disableexperiencemetrics**

  Impedisce l'invio automatico a Citrix delle analisi raccolte durante l'installazione, l'aggiornamento o la rimozione.

- **/enable_hdx_ports**

  Apre le porte del firewall di Windows richieste dal VDA e dalle funzionalità abilitate (ad eccezione di Assistenza remota di Windows), se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall. Per informazioni sulle porte, vedere Porte di rete.

  Per aprire le porte UDP utilizzate dal trasporto adattivo HDX, specificare l'opzione `/enable_hdx_udp_ports`, oltre all'opzione `/enable_hdx_ports`.

- **/enable_hdx_udp_ports**

  Apre le porte UDP del firewall di Windows utilizzate dal trasporto adattivo HDX, se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall. Per informazioni sulle porte, vedere Porte di rete.

  Per aprire le porte utilizzate dal VDA, specificare l'opzione `/enable_hdx_ports`, oltre all'opzione `/enable_hdx_udp_ports`.

- **/enable_real_time_transport**

  Abilita o disabilita l'uso di UDP per i pacchetti audio (RealTime Audio Transport per audio). L'attivazione di questa funzione può migliorare le prestazioni audio. Includere l'opzione `/enable_hdx_ports` se si desidera che le porte UDP vengano aperte automaticamente quando viene rilevato il servizio Windows Firewall.

- **/enable_remote_assistance**

  Abilita la funzionalità di shadowing in Assistenza remota di Windows per utilizzarla con le funzioni **Monitor** (Monitoraggio). Se si specifica questa opzione, Assistenza remota di Windows apre le porte dinamiche del firewall.

- **/enablerestore** o **/enablerestorecleanup**

  (valido solo per VDA a sessione singola) Abilita il ritorno automatico al punto di ripristino, se l'installazione o l'aggiornamento del VDA non vanno a buon fine.

  Se l'installazione/aggiornamento viene completato correttamente:

  - `/enablerestorecleanup` indica al programma di installazione di rimuovere il punto di ripristino.
  - `/enablerestore` indica al programma di installazione di mantenere il punto di ripristino, anche se non è stato utilizzato.

Per ulteriori informazioni, vedere Ripristino in caso di errore di installazione o aggiornamento.

- **/enable_ss_ports**

  Apre le porte del firewall Windows necessarie per la condivisione dello schermo, se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall.

- **/exclude** "*componente*"[,"*componente*"]

  Impedisce l'installazione di uno o più componenti opzionali separati da virgole, ciascuno racchiuso tra virgolette diritte. Ad esempio, l'installazione o l'aggiornamento di un VDA su un' immagine non gestita da MCS richiede il componente Machine Identity Service. I valori validi sono:

  - Machine Identity Service
  - Citrix Profile Management:
  - Plug-in WMI Citrix Profile Management
  - Personalizzazione Citrix per App-V - VDA
  - Strumenti di supportabilità Citrix
  - Citrix MCS IODriver
  - Agente di aggiornamento Citrix VDA
  - Citrix Rendezvous V2

  L'esclusione di Citrix Profile Management dall'installazione (`/exclude "Citrix Profile Management"`) influisce sul monitoraggio e sulla risoluzione dei problemi dei VDA dalla scheda **Monitor** (Monitoraggio). Nelle pagine **User details** (Dettagli utente) ed **EndPoint**, i pannelli Personalization e Logon Duration riportano errori. Nelle pagine **Dashboard** e **Trends** (Trend), il pannello Average Logon Duration (Durata media dell'accesso) visualizza i dati solo per le macchine su cui è installato Profile Management.

  Anche se si utilizza una soluzione di gestione dei profili di terze parti, Citrix consiglia di installare ed eseguire Citrix Profile Management Service. L'attivazione del servizio Citrix Profile Management non è necessaria.

  Se si prevede di utilizzare MCS per il provisioning delle macchine virtuali, non escludere il servizio di identità della macchina.

  Se si specificano sia `/exclude` che `/includeadditional` con lo stesso nome di componente, tale componente non viene installato.

  Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Tale programma di installazione esclude automaticamente molti di questi elementi.

- **/h** o **/help**

  Visualizza la Guida dei comandi.

- **/includeadditional** "*component*"[,"*component*"] …

  Include l'installazione di uno o più componenti opzionali separati da virgole, ciascuno racchiuso tra virgolette diritte. I nomi dei componenti fanno distinzione tra maiuscole e minuscole.

  Questa opzione può risultare utile quando si crea una distribuzione di Accesso remoto PC e si desidera installare altri componenti non inclusi per impostazione predefinita. I valori validi sono:

  - Citrix Profile Management:
  - Plug-in WMI Citrix Profile Management
  - Personalizzazione Citrix per App-V - VDA
  - Strumenti di supportabilità Citrix
  - Citrix MCS IODriver
  - Agente di aggiornamento Citrix VDA
  - Citrix Rendezvous V2
  - Livello di personalizzazione utente
  - Strumento di registrazione Citrix Web Socket VDA

  Se si specificano entrambi `/exclude` e `/includeadditional` con lo stesso nome di componente, tale componente non viene installato.

- **/installdir** *directory*

  Directory vuota esistente in cui verranno installati i componenti. Impostazione predefinita= c:\Programmi\Citrix.

- **/install_mcsio_driver**

  Non utilizzare. Utilizzare invece `/includeadditional "Citrix MCS IODriver"` o `/exclude "Citrix MCS IODriver"`

- **/logpath** *percorso*

  Percorso del file di registro. La cartella specificata deve esistere. Il programma di installazione non la crea. Impostazione predefinita= "%TEMP%\Citrix\XenDesktop Installer"

  Questa opzione non è disponibile nell'interfaccia grafica.

- **/masterimage**

  Valido solo quando si installa un VDA in una macchina virtuale. Imposta il VDA come immagine. Questa opzione è equivalente a `/mastermcsimage`.

  Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`.

- **/mastermcsimage**

  Specifica che questa macchina verrà utilizzata come immagine con Machine Creation Services. Questa opzione è equivalente a `/masterimage`.

- **/masterpvsimage**

  Specifica che la macchina verrà utilizzata come immagine con Citrix Provisioning o uno strumento di provisioning di terze parti (ad esempio Microsoft System Center Configuration Manager).

- **/no_mediafoundation_ack**

  Riconosce che Microsoft Media Foundation non è installato e diverse funzionalità multimediali HDX non sono installate e non funzionano. Se questa opzione viene omessa e Media Foundation non è installato, l'installazione del VDA non riesce. La maggior parte delle edizioni di Windows supportate ha Media Foundation già installato, ad eccezione delle edizioni N.

- **/nodesktopexperience**

  Valida solo quando si installa un VDA con sistema operativo multisessione. Impedisce l'attivazione della funzionalità Enhanced desktop experience. Questa funzione è inoltre controllata con l'impostazione dei criteri Enhanced Desktop Experience Citrix.

- **/noreboot**

  Impedisce un riavvio dopo l'installazione. Il VDA non può essere utilizzato fino a dopo un riavvio.

- **/noresume**

  Per impostazione predefinita, quando è necessario un riavvio della macchina durante un'installazione, il programma di installazione riprende automaticamente al termine del riavvio. Per ignorare il valore predefinito, specificare `/noresume`. Ciò può risultare utile se è necessario rimontare il supporto o acquisire informazioni durante un'installazione automatica.

- **/portnumber** *porta*

  Valido solo quando viene specificata l'opzione `/reconfig`. Numero di porta da abilitare per le comunicazioni tra il VDA e il Controller. La porta configurata in precedenza è disabilitata, a meno che non sia la porta 80.

- **/proxyconfig** "*indirizzo o percorso del file PAC*"

  Valido solo se il comando contiene `/includeadditional "Citrix Rendezvous V2"`. L'indirizzo o il percorso del file PAC del proxy da utilizzare con il protocollo Rendezvous. Per dettagli delle funzionalità, vedere Protocollo Rendezvous.

  - Formato dell'indirizzo proxy: `http://<url-or-ip>:<port>`
  - Formato del file PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** o **/passive**

  Durante l'installazione non viene visualizzata alcuna interfaccia utente. L'unica prova del processo di installazione e configurazione è in Task Manager di Windows. Se questa opzione viene omessa, viene avviata l'interfaccia grafica.

- **/reconfigure**

  Consente di personalizzare le impostazioni del VDA configurate in precedenza se utilizzate con le opzioni `/portnumber`, `/controllers` o `/enable_hdx_ports`. Se si specifica questa opzione senza specificare anche l'opzione `/quiet`, viene avviata l'interfaccia grafica per la personalizzazione del VDA.

- **/remotepc**

  Valido solo per le distribuzioni di Accesso remoto PC (sistema operativo a sessione singola) o per le connessioni mediate (sistema operativo multisessione).

  Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Tale programma di installazione esclude automaticamente l'installazione di questi componenti.

- **/remove_appdisk_ack**

  Autorizza il programma di installazione del VDA a disinstallare il plug-in VDA AppDisks, se è installato.

- **/remove_pvd_ack**

  Autorizza il programma di installazione VDA a disinstallare Personal vDisk se è installato.

- **/remove**

  Rimuove i componenti specificati con l'opzione `/components`.

- **/removeall**

  Rimuove il VDA. Non rimuove l'app Citrix Workspace (se installata).

- **/sendexperiencemetrics**

  Invia automaticamente a Citrix le analisi raccolte durante l'installazione, l'aggiornamento o la rimozione. Se questa opzione viene omessa (o viene specificata l'opzione `/disableexperiencemetrics`), le analisi vengono raccolte localmente, ma non inviate automaticamente.

- **/servervdi**

  Installa un VDA con sistema operativo a sessione singola su un server Windows supportato. Omettere questa opzione quando si installa un VDA multisessione su un server Windows. Prima di utilizzare questa opzione, vedere VDI del server.

- **/site_guid** *guid*

  Identificatore univoco globale (GUID) dell'unità organizzativa (OU) di Active Directory del sito. Questo associa un desktop virtuale a un sito quando si utilizza Active Directory per l'individuazione (l'aggiornamento automatico è il metodo di individuazione consigliato e predefinito). Il GUID del sito è una proprietà del sito visualizzata in **Manage > Full Configuration** (Gestione > Configurazione completa). Non specificare entrambe le opzioni `/site_guid` e `/controllers`.

- **/tempdir** *directory*

  Directory in cui contenere i file temporanei durante l'installazione. Impostazione predefinita= c:\Windows\Temp.

  Questa opzione non è disponibile nell'interfaccia grafica.

- **/virtualmachine**

  Valido solo quando si installa un VDA in una macchina virtuale. Sovrascrive l'individuazione da parte del programma di installazione di una macchina fisica, in cui le informazioni del BIOS passate alle macchine virtuali le fanno apparire come macchine fisiche.

  Questa opzione non è disponibile nell'interfaccia grafica.

- **/xendesktopcloud**

  Indica che il VDA è installato in una distribuzione di Citrix DaaS (Citrix Cloud).

### Esempi: installare un VDA

- **Installare un VDA su un sistema operativo multisessione.** Il seguente comando installa un VDA su un sistema operativo multisessione.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/
  enable_hdx_ports /masterimage
  ```

  Il VDA verrà utilizzato come immagine.

- **Installare un VDA per sistema operativo multisessione o un VDA per sistema operativo a sessione singola.** Il comando seguente installa un VDA per sistema operativo multisessione o un VDA per sistema operativo a sessione singola.

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com",
  "ddc2.abc.com"/enable_hdx_ports /enable_Remote_Assistance /
  enable_real_time_transport /enable_ss_ports /noreboot
  ```

  Separare uno dall'altro i nomi di dominio completi di tutti i controller di consegna con una virgola. Notare che `XXXX` rappresenta la versione del VDA.

- **Installare un Core Services VDA su un sistema operativo a sessione singola.** Il comando seguente installa un VDA di Core Services in un sistema operativo a sessione singola per l'utilizzo in una distribuzione VDA o Accesso remoto PC.

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.
  domain.com"/enable_hdx_ports /noreboot
  ```

  L'app Citrix Workspace e altri servizi non core non vengono installati. Viene specificato l'indirizzo di un Cloud Connector e le porte del servizio Windows Firewall vengono aperte automaticamente. L'amministratore gestisce i riavvii.

### Personalizzare un VDA utilizzando la riga di comando

Dopo aver installato un VDA, è possibile personalizzare diverse impostazioni. Eseguire `XenDesktopVDASetup.exe` utilizzando una o più delle seguenti opzioni.

- `/reconfigure` (necessario per la personalizzazione di un VDA)
- `/h` o `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

### Passaggi successivi

- Creare cataloghi di macchine
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.

## Creare e gestire le connessioni

December 5, 2023

### Introduzione

La configurazione di una connessione include la selezione del tipo di connessione tra gli hypervisor e i servizi cloud supportati e l'archiviazione e la rete selezionate dalle *risorse* per tale connessione.

È necessario essere un amministratore completo per eseguire attività di connessione e gestione delle risorse.

#### Dove trovare informazioni sui tipi di connessione

I requisiti di sistema elencano le versioni supportate dell'hypervisor e del servizio cloud e includono collegamenti ad articoli specifici dell'host.

### Archiviazione host

Un prodotto di archiviazione è supportato se può essere gestito da un hypervisor supportato. Citrix Support assiste i fornitori di prodotti di archiviazione nella risoluzione e nella risoluzione dei problemi e documenta tali problemi nel Knowledge Center, secondo necessità.

Quando si esegue il provisioning delle macchine, i dati sono classificati per tipo:

- Dati del sistema operativo (OS), incluse le immagini.
- Dati temporanei, che includono tutti i dati non persistenti scritti su macchine con provisioning MCS, file di pagina di Windows, dati del profilo utente e tutti i dati sincronizzati con Content Collaboration (precedentemente ShareFile). Questi dati vengono eliminati ogni volta che una macchina si riavvia.

Fornire archiviazione separata per ogni tipo di dati può ridurre il carico e migliorare le prestazioni IOPS su ciascun dispositivo di archiviazione, sfruttando al meglio le risorse disponibili dell'host. Consente inoltre di utilizzare lo storage appropriato per i diversi tipi di dati. La persistenza e la resilienza sono più importanti per alcuni dati rispetto ad altri.

- L'archiviazione può essere condivisa (in posizione centrale, separato da qualsiasi host, utilizzato da tutti gli host) o locale per un hypervisor. Ad esempio, l'archiviazione condivisa centrale può essere costituita da uno o più volumi di archiviazione in cluster di Windows Server 2012 (con o senza archiviazione collegata) o un'appliance di un fornitore di archiviazione. L'archiviazione centrale potrebbe anche fornire ottimizzazioni quali i percorsi di controllo dell'archiviazione dell'hypervisor e l'accesso diretto tramite plug-in di partner.
- L'archiviazione locale di dati temporanei evita di dover attraversare la rete per accedere allo storage condiviso e riduce anche il carico (IOPS) sul dispositivo di archiviazione condiviso. L'archiviazione condivisa può essere più costosa, quindi l'archiviazione locale dei dati può ridurre le spese. I vantaggi devono essere valutati in base alla disponibilità di spazio di archiviazione sufficiente sui server hypervisor.

### Archiviazione condivisa dagli hypervisor

Il metodo di archiviazione condivisa dagli hypervisor memorizza centralmente i dati che necessitano di persistenza a lungo termine, fornendo backup e gestione centralizzati. Tale archiviazione contiene i dischi del sistema operativo.

Quando si seleziona questo metodo, è possibile scegliere se utilizzare l'archiviazione locale (su server nello stesso pool di hypervisor) per i dati temporanei della macchina. Questi dati non richiedono persistenza o la stessa resilienza dei dati nell'archiviazione condivisa. Questa operazione è denominata *cache temporanea dei dati*. Il disco locale aiuta a ridurre il traffico verso l'archiviazione principale del sistema operativo. Il disco viene cancellato dopo ogni riavvio della macchina. Il disco è accessibile tramite una cache di memoria write-through. Tenere presente che se si utilizza l'archiviazione locale per i dati temporanei, il VDA sottoposto a provisioning è collegato a un host hypervisor specifico. Se l'host è in condizione di errore, la macchina virtuale non può essere avviata.

**Eccezione:** se si utilizza Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager non accetta la creazione di dischi di cache dei dati temporanei nell'archiviazione locale.

Se si memorizzano dati temporanei localmente, è possibile abilitare e configurare valori non predefiniti per il disco cache e le dimensioni della memoria di ogni macchina virtuale quando si crea un catalogo di macchine che utilizza tale connessione. Tuttavia, i valori predefiniti sono personalizzati per il tipo di connessione e sono sufficienti nella maggior parte dei casi.

L'hypervisor è inoltre in grado di fornire tecnologie di ottimizzazione attraverso la memorizzazione nella cache in lettura delle immagini del disco a livello locale. Ad esempio, Citrix Hypervisor offre IntelliCache. Ciò consente inoltre di ridurre il traffico di rete verso l'archiviazione centrale.

### Archiviazione locale per l'hypervisor

Il metodo di archiviazione locale per l'hypervisor consente di archiviare i dati localmente sull'hypervisor. Con questo metodo, le immagini e altri dati del sistema operativo vengono trasferiti a tutti gli hypervisor utilizzati nel sito, sia per la creazione iniziale della macchina che per gli aggiornamenti futuri delle immagini. Questo processo si traduce in un traffico significativo sulla rete di gestione. Inoltre il trasferimento delle immagini richiede molto tempo e le immagini diventano disponibili per ciascun host in un momento diverso.

### Creare una connessione e risorse

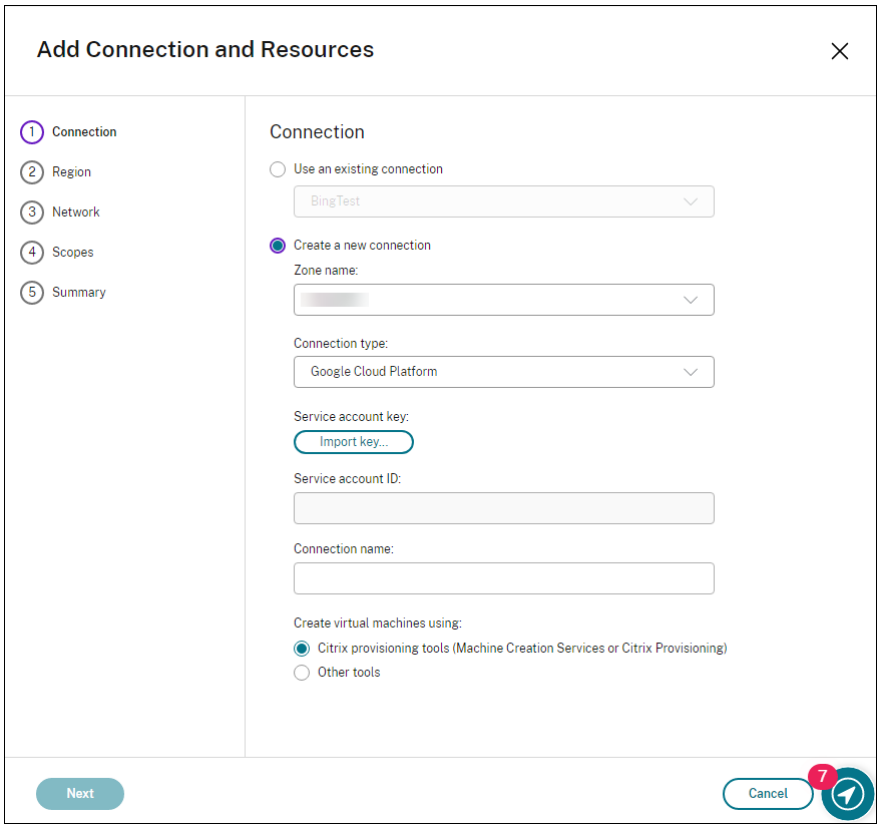
> **Importante:**
>
> Le risorse dell'host (archiviazione e rete) nella posizione delle risorse devono essere disponibili prima della creazione di una connessione.

1. Accedere a Citrix Cloud.
2. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
3. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
4. Selezionare **Add Connections and Resources** (Aggiungi connessioni e risorse) nella barra delle azioni.

5. La procedura guidata guida l'utente attraverso le pagine seguenti. Il contenuto specifico della pagina dipende dal tipo di connessione selezionato. Dopo aver completato ogni pagina, fare clic su **Next** (Avanti) fino a raggiungere la pagina **Summary** (Riepilogo).

### Passaggio 1. Connessione




Nella pagina **Connection**:

- Per creare una connessione, selezionare **Create a new Connection** (Crea una nuova connessione). Per creare una connessione basata sulla stessa configurazione host di una connessione esistente, selezionare **Use an existing Connection** (Usa una connessione esistente) e quindi scegliere la connessione pertinente.
- Selezionare una zona nel campo **Zone name** (Nome zona). Le opzioni sono tutte le posizioni risorsa configurate.
- Selezionare un hypervisor o un servizio cloud nel campo **Connection type** (Tipo di connessione). Le opzioni includono tutti gli hypervisor e i servizi cloud supportati da Citrix:
  - Per una posizione risorsa senza connettori cloud accessibili, sono disponibili solo hypervisor e servizi cloud che supportano le implementazioni senza connettori.

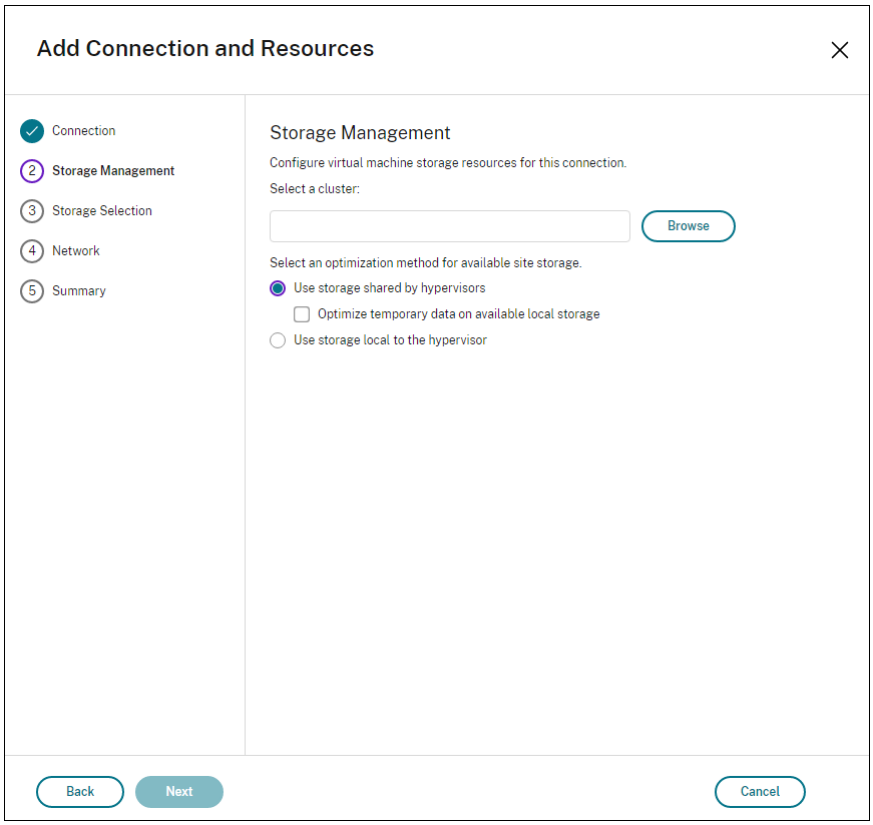
  - Per una posizione risorsa con connettori cloud accessibili, sono disponibili solo gli hypervisor e i servizi cloud i cui plug-in sono installati correttamente su tali connettori.

  In alternativa, è possibile utilizzare il comando PowerShell `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false o true per ottenere l'elenco degli hypervisor e dei servizi cloud disponibili.

- Immettere un nome per la connessione. Questo nome viene visualizzato nel display **Manage** (Gestisci).
- Scegliere lo strumento per creare macchine virtuali: Machine Creation Services o Citrix Provisioning.

Le informazioni nella pagina **Connection** (Connessione) variano a seconda dell'host (tipo di connessione) che si sta utilizzando. Ad esempio, quando si utilizza Azure Resource Manager, è possibile utilizzare un'entità servizio esistente o crearne una nuova. Per ulteriori informazioni, vedere la pagina dell'ambiente di virtualizzazione elencata in System requirements (Requisiti di sistema) per il tipo di connessione.

### Passaggio 2. Gestione dell'archiviazione




Per informazioni sui tipi e sui metodi di gestione dell'archiviazione, vedere Archiviazione host.

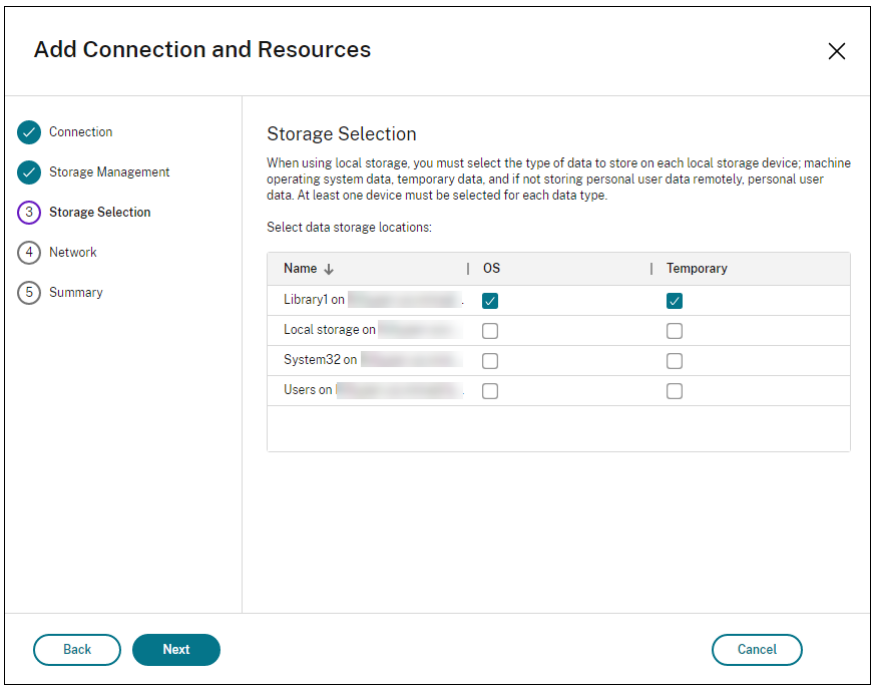
Se si sta configurando una connessione a un host Hyper-V o VMware, selezionare un nome di cluster. Altri tipi di connessione non richiedono un nome di cluster.

Selezionare un metodo di gestione dell'archiviazione: archiviazione condivisa dagli hypervisor o archiviazione locale per l'hypervisor.

- Se si sceglie l'archiviazione condivisa dagli hypervisor, indicare se si desidera conservare i dati temporanei sulla posizione di archiviazione locale disponibile (è possibile specificare dimensioni di archiviazione temporanea non predefinite nei cataloghi di macchine che utilizzano questa connessione). **Eccezione:** quando si utilizza Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager non accetta che vengano creati dischi di cache dei dati temporanei sull'archiviazione locale. La configurazione della gestione dell'archiviazione nella console di **gestione** non riesce.

Se si utilizza l'archiviazione condivisa in un pool Citrix Hypervisor, indicare se si desidera utilizzare IntelliCache per ridurre il carico sul dispositivo di archiviazione condiviso. Vedere Ambienti di virtualizzazione Citrix Hypervisor.

### Passaggio 3. Gestione delle risorse di archiviazione




Per ulteriori informazioni sulla selezione dell'archiviazione, vedere Archiviazione host.

Selezionare almeno un dispositivo di archiviazione host per ogni tipo di dati disponibile. Il metodo di gestione dell'archiviazione selezionato nella pagina precedente influisce sui tipi di dati selezionabili in questa pagina. Selezionare almeno un dispositivo di archiviazione per ogni tipo di dati supportato prima di passare alla pagina successiva della procedura guidata.

La parte inferiore della pagina **Storage Selection** (Selezione archiviazione) contiene ulteriori opzioni di configurazione se si sceglie l'archiviazione condivisa dagli hypervisor e se è stata abilitata l'opzione **Optimize temporary data on available local storage** (Ottimizza i dati temporanei sull'archiviazione locale disponibile). È possibile selezionare i dispositivi di archiviazione locale (nello stesso pool di hypervisor) da utilizzare per i dati temporanei.

Viene visualizzato il numero di dispositivi di archiviazione attualmente selezionati (nell'immagine "1 storage device selected"[1 dispositivo di archiviazione selezionato]). Quando si passa il mouse su quella voce, vengono visualizzati i nomi dei dispositivi selezionati (a meno che non sia stato configurato nessun dispositivo).

1. Scegliere **Select** (Seleziona) per modificare i dispositivi di archiviazione da utilizzare.
2. Nella finestra di dialogo **Select Storage** (Seleziona archiviazione), selezionare o deselezionare le caselle di controllo del dispositivo di archiviazione e quindi selezionare **OK**.

### Passaggio 4. Regione

(Viene visualizzata solo per alcuni tipi di host) La selezione della regione indica dove verranno distribuite le macchine virtuali. Si consiglia di scegliere una regione vicina a quella in cui gli utenti accederanno alle loro applicazioni.

### Passaggio 5. Rete

Immettere un nome per le risorse. Questo nome viene visualizzato nella console di gestione per identificare la combinazione di archiviazione e rete associata alla connessione.

Selezionare una o più reti utilizzate dalle macchine virtuali.

Alcuni tipi di connessione (ad esempio Azure Resource Manager) elencano anche le subnet che verranno utilizzate dalle macchine virtuali. Selezionare una o più subnet.

### Passaggio 6. Riepilogo

Esaminare le selezioni effettuate. Se si desidera apportare modifiche, utilizzare il tasto per tornare alle pagine precedenti della procedura guidata. Una volta completata la valutazione, selezionare **Finish** (Fine).

**Da ricordare**: se si memorizzano dati temporanei localmente, è possibile configurare valori non predefiniti per l'archiviazione temporanea dei dati quando si crea il catalogo contenente le macchine che utilizzano questa connessione.

> **Nota:**
>
> Un ambito non viene mostrato per gli amministratori con accesso completo. Per ulteriori informazioni, vedere Amministratori, ruoli e ambiti.

### Modificare le impostazioni di connessione

Non utilizzare questa procedura per rinominare o creare una connessione. Si tratta di operazioni diverse. Modificare l'indirizzo solo se la macchina host corrente ha un nuovo indirizzo. L'immissione di un indirizzo in una macchina diversa interrompe i cataloghi delle macchine che usano quella connessione.

Non è possibile modificare le impostazioni della GPU per una connessione, poiché i cataloghi che accedono a questa risorsa devono utilizzare un'immagine master specifica della GPU appropriata. Occorre invece creare una nuova connessione.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione e quindi selezionare **Edit Connection** (Modifica connessione) nella barra delle azioni.
3. Seguire le indicazioni per le impostazioni disponibili quando si modifica una connessione.
4. Al termine, selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

Pagina **Connection Properties** (Proprietà connessione):

- Per modificare l'indirizzo e le credenziali di connessione, selezionare **Edit settings...** (Modifica impostazioni) e quindi immettere le nuove informazioni.
- Per specificare i server ad alta disponibilità per una connessione Citrix Hypervisor, selezionare **Edit servers** (Modifica server) e selezionare i server. Citrix consiglia di selezionare tutti i server del pool per consentire la comunicazione con Citrix Hypervisor in caso di errore del pool master.

  > **Nota:**
  >
  > Se si utilizza HTTPS e si desidera configurare server ad alta disponibilità, non installare un certificato wildcard per tutti i server di un pool. È richiesto un certificato individuale per ogni server. Per ulteriori informazioni, vedere Creare una connessione a Citrix Hypervisor.

Pagina **Advanced**:

Le impostazioni della soglia di limitazione consentono di specificare un numero massimo di azioni di alimentazione consentite su una connessione. Queste impostazioni possono essere utili quando le impostazioni di gestione dell'alimentazione consentono l'avvio di troppe o troppo poche macchine

contemporaneamente. Ogni tipo di connessione ha valori predefiniti specifici appropriati per la maggior parte dei casi. Di solito, non hanno bisogno di essere cambiati.

- Le impostazioni **Simultaneous actions (all types)** (Azioni simultanee [tutti i tipi]) e **Simultaneous Personal vDisk inventory updates** (Aggiornamenti simultanei dell'inventario di Personal vDisk) specificano due valori: un numero assoluto massimo che può verificarsi contemporaneamente su questa connessione e una percentuale massima del totale di macchine che utilizzano questa connessione. È necessario specificare valori sia assoluti che percentuali. Il limite effettivo applicato è il valore più basso.

  Ad esempio, in una distribuzione con 34 macchine, se l'opzione **Simultaneous actions (all types)** (Azioni simultanee [tutti i tipi]) è impostata su un valore assoluto di 10 e un valore percentuale di 10, il limite effettivo applicato è 3 (ovvero il 10% di 34 arrotondato al numero intero più vicino, che è inferiore al valore assoluto di 10 macchine).
- Il valore contenuto in **Maximum new actions per minute** (numero massimo di nuove azioni al minuto) è un numero assoluto. Non esiste un valore percentuale.

Pagina **Shared Tenants** (Tenant condivisi):

Aggiungere tenant e sottoscrizioni che condividono la Raccolta di calcolo di Azure con la sottoscrizione di questa connessione. Di conseguenza, quando si creano o si aggiornano i cataloghi, è possibile selezionare immagini condivise da questi tenant e sottoscrizioni.

- Inserire l'**ID applicazione** e il **segreto dell'applicazione** per l'applicazione associata a questa connessione. Con queste informazioni, è possibile autenticarsi in Azure. Si consiglia di cambiare regolarmente le chiavi per garantire la sicurezza.
- Specificare i tenant e le sottoscrizioni condivisi. È possibile aggiungere fino a otto tenant condivisi. Per ogni tenant, è possibile aggiungere fino a otto sottoscrizioni.
- Al termine, fare clic su **Save** (Salva) e su **Apply** (Applica).

Immettere le informazioni nel campo **Connection options** (Opzioni di connessione) solo sotto la guida di un rappresentante dell'assistenza Citrix.

#### Modificare le reti

È possibile cambiare rete per una connessione. Effettuare le seguenti operazioni:

1. Passare a **Manage > Full Configuration > Hosting**.
2. Selezionare le risorse di destinazione all'interno della connessione, quindi selezionare **Edit Network** (Modifica rete) nella barra delle azioni.
3. Selezionare una o più reti che potranno essere utilizzate dalle macchine virtuali.
4. Fare clic su **Save** per salvare le modifiche e uscire.

### Attivare o disattivare la modalità di manutenzione per una connessione

L'attivazione della modalità di manutenzione per una connessione impedisce che qualsiasi nuova azione di alimentazione influisca su qualsiasi macchina archiviata nella connessione. Gli utenti non possono connettersi a una macchina quando è in modalità di manutenzione. Se vi sono utenti già connessi, la modalità di manutenzione ha effetto quando si scollegano.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione. Per attivare la modalità di manutenzione, selezionare **Turn On Maintenance Mode** (Attiva modalità di manutenzione) nella barra delle azioni. Per disattivare la modalità di manutenzione, selezionare **Turn Off Maintenance Mode** (Disattiva modalità di manutenzione).

È inoltre possibile attivare o disattivare la modalità di manutenzione per le singole macchine. È possibile attivare o disattivare la modalità di manutenzione per le macchine incluse nei cataloghi delle macchine o nei gruppi di consegna.

### Eliminare una connessione

> **Attenzione:**
>
> L'eliminazione di una connessione può comportare l'eliminazione di un gran numero di macchine e la perdita di dati. Assicurarsi che i dati utente sulle macchine interessate siano sottoposti a backup o non più necessari.

Prima di eliminare una connessione, assicurarsi che:

- Tutti gli utenti vengono scollegati dalle macchine memorizzate sulla connessione.
- Nessuna sessione utente disconnessa è in esecuzione.
- La modalità di manutenzione è attivata per macchine in pool e dedicate.
- Tutte le macchine presenti nei cataloghi delle macchine utilizzati dalla connessione sono spente.

Un catalogo delle macchine diventa inutilizzabile quando si elimina una connessione a cui fa riferimento. Se a questa connessione viene fatto riferimento da un catalogo, è possibile eliminare il catalogo. Prima di eliminare un catalogo, assicurarsi che non sia utilizzato da altre connessioni.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione e quindi selezionare **Delete Connection** (Elimina connessione) nella barra delle azioni.

3. Se su questa connessione sono archiviate delle macchine, viene chiesto se tali macchine devono essere eliminate. Se devono essere eliminate, specificare cosa fare con gli account computer di Active Directory associati.

### Rinominare o verificare una connessione

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione e quindi scegliere **Rename Connection** (Rinomina connessione) o **Test Connection** (Verifica connessione) nella barra delle azioni.

### Visualizzare i dettagli di una macchina su una connessione

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione e quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.

Il riquadro superiore contiene un elenco delle macchine a cui si accede tramite la connessione. Selezionare una macchina per visualizzarne i dettagli nel riquadro inferiore. Sono inoltre forniti i dettagli della sessione per le sessioni aperte.

Usare la funzione di ricerca per trovare rapidamente le macchine. Selezionare una ricerca salvata dall'elenco nella parte superiore della finestra o creare una nuova ricerca. È possibile eseguire la ricerca digitando il nome della macchina intero o parte di esso oppure creare un'espressione da utilizzare per una ricerca avanzata. Per creare un'espressione, selezionare **Unfold** (Espandi) e quindi selezionare gli elementi desiderati dagli elenchi di proprietà e operatori.

### Gestire le macchine su una connessione

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione e quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
3. Nella barra delle azioni selezionare una delle opzioni seguenti. Alcune azioni potrebbero non essere disponibili in determinati stati della macchina e con determinati tipi di host di connessione.

    - **Start** (Avvia): avvia la macchina se è spenta o in sospeso.

- **Suspend** (Sospendi): mette in pausa la macchina senza arrestarla e aggiorna l'elenco delle macchine.
- **Shut down** (Arresto): richiede l'arresto del sistema operativo.
- **Force shut down** (Spegnimento forzato): spegne forzatamente la macchina e aggiorna l'elenco delle macchine.
- **Restart** (Riavvio): richiede al sistema operativo di arrestare e quindi riavviare la macchina. Se il sistema operativo non è in grado di eseguire la procedura, la macchina rimane nello stato corrente.
- **Enable maintenance mode** (Attiva modalità di manutenzione): interrompe temporaneamente le connessioni a una macchina. Gli utenti non possono connettersi a una macchina che si trova in questo stato. Se vi sono utenti connessi, la modalità di manutenzione avrà effetto quando si scollegheranno. È anche possibile attivare o disattivare la modalità di manutenzione per tutte le macchine a cui si accede tramite una connessione, come descritto sopra.
- **Remove from Delivery Group** (Rimuovi dal gruppo di consegna): la rimozione di una macchina dal gruppo di consegna non la elimina dal catalogo delle macchine utilizzato dal gruppo di consegna. È possibile rimuovere una macchina solo quando non è connesso alcun utente. Attivare la modalità di manutenzione per impedire temporaneamente agli utenti di connettersi durante la rimozione della macchina.
- **Delete** (Elimina): quando si elimina una macchina, gli utenti non potranno più accedervi e la macchina viene eliminata dal catalogo delle macchine. Prima di eliminare una macchina, assicurarsi che tutti i dati utente siano sottoposti a backup o che non siano più necessari. È possibile eliminare una macchina solo quando non vi è connesso alcun utente. Attiva la modalità di manutenzione per impedire temporaneamente agli utenti di connettersi durante l'eliminazione della macchina.

Per le azioni che comportano l'arresto della macchina, se la macchina non chiude la sessione entro 10 minuti, viene spenta. Se Windows tenta di installare aggiornamenti durante l'arresto, c'è il rischio che la macchina venga spenta prima del completamento degli aggiornamenti.

### Modificare lo spazio di archiviazione

È possibile visualizzare lo stato dei server utilizzati per l'archiviazione del sistema operativo e dei dati temporanei e personali (PvD) per le macchine virtuali che utilizzano una connessione. È inoltre possibile specificare quali server utilizzare per l'archiviazione di ciascun tipo di dati.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione e quindi selezionare **Edit Storage** (Modifica archiviazione) nella barra delle azioni.

3. Nel riquadro di sinistra, selezionare il tipo di dati: sistema operativo o temporanei.
4. Selezionare o deselezionare le caselle di controllo di uno o più dispositivi di archiviazione per il tipo di dati selezionato.
5. Selezionare **OK**.

Per ciascun dispositivo di archiviazione incluso nell'elenco sono indicati il nome e lo stato di archiviazione. I valori validi dello stato di archiviazione sono:

- **In use** (In uso): lo spazio di archiviazione è in uso per creare macchine.
- **Superseded** (Sostituito): lo spazio di archiviazione è in uso solo per le macchine esistenti. Non vengono aggiunte nuove macchine a questo spazio di archiviazione.
- **Not in use** (Non in uso): lo spazio di archiviazione non viene utilizzato per la creazione di macchine.

Se si deseleziona la casella di controllo di un dispositivo attualmente in stato **In use**, il suo stato diventa **Superseded**. Le macchine esistenti continueranno a utilizzare quel dispositivo di archiviazione (e potranno scrivervi dati). Pertanto, tale posizione può diventare piena anche dopo che non viene più utilizzata per la creazione di macchine.

### Eliminare, rinominare o testare le risorse

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la risorsa e quindi selezionare la voce appropriata nella barra delle azioni: **Delete Resources** (Elimina risorse), **Rename Resources** (Rinomina risorse) o **Test Resources** (Verifica risorse).

### Rilevare le risorse di Azure orfane

Le risorse orfane sono risorse inutilizzate presenti nel sistema e possono comportare spese inutili.

Questa funzionalità consente di rilevare le risorse Azure orfane negli host del proprio sito cloud.

Effettuare le operazioni seguenti su Citrix DaaS:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare una connessione, quindi selezionare **Detect Orphaned Resources** (Rileva risorse orfane) nella barra delle azioni. La finestra di dialogo **Detect Orphaned Resources** visualizza il rapporto sulle risorse orfane.
3. Per visualizzare il rapporto sulle risorse orfane, selezionare **View Report** (Visualizza rapporto).

In alternativa, è possibile rilevare le risorse Azure orfane usando PowerShell. Per ulteriori informazioni, vedere Recuperare un elenco di risorse orfane.

Per comprendere i motivi alla base delle risorse orfane e per scoprire come procedere ulteriormente, vedere Efficiently manage Orphaned Azure resources with Citrix.

### Timer di connessione

È possibile utilizzare le impostazioni dei criteri Citrix per configurare tre timer di connessione:

- **Maximum connection timer** (Timer di connessione massima): determina la durata massima di una connessione ininterrotta tra un dispositivo utente e un desktop virtuale. Utilizzare le impostazioni dei criteri **Session connection timer** (Timer di connessione sessione) e **Session connection timer interval** (Intervallo del timer di connessione sessione).
- **Connection idle timer** (Timer di inattività della connessione): determina per quanto tempo viene mantenuta una connessione ininterrotta del dispositivo utente a un desktop virtuale se non è presente alcun input da parte dell'utente. Utilizzare le impostazioni dei criteri **Session idle timer** (Timer di inattività sessione) e **Session idle timer interval** (Intervallo del timer di inattività sessione).
- **Disconnect timer** (Timer di disconnessione): determina per quanto tempo un desktop virtuale disconnesso e bloccato può rimanere bloccato prima che la sessione venga scollegata. Utilizzare le impostazioni dei criteri **Disconnected session timer** (Timer sessione disconnessa) e **Disconnected session timer interval** (Intervallo del timer sessione disconnessa).

Quando si aggiorna una di queste impostazioni, assicurarsi che siano coerenti in tutta la distribuzione.

Per ulteriori informazioni, vedere la documentazione sulle impostazioni dei criteri.

### Recuperare un elenco di risorse orfane

È possibile ottenere un elenco di risorse orfane create da MCS ma non più tracciate da MCS. Per ottenere l'elenco, è possibile usare i comandi di PowerShell. È possibile filtrare utilizzando le connessioni.

> **Nota:**
>
> - Questa funzionalità è attualmente applicabile solo agli ambienti Azure.
> - Il comando PowerShell viene rifiutato se è in corso un provisioning o un aggiornamento dell'immagine.
> - Una risorsa gestita dal cliente contrassegnata con tutti i tag Citrix viene rilevata come risorsa orfana. Tuttavia, se si aggiunge a quella risorsa un altro tag CitrixDetectIgnore con valore

> true, la risorsa viene ignorata durante il rilevamento delle risorse orfane.

Limitazioni:

- Solo un utente amministratore completo integrato o amministratore del cloud può eseguire il comando PowerShell e ottenere l'elenco delle risorse orfane.
- Per evitare il riconoscimento errato delle risorse orfane, non accendere le macchine virtuali mentre si stanno filtrando le risorse orfane.
- Circa 2.000 record vengono visualizzati come orfani in caso di possibile carico di lavoro pesante.
- L'elenco dei gruppi di risorse orfane non è attualmente disponibile.

Per visualizzare l'elenco delle risorse orfane:

1. Aprire una finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Eseguire i seguenti comandi:

```
$pluginId = 'AzureRmFactory'
$connections = Get-ChildItem xdhyp:\connections | where {
  $_.PluginId -eq $pluginId  }

get-provorphanedresource -HypervisorConnectionUid $connections.
   HypervisorConnectionUid
<!--NeedCopy-->
```

Per visualizzare l'elenco delle risorse orfane da un ID di abbonamento:

1. Aprire una finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Eseguire i seguenti comandi:

```
$connections = Get-ChildItem xdhyp:\connections | where {
  $_.CustomProperties -match '<subscriptionId>'  }

get-provorphanedresource -HypervisorConnectionUid $connections.
   HypervisorConnectionUid
<!--NeedCopy-->
```

### Passaggi successivi

- Per informazioni sulla connessione a tipi di host specifici, vedere:
  - Connessione ad AWS
  - Connessione a Citrix Hypervisor

- Connessione agli ambienti cloud di Google
- Connessione a Microsoft Azure
- Connessione a Microsoft System Center Virtual Machine Manager
- Connessione a Nutanix
- Connessione alle soluzioni Nutanix Cloud e dei partner
- Connessione a VMware
- Connessione al cloud VMware e alle soluzioni dei partner

Se ci si trova nel processo di distribuzione iniziale, creare un catalogo delle macchine.

## Connessione ad AWS

December 18, 2023

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud AWS.

> **Nota:**
>
> Prima di creare una connessione ad AWS, è prima necessario completare la configurazione del proprio account AWS come posizione delle risorse. Vedere Ambienti cloud AWS.

### Creare una connessione

Quando si crea una connessione dall'interfaccia Full Configuration (Configurazione completa):

- È necessario fornire la chiave API e i valori della chiave segreta. È possibile esportare il file chiave contenente tali valori da AWS e quindi importarli. È inoltre necessario fornire la regione, la zona di disponibilità, il nome del VPC, gli indirizzi delle subnet, il nome di dominio, i nomi dei gruppi di sicurezza e le credenziali.
- Il file delle credenziali per l'account AWS radice (recuperato dalla console AWS) non è formattato come i file delle credenziali scaricati per gli utenti AWS standard. Pertanto, la gestione di Citrix Virtual Apps and Desktops non può utilizzare il file per popolare i campi della chiave API e della chiave segreta. Assicurarsi di utilizzare i file delle credenziali di AWS Identity Access Management (IAM).

> **Nota:**
>
> Dopo aver creato una connessione, i tentativi di aggiornamento della chiave API e della chiave segreta potrebbero non riuscire. Per risolvere il problema, controllare le restrizioni del server proxy o del firewall e assicurarsi che il seguente indirizzo sia contattabile: `https://*`.

> amazonaws.com.

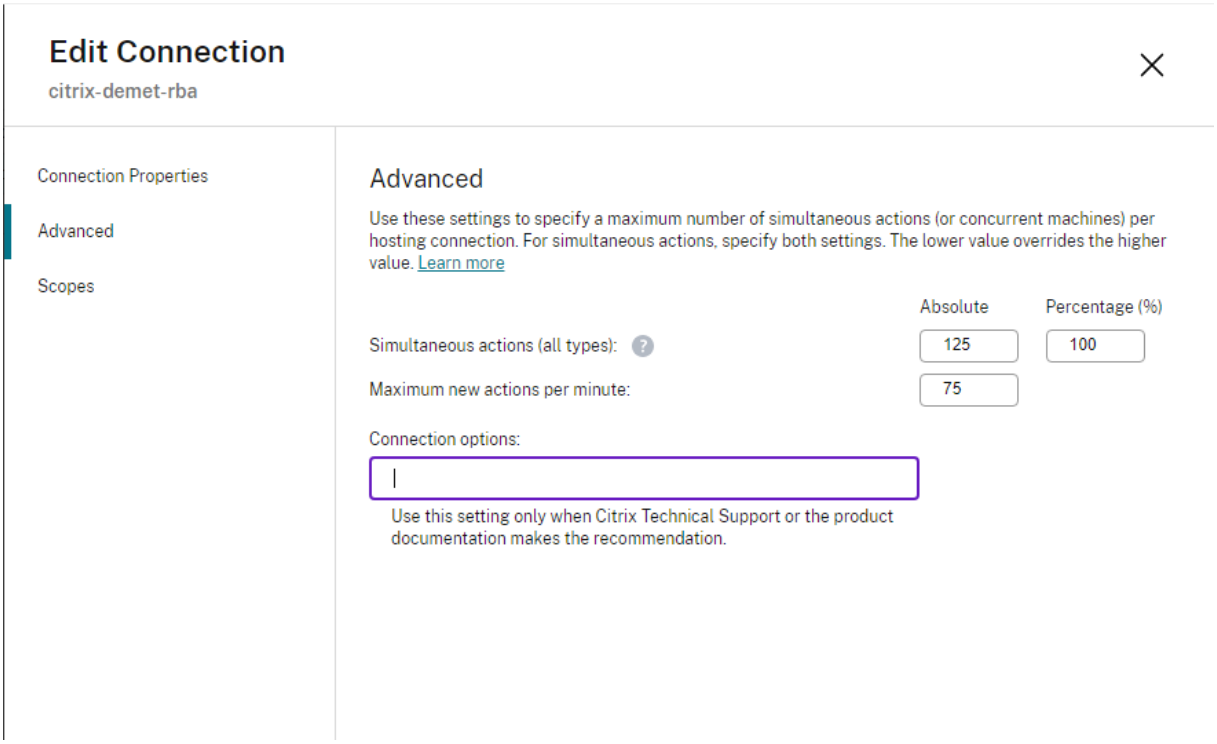
**Valori predefiniti della connessione host**

Nell'interfaccia Full Configuration (Configurazione completa), quando si creano connessioni host in ambienti cloud AWS, vengono visualizzati i seguenti valori predefiniti:

| Opzione | Valore assoluto | Percentuale |
|---|---|---|
| Azioni simultanee (tutti i tipi) | 125 | 100 |
| Numero massimo di nuove azioni al minuto | 125 | |
| Numero massimo di operazioni di provisioning simultanee | 100 | |

MCS supporta 100 operazioni di provisioning simultanee massime per impostazione predefinita.

È possibile configurare questi valori accedendo alla sezione **Advanced** (Avanzate) di Citrix Studio nella schermata **Edit Connection** (Modifica connessione):




MCS supporta massimo 100 operazioni simultanee per impostazione predefinita. In alternativa, è possibile utilizzare l'SDK Remote PowerShell per impostare il numero massimo di operazioni simultanee in modo da raggiungere le impostazioni ottimali per il proprio ambiente.

Utilizzare la proprietà PowerShell personalizzata `MaximumConcurrentProvisioningOperations` per specificare il numero massimo di operazioni di provisioning simultanee di AWS.

Prima della configurazione:

- Assicurarsi di aver installato l'SDK PowerShell per Cloud.
- Tenere presente che il valore predefinito per `MaximumConcurrentProvisioningOperations` è 100.

Per personalizzare il valore `MaximumConcurrentProvisioningOperations`, effettuare le seguenti operazioni:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Inserire `cd xdhyp:\Connections\`.
4. Accedere a `dir` per elencare le connessioni.
5. Modificare o inizializzare la stringa Custom Properties (Proprietà personalizzate):
   - Se la stringa Custom Properties (Proprietà personalizzate) ha un valore, copiare le proprietà personalizzate nel Blocco note. Successivamente, modificare la proprietà `MaximumConcurrentProvisioningOperations` sul valore preferito. È possibile immettere un valore compreso tra 1 e 1000.
     Ad esempio, `<Property xsi:type="IntProperty"Name="MaximumConcurrentProvis`
     `"Value="xyz"/>`.
   - Se la stringa Custom Properties (Proprietà personalizzate) è vuota/null, è necessario inizializzare la stringa immettendo la sintassi corretta sia per lo schema che per la proprietà `MaximumConcurrentProvisioningOperations`.
6. Nella finestra di **PowerShell**, incollare le proprietà personalizzate modificate dal Blocco note e assegnare una variabile alle proprietà personalizzate modificate. Se le proprietà personalizzate sono state inizializzate, aggiungere le righe seguenti seguendo la sintassi:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
   org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'.
   ```

   Questa stringa imposta la proprietà `MaximumConcurrentProvisioningOperations` su 100. Nella stringa Custom Properties (Proprietà personalizzate), è necessario impostare la proprietà `MaximumConcurrentProvisioningOperations` su un valore in linea con le proprie esigenze.

7. Inserire `Get-XDAuthentication`, che richiede di immettere le credenziali.
8. Eseguire `$cred = Get-Credential`, che potrebbe richiedere solo una password (o un nome utente e una password). È inoltre possibile che venga richiesto l'ID dell'applicazione e il segreto associato. Per le connessioni che utilizzano l'autenticazione basata sui ruoli,**role_based_auth** è sia il nome utente che la password. Altrimenti, inserire l'ID e il segreto dell'API AWS.
9. Eseguire `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. È necessario impostare *<connection-name>* sul nome della connessione.
10. Immettere `dir` per verificare la stringa CustomProperties (Priorietà personalizzate) aggiornata.

## URL dell'endpoint del servizio

### URL dell'endpoint del servizio di zona standard

Quando si utilizza MCS, viene aggiunta una nuova connessione AWS con una chiave API e un segreto API. Con queste informazioni, insieme all'account autenticato, MCS interroga AWS per le zone supportate utilizzando la chiamata API EC2 AWS DescribeRegions. La query viene effettuata utilizzando un URL generico dell'endpoint del servizio EC2 `https://ec2.amazonaws.com/`. Utilizzare MCS per selezionare la zona per la connessione dall'elenco delle zone supportate. L'URL dell'endpoint del servizio AWS preferito viene selezionato automaticamente per la zona. Tuttavia, dopo aver creato l'URL dell'endpoint del servizio, non è più possibile impostarlo o modificarlo.

### URL dell'endpoint del servizio non standard

In alcune situazioni potrebbe non essere necessario l'URL dell'endpoint del servizio AWS scelto automaticamente per la connessione. In questi casi, è possibile utilizzare l'SDK Citrix Cloud e PowerShell per creare una connessione con un URL dell'endpoint del servizio non standard. Ad esempio, per creare una connessione utilizzando l'URL dell'endpoint del servizio `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Configurare il Cloud Connector ospitato da AWS e assicurarsi che disponga di connettività.
2. Eseguire i seguenti comandi PowerShell per visualizzare l'elenco dei Cloud Connector.

```
1  PS C:> asnp citrix.*
2  PS C:> Get-XDAuthentication
3  PS C:> Get-ConfigEdgeServer
4 <!--NeedCopy-->
```

3. Individuare lo ZoneUID dal Cloud Connector appena creato e inserirlo nei seguenti comandi PowerShell. Sostituire gli elementi in corsivo con i rispettivi valori.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUidZoneUid-
Name"My New Connection"-ConnectionType "AWS"-HypervisorAddress @
("https://ec2.cn-north-1.amazonaws.com.cn")-UserName"APIkey" -
Password"API Secret" -Persist
PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
 $hyp. HypervisorConnectionUid
```

4. Aggiornare la scheda **Full Configuration > Hosting** (Configurazione completa > Hosting) per verificare che la connessione EC2 sia stata creata.
5. Aggiungere una posizione risorsa utilizzando la nuova connessione.

### Definizione delle autorizzazioni IAM

Utilizzare le informazioni in questa sezione per definire le autorizzazioni IAM per Citrix DaaS su AWS. Il servizio IAM di Amazon consente account con più utenti, che possono essere ulteriormente organizzati in gruppi. Questi utenti possono disporre di autorizzazioni diverse per controllare la loro capacità di eseguire operazioni associate all'account. Per ulteriori informazioni sulle autorizzazioni IAM, vedere Riferimento alla policy JSON IAM.

Per applicare la policy delle autorizzazioni IAM a un nuovo gruppo di utenti:

1. Accedere alla Console di gestione AWS e selezionare il **servizio IAM** dall'elenco a discesa.
2. Selezionare **Create a New Group of Users** (Crea un nuovo gruppo di utenti).
3. Digitare un nome per il nuovo gruppo di utenti e selezionare **Continue** (Continua).
4. Nella pagina **Permissions** (Autorizzazioni), scegliere **Custom Policy** (Criterio personalizzato), quindi **Select** (Seleziona).
5. Digitare un nome per il **criterio Permissions** (Autorizzazioni).
6. Nella sezione **Policy Document** (Documento del criterio), immettere le autorizzazioni pertinenti.

Dopo aver inserito le informazioni sul criterio, selezionare**Continue** (Continua) per completare il gruppo di utenti. Agli utenti del gruppo vengono concesse le autorizzazioni per eseguire solo le azioni richieste per Citrix DaaS.

> **Importante:**
>
> Utilizzare il testo del criterio fornito nell'esempio precedente per elencare le azioni utilizzate da Citrix DaaS per eseguire azioni all'interno di un account AWS senza limitare tali azioni a risorse

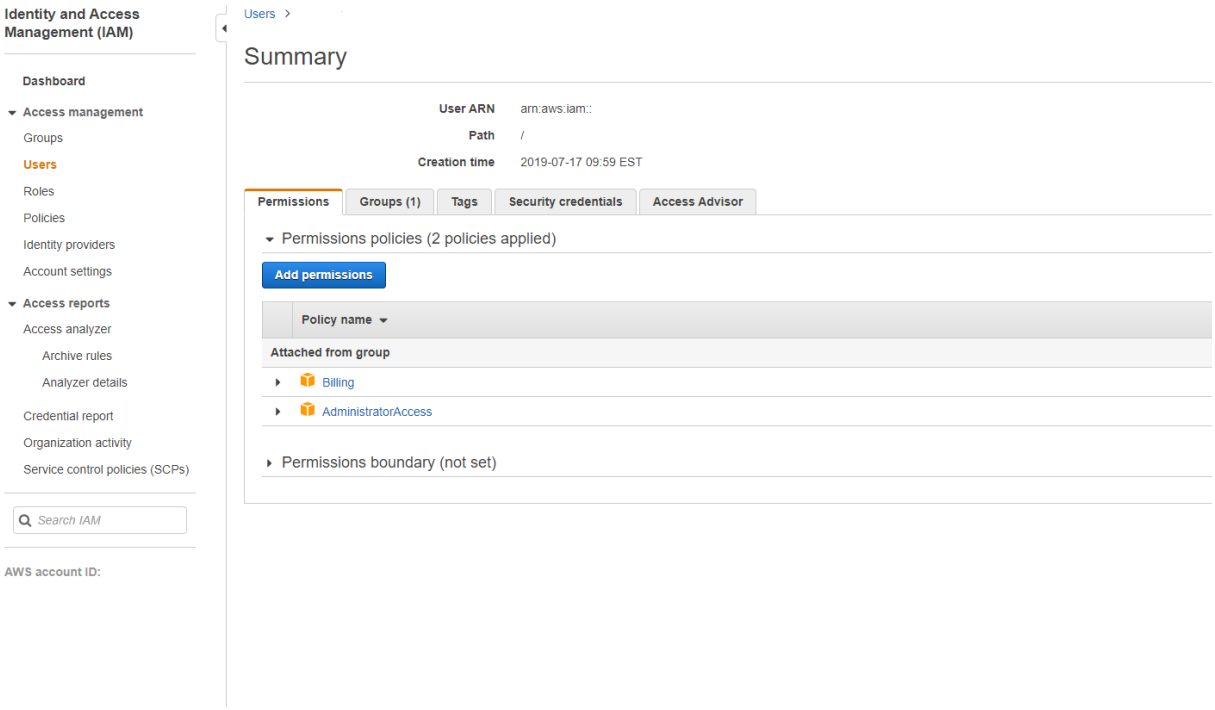
 

> specifiche. Citrix consiglia di utilizzare l'esempio a scopo di test. Per gli ambienti di produzione, è possibile scegliere di aggiungere ulteriori restrizioni sulle risorse.

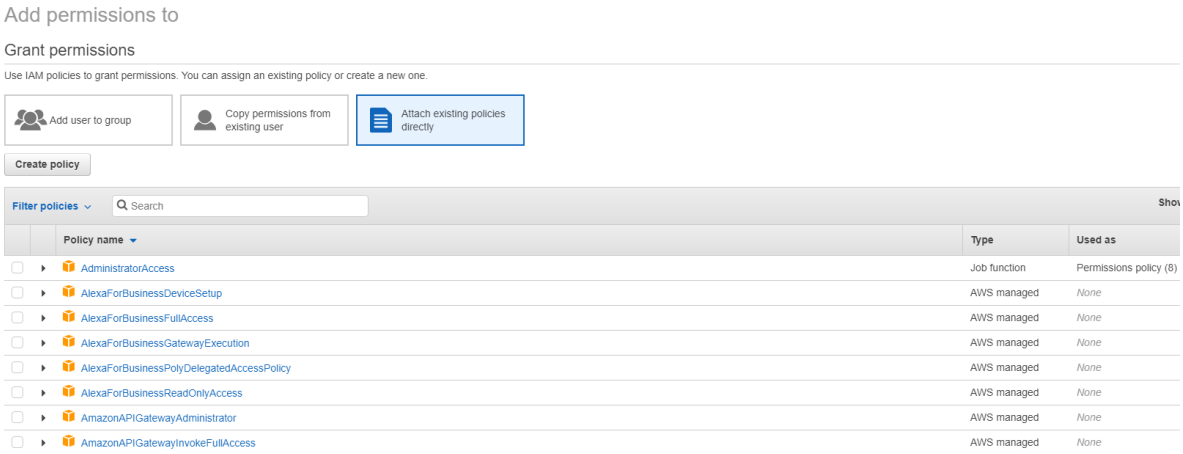
## Aggiunta di autorizzazioni IAM

Impostare le autorizzazioni nella sezione **IAM** della Console di gestione AWS:

1. Nel pannello **Summary** (Riepilogo), selezionare la scheda **Permissions** (Autorizzazioni).
2. Selezionare **Add permissions** (Aggiungi autorizzazioni).

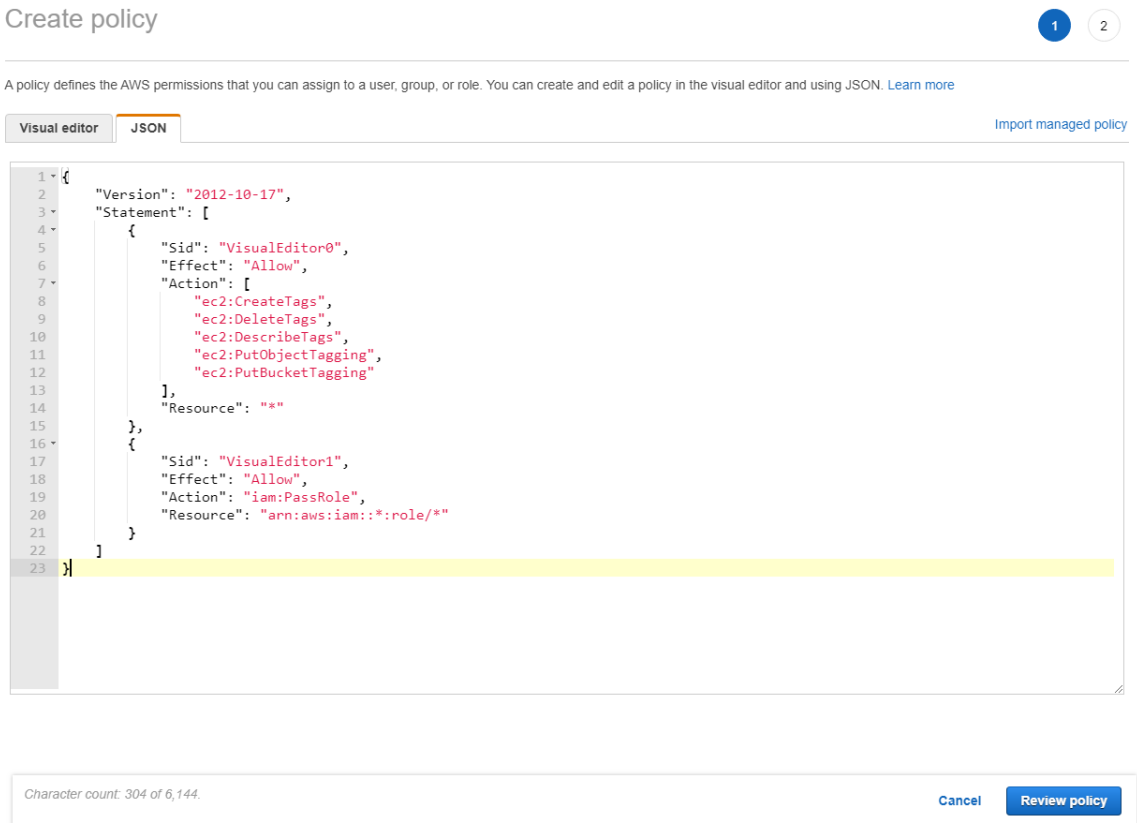



Nella schermata **Add Permissions to** (Aggiungi autorizzazioni a), concedere le autorizzazioni:



Utilizzare il seguente come esempio nella scheda **JSON**:




> **Suggerimento:**
>
> L'esempio JSON indicato potrebbe non includere tutte le autorizzazioni per l'ambiente. Per ulteriori informazioni, consultare l'articolo su come definire le autorizzazioni di gestione delle identità e degli accessi che eseguono Citrix Virtual Apps and Desktops su AWS.

## Informazioni sulle autorizzazioni AWS

Questa sezione contiene l'elenco completo delle autorizzazioni AWS. Usare il set completo di autorizzazioni indicato nella sezione per il corretto funzionamento della funzionalità.

> **Nota:**
>
> L'autorizzazione *iam:PassRole* è necessaria solo per **role_based_auth**.

### Creazione di una connessione host

Viene aggiunta una nuova connessione host utilizzando le informazioni ottenute da AWS.

```
1 {
2
```

```
    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

#### Gestione dell'alimentazione delle macchine virtuali

Le istanze delle macchine sono accese o spente.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

**Creazione, aggiornamento o eliminazione di macchine virtuali**

Un catalogo delle macchine viene creato, aggiornato o eliminato con macchine virtuali di cui viene eseguito il provisioning come istanze AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeElasticGpus",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "\*"
         }
```

```
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "\*"
         }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
}

<!--NeedCopy-->
```

> **Nota:**
>
> - La sezione EC2 relativa a SecurityGroups è necessaria solo se occorre creare un gruppo di sicurezza di isolamento per la macchina virtuale di preparazione durante la creazione del catalogo. Una volta completata questa operazione, queste autorizzazioni non sono necessarie.

**Caricamento e download diretti del disco** Il caricamento diretto del disco elimina il requisito del Volume Worker per il provisioning del catalogo delle macchine e utilizza invece le API pubbliche fornite da AWS. Questa funzionalità riduce i costi associati agli account di archiviazione aggiuntivi e alla complessità di gestire le operazioni di Volume Worker.

> **Nota:**
>
> Il supporto di Volume Worker è obsoleto.

Le seguenti autorizzazioni devono essere aggiunte al criterio:

- ebs:StartSnapshot
- ebs:GetSnapshotBlock
- ebs:PutSnapshotBlock
- ebs:CompleteSnapshot
- ebs:ListSnapshotBlocks
- ebs:ListChangedBlocks
- ec2:CreateSnapshot
- ec2:DescribeLaunchTemplates

> **Importante:**
>
> - È possibile aggiungere una nuova macchina virtuale ai cataloghi delle macchine esistenti senza alcuna operazione di Volume Worker, come l'AMI Volume Worker e la macchina virtuale del Volume Worker.
> - Se si elimina un catalogo esistente che utilizzava Volume Worker in precedenza, vengono eliminati tutti gli artefatti, inclusi quelli correlati a Volume Worker.

#### Crittografia EBS dei volumi creati

EBS può crittografare automaticamente i volumi appena creati se l'AMI è crittografata o EBS è configurato per crittografare tutti i nuovi volumi. Tuttavia, per implementare la funzionalità, è necessario includere le seguenti autorizzazioni nel criterio IAM.

```
1 {
2
```

```
      "Version": "2012-10-17",
      "Statement": [
         {

             "Effect": "Allow",
             "Action": [
                  "kms:CreateGrant",
                  "kms:Decrypt",
                  "kms:DescribeKey",
                  "kms:GenerateDataKeyWithoutPlainText",
                  "kms:GenerateDataKey",
                  "kms:ReEncryptTo",
                  "kms:ReEncryptFrom"
             ],
             "Resource": "*"
          }

     ]
 }

<!--NeedCopy-->
```

**Nota:**

Le autorizzazioni possono essere limitate a chiavi specifiche includendo un blocco di risorse e condizioni a discrezione dell'utente. Ad esempio, **autorizzazioni KMS con condizione**:

```
{

      "Version": "2012-10-17",
      "Statement": [
         {

             "Effect": "Allow",
             "Action": [
                  "kms:CreateGrant",
                  "kms:Decrypt",
                  "kms:DescribeKey",
                  "kms:GenerateDataKeyWithoutPlainText",
                  "kms:GenerateDataKey",
                  "kms:ReEncryptTo",
                  "kms:ReEncryptFrom"
             ],
             "Resource": [
                 "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                    -456d-a12b-a123b4cd56ef"
             ],
             "Condition": {

                 "Bool": {

                     "kms:GrantIsForAWSResource": true
                  }
```

```
26
27                }
28
29            }
30
31       ]
32    }
33
34   <!--NeedCopy-->
```

La seguente dichiarazione dei criteri chiave è l'intero criterio chiave predefinito per le chiavi KMS necessario per consentire all'account di utilizzare i criteri IAM per delegare l'autorizzazione per tutte le azioni (kms:*) sulla chiave KMS.

```
1  {
2
3  "Sid": "Enable IAM policies",
4  "Effect": "Allow",
5  "Principal": {
6
7  "AWS": "arn:aws:iam::111122223333:root"
8   }
9   ,
10 "Action": "kms:",
11 "Resource": ""
12  }
13
14 <!--NeedCopy-->
```

Per ulteriori informazioni, consultare la documentazione ufficiale di AWS Key Management Service.

#### Autenticazione basata su ruoli IAM

Le seguenti autorizzazioni vengono aggiunte per supportare l'autenticazione basata sui ruoli.

```
1  {
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": "iam:PassRole",
9              "Resource": "arn:aws:iam::\*:role/\*"
10          }
11
12      ]
13   }
14
15 <!--NeedCopy-->
```

### Criteri minimi delle autorizzazioni IAM

Il seguente JSON può essere utilizzato per tutte le funzionalità attualmente supportate. È possibile creare connessioni host, creare, aggiornare o eliminare macchine virtuali ed eseguire la gestione dell'alimentazione utilizzando questo criterio.
Il criterio può essere applicato agli utenti come spiegato nelle sezioni Definizione delle autorizzazioni IAM oppure è anche possibile utilizzare l'autenticazione basata su ruoli utilizzando la chiave di sicurezza **role_based_auth** e la chiave segreta.

> **Importante:**
>
> per utilizzare **role_based_auth**, configurare prima il ruolo IAM desiderato nell'istanza ec2 del Cloud Connector durante la configurazione del Cloud Connector. Utilizzando Citrix Studio, aggiungere la connessione di hosting e fornire role_based_auth per la chiave di autenticazione e il segreto. Una connessione di hosting con queste impostazioni utilizza quindi l'autenticazione basata su ruoli.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
```

```
                    "ec2:DescribeSecurityGroups",
                    "ec2:DescribeSnapshots",
                    "ec2:DescribeSubnets",
                    "ec2:DescribeTags",
                    "ec2:DescribeSpotInstanceRequests",
                    "ec2:DescribeInstanceCreditSpecifications",
                    "ec2:DescribeInstanceAttribute",
                    "ec2:DescribeElasticGpus",
                    "ec2:GetLaunchTemplateData",
                    "ec2:DescribeVolumes",
                    "ec2:DescribeVpcs",
                    "ec2:DetachVolume",
                    "ec2:DisassociateIamInstanceProfile",
                    "ec2:RebootInstances",
                    "ec2:RunInstances",
                    "ec2:StartInstances",
                    "ec2:StopInstances",
                    "ec2:TerminateInstances"
                ],
                "Effect": "Allow",
                "Resource": "\*"
            }
    ,
            {

                "Action": [
                    "ec2:AuthorizeSecurityGroupEgress",
                    "ec2:AuthorizeSecurityGroupIngress",
                    "ec2:CreateSecurityGroup",
                    "ec2:DeleteSecurityGroup",
                    "ec2:RevokeSecurityGroupEgress",
                    "ec2:RevokeSecurityGroupIngress"
                ],
                "Effect": "Allow",
                "Resource": "\*"
            }
    ,
            {

                "Action": [
                    "s3:CreateBucket",
                    "s3:DeleteBucket",
                    "s3:DeleteObject",
                    "s3:GetObject",
                    "s3:PutBucketAcl",
                    "s3:PutObject",
                    "s3:PutBucketTagging",
                    "s3:PutObjectTagging"
                ],
                "Effect": "Allow",
                "Resource": "arn:aws:s3:::citrix*"
            }
    ,
```

```
87          {
88
89              "Action": [
90                  "ebs:StartSnapshot",
91                  "ebs:GetSnapshotBlock",
92                  "ebs:PutSnapshotBlock",
93                  "ebs:CompleteSnapshot",
94                  "ebs:ListSnapshotBlocks",
95                  "ebs:ListChangedBlocks",
96                  "ec2:CreateSnapshot"
97              ],
98              "Effect": "Allow",
99              "Resource": "\*"
100          }
101  ,
102         {
103
104             "Effect": "Allow",
105             "Action": [
106                  "kms:CreateGrant",
107                  "kms:Decrypt",
108                  "kms:DescribeKey",
109                  "kms:GenerateDataKeyWithoutPlainText",
110                  "kms:GenerateDataKey",
111                  "kms:ReEncryptTo",
112                  "kms:ReEncryptFrom"
113             ],
114             "Resource": "\*"
115          }
116  ,
117         {
118
119             "Effect": "Allow",
120             "Action": "iam:PassRole",
121             "Resource": "arn:aws:iam::\*:role/\*"
122          }
123
124     ]
125  }
126
127  <!--NeedCopy-->
```

**Nota:**

- La sezione EC2 relativa a SecurityGroups è necessaria solo se occorre creare un gruppo di sicurezza di isolamento per la macchina virtuale di preparazione durante la creazione del catalogo. Una volta completata questa operazione, queste autorizzazioni non sono necessarie.
- La sezione KMS è necessaria solo quando si utilizza la crittografia del volume EBS.
- La sezione delle autorizzazioni iam:PassRole è necessaria solo per **role_based_auth**.

> - È possibile aggiungere autorizzazioni specifiche a livello di risorsa anziché l'accesso completo in base ai requisiti e all'ambiente. Per maggiori dettagli, consultare i documenti AWS Demystifying EC2 Resource-Level Permissions (Sfatare i miti relativi alle autorizzazioni a livello di risorsa EC2) e Gestione degli accessi per le risorse AWS.
> - Usare le autorizzazioni EC2:CreateNetworkInterface ed EC2:DeleteNetworkInterface solo se si utilizza il metodo Volume Worker.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su AWS, vedere Creare un catalogo di AWS.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti cloud AWS

## Connessione a Citrix Hypervisor

January 3, 2023

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione Citrix Hypervisor.

> **Nota:**
>
> Prima di creare una connessione a Citrix Hypervisor, è prima necessario completare la configurazione del proprio account Citrix Hypervisor come posizione delle risorse. Vedere Ambienti di virtualizzazione Citrix Hypervisor.

### Creare una connessione a Citrix Hypervisor

Quando si crea una connessione a Citrix Hypervisor (in precedenza XenServer), è necessario fornire le credenziali di amministratore "power"VM o un utente di livello superiore.

Citrix consiglia di utilizzare HTTPS per proteggere le comunicazioni con Citrix Hypervisor. Per utilizzare HTTPS, è necessario sostituire il certificato TLS predefinito installato su Citrix Hypervisor. Per ulteriori informazioni, vedere Install a TLS certificate on your server.

È possibile configurare la disponibilità elevata se è abilitata sul server Citrix Hypervisor. Citrix consiglia di selezionare tutti i server del pool (da **Edit High Availability**) per consentire la comunicazione con il server Citrix Hypervisor in caso di errore del pool master.

> **Nota:**
>
> Se si utilizza HTTPS e si desidera configurare server ad alta disponibilità, non installare un certificato wildcard per tutti i server di un pool. È richiesto un certificato individuale per ogni server.

È possibile selezionare un tipo di GPU e un gruppo, o pass-through, se Citrix Hypervisor supporta vGPU. Il display indica se la selezione dispone di risorse GPU dedicate.

Quando si utilizza l'archiviazione locale su uno o più host Citrix Hypervisor per l'archiviazione temporanea dei dati, assicurarsi che ogni posizione di archiviazione nel pool abbia un nome univoco. Per modificare un nome in XenCenter, fare clic con il pulsante destro del mouse sulla posizione di archiviazione e modificare la proprietà del nome.

### Utilizzare IntelliCache per le connessioni Citrix Hypervisor

Utilizzando IntelliCache, le distribuzioni VDI ospitate sono più convenienti perché è possibile utilizzare una combinazione di archiviazione condivisa e archiviazione locale. Ciò migliora le prestazioni e riduce il traffico di rete. L'archiviazione locale memorizza nella cache l'immagine master dall'archivio condiviso, riducendo la quantità di letture sulla posizione di archiviazione condivisa. Per i desktop condivisi, le scritture sui dischi diversi vengono scritte nell'archiviazione locale dell'host e non nell'archiviazione condivisa.

- L'archiviazione condivisa deve essere NFS quando si utilizza IntelliCache.
- Citrix consiglia di utilizzare un dispositivo di archiviazione locale ad alte prestazioni per garantire il trasferimento dati più rapido possibile.

Per utilizzare IntelliCache, è necessario attivarlo sia in questo prodotto che in Citrix Hypervisor.

- Durante l'installazione di Citrix Hypervisor, selezionare **Enable thin provisioning (Optimized storage for Citrix Virtual Desktops)** (Abilita thin provisioning [Archiviazione ottimizzata per Virtual Desktops]). Citrix non supporta pool misti di server in cui IntelliCache è abilitato e server in cui non lo è. Per ulteriori informazioni, vedere la documentazione di Citrix Hypervisor.
- In Citrix Virtual Apps and Desktops, IntelliCache è disabilitato per impostazione predefinita. È possibile modificare l'impostazione solo quando si crea una connessione Citrix Hypervisor; non è possibile disabilitare IntelliCache in un secondo momento. Quando si aggiunge una connessione Citrix Hypervisor:
  - Selezionare **Shared** (Condivisa) come tipo di archiviazione.
  - Selezionare la casella di controllo **Use IntelliCache**.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su Citrix Hypervisor, vedere Creare un catalogo di Citrix Hypervisor.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti di virtualizzazione Citrix Hypervisor

## Connessione agli ambienti cloud di Google

November 21, 2023

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici degli ambienti cloud di Google.

> **Nota:**
>
> Prima di creare una connessione agli ambienti cloud di Google, è prima necessario completare la configurazione del proprio account cloud Google come posizione delle risorse. Vedere Ambienti Google Cloud.

### Aggiungere una connessione

Nell'interfaccia Full Configuration (Configurazione completa), seguire le indicazioni in Create a connection and resources(Crea una connessione e risorse). La seguente descrizione guida l'utente nella configurazione di una connessione di hosting:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare **Add Connections and Resources** (Aggiungi connessioni e risorse) nella barra delle azioni.
3. Nella pagina **Connection** (Connessione), selezionare **Create a new Connection** (Crea una nuova connessione) e **Citrix provisioning tools** (Strumenti di provisioning Citrix), quindi selezionare **Next** (Avanti).
    - **Zone name** (Nome zona). Selezionare una zona (equivalente a una posizione risorsa) in cui si desidera che risiedano le risorse host. Le zone vengono create automaticamente

quando si crea una posizione risorsa e si aggiunge un Cloud Connector. Per ulteriori informazioni, vedere Zone.

- **Tipo di connessione**. Selezionare **Google Cloud** dal menu.
- **Chiave dell'account di servizio**. Importare la chiave contenuta nel file delle credenziali di Google (.json). A questo scopo, individuare il file delle credenziali, aprirlo con Blocco note (o qualsiasi editor di testo), quindi copiare il contenuto. Successivamente, tornare alla pagina **Connection** (Connessione), selezionare **Import key** (Chiave di importazione), incollare il contenuto e quindi selezionare **Save** (Salva).
- **ID account di servizio**. Il campo viene compilato automaticamente con le informazioni della chiave importata.
- **Nome connessione**. Digitare un nome per la connessione.
- **Indirizzare il traffico tramite Citrix Cloud Connector**. Per indirizzare le richieste API tramite un connettore Citrix Cloud disponibile, selezionare questa casella di controllo. È anche possibile selezionare la casella di controllo **Enable Google Cloud Build to use private pools** (Abilita Google Cloud Build per utilizzare pool privati) per un ulteriore livello di sicurezza.

  In alternativa, è possibile abilitare questa funzionalità utilizzando PowerShell. Per ulteriori informazioni, vedere Creare un ambiente sicuro per il traffico gestito di GCP.

> **Nota:**
>
> Questa opzione è disponibile solo quando nella distribuzione sono presenti Citrix Cloud Connector attivi. Attualmente, questa funzionalità non è supportata per le Connector Appliance.

4. Nella pagina **Region** (Regione), selezionare un nome di progetto dal menu, selezionare una regione contenente le risorse che si desidera utilizzare, quindi selezionare **Next** (Avanti).
5. Nella pagina **Network** (Rete) digitare un nome per le risorse, selezionare una rete virtuale dal menu, selezionare un sottoinsieme e quindi selezionare **Next** (Avanti). Il nome della risorsa aiuta a identificare la regione e la combinazione di rete. Le reti virtuali con il suffisso *(Shared)* (Condivisa) aggiunto al loro nome rappresentano i VPC condivisi. Se si configura un ruolo IAM a livello di subnet per un VPC condiviso, nell'elenco delle subnet vengono visualizzate solo le subnet specifiche del VPC condiviso.

> **Nota:**
>
> - Il nome della risorsa può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. Nella pagina **Summary** (Riepilogo), confermare le informazioni e quindi selezionare **Finish** (Fine) per uscire dalla finestra **Add Connection and Resources** (Aggiungi connessione e risorse).

Dopo aver creato la connessione e le risorse, vengono elencate la connessione e le risorse create. Per configurare la connessione, selezionare la connessione e quindi selezionare l'opzione applicabile nella barra delle azioni.

Allo stesso modo, è possibile eliminare, rinominare o testare le risorse create con la connessione. A tale scopo, selezionare la risorsa sotto la connessione e quindi selezionare l'opzione applicabile nella barra delle azioni.

### URL dell'endpoint del servizio

È necessario avere accesso ai seguenti URL:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

### Progetti Google Cloud

Esistono fondamentalmente due tipi di progetti Google Cloud:

- Progetto di provisioning: in questo caso, l'account amministratore corrente possiede i computer forniti nel progetto. Questo progetto viene anche definito progetto locale.
- Progetto VPC condiviso: progetto in cui le macchine create nel progetto di provisioning utilizzano il VPC del progetto Shared VPC. L'account amministratore utilizzato per il progetto di provisioning ha autorizzazioni limitate in questo progetto, in particolare solo autorizzazioni per utilizzare il VPC.

### Creare un ambiente sicuro per il traffico gestito di GCP

È possibile consentire solo l'accesso privato di Google ai propri progetti Google Cloud. Questa implementazione migliora la sicurezza per la gestione dei dati sensibili. A questo scopo:

1. Installare Cloud Connectors nel VPC in cui si intende applicare i controlli del servizio VPC. Per ulteriori informazioni, vedere Controlli di servizio VPC.

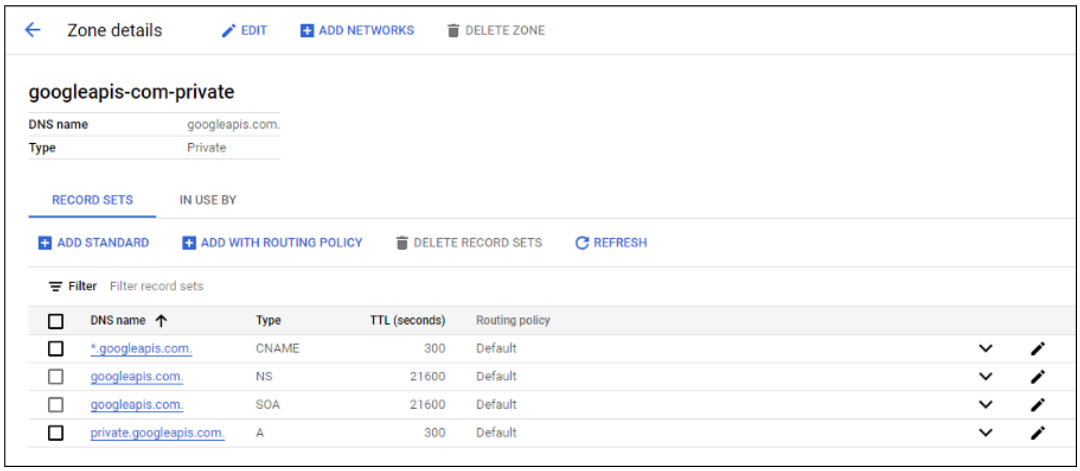
2. Aggiungere `ProxyHypervisorTrafficThroughConnector` in `CustomProperties` in caso di implementazione di Citrix Cloud. Se si utilizza un pool di lavoratori privato, aggiungere `UsePrivateWorkerPool` in `CustomProperties`. Per informazioni sul pool di lavoratori privati, vedere Panoramica dei pool privati.

> **Nota:**
>
> Attualmente, questa funzionalità non è supportata per Connector Appliance.

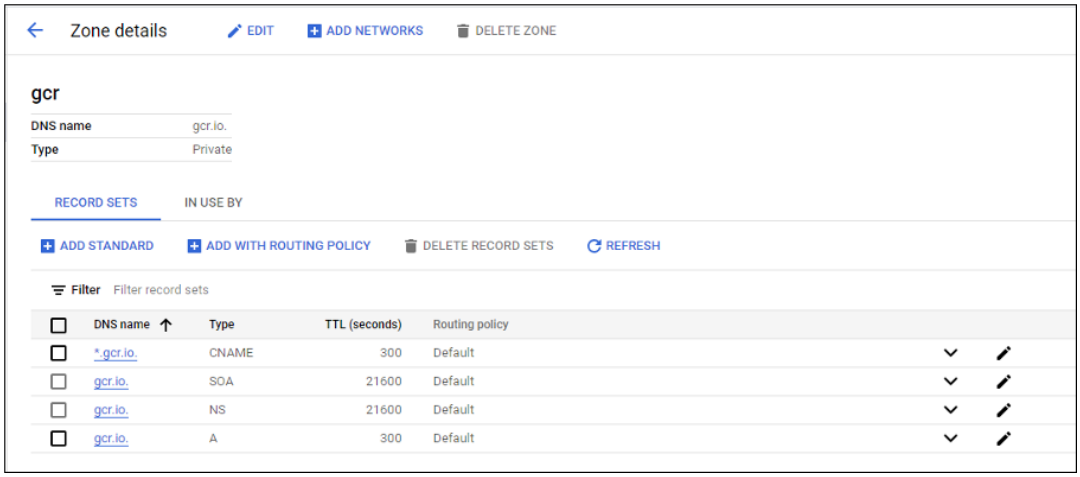
### Requisiti per creare un ambiente sicuro per il traffico gestito da GCP

I requisiti per creare un ambiente sicuro per il traffico gestito GCP sono:

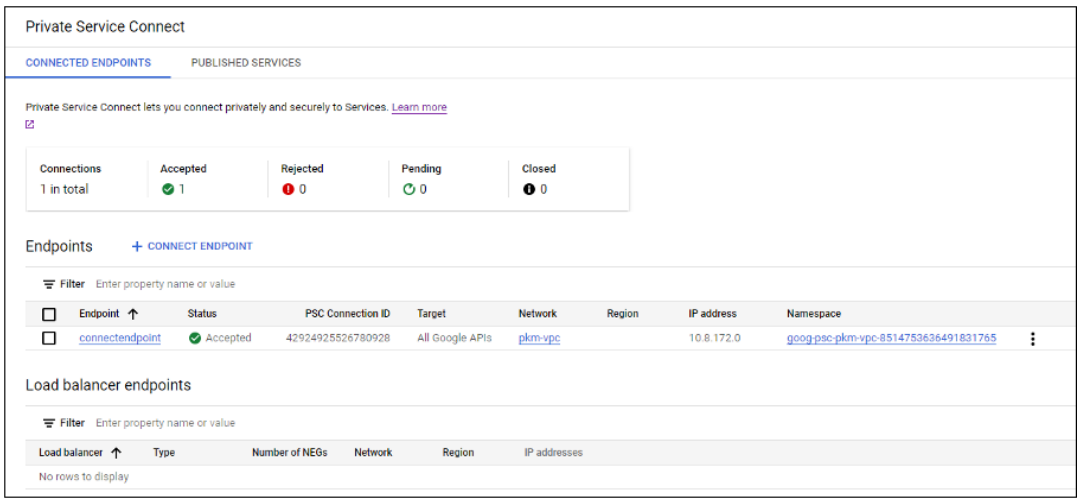
- Assicurarsi che la connessione di hosting sia in modalità di manutenzione durante l'aggiornamento delle proprietà personalizzate.
- Per utilizzare i pool di lavoratori privati, sono necessarie le seguenti modifiche:
  - Per Citrix Cloud Service Account, aggiungere i seguenti ruoli IAM:
    - Account del servizio Cloud Build
    - Amministratore istanze Compute
    - Utente account di servizio
    - Creatore token account di servizio
    - Proprietario del pool di worker Cloud Build
  - Creare l'account di servizio Citrix Cloud nello stesso progetto che si utilizza per creare una connessione di hosting.
  - Configurare le zone DNS per **`private`**`.googleapis.com` e `gcr.io` come descritto nella Configurazione DNS.



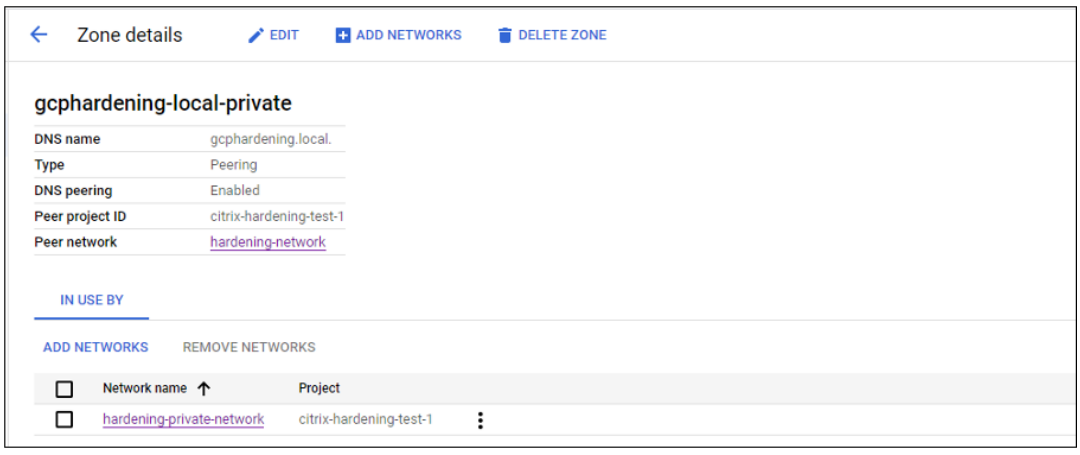

 




- Configurare la traduzione degli indirizzi di rete (NAT) privata o utilizzare la connessione al servizio privato. Per ulteriori informazioni, vedere Accesso alle API di Google tramite gli endpoint.




- Se si utilizza un VPC con peering, creare una zona Cloud DNS che esegue il peering del VPC con peering. Per ulteriori informazioni, vedere Creazione di una zona di peering.




- Nei controlli dei servizi VPC, impostare le regole di uscita in modo che le API e le VM pos-

sano comunicare con Internet. Le regole di ingresso sono opzionali. Ad esempio:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

### Abilitare il proxy

Per abilitare il proxy, impostare le proprietà personalizzate come segue sulla connessione host:

1. Aprire una finestra di PowerShell dall'host Delivery Controller o utilizzare l'SDK Remote PowerShell. Per ulteriori informazioni sull'SDK Remote PowerShell, vedere SDK e API.
2. Eseguire i seguenti comandi:
   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`
3. Copiare le `CustomProperties` dalla connessione a un blocco note.
4. Aggiungere l'impostazione delle proprietà come segue:
   - In caso di implementazione nel cloud (utilizzando pool pubblici): aggiungere l'impostazione delle proprietà `<Property xsi:type="StringProperty"Name ="ProxyHypervisorTrafficThroughConnector"Value="True"/>` alle `CustomProperties` per abilitare il proxy. Ad esempio:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
   -instance" xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation">
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

Consentire la regola di ingresso per l'account del servizio Cloud Build nel perimetro del servizio VPC. Ad esempio:

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
```

```
5   Source > All sources allowed
6   To:
7   Projects =
8   All projects
9   Services =
10  Service name: All services
11  <!--NeedCopy-->
```

Per informazioni sul perimetro del servizio VPC, vedere Dettagli e configurazione dei perimetri di servizio.

- Nel caso di un pool di lavoratori privati in un'implementazione cloud, aggiungere le impostazioni delle proprietà `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>` e `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool "Value="True"/>` alle `CustomProperties` per abilitare il proxy. Ad esempio:

```
1   <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
       -instance" xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation">
2   <Property xsi:type="StringProperty" Name="
       ProxyHypervisorTrafficThroughConnector" Value="True"/>
3   <Property xsi:type="StringProperty" Name="
       UsePrivateWorkerPool" Value="True"/>
4   </CustomProperties>
5   <!--NeedCopy-->
```

5. Nella finestra di PowerShell assegnare una variabile alle proprietà personalizzate modificate. Ad esempio:
   `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Eseguire `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.
7. Eseguire `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Eseguire `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Eseguire quanto segue per aggiornare una connessione host esistente:

```
1  Set-Item -PassThru -Path @('XDHyp:\Connections\\<ENTER YOUR
      CONNECTION NAME HERE>') -SecurePassword $securePassword -
      UserName $gcpServiceAccount -CustomProperties $customProperty
2  <!--NeedCopy-->
```

## Informazioni sulle autorizzazioni GCP

Questa sezione contiene l'elenco completo delle autorizzazioni GCP. Usare il set completo di autorizzazioni indicato nella sezione per il corretto funzionamento della funzionalità.

### Creazione di una connessione host

- Autorizzazioni minime richieste per Citrix Cloud Service Account nel progetto Provisioning:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

  - Amministratore Compute
  - Utente di Cloud Datastore

- Autorizzazioni aggiuntive richieste per Shared VPC for Citrix Cloud Service Account nel progetto Shared VPC:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

  - Utente di rete Compute

### Gestione dell'alimentazione delle macchine virtuali

Autorizzazioni minime richieste per Citrix Cloud Service Account nel progetto Provisioning:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
```

```
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Amministratore Compute
- Utente di Cloud Datastore

#### Creazione, aggiornamento o eliminazione di macchine virtuali

- Autorizzazioni minime richieste per Citrix Cloud Service Account nel progetto Provisioning:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
```

```
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Amministratore Compute
- Amministratore archiviazione
- Editor Cloud Build
- Utente account di servizio
- Utente di Cloud Datastore

- Autorizzazioni aggiuntive necessarie per Shared VPC for Citrix Cloud Service Account nel progetto Shared VPC per creare un'unità di hosting utilizzando VPC e una sottorete del progetto Shared VPC:

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

  - Utente di rete Compute
  - Utente di Cloud Datastore

- Autorizzazioni minime richieste per l'account Cloud Build Service nel progetto Provisioning richieste dal servizio Google Cloud Build quando si scarica il disco di istruzioni di preparazione su MCS:

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
```

```
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Account del servizio Cloud Build
- Amministratore istanze Compute
- Utente account di servizio

- Autorizzazioni minime richieste per l'account Cloud Compute Service nel progetto Provisioning richieste dal servizio Google Cloud Build quando si scarica il disco di istruzioni di preparazione su MCS:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Utente di rete Compute
- Utente dell'account di archiviazione
- Utente di Cloud Datastore

- Autorizzazioni aggiuntive richieste per l'account Shared VPC for Cloud Build Service nel progetto Provisioning richieste dal servizio Google Cloud Build quando si scarica il disco di istruzioni di preparazione su MCS:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

- Utente di rete Compute

  - Utente dell'account di archiviazione
  - Utente di Cloud Datastore

- Autorizzazioni aggiuntive richieste per Cloud Key Management Service (KMS) per Citrix Cloud Service Account nel progetto Provisioning:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

  I seguenti ruoli definiti da Google dispongono delle autorizzazioni elencate sopra:

  - Visualizzatore KMS Compute

#### Autorizzazioni generali

Di seguito sono riportate le autorizzazioni per Citrix Cloud Service Account nel progetto di Provisioning per tutte le funzionalità supportate in MCS. Queste autorizzazioni garantiscono la migliore compatibilità in futuro:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
```

```
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
```

```
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su Google Cloud Platform (GCP), vedere Creare un catalogo di Google Cloud Platform.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti Google Cloud.

## Connessione a HPE Moonshot (Preview)

December 5, 2023

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano dettagli specifici di HPE Moonshot.

> **Nota:**
>
> Prima di creare una connessione a HPE Moonshot, è necessario completare la configurazione del proprio account HPE. Vedere Ambienti di virtualizzazione HPE Moonshot.

### Creare una connessione

È possibile creare una connessione a HPE Moonshot mediante:

- Interfaccia Full Configuration
- Comandi PowerShell

#### Creare una connessione utilizzando l'interfaccia Full Configuration

1. Nella pagina **Add Connection and Resources** (Aggiungi connessione e risorse), selezionare **HPE Moonshot** come tipo di connessione.
2. Inserire l'indirizzo di connessione del proprio Moonshot iLO Chassis Manager. È possibile utilizzare un indirizzo IP, un nome host o un FQDN per l'indirizzo.
3. Inserire le credenziali amministrative dello chassis e un nome di connessione descrittivo.

La configurazione della connessione si interrompe quando si verifica una delle seguenti situazioni:

- DaaS riceve un certificato pubblico firmato da un'autorità di certificazione contenente errori: viene visualizzato un messaggio di errore. Seguire le istruzioni sullo schermo per risolvere il problema. Altrimenti non sarà possibile procedere con la creazione della connessione.
- DaaS riceve un certificato privato firmato da un'autorità di certificazione. Viene visualizzata una pagina di avviso. Confrontare l'impronta digitale ricevuta con quella del server per la validità del certificato. Se è valido, selezionare **Trust certificate** (Certificato di fiducia) e fare clic su **OK** per procedere con la creazione della connessione. DaaS considererà quindi attendibile il certificato e memorizzerà l'impronta digitale per la convalida futura.

#### Creare una connessione utilizzando i comandi PowerShell

Quando si crea una connessione utilizzando un comando PowerShell, è necessario fornire le seguenti informazioni:

- IP: indirizzo IP del server HPE
- Nome utente: nome utente HPE
- Password: password HPE

Ad esempio:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
 "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
  -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
     HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
     $UserName -sslthumbprint $SslThumbprint New-
     BrokerHypervisorConnection -HypHypervisorConnectionUid
     $HypervisorConnectionID
<!--NeedCopy-->
```

> **Nota:**
>
> Il parametro `sslthumbprint` è obbligatorio solo per i certificati privati firmati da un'autorità di certificazione.

### Convalida del certificato e dell'impronta digitale

Per creare una connessione corretta a **HPE Moonshot**, il certificato non deve contenere errori e l'impronta digitale deve avere un valore corretto. Di seguito sono riportati i casi d'uso relativi alla convalida del certificato e dell'impronta digitale:

- Il certificato pubblico firmato da un'autorità di certificazione contiene errori. La connessione non viene creata correttamente. Visualizzare i dettagli dell'errore e risolvere il problema.
- Certificato pubblico firmato da un'autorità di certificazione senza errori. La connessione viene creata correttamente e il valore di `SslThumbprints` è **Null**.
- Certificato privato firmato da un'autorità di certificazione senza errori e valore `sslthumbprint`. La connessione viene creata correttamente con un valore di `SslThumbprints` corretto.
- Certificato privato firmato da un'autorità di certificazione con un valore di impronta digitale errato. La connessione non viene creata correttamente.
- Certificato privato firmato da un'autorità di certificazione senza errori. La connessione è stata creata correttamente. Il valore di `SSlThumbprints` è **Null** quando si crea la connessione. Il valore di `SSlThumbprints` viene aggiornato a un valore dal servizio del sito.

### Gestire le connessioni

Questa sezione descrive in dettaglio come gestire le connessioni:

- Risolvere i problemi relativi ai certificati utilizzando l'interfaccia Full Configuration
- Aggiornare il valore dell'impronta digitale mediante comando PowerShell

#### Risolvere i problemi relativi ai certificati

DaaS blocca una connessione HPE Moonshot in caso di problemi con i certificati, impedendo di erogare e gestire i carichi di lavoro sui nodi HPE Moonshot associati. Verrà visualizzata un'icona di errore accanto alla connessione nell'elenco **Host connections** (Connessioni host). Vedere la tabella seguente per problemi specifici e le relative soluzioni.

| Problema | Soluzione |
| --- | --- |
| Si verifica un errore nel certificato pubblico firmato dall'autorità di certificazione | Fare clic sulla connessione e selezionare la scheda **Troubleshoot** (Risoluzione dei problemi). Visualizzare i dettagli dell'errore e risolvere il problema. |

| Problema | Soluzione |
| --- | --- |
| Il certificato ricevuto è privato e firmato da un'autorità di certificazione o scaduto. | Modificare la connessione host per aggiornare l'impronta personale del certificato. Passaggi dettagliati<br>1. Selezionare la connessione e fare clic su **Edit Connection** (Modifica connessione).<br>1. Nella pagina **Connection Properties** (Proprietà della connessione), fare clic su **Edit settings** (Modifica impostazioni).<br>1. **Inserire la password per connettersi allo chassis HPE Moonshot, quindi fare clic su Save.**<br>1. Nella pagina di **Warning** (Avviso) visualizzata, confrontare l'impronta digitale ricevuta con quella del server per la validità del certificato.<br>1. Se sono uguali, selezionare **Trust certificate** (Certificato di attendibilità) e fare clic su **OK**. |

#### Aggiornare il valore dell'impronta digitale

Dopo aver creato la connessione, è possibile aggiornare il valore dell'impronta digitale di una connessione utilizzando il comando PowerShell `Set-Item`. Ad esempio, eseguire i seguenti comandi:

1. Ottenere i dettagli di connessione di una connessione. Ad esempio:

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
2 <!--NeedCopy-->
```

2. Aggiornare il valore dell'impronta digitale. Ad esempio:

```
1 Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
      Administrator -SslThumbprint
     xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
2 <!--NeedCopy-->
```

3. Controllare il valore dell'impronta digitale aggiornato. Ad esempio:

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

```
<!--NeedCopy-->
```

> **Nota:**
>
> L'aggiornamento non riesce se si fornisce un valore di impronta digitale errato nel comando `Set-Item`.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su HPE Moonshot, vedere Creare un catalogo di macchine di HPE Moonshot.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti di virtualizzazione HPE Moonshot

## Connessione a Microsoft Azure

November 3, 2023

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Azure Resource Manager.

> **Nota:**
>
> Prima di creare una connessione a Microsoft Azure, è necessario completare la configurazione del proprio account Azure come posizione delle risorse. Vedere Ambienti cloud Microsoft Azure Resource Manager.

### Creare entità servizio e connessioni

Prima di creare connessioni, è necessario configurare le entità servizio usate dalle connessioni per accedere alle risorse di Azure. È possibile creare una connessione in due modi:

- Creare un'entità servizio e una connessione allo stesso tempo utilizzando Full Configuration
- Creare una connessione utilizzando un'entità servizio creata in precedenza

Questa sezione mostra come completare queste attività:

- Creare un'entità servizio e una connessione utilizzando Full Configuration
- Creare un'entità servizio utilizzando PowerShell
- Ottenere il segreto dell'applicazione in Azure
- Creare una connessione utilizzando un'entità servizio esistente

#### Considerazioni

Prima di iniziare, tenere presenti queste considerazioni:

- Citrix consiglia di utilizzare entità servizio con il ruolo di *Contributor*. Tuttavia, consulta la sezione Autorizzazioni minime per ottenere l'elenco delle autorizzazioni minime.
- Quando si crea la prima connessione, Azure richiede di concederle le autorizzazioni necessarie. Per le connessioni future è comunque necessario autenticarsi, ma Azure ricorda il consenso precedente e non visualizza più la richiesta.
- Gli account utilizzati per l'autenticazione devono essere co-amministratori della sottoscrizione.
- L'account utilizzato per l'autenticazione deve essere un membro della directory della sottoscrizione. Esistono due tipi di account di cui tenere conto: "lavoro o scuola" e "account Microsoft personale". Vedere CTX219211 per i dettagli.
- Sebbene sia possibile utilizzare un account Microsoft esistente aggiungendolo come membro della directory della sottoscrizione, possono verificarsi complicazioni se all'utente è stato precedentemente concesso l'accesso come ospite a una delle risorse della directory. In questo caso, potrebbe essere presente una voce di segnaposto nella directory che non concede loro le autorizzazioni necessarie e viene restituito un errore.

  Correggere questo problema rimuovendo le risorse dalla directory e aggiungendole di nuovo esplicitamente. Tuttavia, utilizzare questa opzione con attenzione, perché ha effetti indesiderati su altre risorse a cui può accedere questo account.
- Esiste un problema noto per cui alcuni account vengono rilevati come ospiti della directory quando invece sono membri. Configurazioni come questa si verificano in genere con account di directory consolidati precedenti. Soluzione: aggiungere un account alla directory, che assume il valore di appartenenza corretto.
- I gruppi di risorse sono semplicemente contenitori per le risorse e possono contenere risorse provenienti da regioni diverse dalla propria. Ciò può creare potenzialmente confusione se si prevede che le risorse visualizzate nella regione di un gruppo di risorse siano disponibili.
- Assicurarsi che la rete e la subnet siano sufficientemente grandi da ospitare il numero di macchine necessarie. Ciò richiede una certa lungimiranza, ma Microsoft aiuta a specificare i valori corretti, con indicazioni sulla capacità dello spazio degli indirizzi.

### Creare un'entità servizio e una connessione utilizzando Full Configuration

> **Importante:**
>
> Questa funzionalità non è ancora disponibile per le sottoscrizioni di Azure in Cina.

Con Full Configuration, è possibile creare sia un'entità servizio che una connessione in un unico flusso di lavoro. Le entità servizio consentono alle connessioni di accedere alle risorse di Azure. Quando si esegue l'autenticazione in Azure per creare un'entità servizio, un'applicazione viene registrata in Azure. Viene creata una chiave segreta (chiamata *segreto del client* o *segreto dell'applicazione*) per l'applicazione registrata. L'applicazione registrata (in questo caso una *connessione*) utilizza il segreto del client per l'autenticazione in Azure AD.

Prima di iniziare, assicurarsi che siano soddisfatti questi prerequisiti:

- Avere un account utente nel tenant Azure Active Directory della propria sottoscrizione.
- L'account utente Azure AD sia anche co-amministratore per la sottoscrizione di Azure che si desidera utilizzare per il provisioning delle risorse.
- Si dispone delle autorizzazioni di amministratore globale, amministratore dell'applicazione o sviluppatore di applicazioni per l'autenticazione. Le autorizzazioni possono essere revocate dopo aver creato una connessione host. Per ulteriori informazioni sui ruoli, vedere Ruoli predefiniti di Azure AD.

Utilizzare la procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse) per creare insieme un'entità servizio e una connessione allo stesso tempo:

1. Nella pagina **Connection** (Connessione), selezionare **Create a new connetion** (Crea una nuova connessione), il tipo di connessione **Microsoft Azure** e l'ambiente Azure.
2. Selezionare gli strumenti da utilizzare per creare le macchine virtuali, quindi selezionare **Next** (Avanti).
3. Nella pagina **Connection Details** (Dettagli della connessione), creare un'entità servizio e impostare il nome della connessione come segue:

    a) Per concedere l'autorizzazione di connessione per pulire automaticamente i dispositivi aggiunti ad Azure AD obsoleti, selezionare **Enable Azure AD joined device management** (Abilita la gestione dei dispositivi aggiunti ad Azure AD). Consigliamo di selezionare questa opzione se si desidera creare macchine aggiunte ad Azure AD tramite questa connessione. Per altre informazioni, vedere Abilitare la gestione dei dispositivi aggiunti ad Azure AD.

    b) Inserire il proprio ID della sottoscrizione di Azure e un nome da dare alla connessione. Dopo aver inserito l'ID sottoscrizione, viene abilitato il pulsante **Create new** (Crea nuova).

> **Nota:**
>
> Il nome della connessione può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.

a) Selezionare **Create new** (Crea nuova), quindi inserire il nome utente e la password dell'account Azure Active Directory.

b) Selezionare **Sign in** (Accedi).

c) Selezionare **Accept** per concedere a Citrix DaaS le autorizzazioni elencate. Azure crea un'entità servizio che consente a Citrix DaaS di gestire le risorse di Azure per conto dell'utente specificato.

d) Dopo aver selezionato **Accept**, si torna alla pagina **Connection Details**.

> **Nota:**
>
> Dopo aver eseguito l'autenticazione in Azure, i pulsanti **Create new** (Crea nuova) e **Use existing** (Usa esistente) scompaiono. Viene visualizzato il testo **Connection successful** (Connessione riuscita), con un segno di spunta verde che indica la connessione riuscita alla sottoscrizione di Azure.

e) Per instradare le richieste API verso Azure tramite Citrix Cloud Connectors, selezionare la casella di controllo **Route traffic through Citrix Cloud Connectors** (Instrada il traffico tramite Citrix Cloud Connector).

In alternativa, è possibile abilitare questa funzionalità utilizzando PowerShell. Per ulteriori informazioni, vedere Creare un ambiente sicuro per il traffico gestito di Azure.

> **Nota:**
>
> Questa opzione è disponibile solo quando nella distribuzione sono presenti Citrix Cloud Connector attivi. Attualmente, questa funzionalità non è supportata per le Connector Appliance.

f) Selezionare **Next** (Avanti).

> **Nota:**
>
> Non è possibile passare alla pagina successiva finché non ci si autentica correttamente in Azure e non si acconsente a concedere le autorizzazioni richieste.

4. Configurare le risorse per la connessione come segue:

- Nella pagina **Region** (Regione), selezionare una regione.
- Nella pagina **Network** (Rete), procedere come segue:

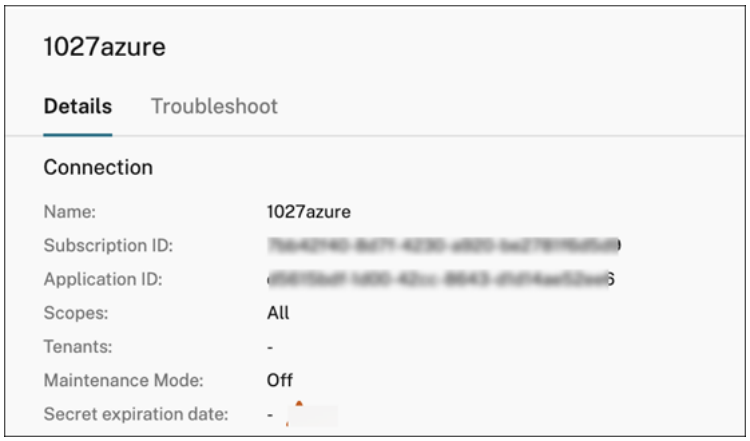
 

- Digitare un nome da 1 a 64 caratteri per la risorsa, per semplificare l'identificazione della combinazione di regione e rete. Il nome di una risorsa non può contenere solo spazi vuoti e nemmeno i caratteri `\/;:#.*?=<>|[]{ } "'()'`.
- Selezionare una coppia rete virtuale/gruppo di risorse (se si dispone di più di una rete virtuale con lo stesso nome, l'associazione del nome della rete con il gruppo di risorse fornisce combinazioni univoche). Se la regione selezionata nella pagina precedente non dispone di reti virtuali, tornare a quella pagina e selezionare una regione con reti virtuali.

5. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per completare la configurazione.

**Visualizzare l'ID dell'applicazione** Dopo aver creato una connessione, è possibile visualizzare l'ID dell'applicazione utilizzata dalla connessione per accedere alle risorse di Azure.

Nell'elenco **Add Connection and Resources** (Aggiungi connessione e risorse), selezionare la connessione per visualizzare i dettagli. La scheda **Details** (Dettagli) mostra l'ID dell'applicazione.




### Creare un'entità servizio utilizzando PowerShell

Per creare un'entità servizio utilizzando PowerShell, connettersi alla sottoscrizione di Azure Resource Manager e utilizzare i cmdlet PowerShell forniti nelle sezioni seguenti.

Assicurarsi di avere a portata di mano quanto segue:

- **SubscriptionId:** `SubscriptionID` di Azure Resource Manager per la sottoscrizione in cui si desidera eseguire il provisioning di VDA.
- **ActiveDirectoryID**: ID tenant dell'applicazione registrata con Azure AD.
- **ApplicationName:** nome dell'applicazione da creare in Azure AD.

I passaggi dettagliati sono i seguenti:

1. Connettersi alla sottoscrizione Azure Resource Manager.

   ```
   Connect-AzAccount
   ```

2. Selezionare la sottoscrizione Azure Resource Manager in cui si desidera creare l'entità servizio.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

3. Creare l'applicazione nel proprio tenant AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. Creare un'entità servizio.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. Assegnare un ruolo all'entità servizio.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

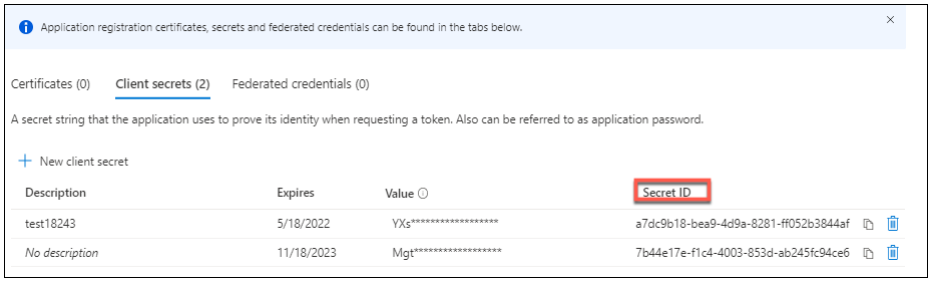
6. Dalla finestra di output della console PowerShell, prendere nota dell'ApplicationId. Fornire questo ID quando si crea la connessione host.

### Ottenere il segreto dell'applicazione in Azure

Per creare una connessione utilizzando un'entità servizio esistente, è prima necessario ottenere l'ID e il segreto dell'applicazione dell'entità servizio nel portale di Azure.

I passaggi dettagliati sono i seguenti:

1. Ottenere l'**ID dell'applicazione** dall'interfaccia Full Configuration o utilizzando PowerShell.
2. Accedere al portale di Azure.
3. In Azure, selezionare **Azure Active Directory**.
4. Da **Registrazioni app** in Azure AD, selezionare la propria applicazione.
5. Andare a **Certificati e segreti**.
6. Fare clic su **Client secrets** (Segreti client).



### Creare una connessione utilizzando un'entità servizio esistente

Se si dispone già di un'entità servizio, è possibile utilizzarla per creare una connessione utilizzando Full Configuration.

Assicurarsi di avere a portata di mano quanto segue:

- SubscriptionId
- ActiveDirectoryID (tenant ID)
- ID applicazione
- Segreto dell'applicazione

  Per ulteriori informazioni, vedere Ottenere il segreto dell'applicazione.
- Data di scadenza del segreto

I passaggi dettagliati sono i seguenti:

Nella procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse):

1. Nella pagina **Connection** (Connessione), selezionare **Create a new connetion** (Crea una nuova connessione), il tipo di connessione **Microsoft Azure** e l'ambiente Azure.
2. Selezionare gli strumenti da utilizzare per creare le macchine virtuali, quindi selezionare **Next** (Avanti).
3. Nella pagina **Connection Details** (Dettagli connessione), inserire il proprio ID sottoscrizione di Azure e un nome per la connessione.

   > **Nota:**
   >
   > Il nome della connessione può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.

4. Selezionare **Use existing** (Usa esistente). Nella finestra **Existing Service Principal Details** (Dettagli entità servizio esistente), immettere le seguenti impostazioni per l'entità servizio esistente. Dopo aver inserito i dettagli, il pulsante **Save** (Salva) è abilitato. Selezionare **Save** (Salva). Non è possibile andare oltre questa pagina finché non si forniscono dettagli validi.

   - **Subscription ID** (ID sottoscrizione). Inserire il proprio ID sottoscrizione di Azure. Per ottenere l'ID sottoscrizione, accedere al portale di Azure e andare a **Sottoscrizioni > Panoramica**.
   - **Active Directory ID** (ID Active Directory) (ID tenant). Inserire l'ID Directory (tenant) dell'applicazione che si è registrata con Azure AD.

- **Application ID** (ID applicazione). Inserire l'ID applicazione (client) dell'applicazione registrata con Azure AD.
- **Application secret** (Segreto dell'applicazione). Inserire una chiave segreta (segreto del client). L'applicazione registrata utilizza la chiave per l'autenticazione in Azure AD. Si consiglia di cambiare le chiavi regolarmente per motivi di sicurezza. Assicurarsi di salvare la chiave, perché non è possibile recuperarla in un secondo momento.
- **Secret expiration date** (Data di scadenza del segreto). Immettere la data dopo la quale il segreto dell'applicazione scade. Si riceverà un avviso sulla console prima della scadenza della chiave segreta. Tuttavia, se la chiave segreta scade, si ricevono errori.

  > **Nota:**
  >
  > Per motivi di sicurezza, il periodo di scadenza non può essere superiore a due anni da oggi.

- **Authentication URL** (URL di autenticazione). Questo campo viene compilato automaticamente e non è modificabile.
- **Management URL** (URL di gestione). Questo campo viene compilato automaticamente e non è modificabile.
- **Storage suffix** (Suffisso di archiviazione). Questo campo viene compilato automaticamente e non è modificabile.

  L'accesso ai seguenti endpoint è necessario per creare un catalogo MCS in Azure. L'accesso a questi endpoint ottimizza la connettività tra la rete e il portale di Azure e i relativi servizi.

  - Authentication URL: https://login.microsoftonline.com/
  - Management URL: https://management.azure.com/. Questo è un URL di richiesta per le API del provider di Azure Resource Manager. L'endpoint per la gestione dipende dall'ambiente. Ad esempio, per Azure Global è https://management.azure.com/ e per Azure US Government è https://management.usgovcloudapi.net/.
  - Storage suffix: https://*.core.windows.net./. Questo (*) è un carattere jolly per il suffisso di archiviazione. Ad esempio, https://demo.table.core.windows.net/.

5. Dopo aver selezionato **Save**, si torna alla pagina **Connection Details** (Dettagli connessione). Selezionare **Next** (Avanti) per passare alla pagina successiva.
6. Configurare le risorse per la connessione come segue:

   - Nella pagina **Region** (Regione), selezionare una regione.
   - Nella pagina **Network** (Rete), procedere come segue:

- Digitare un nome da 1 a 64 caratteri per la risorsa, per semplificare l'identificazione della combinazione di regione e rete. Il nome di una risorsa non può contenere solo spazi vuoti e nemmeno i caratteri `\/;:#.*?=<>|[]{ } "'()'`.
- Selezionare una coppia rete virtuale/gruppo di risorse (se si dispone di più di una rete virtuale con lo stesso nome, l'associazione del nome della rete con il gruppo di risorse fornisce combinazioni univoche). Se la regione selezionata nella pagina precedente non dispone di reti virtuali, tornare a quella pagina e selezionare una regione con reti virtuali.

7. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per completare la configurazione.

## Gestire le entità servizio e le connessioni

Questa sezione descrive in dettaglio come gestire le entità servizio e le connessioni:

- Configurare le impostazioni di limitazione delle richieste di Azure
- Abilitare la gestione dei dispositivi aggiunti ad Azure AD
- Abilitare la condivisione di immagini in Azure
- Aggiungere tenant condivisi a una connessione utilizzando Full Configuration
- Implementare la condivisione di immagini tramite PowerShell
- Creare un ambiente sicuro per il traffico gestito di Azure
- Gestire il segreto dell'applicazione e la data di scadenza del segreto

### Configurare le impostazioni di limitazione delle richieste di Azure

Azure Resource Manager limita le richieste di sottoscrizione e tenant, instradando il traffico in base a limiti definiti, a seconda delle esigenze specifiche del provider. Per ulteriori informazioni, vedere Limitazione delle richieste di Resource Manager sul sito Microsoft. Sono previsti dei limiti per sottoscrizioni e tenant, a causa dei quali la gestione di molte macchine può diventare problematica. Ad esempio, in una sottoscrizione contenente molte macchine potrebbero verificarsi dei problemi di prestazioni relativi alle operazioni di alimentazione.

> **Suggerimento:**
>
> Per ulteriori informazioni, vedere Miglioramento delle prestazioni di Azure con Machine Creation Services.

Per contribuire a mitigare questi problemi, Citrix DaaS consente di rimuovere la limitazione delle richieste interna di MCS per utilizzare maggiormente la quota di richieste disponibile da Azure.

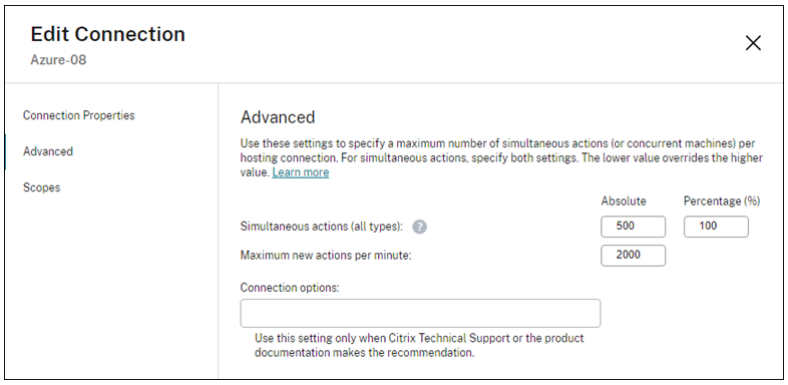
Si consigliano le seguenti impostazioni ottimali quando si accendono o si spengono le macchine virtuali in sottoscrizioni di grandi dimensioni, ad esempio quelle contenenti 1.000 macchine virtuali:

- Operazioni simultanee assolute: 500
- Numero massimo di nuove operazioni al minuto: 2.000
- Numero massimo di operazioni simultanee: 500

Utilizzare l'interfaccia Full Configuration (Configurazione completa) per configurare le operazioni di Azure per una determinata connessione host:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare una connessione correlata ad Azure per modificarla.
3. Nella procedura guidata **Edit Connection** (Modifica connessione), selezionare **Advanced** (Avanzate).
4. Nella pagina **Advanced** (Avanzate), utilizzare le opzioni di configurazione per specificare il numero di azioni simultanee e il numero massimo di nuove azioni al minuto, nonché eventuali opzioni di connessione aggiuntive.




MCS supporta massimo 500 operazioni simultanee per impostazione predefinita. In alternativa, è possibile utilizzare l'SDK Remote PowerShell per impostare il numero massimo di operazioni simultanee.

Utilizzare la proprietà **PowerShell** `MaximumConcurrentProvisioningOperations` per specificare il numero massimo di operazioni di provisioning simultanee di Azure. Quando si utilizza questa proprietà, considerare:

- Il valore predefinito di `MaximumConcurrentProvisioningOperations` è 500.
- Configurare il parametro `MaximumConcurrentProvisioningOperations` utilizzando il comando PowerShell `Set-item`.

#### Abilitare la gestione dei dispositivi aggiunti ad Azure AD

La presenza di dispositivi aggiunti ad Azure AD obsoleti in Azure potrebbe impedire l'aggiunta di nuove macchine ad Azure AD, causandone un funzionamento improprio. Per evitare potenziali problemi, è possibile concedere l'autorizzazione di connessione per gestire i dispositivi aggiunti ad Azure

AD. Con questa autorizzazione, le connessioni possono ripulire automaticamente i dispositivi aggiunti ad Azure AD obsoleti.

> **Nota:**
>
> I dispositivi aggiunti ad Azure AD non possono essere eliminati da Azure AD quando si eliminano macchine o cataloghi di macchine.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare Hosting nel riquadro di sinistra.
2. Selezionare la connessione e quindi selezionare **Edit Connection** (Modifica connessione) nella barra delle azioni.
3. Selezionare **Connection Properties** (Proprietà di connessione) nel riquadro di sinistra.
4. Nella pagina **Connection Properties** visualizzata, seguire questi passaggi:
    a) Selezionare **Enable Azure AD joined device management** (Abilita la gestione dei dispositivi aggiunti ad Azure AD).
    b) Fare clic su **Salva**.
    c) Nella finestra di accesso ad Azure visualizzata, inserire la password della sottoscrizione e quindi fare clic su **Sign in**.

    Una volta completato l'accesso, si è riportati all'elenco delle connessioni e delle risorse di hosting. Fare clic sulla connessione nell'elenco e quindi sulla scheda **Details** (Dettagli) nel riquadro inferiore. Si noterà che il campo **Azure AD joined device management** (Gestione dispositivi aggiunti ad Azure AD) riporta la dicitura **Enabled** (Abilitata).

Quando si abilita la gestione dei dispositivi aggiunti ad Azure AD con Full Configuration, è necessario autenticarsi con Azure AD indipendentemente dal metodo di creazione della connessione host scelto (crearne una nuova o usare quella esistente). Il ruolo **Cloud Device Administrator** integrato in Azure AD viene assegnato all'entità servizio. Per adottare le autorizzazioni minime per la gestione dei dispositivi aggiunti ad Azure AD, puoi rimuovere manualmente l'assegnazione del ruolo **Cloud Device Administrator** dall'entità servizio e creare un ruolo personalizzato di Azure AD che includa solo le autorizzazioni minime e assegnarlo all'entità servizio.

> **Nota:**
>
> - Le autorizzazioni minime per la gestione dei dispositivi aggiunti ad Azure AD sono le autorizzazioni di Azure AD e non le autorizzazioni di Azure Resource Manager. Non possono essere assegnate esplicitamente a un'entità servizio. È necessario creare un ruolo personalizzato in Azure AD che includa tali autorizzazioni e assegnarlo all'entità servizio. Per ulteriori informazioni, vedere Creare e assegnare un ruolo personalizzato in Azure Active Directory.
> - Per creare un ruolo personalizzato in Azure AD, è necessaria la licenza Azure AD Premium

> P1 o P2.

**Abilitare la condivisione di immagini in Azure**

Quando si creano o si aggiornano cataloghi delle macchine, è possibile selezionare immagini condivise provenienti da diverse sottoscrizioni e tenant di Azure (condivise tramite la Raccolta di calcolo di Azure). Per abilitare la condivisione di immagini all'interno di tenant o fra uno e l'altro, è necessario configurare le impostazioni necessarie in Azure:

- Condividere immagini all'interno di un tenant (tra abbonamenti)
- Condividere immagini tra tenant

**Condividere immagini all'interno di un tenant (tra abbonamenti)** Perché sia possibile selezionare in Raccolta di calcolo di Azure un'immagine che appartiene a una sottoscrizione diversa, l'immagine deve essere condivisa con l'entità servizio (SPN) di quella sottoscrizione.

Ad esempio, se esiste un'entità servizio (SPN 1) configurata in Studio come:

Entità servizio: SPN 1

Subscription: subscription 1

Tenant: tenant 1

L'immagine è in una sottoscrizione diversa, che è configurata in Studio come:

Subscription: subscription 2

Tenant: tenant 1

Se si intende condividere l'immagine della sottoscrizione 2 con la sottoscrizione 1 (SPN 1), passare alla sottoscrizione2 e condividere il gruppo di risorse con SPN1.

L'immagine deve essere condivisa con un altro SPN utilizzando il controllo degli accessi in base al ruolo di Azure (RBAC). Azure RBAC è il sistema di autorizzazione usato per gestire l'accesso alle risorse di Azure. Per ulteriori informazioni su Azure RBAC, vedere il documento Microsoft Che cos'è il controllo degli accessi in base al ruolo di Azure. Per concedere l'accesso, si assegnano ruoli alle entità servizio nell'ambito del gruppo di risorse con il ruolo di Contributor. Per assegnare i ruoli di Azure, è necessario disporre di un'autorizzazione `Microsoft.Authorization/roleAssignments/write`, come nel caso di un Amministratore Accesso utenti o un Proprietario. Per ulteriori informazioni sulla condivisione di immagini con un altro SPN, vedere il documento Microsoft Assegnare ruoli di Azure usando il portale di Azure.

**Condividere immagini tra tenant** Per condividere immagini tra tenant con la Raccolta di calcolo di Azure, creare una registrazione dell'applicazione.

Ad esempio, se ci sono due tenant (Tenant 1 e Tenant 2) e si desidera condividere la propria galleria di immagini con Tenant 1, allora:

1. Creare una domanda di registrazione per Tenant 1. Per ulteriori informazioni, vedere Creare la registrazione dell'app.
2. Consentire a Tenant 2 di accedere all'applicazione richiedendo l'accesso tramite un browser. Sostituire `Tenant2 ID` con l'ID tenant del Tenant 1. Sostituire `Application (client) ID` con l'ID dell'applicazione della registrazione dell'applicazione creata. Quando si sono completate le sostituzioni, incollare l'URL in un browser e seguire le istruzioni di accesso per accedere al Tenant 2. Ad esempio:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
      client_id=<Application (client) ID>&response_type=code&
      redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   <!--NeedCopy-->
   ```

   Per ulteriori informazioni, vedere Concedere l'accesso al tenant 2.
3. Concedere all'applicazione l'accesso al gruppo di risorse Tenant 2. Accedere come Tenant 2 e concedere alla registrazione dell'app l'accesso al gruppo di risorse che contiene l'immagine della raccolta. Per ulteriori informazioni, vedere Eseguire l'autenticazione delle richieste su più tenant.

#### Aggiungere tenant condivisi a una connessione utilizzando Full Configuration

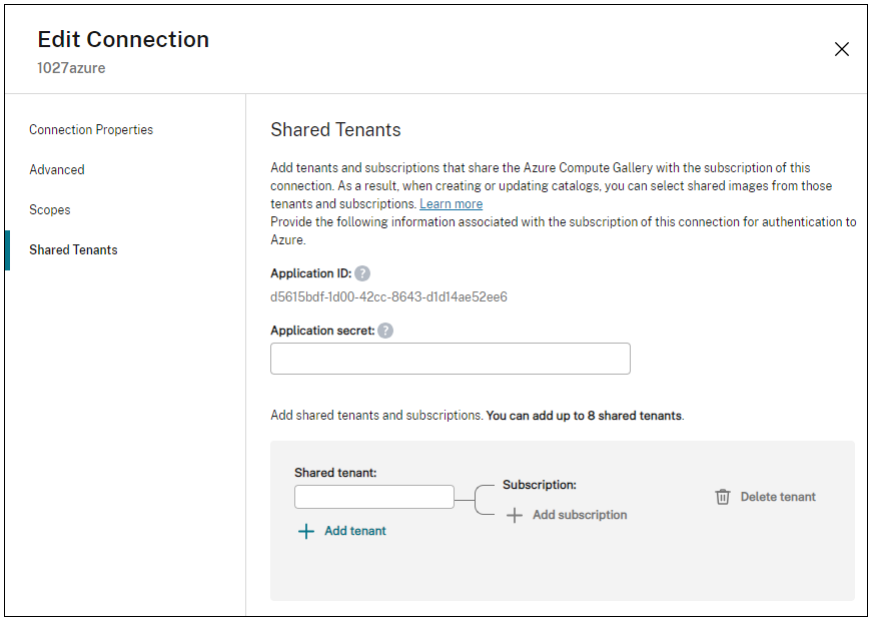
Quando si creano o si aggiornano cataloghi delle macchine nell'interfaccia Full Configuration (Configurazione completa), è possibile selezionare immagini condivise provenienti da diverse sottoscrizioni e tenant di Azure (condivise tramite la Raccolta di calcolo di Azure). La funzionalità richiede che vengano fornite informazioni condivise sul tenant e sulla sottoscrizione per le connessioni host associate.

> **Nota:**
>
> Assicurarsi di aver configurato le impostazioni necessarie in Azure per abilitare la condivisione di immagini tra tenant. Per ulteriori informazioni, vedere Condividere immagini tra tenant.

Completare i seguenti passaggi per una connessione:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione e quindi selezionare **Edit Connection** (Modifica connessione) nella barra delle azioni.




3. In **Shared Tenants** (Tenant condivisi), procedere come segue:

   a) Fornire l'ID dell'applicazione e il segreto dell'applicazione associati alla sottoscrizione della connessione. DaaS utilizza queste informazioni per l'autenticazione in Azure AD.
   b) Aggiungere tenant e sottoscrizioni che condividono la Raccolta di calcolo di Azure con la sottoscrizione della connessione. È possibile aggiungere fino a otto tenant condivisi e otto sottoscrizioni per ogni tenant.

4. Al termine, selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

### Implementare la condivisione di immagini tramite PowerShell

Questa sezione illustra i processi di condivisione delle immagini tramite PowerShell:

- Selezionare un'immagine da un'altra sottoscrizione
- Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi
- Selezionare un'immagine da un altro tenant

**Selezionare un'immagine da un'altra sottoscrizione** È possibile selezionare un'immagine in Raccolta di calcolo di Azure che appartiene a una sottoscrizione condivisa diversa all'interno dello stesso tenant di Azure per creare e aggiornare i cataloghi MCS usando i comandi di PowerShell.

1. Nella cartella principale dell'unità di hosting, Citrix crea una nuova cartella di sottoscrizione condivisa chiamata `sharedsubscription`.
2. Elencare tutte le sottoscrizioni condivise di un tenant.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
<!--NeedCopy-->
```

3. Selezionare un abbonamento condiviso, quindi elencare tutti i gruppi di risorse condivise di quella sottoscrizione condivisa.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
<!--NeedCopy-->
```

4. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
<!--NeedCopy-->
```

7. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

   Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

**Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi**
Utilizzare `Set-Item` per aggiornare le proprietà personalizzate della connessione di hosting con ID tenant e ID di abbonamento condivisi. Aggiungere una proprietà `SharedTenants` in `CustomProperties`. Il formato di `Shared Tenants` è:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

Ad esempio:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
    123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
    =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
    Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
    core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
    " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
     {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
    advc345" -SecurePassword
$psd
<!--NeedCopy-->
```

> **Nota:**
>
> È possibile aggiungere più di un tenant. Ogni inquilino può avere più di una sottoscrizione.

**Selezionare un'immagine da un altro tenant** È possibile selezionare nella Raccolta di calcolo di Azure un'immagine che appartiene a un diverso tenant di Azure per creare e aggiornare i cataloghi MCS usando i comandi di PowerShell.

1. Nella cartella principale dell'unità di hosting, Citrix crea una nuova cartella di sottoscrizione condivisa chiamata `sharedsubscription`.
2. Elencare tutte le sottoscrizioni condivise.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
<!--NeedCopy-->
```

3. Selezionare un abbonamento condiviso, quindi elencare tutti i gruppi di risorse condivise di quella sottoscrizione condivisa.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
<!--NeedCopy-->
```

4. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

   Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

#### Creare un ambiente sicuro per il traffico gestito di Azure

MCS consente il routing del traffico di rete (chiamate API da Citrix Cloud all'hypervisor Azure) tramite Cloud Connectors nel proprio ambiente. Questa implementazione aiuta a proteggere la propria sottoscrizione di Azure per consentire il traffico di rete da indirizzi IP specifici. Per fare ciò, aggiungere `ProxyHypervisorTrafficThroughConnector` in `CustomProperties`. Dopo aver impostato le proprietà personalizzate, è possibile configurare i criteri di Azure per avere accesso privato ai dischi gestiti di Azure.

Se si configurano i criteri di Azure per creare automaticamente accessi al disco in modo che ciascun nuovo disco utilizzi endpoint privati, non è possibile caricare o scaricare più di cinque dischi o snapshot contemporaneamente con lo stesso oggetto di accesso al disco applicato da Azure. Questo limite vale per ogni catalogo di macchine se si configurano i criteri di Azure a livello di gruppo di risorse e per tutti i cataloghi di macchine se si configurano i criteri di Azure a livello di sottoscrizione.
Se si configurano i criteri di Azure per creare automaticamente accessi al disco in modo che ciascun nuovo disco utilizzi endpoint privati, il limite di cinque operazioni simultanee non viene applicato.

> **Nota:**
>
> Attualmente, questa funzionalità non è supportata per Connector Appliance.

**Limiti** A causa delle limitazioni di Azure, questa funzionalità non è attualmente supportata quando i dischi gestiti sono dotati di crittografia lato server con chiavi gestite dal cliente. Per altre limitazioni correlate, vedere Limitare l'accesso all'importazione/esportazione per i dischi gestiti usando un collegamento privato di Azure.

Per altre informazioni sulla crittografia lato server, vedere Crittografia lato server di Azure.

**Abilitare il proxy** Per abilitare il proxy, impostare le proprietà personalizzate come segue sulla connessione host:

1. Aprire una finestra di PowerShell utilizzando l'SDK Remote PowerShell. Per ulteriori informazioni, vedere https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/.
2. Eseguire i seguenti comandi:
   a) `Add-PSSnapin citrix*.`
   b) `cd XDHyp:\Connections\`
   c) `dir`
3. Copiare `CustomProperties` dalla connessione a un blocco note e aggiungere l'impostazione della proprietà `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>` a `CustomProperties` per abilitare il proxy. Ad esempio:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint" Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority" Value="https://login.microsoftonline.com/" />
```

```
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>
<!--NeedCopy-->
```

4. Nella finestra di PowerShell assegnare una variabile alle proprietà personalizzate modificate. Ad esempio:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value
    ="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Eseguire `$cred = Get-Credential`. Se richiesto, fornire le credenziali di connessione. Le credenziali sono l'ID e il segreto dell'applicazione di Azure.

6. Eseguire `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`.

> **Importante:**
>
> Se si riceve un messaggio che indica che manca `SubscriptionId`, sostituire tutte le virgolette (") con un apice inverso seguito da virgolette ("") nella proprietà personalizzata. Ad esempio:

```
<CustomProperties xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`" xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
    Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
    Value=`"https://management.azure.com/`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"
    AuthenticationAuthority`" Value=`"https://login.microsoftonline
    .com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value
    =`"core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"5
    cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"
    ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />
</CustomProperties>
<!--NeedCopy-->
```

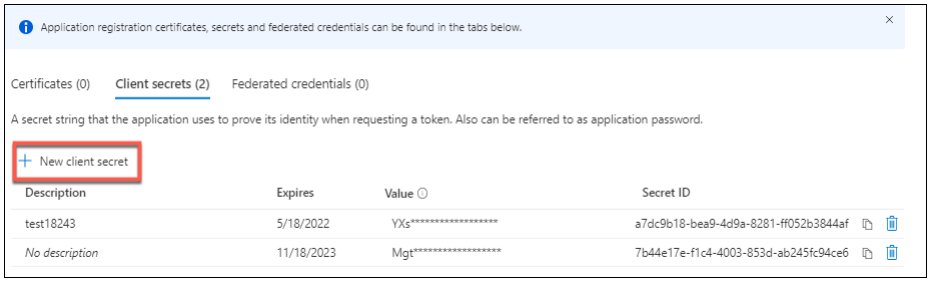
7. Eseguire `dir` per verificare le impostazioni aggiornate di `CustomProperties`.

### Gestire il segreto dell'applicazione e la data di scadenza del segreto

Accertarsi di aver modificato il segreto dell'applicazione per una connessione prima della scadenza del segreto. Si riceverà un avviso sull'interfaccia Full Configuration prima della scadenza della chiave segreta.

**Creare un segreto dell'applicazione in Azure** È possibile creare un segreto dell'applicazione per una connessione tramite il portale di Azure.

1. Selezionare **Azure Active Directory**.
2. Da **Registrazioni app** in Azure AD, selezionare la propria applicazione.
3. Andare a **Certificati e segreti**.
4. Fare clic su **Segreti client > Nuovo segreto client**.




5. Fornire una descrizione del segreto e specificare una durata. Al termine, selezionare **Add** (Aggiungi).

> **Nota:**
>
> Assicurarsi di salvare il segreto del client, perché non è possibile recuperarlo in un secondo momento.

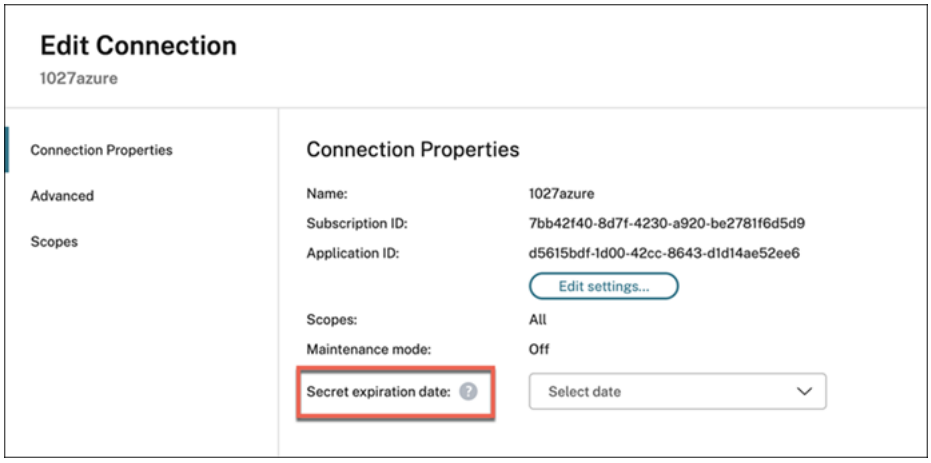
6. Copiare il valore del segreto del client e la data di scadenza.

7. Nell'interfaccia Full Configuration (Configurazione completa), modificare la connessione corrispondente e sostituire il contenuto nei campi **Application secret** (Segreto applicazione) e **Secret expiration date** (Data di scadenza del segreto) con i valori copiati.

**Modificare la data di scadenza del segreto** È possibile utilizzare l'interfaccia Full Configuration (Configurazione completa) per aggiungere o modificare la data di scadenza del segreto dell'applicazione in uso.

1. Nella procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse), fare clic con il pulsante destro del mouse su una connessione e fare clic su **Edit Connection** (Modifica connessione).
2. Nella pagina **Connection Properties** (Proprietà connessione), fare clic su **Secret expiration date** (Data di scadenza del segreto) per aggiungere o modificare la data di scadenza del segreto dell'applicazione in uso.




## Autorizzazioni Azure richieste

Questa sezione contiene i dettagli delle autorizzazioni minime e generali richieste per Azure.

### Autorizzazioni minime

Le autorizzazioni minime offrono un migliore controllo della sicurezza. Tuttavia, le nuove funzionalità che richiedono autorizzazioni aggiuntive non funzioneranno se vengono fornite solo le autorizzazioni minime. Questa sezione elenca le autorizzazioni minime per azione.

**Creazione di una connessione host** Aggiungere una connessione host utilizzando le informazioni ottenute da Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
<!--NeedCopy-->
```

**Gestione dell'alimentazione delle macchine virtuali** Accendere o spegnere le istanze della macchina.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
<!--NeedCopy-->
```

**Creazione, aggiornamento o eliminazione di macchine virtuali** Creare un catalogo delle macchine, quindi aggiungere, eliminare, aggiornare le macchine ed eliminare il catalogo delle macchine.

Di seguito è riportato l'elenco delle autorizzazioni minime richieste quando le immagini master sono dischi gestiti o snapshot che si trovano nella stessa area geografica della connessione di hosting.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
```

```
28 <!--NeedCopy-->
```

Sono necessarie le seguenti autorizzazioni aggiuntive basate su autorizzazioni minime per le seguenti funzionalità:

- Se l'immagine master è un disco rigido virtuale (VHD) in un account di archiviazione situato nella stessa area geografica della connessione host:

```
1 "Microsoft.Storage/storageAccounts/read",
2 "Microsoft.Storage/storageAccounts/listKeys/action",
3 <!--NeedCopy-->
```

- Se l'immagine master è una ImageVersion della Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise):

```
1 "Microsoft.Compute/galleries/read",
2 "Microsoft.Compute/galleries/images/read",
3 "Microsoft.Compute/galleries/images/versions/read",
4 <!--NeedCopy-->
```

- Se l'immagine master è un disco gestito o una snapshot o se il VHD si trova in una regione diversa dalla regione della connessione di hosting:

```
1 "Microsoft.Storage/storageAccounts/read",
2 "Microsoft.Storage/storageAccounts/listKeys/action",
3 "Microsoft.Storage/storageAccounts/write",
4 "Microsoft.Storage/storageAccounts/delete",
5 <!--NeedCopy-->
```

- Se si utilizza un gruppo di risorse gestito da Citrix:

```
1 "Microsoft.Resources/subscriptions/resourceGroups/write",
2 "Microsoft.Resources/subscriptions/resourceGroups/delete",
3 <!--NeedCopy-->
```

- Se si colloca l'immagine master nella Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise):

```
1  "Microsoft.Compute/galleries/write",
2  "Microsoft.Compute/galleries/images/write",
3  "Microsoft.Compute/galleries/images/versions/write",
4  "Microsoft.Compute/galleries/read",
5  "Microsoft.Compute/galleries/images/read",
6  "Microsoft.Compute/galleries/images/versions/read",
7  "Microsoft.Compute/galleries/delete",
8  "Microsoft.Compute/galleries/images/delete",
9  "Microsoft.Compute/galleries/images/versions/delete",
10 <!--NeedCopy-->
```

- Se si utilizza il supporto degli host dedicati di Azure:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- Se si utilizza la crittografia lato server (SSE) con le chiavi gestite dal cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

- Se si distribuiscono macchine virtuali utilizzando modelli ARM (profilo macchina):

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
<!--NeedCopy-->
```

- Se si utilizza la specifica del modello di Azure come profilo macchina:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

**Creazione, aggiornamento ed eliminazione di macchine con disco non gestito** Di seguito è riportato l'elenco delle autorizzazioni minime richieste quando l'immagine master è un VHD e utilizza il gruppo di risorse come fornito dall'amministratore:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action"
<!--NeedCopy-->
```

**Gestire i dispositivi aggiunti ad Azure AD** Di seguito è riportato l'elenco delle autorizzazioni minime richieste per la gestione dei dispositivi aggiunti ad Azure AD:

```
microsoft.directory/devices/standard/read
microsoft.directory/devices/delete
<!--NeedCopy-->
```

### Autorizzazioni generali

Il ruolo di collaboratore ha accesso completo per gestire tutte le risorse. Questo set di autorizzazioni non impedisce di ottenere nuove funzionalità.

Il seguente set di autorizzazioni fornisce la migliore compatibilità in futuro, sebbene includa più autorizzazioni del necessario con il set di funzionalità corrente:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
```

```
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

**Autorizzazione Azure AD** Se si creano cataloghi di macchine aggiunte ad Azure AD, MCS è responsabile della gestione dei dispositivi Azure AD quando si abilita la gestione dei dispositivi collegati ad Azure AD. Il ruolo di **amminstratore del dispositivo cloud** integrato in Azure AD offre la migliore compatibilità verso il futuro, sebbene includa più autorizzazioni di quelle necessarie per l'insieme di funzionalità corrente.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su Azure, vedere Creare un catalogo di Microsoft Azure.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti cloud Microsoft Azure Resource Manager

## Connessione a Microsoft System Center Virtual Machine Manager

December 21, 2022

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano dettagli specifici di Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Prima di creare una connessione a VMM, è necessario completare la configurazione del proprio account VMM come posizione delle risorse. Vedere Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.

### Creare una connessione

Se è stato utilizzato MCS per eseguire il provisioning delle macchine virtuali, eseguire le seguenti operazioni nella procedura guidata di creazione della connessione:

- Immettere l'indirizzo come nome di dominio completo del server host.
- Inserire le credenziali per l'account amministratore impostato in precedenza. Questo account deve disporre dell'autorizzazione a creare nuove macchine virtuali.
- Nella finestra di dialogo Host Details (Dettagli host) selezionare il cluster o l'host autonomo da utilizzare per la creazione di macchine virtuali.

  > **Importante**
  >
  > Cercare un cluster o un host autonomo anche se si utilizza una singola distribuzione host Hyper-V.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per creare cataloghi di macchine con MCS sulla condivisione di file SMB 3, vedere Creare un catalogo di Microsoft System Center Virtual Machine Manager.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.

## Connessione a Nutanix

December 21, 2022

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici di Nutanix.

> **Nota:**
>
> Prima di creare una connessione a Nutanix, è necessario completare la configurazione del proprio account Nutanix come posizione delle risorse. Vedere Ambienti di virtualizzazione Nutanix.

### Creare una connessione a Nutanix

Le seguenti informazioni sono un'aggiunta alle linee guida in Creare e gestire connessioni. Per creare una connessione Nutanix, seguire la guida generale di quell'articolo, tenendo conto dei dettagli specifici di Nutanix.

Nella procedura guidata **Add Connection and Resources** (Aggiungere connessioni e risorse), selezionare il tipo di connessione **Nutanix** nella pagina **Connection** (Connessione), quindi specificare l'indirizzo e le credenziali, oltre a un nome per la connessione. Nella pagina **Network** selezionare una rete per l'unità di hosting.

Sono disponibili i seguenti tipi di connessione da selezionare: **Nutanix AHV**, **Nutanix AHV XI** e **Nutanix AHV PC**.

- Per **Nutanix AHV** specificare l'indirizzo e le credenziali del cluster Prism Element (PE).
- Per **Nutanix AHV PC**, specificare l'indirizzo e le credenziali dell'hypervisor.
- Per **Nutanix AHV XI**, specificare il proprio indirizzo e nome utente, quindi importare le chiavi pubbliche e private contenute nei file di credenziali di Nutanix XI (`.pem`). (le chiavi pubbliche e private sono generate nel cloud Nutanix XI dagli amministratori di Nutanix XI).
  - Per importare la chiave, individuare il file delle credenziali, aprilo con Blocco note (o qualsiasi editor di testo), quindi copiare il contenuto. Successivamente, tornare alla pagina **Connection** (Connessione), selezionare **Import key** (Chiave di importazione), incollare il contenuto e quindi selezionare **Save** (Salva).

  Attenzione: non modificare il contenuto delle credenziali o il relativo formato.

> **Suggerimento:**
>
> Se si distribuiscono macchine utilizzando Nutanix AHV (Prism Element) come risorsa, selezionare il contenitore in cui risiede il disco della macchina virtuale.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su Nutanix, vedere Creare un catalogo di Nutanix.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti di virtualizzazione Nutanix
- Soluzioni Nutanix Cloud e dei partner

## Connessione alle soluzioni Nutanix Cloud e dei partner

June 8, 2023

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici delle soluzioni Nutanix Cloud e dei partner.

Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) supporta la seguente soluzione Nutanix Cloud e dei partner:

- Nutanix Cloud Clusters su AWS

> **Nota:**
>
> Prima di creare una connessione a Nutanix Cloud e dei partner, è necessario completare la configurazione del proprio account come posizione delle risorse. Scopri le Soluzioni Nutanix Cloud e dei partner.

### Connettersi a Nutanix Prism

Dopo aver creato un cluster Nutanix, connettersi a Nutanix Prism.
Per connettersi a Nutanix Prism:

1. Creare una macchina virtuale bastion nella subnet 10.0.129.0/24.
2. Creare una connessione RDP alla macchina virtuale bastion, andare all'URL del **Prism Element** copiato nella sezione precedente.
3. Accedere utilizzando le credenziali predefinite: `admin`:`nutanix`/`4u`. Ricordarsi di cambiare la password.

### Creare una macchina virtuale sul cluster Nutanix

Dopo essersi connessi a **Nutanix Prism**, creare macchine virtuali sul cluster Nutanix.

#### Se la macchina virtuale ha bisogno di accesso a Internet

1. Andare alla console AWS.
2. Creare una nuova subnet 10.0.130.0/24 nello stesso VPC di quella creata da Nutanix CFS.
3. Aggiungere un percorso alla tabella di instradamento di questa subnet per indirizzare tutto il traffico locale al gateway NAT sopra indicato.
4. Creare una connessione RDP alla macchina virtuale bastion, andare all'URL del **Prism Element** copiato nella sezione precedente e accedere.
5. Aggiungere una nuova rete. Andare a **Settings>Network Configuration>Create Subnet** (Impostazioni> Configurazione di rete> Crea subnet). Utilizzare la stessa sottorete 10.0.130.0/24 utilizzata in AWS.
6. Creare tutte le macchine virtuali (AD, CC, VDA e così via) in quella nuova subnet.

#### Se la macchina virtuale non ha bisogno di accesso a Internet

1. Creare una connessione RDP alla macchina virtuale bastion, andare all'URL del **Prism Element** copiato nella sezione precedente e accedere.
2. Aggiungere una nuova rete. Andare a **Settings>Network Configuration>Create Subnet** (Impostazioni> Configurazione di rete> Crea subnet). Usare la subnet 10.0.129.0/24.
3. Creare tutte le macchine virtuali (AD, CC, VDA e così via) in quella subnet.

> **Suggerimento:**
>
> Assicurarsi che le informazioni relative all'ora e al fuso orario nelle macchine virtuali siano impostate correttamente. Questo è particolarmente importante per AD.

### Creare una connessione host

1. Avviare Citrix Studio.
2. Selezionare il nodo di hosting e fare clic su **Add Connection and Resources** (Aggiungi connessione e risorse).
3. Nella schermata **Connection** (Connessione), selezionare **Create a new Connection** (Crea una nuova connessione) e nel campo **Connection address** (Indirizzo di connessione) immettere `https://xxx.xxx.xxx.xxx:9440`.
4. Seguire l'interfaccia utente per completare la procedura guidata.

> **Nota:**
>
> Tutte le VM dei connettori devono avere il plug-in Nutanix installato affinché l'opzione Nutanix sia disponibile in Citrix Studio, anche se i plug-in non vengono utilizzati nella zona Nutanix.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su Nutanix, vedere Creare un catalogo di Nutanix.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti di virtualizzazione Nutanix
- Soluzioni Nutanix Cloud e dei partner

## Connessione a VMware

December 5, 2023

Creare e gestire connessioni descrive le procedure guidate che creano una connessione. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione VMware.

> **Nota:**
>
> Prima di creare una connessione a VMware, è necessario completare la configurazione del proprio account VMware come posizione delle risorse. Vedere Ambienti di virtualizzazione VMware.

### Autorizzazioni richieste

Creare un account utente VMware e uno o più ruoli VMware con un insieme delle autorizzazioni o con tutte le autorizzazioni elencate in questo articolo. Basare la creazione dei ruoli sul livello specifico di granularità richiesto rispetto alle autorizzazioni dell'utente per richiedere le varie operazioni di Citrix Virtual Apps o Citrix Virtual Desktops in qualsiasi momento. Per concedere autorizzazioni specifiche per l'utente in qualsiasi momento, associarle al rispettivo ruolo, almeno a livello di centro dati.

Nelle tabelle seguenti vengono illustrati i mapping tra le operazioni di Citrix Virtual Apps and Desktops e le autorizzazioni VMware minime richieste.

### Aggiungere connessioni e risorse

| SDK | Interfaccia utente |
| --- | --- |
| System.Anonymous, System.Read e System.View | Aggiunto automaticamente. È possibile utilizzare il ruolo di sola lettura incorporato. |

**Gestione dell'alimentazione**

| SDK | Interfaccia utente |
| --- | --- |
| VirtualMachine.Interact.PowerOff | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni) |
| VirtualMachine.Interact.PowerOn | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power On (Accendi) |
| VirtualMachine.Interact.Reset | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Reset (Reimposta) |
| VirtualMachine.Interact.Suspend | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Suspend (Sospendi) |

**Provisioning di macchine (Machine Creation Services)**

Per effettuare il provisioning delle macchine tramite MCS, le seguenti autorizzazioni sono obbligatorie:

| SDK | Interfaccia utente |
| --- | --- |
| Datastore.AllocateSpace | Datastore > Allocate space (Alloca spazio) |
| Datastore.Browse | Datastore > Browse datastore (Sfoglia datastore) |
| Datastore.FileManagement | Datastore > Low level file operations (Operazioni file di basso livello) |
| Network.Assign | Network (Rete) > Assign network (Assegna rete) |
| Resource.AssignVMToPool | Resource (Risorsa) > Assign virtual machine to resource pool (Assegna macchina virtuale al pool di risorse) |
| VirtualMachine.Config.AddExistingDisk | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add existing disk (Aggiungi disco esistente) |

| SDK | Interfaccia utente |
| --- | --- |
| VirtualMachine.Config.AddNewDisk | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add new disk (Aggiungi nuovo disco) |
| VirtualMachine.Config.AdvancedConfig | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Advanced (Avanzate) |
| VirtualMachine.Config.RemoveDisk | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Remove disk (Rimuovi disco) |
| VirtualMachine.Config.CPUCount | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change CPU Count (Modifica conteggio CPU) |
| VirtualMachine.Config.Memory | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change memory (Modifica memoria) |
| VirtualMachine.Config.Settings | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change settings (Modifica impostazioni) |
| VirtualMachine.Interact.PowerOff | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni) |
| VirtualMachine.Interact.PowerOn | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power On (Accendi) |
| VirtualMachine.Interact.Reset | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Reset (Reimposta) |
| VirtualMachine.Interact.Suspend | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Suspend (Sospendi) |
| VirtualMachine.Inventory.CreateFromExisting | Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create from existing (Crea da esistente) |
| VirtualMachine.Inventory.Create | Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create new (Crea nuova) |
| VirtualMachine.Inventory.Delete | Virtual machine (Macchina virtuale) > Inventory (Inventario) > Remove (Rimuovi) |
| VirtualMachine.Provisioning.Clone | Virtual machine (Macchina virtuale) > Provisioning > Clone virtual machine (Clona macchina virtuale) |

| SDK | Interfaccia utente |
| --- | --- |
| VirtualMachine.State.CreateSnapshot | vSphere 5.0, Update 2, vSphere 5.1, Update 1 e vSphere 6.x, Update 1: Virtual machine (Macchina virtuale) > State (Stato) > Create snapshot (Crea snapshot); vSphere 5.5: Virtual machine (Macchina virtuale) > Snapshot management (Gestione snapshot) > Create snapshot (Crea snapshot) |

**Aggiornamento e rollback delle immagini**

| SDK | Interfaccia utente |
| --- | --- |
| Datastore.AllocateSpace | Datastore > Allocate space (Alloca spazio) |
| Datastore.Browse | Datastore > Browse datastore (Sfoglia datastore) |
| Datastore.FileManagement | Datastore > Low level file operations (Operazioni file di basso livello) |
| Network.Assign | Network (Rete) > Assign network (Assegna rete) |
| Resource.AssignVMToPool | Resource (Risorsa) > Assign virtual machine to resource pool (Assegna macchina virtuale al pool di risorse) |
| VirtualMachine.Config.AddExistingDisk | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add existing disk (Aggiungi disco esistente) |
| VirtualMachine.Config.AddNewDisk | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add new disk (Aggiungi nuovo disco) |
| VirtualMachine.Config.AdvancedConfig | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Advanced (Avanzate) |
| VirtualMachine.Config.RemoveDisk | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Remove disk (Rimuovi disco) |
| VirtualMachine.Interact.PowerOff | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni) |

| SDK | Interfaccia utente |
| --- | --- |
| VirtualMachine.Interact.PowerOn | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power On (Accendi) |
| VirtualMachine.Interact.Reset | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Reset (Reimposta) |
| VirtualMachine.Inventory.CreateFromExisting | Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create from existing (Crea da esistente) |
| VirtualMachine.Inventory.Create | Virtual machine (Macchina virtuale) > Inventory (Inventario) > Create new (Crea nuova) |
| VirtualMachine.Inventory.Delete | Virtual machine (Macchina virtuale) > Inventory (Inventario) > Remove (Rimuovi) |
| VirtualMachine.Provisioning.Clone | Virtual machine (Macchina virtuale) > Provisioning > Clone virtual machine (Clona macchina virtuale) |

**Eliminare le macchine con provisioning**

| SDK | Interfaccia utente |
| --- | --- |
| Datastore.Browse | Datastore > Browse datastore (Sfoglia datastore) |
| Datastore.FileManagement | Datastore > Low level file operations (Operazioni file di basso livello) |
| VirtualMachine.Config.RemoveDisk | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Remove disk (Rimuovi disco) |
| VirtualMachine.Interact.PowerOff | Virtual machine (Macchina virtuale) > Interaction (Interazione) > Power Off (Spegni) |
| VirtualMachine.Inventory.Delete | Virtual machine (Macchina virtuale) > Inventory (Inventario) > Remove (Rimuovi) |

**Profilo di storage (vSAN)**

Per visualizzare, creare o eliminare i criteri di archiviazione durante la creazione di cataloghi su un datastore vSAN, sono obbligatorie le seguenti autorizzazioni:

| SDK | Interfaccia utente |
| --- | --- |
| storage.Profile-driven storage update | PROFILE-DRIVEN STORAGE > Profile-driven storage update |
| storage.Profile-driven storage view | PROFILE-DRIVEN STORAGE > Profile-driven storage view |

**Tag e attributi personalizzati**

I tag e gli attributi personalizzati consentono di allegare metadati alle macchine virtuali create nell'inventario di vSphere e semplificano la ricerca e il filtraggio di questi oggetti. Per creare, modificare, assegnare ed eliminare tag o categorie, sono obbligatorie le seguenti autorizzazioni:

| SDK | Interfaccia utente |
| --- | --- |
| Tagging.Create | vSphere Tagging > Create vSphere Tag (Crea tag vSphere) |
| Tagging.Create | vSphere Tagging > Create vSphere Tag Category (Crea categoria di tag vSphere) |
| Tagging.Edit | vSphere Tagging > Edit vSphere Tag (Modifica tag vSphere) |
| Tagging.Edit | vSphere Tagging > Edit vSphere Tag Category (Modifica categoria di tag vSphere) |
| Tagging.Delete | vSphere Tagging > Delete vSphere Tag (Elimina tag vSphere) |
| Tagging.Delete | vSphere Tagging > Delete vSphere Tag Category (Elimina categoria di tag vSphere) |
| Tagging.Assign | vSphere Tagging > Assign or Unassign vSphere Tag (Assegna o annulla assegnazione del tag vSphere) |
| Tagging.Assign | vSphere Tagging > Assign or Unassign vSphere Tag on Object (Assegna o annulla l'assegnazione di tag vSphere all'oggetto) |
| Global.ManageCustomFields | Global (Globali) > Manage custom attributes (Gestisci attributi personalizzati) |
| Global.SetCustomField | Global (Globali) > Set custom attribute (Imposta attributo personalizzato) |

> **Nota:**
>
> Quando MCS crea un catalogo di macchine, assegna alle VM di destinazione speciali tag con nomi. Questi tag differenziano l'immagine master dalle VM create da MCS e impediscono l'utilizzo di macchine virtuali create da MCS per la preparazione delle immagini. È possibile identificare la differenza in base al valore dell'attributo `XdProvisioned` in vCenter. L'attributo è impostato su **True** se MCS crea macchine virtuali.

### Operazioni crittografiche

I privilegi delle operazioni crittografiche controllano quali utenti possono eseguire i diversi tipi di operazioni crittografiche e su quale tipo di oggetto. vSphere Native Key Provider utilizza i privilegi `Cryptographer.*`. Per le operazioni crittografiche sono necessarie le seguenti autorizzazioni minime:

> **Nota:**
>
> Queste autorizzazioni sono necessarie per creare cataloghi di macchine MCS con VM dotata di vTPM.

| SDK | Interfaccia utente |
|---|---|
| Cryptographic operations.Direct Access | Privileges > All Privileges > Cryptographic operations > Direct Access (Privilegi > Tutti i privilegi > Operazioni crittografiche > Accesso diretto) |
| Cryptographic operations.Add disk | Privileges > All Privileges > Cryptographic operations > Add disk (Privilegi > Tutti i privilegi > Operazioni crittografiche > Aggiungi disco) |
| Cryptographic operations.Clone | Privileges > All Privileges > Cryptographic operations > Clone (Privilegi > Tutti i privilegi > Operazioni crittografiche > Clone) |
| Cryptographic operations.Encrypt | Privileges > All Privileges > Cryptographic operations > Encrypt (Privilegi > Tutti i privilegi > Operazioni crittografiche > Crittografa) |
| Cryptographic operations.Encrypt new | Privileges > All Privileges > Cryptographic operations > Encrypt new (Privilegi > Tutti i privilegi > Operazioni crittografiche > Crittografa nuovo) |

| SDK | Interfaccia utente |
| --- | --- |
| Cryptographic operations.Decrypt | Privileges > All Privileges > Cryptographic operations > Decrypt (Privilegi > Tutti i privilegi > Operazioni crittografiche > Decrittografa) |
| Operazioni crittografiche. Migrazione | Privileges > All Privileges > Cryptographic operations > Migrate (Privilegi > Tutti i privilegi > Operazioni crittografiche > Migrazione) |
| Operazioni crittografiche. Leggi le informazioni KMS | Privileges > All Privileges > Cryptographic operations > Read KMS information (Privilegi > Tutti i privilegi > Operazioni crittografiche > Leggi le informazioni KMS) |

**Provisioning delle macchine (Citrix Provisioning)**

Tutte le autorizzazioni del comando di **provisioning delle macchine (Machine Creation Services)** e i seguenti.

| SDK | Interfaccia utente |
| --- | --- |
| VirtualMachine.Config.AddRemoveDevice | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Add or remove device (Aggiungi o rimuovi dispositivo) |
| VirtualMachine.Config.CPUCount | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Change CPU Count (Modifica conteggio CPU) |
| VirtualMachine.Config.Memory | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Memory (Memoria) |
| VirtualMachine.Config.Settings | Virtual machine (Macchina virtuale) > Configuration (Configurazione) > Settings (Impostazioni) |
| VirtualMachine.Provisioning.CloneTemplate | Virtual machine (Macchina virtuale) > Provisioning > Clone template (Clona modello) |
| VirtualMachine.Provisioning.DeployTemplate | Virtual machine (Macchina virtuale) > Provisioning > Deploy template (Distribuisci modello) |
| vApp.Export | vApp > Export (Esporta) |

> **Nota:**
>
> - Le autorizzazioni per clonare e distribuire un modello sono necessarie per fornire macchine virtuali utilizzando l'installazione guidata di Citrix Virtual Apps and Desktops e la procedura guidata Export Devices tramite la console Citrix Provisioning.
> - `vApp.Export` è necessario per creare cataloghi di macchine MCS utilizzando il profilo macchina.

## Proteggere le connessioni all'ambiente VMware

L'utilizzo di connessioni HTTPS / SSL a vCenter richiede che la connessione sia considerata affidabile da Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops).

Sono disponibili due opzioni:

- Ogni connettore cloud considera attendibile il certificato vCenter e i servizi sul connettore riutilizzano tale attendibilità. L'attendibilità può provenire da:
  - Certificato vCenter, rilasciato dall'autorità di certificazione e considerato attendibile da Windows, che crea un'affidabilità consolidata tra Windows e vCenter.
  - Certificato vCenter installato su Windows, che crea un'affidabilità consolidata tra Windows e vCenter.
- In alternativa, nel database Citrix Virtual Apps and Desktops è installata l'impronta digitale SSL. Questa impronta digitale viene utilizzata da Citrix DaaS su ciascun Cloud Connector per l'affidabilità delle connessioni a vCenter.

> **Nota:**
>
> Il certificato vCenter e l'impronta digitale SSL VMware non sono richiesti per VMware Cloud e le relative soluzioni partner.

### Ottenere e importare un certificato

Per proteggere le comunicazioni vSphere, Citrix consiglia di utilizzare HTTPS anziché HTTP. HTTPS richiede certificati digitali. Citrix consiglia di utilizzare un certificato digitale emesso da un'autorità di certificazione in conformità con i criteri di sicurezza dell'organizzazione.

Se non si è in grado di utilizzare un certificato digitale emesso da un'autorità di certificazione e i criteri di sicurezza dell'organizzazione lo consentono, è possibile utilizzare il certificato autofirmato installato da VMware. Aggiungere il certificato VMware vCenter a ciascun Cloud Connector.

1. Aggiungere il nome di dominio completo (FQDN) del computer che esegue vCenter Server al file hosts su quel server, situato in %SystemRoot%/WINDOWS/system32/Drivers/etc/. Questo

passaggio è necessario solo se il nome di dominio completo del computer che esegue vCenter Server non è già presente nel sistema dei nomi di dominio.

2. Ottenere il certificato vCenter utilizzando uno dei tre metodi seguenti:

   **Dal server vCenter:**

   a) Copiare il file rui.crt dal server vCenter in una posizione accessibile sui Cloud Connector.
   b) Sul Cloud Connector, passare alla posizione del certificato esportato e aprire il file rui.crt.

   **Scaricare il certificato utilizzando un browser Web:** se si utilizza Internet Explorer, a seconda del proprio account utente, è necessario fare clic con il pulsante destro del mouse su Internet Explorer e scegliere **Esegui come amministratore** per scaricare o installare il certificato.

   a) Aprire il browser Web e stabilire una connessione Web sicura al server vCenter (ad esempio https://server1.domain1.com).
   b) Accettare gli avvisi di sicurezza.
   c) Fare clic sulla barra degli indirizzi che visualizza l'errore del certificato.
   d) Visualizzare il certificato e fare clic sulla scheda Dettagli.
   e) Selezionare **Copy to file and export in .CER format** (Copia su file ed esporta in formato.CER), fornendo un nome quando richiesto.
   f) Salvare il certificato esportato.
   g) Passare alla posizione del certificato esportato e aprire il file .CER.

   **Importare direttamente da Internet Explorer in esecuzione come amministratore:**

   a) Aprire il browser Web e stabilire una connessione Web sicura al server vCenter (ad esempio https://server1.domain1.com).
   b) Accettare gli avvisi di sicurezza.
   c) Fare clic sulla barra degli indirizzi che visualizza l'errore del certificato.
   d) Visualizzare il certificato.

3. Importare il certificato nell'archivio dei certificati su ogni Cloud Connector.

   a) Fare clic sull'opzione **Install certificate** (Installa certificato), selezionare **Local Machine** (Macchina locale) e quindi fare clic su **Next** (Avanti).
   b) Selezionare **Place all certificates in the following store** (Inserisci tutti i certificati nell'archivio seguente) e quindi fare clic su **Browse** (Sfoglia). In una versione supportata successiva: selezionare **Trusted People** (Persone attendibili) e quindi fare clic su **OK**. Fare clic su **Next** e quindi su **Finish**.

> **Importante:**

> Se si modifica il nome del server vSphere dopo l'installazione, è necessario generare un nuovo certificato autofirmato su tale server prima di importare il nuovo certificato.

#### Impronta digitale SSL di VMware

La funzionalità dell'impronta digitale SSL di VMware risolve un errore segnalato frequentemente durante la creazione di una connessione host a un hypervisor VMware vSphere. In precedenza, gli amministratori dovevano creare manualmente una relazione di trust tra i Delivery Controller gestiti da Citrix nel sito e il certificato dell'hypervisor prima di creare una connessione. La funzionalità dell'impronta digitale SSL VMware rimuove questo requisito manuale: l'impronta digitale del certificato non attendibile viene memorizzata nel database del sito in modo che l'hypervisor possa essere continuamente identificato come attendibile da Citrix Virtual Apps o Citrix Virtual Desktops, anche se non dai controller.

Quando si crea una connessione host vSphere, una finestra di dialogo consente di visualizzare il certificato della macchina a cui ci si connette. È quindi possibile scegliere se considerarlo affidabile.

L'impronta digitale SSL di VMware può essere aggiornata in seguito utilizzando l'SDK PowerShell `Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>`.

> **Suggerimento:**
>
> L'impronta digitale del certificato deve essere scritta in lettere maiuscole.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su VMware, vedere Creare un catalogo di VMware.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti di virtualizzazione VMware
- Soluzioni VMware Cloud e dei partner

## Connessione alle soluzioni VMware Cloud e dei partner

December 21, 2022

Dopo aver configurato il cluster Azure VMware Solution (AVS), Google Cloud VMware Engine e il cloud VMware su AWS, creare le connessioni. Vedere Connessione agli ambienti di virtualizzazione VMware per creare connessioni.

### Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine.
- Per informazioni specifiche su VMware, vedere Creare un catalogo di VMware.

### Ulteriori informazioni

- Connessioni e risorse
- Ambienti di virtualizzazione VMware
- Soluzioni VMware Cloud e dei partner

## Creare cataloghi di macchine

November 21, 2023

> **Nota:**
>
> In questo articolo viene descritto come creare cataloghi utilizzando l'interfaccia Full Configuration (Configurazione completa). Se si utilizza Quick Deploy (Distribuzione rapida) per creare risorse di Azure, seguire le indicazioni riportate in Creare cataloghi con Quick Deploy (Distribuzione rapida).

Le raccolte di macchine fisiche o virtuali vengono gestite in una singola entità denominata catalogo di macchine. Tutte le macchine in un catalogo hanno lo stesso tipo di sistema operativo: sistema operativo multisessione o sistema operativo a sessione singola e macchine Windows o Linux.

L'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa) guida l'utente nella creazione del primo catalogo delle macchine. Dopo aver creato il primo catalogo, si crea il primo gruppo di consegna. In seguito, è possibile modificare il catalogo creato e creare altri cataloghi.

### Panoramica

Quando si crea un catalogo di macchine virtuali, è necessario specificare come eseguire il provisioning di tali macchine virtuali. È possibile utilizzare Machine Creation Services (MCS). In alternativa, è possibile utilizzare i propri strumenti per il provisioning delle macchine.

- Se si utilizza MCS per il provisioning di macchine virtuali, fornire un'immagine (o una snapshot) per creare macchine virtuali identiche nel catalogo. Prima di creare il catalogo, è innanzitutto necessario utilizzare gli strumenti dell'hypervisor o del servizio cloud per creare e configurare l'immagine. Questo processo include l'installazione di un Virtual Delivery Agent (VDA) sull'immagine. Quindi si crea il catalogo delle macchine nell'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa). Selezionare l'immagine (o la snapshot di un'immagine), specificare il numero di macchine virtuali da creare nel catalogo e configurare le informazioni aggiuntive.
- Se le macchine sono già disponibili, è comunque necessario creare uno o più cataloghi di macchine per importare queste macchine virtuali nel catalogo.

Quando si utilizza MCS per creare il primo catalogo, è necessario specificare un'unità di hosting creata in precedenza. L'unità di hosting fornisce la configurazione delle risorse per creare una macchina virtuale. Successivamente (dopo aver creato il primo catalogo e il primo gruppo di consegna), è possibile modificare le informazioni su quell'unità di hosting o sulla sua connessione host principale oppure creare altre connessioni e unità di hosting.

Se un Cloud Connector non funziona correttamente, le operazioni di provisioning MCS (come gli aggiornamenti del catalogo) richiedono molto più tempo del solito e le prestazioni dell'interfaccia di gestione peggiorano in modo significativo.

#### Controllo licenza Servizi Desktop remoto

La creazione di un catalogo delle macchine contenente macchine con sistema operativo Windows multisessione include un controllo automatico delle licenze Microsoft RDS valide. Viene eseguita una ricerca nel catalogo per trovare una macchina in funzione e registrata su cui eseguire il controllo.

- Se non è possibile trovare una macchina in funzione e registrata, viene visualizzato un avviso che indica che il controllo delle licenze RDS non può essere eseguito.
- Se viene individuata una macchina e viene rilevato un errore, **Manage > Full Configuration** (Gestisci > Configurazione completa) visualizza un messaggio di avviso per il catalogo contenente il problema rilevato. Per rimuovere un avviso di licenza RDS da un catalogo (in modo che non appaia più sullo schermo), selezionare il catalogo. Selezionare **Remove RDS license warning** (Rimuovi avviso di licenza RDS). Quando richiesto, confermare l'azione.

#### Registrazione dei VDA

Un VDA deve essere registrato con un Cloud Connector per essere preso in considerazione quando si avviano sessioni con intermediario. I VDA non registrati possono causare un sottoutilizzo di risorse altrimenti disponibili. Un VDA potrebbe non venire registrato per vari motivi, molti dei quali sono risolvi-

bili. Le informazioni sulla risoluzione dei problemi sono fornite nella procedura guidata di creazione del catalogo e dopo aver aggiunto un catalogo a un gruppo di consegna.

Nella procedura guidata di creazione del catalogo, dopo che sono state aggiunte macchine esistenti mediante la procedura guidata, l'elenco dei nomi di account computer indica se ogni macchina è adatta per l'aggiunta al catalogo. Passare il mouse sull'icona accanto a ogni macchina per visualizzare un messaggio informativo su quella macchina.

Se il messaggio identifica una macchina problematica, è possibile rimuoverla (utilizzando il pulsante **Remove**) o aggiungerla. Ad esempio, se un messaggio indica che non è possibile ottenere informazioni su una macchina (forse perché non era mai stata registrata), è possibile scegliere di aggiungere comunque la macchina.

Per ulteriori informazioni sulla risoluzione dei problemi relativi alla registrazione dei VDA, vedere CTX136668.

#### Riepilogo della creazione del catalogo MCS

Ecco una breve panoramica delle azioni MCS predefinite dopo che sono state fornite le informazioni nella creazione guidata catalogo.

- Se è stata selezionata un'immagine (anziché una snapshot), MCS crea una snapshot.
- MCS crea una copia completa dell'istantanea e la posiziona in ciascuna posizione di archiviazione definita nella connessione host.
- MCS aggiunge le macchine ad Active Directory, che crea identità univoche.
- MCS crea il numero di macchine virtuali specificato nella procedura guidata, definendo due dischi per ciascuna macchina virtuale. Oltre ai due dischi per macchina virtuale, viene memorizzato anche un master nella stessa posizione di archiviazione. Se sono stati definiti più percorsi di archiviazione, ciascuno di essi ottiene i seguenti tipi di disco:
  - Copia completa della snapshot (come indicato sopra), di sola lettura e condivisa tra le macchine virtuali appena create.
  - Un disco di identità univoco da 16 MB che conferisce a ciascuna macchina virtuale un'identità univoca. Ogni macchina virtuale ottiene un disco di identità.
  - Un disco di differenza univoco per archiviare le scritture effettuate nella macchina virtuale. Questo disco è sottoposto a thin provisioning (se supportato dall'archiviazione host) e aumenta fino alle dimensioni massime dell'immagine master, se necessario. Ogni macchina virtuale ottiene un disco di differenza. Il disco di differenza contiene le modifiche apportate durante le sessioni. È permanente per i desktop dedicati. Per i desktop in pool, viene eliminato e ne viene creato uno nuovo dopo ogni riavvio.

In alternativa, durante la creazione di macchine virtuali per la distribuzione di desktop statici, è possibile specificare (nella pagina **Machines** della creazione guidata catalogo) duplicati di macchine virtu-

ali spesse (copia completa). I cloni completi non richiedono la conservazione dell'immagine master in ogni archivio dati. Ogni macchina virtuale dispone di un proprio file.

#### Considerazioni sull'archiviazione MCS

Ci sono molti fattori da valutare quando si scelgono le soluzioni di archiviazione, le configurazioni e le capacità per MCS. Le seguenti informazioni forniscono considerazioni appropriate per la capacità di archiviazione:

*Considerazioni sulla capacità:*

- Dischi

  I dischi Delta o Differencing (Diff) occupano la maggior quantità di spazio nella maggior parte delle distribuzioni MCS per ogni macchina virtuale. Ogni macchina virtuale creata da MCS viene fornita con almeno 2 dischi al momento della creazione.

  - Disk0= Diff Disk: contiene il sistema operativo quando viene copiato dall'immagine di base principale.
  - Disk1 = Disco di identità: 16 MB - contiene i dati di Active Directory per ogni macchina virtuale.

  Mano mano che il prodotto si evolve, potrebbe essere necessario aggiungere altri dischi per soddisfare determinati casi d'uso e il consumo di funzionalità. Ad esempio:

  - MCS Storage Optimization crea un disco in stile cache di scrittura per ogni macchina virtuale.
  - MCS ha aggiunto la possibilità di utilizzare cloni completi invece dello scenario del disco Delta descritto nella sezione precedente.

  Anche le funzionalità dell'hypervisor potrebbero essere considerate. Ad esempio:

  - Citrix Hypervisor IntelliCache crea un disco di lettura sull'archiviazione locale per ogni Citrix Hypervisor. Questa opzione risparmia IOPS rispetto all'immagine che potrebbe essere salvata nella posizione di archiviazione condivisa.

- Sovraccarico Hypervisor

  I diversi hypervisor utilizzano file specifici che creano un sovraccarico per le macchine virtuali. Gli hypervisor utilizzano l'archiviazione anche per la gestione e le operazioni di registrazione generali. Calcolare lo spazio per includere il sovraccarico per:

  - File di registro
  - File specifici dell'hypervisor. Ad esempio:

        * VMware aggiunge altri file alla cartella di **VM storage**. Vedere le best practice di VMware.
        * Calcola i requisiti di dimensioni totali delle macchine virtuali. Si consideri una macchina virtuale contenente 20 GB per il disco virtuale, 16 GB per il file di scambio e 100 MB per i file di registro, con un consumo totale di 36,1 GB.
    - Snapshot per XenServer; Snapshot per VMware.

- Sovraccarico del processo

  La creazione di un catalogo, l'aggiunta di un computer e l'aggiornamento di un catalogo hanno implicazioni di archiviazione uniche nel loro genere. Ad esempio:

    - La creazione iniziale del catalogo richiede la copia del disco di base da copiare in ogni posizione di archiviazione.
        * È inoltre necessario creare temporaneamente una macchina virtuale di preparazione.
    - L'aggiunta di una macchina a un catalogo non richiede la copia del disco di base in ciascuna posizione di archiviazione. La creazione del catalogo varia in base alle funzioni selezionate.
    - Aggiornare il catalogo per creare un disco di base aggiuntivo su ogni posizione di archiviazione. Gli aggiornamenti del catalogo presentano anche un picco di archiviazione temporaneo in cui ogni macchina virtuale del catalogo dispone di 2 dischi Diff per un certo periodo di tempo.

*Altre considerazioni:*

- **Dimensionamento RAM:** influisce sulle dimensioni di alcuni file e dischi dell'hypervisor, quali i dischi di ottimizzazione I/O, la cache di scrittura e i file istantanea.
- **Thin/Thick provisioning:** l'archiviazione NFS è preferita grazie alle funzionalità di thin provisioning.

#### Ottimizzazione dell'archiviazione MCS (Machine Creation Services)

La funzionalità di ottimizzazione dell'archiviazione di Machine Creation Services (MCS) è nota anche come MCS I/O ed è disponibile solo su Azure, GCP, Citrix Hypervisor, VMware e SCVMM.

- Il contenitore della cache di scrittura è *basato su file*, la stessa funzionalità che si trova in Citrix Provisioning. Ad esempio, il nome del file della cache di scrittura di Citrix Provisioning è `D:\vdiskdif.vhdx` e il nome del file della cache di scrittura I/O MCS è `D:\mcsdif.vhdx`.
- Si ottengono miglioramenti diagnostici includendo il supporto di un file di dettagli arresto anomalo di Windows scritto sul disco della cache di scrittura.

- MCS I/O conserva la tecnologia *cache nella RAM con overflow sul disco rigido* per fornire la soluzione ottimale di cache di scrittura multi-livello. Questa funzionalità consente all'amministratore di ottenere un equilibrio fra il costo in ciascun livello, ciascuna RAM e ciascun disco e le prestazioni per soddisfare le aspettative del carico di lavoro desiderato.

L'aggiornamento del metodo della cache di scrittura da *basato su disco* a *basato su file* richiede le seguenti modifiche:

1. MCS I/O non supporta più la cache solo RAM. Specificare le dimensioni del disco durante la creazione del catalogo delle macchine.
2. Il disco della cache di scrittura della macchina virtuale viene creato e formattato automaticamente al primo avvio di una macchina virtuale. Una volta che la macchina virtuale è attivata, il file della cache di scrittura `mcsdif.vhdx` viene scritto nel volume formattato `MCSWCDisk`.
3. Il file di paging viene reindirizzato al volume `MCSWCDisk` formattato. Di conseguenza, questa dimensione del disco considera la quantità totale di spazio su disco. Include il delta tra la dimensione del disco e il carico di lavoro generato più la dimensione del file di paging. Questo è in genere associato alle dimensioni della RAM della macchina virtuale.

**Attivare gli aggiornamenti per l'ottimizzazione dell'archiviazione MCS** Per abilitare la funzionalità di ottimizzazione dell'archiviazione MCS I/O, aggiornare il Delivery Controller e il VDA alla versione più recente di Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Se si aggiorna una distribuzione esistente che ha MCS I/O abilitato, non è richiesta alcuna configurazione aggiuntiva. L'aggiornamento del VDA e del Delivery Controller gestisce l'aggiornamento di MCS I/O.

### Assegnare una lettera di unità specifica al disco di cache write-back MCS I/O

È possibile assegnare una lettera di unità specifica al disco della cache di scrittura I/O MCS. Questa implementazione consente di evitare conflitti tra la lettera di unità di qualsiasi applicazione utilizzata e la lettera di unità del disco di cache write-back I/O MCS. Per fare ciò, utilizzare i comandi PowerShell. Gli hypervisor supportati sono Azure, GCP, VMware, SCVMM e Citrix Hypervisor.

> **Nota:**
>
> Questa funzionalità richiede VDA versione 2305 o successiva.

#### Limiti

- Applicabile solo al sistema operativo Windows

- Lettera di unità applicabile per il disco della cache di scrittura: da `E` a `Z`
- Non applicabile quando il disco temporaneo di Azure viene usato come disco di cache di write-back
- Applicabile solo quando si crea un nuovo catalogo di macchine

#### Assegnare una lettera di unità al disco della cache write-back

Per assegnare una lettera di unità al disco della cache write-back:

1. Aprire la finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Creare un pool di identità se non è già stato creato.
4. Creare uno schema di provisioning utilizzando il comando `New-ProvScheme` con la proprietà `WriteBackCacheDriveLetter`. Ad esempio:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
   />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
   false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
    />
```

```
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
    ="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
     />
</CustomProperties>'
<!--NeedCopy-->
```

5. Completare la creazione del catalogo di macchine. Per ulteriori informazioni, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Preparare un'immagine master sull'hypervisor o sul servizio cloud

L'immagine master contiene il sistema operativo, le applicazioni non virtualizzate, il VDA e altro software.

Buono a sapersi:

- Un'immagine master potrebbe anche essere nota come immagine clone, immagine dorata, macchina virtuale di base o immagine di base. I fornitori di host e i fornitori di servizi cloud potrebbero utilizzare termini diversi.
- Assicurarsi che l'hypervisor o il servizio cloud disponga di processori, memoria e archiviazione sufficienti per supportare il numero di macchine create.
- Configurare la quantità corretta di spazio su disco rigido necessaria per desktop e applicazioni. Tale valore non può essere modificato in un secondo momento o nel catalogo macchine.
- I cataloghi di macchine Accesso remoto PC non utilizzano immagini master.
- Considerazioni sull'attivazione del servizio di gestione delle chiavi di Microsoft quando si utilizza MCS: se la distribuzione include VDA 7.x con un host XenServer 6.1 o 6.2, vSphere o Microsoft System Center Virtual Machine Manager, non è necessario riattivare manualmente Microsoft Windows o Microsoft Office.

Installare e configurare il seguente software nell'immagine master:

- Strumenti di integrazione per l'hypervisor (ad esempio Citrix VM Tools, Hyper-V Integration Services o strumenti VMware). Se si omette questo passaggio, applicazioni e desktop potrebbero non funzionare correttamente.
- Un VDA. Citrix consiglia di installare la versione più recente per consentire l'accesso alle funzionalità più recenti. La mancata installazione di un VDA nell'immagine master causa l'esito negativo della creazione del catalogo.

- Strumenti di terze parti, se necessario, come software antivirus o agenti di distribuzione software elettronici. Configurare i servizi con impostazioni appropriate per gli utenti e il tipo di computer (ad esempio l'aggiornamento delle funzionalità).
- Applicazioni di terze parti che non si stanno virtualizzando. Citrix consiglia di virtualizzare le applicazioni. La virtualizzazione riduce i costi eliminando la necessità di aggiornare l'immagine master dopo l'aggiunta o la riconfigurazione di un'applicazione. Inoltre, un numero inferiore di applicazioni installate riduce le dimensioni dei dischi rigidi dell'immagine master, risparmiando così sui costi di archiviazione.
- Client App-V con le impostazioni consigliate, se si prevede di pubblicare applicazioni App-V. Il client App-V è disponibile da Microsoft.
- Quando si utilizza MCS, se si localizza Microsoft Windows, installare le impostazioni internazionali e i Language Pack. Durante il provisioning, quando viene creata una copia istantanea, le macchine virtuali di cui viene eseguito il provisioning utilizzano le impostazioni internazionali e i Language Pack installati.

> **Importante:**
>
> Se si utilizza MCS, non eseguire Sysprep sulle immagini master.

Per preparare un'immagine master:

1. Utilizzando lo strumento di gestione dell'hypervisor, creare un'immagine master e quindi installare il sistema operativo, oltre a tutti i service pack e gli aggiornamenti. Specificare il numero di vCPU. È inoltre possibile specificare il valore vCPU se si crea il catalogo macchine utilizzando PowerShell. Non è possibile specificare il numero di vCPU durante la creazione di un catalogo da **Manage > Full Configuration** (Gestione > Configurazione completa). Configurare la quantità di spazio su disco rigido necessaria per desktop e applicazioni. Tale valore non può essere modificato in un secondo momento o nel catalogo.
2. Assicurarsi che il disco rigido sia collegato alla posizione del dispositivo 0. La maggior parte dei modelli di immagini master standard configura questa posizione per impostazione predefinita, ma alcuni modelli personalizzati potrebbero non farlo.
3. Installare e configurare il software di cui sopra nell'immagine master.
4. Se non si utilizza MCS, aggiungere l'immagine master al dominio di cui sono membri le applicazioni e i desktop. Assicurarsi che l'immagine master sia disponibile sull'host in cui vengono create le macchine. Se si utilizza MCS, non è necessario unire l'immagine master a un dominio. Le macchine di cui viene eseguito il provisioning vengono aggiunte al dominio specificato nella creazione guidata catalogo.
5. Citrix consiglia di creare e denominare una snapshot dell'immagine master in modo che possa essere identificata in un secondo momento. Se si specifica un'immagine master anziché una snapshot durante la creazione di un catalogo, l'interfaccia di gestione crea una snapshot, ma non è possibile assegnarle un nome.

### Attivazione dei contratti multilicenza

MCS supporta l'attivazione dei contratti multilicenza per automatizzare e gestire l'attivazione dei sistemi operativi Windows e di Microsoft Office. I tre modelli supportati da MCS per l'attivazione dei contratti multilicenza sono:

- Key Management Service (KMS)
- Attivazione basata su Active Directory (ADBA)
- Chiave di attivazione multipla (MAK)

È possibile modificare l'impostazione di attivazione dopo aver creato il catalogo delle macchine.

#### Key Management Service (KMS)

KMS è un servizio leggero che non richiede un sistema dedicato e può essere facilmente ospitato in cohosting su un sistema che fornisce altri servizi. Questa funzionalità è supportata in tutte le versioni di Windows supportate da Citrix. Durante la preparazione delle immagini, MCS esegue il ripristino di Microsoft Windows e Microsoft Office tramite KMS. È possibile saltare il ripristino eseguendo il comando `Set-Provserviceconfigurationdata`. Per ulteriori informazioni sul ripristino di Microsoft Windows e Microsoft Office tramite KMS durante la preparazione delle immagini, vedere MCS (Machine Creation Services): panoramica della preparazione delle immagini e rilevamento di problemi. Per ulteriori informazioni sull'attivazione di KMS, consultare Attivare tramite KMS (Key Management Service).

> **Nota:**
>
> Tutti i cataloghi delle macchine creati dopo l'esecuzione del comando `Set-Provserviceconfiguration` hanno le stesse impostazioni fornite nel comando.

#### Attivazione basata su Active Directory (ADBA)

ADBA consente di attivare le macchine tramite le relative connessioni di dominio. Le macchine vengono attivate immediatamente quando entrano a far parte del dominio. Queste macchine rimangono attivate finché rimangono unite al dominio e sono in contatto con il dominio stesso. Questa funzionalità è supportata in tutte le versioni di Windows supportate da Citrix, ad eccezione di Windows Server 2022. Per ulteriori informazioni sull'attivazione basata su Active Directory, vedere Attivazione basata su Active Directory.

#### Chiave di attivazione multipla (MAK)

MAK è un modo di attivare il volume e autenticare il sistema Windows con l'aiuto del server Microsoft. È necessario acquistare da Microsoft la chiave MAK, a cui è assegnato un numero fisso di conteggi

di attivazione. Ogni volta che viene attivato un sistema Windows, il numero di attivazioni si riduce. Esistono due modi per attivare il sistema:

- Attivazione online: se il sistema Windows che si desidera attivare dispone di accesso a Internet, il sistema attiva automaticamente Windows al momento dell'installazione del codice prodotto. Questo processo riduce il numero di attivazioni di 1 per il MAK corrispondente.
- Attivazione offline: se il sistema Windows non è in grado di connettersi a Internet per eseguire l'attivazione online, MCS riceve un ID di conferma e un ID di installazione dal server Microsoft per attivare il sistema Windows. Questa modalità di attivazione è utile per i cataloghi di macchine non persistenti.

**Requisiti chiave**

- Il Delivery Controller deve avere accesso a Internet.
- Creare un nuovo catalogo se la nuova immagine da aggiornare ha una chiave MAK diversa dall'originale.
- Installare la chiave MAK sull'immagine master. Per i passaggi per installare la chiave MAK su un sistema Windows, vedere Deploy MAK Activation.
- Se non si utilizza la preparazione delle immagini:

  1. Aggiungere il valore DWORD del registro `Manual` in`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
  2. Impostare il valore su 1.

**Conteggi delle attivazioni** Per visualizzare il numero di attivazioni rimanenti per la chiave MAK o per verificare se una macchina virtuale stia facendo uso di due o più attivazioni, utilizzare lo Strumento di gestione dell'attivazione dei contratti multilicenza (VAMT). Vedere Installare VAMT.

**Attivare il sistema Windows utilizzando MAK** Per attivare il sistema Windows utilizzando MAK:

1. Installare il codice prodotto sull'immagine principale. Questo passaggio richiede un conteggio delle attivazioni.
2. Creare un catalogo di macchine MCS.
3. Se non si utilizza la preparazione delle immagini:

   a) Aggiungere il valore DWORD del registro `Manual` in`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.

b) Impostare il valore su 1.

Questo metodo disabilita l'opzione di attivazione online.

4. Aggiungere macchine virtuali al catalogo delle macchine.
5. Accendere le macchine virtuali.
6. A seconda che si tratti di attivazione online o offline, il sistema Windows viene attivato o meno.

   - Se l'attivazione è online, il sistema Windows viene attivato dopo l'installazione del codice prodotto.
   - Se l'attivazione è offline, MCS comunica con le macchine virtuali fornite per ottenere lo stato di attivazione del sistema Windows. MCS recupera quindi un ID di conferma e un ID installato dal server Microsoft. Questi ID vengono utilizzati per attivare il sistema Windows.

**Risoluzione dei problemi** Se la VM di cui è stato eseguito il provisioning non viene attivata con la chiave MAK installata, eseguire il comando `Get-ProvVM` o `Get-ProvScheme` in una finestra di PowerShell.

- Il comando `Get-ProvScheme`: vedere il parametro `WindowsActivationType` associato al catalogo di macchine MCS dall'ultima immagine master.
- Il comando `Get-ProvVM`. Vedere i parametri `WindowsActivationType`, `WindowsActivationStat` , `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

È possibile controllare l'errore e verificare i passaggi per risolvere il problema.

### Iniziare a creare il catalogo

Prima di creare un catalogo:

- Consultare questa sezione per conoscere le scelte da fare e le informazioni da fornire.
- Assicurarsi di aver creato una connessione all'hypervisor, al servizio cloud o ad altre risorse che ospitano le macchine.
- Se è stata creata un'immagine master per eseguire il provisioning delle macchine, assicurarsi di aver installato un VDA su tale immagine.

Per avviare la procedura guidata di creazione del catalogo:

1. Accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Selezionare **Manage** (Gestisci).

3. Se questo è il primo catalogo creato, si viene guidati alla selezione corretta (ad esempio "Set up the machines and create machine catalogs to run apps and desktops"[Configura le macchine e crea cataloghi delle macchine per eseguire app e desktop]). Si apre la procedura guidata di creazione del catalogo.
4. Se è già stato creato un catalogo e si desidera crearne un altro, attenersi alla seguente procedura:

    a) Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.

    b) Per organizzare i cataloghi utilizzando le cartelle, creare cartelle nella cartella **Machine Catalogs** (Cataloghi delle macchine) predefinita. Per ulteriori informazioni, consultare Creare una cartella del catalogo.

    c) Selezionare la cartella in cui si desidera creare il catalogo, quindi fare clic su **Create Machine Catalog** (Crea catalogo delle macchine). Si apre la procedura guidata di creazione del catalogo.

La procedura guidata comprende le pagine descritte nella sezione seguente. Le pagine visualizzate potrebbero differire a seconda delle selezioni effettuate e della connessione (a un host) utilizzata. Hosts/virtualization resources (Host/risorse di virtualizzazione) elenca le origini delle informazioni per i tipi di host supportati.

### Sistema operativo

Ciascun catalogo contiene macchine di un solo tipo:

- **Multi-session OS** (Sistema operativo multisessione): un catalogo con sistema operativo multisessione fornisce desktop condivisi ospitati. Le macchine possono eseguire versioni supportate dei sistemi operativi Windows o Linux, ma il catalogo non può contenere entrambi i sistemi operativi
- **Single-session OS** (Sistema operativo a sessione singola): un catalogo con sistemi operativi a sessione singola fornisce desktop VDI che è possibile assegnare a vari utenti diversi.
- **Remote PC Access:** un catalogo Accesso remoto PC consente agli utenti di accedere in remoto ai computer desktop dell'ufficio fisico. Accesso remoto PC non richiede una VPN per garantire la sicurezza.

### Gestione macchine

Questa pagina non viene visualizzata quando si crea un catalogo di Remote PC Access (Accesso remoto PC).

La pagina **Machine Management** (Gestione macchine) indica la modalità di gestione delle macchine e lo strumento utilizzato per distribuirle.

Scegliere se l'alimentazione delle macchine del catalogo verrà gestita tramite l'interfaccia Full Configuration (Configurazione completa).

- Le macchine vengono gestite a livello di alimentazione tramite l'interfaccia Full Configuration (Configurazione completa) o ne viene eseguito il provisioning tramite un ambiente cloud, ad esempio macchine virtuali o PC blade. Questa opzione è disponibile solo se è già stata configurata una connessione a un hypervisor o a un servizio cloud.
- Le macchine non hanno l'alimentazione non gestita tramite l'interfaccia Full Configuration (Configurazione completa), ad esempio le macchine fisiche.

Se si è indicato che le macchine sono gestite a livello di alimentazione tramite l'interfaccia Full Configuration (Configurazione completa) o se ne viene eseguito il provisioning tramite un ambiente cloud, scegliere lo strumento da utilizzare per creare le macchine virtuali.

- **Citrix Machine Creation Services (MCS):** utilizza un'immagine master per creare e gestire macchine virtuali. I cataloghi delle macchine negli ambienti cloud utilizzano MCS. MCS non è disponibile per le macchine fisiche.
- **Other (Altro):** uno strumento che gestisce le macchine che è già presente nel data center. Citrix consiglia di utilizzare Microsoft System Center Configuration Manager o un'altra applicazione di terze parti per garantire che le macchine nel catalogo siano coerenti.

### Tipi di desktop (esperienza desktop)

Questa pagina viene visualizzata quando si crea un catalogo contenente macchine con sistema operativo a sessione singola o multisessione.

- Per le macchine con sistema operativo a sessione singola:

  Nella pagina **Desktop Experience** (Esperienza desktop), è possibile determinare cosa succede ogni volta che gli utenti eseguono l'accesso e si scollegano. Selezionare una delle seguenti opzioni:

  - Agli utenti viene assegnato un nuovo desktop (casuale) ogni volta che eseguono l'accesso.
  - Agli utenti viene assegnato lo stesso desktop (statico) ogni volta che eseguono l'accesso. È inoltre possibile decidere se le modifiche apportate dagli utenti verranno salvate o eliminate dopo che si scollegano.

- Per le macchine con sistema operativo multisessione:

  Agli utenti viene assegnato un desktop casuale ogni volta che eseguono l'accesso. Nella pagina Desktop Experience, è possibile determinare cosa succede ogni volta che si scollegano. Selezionare una delle seguenti opzioni:

- Le modifiche apportate dagli utenti al desktop verranno salvate (persistenti).
- Le modifiche apportate dagli utenti al desktop verranno ignorate (non persistenti).

> **Nota:**
>
> Nel caso delle macchine multisessione persistenti, le modifiche apportate dagli utenti ai desktop verranno salvate e saranno accessibili a tutti gli utenti autorizzati.

### Immagine master

Questa pagina viene visualizzata solo quando si utilizza MCS per effettuare il provisioning delle macchine virtuali. Seguire questi passaggi per completare le impostazioni:

1. Selezionare la snapshot o la macchina virtuale creata in precedenza come immagine principale. Se necessario, è possibile aggiungere una nota per l'immagine selezionata.

   > **Nota:**
   >
   > - Quando si utilizza MCS, non eseguire Sysprep sulle immagini master.
   > - Se si specifica un'immagine master anziché una snapshot, l'interfaccia di gestione crea una snapshot, ma non è possibile assegnarle un nome.
   > - Viene visualizzato un messaggio di errore se si seleziona un'istantanea o una macchina virtuale non compatibile con la tecnologia di gestione computer selezionata in precedenza nella procedura guidata.
   > - Per aggiornare le immagini all'interno di un nodo immagine, selezionalo nell'albero, quindi fai clic sull'opzione **Refresh** (Aggiorna) nell'angolo in alto a destra. Se non si seleziona alcun nodo immagine, facendo clic su **Refresh** vengono aggiornate tutte le immagini dell'albero. Per cancellare un nodo selezionato nell'albero, tenere premuto **CTRL** e fare clic sul nodo.

2. Per utilizzare una macchina virtuale esistente come profilo macchina, selezionare **Use a machine profile** (Usa un profilo macchina), quindi selezionare la macchina virtuale.

   > **Nota:**
   >
   > Attualmente, l'uso dei profili macchina è limitato alle macchine virtuali Azure, AWS e GCP.

3. Selezionare il livello funzionale minimo per il catalogo. Per abilitare l'uso delle funzionalità più recenti del prodotto, verificare che nell'immagine master sia installata la versione più recente del VDA.

### Piattaforme cloud e ambienti di servizio

Quando si utilizza un servizio cloud o una piattaforma per ospitare macchine virtuali, la procedura guidata per la creazione del catalogo potrebbe contenere pagine aggiuntive specifiche per tale host. Ad esempio, quando si utilizza un'immagine master di Azure Resource Manager, la procedura guidata per la creazione del catalogo contiene una pagina **Storage and License Types**(Archiviazione e tipi di licenza).

Per informazioni specifiche sull'host, seguire il collegamento appropriato elencato in Iniziare a creare il catalogo.

### Macchine

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso remoto PC.

Il titolo di questa pagina dipende da ciò che è stato selezionato nella pagina **Machine Management** (Gestione delle macchine): **Machines** (Macchine), **Virtual Machines** (Macchine virtuali) o **Machines and Users** (Macchine e utenti).

> **Nota:**
>
> È possibile creare un catalogo vuoto, ossia un catalogo che non contiene macchine.

- **Quando si utilizza MCS per creare macchine:**
  - Specificare quante macchine virtuali creare. Immettete **0** (zero) se non si desidera crearne. Successivamente, per creare macchine virtuali per un catalogo vuoto, è possibile eseguire il comando **Add machines** (Aggiungi macchine).
  - Scegliere la quantità di memoria (in MB) a disposizione di ciascuna macchina virtuale.
  - **Importante:** ogni macchina virtuale creata dispone di un disco rigido. Le dimensioni sono impostate nell'immagine master; non è possibile modificare le dimensioni del disco rigido nel catalogo.
  - Se nella pagina **Desktop Experience** (Esperienza desktop) è stato indicato che le modifiche dell'utente ai desktop statici devono essere salvate in un vDisk personale separato, specificare le dimensioni del disco virtuale in GB e la lettera dell'unità.
  - Se la distribuzione utilizza più di una zona (posizione risorsa), è possibile selezionare una zona per il catalogo.
  - Se si creano macchine virtuali desktop statiche, selezionare una modalità di copia della macchina virtuale. Vedere Modalità di copia della macchina virtuale.
  - Se si creano macchine virtuali desktop casuali non persistenti, è possibile abilitare e configurare la cache di write-back per i dati temporanei sulle macchine per migliorare le prestazioni di I/O. Per maggiori informazioni, consultare Configurare la cache per i dati temporanei.

- **Quando si utilizzano altri strumenti per fornire macchine:**

  Aggiungere (o importare un elenco di) nomi di account delle macchine. È possibile modificare il nome dell'account per una macchina virtuale dopo averla aggiunta o importata. Se nella pagina **Desktop Experience** (Esperienza desktop) sono state specificate macchine statiche, è possibile specificare facoltativamente il nome utente per ogni macchina virtuale aggiunta.

  > **Suggerimento:**
  >
  > Per aggiungere utenti, è possibile selezionarli o immettere manualmente un elenco di nomi utente separato da punti e virgole. Se gli utenti si trovano in Active Directory, immettere direttamente i nomi. In caso contrario, inserire i nomi in questo formato: `<identity provider>:<user name>`. Esempio: `AzureAD:username`.

  Dopo aver aggiunto o importato i nomi, è possibile utilizzare il pulsante **Remove** (Rimuovi) per eliminare i nomi dall'elenco, mentre ci si trova ancora nella pagina della procedura guidata.

- **Quando si utilizzano altri strumenti (ad eccezione di MCS):**

  Un'icona e una descrizione comando per ogni macchina aggiunta (o importata) aiutano a identificare le macchine che potrebbero non essere idonee a essere aggiunte al catalogo o non essere in grado di registrarsi con un Cloud Connector.

#### Aggiungere i SID durante la creazione di macchine virtuali

È ora possibile aggiungere il parametro `ADAccountSid` per identificare in modo univoco le macchine durante la creazione di nuove macchine virtuali.

A questo scopo:

1. Creare un catalogo con il tipo di identità supportato.
2. Aggiungere macchine al catalogo utilizzando `NewProvVM`. Ad esempio:

```
1 New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
      )  -RunAsynchronously
2 <!--NeedCopy-->
```

Tuttavia, non è possibile effettuare il provisioning di una macchina con:

- Un account AD che non fa parte del pool di identità del catalogo
- Un account AD che non è in stato disponibile

#### Modalità di copia della macchina virtuale

La modalità di copia specificata nella pagina **Machines** determina se MCS crea duplicati sottili (copia rapida) o spessi (copia completa) dall'immagine master. (Impostazione predefinita= cloni sottili)

- Usa duplicati a copia veloce per un utilizzo più efficiente dell'archiviazione e una creazione più rapida della macchina.
- Utilizzare duplicati a copia completa per migliorare il supporto del ripristino e della migrazione dei dati, con IOPS potenzialmente ridotti dopo la creazione delle macchine.

### Configurare la cache per i dati temporanei

Quando si utilizza MCS per gestire le macchine casuali non persistenti di un catalogo, è possibile abilitare la cache di write-back perché le macchine abbiano migliori prestazioni di I/O.

La cache di write-back viene denominata MCSIO. Per ulteriori informazioni, vedere questo articolo del blog.

**Prerequisiti** Per abilitare la cache di write-back, il catalogo deve soddisfare questi requisiti:

- Utilizzare una connessione in cui specificata l'archiviazione per i dati temporanei. Per ulteriori informazioni, vedere Connessioni e risorse.
- I VDA devono essere almeno di versione 7.9 e installati con un driver MCSIO corrente.

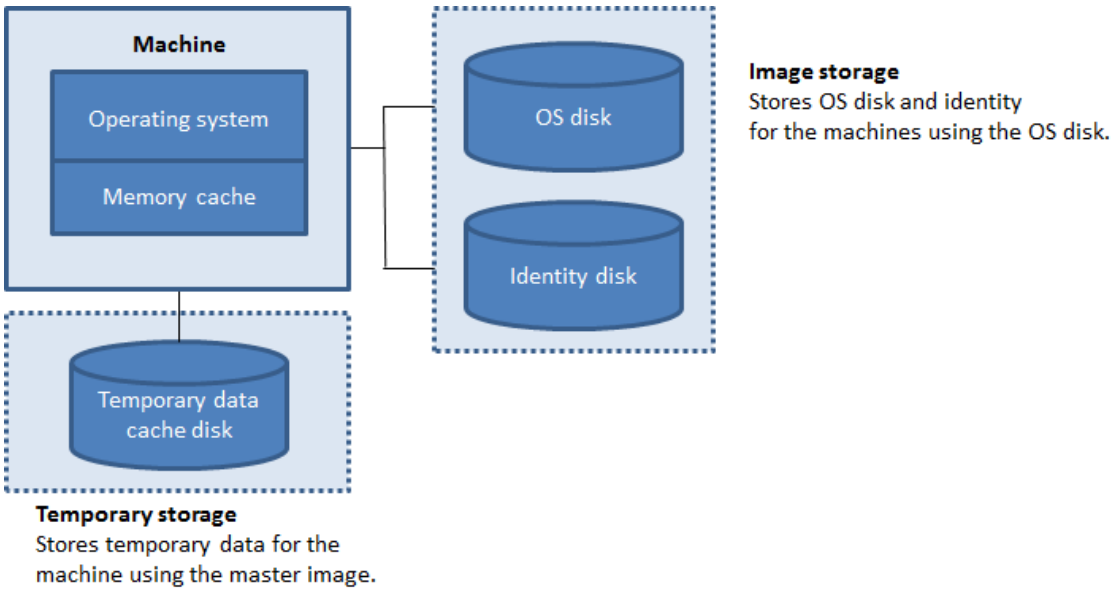
  > **Nota:**
  >
  > L'installazione di questo driver è un'opzione disponibile quando si installa o si aggiorna un VDA. Per impostazione predefinita, tale driver non è installato.

- Per abilitare l'assegnazione delle lettere di unità alle cache su disco, le macchine virtuali devono soddisfare i seguenti requisiti aggiuntivi:
  - Sistema operativo: Windows
  - Versione VDA: 2305 o successiva

### Considerazioni

- Le cache di write-back sono disponibili nella cache della *memoria* e nella cache del *disco*. Per impostazione predefinita, i valori predefiniti variano a seconda del tipo di connessione. Generalmente, i valori predefiniti sono sufficienti per la maggior parte dei casi; tuttavia, tenere conto dello spazio necessario per:
  - File di dati temporanei creati da Windows stesso, incluso il file di paging di Windows.
  - Dati del profilo utente.
  - Dati ShareFile sincronizzati con le sessioni degli utenti.
  - Dati che potrebbero essere creati o copiati da un utente di sessione o da qualsiasi applicazione che gli utenti potrebbero installare all'interno della sessione.




- Se si attiva la casella di controllo **Memory cache size (MB) (recommended)** [Dimensione della cache di memoria (MB) (scelta consigliata)], i dati temporanei vengono inizialmente scritti nella cache di memoria. Quando la cache di memoria raggiunge il limite configurato, i dati meno recenti vengono spostati sul disco temporaneo della cache dei dati.
- La cache di memoria fa parte della quantità totale di memoria disponibile su ogni computer. Pertanto, se si abilita la casella di controllo **Memory cache size (MB) (recommended)** [Dimensione della cache di memoria (MB) (scelta consigliata)], è consigliabile aumentare la quantità totale di memoria su ogni macchina.
- Se si mantiene deselezionata la casella di controllo **Memory cache size (MB) (recommended)**, i dati temporanei vengono scritti direttamente nella cache del disco, utilizzando una quantità minima di memoria.
- La modifica dell'opzione **Disk cache size (GB)** [Dimensione della cache del disco (GB)] rispetto al valore predefinito può influire sulle prestazioni. La dimensione deve corrispondere ai requisiti dell'utente e al carico posto sulla macchina.

> **Importante:**
>
> Se la cache del disco esaurisce lo spazio, la sessione dell'utente diventa inutilizzabile.

Se si deseleziona la casella di controllo **Disk cache size** (Dimensioni della cache del disco), non viene creato alcun disco della cache. In questo caso, specificare un valore per l'opzione **Memory allocated to cache** (Memoria allocata alla cache) sufficientemente grande da contenere tutti i dati temporanei. Ciò è possibile solo se sono disponibili grandi quantità di RAM per l'allocazione a ciascuna macchina virtuale.

Se si deselezionano entrambe le caselle di controllo, i dati temporanei non vengono memorizzati nella

cache. Vengono scritti sul disco di differenza (situato nella posizione di archiviazione del sistema operativo) per ciascuna macchina virtuale (questa è l'azione di provisioning nelle versioni precedenti alla 7.9).

Non abilitare la memorizzazione nella cache se si intende utilizzare questo catalogo per creare AppDisk.

Non è possibile modificare i valori della cache in un catalogo delle macchine dopo averlo creato.

#### Utilizzo di file CSV per aggiungere macchine in blocco

Se si utilizza l'interfaccia di gestione **Full Configuration** (Configurazione completa), è possibile aggiungere macchine in blocco utilizzando file CSV. La funzionalità è disponibile per tutti i cataloghi ad eccezione dei cataloghi creati tramite MCS.

Di seguito è riportato un flusso di lavoro generale per utilizzare file CSV per aggiungere macchine in blocco:

1. Nella pagina **Machines** (Macchine), selezionare **Add CSV File** (Aggiungi file CSV). Viene visualizzata la finestra **Add Machines in Bulk** (Aggiungi macchine in blocco).
2. Selezionare **Download CSV Template** (Scarica modello CSV).
3. Compilare il file del modello.
4. Trascinare o sfogliare il file per caricarlo.
5. Selezionare **Validate** (Convalida) per eseguire controlli di convalida sull'importazione.
6. Selezionare **Import** (Importa) per completare l'operazione.

Per informazioni sulle considerazioni relative ai file CSV, vedere Considerazioni sull'utilizzo di file CSV per aggiungere macchine.

È inoltre possibile esportare macchine da un catalogo nella stessa pagina Machines (Macchine). Il file CSV esportato delle macchine può quindi essere utilizzato come modello quando si aggiungono macchine in blocco. Per esportare macchine:

1. Nella pagina **Machines** (Macchine), selezionare **Export to CSV file** (Esporta in un file CSV). Viene scaricato un file CSV contenente un elenco delle macchine.
2. Aprire il file CSV per aggiungere o modificare le macchine secondo necessità. Per aggiungere macchine in blocco utilizzando il file CSV salvato, vedere la sezione precedente, Utilizzo di file CSV per aggiungere macchine in blocco.

> **Nota:**
>
> - Questa funzionalità non è disponibile per i cataloghi Remote PC Access (Accesso remoto

> PC).
>
> - L'esportazione e l'importazione di macchine in file CSV sono supportate solo tra cataloghi dello stesso tipo.

### NIC

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso remoto PC.

Se si prevede di utilizzare più NIC, associare una rete virtuale a ciascuna scheda. Ad esempio, è possibile assegnare una scheda per accedere a una rete protetta specifica e un'altra scheda per accedere a una rete utilizzata più comunemente. È inoltre possibile aggiungere o rimuovere schede di interfaccia di rete da questa pagina.

### Account macchina

Questa pagina viene visualizzata solo quando si creano cataloghi di Accesso remoto PC.

Specificare gli account delle macchine di Active Directory o le unità organizzative (OU) da aggiungere che corrispondono a utenti o gruppi di utenti. Non utilizzare una barra (/) in un nome di unità organizzativa.

È possibile scegliere una connessione con gestione dell'alimentazione configurata in precedenza o scegliere di non utilizzare la gestione dell'alimentazione. Se si desidera utilizzare la gestione dell'alimentazione, ma non è stata ancora configurata una connessione adeguata, è possibile crearla in un secondo momento e quindi modificare il catalogo delle macchine per aggiornare le impostazioni di gestione dell'alimentazione.

È possibile aggiungere macchine in blocco utilizzando file CSV. Un flusso di lavoro generale per procedere in questo modo è il seguente:

1. Nella pagina **Machine Accounts** (Account macchine), selezionare **Add CSV File** (Aggiungi file CSV). Viene visualizzata la finestra **Add Machines in Bulk** (Aggiungi macchine in blocco).
2. Selezionare **Download CSV Template** (Scarica modello CSV).
3. Compilare il file del modello.
4. Trascinare o sfogliare il file per caricarlo.
5. Selezionare **Validate** (Convalida) per eseguire controlli di convalida sull'importazione.
6. Selezionare **Import** (Importa) per completare l'operazione.

Per informazioni sulle considerazioni relative ai file CSV, vedere Considerazioni sull'utilizzo di file CSV per aggiungere macchine.

### Identità macchina

Questa pagina viene visualizzata solo quando si utilizza MCS per creare macchine virtuali.

Ogni macchina del catalogo deve avere un'identità unica. Questa pagina consente di configurare le identità per le macchine del catalogo. Le macchine vengono unite all'identità dopo il provisioning. Non è possibile modificare il tipo di identità dopo aver creato il catalogo.

Di seguito è riportato un flusso di lavoro generale per configurare le impostazioni in questa pagina:

1. Selezionare un'identità dall'elenco.
2. Indicare se creare account o utilizzare quelli esistenti e la posizione (dominio) per tali account.

È possibile selezionare una delle seguenti opzioni:

- **On-premises Active Directory** (Active Directory locale). Macchine di proprietà di un'organizzazione e che hanno effettuato l'accesso con un account Active Directory appartenente a tale organizzazione. Esistono in locale.

  > **Nota:**
  >
  > Per impostazione predefinita, viene selezionato il dominio in cui risiede la risorsa (connessione).

- **Azure Active Directory joined** (Macchine aggiunte ad Azure Active Directory). Macchine di proprietà di un'organizzazione e che hanno effettuato l'accesso con un account Azure Active Directory appartenente a tale organizzazione. Esistono solo nel cloud. Per informazioni su requisiti, limitazioni e considerazioni, vedere Macchine aggiunte ad Azure Active Directory.

  > **Nota:**
  >
  > Questa opzione richiede che l'immagine master soddisfi i prerequisiti del sistema operativo. Per ulteriori informazioni, vedere la documentazione Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join.

- **Unito ad Azure Active Directory ibrido**. Macchine di proprietà di un'organizzazione che hanno effettuato l'accesso con un account Active Directory Domain Services appartenente a tale organizzazione. Esistono nel cloud e on-premise. Per informazioni su requisiti, limitazioni e considerazioni, vedere Macchine aggiunte ad Azure Active Directory ibrido.

  > **Nota:**
  >
  > - Prima di poter utilizzare macchine aggiunte ad Azure Active Directory ibrido, assicurarsi che l'ambiente Azure soddisfi i prerequisiti. Vedere https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains.
  > - Questa opzione richiede che l'immagine master soddisfi i prerequisiti del sistema op-

> erativo. Per ulteriori informazioni, vedere la documentazione Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid.

- **Non-domain-joined** (Non aggiunte al dominio). Macchine non aggiunte a nessun dominio. Per informazioni sui requisiti e le limitazioni, consultare Macchine non aggiunte a un dominio.

> **Importante:**
>
> - Se si seleziona **On-premises Active Directory** (Active Directory on-premise) o **Hybrid Azure Active Directory joined** (Macchine aggiunte ad Azure Active Directory ibrido) come tipo di identità, ogni macchina del catalogo deve disporre di un account computer Active Directory corrispondente.
> - Il tipo di identità **Non-domain-joined** (Non aggiunte al dominio) richiede la versione 1811 o successiva del VDA come livello di funzionalità minimo per il catalogo. Per renderla disponibile, aggiornare il livello funzionale minimo.
> - I tipi di identità **Azure Active Directory joined** (Macchine aggiunte ad Azure Active Directory) e **Hybrid Azure Active Directory joined** (Macchine ibride aggiunte ad Azure Active Directory) richiedono la versione 2203 o successiva del VDA come livello funzionale minimo per il catalogo. Per renderli disponibili, aggiornare il livello funzionale minimo.

Prima di creare account, assicurarsi di avere l'autorizzazione per creare account computer nell'unità organizzativa in cui risiedono i computer. Ogni macchina del catalogo deve avere un nome univoco. Specificate come si desidera creare le identità delle macchine:

- Specificare l'unità organizzativa e lo schema di denominazione della macchina. Per ulteriori informazioni, vedere Schema di denominazione degli account delle macchine. Quando si crea un catalogo, viene creato automaticamente un pool di identità per contenere tutte le identità delle macchine definite per questo catalogo.
- Scegliere un pool di identità esistente nel proprio ambiente.

> **Nota:**
>
> Assicurarsi che i nomi delle unità organizzative non utilizzino barre (/).

Se si utilizzano account esistenti, selezionare gli account oppure fare clic su **Import** (Importa) e specificare un file .csv contenente i nomi degli account. Il contenuto del file importato deve essere nel formato seguente:

- [ADComputerAccount] ADcomputeraccountname.domain

Assicurarsi che ci siano account sufficienti per tutte le macchine che si stanno aggiungendo. L'interfaccia Full Configuration (Configurazione completa) gestisce questi account. Pertanto, consentire all'interfaccia di reimpostare le password per tutti gli account o specificare la password dell'account, che deve essere la stessa per tutti gli account.

Per i cataloghi contenenti macchine fisiche o esistenti, selezionare o importare account esistenti e assegnare ciascuna macchina sia a un account computer Active Directory che a un account utente.

#### Schema di denominazione degli account delle macchine

Ogni macchina in un catalogo deve avere un nome univoco. È necessario specificare uno schema di denominazione degli account delle macchine quando si crea un catalogo. Utilizzare caratteri jolly (cancelletti) come segnaposto per numeri o lettere sequenziali che appaiono nel nome.

Quando si specifica uno schema di denominazione, tenere presente le seguenti regole:

- Lo schema di denominazione deve contenere almeno un carattere jolly. È necessario mettere insieme tutti i caratteri jolly.
- L'intero nome, compresi i caratteri jolly, deve contenere almeno 2 ma non più di 15 caratteri. Deve includere almeno un carattere non numerico e un carattere # (carattere jolly).
- Il nome non deve includere spazi o uno dei seguenti caratteri: `,~!@'$%^&.()} { \/*?"<>|=+[];:_".`.
- Il nome non può terminare con un trattino (-).

Inoltre, lasciare spazio sufficiente per l'espansione quando si specifica lo schema di denominazione. Si consideri questo esempio: se si creano 1.000 account macchina con lo schema «veryverylong#», l'ultimo nome account creato (veryverylong1000) contiene 16 caratteri. Pertanto, lo schema di denominazione comporterà uno o più nomi di macchine che superano il massimo di 15 caratteri.

È possibile indicare se i valori sequenziali sono numeri (0-9) o lettere (A-Z):

- **0-9**. Se l'opzione è selezionata, i caratteri jolly specificati vengono risolti in numeri sequenziali.

  > **Nota:**
  >
  > Se è presente un solo carattere jolly (#), i nomi degli account iniziano con 1. Se ce ne sono due, i nomi degli account iniziano con 01. Se ce ne sono tre, i nomi degli account iniziano con 001 e così via.

- **A-Z**. Se l'opzione è selezionata, i caratteri jolly specificati vengono risolti in lettere sequenziali.

Ad esempio, uno schema di denominazione PC-Sales-## (in cui l'opzione **0-9** è selezionata) genera account denominati PC-Sales-01, PC-Sales-02, PC-Sales-03 e così via.

Facoltativamente, è possibile specificare con cosa iniziano i nomi degli account.

- Se si seleziona **0-9**, gli account vengono denominati in sequenza, a partire dai numeri specificati. Immettere una o più cifre, a seconda del numero di caratteri jolly utilizzati nel campo precedente. Ad esempio, se si utilizzano due caratteri jolly, immettere due o più cifre.

- Se si seleziona **A-Z**, gli account vengono denominati in sequenza, a partire dalle lettere specificate. Immettere una o più lettere, a seconda del numero di caratteri jolly utilizzati nel campo precedente. Ad esempio, se si utilizzano due caratteri jolly, immettere due o più lettere.

### Credenziali di dominio

Selezionare **Enter credentials** (Immetti credenziali) e immettere le credenziali di un amministratore con l'autorizzazione a eseguire operazioni sull'account nel dominio Active Directory di destinazione.

Utilizzare l'opzione **Check name** (Controlla nome) per verificare se il nome utente è valido o univoco. L'opzione è utile, ad esempio, quando:

- Lo stesso nome utente esiste in più domini. Viene richiesto di selezionare l'utente desiderato.
- Non si ricorda il nome del dominio. È possibile immettere il nome utente senza specificare il nome del dominio. Se il controllo viene superato, il nome del dominio viene popolato automaticamente.

> **Nota:**
>
> Se il tipo di identità selezionato in **Machine Identities** (Identità macchine) è **Hybrid Azure Active Directory joined** (Macchine aggiunte ad Azure Active Directory ibrido), le credenziali immesse devono aver ottenuto l'autorizzazione `Write userCertificate`.

### Workspace Environment Management (opzionale)

Questa pagina viene visualizzata solo quando si utilizza l'edizione Advanced o Premium di Citrix DaaS.

Selezionare un set di configurazione WEM (Workspace Environment Management) a cui si desidera associare il catalogo. Un set di configurazione è un contenitore logico utilizzato per organizzare un set di configurazioni WEM. L'associazione di un catalogo a un set di configurazione consente di utilizzare WEM per offrire agli utenti la migliore esperienza Workspace possibile.

> **Importante:**
>
> - Prima di poter associare un catalogo a un set di configurazione, è necessario configurare la distribuzione del servizio WEM. Accedere a Citrix Cloud e quindi avviare il servizio WEM. Per ulteriori informazioni, vedere Introduzione al servizio Workspace Environment Management.
> - Se si utilizza già WEM, le macchine del catalogo di cui si sta per eseguire il provisioning potrebbero essere già presenti in un set di configurazione, ad esempio tramite Active Directory. In tal caso, si consiglia di utilizzare Active Directory in modo coerente per eseguire la

> configurazione e saltare questa configurazione.

Se il set di configurazione selezionato non contiene impostazioni relative alla configurazione di base di WEM, viene visualizzata la seguente opzione:

- **Apply basic settings to configuration set** (Applica le impostazioni di base al set di configurazione). L'opzione consente di iniziare rapidamente a usare WEM applicando le impostazioni di base al set di configurazione. Le impostazioni di base includono la protezione dai picchi della CPU, la prevenzione automatica dei picchi della CPU e l'ottimizzazione intelligente della CPU. Per visualizzare le impostazioni di base, fare clic sul collegamento *qui*. Per modificarle, utilizzare la console WEM.

### Aggiornamento VDA (opzionale)

> **Importante:**
>
> - Per garantire un aggiornamento senza problemi, assicurarsi di soddisfare i prerequisiti ed esaminare i problemi noti prima di aggiornare i VDA alle versioni CR o LTSR CU. Vedere Aggiornare i VDA utilizzando l'interfaccia Full Configuration.
> - Quando si aggiornano i VDA LTSR alle versioni LTSR CU (Cumulative Update), assicurarsi che la versione dei VDA Upgrade Agent in esecuzione sui VDA sia la 7.36.0.7 o una versione successiva. Per ulteriori informazioni, vedere Upgrade VDAs using the Full Configuration interface.

Questa funzionalità si applica ai seguenti tipi di macchine:

- Macchine persistenti di cui è stato eseguito il provisioning con MCS. È possibile distribuirle utilizzando **Citrix Machine Creation Services** nella pagina **Machine Management** (Gestione macchine) durante la creazione del catalogo.
- Macchine che non vengono create utilizzando MCS (ad esempio, macchine fisiche). È possibile distribuirle utilizzando **Other service or technology** (Altro servizio o tecnologia) nella pagina **Machine Management** (Gestione macchine) durante la creazione del catalogo.

Per ulteriori informazioni sulle due opzioni, vedere Gestione delle macchine.

Nella pagina **VDA Upgrade** (Aggiornamento VDA), selezionare la versione del VDA a cui eseguire l'aggiornamento. Se specificato, i VDA nel catalogo in cui è installato l'agente di aggiornamento dei VDA possono eseguire l'aggiornamento alla versione selezionata, immediatamente o a un'ora pianificata.

> **Nota:**
>
> - Questa funzione supporta solo l'aggiornamento alla versione più recente di VDA. Il momento in cui si crea una pianificazione di aggiornamento VDA o si aggiorna un VDA deter-

> mina la versione più recente del VDA.
> - Dopo aver configurato le impostazioni di aggiornamento VDA, potrebbero essere necessari fino a 15 minuti prima che il campo **VDA Upgrade** (Aggiornamento VDA) rifletta lo stato più recente. Per visualizzare la colonna **VDA Upgrade** (Aggiornamento VDA), fare clic sull'icona Columns to display (Colonne da visualizzare) nell'angolo in alto a destra, selezionare **Machine Catalog > VDA Upgrade** (Catalogo delle macchine > Aggiornamento VDA) e fare clic su **Save** (Salva).

Scegliere una traccia VDA adatta alla propria distribuzione:

> **Importante:**
>
> È possibile passare dal VDA CR al VDA LTSR purché si passi da una versione precedente a una versione successiva. Non è possibile passare da una versione successiva a una versione precedente perché questo è considerato un downgrade. Ad esempio, non è possibile effettuare il downgrade da 2212 CR a 2203 LTSR (qualsiasi CU), ma è possibile eseguire l'upgrade da 2112 CR a 2203 LTSR (qualsiasi CU).

- **Latest CR VDA** (VDA - CR più recenti). Le versioni correnti (CR) offrono le funzionalità di virtualizzazione di app, desktop e server più recenti e innovative.
- **Latest LTSR VDA** (VDA - LTSR più recenti). Le LTSR (Long Term Service Release) sono ideali per ambienti di produzione aziendali di grandi dimensioni che preferiscono mantenere la stessa versione di base per un periodo prolungato.

Dopo la creazione del catalogo, è possibile aggiornare i VDA in base alle esigenze. Per ulteriori informazioni, vedere Aggiornare i VDA.

Se si desidera abilitare l'aggiornamento dei VDA in un secondo momento, è possibile tornare a questa pagina modificando il catalogo dopo la creazione del catalogo. Per ulteriori informazioni, consultare Configurare le impostazioni di aggiornamento dei VDA modificando un catalogo.

### Riepilogo, nome e descrizione

Nella pagina **Summary** controllare le impostazioni specificate. Immettere un nome e una descrizione per il catalogo. Queste informazioni vengono visualizzate nell'interfaccia di gestione Full Configuration (Configurazione completa).

Al termine, selezionare **Finish** (Fine) per avviare la creazione del catalogo.

In **Machine Catalogs** (Cataloghi delle macchine), il nuovo catalogo viene visualizzato con una barra di avanzamento in linea.

Per visualizzare i dettagli dell'avanzamento della creazione:

1. Passare il mouse sul catalogo delle macchine.

2. Nella descrizione comando visualizzata, fare clic su **View details** (Visualizza dettagli).

   Viene visualizzato un grafico di avanzamento dettagliato in cui è possibile visualizzare quanto segue:

   - Cronologia dei passaggi
   - Avanzamento e tempo di esecuzione del passaggio corrente
   - Passaggi rimanenti

### Considerazione importante sull'impostazione di proprietà personalizzate

Le proprietà personalizzate devono essere impostate correttamente su `New-ProvScheme` e `Set-ProvScheme` negli ambienti GCP e Azure. Se si specificano proprietà o proprietà personalizzate non esistenti, viene visualizzato il seguente messaggio di errore e i comandi non vengono eseguiti.

```
Invalid property found: <invalid property>. Ensure that the CustomProperties
 parameter supports the property.
```

### Considerazione importante sull'impostazione dei parametri ProvScheme

Quando si utilizza MCS per creare un catalogo, viene visualizzato un messaggio di errore se:

- Si impostano i seguenti parametri `New-ProvScheme` negli hypervisor non supportati quando si crea un catalogo delle macchine:

| Parametro | Hypervisor supportato |
|---|---|
| `UseWriteBackCache` | VMware |
| | Hyper-V |
| | Citrix Hypervisor |
| | Azure |
| | GCP |
| `DedicatedTenancy` | Azure |
| | GCP |
| | AWS |
| `TenancyType` | Azure |
| | GCP |
| | AWS |

| Parametro | Hypervisor supportato |
| --- | --- |
| `UseFullDiskCloneProvisioning` | VMware<br>Hyper-V<br>Citrix Hypervisor |

- Si aggiornano i seguenti parametri `Set-ProvScheme` dopo aver creato il catalogo delle macchine:
  - `CleanOnBoot`
  - `UseWriteBackCache`
  - `DedicatedTenancy`
  - `TenancyType`
  - `UseFullDiskCloneProvisioning`

### Passaggi successivi

Per informazioni sulla creazione di cataloghi di hypervisor specifici, vedere:

- Creare un catalogo di AWS
- Creare un catalogo di Citrix Hypervisor
- Creare un catalogo di Google Cloud Platform
- Creare un catalogo di Microsoft Azure
- Creare un catalogo di Microsoft System Center Virtual Machine Manager
- Creare un catalogo di Nutanix
- Creare un catalogo di VMware

Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.

Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.

### Ulteriori informazioni

- Gestione delle immagini di Citrix Virtual Apps and Desktops
- Connessioni e risorse
- Creare cataloghi aggiunti a identità di macchine
- Gestire i cataloghi delle macchine

# Creare un catalogo di AWS

December 18, 2023

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le informazioni che seguono riguardano i dettagli specifici degli ambienti di virtualizzazione AWS.

> **Nota:**
>
> Prima di creare un catalogo di AWS, è necessario completare la creazione di una connessione ad AWS. Vedere Connessione ad AWS.

## Impostazioni di rete durante la preparazione dell'immagine

Durante la preparazione dell'immagine, viene creata una macchina virtuale (VM) di preparazione basata sulla macchina virtuale originale. Questa macchina virtuale di preparazione è disconnessa dalla rete. Per disconnettere la rete dalla macchina virtuale di preparazione, viene creato un gruppo di sicurezza di rete per negare tutto il traffico in entrata e in uscita. Questo gruppo di sicurezza di rete persiste e viene riutilizzato. Il nome del gruppo di sicurezza di rete è `Citrix.XenDesktop.IsolationGroup-GUID`, dove il GUID viene generato casualmente.

## Tenancy di AWS

AWS offre le seguenti opzioni di tenancy: tenancy condivisa (il tipo predefinito) e tenancy dedicata. "Tenacy condivisa"significa che più istanze di Amazon EC2 di clienti diversi potrebbero risiedere sullo stesso componente hardware fisico. "Tenancy dedicata"significa che le istanze di EC2 vengono eseguite solo su hardware con altre istanze distribuite. Gli altri clienti non utilizzano lo stesso hardware.

È possibile utilizzare MCS per eseguire il provisioning di host AWS dedicati utilizzando l'interfaccia Full Configuration (Configurazione completa) o PowerShell.

### Configurare la tenancy dell'host AWS dedicato utilizzando l'interfaccia Full Configuration (Configurazione completa)

Quando si utilizza MCS per creare un catalogo per il provisioning delle macchine in AWS, la pagina **Machine Catalog Setup > Security** (Configurazione del catalogo delle macchine > Sicurezza) presenta le seguenti opzioni:

- **Use shared hardware** (Usa hardware condiviso). Questa impostazione è adatta per la maggior parte delle distribuzioni. Più clienti condividono componenti hardware anche se non interagiscono tra loro. L'utilizzo di hardware condiviso è l'opzione meno costosa per l'esecuzione delle istanze di Amazon EC2.
- **Use dedicated host** (Usa un host dedicato). Un host dedicato di Amazon EC2 è un server fisico con capacità di istanza EC2 completamente dedicata, che consente di utilizzare licenze software esistenti per socket o per macchina virtuale. Gli host dedicati hanno un utilizzo preimpostato in base al tipo di istanza. Ad esempio, un singolo host dedicato allocato di tipi di istanza C4 Large è limitato all'esecuzione di 16 istanze. Per ulteriori informazioni, consultare il sito di AWS.

  I requisiti per il provisioning sugli host AWS includono:

  - Un'immagine BYOL (Bring Your Own License) importata (AMI). Con host dedicati, utilizzare e gestire le licenze esistenti.
  - Un'allocazione di host dedicati con un utilizzo sufficiente per soddisfare le richieste di provisioning.
  - Abilitazione del **posizionamento automatico**.

  Questa impostazione è adatta per le distribuzioni con restrizioni di licenza o requisiti di sicurezza che richiedono l'uso di un host dedicato. Con un host dedicato, si possiede un intero host fisico e l'addebito viene effettuato su base oraria. La proprietà di tale host consente di avviare tante istanze EC2 quante ne consente l'host, senza costi aggiuntivi.

  In alternativa, è possibile effettuare il provisioning di host AWS dedicati tramite PowerShell. A tale scopo, utilizzare il cmdlet `New-ProvScheme` con il parametro `TenancyType` impostato su `Host`. Per ulteriori informazioni, consultare la documentazione per gli sviluppatori Citrix.
- **Use dedicated instance** (Usa un'istanza dedicata). Questa impostazione è più adatta per le distribuzioni con requisiti di sicurezza o conformità specifici. Con un'istanza dedicata, si hanno comunque i vantaggi di avere un host separato dagli altri clienti AWS, ma non si paga per l'intero host. La capacità dell'host non è motivo di preoccupazione, ma viene addebitata una tariffa più alta per le istanze.

#### Configurare la tenancy dell'host AWS dedicato utilizzando PowerShell

È possibile creare un catalogo di macchine con tenancy host definita tramite PowerShell.

Un host dedicato Amazon [EC2] è un server fisico con capacità di istanza [EC2] completamente dedicata, che consente di utilizzare licenze software esistenti per socket o per macchina virtuale.

Gli host dedicati hanno un utilizzo preimpostato in base al tipo di istanza. Ad esempio, un singolo host dedicato allocato di tipi di istanza C4 Large è limitato all'esecuzione di 16 istanze. Per ulteriori informazioni, consultare il sito di AWS.

I requisiti per il provisioning sugli host AWS includono:

- Un'immagine BYOL (Bring Your Own License) importata (AMI). Con host dedicati, utilizzare e gestire le licenze esistenti.
- Un'allocazione di host dedicati con un utilizzo sufficiente per soddisfare le richieste di provisioning.
- abilitare il **posizionamento automatico**.

Per eseguire il provisioning su un host dedicato in AWS utilizzando PowerShell, utilizzare il cmdlet **New-ProvScheme** con il parametro TenancyType impostato su *Host*.

Per ulteriori informazioni, consultare la documentazione per gli sviluppatori Citrix.

### Acquisire la proprietà dell'istanza AWS

Quando si crea un catalogo per il provisioning di macchine utilizzando Machine Creation Services (MCS) in AWS, si seleziona un'AMI per rappresentare l'immagine master/golden di quel catalogo. Da tale AMI, MCS utilizza una snapshot del disco. Nelle versioni precedenti, se si voleva avere ruoli o tag sulle macchine si utilizzava la console AWS per impostarli individualmente. Questa funzionalità è abilitata per impostazione predefinita.

> **Suggerimento:**
>
> Per utilizzare l'acquisizione delle proprietà delle istanze AWS, è necessario disporre di una macchina virtuale associata all'AMI.

Per migliorare questo processo, **MCS legge** le proprietà dall'istanza da cui è stata presa l'AMI e applica il ruolo di Identity Access Management (IAM) e i tag della macchina alle macchine di cui è stato eseguito il provisioning per un determinato catalogo. Quando si utilizza questa funzione facoltativa, il processo di creazione del catalogo trova l'istanza dell'origine AMI selezionata che legge un insieme limitato di proprietà. Queste proprietà vengono quindi archiviate in un modello di avvio AWS, utilizzato per il provisioning di macchine per quel catalogo. Qualsiasi macchina nel catalogo eredita le proprietà dell'istanza acquisita.

Le proprietà acquisite includono:

- Ruoli IAM: applicati alle istanze di cui è stato eseguito il provisioning.
- Tag: applicati alle istanze di cui è stato eseguito il provisioning, il relativo disco e le NIC. Questi tag vengono applicati alle risorse Citrix transitorie, tra cui: bucket e oggetti S3, AMI, snapshot e modelli di avvio.

> **Suggerimento:**
>
> L'etichettatura delle risorse Citrix transitorie è facoltativa ed è configurabile utilizzando la pro-

> prietà personalizzata `AwsOperationalResourcesTagging`. Per applicare correttamente i tag e creare un catalogo di AWS con tag delle risorse operative, non eliminare l'istanza EC2 utilizzata per creare l'immagine AMI.

#### Acquisire la proprietà dell'istanza AWS

È possibile utilizzare questa funzionalità specificando una proprietà personalizzata, `AwsCaptureInstancePro`, durante la creazione di uno schema di provisioning per una connessione di hosting AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

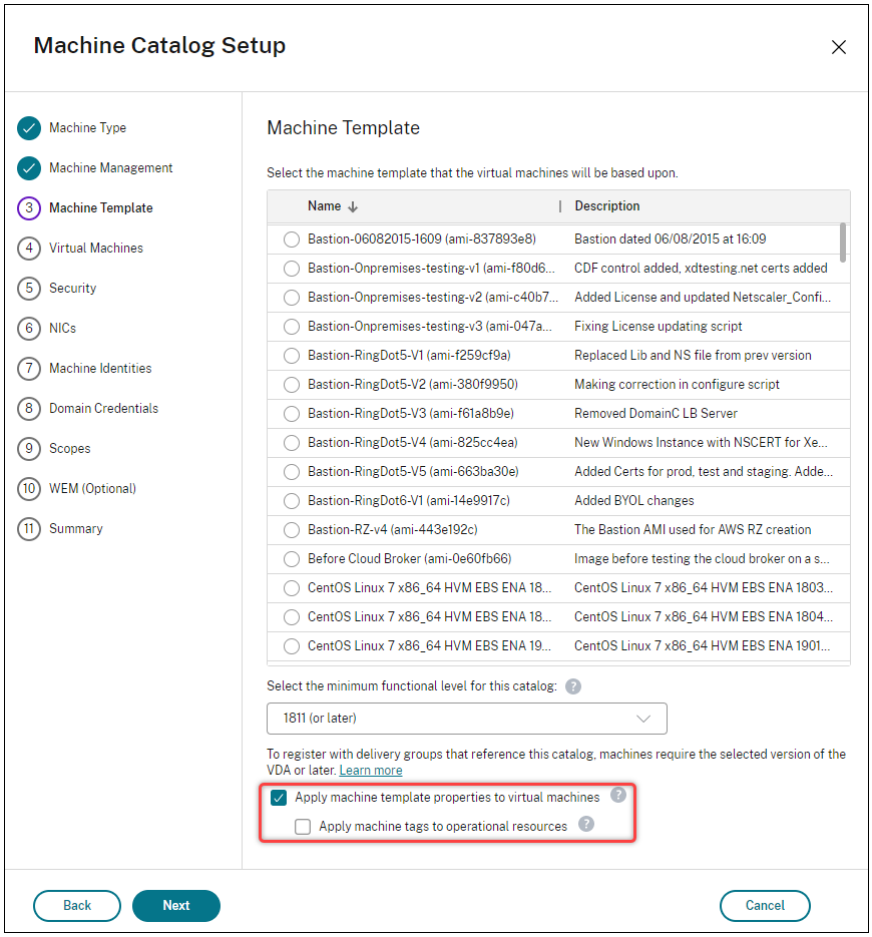
Per ulteriori informazioni, consultare la documentazione per gli sviluppatori Citrix.

> **Nota:**
>
> `AwsCaptureInstanceProperties` è obsoleto.

### Applicare le proprietà delle istanze AWS e assegnare tag alle risorse operative nell'interfaccia Full Configuration

Quando si crea un catalogo per il provisioning delle macchine in AWS utilizzando MCS, è possibile controllare se applicare il ruolo IAM e le proprietà dei tag a tali macchine. È inoltre possibile controllare se applicare tag delle macchine alle risorse operative. Sono disponibili le due opzioni seguenti:




- **Apply machine template properties to virtual machines** (Applica le proprietà dei modelli di macchine alle macchine virtuali)
  - Controlla se applicare il ruolo IAM e le proprietà dei tag associati al modello di macchina selezionato alle macchine virtuali in questo catalogo.
- **Apply machine tags to operational resources** (Applica i tag delle macchine alle risorse operative)
  - Controlla se applicare i tag delle macchine a ogni elemento creato nell'ambiente AWS che facilita il provisioning delle macchine. Le risorse operative vengono create come sottoprodotti della creazione del catalogo. Includono risorse sia temporanee che persistenti, come l'istanza delle macchine virtuali di preparazione e l'AMI.

## Applicare tag a una risorsa operativa AWS

Un'Amazon Machine Image (AMI) rappresenta un tipo di appliance virtuale utilizzata per creare una macchina virtuale all'interno dell'ambiente Amazon Cloud, comunemente denominato EC2. È possibile utilizzare un'AMI per distribuire servizi che utilizzano l'ambiente EC2. Quando si crea un catalogo

per eseguire il provisioning di macchine utilizzando MCS per AWS, selezionare l'**AMI** che funge da immagine golden per quel catalogo.

> **Importante:**
>
> La creazione di cataloghi mediante l'acquisizione di una proprietà di istanza e di un modello di avvio è necessaria per utilizzare la codifica delle risorse operative.

Per creare un catalogo di AWS, è necessario innanzitutto creare un'AMI per l'istanza in cui si desidera collocare l'immagine golden. MCS legge i tag di quell'istanza e li incorpora nel modello di avvio. I tag del modello di avvio vengono quindi applicati a tutte le risorse Citrix create nell'ambiente AWS, tra cui:

- Macchine virtuali
- Dischi delle macchine virtuali
- Interfacce di rete delle macchine virtuali
- Bucket S3
- Oggetti S3
- Modelli di lancio
- AMI

#### Applicare tag a una risorsa operativa

Per utilizzare PowerShell per etichettare le risorse:

1. Aprire una finestra di PowerShell dall'host DDC.
2. Eseguire il comando `asnp citrix` per caricare i moduli PowerShell specifici di Citrix.

Per etichettare una risorsa per una macchina virtuale di cui è stato eseguito il provisioning, utilizzare la nuova proprietà personalizzata `AwsOperationalResourcesTagging`. La sintassi di questa proprietà è la seguente:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" ...<standard provscheme parameters
>
```

### Creare un catalogo utilizzando un profilo macchina

È possibile utilizzare un profilo macchina per acquisire le proprietà hardware da un'istanza EC2 (VM) o da una versione del modello di avvio e applicarle alle macchine di cui è stato effettuato il provisioning. Le proprietà acquisite possono includere, ad esempio, le proprietà del volume EBS, il tipo di istanza, l'ottimizzazione EBS, la grafica elastica e altre configurazioni AWS supportate.

È possibile utilizzare un'istanza (VM) AWS EC2 o una versione AWS Launch Template come input del profilo macchina.

> **Nota:**
>
> Le proprietà del volume EBS derivano solo dal profilo di una macchina.

#### Considerazioni importanti

Le considerazioni importanti durante la creazione di un catalogo di macchine MCS sono:

- Se si aggiungono i parametri delle proprietà hardware della macchina nei comandi `New-ProvScheme` e `Set-ProvScheme`, i valori forniti nei parametri sovrascrivono i valori indicati nel profilo della macchina.
- Se si imposta `AwsCaptureInstanceProperties` su **`true`** e non si imposta una proprietà `MachineProfile`, vengono acquisiti solo i ruoli e i tag IAM.
- Non è possibile impostare sia `AwsCaptureInstanceProperties` che `MachineProfile` contemporaneamente.

  > **Nota:
  >
  > `AwsCaptureInstanceProperties` è obsoleto.

- È necessario fornire esplicitamente i valori delle seguenti proprietà:
  - TenancyType
  - Gruppo di sicurezza
  - NIC o rete virtuale
- È possibile abilitare `AwsOperationalResourcesTagging` solo se si abilita `AwsCaptureInstanceP` o si specifica un profilo macchina.

Le considerazioni importanti dopo la creazione di un catalogo di macchine MCS sono:

- Solo le nuove macchine virtuali aggiunte al catalogo sono interessate dalla modifica.
- Non è possibile trasformare un catalogo da basato su profili di macchina in non basato su profili macchina.

#### Creare un catalogo di macchine utilizzando un profilo macchina

Per creare un catalogo di macchine utilizzando un profilo macchina:

1. Aprire una finestra di **PowerShell**.

2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Creare un pool di identità se non è già stato creato. Ad esempio,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain abcdf -NamingSchemeType Numeric
<!--NeedCopy-->
```

4. Eseguire il comando New-ProvScheme. Ad esempio:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1
-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
-CleanOnBoot
-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
    demet-ami.0 (ami-0ca813xxxxxx061ef).template'
-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
    -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
    vm'
<!--NeedCopy-->
```

5. Completare la creazione del catalogo. Per ulteriori informazioni, vedere Citrix PowerShell SDK.

Per aggiornare il profilo macchina su un catalogo di cui inizialmente era stato effettuato il provisioning con un profilo macchina:

1. Eseguire il comando `Set-ProvScheme`. Ad esempio,

```
Set-ProvScheme `
-ProvisioningSchemeUid "<ID" `
-MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
    availabilityzone\citrix-cvad-machineprofile-instance (i-0
    xxxxxxxx).vm"
<!--NeedCopy-->
```

#### Creare un catalogo con la versione del modello di avvio

È possibile creare un catalogo di macchine MCS con una versione del modello di avvio come input per il profilo macchina. È inoltre possibile aggiornare l'input di un catalogo di profili di macchina da una macchina virtuale a una versione del modello di avvio e da una versione del modello di avvio a una macchina virtuale.

Sulla console AWS EC2, è possibile fornire le informazioni di configurazione dell'istanza di un modello di avvio insieme al numero di versione. Quando si specifica la versione del modello di avvio come input del profilo macchina durante la creazione o l'aggiornamento di un catalogo di macchine, le proprietà di quella versione del modello di avvio vengono copiate nelle VM dei VDA di cui è stato eseguito il provisioning.

Le seguenti proprietà possono essere fornite utilizzando l'input del profilo macchina o esplicitamente come parametri nei comandi `New-ProvScheme` o `Set-ProvScheme`. Se sono forniti nei comandi `New-ProvScheme` o `Set-ProvScheme`, hanno la precedenza sui valori del profilo macchina di queste proprietà.

- Offerta di servizi
- Reti
- Gruppi di sicurezza
- Tipo di tenancy

> **Nota:**
>
> Se l'offerta di servizi non è fornita nel modello di avvio con profilo macchina o come parametro nel comando `New-ProvScheme`, viene visualizzato un errore appropriato.

Per creare un catalogo utilizzando la versione del modello di avvio come input del profilo macchina:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Ottenere l'elenco delle versioni del modello di avvio di un modello di avvio. Ad esempio:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. Creare un pool di identità se non è già stato creato. Ad esempio:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```

5. Creare uno schema di provisioning con una versione del modello di avvio come input del profilo macchina. Ad esempio:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
```

```
<!--NeedCopy-->
```

È anche possibile ignorare parametri quali offerta di servizi, gruppi di sicurezza, tenancy e reti. Ad esempio:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion"
    `
-ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large Instance.
   serviceoffering"
<!--NeedCopy-->
```

6. Registrare lo schema di provisioning come catalogo del broker. Ad esempio:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. Completare la creazione del catalogo. Per ulteriori informazioni, vedere Citrix PowerShell SDK.

È inoltre possibile aggiornare l'input di un catalogo di profili di macchina da una macchina virtuale a una versione del modello di avvio e da una versione del modello di avvio a una macchina virtuale. Ad esempio:

- Per aggiornare l'input di un catalogo di profili macchina da una macchina virtuale a una versione del modello di avvio:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

- Per aggiornare l'input di un catalogo di profili macchina da una versione del modello di avvio a una macchina virtuale:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
```

```
-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
<!--NeedCopy-->
```

### Creare un catalogo di macchine virtuali abilitate con l'acceleratore Grafica elastica

Utilizzando un flusso di lavoro basato sul profilo macchina, è possibile creare un catalogo di macchine virtuali abilitate con l'acceleratore Grafica elastica. È possibile utilizzare una macchina virtuale e un modello di avvio come input del profilo macchina.

I passaggi dettagliati per creare un catalogo sono:

1. Abilitare un acceleratore Grafica elastica su una macchina virtuale o su un modello di avvio. Per informazioni sull'attivazione dell'acceleratore Grafica elastica, vedere Utilizzo di Grafica elastica.
2. Verifica il tipo di acceleratore Grafica elastica utilizzato dalla macchina virtuale o dalla versione del modello di avvio. Se la chiave `ElasticGpuType` non è presente nei dati aggiuntivi, la macchina virtuale o il modello di avvio non hanno l'acceleratore Grafica elastica abilitato.
   - Ad esempio: per una macchina virtuale

     ```
     (Get-Item -LiteralPath 'XDHyp:\HostingUnits\abc-resources\us-
        eat-1a.availibilityzone\abcelastic (i-0584xxxxxab8b2206).
        vm').AdditionalData
     <!--NeedCopy-->
     ```

   - Ad esempio: per un modello di lancio

     ```
     (Get-Item -LiteralPath 'XDHyp:\HostingUnits\abc-resources\
        ElasticGC (lt-015f531351188cd2e).launchtemplate\lt-015
        f531351188cd2e (1).launchtemplateversion).AdditionalData
     <!--NeedCopy-->
     ```

3. Creare un catalogo di macchine MCS con il flusso di lavoro dei profili macchina, selezionando una VM o specifiche del modello. È possibile creare il catalogo delle macchine utilizzando Web Studio o eseguendo i comandi PowerShell.

> **Nota:**
>
> Il catalogo di macchine deve soddisfare i prerequisiti di Grafica elastica per una corretta creazione del catalogo di macchine. Pertanto, assicurati che il tipo di istanza EC2 sia compatibile con Grafica elastica. Per informazioni, vedere Nozioni di base su Grafica elastica.

### Filtrare le istanze di VM

Un'istanza di macchina virtuale AWS che si usa come macchina virtuale con profilo macchina deve essere compatibile perché il catalogo macchine venga creato e funzioni correttamente. Per elencare le istanze di macchine virtuali AWS che possono essere utilizzate come macchine virtuali di input per il profilo macchina, è possibile utilizzare il comando `Get-HypInventoryItem`. Il comando può effettuare il paging e filtrare l'inventario delle VM disponibili su un'unità di hosting.

**Paging:**

**Get-HypInventoryItem** supporta due modalità di paging:

- La modalità di paging utilizza i parametri `-MaxRecords` e `-Skip` per restituire set di elementi:
  - `-MaxRecords`: l'impostazione predefinita è **1**. Questo controlla quanti elementi restituire.
  - `-Skip`: l'impostazione predefinita è **0**. Questo controlla quanti elementi saltare dall'inizio assoluto (o dalla fine assoluta) dell'elenco nell'hypervisor.
- La modalità di scorrimento utilizza i parametri `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` per consentire lo scorrimento dei record:
  - `-ForwardDirection`: l'impostazione predefinita è **True**. Questa viene utilizzata con `-MaxRecords` per restituire il set successivo di record corrispondenti o il precedente set di record corrispondenti.
  - `-ContinuationToken`: restituisce gli elementi immediatamente dopo (o prima se `ForwardDirection` è **falso**) ma non include l'articolo indicato nel `ContinuationToken` .

Esempi di paging:

- Per restituire un singolo record del modello di macchina con il nome più basso. Il campo `AdditionalData` contiene `TotalItemsCount` e `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template
<!--NeedCopy-->
```

- Per restituire dieci record del modello di macchina con il nome più basso:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 10 | select Name
<!--NeedCopy-->
```

- Per restituire una matrice di record che termina con il nome più alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
```

```
<!--NeedCopy-->
```

- Per restituire una matrice di record a partire dal modello di macchina associato al `ContinuationToken` dato:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
<!--NeedCopy-->
```

**Filtraggio:**

I seguenti parametri opzionali aggiuntivi sono supportati per il filtraggio. È possibile combinare questi parametri con le opzioni di paging.

- `-ContainsName "my_name"`: se la stringa specificata corrisponde a una parte del nome AMI, l'AMI viene incluso nel risultato di `Get`. Ad esempio:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ' apollo '
     | select Name
<!--NeedCopy-->
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '` : Se un'AMI ha almeno uno di questi tag, viene incluso nel risultato di `Get` . Ad esempio:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```

> **Nota:**
>
> Sono supportati due valori di tag. Il valore del tag **Not Tagged** corrisponde agli elementi che non contengono il tag specificato nel loro elenco di tag. Il valore del tag **All values** corrisponde agli elementi che contengono il tag indipendentemente dal valore del tag. Altrimenti, la corrispondenza avviene solo se l'elemento contiene il tag e il valore è uguale a quello indicato nel filtro.

- `-Id "ami-0a2d913927e0352f3"`: se l'AMI corrisponde all'ID specificato, viene incluso nel risultato di `Get`. Ad esempio:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
<!--NeedCopy-->
```

**Filtraggio in base al parametro AdditionalData:**

Il parametro di filtraggio `AdditionalData` elenca i modelli o le macchine virtuali in base alla loro capacità, all'offerta di servizi o a qualsiasi proprietà presente in AdditionalData. Ad esempio:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
   AdditionalData
<!--NeedCopy-->
```

È inoltre possibile aggiungere un parametro `-Warn` per indicare le macchine virtuali incompatibili. Le macchine virtuali sono incluse in un campo `AdditionalData` denominato **Warning** (Avviso). Ad esempio:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
   -015xxxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di AWS.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione ad AWS
- Creare cataloghi di macchine

## Creare un catalogo di Citrix Hypervisor

August 30, 2023

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione Citrix Hypervisor.

> **Nota:**
>
> Prima di creare un catalogo di Citrix Hypervisor, è necessario completare la creazione di una connessione a Citrix Hypervisor. Vedere Connessione a Citrix Hypervisor.

### Creare un catalogo di macchine utilizzando una connessione Citrix Hypervisor

Le macchine compatibili con GPU richiedono un'immagine master dedicata. Queste macchine virtuali richiedono driver di schede video che supportino le GPU. Configurare macchine compatibili con GPU per consentire alla macchina virtuale di operare con software che utilizza la GPU per le operazioni.

1. In XenCenter creare una VM con VGA, reti e vCPU standard.
2. Aggiornare la configurazione della VM per abilitare l'uso della GPU (Passthrough o vGPU).
3. Installare un sistema operativo supportato e abilitare RDP.
4. Installare Citrix VM Tools e driver NVIDIA.
5. Disattivare la Console di amministrazione Virtual Network Computing (VNC) per ottimizzare le prestazioni, quindi riavviare la macchina virtuale.
6. Viene richiesto di utilizzare RDP. Utilizzando RDP, installare il VDA e riavviare la macchina virtuale.
7. Facoltativamente, creare un'istantanea della macchina virtuale come modello di base per altre immagini master GPU.
8. Utilizzando RDP, installare applicazioni specifiche del cliente che sono configurate in XenCenter e utilizzano le funzionalità GPU.

### Creare un catalogo di macchine utilizzando un profilo macchina

Quando si crea un catalogo per il provisioning delle macchine utilizzando MCS, è possibile utilizzare un profilo macchina per acquisire le proprietà hardware da una macchina virtuale e applicarle alle macchine virtuali di cui è stato appena effettuato il provisioning nel catalogo. Se il parametro `MachineProfile` non viene utilizzato, le proprietà hardware vengono acquisite dalla VM o dalla snapshot dell'immagine master.

> **Nota:**
>
> Attualmente, è possibile utilizzare solo una macchina virtuale come input del profilo macchina.

È possibile configurare in modo esplicito i seguenti parametri perché sovrascrivano i valori dei parametri nell'input del profilo macchina:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Per creare un catalogo con un profilo macchina:

1. Aprire la finestra di PowerShell.
2. Eseguire `asnp citrix*`.
3. Creare un pool di identità. Il pool di identità è un contenitore per gli account Active Directory (AD) per le macchine virtuali da creare. Ad esempio:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
    IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
    -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
<!--NeedCopy-->
```

4. Creare gli account di computer AD richiesti in Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
<!--NeedCopy-->
```

5. Eseguire il `New-ProvScheme` comando per creare un catalogo. Ad esempio:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm"
<!--NeedCopy-->
```

6. Registrare lo schema di provisioning come catalogo del broker. Ad esempio:

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
<!--NeedCopy-->
```

7. Aggiungere macchine virtuali al catalogo.

Per aggiornare un catalogo con un nuovo profilo macchina:

1. Eseguire il comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
    snapshot"
<!--NeedCopy-->
```

   Per ulteriori informazioni sul comando Set-ProvScheme, vedere Set-ProvScheme.

> **Nota:**
>
> - Il comando `Set-ProvScheme` in questo caso non modifica il profilo macchina delle VM esistenti nel catalogo. Solo le VM appena create aggiunte al catalogo hanno il nuovo profilo macchina.
> - Non è possibile convertire un catalogo di macchine basato su profili macchina in un catalogo di macchine non basato su profili macchina.

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Citrix Hypervisor.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a Citrix Hypervisor
- Creare cataloghi di macchine

## Creare un catalogo di Google Cloud Platform

September 12, 2023

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti cloud di Google.

> **Nota:**
>
> Prima di creare un catalogo di Google Cloud Platform (GCP), è necessario completare la creazione di una connessione a GCP. Vedere Connessione agli ambienti cloud di Google.

### Preparare un'istanza di macchina virtuale master e un disco persistente

> **Suggerimento:**
>
> "Disco persistente"è il termine Google Cloud per il disco virtuale.

Per preparare l'istanza della macchina virtuale master, creare e configurare un'istanza di macchina virtuale con proprietà che corrispondono alla configurazione desiderata per le istanze VDA clonate nel catalogo delle macchine pianificato. La configurazione non si applica solo alle dimensioni e al tipo di istanza. Include anche attributi di istanza come metadati, tag, assegnazioni GPU, tag di rete e proprietà degli account di servizio.

Nell'ambito del processo di mastering, MCS utilizza l'istanza della macchina virtuale master per creare il *modello di istanza* di Google Cloud. Il modello di istanza viene quindi utilizzato per creare le istanze VDA clonate che costituiscono il catalogo delle macchine. Le istanze clonate ereditano le proprietà (ad eccezione delle proprietà del VPC, della subnet e del disco persistente) dell'istanza della macchina virtuale master da cui è stato creato il modello di istanza.

Dopo aver configurato le proprietà dell'istanza della macchina virtuale master in base alle proprie specifiche, avviare l'istanza e quindi preparare il disco persistente per l'istanza.

Si consiglia di creare manualmente una snapshot del disco. Ciò consente di utilizzare una convenzione di denominazione significativa per tenere traccia delle versioni, offre più opzioni per gestire le versioni precedenti dell'immagine master e consente di risparmiare tempo per la creazione del catalogo delle macchine. Se non si crea una snapshot personalizzata, MCS crea un'istantanea temporanea (che viene eliminata al termine del processo di provisioning).

### Creare un catalogo di macchine

> **Nota:**
>
> Creare le risorse prima di creare un catalogo delle macchine. Utilizzare le convenzioni di denominazione stabilite da Google Cloud durante la configurazione dei cataloghi delle macchine. Per maggiori informazioni, consultare le Linee guida per la denominazione di bucket e oggetti.

Seguire le indicazioni in Creare cataloghi delle macchine. La seguente descrizione vale esclusivamente per i cataloghi di Google Cloud.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare **Create Machine Catalog** (Crea catalogo delle macchine) nella barra delle azioni.
3. Nella pagina **Machine Type** (Tipo di macchina), selezionare **Multi-session OS** (Sistema operativo multisessione), quindi selezionare **Next** (Avanti).

   - Citrix DaaS supporta anche il sistema operativo a sessione singola.

4. Nella pagina **Machine Management** (Gestione macchine), selezionare le opzioni **Machines that are power managed** (Macchine con gestione dell'alimentazione) e **Citrix Machine Creation Services** (Servizi di creazione macchine Citrix) e fare clic su **Next** (Avanti). Se ci sono più risorse, selezionarne una dal menu.
5. Nella pagina **Master Image** (Immagine principale), completare questi passaggi in base alle esigenze, quindi fare clic su **Next** (Avanti).

   a) Selezionare una snapshot o una macchina virtuale come immagine principale. Se si desidera utilizzare la funzionalità single-tenancy, assicurarsi di selezionare un'immagine la cui proprietà del gruppo di nodi sia configurata correttamente. Vedere Abilitare la selezione delle zone.

   b) Per utilizzare una macchina virtuale esistente come profilo macchina, selezionare **Use a machine profile** (Usa un profilo macchina), quindi selezionare la macchina virtuale.

      > **Nota:**
      >
      > Attualmente, le macchine virtuali di questo catalogo ereditano dal profilo della macchina queste impostazioni: ID del set di crittografia del disco, dimensione della macchina, tipo di archiviazione e zona.

   c) Selezionare il livello funzionale minimo per il catalogo.

6. Nella pagina **Storage** (Archiviazione), selezionare il tipo di archiviazione utilizzato per contenere il sistema operativo per questo catalogo delle macchine. Ognuna delle seguenti opzioni di archiviazione ha caratteristiche di prezzo e prestazioni diverse (un disco di identità viene sempre creato utilizzando il disco persistente standard della zona).

   - Disco persistente standard
   - Disco persistente bilanciato
   - Disco persistente SSD

   Per ulteriori informazioni sulle opzioni di archiviazione di Google Cloud, vedere https://cloud.google.com/compute/docs/disks/.

7. Nella pagina **Virtual Machines** (Macchine virtuali), specificare quante macchine virtuali si desidera creare, visualizzare le specifiche dettagliate delle macchine virtuali e quindi selezionare **Next** (Avanti). Se si utilizzano i gruppi di nodi single-tenant per i cataloghi delle macchine, assicurarsi di selezionare **solo** le zone in cui sono disponibili i nodi single-tenant riservati. Vedere Abilitare la selezione delle zone.
8. Nella pagina **Disk Settings** (Impostazioni disco), è possibile configurare le seguenti impostazioni:

   - Scegliere se abilitare la cache write-back. Dopo aver abilitato la cache write-back, è possibile procedere come segue:

     – Configurare le dimensioni del disco e della RAM utilizzati per la memorizzazione nella cache dei dati temporanei. Per maggiori informazioni, consultare Configurare la cache per i dati temporanei.

     – Selezionare il tipo di archiviazione per il disco della cache write-back. Sono disponibili le seguenti opzioni di archiviazione per il disco della cache write-back:

       * Disco persistente standard
       * Disco persistente bilanciato
       * Disco persistente SSD

       Per ulteriori informazioni sulle opzioni di archiviazione di GCP, vedere https://cloud.google.com/compute/docs/disks/.

     – Selezionare il tipo per il disco della cache write-back.

       * **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se questa opzione è selezionata, il disco della cache write-back non persiste per le macchine virtuali di cui è stato eseguito il provisioning. Il disco viene eliminato durante i cicli di alimentazione e tutti i dati reindirizzati al disco andranno persi.
       * **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se questa opzione è selezionata, il disco della cache write-back persiste per le macchine virtuali di cui è stato eseguito il provisioning. L'attivazione di questa opzione aumenta i costi di archiviazione.

   - Quando l'ottimizzazione dell'archiviazione MCS (MCS I/O) è abilitata, è possibile scegliere se conservare i dischi di sistema per i VDA durante i cicli di alimentazione. Per ulteriori informazioni, vedere Abilitazione degli aggiornamenti per l'ottimizzazione dell'archiviazione MCS.

   - Scegliere se utilizzare la propria chiave per proteggere il contenuto del disco. Per utilizzare questa funzionalità, è necessario prima creare le proprie CMEK (Customer Managed Encryption Keys, chavi di crittografia gestite dal cliente). Per ulteriori informazioni,

vedere Utilizzo di CMEK (Customer Managed Encryption Keys, chavi di crittografia gestite dal cliente).

> **Nota:**
>
> È disponibile solo nell'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa).

Dopo aver creato le chiavi, è possibile selezionare una di queste chiavi dall'elenco. Non è possibile modificare la chiave dopo aver creato il catalogo. Google Cloud non supporta la rotazione delle chiavi su dischi o immagini persistenti esistenti. Pertanto, dopo aver eseguito il provisioning di un catalogo, il catalogo viene associato a una versione specifica della chiave. Se la chiave viene disabilitata o distrutta, le istanze e i dischi crittografati con tale chiave diventano inutilizzabili fino a quando la chiave non viene riabilitata o ripristinata.

9. Nella pagina **Machine Identities** (Identità macchine), selezionare un account di Active Directory e quindi selezionare **Next** (Avanti).
    - Se si seleziona **Create new Active Directory accounts** (Crea nuovi account di Active Directory), selezionare un dominio e quindi immettere la sequenza di caratteri che rappresenta lo schema di denominazione per gli account delle macchine virtuali di cui è stato eseguito il provisioning creati in Active Directory. Lo schema di denominazione degli account può contenere da 1 a 64 caratteri e non può contenere spazi vuoti, caratteri non ASCII o caratteri speciali.
    - Se si seleziona **Use existing Active Directory accounts** (Usa account Active Directory esistenti), selezionare **Browse** (Sfoglia) per passare agli account delle macchine di Active Directory esistenti per le macchine selezionate.
10. Nella pagina **Domain Credentials** (Credenziali di dominio), selezionare **Enter credentials** (Immetti le credenziali), digitare il nome utente e la password, selezionare **Save** (Salva), quindi selezionare **Next** (Avanti).
    - La credenziale digitata deve disporre delle autorizzazioni per eseguire le operazioni relative agli account di Active Directory.
11. Nella pagina **Scopes** (Ambiti), selezionare gli ambiti per il catalogo delle macchine, quindi selezionare **Next** (Avanti).
    - È possibile selezionare ambiti opzionali o selezionare un **ambito personalizzato** per personalizzare gli ambiti in base alle esigenze.
12. Nella pagina **Summary** (Riepilogo), confermare le informazioni, specificare un nome per il catalogo e quindi selezionare **Finish** (Fine).

> **Nota:**
>
> Il nome del catalogo può contenere da 1 a 39 caratteri e non può contenere solo spazi vuoti o caratteri `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

Il completamento della creazione del catalogo delle macchine potrebbe richiedere molto tempo. Al termine, il catalogo viene elencato. È possibile verificare che le macchine vengano create nei gruppi di nodi di destinazione nella console di Google Cloud.

#### Utilizzo di PowerShell per creare un catalogo con disco di cache write-back persistente

Per configurare un catalogo con disco di cache write-back persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`.

> **Suggerimento:**
>
> Utilizzare il parametro PowerShell `New-ProvScheme CustomProperties` solo per le connessioni di hosting basate su cloud. Se si desidera eseguire il provisioning di macchine utilizzando un disco di cache write-back persistente per una soluzione locale (ad esempio, Citrix Hypervisor), PowerShell non è necessario perché il disco persiste automaticamente.

Questo parametro supporta una proprietà aggiuntiva, `PersistWBC`, utilizzata per determinare il modo in cui il disco della cache write-back persiste per le macchine di cui è stato eseguito il provisioning con MCS. La proprietà `PersistWBC` viene utilizzata solo quando viene specificato il parametro`UseWriteBackCache` e quando il parametro `WriteBackCacheDiskSize` è impostato per indicare che viene creato un disco.

> **Nota:**
>
> Questo comportamento si applica sia ad Azure che a GCP nei casi in cui il disco della cache write-back MCSIO predefinito viene eliminato e ricreato durante il ciclo di alimentazione. È possibile scegliere di rendere persistente il disco in modo da evitare l'eliminazione e la ri-creazione del disco della cache write-back MCSIO.

Esempi di proprietà trovate nel parametro `CustomProperties` prima del supporto `PersistWBC` sono:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

> **Nota:**
>
> Questo esempio si applica solo ad Azure. Le proprietà sono diverse nell'ambiente GCP.

Quando si utilizzano queste proprietà, considerare che contengono valori predefiniti se le proprietà vengono omesse dal parametro `CustomProperties`. La proprietà `PersistWBC` ha due valori possibili: **true** o **false**.

L'impostazione della proprietà `PersistWBC` su **true** non elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops spegne la macchina dall'interfaccia di gestione.

L'impostazione della proprietà `PersistWBC` su **false** elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops arresta la macchina dall'interfaccia di gestione.

> **Nota:**
>
> Se la proprietà `PersistWBC` viene omessa, il valore predefinito della proprietà è **false** e la cache write-back viene eliminata quando la macchina viene arrestata dall'interfaccia di gestione.

Ad esempio, utilizzando il parametro `CustomProperties` per impostare `PersistWBC` su true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Importante:**
>
> La proprietà `PersistWBC` può essere impostata solo utilizzando il cmdlet PowerShell `New-ProvScheme`. Il tentativo di modificare le `CustomProperties` di uno schema di provisioning dopo la creazione non ha alcun impatto sul catalogo macchine e sulla persistenza del disco della cache write-back quando un computer viene arrestato.

Ad esempio, impostare `New-ProvScheme` perché utilizzi la cache write-back mentre si imposta la proprietà `PersistWBC` su true:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

**Migliorare le prestazioni di avvio con MCSIO**

È possibile migliorare le prestazioni di avvio per i dischi gestiti di Azure e GCP quando MCSIO è abilitato. Utilizzare la proprietà personalizzata di PowerShell `PersistOSDisk` nel comando `New-ProvScheme` per configurare questa funzionalità. Le opzioni associate a `New-ProvScheme` includono:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
``````<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

Per abilitare questa funzionalità, impostare la proprietà personalizzata `PersistOSDisk` su **true**. Ad esempio:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Creare un catalogo di macchine utilizzando un profilo macchina

Quando si crea un catalogo per il provisioning delle macchine utilizzando Machine Creation Services (MCS), è possibile utilizzare un profilo macchina per acquisire le proprietà hardware da una macchina virtuale e applicarle alle macchine virtuali di cui è stato appena effettuato il provisioning nel catalogo. Quando il parametro `MachineProfile` non viene utilizzato, le proprietà hardware vengono acquisite dalla VM o dalla snapshot dell'immagine master.
Alcune proprietà vengono definite in modo esplicito; ad esempio `StorageType`, `CatalogZones` e `CryptoKeyIs` vengono ignorate dal profilo del computer.

- Per creare un catalogo con un profilo macchina, utilizzare il comando `New-ProvScheme`. Ad esempio, `New-ProvScheme –MachineProfile "path to VM"`. Se non si specifica il parametro `MachineProfile`, le proprietà hardware vengono acquisite dalla VM dell'immagine master.
- Per aggiornare un catalogo con un nuovo profilo macchina, utilizzare il comando `Set-ProvScheme`. Ad esempio, `Set-ProvScheme –MachineProfile "path to` **new**

VM". Questo comando non modifica il profilo macchina delle VM esistenti nel catalogo. Solo le VM appena create aggiunte al catalogo hanno il nuovo profilo macchina.

- È anche possibile aggiornare l'immagine master, tuttavia, quando si aggiorna l'immagine master e le proprietà hardware non vengono aggiornate. Se si desidera aggiornare le proprietà hardware, è necessario aggiornare il profilo della macchina utilizzando il comando `Set-ProvScheme`. Queste modifiche si applicheranno solo alle nuove macchine del catalogo. Per aggiornare le proprietà hardware di una macchina esistente, è possibile utilizzare il comando `Set-ProvVMUpdateTimeWindow` con i parametri `-StartsNow` e `-DurationInMinutes -1`.

  > **Nota:**
  >
  > - `StartsNow` indica che l'ora di inizio pianificata è l'ora corrente.
  > - `DurationInMinutes` con un numero negativo (ad esempio -1) indica che non vi è alcun limite superiore nella finestra oraria della pianificazione.

### Creare un catalogo di macchine con il profilo della macchina come modello di istanza

È possibile selezionare un modello di istanza GCP come input per il profilo della macchina. I modelli di istanza sono risorse leggere in GCP, quindi sono molto convenienti.

Per creare un nuovo catalogo di macchine con il profilo della macchina come modello di istanza utilizzando i comandi PowerShell:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Trovare un modello di istanza nel proprio progetto GCP usando il seguente comando:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. Creare un nuovo catalogo di macchine con il profilo della macchina come modello di istanza utilizzando il comando NewProvScheme:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName> \Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

   Per ulteriori informazioni sul comando New-ProvScheme, vedere https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Completare la creazione del catalogo delle macchine utilizzando i comandi PowerShell.

Per modificare il profilo macchine di un catalogo di macchine esistente in modo che diventi un modello di istanza:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il seguente comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

   Per informazioni sul comando Set-ProvScheme, vedere https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Utilizzo di PowerShell per creare un catalogo con VM schermate

È possibile creare un catalogo di macchine MCS con le proprietà delle VM schermate. Una macchina virtuale schermata è rafforzata da una serie di controlli di sicurezza che forniscono l'integrità verificabile delle istanze di Compute Engine, utilizzando funzionalità avanzate di sicurezza della piattaforma quali l'avvio sicuro, un modulo di piattaforma attendibile virtuale, firmware UEFI e monitoraggio dell'integrità.

MCS supporta la creazione del catalogo utilizzando il flusso di lavoro del profilo macchina. Se si utilizza il workflow del profilo macchina, è necessario abilitare le proprietà delle VM schermate di un'istanza di macchina virtuale. È quindi possibile utilizzare questa istanza di macchina virtuale come input del profilo della macchina.

Per creare un catalogo di macchine MCS con macchina virtuale schermata utilizzando il flusso di lavoro del profilo macchina.

1. Abilitare le opzioni delle VM schermate di un'istanza di macchina virtuale nella console di Google Cloud. Vedere Avvio rapido: Abilitare le opzioni delle VM schermate.
2. Creare un catalogo di macchine MCS con il flusso di lavoro del profilo macchina utilizzando l'istanza di VM.
   a) Aprire una finestra di PowerShell.
   b) Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
   c) Creare un pool di identità se non è già stato creato.
   d) Eseguire il comando `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-machine.vm
<!--NeedCopy-->
```

3. Completate la creazione del catalogo di macchine.

Per aggiornare il catalogo macchine con un nuovo profilo macchina:

1. Eseguire il comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.vm
<!--NeedCopy-->
```

Per applicare la modifica effettuata in `Set-ProvScheme` alle macchine virtuali esistenti, eseguire il comando `Set-ProvVMUpdateTimeWindow`.

1. Eseguire il comando `Set-ProvVMUpdateTimeWindow`. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Riavviare le macchine virtuali.

### Importare macchine di Google Cloud create manualmente

È possibile *creare una connessione a Google Cloud* e quindi *creare un catalogo contenente macchine Google Cloud*. Quindi, è possibile spegnere e riaccendere manualmente le macchine Google Cloud tramite Citrix DaaS. Con questa funzionalità, è possibile:

- Importare macchine Google Cloud con sistema operativo multisessione create manualmente in un catalogo delle macchine di Citrix Virtual Apps and Desktops.
- Rimuovere macchine Google Cloud con sistema operativo multisessione create manualmente da un catalogo Citrix Virtual Apps and Desktops.
- Utilizzare le funzionalità esistenti di gestione dell'alimentazione di Citrix Virtual Apps and Desktops per gestire l'alimentazione delle macchine Google Cloud con sistema operativo multisessione Windows. Ad esempio, impostare un programma di riavvio per tali macchine.

Questa funzionalità non richiede modifiche a un flusso di lavoro di provisioning esistente di Citrix Virtual Apps and Desktops, né la rimozione di alcuna funzionalità esistente. Si consiglia di utilizzare

MCS per eseguire il provisioning delle macchine nell'interfaccia Full Configuration (Configurazione completa) in Citrix DaaS anziché importare le macchine Google Cloud create manualmente.

### Cloud privato virtuale condiviso

I cloud privati virtuali (VPC) condivisi comprendono un progetto host, da cui vengono rese disponibili le subnet condivise, e uno o più progetti di servizio che utilizzano la risorsa. I VPC condivisi sono desiderabili per installazioni di grandi dimensioni, perché forniscono controllo, utilizzo e amministrazione centralizzati delle risorse aziendali condivise di Google Cloud. Per ulteriori informazioni, consultare il sito della documentazione di Google.

Con questa funzionalità, Machine Creation Services (MCS) supporta il provisioning e la gestione dei cataloghi delle macchine distribuiti su VPC condivisi. Questo supporto, che dal punto di vista funzionale è equivalente al supporto attualmente fornito nei VPC locali, si differenzia sotto due aspetti:

1. È necessario concedere autorizzazioni aggiuntive all'account di servizio utilizzato per creare la connessione host. Questo processo consente a MCS di accedere e utilizzare le risorse VPC condivise.
2. È necessario creare due regole firewall, una per l'ingresso e una per l'uscita. Queste regole firewall vengono utilizzate durante il processo di mastering delle immagini.

#### Sono necessarie nuove autorizzazioni

Per la creazione della connessione host è necessario un account di servizio Google Cloud con autorizzazioni specifiche. Queste autorizzazioni aggiuntive devono essere concesse a tutti gli account di servizio utilizzati per creare connessioni host basate su VPC condivisi.

> **Suggerimento:**
>
> Queste autorizzazioni aggiuntive non sono nuove in Citrix DaaS. Sono utilizzate per facilitare l'implementazione di VPC locali. Con i VPC condivisi, queste autorizzazioni aggiuntive consentono l'accesso ad altre risorse VPC condivise.

È necessario concedere un massimo di quattro autorizzazioni aggiuntive all'account di servizio associato alla connessione host per supportare i VPC condivisi:

1. **compute.firewalls.list**: questa autorizzazione è obbligatoria. Consente a MCS di recuperare l'elenco delle regole firewall presenti nel VPC condiviso.
2. **compute.networks.list**: questa autorizzazione è obbligatoria. Consente a MCS di identificare le reti VPC condivise disponibili per l'account di servizio.
3. **compute.subnetworks.list**: questa autorizzazione è facoltativa, a seconda di come si utilizzano i VPC. Consente a MCS di identificare le subnet all'interno dei VPC condivisi visibili. Questa

autorizzazione è già richiesta quando si utilizzano VPC locali, ma deve essere assegnata anche nel progetto host del VPC condiviso.

4. **compute.subnetworks.use**: questa autorizzazione è facoltativa, a seconda di come si utilizzano i VPC. È necessario utilizzare le risorse di subnet nei cataloghi delle macchine di cui è stato eseguito il provisioning. Questa autorizzazione è già necessaria per l'utilizzo di VPC locali, ma deve essere assegnata anche nel progetto host del VPC condiviso.

Quando si utilizzano queste autorizzazioni, tenere presente che esistono diversi approcci in base al tipo di autorizzazione utilizzato per creare il catalogo delle macchine:

- Autorizzazione a livello di progetto:
  - Consente l'accesso a tutti i VPC condivisi all'interno del progetto host.
  - Richiede che le autorizzazioni 3 e 4 vengano assegnate all'account di servizio.
- Autorizzazione a livello di subnet:
  - Consente l'accesso a subnet specifiche all'interno del VPC condiviso.
  - Le autorizzazioni 3 e 4 sono intrinseche all'assegnazione a livello di subnet e quindi non devono essere assegnate direttamente all'account di servizio.

Selezionare l'approccio più adatto alle esigenze e agli standard di sicurezza della propria azienda.

> **Suggerimento:**
>
> Per ulteriori informazioni sulle differenze tra le autorizzazioni a livello di progetto e di subnet, consultare la documentazione di Google Cloud.

#### Regole firewall

Durante la preparazione di un catalogo delle macchine, viene preparata un'immagine della macchina che funge da disco di sistema dell'immagine master per il catalogo. Quando si verifica questo processo, il disco viene temporaneamente collegato a una macchina virtuale. Questa macchina virtuale deve essere eseguita in un ambiente isolato che impedisca tutto il traffico di rete in entrata e in uscita. Ciò si ottiene attraverso una coppia di regole firewall "nega tutto", una per il traffico in ingresso e una per il traffico in uscita. Quando si utilizzano i VCP locali di Google Cloud, MCS crea questo firewall nella rete locale e lo applica alla macchina per il mastering. Al termine del mastering, la regola firewall viene rimossa dall'immagine.

Si consiglia di ridurre al minimo il numero di nuove autorizzazioni necessarie per utilizzare i VPC condivisi. I VPC condivisi sono risorse aziendali di livello superiore e in genere dispongono di protocolli di sicurezza più rigidi. Per questo motivo, è necessario creare una coppia di regole firewall nel progetto host sulle risorse VPC condivise, una per l'ingresso e una per l'uscita. Assegnare a tali regole la massima priorità. Applicare un nuovo tag di destinazione a ciascuna di queste regole, utilizzando il valore seguente:

`citrix-provisioning-quarantine-firewall`

Quando MCS crea o aggiorna un catalogo delle macchine, cerca le regole del firewall contenenti questo tag di destinazione. Quindi esamina le regole per verificarne la correttezza e le applica alla macchina utilizzata per preparare l'immagine master per il catalogo. Se le regole firewall non vengono trovate o le regole vengono trovate ma non sono corrette (o le relative priorità non sono corrette), viene visualizzato un messaggio simile al seguente:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag ‘citrix-provisioning-
quarantine-firewall'and proper priority." "Refer to Citrix Documentation
 for details."
```

#### Configurazione del VPC condiviso

Prima di aggiungere il VPC condiviso come connessione host nell'interfaccia Full Configuration (Configurazione completa) in Citrix DaaS, completare i seguenti passaggi per aggiungere account di servizio dal progetto in cui si intende effettuare il provisioning:

1. Creare un ruolo IAM.
2. Aggiungere l'account di servizio utilizzato per creare una connessione host CVAD al ruolo IAM del progetto host del VPC condiviso.
3. Aggiungere l'account di servizio Cloud Build dal progetto di cui si intende eseguire il provisioning al ruolo IAM del progetto host del VPC condiviso.
4. Creare regole firewall.

**Creare un ruolo IAM** Determinare il livello di accesso del ruolo: *accesso a livello di progetto* o un modello più limitato utilizzando l'*accesso a livello di subnet*.

**Accesso a livello di progetto per il ruolo IAM**. Per il ruolo IAM a livello di progetto, includere le seguenti autorizzazioni:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Per creare un ruolo IAM a livello di progetto:

1. Nella console di Google Cloud, andare a **IAM e amministrazione > Ruoli**.
2. Nella pagina **Ruoli**, selezionare **CREA RUOLO**.

3. Nella pagina **Crea ruolo**, specificare il nome del ruolo. Selezionare **AGGIUNGI AUTORIZZAZIONI**.

    a) Nella pagina **Aggiungi autorizzazioni**, aggiungere le autorizzazioni al ruolo, singolarmente. Per aggiungere un'autorizzazione, digitare il nome dell'autorizzazione nel campo **Filtra tabella**. Selezionare l'autorizzazione e quindi selezionare **AGGIUNGI**.
    b) Selezionare **CREA**.

**Ruolo IAM a livello di subnet**. Questo ruolo omette l'aggiunta delle autorizzazioni `compute.subnetworks.list` e `compute.subnetworks.use` dopo aver selezionato **CREA RUOLO**. Per questo livello di accesso IAM, le autorizzazioni `compute.firewalls.list` e `compute.networks.list` devono essere applicate al nuovo ruolo.

Per creare un ruolo IAM a livello di subnet:

1. Nella console di Google Cloud, andare a **Rete VPC** > **VPC condiviso**. Viene visualizzata la pagina **VPC condiviso**, in cui sono visualizzate le subnet delle reti VPC condivise contenute nel progetto host.
2. Nella pagina **VPC condiviso**, selezionare la subnet a cui si desidera accedere.
3. Nell'angolo in alto a destra, selezionare **AGGIUNGI MEMBRO** per aggiungere un account di servizio.
4. Nella pagina **Aggiungi membri**, completare questi passaggi:

    a) Nel campo **Nuovi membri**, digitare il nome del proprio account di servizio e quindi selezionare l'account di servizio nel menu.
    b) Selezionare il campo **Seleziona un ruolo** e quindi **Utente di rete Compute**.
    c) Selezionare **SALVA**.

5. Nella console di Google Cloud, andare a **IAM e amministrazione** > **Ruoli**.
6. Nella pagina **Ruoli**, selezionare **CREA RUOLO**.
7. Nella pagina **Crea ruolo**, specificare il nome del ruolo. Selezionare **AGGIUNGI AUTORIZZAZIONI**.

    a) Nella pagina **Aggiungi autorizzazioni**, aggiungere le autorizzazioni al ruolo, singolarmente. Per aggiungere un'autorizzazione, digitare il nome dell'autorizzazione nel campo **Filtra tabella**. Selezionare l'autorizzazione, quindi seleziona **AGGIUNGI**.
    b) Selezionare **CREA**.

**Aggiungere un account di servizio al ruolo IAM del progetto host** Dopo aver creato un ruolo IAM, per aggiungere un account di servizio per il progetto host, procedere come segue:

1. Nella console di Google Cloud, accedere al progetto host e quindi a **IAM e amministrazione > IAM**.
2. Nella pagina **IAM**, selezionare **AGGIUNGI** per aggiungere un account di servizio.

3. Nella pagina **Aggiungi membri**:

    a) Nel campo **Nuovi membri**, digitare il nome del proprio account di servizio e quindi selezionare l'account di servizio nel menu.
    b) Selezionare un campo ruolo, digitare il ruolo IAM creato e quindi selezionare il ruolo nel menu.
    c) Selezionare **SALVA**.

L'account di servizio è ora configurato per il progetto host.

**Aggiungere l'account del servizio di compilazione cloud al VPC condiviso** Ogni sottoscrizione a Google Cloud ha un account di servizio che prende il nome dal numero ID del progetto, seguito da `cloudbuild.gserviceaccount`. Ad esempio: `705794712345@cloudbuild.gserviceaccount`.

È possibile determinare qual è il numero ID del progetto per il proprio progetto selezionando **Home page** e **Dashboard** nella console di Google Cloud:

Trovare il **numero del progetto** sotto l'area **Informazioni sul progetto** dello schermo.

Eseguire i seguenti passaggi per aggiungere l'account del servizio Cloud Build al VPC condiviso:

1. Nella console di Google Cloud, accedere al progetto host e quindi a **IAM e amministrazione** > **IAM**.
2. Nella pagina **Autorizzazioni**, selezionare **AGGIUNGI** per aggiungere un account.
3. Nella pagina **Aggiungi membri**, completare questi passaggi:

    a) Nel campo **Nuovi membri**, digitare il nome dell'account di servizio Cloud Build, quindi selezionare il proprio account di servizio nel menu.
    b) Selezionare il campo **Seleziona un ruolo**, digitare `Computer Network User`, quindi selezionare il ruolo nel menu.
    c) Selezionare **SALVA**.

**Creare regole firewall** Come parte del processo di mastering, MCS copia l'immagine della macchina selezionata e la utilizza per preparare il disco di sistema dell'immagine master per il catalogo. Durante il processo di mastering, MCS collega il disco a una macchina virtuale temporanea, che in seguito esegue gli script di preparazione. Questa macchina virtuale deve essere eseguita in un ambiente isolato che vieti tutto il traffico di rete in entrata e in uscita. Per creare un ambiente isolato, MCS richiede due regole firewall *"nega tutto"* (una regola di ingresso e una regola di uscita). Pertanto, creare due regole firewall nel *progetto host* come segue:

1. Nella console di Google Cloud, andare al progetto host e quindi a **Rete VPC > Firewall**.
2. Nella pagina **Firewall**, selezionare **CREA REGOLA FIREWALL**.

3. Nella pagina **Crea una regola firewall**, completare quanto segue:
    - **Name**. Digitare un nome per la regola.
    - **Rete**. Selezionare la rete VPC condivisa a cui applicare la regola firewall in ingresso.
    - **Priorità**. Più piccolo è il valore, maggiore è la priorità della regola. Si consiglia un valore piccolo (ad esempio, 10).
    - **Direzione del traffico**. Selezionare **In entrata**.
    - **Azione in caso di corrispondenza**. Selezionare **Nega**.
    - **Destinazioni**. Utilizzare l'opzione predefinita, **Tag di destinazione specificati**.
    - **Tag di destinazione**. Digitare `citrix-provisioning-quarantine-firewall`.
    - **Filtro di origine**. Utilizzare l'opzione predefinita, **Intervalli IP**.
    - **Intervalli IP di origine**. Digitare un intervallo che corrisponda a tutto il traffico. Digitare `0.0.0.0/0`.
    - **Protocolli e porte**. Selezionare **Nega tutto**.
4. Selezionare **CREA** per creare la regola.
5. Ripetere i passaggi da 1 a 4 per creare un'altra regola. Per **Direzione del traffico**, selezionare **In uscita**.

**Aggiungere una connessione** Dopo aver aggiunto le interfacce di rete all'istanza di Cloud Connector, aggiungere una connessione.

### Abilitare la selezione delle zone

Citrix DaaS supporta la selezione delle zone. Con la selezione delle zone, è possibile specificare le zone in cui si desidera creare macchine virtuali. Con la selezione delle zone, gli amministratori possono posizionare nodi single-tenant nelle zone di loro scelta. Per configurare la single-tenancy, è necessario completare quanto segue su Google Cloud:

- Prenotare un nodo single-tenant di Google Cloud
- Creare l'immagine master del VDA

#### Prenotazione di un nodo single-tenant di Google Cloud

Per prenotare un nodo single-tenant, consultare la documentazione di Google Cloud.

> **Importante:**
>
> Un modello di nodo viene utilizzato per indicare le caratteristiche prestazionali del sistema riservato nel gruppo di nodi. Tali caratteristiche includono il numero di vGPU, la quantità di memoria allocata al nodo e il tipo di macchina utilizzato per le macchine create sul nodo. Per ulteriori

> informazioni, consultare la documentazione di Google Cloud.

#### Creazione dell'immagine master VDA

Per distribuire correttamente le macchine sul nodo single-tenant, è necessario eseguire ulteriori passaggi durante la creazione di un'immagine master della macchina virtuale. Le istanze delle macchine su Google Cloud hanno una proprietà chiamata *etichette di affinità nodo*. Le istanze utilizzate come immagini master per i cataloghi distribuiti nel nodo single-tenant richiedono un'*etichetta di affinità nodo* che corrisponda al nome del **gruppo di nodi di destinazione**. Per raggiungere questo obiettivo, tenere presente quanto segue:

- Per una nuova istanza, impostare l'etichetta nella console di Google Cloud quando si crea un'istanza. Per informazioni dettagliate, consultare Impostare un'etichetta di affinità nodo durante la creazione di un'istanza.
- Per un'istanza esistente, impostare l'etichetta usando la riga di comando **gcloud**. Per informazioni dettagliate, consultare Impostare un'etichetta di affinità nodo per un'istanza esistente.

> **Nota:**
>
> Se si intende utilizzare la single-tenancy con un VPC condiviso, consultare Cloud privato virtuale condiviso.

**Impostare un'etichetta di affinità nodo durante la creazione di un'istanza** Per impostare l'etichetta di affinità nodo:

1. Nella console di Google Cloud, andare a **Compute Engine > Istanze VM**.
2. Nella pagina **Istanze VM**, selezionare **Crea istanza**.
3. Nella pagina **Creazione istanza**, digitare o configurare le informazioni richieste e quindi selezionare **Gestione, sicurezza, dischi, networking, single-tenancy** per aprire il pannello delle impostazioni.
4. Nella scheda **Single-tenancy**, selezionare **Sfoglia** per visualizzare i gruppi di nodi disponibili nel progetto corrente. Viene visualizzata la pagina **Nodo single-tenant**, che mostra un elenco dei gruppi di nodi disponibili.
5. Nella pagina **Nodo single-tenant**, selezionare il gruppo di nodi applicabile dall'elenco, quindi selezionare **Seleziona** per tornare alla scheda **Single-tenancy**. Il campo delle etichette di affinità nodo viene compilato con le informazioni selezionate. Questa impostazione garantisce che i cataloghi delle macchine creati dall'istanza vengano distribuiti nel gruppo di nodi selezionato.
6. Selezionare **Crea** per creare l'istanza.

**Impostare un'etichetta di affinità nodo per un'istanza esistente** Per impostare l'etichetta di affinità nodo:

1. Nella finestra del terminale di Google Cloud Shell, utilizzare il comando *gcloud compute instances* per impostare un'etichetta di affinità nodo. Includere le seguenti informazioni nel comando **gcloud**:

   - **Nome della macchina virtuale**. Ad esempio, utilizzare una macchina virtuale esistente denominata `s*2019-vda-base`.*
   - **Nome del gruppo di nodi**. Utilizzare il nome del gruppo di nodi creato in precedenza. Ad esempio, `mh-sole-tenant-node-group-1`.
   - **La zona in cui risiede l'istanza**. Ad esempio, la macchina virtuale risiede nella zona `*us-east-1b* zone`.

   Ad esempio, digitare il seguente comando nella finestra del terminale:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   Per ulteriori informazioni sul comando *gcloud compute instances*, consultare la documentazione di Google Developer Tools all'indirizzo https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Passare alla pagina **Dettagli istanza VM** dell'istanza e verificare che il campo **Affinità del nodo** venga compilato con l'etichetta.

**Creare un catalogo di macchine** Dopo aver impostato l'etichetta di affinità nodo, configurare il catalogo delle macchine.

### Utilizzare le chiavi di crittografia gestite dal cliente (CMEK)

È possibile utilizzare le chiavi di crittografia gestite dal cliente (CMEK) per i cataloghi MCS. Quando si utilizza questa funzionalità, si assegna il ruolo `CryptoKey Encrypter/Decrypter` di Google Cloud Key Management Service all'agente del servizio Compute Engine. L'account Citrix DaaS deve disporre delle autorizzazioni corrette nel progetto in cui è memorizzata la chiave. Per ulteriori informazioni, consultare Aiutare a proteggere le risorse utilizzando le chiavi di Cloud KMS.

L'agente del servizio Compute Engine ha il seguente formato: `service-<Project _Number>@compute-system.iam.gserviceaccount.com`. Questo formato è diverso dall'account predefinito del servizio Compute Engine.

> **Nota:**
>
> Questo account del servizio Compute Engine potrebbe non essere visualizzato nella schermata **IAM/Autorizzazioni** di Google Cloud Console. In questi casi, utilizzare il comando `gcloud` come descritto in Aiutare a proteggere le risorse utilizzando le chiavi di Cloud KMS.

#### Assegnazione delle autorizzazioni all'account Citrix DaaS

Le autorizzazioni di Google Cloud KMS possono essere configurate in vari modi. È possibile fornire autorizzazioni KMS a *livello di progetto* o autorizzazioni KMS *a livello di risorsa*. Vedere Autorizzazioni e ruoli per ulteriori informazioni.

**Autorizzazioni a livello di progetto** Un'opzione è fornire all'account Citrix DaaS autorizzazioni a livello di progetto per esplorare le risorse di Cloud KMS. A tale scopo, creare un ruolo personalizzato e aggiungere le seguenti autorizzazioni:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Assegnare questo ruolo personalizzato all'account Citrix DaaS. Questo consente di sfogliare le chiavi regionali nel progetto pertinente nell'inventario.

**Autorizzazioni a livello di risorsa** Per l'altra opzione, le autorizzazioni a livello di risorsa, nella console di Google Cloud selezionare la `cryptoKey` utilizzata per il provisioning MCS. Aggiungere un account Citrix DaaS a un portachiavi o a una chiave utilizzata per il provisioning del catalogo.

> **Suggerimento:**
>
> Con questa opzione non è possibile sfogliare le chiavi regionali per il progetto nell'inventario perché l'account Citrix DaaS non dispone delle autorizzazioni elenco a livello di progetto per le risorse Cloud KMS. Tuttavia, è comunque possibile eseguire il provisioning di un catalogo utilizzando CMEK specificando l'`cryptoKeyId` nelle proprietà personalizzate `ProvScheme`, come descritto di seguito.

#### Provisioning con CMEK utilizzando le proprietà personalizzate

Quando si crea lo schema di provisioning tramite PowerShell, specificare una proprietà `CryptoKeyId` in `ProvScheme CustomProperties`. Ad esempio:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
       yourCryptoKeyId>" />
</CustomProperties>'
<!--NeedCopy-->
```

L'`cryptoKeyId` deve essere specificato nel seguente formato:

`projectId:location:keyRingName:cryptoKeyName`

Ad esempio, se si desidera utilizzare la chiave `my-example-key` nel keyring `my-example-key-ring` nella regione `us-east1` e nel progetto con ID `my-example-project-1`, le impostazioni personalizzate `ProvScheme` saranno simili a:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
       example-project-1:us-east1:my-example-key-ring:my-example-key"
       />
</CustomProperties>'
<!--NeedCopy-->
```

Tutti i dischi e le immagini di cui è stato eseguito il provisioning tramite MCS relativi a questo schema di provisioning utilizzano questa chiave di crittografia gestita dal cliente.

> **Suggerimento:**
>
> Se si utilizzano le chiavi globali, la posizione delle proprietà del cliente deve indicare `global` e non il nome della **regione**, che nell'esempio precedente è **us-east1**. Ad esempio: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

#### Rotazione delle chiavi gestite dal cliente

Google Cloud non supporta la rotazione delle chiavi su dischi o immagini persistenti esistenti. Una volta eseguito il provisioning di una macchina, questa viene associata alla versione della chiave in uso al momento della creazione. Tuttavia, è possibile creare una nuova versione della chiave e tale nuova chiave viene utilizzata per le macchine o le risorse di cui è stato recentemente eseguito il provisioning create quando un catalogo viene aggiornato con una nuova immagine master.

**Considerazioni importanti sui keyring** I keyring non possono essere rinominati o eliminati. Inoltre, si potrebbero ricevere addebiti imprevisti quando vengono configurati. Quando si elimina o si rimuove un keyring, Google Cloud visualizza un messaggio di errore:

```
Sorry, you can't delete or rename keys or key rings. We were concerned about the security implications of allowing multiple keys or key versions over time to have the same resource name, so we decided to make names immutable. (And you can't delete them, because we wouldn't be able to do a true deletion--there would still have to be a tombstone tracking that this name had been used and couldn't be reused).
We're aware that this can make things untidy, but we have no immediate plans to change this.
If you want to avoid getting billed for a key or otherwise make it unavailable, you can do so by deleting all the key versions; neither keys nor key rings are billed for, just the active key versions within the keys.
<!--NeedCopy-->
```

> **Suggerimento:**
>
> Per ulteriori informazioni, consultare Modificare o eliminare un keyring dalla console.

### Compatibilità dell'accesso uniforme a livello di bucket

Citrix DaaS è compatibile con criteri uniformi di controllo degli accessi a livello di bucket su Google Cloud. Questa funzionalità espande l'uso del criterio IAM che concede autorizzazioni a un account di servizio per consentire la manipolazione delle risorse, inclusi i bucket di archiviazione. Con un controllo dell'accesso uniforme a livello di bucket, Citrix DaaS consente di utilizzare un elenco di controllo degli accessi (ACL) per controllare l'accesso ai bucket di archiviazione o agli oggetti memorizzati in essi. Consultare Accesso uniforme a livello di bucket per informazioni generali sull'accesso uniforme a livello di bucket di Google Cloud. Per informazioni sulla configurazione, vedere Richiedere un accesso uniforme a livello di bucket.

### Google Cloud Marketplace

È possibile sfogliare e selezionare le immagini offerte da Citrix su Google Cloud Marketplace per creare cataloghi di macchine. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità.

Per cercare il prodotto Citrix VDA VM tramite Google Cloud Marketplace, accedere a https://console.cloud.google.com/marketplace/.

È possibile utilizzare un'immagine personalizzata o un'immagine Citrix Ready su Google Cloud Marketplace per aggiornare l'immagine di un catalogo di macchine.

> **Nota:**
>
> Se il profilo della macchina non contiene informazioni sul tipo di archiviazione, il valore viene

> derivato da proprietà personalizzate.

Le immagini supportate da Google Cloud Marketplace sono:

- Windows 2019 a sessione singola
- Windows 2019 multisessione
- Ubuntu

Esempio di utilizzo di un'immagine pronta per Citrix come fonte per la creazione di un catalogo di macchine:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Google Cloud Platform.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione agli ambienti cloud di Google
- Creare cataloghi di macchine

## Creare un catalogo di macchine di HPE Moonshot (anteprima)

December 5, 2023

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano dettagli specifici degli ambienti HPE Moonshot.

> **Nota:**
>
> - Creare una connessione a HPE Moonshot
> - Assicurarsi di avere uno o più nodi HPE Moonshot disponibili e installare i VDA su tali nodi.
> - Per informazioni sulla creazione dell'immagine iniziale della cartuccia HPE Moonshot, consultare la Guida per l'utente OS Deployment on Moonshot User Guide.

È possibile creare un catalogo di macchine di HPE Moonshot utilizzando:

- Interfaccia Full Configuration
- Comandi PowerShell

### Creare un catalogo di macchine utilizzando l'interfaccia Full Configuration

Nella procedura guidata **Machine Catalog Setup** (Configurazione del catalogo macchine):

1. Nella pagina **Operating System** (Sistema operativo) selezionare **Multi-session OS** (Sistema operativo a sessione singola) o **Single-session OS** (Sistema operativoa sessione singola).
2. Nella pagina **Machine Management** (Gestione macchine), selezionare **Machines that are power managed** (Macchine con alimentazione gestita) e **Another service or technology** (Altro servizio o tecnologia).
3. Nella pagina **Virtual Machines** (Macchine virtuali), aggiungere le macchine e i relativi account macchina di Active Directory. È possibile effettuare una delle seguenti operazioni:
   - Fare clic su **Add Machines** (Aggiungi macchine) per aggiungere le macchine manualmente. Viene visualizzata la finestra **Select VMs** (Seleziona macchine virtuali). Espandere la connessione allo chassis HPE Moonshot creato in precedenza e seleziona i nodi (VM) che desideri aggiungere. Quindi aggiungere i nomi degli account delle macchine associate.
   - Fare clic su **Add CSV File** (Aggiungi file CSV) per aggiungere macchine in blocco. Per informazioni sull'utilizzo dei file CSV per aggiungere macchine, vedere Utilizzare i file CSV per aggiungere macchine in blocco a un catalogo.

Le pagine **Scopes** (Ambiti) e **Summary** (Riepilogo) non contengono informazioni specifiche su HPE Moonshot.

### Creare un catalogo di macchine usando i comandi PowerShell

Eseguire i comandi PowerShell `New-BrokerCatalog` e `New-BrokerMachine` per creare un catalogo di broker e importare macchine nel catalogo del broker.

Ad esempio:

```
New-BrokerCatalog  -AdminAddress "localhost:19097" -AdminClientIP "
    103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
    MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
    BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
    Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
    -4578-bc07-bcf2a82d1463"
New-BrokerMachine  -AdminAddress "localhost:19097" -AdminClientIP "
    103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1" -
    HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
    -1-5-21-2589939477-3963209805-1860259709-1121"
<!--NeedCopy-->
```

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di HPE Moonshot.

### Ulteriori informazioni

- Creare e gestire le connessioni
- Connessione a HPE Moonshot
- Creare cataloghi di macchine

## Creare un catalogo di Microsoft Azure

December 20, 2023

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Microsoft Azure Resource Manager.

> **Nota:**
>
> Prima di creare un catalogo di Microsoft Azure, è necessario completare la creazione di una connessione a Microsoft Azure. Vedere Connessione a Microsoft Azure.

### Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager

Le seguenti informazioni sono un'aggiunta alle linee guida della sezione Creare cataloghi delle macchine.

Un'immagine può essere un disco, una snapshot o una versione immagine di una definizione di immagine all'interno della Raccolta di calcolo di Azure utilizzata per creare le macchine virtuali in un catalogo di macchine. Prima di creare il catalogo delle macchine, creare un'immagine in Azure Resource Manager. Per informazioni generali sulle immagini, vedere Creare cataloghi delle macchine.

> **Suggerimento:**
>
> L'uso di un disco non gestito per il provisioning delle macchine virtuali è obsoleto.

Durante la preparazione dell'immagine, viene creata una macchina virtuale (VM) di preparazione basata sulla macchina virtuale originale. Questa macchina virtuale di preparazione è disconnessa dalla rete. Per disconnettere la rete dalla macchina virtuale di preparazione, viene creato un gruppo di sicurezza di rete per negare tutto il traffico in entrata e in uscita. Il gruppo di sicurezza di rete viene creato automaticamente una volta per catalogo. Il nome del gruppo di sicurezza di rete è `Citrix-Deny-All-a3pgu-GUID`, dove il GUID viene generato casualmente. Ad esempio, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

Nella procedura guidata di creazione del catalogo delle macchine:

- Le pagine **Machine Type** (Tipo di macchina) e **Machine Management** (Gestione macchina) non contengono informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Master Image** (Immagine master), selezionare un'immagine da utilizzare come immagine mater per tutte le macchine del catalogo. Viene visualizzata la procedura guidata **Select an image** (Seleziona un'immagine). Seguire questi passaggi per selezionare un'immagine:

  1. (Applicabile solo alle connessioni configurate con immagini condivise all'interno di uno stesso tenant o tra tenant diversi) Selezionare un abbonamento in cui risiede l'immagine.
  2. Selezionare un gruppo di risorse.
  3. Passare ad Azure VHD, alla Raccolta di calcolo di Azure o alla versione immagine di Azure.

  Quando selezionate un'immagine, tenere presente quanto segue:

  - Verificare che sull'immagine sia installato un Citrix VDA.
  - Se si seleziona un disco rigido virtuale collegato a una macchina virtuale, è necessario spegnere la VM prima di procedere al passaggio successivo.

**Nota:**

- La sottoscrizione corrispondente alla connessione (host) che ha creato le macchine nel catalogo è contrassegnata da un punto verde. Le altre sottoscrizioni sono quelle con Raccolta di calcolo di Azure condivisa con quella sottoscrizione. In queste sottoscrizioni vengono mostrate solo le gallerie condivise. Per informazioni su come configurare gli abbonamenti condivisi, vedere Condividere immagini all'interno di un tenant (tra abbonamenti) e Condividere immagini tra tenant.
- L'uso di un profilo macchina con un avvio attendibile quale **Security Type** (Tipo di sicurezza) è obbligatorio quando si seleziona un'immagine o una snapshot con avvio attendibile abilitato. È quindi possibile abilitare o disabilitare SecureBoot e vTPM specificandone i valori nel profilo macchina. Per informazioni sull'avvio attendibile di Azure, vedere https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
- È possibile creare uno schema di provisioning utilizzando il disco del sistema operativo temporaneo su Windows con avvio attendibile. Quando si seleziona un'immagine con avvio attendibile, è necessario selezionare un profilo macchina con avvio attendibile abilitato con vTPM. Per creare cataloghi delle macchine utilizzando un disco del sistema operativo temporaneo, vedere Come creare macchine utilizzando dischi del sistema operativo temporanei.
- Quando è in corso la replica dell'immagine, è possibile procedere e selezionare l'immagine come immagine master e completare la configurazione. Tuttavia, il completamento della creazione del catalogo potrebbe richiedere più tempo durante la replica dell'immagine. MCS richiede che la replica venga completata entro un'ora a partire dalla creazione del catalogo. In caso di timeout della replica, la creazione del catalogo non riesce. È possibile verificare lo stato della replica in Azure. Riprovare se la replica è ancora in sospeso o dopo il completamento della replica.
- Quando si seleziona un'immagine master per i cataloghi di macchine in Azure, il profilo della macchina viene filtrato in base all'immagine master selezionata. Ad esempio, il profilo del computer viene filtrato in base al sistema operativo Windows, al tipo di sicurezza, al supporto per l'ibernazione e all'ID del set di crittografia del disco dell'immagine master.
- È possibile effettuare il provisioning di un catalogo di macchine virtuali Gen2 utilizzando un'immagine Gen2 per migliorare le prestazioni in fase di avvio. Tuttavia, la creazione di un catalogo di macchine Gen2 utilizzando un'immagine Gen1 non è supportata. Allo stesso modo, non è supportata la creazione di un catalogo di macchine Gen1 utilizzando un'immagine Gen2. Inoltre, qualsiasi immagine precedente che non contiene informazioni sulla generazione è un'immagine Gen1.

Scegliere se le VM del catalogo debbano ereditare le configurazioni da un profilo macchina. Per impostazione predefinita, la casella di controllo **Use a machine profile (mandatory for Azure**

**Active Directory)** [Usa un profilo macchina (obbligatoria per Azure Active Directory)] è selezionata. Fare clic su **Select a machine profile** (Seleziona un profilo macchina) per accedere a una VM o a una specifica di modello ARM da un elenco di gruppi di risorse.

Convalidare la specifica del modello ARM per accertarsi che possa essere utilizzata come profilo macchina per creare un catalogo delle macchine. Per informazioni sulla creazione di una specifica del modello di Azure, vedere Creare una specifica del modello di Azure. Esistono due modi per convalidare la specifica di modello ARM:

- Dopo aver selezionato la specifica del modello ARM dall'elenco dei gruppi di risorse, fare clic su **Next** (Avanti). Se la specifica del modello ARM contiene errori, vengono visualizzati messaggi di errore.
- Eseguire uno dei seguenti comandi PowerShell:
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  * `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

  Ad esempio:

```
1  Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet" -
       InventoryPath machineprofile.folder/vdi01-d-rg.
       resourcegroup/VDD-templ-spec.templatespec/1.5.
       templatespecversion
2  <!--NeedCopy-->
```

Alcuni esempi di configurazioni che le macchine virtuali possono ereditare da un profilo macchina includono:

- Networking accelerato
- Diagnostica di avvio
- Memorizzazione nella cache del disco host (relativa ai dischi del sistema operativo e MCSIO)
- Dimensioni della macchina (se non diversamente specificato)
- Tag posizionati sulla macchina virtuale

Dopo aver creato il catalogo, è possibile visualizzare le configurazioni che l'immagine eredita dal profilo della macchina. Nel nodo **Machine Catalogs** (Cataloghi delle macchine), selezionare il catalogo per visualizzare i relativi dettagli nel riquadro inferiore. Quindi, fare clic sulla scheda **Template Properties** (Proprietà modello) per visualizzare le proprietà del profilo della macchina. La sezione **Tags** (Tag) visualizza fino a tre tag. Per visualizzare tutti i tag posizionati sulla macchina virtuale, fare clic su **View all** (Visualizza tutto).

Se si desidera che MCS esegua il provisioning delle macchine virtuali in un host dedicato di

Azure, abilitare la casella di controllo **Use a host group** (Utilizza un gruppo host) e quindi selezionare un gruppo host dall'elenco. Un gruppo di host è una risorsa che rappresenta una raccolta di host dedicati. Un host dedicato è un servizio che fornisce server fisici che ospitano una o più macchine virtuali. Il server dedicato alla sottoscrizione di Azure non è condiviso con altri sottoscrittori. Quando si utilizza un host dedicato, Azure garantisce che le macchine virtuali siano le uniche macchine in esecuzione su quell'host. Questa funzionalità è adatta per gli scenari in cui è necessario soddisfare i requisiti normativi o di sicurezza interni. Per ulteriori informazioni sui gruppi di host e sulle considerazioni per il loro utilizzo, vedere Host dedicati di Azure.

> **Importante:**
>
> – Vengono visualizzati solo i gruppi di host per i quali è abilitato il posizionamento automatico di Azure.
> – L'utilizzo di un gruppo host modifica la pagina **Virtual Machines** (Macchine virtuali) mostrata più avanti nella procedura guidata. In questa pagina vengono mostrate solo le dimensioni delle macchine contenute nel gruppo host selezionato. Inoltre, le zone di disponibilità vengono selezionate automaticamente e non sono disponibili per la selezione.

- La pagina **Storage and License Types** (Tipi di archiviazione e licenze) viene visualizzata solo quando si utilizza un'immagine di Azure Resource Manager.

  Sono disponibili i seguenti tipi di archiviazione da utilizzare per il catalogo delle macchine:

  – **SSD premium**. Offre un'opzione di archiviazione su disco ad alte prestazioni e a bassa latenza adatta per macchine virtuali con carichi di lavoro a uso intensivo di I/O.
  – **SSD standard**. Offre un'opzione di archiviazione conveniente adatta a carichi di lavoro che richiedono prestazioni costanti a livelli di IOPS inferiori.
  – **HDD standard**. Offre un'opzione di archiviazione su disco affidabile e a basso costo adatta per macchine virtuali che eseguono carichi di lavoro non sensibili alla latenza.
  – **Disco del sistema operativo temporaneo di Azure**. Offre un'opzione di archiviazione conveniente che riutilizza il disco locale delle macchine virtuali per ospitare il disco del sistema operativo. In alternativa, è possibile utilizzare PowerShell per creare macchine che utilizzano dischi dei sistemi operativi temporanei. Per ulteriori informazioni, vedere Dischi temporanei di Azure. Tenere presenti le seguenti considerazioni quando si utilizza un disco del sistema operativo temporaneo:

    * Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.
    * Per aggiornare le macchine che utilizzano dischi dei sistemi operativi temporanei, è necessario selezionare un'immagine la cui dimensione non superi la dimensione del disco della cache o del disco temporaneo della macchina virtuale.

* Non è possibile utilizzare l'opzione **Retain VM and system disk during power cycles** (Conserva la VM e il disco di sistema durante i cicli di alimentazione) disponibile più avanti nella procedura guidata.

> **Nota:**
>
> Il disco di identità viene sempre creato utilizzando SSD standard indipendentemente dal tipo di archiviazione scelto.

Il tipo di archiviazione determina le dimensioni delle macchine disponibili nella pagina **Virtual Machines** (Macchine virtuali) della procedura guidata. MCS configura dischi premium e standard per l'utilizzo dell'archiviazione con ridondanza locale (LRS). LRS esegue più copie sincrone dei dati del disco all'interno di un singolo centro dati. I dischi del sistema operativo temporaneo di Azure utilizzano il disco locale delle macchine virtuali per archiviare il sistema operativo. Per informazioni dettagliate sui tipi di archiviazione di Azure e sulla replica dell'archiviazione, vedere quanto segue:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Selezionare se utilizzare le licenze Windows o Linux esistenti.

- Licenze Windows: l'utilizzo di licenze Windows insieme a immagini Windows (immagini di supporto o immagini personalizzate della piattaforma Azure) consente di eseguire macchine virtuali Windows in Azure a un costo ridotto. Esistono due tipi di licenze:
  * **Licenza Windows Server**. Consente di utilizzare le licenze Windows Server o Azure Windows Server, consentendo l'utilizzo dei Vantaggi di Azure ibrido. Per i dettagli, vedere https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. I vantaggi di Azure ibrido riducono il costo di esecuzione delle macchine virtuali in Azure alla tariffa di elaborazione di base, eliminando il costo delle licenze aggiuntive di Windows Server dalla raccolta di Azure.
  * **Licenza client Windows**. Consente di trasferire le licenze di Windows 10 e Windows 11 in Azure, consentendo di eseguire macchine virtuali Windows 10 e Windows 11 in Azure senza la necessità di licenze aggiuntive. Per i dettagli, vedere Licenze di accesso client e licenze di gestione.

È possibile verificare che la macchina virtuale di cui è stato eseguito il provisioning stia utilizzando il vantaggio di licenza eseguendo il seguente comando PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Per il tipo di licenza Windows Server, verificare che il tipo di licenza sia **Windows_Server**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Per il tipo di licenza client Windows, verificare che il tipo di licenza sia **Windows_Client**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

In alternativa, è possibile utilizzare l'SDK PowerShell `Get-Provscheme` per eseguire la verifica. Ad esempio: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Per ulteriori informazioni su questo cmdlet, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licenze Linux: con le licenze Linux BYOS (Bring-Your-Own-Subscription), non è necessario pagare per il software. La tariffa BYOS include solo la tariffa per l'hardware di elaborazione. Esistono due tipi di licenze:
  - **RHEL_BYOS**: per utilizzare correttamente il tipo RHEL_BYOS, abilitare Red Hat Cloud Access nella sottoscrizione di Azure.
  - **SLES_BYOS**: le versioni BYOS di SLES includono il supporto di SUSE.

  È possibile impostare il valore LicenseType sulle opzioni Linux in `New-ProvScheme` e `Set-ProvScheme`.

  Esempio di impostazione di LicenseType su RHEL_BYOS per `New-ProvScheme`:

```
1 New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
      azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
      @() -CustomProperties '<CustomProperties xmlns="http://
      schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http
      ://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="
      StringProperty" Name="UseManagedDisks" Value="true" /><
      Property xsi:type="StringProperty" Name="StorageAccountType
      " Value="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
      /><Property xsi:type="StringProperty" Name="OsType" Value="
      Linux" /><Property xsi:type="StringProperty" Name="
      LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
2 <!--NeedCopy-->
```

  Esempio di impostazione di LicenseType su SLES_BYOS per `Set-ProvScheme`:

```
1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
      CustomProperties '<CustomProperties xmlns="http://schemas.
      citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
      w3.org/2001/XMLSchema-instance"><Property xsi:type="
      StringProperty" Name="UseManagedDisks" Value="true" /><
      Property xsi:type="StringProperty" Name="StorageAccountType
      " Value="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
```

```
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="SLES_BYOS" /></CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Se il valore `LicenseType` è vuoto, i valori predefiniti sono Azure Windows Server License (Licenza Azure Windows Server) o Azure Linux License (Licenza Azure Linux), a seconda del valore di OSType.

Esempio di impostazione di LicenseType su un valore vuoto:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /></CustomProperties>'
<!--NeedCopy-->
```

Consultare i seguenti documenti per comprendere i tipi di licenza e i relativi vantaggi:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

La Raccolta di calcolo di Azure è un repository per la gestione e la condivisione di immagini. Consente di rendere disponibili le immagini in tutta l'organizzazione. Si consiglia di memorizzare un'immagine nella Raccolta di calcolo di Azure quando si creano cataloghi delle macchine di grandi dimensioni non persistenti, perché in questo modo è possibile reimpostare più velocemente i dischi del sistema operativo VDA. Dopo aver selezionato **Place image in Azure Compute Gallery** (Inserisci immagine nella Raccolta di calcolo di Azure), viene visualizzata la sezione **Azure Compute Gallery settings** (Impostazioni della Raccolta di calcolo di Azure), che consente di specificare altre impostazioni della Raccolta di calcolo di Azure:

- **Ratio of virtual machines to image replicas** (Rapporto tra macchine virtuali e repliche di immagini). Consente di specificare il rapporto tra macchine virtuali e repliche di immagini che si desidera conservare in Azure. Per impostazione predefinita, Azure conserva una singola replica di immagine ogni 40 macchine non persistenti. Per le macchine persistenti, l'impostazione predefinita del numero è 1.000.

  - **Maximum replica count** (Numero massimo di repliche). Consente di specificare il numero massimo di repliche di immagini che si desidera conservare in Azure. L'impostazione predefinita è 10.

- Nella pagina **Virtual Machines** (Macchine virtuali), indicare quante macchine virtuali si desidera creare. È necessario specificarne almeno uno e selezionare una dimensione della macchina. Dopo la creazione del catalogo, è possibile modificare le dimensioni della macchina modificando il catalogo.
- La pagina **NIC** non contiene informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Disk Settings** (Impostazioni disco), scegliere se abilitare la cache write-back. Con la funzione di ottimizzazione dell'archiviazione MCS abilitata, è possibile configurare le seguenti impostazioni durante la creazione di un catalogo. Queste impostazioni si applicano sia agli ambienti Azure che agli ambienti GCP.

  Dopo aver abilitato la cache write-back, è possibile procedere come segue:

  - Configurare le dimensioni del disco e della RAM utilizzati per la memorizzazione nella cache dei dati temporanei. Per maggiori informazioni, consultare Configurare la cache per i dati temporanei.
  - Selezionare il tipo di archiviazione per il disco della cache write-back. Sono disponibili le seguenti opzioni di archiviazione per il disco della cache write-back:
    * Premium SSD (SSD premium)
    * Standard SSD (SSD standard)
    * Standard HDD (HDD standard)
  - Scegliere se si desidera che il disco della cache write-back venga mantenuto per le macchine virtuali di cui è stato eseguito il provisioning. Selezionare **Enable write-back cache** (Abilita cache write-back) per rendere disponibili le opzioni. Per impostazione predefinita, l'opzione **Use non-persistent write-back cache disk** (Usa disco della cache write-back non persistente) è selezionata.
  - https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
  - https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
  - https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/
  - Selezionare il tipo per il disco della cache write-back.
    * **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se selezionato, il disco della cache write-back viene eliminato durante i cicli

di alimentazione. Tutti i dati reindirizzati a tale disco andranno persi. Se il disco temporaneo della macchina virtuale dispone di spazio sufficiente, viene utilizzato per ospitare il disco della cache write-back per ridurre i costi. Dopo la creazione del catalogo, è possibile verificare se le macchine di cui è stato eseguito il provisioning utilizzano il disco temporaneo. A tale scopo, fare clic sul catalogo e verificare le informazioni nella scheda **Template Properties** (Proprietà modello). Se viene utilizzato il disco temporaneo, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **Yes (using VM's temporary disk)** (Sì, utilizzando il disco temporaneo della macchina virtuale). In caso contrario, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **No (not using VM's temporary disk)** (No, non utilizzando il disco temporaneo della macchina virtuale).

* **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se questa opzione è selezionata, il disco della cache write-back persiste per le macchine virtuali di cui è stato eseguito il provisioning. L'abilitazione dell'opzione aumenta i costi di archiviazione.

– Scegliere se conservare le VM e i dischi di sistema per i VDA durante i cicli di alimentazione.

**Retain VM and system disk during power cycles (Conserva la VM e il disco di sistema durante i cicli di alimentazione).** Disponibile quando si è selezionato **Enable write-back cache** (Abilita cache di write-back). Per impostazione predefinita, le VM e i dischi di sistema vengono eliminati all'arresto e ricreati all'avvio. Se si desidera ridurre i tempi di riavvio delle VM, selezionare questa opzione. Tenere presente che l'attivazione di questa opzione aumenta anche i costi di archiviazione.

– Scegliere se abilitare i risparmi sui costi di archiviazione mediante l'opzione **Enable storage cost saving**. Se abilitato, risparmia sui costi di archiviazione eseguendo il downgrade del disco di archiviazione ad HDD standard all'arresto della VM. La VM torna alle impostazioni originali al momento del riavvio. L'opzione si applica sia ai dischi di archiviazione che ai dischi cache write-back. In alternativa, è anche possibile usare PowerShell. Vedere Portare il tipo di archiviazione a un livello inferiore quando una VM viene arrestata.

> **Nota:**
>
> Microsoft impone restrizioni sulla modifica del tipo di archiviazione durante l'arresto della macchina virtuale. È anche possibile che Microsoft in futuro blocchi le modifiche al tipo di archiviazione. Per ulteriori informazioni, vedere questo articolo di Microsoft.

– Scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente

di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Per ulteriori informazioni, vedere Crittografia lato server di Azure.

- Nella pagina **Resource Group** (Gruppo di risorse), scegliere se creare gruppi di risorse o utilizzare gruppi esistenti.
  - Se si sceglie di creare gruppi di risorse, selezionare **Next** (Avanti).
  - Se si sceglie di utilizzare gruppi di risorse esistenti, selezionare i gruppi dall'elenco **Available Provisioning Resource Groups** (Gruppi di risorse di provisioning disponibili). **Da ricordare**: selezionare un numero sufficiente di gruppi per ospitare le macchine che si stanno creando nel catalogo. Se se ne scelgono troppo pochi, viene visualizzato un messaggio. Si potrebbe voler selezionare un numero superiore al minimo richiesto se si prevede di aggiungere altre macchine virtuali al catalogo in un secondo momento. Non è possibile aggiungere altri gruppi di risorse a un catalogo dopo la creazione del catalogo.

  Per ulteriori informazioni, vedere Gruppi di risorse di Azure.

- Nella pagina **Machine Identities** (Identità macchine), scegliere un tipo di identità e configurare le identità per le macchine in questo catalogo. Se si selezionano le macchine virtuali come aggiunte ad **Azure Active Directory**, èpossibile aggiungerle a un gruppo di sicurezza di Azure AD. I passaggi dettagliati sono i seguenti:

  1. Nel campo **Identity type** (Tipo di identità), selezionare **Azure Active Directory joined**. Viene visualizzata l'opzione **Azure AD security group (optional)** [Gruppo di sicurezza di Azure AD (opzionale)].
  2. Fare clic su **Azure AD security group: Create new** (Gruppo di sicurezza Azure AD: Crea nuovo).
  3. Inserire un nome per il gruppo, quindi fare clic su **Create**.
  4. Seguire le istruzioni sullo schermo per accedere ad Azure.
     Se il nome del gruppo non esiste in Azure, viene visualizzata un'icona verde. In caso contrario, viene visualizzato un messaggio di errore che richiede di inserire un nuovo nome.
  5. Per aggiungere il gruppo di sicurezza a un gruppo di sicurezza assegnato, selezionare **Join an assigned security group as a member** (Partecipa a un gruppo di sicurezza assegnato come membro), quindi fare clic su **Select a group** (Seleziona un gruppo) per scegliere un gruppo assegnato a cui aderire.
  6. Inserire lo schema di denominazione degli account macchina per le macchine virtuali.

  Dopo la creazione del catalogo, Citrix DaaS accede ad Azure per conto dell'utente e crea il gruppo di sicurezza e una regola di appartenenza dinamica per il gruppo. In base alla regola, le macchine virtuali con lo schema di denominazione specificato in questo catalogo vengono aggiunte automaticamente al gruppo di sicurezza.

  L'aggiunta di macchine virtuali con uno schema di denominazione diverso a questo catalogo

richiede l'accesso ad Azure. Citrix DaaS può quindi accedere ad Azure e creare una regola di appartenenza dinamica basata sul nuovo schema di denominazione.

Quando si elimina questo catalogo, l'eliminazione del gruppo di sicurezza da Azure richiede anche l'accesso ad Azure.

> **Nota:**
>
> Per rinominare il gruppo di sicurezza di Azure AD dopo la creazione del catalogo, modificare il catalogo e passare ad **Azure AD Security Group** dalla barra di navigazione a sinistra. I nomi dei gruppi di sicurezza di Azure AD non devono contenere i seguenti caratteri: `@ " \ / ; : # . * ? = < > | [ ] ( )'`.

- Le pagine **Domain Credentials** (Credenziali di dominio) e **Summary** (Riepilogo) non contengono informazioni specifiche di Azure. Seguire le istruzioni riportate nell'articolo Creare cataloghi di macchine.

Completare la procedura guidata.

#### Condizioni perché il disco temporaneo di Azure sia idoneo per il disco della cache write-back

È possibile utilizzare il disco temporaneo di Azure come disco della cache write-back solo se vengono soddisfatte tutte le seguenti condizioni:

- Il disco della cache write-back non deve persistere poiché il disco temporaneo di Azure non è appropriato per i dati persistenti.
- La dimensione della macchina virtuale di Azure scelta deve includere un disco temporaneo.
- Non è necessario abilitare il disco del sistema operativo temporaneo.
- Accettare di inserire il file della cache write-back sul disco temporaneo di Azure.
- La dimensione temporanea del disco di Azure deve essere maggiore della dimensione totale di (dimensione del disco della cache write-back + spazio riservato per il file di paging + 1 GB di spazio buffer).

#### Utilizzo di PowerShell per creare un catalogo con disco della cache write-back non persistente

Per configurare un catalogo con il disco della cache write-back non persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. Le proprietà personalizzate sono:

- `UseTempDiskForWBC`. Questa proprietà indica se si sta accettando di utilizzare l'archiviazione temporanea di Azure per archiviare il file della cache write-back. Questo deve essere configurato su true durante l'esecuzione di `New-ProvScheme` se si desidera utilizzare il disco

temporaneo come disco della cache write-back. Se questa proprietà non viene specificata, il parametro è impostato su False per impostazione predefinita.

Ad esempio, utilizzando il parametro `CustomProperties` per impostare `UseTempDiskForWBC` su true:

```
1     -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.
         com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
         XMLSchema-instance"> `
2     <Property xsi:type="StringProperty" Name="PersistWBC" Value="false
         "/> `
3     <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
         false"/> `
4     <Property xsi:type="StringProperty" Name="PersistVm" Value="false
         "/> `
5     <Property xsi:type="StringProperty" Name="StorageAccountType" Value
         ="Premium_LRS"/> `
6     <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value
         ="Premium_LRS"/> `
7     <Property xsi:type="StringProperty" Name="LicenseType" Value="
         Windows_Client"/> `
8     <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
         ="true"/> `
9     </CustomProperties>'
10 <!--NeedCopy-->
```

> **Nota:**
>
> Dopo aver eseguito il commit del catalogo delle macchine per l'utilizzo dell'archiviazione temporanea locale di Azure per il file della cache write-back, non può essere modificato per utilizzare l'unità disco rigido virtuale in un secondo momento.

#### Scenari relativi al disco della cache write-back non persistente

La tabella seguente descrive tre diversi scenari in cui il disco temporaneo viene utilizzato per la cache write-back durante la creazione del catalogo delle macchine.

| Scenario | Risultato |
| --- | --- |
| Tutte le condizioni per utilizzare il disco temporaneo per la cache write-back sono soddisfatte. | Il file WBC `mcsdif.vhdx` viene inserito nel disco temporaneo. |
| Lo spazio sul disco temporaneo non è sufficiente per l'utilizzo della cache write-back. | Viene creato un disco VHD "MCSWCDisk"e il file WBC `mcsdif.vhdx` viene inserito su questo disco. |

| Scenario | Risultato |
| --- | --- |
| Il disco temporaneo ha spazio sufficiente per l'utilizzo della cache write-back, ma `UseTempDiskForWBC` è impostato su false. | Viene creato un disco VHD "MCSWCDisk"e il file WBC `mcsdif.vhdx` viene inserito su questo disco. |

#### Utilizzo di PowerShell per creare un catalogo con disco di cache write-back persistente

Per configurare un catalogo con il disco della cache write-back persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`.

> **Suggerimento:**
>
> Utilizzare il parametro PowerShell `New-ProvScheme CustomProperties` solo per le connessioni di hosting basate su cloud. Se si desidera eseguire il provisioning di macchine utilizzando un disco di cache write-back persistente per una soluzione locale (ad esempio, Citrix Hypervisor), PowerShell non è necessario perché il disco persiste automaticamente.

Questo parametro supporta una proprietà aggiuntiva, `PersistWBC`, utilizzata per determinare il modo in cui il disco della cache write-back persiste per le macchine di cui è stato eseguito il provisioning con MCS. La proprietà `PersistWBC` viene utilizzata solo quando viene specificato il parametro`UseWriteBackCache` e quando il parametro `WriteBackCacheDiskSize` è impostato per indicare che viene creato un disco.

> **Nota:**
>
> Questo comportamento si applica sia ad Azure che a GCP nei casi in cui il disco della cache write-back MCSIO predefinito viene eliminato e ricreato durante il ciclo di alimentazione. È possibile scegliere di rendere persistente il disco in modo da evitare l'eliminazione e la ri-creazione del disco della cache write-back MCSIO.

Esempi di proprietà trovate nel parametro `CustomProperties` prima del supporto `PersistWBC` sono:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```

> **Nota:**
>
> Questo esempio si applica solo ad Azure. Le proprietà sono diverse nell'ambiente GCP.

Quando si utilizzano queste proprietà, considerare che contengono valori predefiniti se le proprietà vengono omesse dal parametro `CustomProperties`. La proprietà `PersistWBC` ha due valori possibili: **true** o **false**.

L'impostazione della proprietà `PersistWBC` su **true** non elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops spegne la macchina dall'interfaccia di gestione.

L'impostazione della proprietà `PersistWBC` su **false** elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops arresta la macchina dall'interfaccia di gestione.

> **Nota:**
>
> Se la proprietà `PersistWBC` viene omessa, il valore predefinito della proprietà è **false** e la cache write-back viene eliminata quando la macchina viene arrestata dall'interfaccia di gestione.

Ad esempio, utilizzando il parametro `CustomProperties` per impostare `PersistWBC` su true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Importante:**
>
> La proprietà `PersistWBC` può essere impostata solo utilizzando il cmdlet PowerShell `New-ProvScheme`. Il tentativo di modificare le `CustomProperties` di uno schema di provisioning dopo la creazione non ha alcun impatto sul catalogo macchine e sulla persistenza del disco della cache write-back quando un computer viene arrestato.

Ad esempio, impostare `New-ProvScheme` perché utilizzi la cache write-back mentre si imposta la proprietà `PersistWBC` su true:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`">
```

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"benvaldev5RG3`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`" />
</CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSIO-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualprivatecloud\adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

#### Migliorare le prestazioni di avvio con MCSIO

È possibile migliorare le prestazioni di avvio per i dischi gestiti di Azure e GCP quando MCSIO è abilitato. Utilizzare la proprietà personalizzata di PowerShell `PersistOSDisk` nel comando `New-ProvScheme` per configurare questa funzionalità. Le opzioni associate a `New-ProvScheme` includono:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
``````<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

Per abilitare questa funzionalità, impostare la proprietà personalizzata `PersistOSDisk` su **true**. Ad

esempio:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Creare una specifica del modello di Azure

È possibile creare una specifica del modello di Azure nel portale di Azure e utilizzarla nell'interfaccia **Full configuration** e nei comandi PowerShell per creare o aggiornare un catalogo di macchine MCS.

Per creare una specifica del modello di Azure per una macchina virtuale esistente:

1. Andare al portale di Azure. Selezionare un gruppo di risorse, quindi selezionare la macchina virtuale e l'interfaccia di rete. Nel menu **...** in alto, fare clic su **Export template** (Esporta modello).
2. Deselezionare la casella di controllo **Include parameters** (Includi parametri) se si desidera creare una specifica del modello di provisioning del catalogo.
3. Fare clic su **Add to library** (Aggiungi alla libreria) per modificare le specifiche del modello in un secondo momento.
4. Nella pagina **Importing template** (Modello di importazione), inserire le informazioni richieste: **Name** (nome), **Subscription** (abbonamento), **Resource Group** (Gruppo di risorse), **Location** (Posizione) e **Version** (Versione). Fare clic su **Next: Edit Template** (Avanti: Modifica modello).

5. È inoltre necessaria un'interfaccia di rete come risorsa indipendente se si desidera effettuare il provisioning di cataloghi. Pertanto, è necessario rimuovere qualsiasi elemento `dependsOn` specificato nelle specifiche del modello. Ad esempio:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
<!--NeedCopy-->
```

6. Creare **Review+Create** (Rivedi+Crea) e le specifiche del modello.
7. Nella pagina **Template Specs** (Specifiche del modello), verificare le specifiche del modello appena creato. Fare clic sulle specifiche del modello. Nel pannello di sinistra, fare clic su **Versions** (Versioni).
8. È possibile creare una nuova versione facendo clic su **Create new version** (Crea nuova versione). Specificare un nuovo numero di versione, apportare le necessarie modifiche alle specifiche del modello corrente e fare clic su **Review + Create** per creare la nuova versione della specifica del modello.

È possibile ottenere informazioni sulle specifiche del modello e sulla versione del modello utilizzando i seguenti comandi PowerShell:

- Per ottenere informazioni sulle specifiche del modello, eseguire:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
   resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- Per ottenere informazioni sulla versione delle specifiche del modello, eseguire:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
   resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
   templatespecversion
<!--NeedCopy-->
```

#### Utilizzare le specifiche del modello per creare o aggiornare un catalogo

È possibile creare o aggiornare un catalogo di macchine MCS utilizzando una specifica di modello come input del profilo della macchina. A tale scopo, è possibile utilizzare l'interfaccia **Full Configuration** o i comandi di PowerShell.

Utilizzare l'interfaccia di **Full Configuration**: vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

Utilizzare i comandi PowerShell:

1. Aprire la finestra di **PowerShell**.

2. Eseguire `asnp citrix*`.
3. Creare o aggiornare un catalogo.

   - Per creare un catalogo:

     a) Utilizzare il comando `New-ProvScheme` con una specifica del modello come input per il profilo macchina. Ad esempio:

     ```
     New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
         image.folder/fgthj.resourcegroup/nab-ws-
         vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/test.templatespec/V1.
         templatespecversion"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>
     [-LoggingId <Guid>]
     [-BearerToken <String>][-AdminAddress <String>]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

     b) Completare la creazione del catalogo di macchine.

   - Per aggiornare un catalogo, utilizzare il comando `Set-ProvScheme` con una specifica di modello come input del profilo macchina. Ad esempio:

     ```
     Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
         Us.region/vm.folder/MasterDisk.vm'
     MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/testing.templatespec/V1.
         templatespecversion'
     [-ProvisioningSchemeName] <String>
     [-CustomProperties <String>][-ServiceOffering <String>] [-
         PassThru]
     [-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
         String>] [<CommonParameters>]
     <!--NeedCopy-->
     ```

### Cataloghi di macchine con avvio attendibile

Per creare correttamente un catalogo di macchine con avvio attendibile, utilizzare:

- Un profilo macchina con avvio attendibile
- Una dimensione di macchina virtuale che supporti l'avvio attendibile
- Una versione di macchina virtuale Windows che supporti l'avvio attendibile. Attualmente, Windows 10, 2016, 2019 e 2022 supportano l'avvio attendibile.

> **Importante:**
>
> L'avvio attendibile richiede la creazione di nuove macchine virtuali. Non è possibile abilitare l'avvio attendibile sulle macchine virtuali esistenti che erano state create inizialmente senza di esso.

Per visualizzare gli elementi di inventario di Citrix DaaS e determinare se le dimensioni della macchina virtuale supportano l'avvio attendibile, eseguire il seguente comando:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il seguente comando:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
<!--NeedCopy-->
```

4. Eseguire `$s | select -ExpandProperty Additionaldata`
5. Controllare il valore dell'attributo `SupportsTrustedLaunch`.
    - Se `SupportsTrustedLaunch` è **True**, la dimensione della macchina virtuale supporta l'avvio attendibile.
    - Se `SupportsTrustedLaunch` è **False**, la dimensione della macchina virtuale non supporta l'avvio attendibile.

Come da PowerShell di Azure, è possibile usare il seguente comando per determinare le dimensioni di macchina virtuale che supportano l'avvio attendibile:

```
(Get-AzComputeResourceSku | where {
 $\_.Locations.Contains($region) -and ($\_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

Di seguito sono riportati alcuni esempi che descrivono se la dimensione della macchina virtuale supporta l'avvio attendibile dopo l'esecuzione del comando Azure PowerShell.

- *Esempio 1*: se la macchina virtuale di Azure supporta solo la generazione 1, quella macchina virtuale non supporta l'avvio attendibile. Pertanto, la funzionalità `TrustedLaunchDisabled` non viene visualizzata dopo l'esecuzione del comando Azure PowerShell.
- *Esempio 2*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità`TrustedLaunchDisabled` è **True**, la dimensione della macchina virtuale di generazione 2 non è supportata per l'avvio attendibile.
- *Esempio 3*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità `TrustedLaunchDisabled` non viene visualizzata dopo l'esecuzione del comando PowerShell, la dimensione della VM di generazione 2 è supportata per l'avvio attendibile.

Per ulteriori informazioni sull'avvio attendibile per le macchine virtuali Azure, vedere il documento Microsoft Avvio attendibile per le macchine virtuali di Azure.

#### Errori nella creazione di cataloghi di macchine con avvio attendibile

Si ottengono errori appropriati nei seguenti scenari durante la creazione di un catalogo di macchine con avvio attendibile:

| Scenario | Errore |
| --- | --- |
| Se si seleziona un profilo macchina durante la creazione di un catalogo non gestito | `MachineProfileNotSupportedForUnmanagedCata` |
| Se si seleziona un profilo macchina che supporta l'avvio attendibile durante la creazione di un catalogo con un disco non gestito come immagine master | `SecurityTypeNotSupportedForUnmanagedDisk` |
| Se non si seleziona il profilo macchina durante la creazione di un catalogo gestito con un' immagine master con l'avvio attendibile come tipo di sicurezza | `MachineProfileNotFoundForTrustedLaunchMaste` |
| Se si seleziona un profilo macchina con un tipo di sicurezza diverso dal tipo di protezione dell' immagine master | `SecurityTypeConflictBetweenMasterImageAndMa` |
| Se si seleziona una dimensione di macchina virtuale che non supporta l'avvio attendibile, ma utilizza un'immagine master che supporta l' avvio attendibile durante la creazione di un catalogo | `MachineSizeNotSupportTrustedLaunch` |

### Utilizzare i valori delle proprietà del profilo macchina

Il catalogo delle macchine utilizza le seguenti proprietà definite nelle proprietà personalizzate:

- Zona di disponibilità
- ID gruppo host dedicato
- ID set crittografia disco
- Tipo di sistema operativo
- Tipo di licenza
- Tipo di archiviazione

Se queste proprietà personalizzate non sono definite in modo esplicito, i valori delle proprietà vengono impostati in base alla specifica del modello ARM o alla macchina virtuale, a seconda di quale sia utilizzata come profilo macchina. Inoltre, se non è specificato `ServiceOffering`, questo viene impostato in base al profilo della macchina.

> **Nota:**
>
> Se alcune delle proprietà non sono presenti nel profilo macchina e non sono definite nelle proprietà personalizzate, vengono adottati i valori predefiniti delle proprietà laddove è applicabile.

La sezione seguente descrive alcuni scenari in `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` hanno tutte le proprietà definite o qando i valori sono derivati da MachineProfile.

- Scenari New-ProvScheme
  - MachineProfile ha tutte le proprietà e le CustomProperties non sono definite. Esempio:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
          machinecreation" xmlns:xsi="http://www.w3.org/2001/
          XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
           Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
          -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
          "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
          " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
          DedicatedHostGroupId" Value="<mpA-value>"/>
    8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
          value>"/>
    9  </CustomProperties>
    10 <!--NeedCopy-->
    ```

  - MachineProfile ha alcune proprietà e le CustomProperties non sono definite. Esempio: MachineProfile ha solo LicenseType e OSType.

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
    -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpA-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Sia MachineProfile che CustomProperties definiscono tutte le proprietà. Esempio:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Le proprietà personalizzate hanno la priorità. I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  ```
  Get-ProvScheme | select CustomProperties
  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
      " Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="
      DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="Zones" Value="<
      CustomPropertiesA-value>"/>
  </CustomProperties>
  <!--NeedCopy-->
  ```

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Esempio:

  * In CustomProperties sono definite LicenseType e StorageAccountType
  * In MachineProfile sono definite LicenseType, OSType e Zones

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
    -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Inoltre, ServiceOffering non è definito. Esempio:
  - In CustomProperties è definito StorageType
  - In MachineProfile è definito LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
    serviceoffering.folder<explicit-machine-size>.
    serviceoffering"
<!--NeedCopy-->
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- Se OsType e non si trova né in CustomProperties né in MachineProfile, allora:
  - Il valore viene letto dall'immagine master.
  - Se l'immagine master è un disco non gestito, OsType è impostato su Windows. Esempio:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
```

```
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

Il valore dell'immagine master viene scritto nelle proprietà personalizzate, in questo caso Linux.

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="OSType" Value="
      Linux"/>
4  </CustomProperties>
5  <!--NeedCopy-->
```

- Scenari Set-ProvScheme
  - Un catalogo esistente con:
    - CustomProperties per `StorageAccountType` e OsType
    - MachineProfile `mpA.vm` che definisce le zone
  - Aggiornamenti:
    - MachineProfile mpB.vm che definisce StorageAccountType
    - Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce LicenseType e OsType

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6       </CustomProperties>
7  <!--NeedCopy-->
```

  - Un catalogo esistente con:
    - CustomProperties per `StorageAccountType` e OsType

    * MachineProfile `mpA.vm` che definisce StorageAccountType e LicenseType

- Aggiornamenti:

    * Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce StorageAccountType e OsType.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
       CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mp-A-value>"/>
6  </CustomProperties>
7  <!--NeedCopy-->
```

- Un catalogo esistente con:

    * CustomProperties per `StorageAccountType` e OsType
    * MachineProfile `mpA.vm` che definisce le zone

- Aggiornamenti:

    * Un MachineProfile mpB.vm che definisce StorageAccountType e LicenseType
    * `ServiceOffering` non è specificato

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1  Get-ProvScheme | select ServiceOffering
2  serviceoffering.folder<value-from-machineprofile>.
       serviceoffering
3
4  Get-ProvScheme | select CustomProperties
5  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
6  <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<mpB-value>"/>
7  <Property xsi:type="StringProperty" Name="OSType" Value="<
       prior-CustomProperties-value>"/>
8  <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpB-value>"/>
```

```
</CustomProperties>
<!--NeedCopy-->
```

### Creare o aggiornare un catalogo con più NIC per macchina virtuale

MCS supporta più NIC per macchina virtuale. È possibile associare più NIC presenti su una macchina virtuale a più sottoreti, tuttavia, tali sottoreti devono trovarsi nella stessa rete virtuale (vNet). È possibile utilizzare comandi PowerShell per:

- Creare un catalogo con più NIC su una macchina virtuale
- Aggiornare la configurazione di un catalogo esistente per avere più NIC su una VM in modo che le nuove VM create abbiano più NIC
- Aggiornare una macchina virtuale esistente perché abbia più NIC

È possibile creare o aggiornare un catalogo di macchine non basato su profili macchina e un catalogo di macchine basato su profili macchina in modo che disponga di più NIC su una macchina virtuale. Attualmente, in un catalogo macchine basato su profili macchina, è possibile avere solo lo stesso numero di NIC specificato nell'origine del profilo macchina.

Proprietà come la rete accelerata e il gruppo di sicurezza di rete derivano dall'origine del profilo del computer.

> **Nota:**
>
> La dimensione della macchina virtuale deve supportare lo stesso numero di NIC e la rete accelerata corrispondente, altrimenti viene visualizzato un errore.

È possibile recuperare il numero massimo di NIC associate a una dimensione di VM selezionata. Una proprietà PowerShell denominata `MaxNetworkInterfaces` visualizza il numero massimo di NIC quando si esegue il comando PowerShell `get-item` con il parametro `AdditionalData`.

### Recuperare il numero massimo di NIC

Per recuperare il numero massimo di NIC:

1. Aprire una finestra **PowerShell** dall'host Delivery Controller.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` per elencare tutte le dimensioni di VM disponibili.
4. Eseguire `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`

5. Verificare `MaxNetworkInterfaces` per scoprire il numero massimo di NIC disponibile.

### Creare un catalogo con più NIC su una macchina virtuale

Per creare un catalogo con più NIC su una macchina virtuale, procedere come segue:

1. Aprire una finestra PowerShell dall'host Delivery Controller.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Creare un pool di identità se non è già stato creato.
4. Creare lo schema di provisioning:

   - Se si sta creando un catalogo di macchine non basato su profili macchina, eseguire il comando `New-ProvScheme` con il parametro `NetworkMappings`. È possibile aggiungere più sottoreti al parametro `NetworkMappings`. Ad esempio:

     ```
     New-Provscheme -NetworkMappings @{
     "0"="subnetpath1";"1"="subnetpath1" }

     <!--NeedCopy-->
     ```

   - Se si crea un catalogo di macchine basato su profili macchina:

     a) In Azure, creare una macchina virtuale che disponga di più NIC. Per informazioni, vedere Creare e gestire una macchina virtuale Windows che ha più schede di interfaccia di rete. È possibile anche creare una nuova macchina virtuale e quindi collegare un'interfaccia di rete nella pagina Networking del portale Azure.

     b) Eseguire il comando `New-ProvScheme` con la VM come input del profilo macchina.

     > **Nota:**
     >
     > Quando si crea un catalogo di macchine basato su profili macchina, il numero di `NetworkMappings` deve essere uguale a quello del `NetworkInterfaceCount` del profilo della macchina. `NetworkInterfaceCount` può essere recuperato da `AdditionalData` di `Get-item -Path "machine profile path"`.

5. Completare la creazione del catalogo di macchine.

### Aggiornare un catalogo per avere più NIC su una macchina virtuale

Per aggiornare un catalogo in modo che disponga di più NIC su una macchina virtuale, procedere come segue:

1. Aprire una finestra **PowerShell** dall'host Delivery Controller.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Aggiornare lo schema di provisioning:

- Se si sta creando un catalogo di macchine non basato su profili macchina, eseguire il comando `Set-ProvScheme` con il parametro `NetworkMappings`. È possibile aggiungere più sottoreti al parametro `NetworkMappings`. Ad esempio:

```
Set-Provscheme -NetworkMappings @{
"0"="subnetpath1";"1"="subnetpath1" }

<!--NeedCopy-->
```

- Se si crea un catalogo di macchine basato su un profilo macchina:

  a) In Azure, creare una macchina virtuale che disponga di più NIC. Per informazioni, vedere Creare e gestire una macchina virtuale Windows che ha più schede di interfaccia di rete.
  b) Eseguire il comando `Set-ProvScheme` con la VM come input del profilo macchina.

#### Aggiornare una macchina virtuale esistente per avere più NIC su una macchina virtuale

È inoltre possibile aggiornare una macchina virtuale esistente utilizzando `Set-ProvVMUpdateTimeWindow` ed eseguire un ciclo di alimentazione sulla macchina virtuale esistente durante la finestra temporale di aggiornamento. Per ulteriori informazioni, vedere Aggiornare le macchine di cui è stato eseguito il provisioning allo stato corrente dello schema di provisioning.

### Effettuare il provisioning delle VM del catalogo con l'agente di Monitoraggio di Azure installato

Il monitoraggio di Azure è un servizio utilizzabile per raccogliere, analizzare e agire sui dati di telemetria dai propri ambienti Azure e locali.

L'agente di Monitoraggio di Azure (AMA) raccoglie i dati di monitoraggio da risorse di elaborazione come le macchine virtuali e li fornisce ad Azure Monitor. Attualmente supporta la raccolta di metriche Event Logs, Syslog e Performance e la invia alle fonti dati di Azure Monitor Metrics e Azure Monitor Logs.

Per abilitare il monitoraggio identificando in modo univoco le VM nei dati di monitoraggio, è possibile effettuare il provisioning delle VM di un catalogo di macchine MCS con AMA installato come estensione.

#### Requisiti

- Autorizzazioni: assicurarsi di disporre delle autorizzazioni minime di Azure come specificato in Informazioni sulle autorizzazioni di Azure e le seguenti autorizzazioni all'uso di Azure Monitor:

```
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Insights/DataCollectionRuleAssociations/Read
- Microsoft.Insights/dataCollectionRuleAssociations/write
- Microsoft.Insights/DataCollectionRules/Read
```

- Regola di raccolta dati: impostare una regola di raccolta dati nel portale di Azure. Per informazioni sulla configurazione di un DCR, vedere Creare una regola di raccolta dati. Un DCR è specifico per una piattaforma (Windows o Linux). Assicurarsi di creare un DCR corretto per la piattaforma richiesta.
  L'AMA utilizza le regole di raccolta dati (DCR) per gestire la mappatura tra le risorse, quali le macchine virtuali, e le fonti di dati, quali Azure Monitor Metrics e Azure Monitor Logs.
- Area di lavoro predefinita: creare un'area di lavoro nel portale di Azure. Per informazioni sulla creazione di un'area di lavoro, vedere Creare un'area di lavoro Log Analytics. Quando si raccolgono registri e dati, le informazioni vengono archiviate in un'area di lavoro. Un'area di lavoro ha un ID dell'area di lavoro e un ID risorsa univoci. Il nome dell'area di lavoro deve essere univoco per un determinato gruppo di risorse. Dopo aver creato un'area di lavoro, configurare le fonti di dati e le soluzioni in modo che archivino i relativi dati in essa.
- L'estensione del monitor inserita nella whitelist: le estensioni `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` sono estensioni inserite nella whitelist definite da Citrix. Per visualizzare l'elenco delle estensioni inserite nella whitelist, utilizzare il comando PoSH `Get-ProvMetadataConfiguration`.
- Immagine master: Microsoft consiglia di rimuovere le estensioni da una macchina esistente prima di crearne una nuova da essa. Se le estensioni non vengono rimosse, si potrebbero riscontrare file rimanenti e comportamenti imprevisti. Per ulteriori informazioni, vedere Se la macchina virtuale viene ricreata da una macchina virtuale esistente.

Per eseguire il provisioning delle VM del catalogo con AMA abilitato:

1. Configurare un modello di profilo macchina.
   - Se si desidera utilizzare una macchina virtuale come modello di profilo macchina:
     a) Creare una macchina virtuale nel portale di Azure.
     b) Accendere la VM.
     c) Aggiungere la VM alla regola di raccolta dati in **Resources**. Ciò richiama l'installazione dell'agente sulla macchina virtuale modello.

     > **Nota:**
     >
     > Se si deve creare un catalogo Linux, configurare una macchina Linux.

   - Se si desidera utilizzare una specifica di modello come modello di profilo macchina:

a) Impostare una specifica di modello.

b) Aggiungere la seguente associazione di regole di estensione e raccolta dati alla specifica di modello generata:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
 {

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
    "Microsoft.Compute/virtualMachines/<vm-name>/extensions
       /AzureMonitorWindowsAgent"
    ],
    "properties": {

       "description": "Association of data collection rule.
           Deleting this association will break the data
          collection for this Arc server.",
     "dataCollectionRuleId": "/subscriptions/<azure-
        subscription>/resourcegroups/<azure-resource-group
        >/providers/microsoft.insights/datacollectionrules
        /<azure-data-collection-rule>"
      }

     }

<!--NeedCopy-->
```

2. Creare o aggiornare un catalogo di macchine MCS esistente.

- Per creare un nuovo catalogo MCS:

  a) Selezionare la VM o la specifica del modello come profilo macchina nell'interfaccia Full Configuration.
  b) Procedere ai passaggi successivi per creare il catalogo.

- Per aggiornare un catalogo MCS esistente, utilizzare i seguenti comandi PoSH:

  - Per fare in modo che le nuove VM ottengano il modello di profilo macchina aggiornato, eseguire il seguente comando:

    ```
    Set-ProvScheme -ProvisioningSchemeName "name"
    -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
        folder\abc.resourcegroup\ab-machine-profile.vm"
    <!--NeedCopy-->
    ```

  - Per aggiornare le macchine virtuali esistenti con il modello di profilo macchina aggiornato:

    ```
    Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
        catalog -StartsNow -DurationInMinutes -1
    <!--NeedCopy-->
    ```

3. Accendere le macchine virtuali del catalogo.
4. Passare al portale di Azure e controllare se l'estensione del monitor è installata sulla macchina virtuale e se la macchina virtuale viene visualizzata nelle risorse di DCR. Dopo alcuni minuti i dati di monitoraggio vengono visualizzati su Azure Monitor.

#### Risoluzione dei problemi

Per informazioni sulle linee guida alla risoluzione dei problemi per l'agente di Monitoraggio di Azure, vedere quanto segue:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Utilizzare PowerShell per abilitare le estensioni delle macchine virtuali di Azure

Dopo aver selezionato la specifica del modello ARM, eseguire i seguenti comandi PowerShell per utilizzare le estensioni delle macchine virtuali di Azure:

- Per visualizzare l'elenco delle estensioni delle macchine virtuali di Azure supportate: `Get-ProvMetadataConfiguration`

- Per aggiungere altre estensioni delle macchine virtuali: `Add-ProvMetadataConfiguration`. Ad esempio, `Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

  Se si tenta di aggiungere uno dei seguenti elementi, il comando non riesce e viene visualizzato un messaggio di errore:

  - Estensione definita da Citrix.
  - Estensione esistente definita dall'utente.
  - Chiavi di configurazione non supportate. Attualmente, la chiave di configurazione supportata è `Extension`.

- Per rimuovere le estensioni dall'elenco: `Remove-ProvMetadataConfiguration`. È possibile rimuovere le estensioni aggiunte.

### Posizione del file di paging

Negli ambienti Azure, il percorso del file di paging viene impostato quando si crea una macchina virtuale per la prima volta. Il formato dell'impostazione del file di paging è: posizione del file di paging [dimensione minima] [dimensione massima] (dimensione in MB). Per ulteriori informazioni, consultare Come determinare la dimensione appropriata del file di paging.

Durante la preparazione dell'immagine, quando si crea lo schema di provisioning, MCS determina la posizione del file di paging in base a determinate regole. Dopo aver creato lo schema di provisioning, non è possibile:

- Modificare le dimensioni della macchina virtuale
- Aggiornare il profilo della macchina
- Modificare le proprietà I/O EOS e MCS

#### Determinazione della posizione del file di paging

Le funzionalità come EOS e MCS/IO hanno la propria posizione prevista per il file di paging e si escludono a vicenda. La tabella seguente mostra la posizione prevista del file di paging per ciascuna funzionalità:

| Funzionalità | Posizione prevista del file di paging |
|---|---|
| EOS | Disco del sistema operativo |
| MCS I/O | Prima il disco temporaneo di Azure, altrimenti il disco cache di write-back |

> **Nota:**
>
> Anche se la preparazione dell'immagine è disaccoppiata dalla creazione dello schema di provisioning, MCS determina correttamente la posizione del file di paging. Il percorso predefinito del file di paging è sul disco del sistema operativo.

#### Scenari di configurazione del file di paging

La tabella seguente descrive alcuni possibili scenari di configurazione del file di paging durante la preparazione dell'immagine e l'aggiornamento dello schema di provisioning:

| Durante | Scenario | Risultato |
|---|---|---|
| Preparazione delle immagini | Il file di paging dell'immagine di origine viene impostato sul disco temporaneo, mentre le dimensioni della macchina virtuale specificate nello schema di provisioning non hanno alcun disco temporaneo | Il file di paging viene inserito nel sistema operativo |
| Preparazione delle immagini | Il file di paging dell'immagine di origine viene impostato sul disco del sistema operativo, mentre la dimensione della macchina virtuale specificata nello schema di provisioning ha un disco temporaneo | Il file di paging viene inserito nel disco temporaneo |
| Preparazione delle immagini | Il file di paging dell'immagine di origine viene impostato sul disco temporaneo e si abilita il disco temporaneo del sistema operativo nello schema di provisioning | Il file di paging viene inserito nel disco del sistema operativo |

| Durante | Scenario | Risultato |
| --- | --- | --- |
| Aggiornamento dello schema di provisioning | Si tenta di aggiornare lo schema di provisioning. La dimensione originale della macchina virtuale ha un disco temporaneo, mentre la macchina virtuale di destinazione non ha un disco temporaneo | Rifiuta la modifica con un messaggio di errore |
| Aggiornamento dello schema di provisioning | Si tenta di aggiornare lo schema di provisioning. La dimensione originale della macchina virtuale non ha un disco temporaneo, mentre la macchina virtuale di destinazione ha un disco temporaneo | Rifiuta la modifica con un messaggio di errore |

### Aggiornare l'impostazione del file di paging

Utilizzando i comandi PowerShell, è possibile specificare le impostazioni del file di paging, incluse la posizione e le dimensioni. Ciò sostituisce le impostazioni del file di paging determinate da MCS. È possibile eseguire questa operazione durante la creazione del catalogo delle macchine, eseguendo il seguente comando `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot `
    -HostingUnitName "zijinnet" `
    -IdentityPoolName "PageFileSettingExample" `
    -ProvisioningSchemeName "PageFileSettingExample" `
    -InitialBatchSizeHint 1 `
    -MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-
       zijincloud-resources.resourcegroup\
       CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.
       manageddisk" `
    -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\neal-zijincloud-resources.
    resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\
    default.network" }
  `
    -ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.
       folder\Standard_B2ms.serviceoffering" `
    -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.
```

```
            com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
            XMLSchema-instance"> `
12      <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
            false"/> `
13      <Property xsi:type="StringProperty" Name="PersistVm" Value="false
            "/> `
14      <Property xsi:type="StringProperty" Name="
            PageFileDiskDriveLetterOverride" Value="d"/> `
15      <Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
            Value="2048"/> `
16      <Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
            Value="8196"/> `
17      <Property xsi:type="StringProperty" Name="StorageAccountType" Value
            ="Premium_LRS"/> `
18      <Property xsi:type="StringProperty" Name="LicenseType" Value="
            Windows_Client"/> `
19      </CustomProperties>'
20  <!--NeedCopy-->
```

Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere Creazione di un catalogo utilizzando PowerShell.

Vincoli:

- È possibile aggiornare l'impostazione del file di paging solo quando si crea lo schema di provisioning eseguendo il comando `New-ProvScheme`. Non è possibile modificare l'impostazione del file di paging in seguito.
- È necessario specificare nel comando `New-ProvScheme` tutte le proprietà personalizzate ( "PageFileDiskDriveLetterOverride", "InitialPageFileSizeInMB"e "MaxPageFileSizeInMB") o nessuna di esse.
- Questa funzionalità non è supportata in Citrix Studio.
- La dimensione iniziale del file di paging deve essere compresa tra 16 MB e 16777216 MB.
- La dimensione massima del file di paging deve essere maggiore o uguale alla dimensione iniziale del file di paging e inferiore a 16777216 MB.
- È possibile impostare contemporaneamente sia la dimensione iniziale del file di paging che la dimensione massima del file di paging su zero.

### Gruppi di risorse di Azure

I gruppi di risorse di provisioning di Azure offrono un modo per eseguire il provisioning delle macchine virtuali che forniscono applicazioni e desktop agli utenti. È possibile aggiungere gruppi di risorse di Azure vuoti esistenti quando si crea un catalogo delle macchine MCS o quando vengono creati nuovi gruppi di risorse per conto dell'utente. Per informazioni sui gruppi di risorse di Azure, consultare la documentazione Microsoft.

### Utilizzo dei gruppi di risorse di Azure

Non ci sono limiti al numero di macchine virtuali, dischi gestiti, snapshot e immagini per ciascun gruppo di risorse di Azure (il limite di 240 macchine virtuali per 800 dischi gestiti per ciascun gruppo di risorse di Azure è stato rimosso).

- Quando si utilizza un'entità servizio con ambito completo per creare un catalogo delle macchine, MCS crea un solo gruppo di risorse di Azure e utilizza tale gruppo per il catalogo.
- Quando si utilizza un'entità servizio con ambito limitato per creare un catalogo delle macchine, è necessario fornire un gruppo di risorse di Azure vuoto e pre-creato per il catalogo.

### Dischi temporanei di Azure

Un disco temporaneo di Azure consente di riutilizzare il disco della cache o il disco temporaneo per archiviare il disco del sistema operativo per una macchina virtuale abilitata per Azure. Questa funzionalità è utile per gli ambienti Azure che richiedono un disco SSD a prestazioni più elevate rispetto a un disco rigido standard. Per utilizzare dischi temporanei, è necessario impostare la proprietà personalizzata `UseEphemeralOsDisk` su **true** durante l'esecuzione di `New-ProvScheme`.

> **Nota:**
>
> Se la proprietà personalizzata `UseEphemeralOsDisk` è impostata su **false** o non viene specificato un valore, tutti i VDA di cui è stato eseguito il provisioning continuano a utilizzare un disco del sistema operativo di cui è stato eseguito il provisioning.

Di seguito è riportato un esempio di set di proprietà personalizzate da utilizzare nello schema di provisioning:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
```

```
20              {
21
22                  "Name": "SharedImageGalleryReplicaRatio",
23                  "Value": "40"
24               }
25  ,
26              {
27
28                  "Name": "SharedImageGalleryReplicaMaximum",
29                  "Value": "10"
30               }
31  ,
32              {
33
34                  "Name": "LicenseType",
35                  "Value": "Windows_Server"
36               }
37  ,
38              {
39
40                  "Name": "UseEphemeralOsDisk",
41                  "Value": "true"
42               }
43
44          ],
45  <!--NeedCopy-->
```

**Come creare macchine usando dischi del sistema operativo temporanei** I dischi del sistema operativo temporanei sono controllati in base alla proprietà `UseEphemeralOsDisk` nel parametro `CustomProperties`.

**Considerazioni importanti per i dischi temporanei** Per eseguire il provisioning di dischi del sistema operativo temporanei utilizzando `New-ProvScheme`, considerare i seguenti vincoli:

- La dimensione della macchina virtuale utilizzata per il catalogo deve supportare i dischi operativi temporanei.
- La dimensione della cache o del disco temporaneo associato alla dimensione della macchina virtuale deve essere maggiore o uguale alla dimensione del disco del sistema operativo.
- La dimensione del disco temporaneo deve essere maggiore della dimensione del disco della cache.

Tenere presenti questi problemi anche quando:

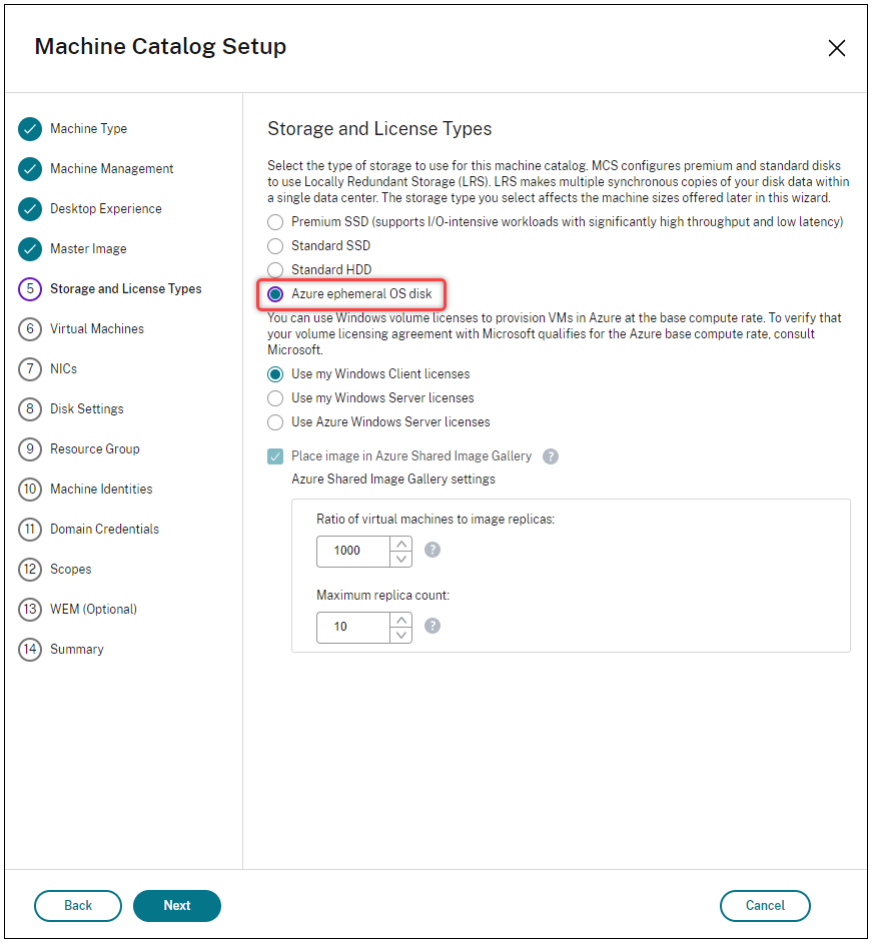
- Si crea lo schema di provisioning.
- Si modifica lo schema di provisioning.
- Si aggiorna l'immagine.

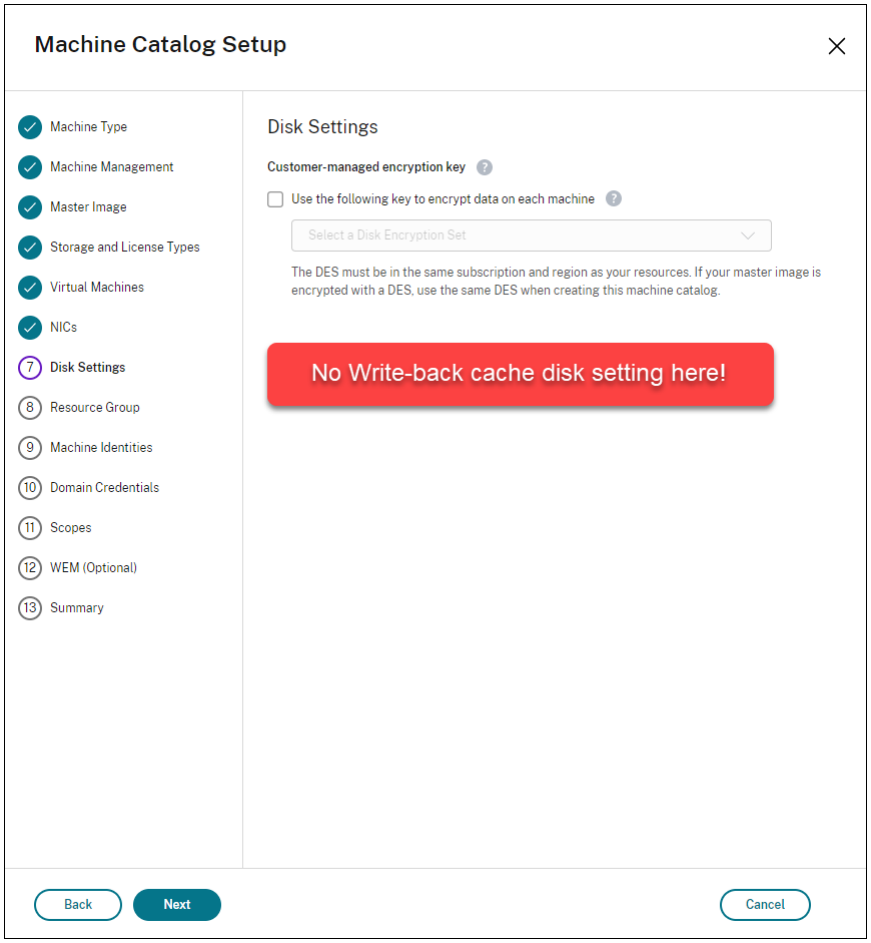
**Ottimizzazione dell'archiviazione di dischi temporanei di Azure e Machine Creation Services (MCS) (I/O MCS)** Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.

Le considerazioni importanti sono le seguenti:

- Non è possibile creare un catalogo delle macchine con il disco del sistema operativo temporaneo e l'I/O MCS abilitati contemporaneamente.
- Nella procedura guidata **Machine Catalog Setup** (Configurazione del catalogo delle macchine), se si seleziona **Azure ephemeral OS disk** (Disco del sistema operativo temporaneo di Azure) nella pagina **Storage and License Types** (Tipi di licenze e di archiviazione) non si ottiene l'opzione per le impostazioni del disco della cache write-back nella pagina **Disk Settings** (Impostazioni disco).






- I parametri PowerShell (`UseWriteBackCache` e `UseEphemeralOsDisk`) impostati su **true** in `New-ProvScheme` o `Set-ProvScheme` restituiscono un messaggio di errore.
- Per i cataloghi delle macchine esistenti creati con entrambe le funzionalità abilitate, è comunque possibile:
  - aggiornare un catalogo delle macchine
  - aggiungere o eliminare macchine virtuali
  - eliminare un catalogo delle macchine

### Crittografia lato server di Azure

Citrix DaaS supporta le chiavi di crittografia gestite dal cliente per i dischi gestiti di Azure tramite Azure Key Vault. Con questo supporto è possibile gestire i requisiti organizzativi e di conformità crittografando i dischi gestiti del catalogo delle macchine utilizzando la propria chiave di crittografia. Per ulteriori informazioni, vedere Crittografia lato server dell'archiviazione su disco di Azure.

Quando si utilizza questa funzionalità per i dischi gestiti:

- Per cambiare la chiave con cui è crittografato il disco, è necessario modificare la chiave corrente in `DiskEncryptionSet`. Tutte le risorse associate a tale modifica `DiskEncryptionSet` devono essere crittografate con la nuova chiave.
- Quando si disabilita o si elimina la chiave, tutte le macchine virtuali con dischi che utilizzano tale chiave si spengono automaticamente. Dopo lo spegnimento, le macchine virtuali non sono utilizzabili a meno che la chiave non venga nuovamente abilitata o non venga assegnata una nuova chiave. Qualsiasi catalogo che utilizza la chiave non può essere acceso e non è possibile aggiungervi macchine virtuali.

#### Considerazioni importanti quando si utilizzano chiavi di crittografia gestite dal cliente

Quando si utilizza questa funzionalità, tenere presente quanto segue:

- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono risiedere nella stessa sottoscrizione e area geografica.
- Dopo aver abilitato la chiave di crittografia gestita dal cliente, non è possibile disabilitarla in un secondo momento. Se si desidera disabilitare o rimuovere la chiave di crittografia gestita dal cliente, copiare tutti i dati su un disco gestito diverso che non utilizza la chiave di crittografia gestita dal cliente.
- I dischi creati da immagini personalizzate crittografate utilizzando la crittografia lato server e le chiavi gestite dal cliente devono essere crittografati utilizzando le stesse chiavi gestite dal cliente. Questi dischi devono trovarsi nella stessa sottoscrizione.
- Le snapshot create da dischi crittografati con crittografia lato server e chiavi gestite dal cliente devono essere crittografate con le stesse chiavi gestite dal cliente.
- I dischi, le snapshot e le immagini crittografati con chiavi gestite dal cliente non possono passare a un altro gruppo di risorse e a un'altra sottoscrizione.
- I dischi gestiti attualmente o precedentemente crittografati utilizzando Crittografia dischi di Azure non possono essere crittografati utilizzando chiavi gestite dal cliente.
- Fare riferimento al sito Microsoft per le limitazioni sui set di crittografia dei dischi per ciascuna regione.

> **Nota:**
>
> Per informazioni sulla configurazione della crittografia lato server di Azure, vedere Guida rapida: creare un insieme di credenziali delle chiavi utilizzando il portale di Azure.

### Chiave di crittografia gestita dal cliente di Azure

Quando si crea un catalogo delle macchine, è possibile scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Un set di crittografia dei dischi (DES, Disk Encryption Set) rappresenta una chiave gestita dal cliente. Per utilizzare questa funzionalità, è necessario prima creare il DES in Azure. Un DES ha il formato seguente:

- /subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption

Selezionare un DES dall'elenco. Il DES selezionato deve essere nella stessa sottoscrizione e nella stessa regione delle risorse. Se l'immagine è crittografata con un DES, utilizzare lo stesso DES durante la creazione del catalogo delle macchine. Non è possibile modificare il DES dopo aver creato il catalogo.

Se si crea un catalogo con una chiave di crittografia e successivamente si disabilita il DES corrispondente in Azure, non si potrà più accendere alle macchine nel catalogo o aggiungervi macchine.

Se si desidera creare un catalogo di macchine utilizzando comandi PowerShell, in cui la chiave di crittografia sia una chiave gestita dal cliente, procedere come segue:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Inserire `cd xdhyp:/`.
4. Inserire `cd .\HostingUnits\(your hosting unit)`.
5. Immettere cd diskencryptionset.folder.
6. Immettere dir per ottenere l'elenco dei set di crittografia del disco.
7. Copiare l'ID di un set di crittografia del disco.
8. Creare una stringa di proprietà personalizzata che includa l'ID del set di crittografia del disco. Ad esempio:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value=`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
     Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
    resourceGroups/abc/providers/Microsoft.Compute/
    diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

9. Creare un pool di identità se non è già stato creato. Ad esempio:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

10. Eseguire il comando New-ProvScheme: Ad esempio:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
    resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
     def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
     " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
    folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
    def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. Completate la creazione del catalogo di macchine.

### Crittografia del disco di Azure sull'host

È possibile creare un catalogo di macchine MCS con crittografia in modalità host. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità. È possibile utilizzare una VM o specifiche di modello come input per il profilo di una macchina.

Questo metodo di crittografia non crittografa i dati tramite l'archiviazione di Azure. Il server che ospita la macchina virtuale crittografa i dati e quindi i dati crittografati fluiscono attraverso il server di archiviazione di Azure. Quindi, questo metodo di crittografia crittografa i dati per tutto il loro percorso dall'inizio alla fine.

**Restrizioni:**

La crittografia del disco di Azure sull'host è:

- non supportata per tutte le dimensioni delle macchine di Azure

- incompatibile con la crittografia del disco di Azure

Per creare un catalogo di macchine con funzionalità di crittografia sull'host:

1. Verificare se l'abbonamento ha la funzionalità di crittografia sull'host abilitata o meno. A questo scopo, vedere https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Se non è abilitata, è necessario abilitarla per l'abbonamento. Per informazioni sull'attivazione della funzionalità per l'abbonamento, vedere https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Verificare se una particolare dimensione di macchina virtuale di Azure supporta o meno la crittografia sull'host. A questo scopo, in una finestra di PowerShell, eseguire uno dei seguenti comandi:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Creare una macchina virtuale o specifiche di modello come input per il profilo della macchina nel portale di Azure con la crittografia sull'host abilitata.

   - Se si desidera creare una macchina virtuale, selezionare una dimensione di macchina virtuale che supporti la crittografia sull'host. Dopo aver creato la macchina virtuale, viene abilitata la relativa proprietà **Encryption at host** (Crittografia sull'host).
   - Se si desidera utilizzare specifiche di modello, assegnare al parametro `Encryption at Host` il valore **true** all'interno di `securityProfile`.

4. Creare un catalogo di macchine MCS con il flusso di lavoro dei profili delle macchine, selezionando una VM o specifiche di modello.

   - Disco del sistema operativo/disco dati: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma
   - Disco del sistema operativo temporaneo: viene crittografato solo tramite chiave gestita dalla piattaforma
   - Disco cache: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma

   È possibile creare il catalogo delle macchine utilizzando l'interfaccia Full Configuration o eseguendo i comandi PowerShell.

### Recuperare le informazioni sulla crittografia dell'host da un profilo macchina

È possibile recuperare le informazioni sulla crittografia sull'host da un profilo di macchina quando si esegue il comando PowerShell con il parametro `AdditionalData`. Se il parametro `EncryptionAtHost` è **True**, significa che la crittografia sull'host è abilitata per il profilo macchina.

Ad esempio: quando l'input del profilo macchina è una VM, eseguire il seguente comando:

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
     resourcegroup\def.vm).AdditionalData
2 <!--NeedCopy-->
```

Ad esempio: quando l'input del profilo macchina è una specifica di modello, eseguire il seguente comando:

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
     resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
     templatespecversion).AdditionalData
2 <!--NeedCopy-->
```

### Doppia crittografia su disco gestito

È possibile creare un catalogo di macchine con doppia crittografia. In tutti i cataloghi creati con questa funzionalità tutti i dischi lato server sono crittografati con chiavi gestite dalla piattaforma e dal cliente. L'utente possiede e gestisce Azure Key Vault, Encryption Key e Disk Encryption Sets (DES).

La doppia crittografia è la crittografia lato piattaforma (impostazione predefinita) e la crittografia gestita dal cliente (CMEK). Pertanto, se si è un cliente altamente sensibile alla sicurezza e si nutre preoccupazione per il rischio associato a qualsiasi algoritmo di crittografia, implementazione o chiave compromessa, è possibile optare per questa doppia crittografia. Il sistema operativo persistente e i dischi di dati, le snapshot e le immagini sono tutti crittografati quando inattivi con doppia crittografia.

> **Nota:**
>
> - È possibile creare e aggiornare un catalogo di macchine con doppia crittografia utilizzando l'interfaccia Full Configuration e i comandi PowerShell.
> - È possibile utilizzare un flusso di lavoro non basato su profili macchina o un flusso di lavoro basato sul profilo macchina per creare o aggiornare un catalogo di macchine con doppia crittografia.
> - Se si utilizza un flusso di lavoro non basato su profili di macchina per creare un catalogo di macchine, è possibile riutilizzare il valore `DiskEncryptionSetId` archiviato.
> - Se si utilizza un profilo macchina, è possibile utilizzare una VM o un specifica di modello

> come input per il profilo della macchina.

Limitazioni:

- La doppia crittografia non è supportata per i dischi Ultra Disks o Premium SSD v2.
- La doppia crittografia non è supportata sui dischi non gestiti.
- Se si disattiva una chiave del Disk Encryption Set associata a un catalogo, le VM del catalogo vengono disattivate.
- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono essere nella stessa sottoscrizione e area geografica.
- È possibile creare solo fino a 50 set di crittografia del disco per regione per abbonamento.
- Non è possibile aggiornare un catalogo macchine che ha già `DiskEncryptionSetId` con un `DiskEncryptionSetId` diverso.

#### Creare un catalogo di macchine con doppia crittografia

1. Creare un Azure Key Vault e DES con chiavi gestite dalla piattaforma e gestite dal cliente. Per informazioni su come creare un Azure Key Vault e un DES, vedere Usare il portale di Azure per abilitare la doppia crittografia dei dati inattivi per i dischi gestiti.
2. Per sfogliare i set di crittografia del disco disponibili nella propria connessione di hosting:

   a) Aprire una finestra di **PowerShell**.
   b) Eseguire i seguenti comandi PowerShell:
      i. asnp citrix*
      ii. cd xdhyp:
      iii. cd HostingUnits
      iv. cd yourHostingUnitName (ad esempio azure-est)
      v. cd diskencryptionset.folder
      vi. dir

   È possibile utilizzare un ID del `DiskEncryptionSet` per creare o aggiornare un catalogo utilizzando proprietà personalizzate.
3. Se si desidera utilizzare il flusso di lavoro del profilo macchina, creare una VM o una specifica di modello come input per il profilo della macchina.

   - Se si desidera utilizzare una VM come input del profilo macchina:
     a) Creare una macchina virtuale nel portale di Azure.
     b) Passare a **Dischi > Gestione delle chiavi** per crittografare la VM direttamente con qualsiasi `DiskEncryptionSetID`.

- Se si desidera utilizzare una specifica di modello come input del profilo della macchina:
  a) Nel modello, in `properties>storageProfile>osDisk>managedDisk`, aggiungere il parametro `diskEncryptionSet` e l'ID del DES a doppia crittografia.

4. Creare il catalogo di macchine.

   - Se si utilizza Web Studio, eseguire una delle seguenti operazioni oltre alla procedura descritta in Creare cataloghi di macchine.

     – Se non si utilizza un flusso di lavoro basato sul profilo macchina, nella pagina **Impostazioni disco** selezionare **Use the following key to encrypt data on each machine** (Usa la seguente chiave per crittografare i dati su ciascuna macchina). Quindi, selezionare il proprio DES a doppia crittografia dal menu a discesa. Continuare a creare il catalogo.
     – Se si utilizza il flusso di lavoro del profilo macchina, nella pagina **Master Image** selezionare un'immagine master e un profilo macchina. Assicurarsi che il profilo macchina abbia un ID set crittografia disco nelle sue proprietà.

   Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

   - Se si utilizlzano i comandi di PowerShell, eseguire una delle seguenti operazioni:

     – Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata `DiskEncryptionSetId` nel comando `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<
   CustomProperties xmlns="http://schemas.citrix.com/2014/
   xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks"
    Value="true" />
<Property xsi:type="StringProperty" Name="
   StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
```

```
-ServiceOffering "Redacted"
<!--NeedCopy-->
```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

Completare la creazione di un catalogo utilizzando l'SDK Remote PowerShell. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

#### Convertire un catalogo non crittografato per utilizzare la doppia crittografia

È possibile aggiornare il tipo di crittografia di un catalogo di macchine (utilizzando proprietà personalizzate o il profilo macchina) solo se il catalogo in precedenza non era crittografato.

- Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata DiskEncryptionSetId nel comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
   resourceGroups/Sample-RG/providers/Microsoft.Compute/
   diskEncryptionSets/SampleEncryptionSet" />
</CustomProperties>'
<!--NeedCopy-->
```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
    XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
   resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

Una volta completata l'operazione, tutte le nuove macchine virtuali aggiunte al catalogo vengono crittografate due volte dalla chiave associata al DES selezionato.

#### Verificare che il catalogo sia crittografato con doppia crittografia

- In Web Studio:
  1. Passare a **Machine Catalogs** (Cataloghi di macchine).
  2. Selezionare il catalogo da verificare. Fare clic sulla scheda **Template Properties** (Proprietà del modello) situata nella parte inferiore dello schermo.
  3. In **Azure Details** (Dettagli di Azure) verificare l'ID del set di crittografia del disco in **Disk Encryption Set**. Se l'ID DES del catalogo è vuoto, il catalogo non è crittografato.
  4. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.
- Utilizzando i comandi PowerShell:
  1. Aprire la finestra di **PowerShell**.
  2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
  3. Utilizzare `Get-ProvScheme` per ottenere le informazioni del proprio catalogo macchine. Ad esempio:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
<!--NeedCopy-->
```

  4. Recuperare la proprietà personalizzata DES Id del catalogo di macchine. Ad esempio:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions
   /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
   -RG/providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
<!--NeedCopy-->
```

  5. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.

### Host dedicati di Azure

È possibile utilizzare MCS per eseguire il provisioning di macchine virtuali su host dedicati di Azure. Prima di eseguire il provisioning delle macchine virtuali su host dedicati di Azure:

- Creare un gruppo host.
- Creare host nel gruppo host.
- Assicurarsi che la capacità host sia sufficiente per la creazione di cataloghi e macchine virtuali.

È possibile creare un catalogo di macchine con tenancy host definita tramite il seguente script PowerShell:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

Quando si utilizza MCS per eseguire il provisioning di macchine virtuali su host Azure dedicati, tenere in considerazione quanto segue:

- Un *host dedicato* è una proprietà del catalogo e non può essere modificata una volta creato il catalogo. La tenancy dedicata non è attualmente supportata in Azure.
- Quando si utilizza il parametro `HostGroupId`, è necessario un gruppo host di Azure preconfigurato nella regione dell'unità di hosting.
- È necessario il posizionamento automatico di Azure. Questa funzionalità invia una richiesta di eseguire l'onboarding della sottoscrizione associata al gruppo host. Per ulteriori informazioni, vedere Set di scalabilità VM negli host dedicati di Azure - Anteprima pubblica. Se il posizionamento automatico non è abilitato, MCS genererà un errore durante la creazione del catalogo.

### Raccolta di calcolo di Azure

Utilizzare la Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise di Azure) come repository di immagini pubblicate per macchine di cui è stato eseguito il provisioning con MCS in Azure. È possibile archiviare un'immagine pubblicata nella raccolta per accelerare la creazione e l'attivazione dei dischi del sistema operativo, migliorando i tempi di avvio del sistema e delle applicazioni per le macchine virtuali non persistenti. La Raccolta di calcolo di Azure contiene i tre elementi seguenti:

- Raccolta. Le immagini sono memorizzate qui. MCS crea una raccolta per ogni catalogo delle macchine.

- Definizione dell'immagine della raccolta. Questa definizione include informazioni (tipo e stato del sistema operativo, regione di Azure) sull'immagine pubblicata. MCS crea una definizione di immagine per ogni immagine creata per il catalogo.
- Versione dell'immagine della raccolta. Ogni immagine in una Raccolta di calcolo di Azure può avere più versioni e ogni versione può avere più repliche in regioni diverse. Ogni replica è una copia completa dell'immagine pubblicata. Citrix DaaS crea una versione dell'immagine Standard_LRS (versione 1.0.0) per ogni immagine con il numero appropriato di repliche nella regione del catalogo, in base al numero di macchine nel catalogo, al rapporto di replica configurato e al numero massimo configurato di repliche.

> **Nota:**
>
> La funzionalità Raccolta di calcolo di Azure è compatibile solo con i dischi gestiti. Non è disponibile per i cataloghi delle macchine legacy.

Per ulteriori informazioni, vedere Panoramica della Raccolta immagini condivise di Azure.

#### Accedi alle immagini dalla Raccolta di calcolo di Azure

Quando si seleziona un'immagine da utilizzare per la creazione di un catalogo delle macchine, è possibile selezionare le immagini create nella Raccolta di calcolo di Azure. Queste immagini vengono visualizzate nell'elenco delle immagini nella schermata **Master Image** (Immagine master) della procedura guidata di configurazione del catalogo delle macchine.

Per visualizzare queste immagini, è necessario:

1. Configurare un sito Citrix Virtual Apps and Desktops.
2. Connettersi ad Azure Resource Manager.
3. Nel portale di Azure, creare un gruppo di risorse. Per ulteriori informazioni, consultare Creare una Raccolta immagini condivise di Azure utilizzando il portale.
4. Nel gruppo di risorse, creare una Raccolta di calcolo di Azure.
5. Nella Raccolta di calcolo di Azure, creare una definizione di immagine.
6. Nella definizione dell'immagine, creare una versione dell'immagine.

#### Configurare la Raccolta di calcolo di Azure

Utilizzare il comando `New-ProvScheme` per creare uno schema di provisioning con il supporto della Raccolta di calcolo di Azure. Utilizzare il comando `Set-ProvScheme` per abilitare o disabilitare questa funzionalità per uno schema di provisioning e per modificare il rapporto di replica e i valori massimi della replica.

Sono state aggiunte tre proprietà personalizzate agli schemi di provisioning per supportare la funzionalità Raccolta di calcolo di Azure:

`UseSharedImageGallery`

- Definisce se usare la Raccolta di calcolo di Azure per archiviare le immagini pubblicate. Se impostata su **True**, l'immagine viene memorizzata come immagine della Raccolta di calcolo di Azure, altrimenti viene memorizzata come snapshot.
- I valori validi sono **True** e **False**.
- Se la proprietà non è definita, il valore predefinito è **False**.

`SharedImageGalleryReplicaRatio`

- Definisce il rapporto tra macchine e repliche di versioni di immagini della raccolta.
- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, vengono utilizzati i valori predefiniti. Il valore predefinito per i dischi del sistema operativo persistenti è 1.000 e il valore predefinito per i dischi del sistema operativo non persistenti è 40.

`SharedImageGalleryReplicaMaximum`

- Definisce il numero massimo di repliche per ogni versione dell'immagine della raccolta.
- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, il valore predefinito è 10.
- Azure attualmente supporta fino a 10 repliche per una singola versione dell'immagine della raccolta. Se la proprietà è impostata su un valore maggiore di quello supportato da Azure, MCS tenta di utilizzare il valore specificato. Azure genera un errore, che viene registrato da MCS, e lascia invariato il numero di repliche corrente.

> **Suggerimento:**
>
> Quando si utilizza la Raccolta di calcolo di Azure per archiviare un'immagine pubblicata per i cataloghi di cui è stato eseguito il provisioning con MCS, MCS imposta il numero di repliche delle versioni delle immagini della raccolta in base al numero di macchine nel catalogo, al rapporto di replica e al numero massimo di repliche. Il conteggio delle repliche viene calcolato dividendo il numero di macchine nel catalogo per il rapporto di replica (arrotondando per eccesso al valore intero più vicino) e quindi limitando il valore al numero massimo di repliche. Ad esempio, con un rapporto di replica di 20 e un massimo di 5, per 0-20 macchine viene creata una replica, per 21-40 macchine vengono create 2 repliche, per 41-60 macchine vengono create 3 repliche, per 61-80 macchine vengono create 4 repliche e per 81 macchine o più vengono create 5 repliche.

**Caso d'uso: aggiornamento del rapporto di replica e del numero massimo di repliche della Raccolta di calcolo di Azure** Il catalogo di macchine esistente utilizza la Raccolta di calcolo di Azure.

Utilizzare il comando `Set-ProvScheme` per aggiornare le proprietà personalizzate per tutte le macchine esistenti nel catalogo e per tutte le macchine future:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

**Caso d'uso: convertire un catalogo di snapshot in un catalogo della Raccolta di calcolo di Azure**

Per questo caso d'uso:

1. Eseguire `Set-ProvScheme` con il contrassegno `UseSharedImageGallery` impostato su **True**. Facoltativamente, includere le proprietà `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Suggerimento:**
>
> I parametri `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` non sono richiesti. Dopo che il comando `Set-ProvScheme` è completato, l'immagine della Raccolta di calcolo di Azure non è stata ancora creata. Una volta configurato il catalogo per l'utilizzo della raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata nella raccolta. Il comando di aggiornamento del catalogo crea la raccolta, l'immagine della raccolta e la versione dell'immagine. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto il conteggio delle repliche viene aggiornato, se appropriato.

> Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando l'immagine della Raccolta di calcolo di Azure e tutte le macchine di cui è stato eseguito il provisioning vengono create utilizzando l'immagine. La vecchia snapshot viene ripulita automaticamente entro poche ore.

**Caso d'uso: conversione di un catalogo della Raccolta di calcolo di Azure in un catalogo di istantanee** Per questo caso d'uso:

1. Eseguire `Set-ProvScheme` con il contrassegno `UseSharedImageGallery` impostato su **False** o non definito.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance"> <Property xsi:type="StringProperty" Name="StorageType"
     Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
     UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
     Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
2 <!--NeedCopy-->
```

> **Suggerimento:**
>
> A differenza dell'aggiornamento da una snapshot a un catalogo della Raccolta di calcolo di Azure, i dati personalizzati per ogni macchina non sono ancora aggiornati per riflettere le nuove proprietà personalizzate. Eseguire il comando seguente per visualizzare le proprietà personalizzate originali della Raccolta di calcolo di Azure: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Dopo il completamento del comando `Set-ProvScheme`, la snapshot dell'immagine non è stata ancora creata. Una volta configurato il catalogo per non utilizzare la raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata come snapshot. Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando la snapshot e tutte le macchine di cui è stato eseguito il provisioning vengono create dalla snapshot. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto i dati della macchina personalizzati vengono aggiornati per riflettere che `UseSharedImageGallery` è impostato su **False**. Le vecchie risorse della Raccolta di calcolo di Azure (raccolta, immagine e versione) vengono ripulite automaticamente nel giro di poche ore.

### Eseguire il provisioning delle macchine in zone di disponibilità specificate

È possibile effettuare il provisioning delle macchine in zone di disponibilità specifiche in ambienti Azure. È possibile farlo utilizzando l'interfaccia Full Configuration (Configurazione completa) o PowerShell.

> **Nota:**
>
> Se non viene specificata alcuna zona, MCS consente ad Azure di posizionare le macchine all'interno della regione. Se viene specificata più di una zona, MCS distribuisce in modo casuale le macchine nelle zone.

#### Configurazione delle zone di disponibilità nell'interfaccia Full Configuration (Configurazione completa)

Quando si crea un catalogo delle macchine, è possibile specificare le zone di disponibilità in cui si desidera eseguire il provisioning delle macchine. Nella pagina **Virtual Machines** (Macchine virtuali), selezionare una o più zone di disponibilità in cui si desidera creare macchine.

Vi sono due motivi per cui non sono disponibili zone di disponibilità: la regione non ha zone di disponibilità o la dimensione della macchina selezionata non è disponibile.

#### Configurazione delle zone di disponibilità tramite PowerShell

Tramite PowerShell, è possibile visualizzare gli elementi di inventario offerti da Citrix DaaS utilizzando `Get-Item`. Ad esempio, per visualizzare l'offerta di servizi *Eastern US region* `Standard_B1ls` (Regione degli Stati Uniti orientali):

```
1 $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
     name\East US.region\serviceoffering.folder\Standard_B1ls.
     serviceoffering"
2 <!--NeedCopy-->
```

Per visualizzare le zone, utilizzare il parametro `AdditionalData` per l'elemento:

```
$serviceOffering.AdditionalData
```

Se le zone di disponibilità non sono specificate, non vi è alcun cambiamento nel modo in cui viene eseguito il provisioning delle macchine.

Per configurare le zone di disponibilità tramite PowerShell, utilizzare la proprietà personalizzata **Zones** (Zone) disponibile con l'operazione `New-ProvScheme`. La proprietà **Zones** (Zone) definisce un elenco di zone di disponibilità in cui eseguire il provisioning delle macchine. Tali zone possono includere una o più zone di disponibilità. Ad esempio, `<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` per le zone 1 e 3.

Utilizzare il comando `Set-ProvScheme` per aggiornare le zone per uno schema di provisioning.

Se viene fornita una zona non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore che fornisce istruzioni su come correggere il comando non valido.

> **Suggerimento:**
>
> Se si specifica una proprietà personalizzata non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore pertinente.

### Usare gruppi di host e zone di disponibilità di Azure allo stesso tempo

Esiste un controllo preliminare per valutare se la creazione di un catalogo di macchine avrà esito positivo in base alla zona di disponibilità specificata nella proprietà personalizzata e alla zona del gruppo host. La creazione del catalogo non riesce se la proprietà personalizzata della zona di disponibilità non corrisponde alla zona del gruppo host.

Per informazioni sulla configurazione delle zone di disponibilità tramite PowerShell, vedere Configurazione delle zone di disponibilità tramite PowerShell.

Per informazioni sugli host dedicati di Azure, vedere Host dedicati di Azure.

La tabella seguente descrive le varie combinazioni di zona di disponibilità e zona del gruppo host e indica quali determinano la creazione riuscita o non riuscita di un catalogo di macchine.

| Zona del gruppo ospitante | Zona di disponibilità nella proprietà personalizzata | Risultato della creazione del catalogo di macchine |
|---|---|---|
| Specificato. Ad esempio, il gruppo host si trova nella Zona 1 | Non specificato | Riuscito. Le macchine vengono create nella zona del gruppo ospitante |
| Specificato. Ad esempio, il gruppo host si trova nella Zona 1 | Stessa zona della zona del gruppo ospitante. Ad esempio, la zona nella proprietà personalizzata è impostata su 1 | Riuscito. Vengono create macchine nella Zona 1 |
| Specificato. Ad esempio, il gruppo host si trova nella Zona 1 | Diversa dalla zona del gruppo ospitante. Ad esempio, la zona nella proprietà personalizzata è impostata su 2 | Poiché la zona di disponibilità specificata e la zona del gruppo host non corrispondono, la creazione del catalogo non riesce e durante i controlli preliminari viene restituito un errore pertinente |

| Zona del gruppo ospitante | Zona di disponibilità nella proprietà personalizzata | Risultato della creazione del catalogo di macchine |
|---|---|---|
| Specificato. Ad esempio, il gruppo host si trova nella Zona 1 | Più zone specificate. Ad esempio, le zone nelle proprietà personalizzate sono impostate su 1,2 o 2,3 | Poiché la zona di disponibilità specificata e la zona del gruppo host non corrispondono, la creazione del catalogo non riesce e durante i controlli preliminari viene restituito un errore pertinente |
| Non specificato. Ad esempio, la zona del gruppo ospitante è None | Non specificato | Poiché la zona di disponibilità specificata e la zona del gruppo host corrispondono (ovvero nessuna zona), la creazione del catalogo riesce. Non vengono create macchine in nessuna zona |
| Non specificato. Ad esempio, la zona del gruppo ospitante è None | Specificato. Ad esempio, le zone nella proprietà personalizzata sono impostate su una o più zone | Poiché la zona di disponibilità specificata e la zona del gruppo host non corrispondono, la creazione del catalogo non riesce e durante i controlli preliminari viene restituito un errore pertinente |

### Disco temporaneo di Azure

I dischi temporanei di Azure consentono di riutilizzare il disco della cache o il disco temporaneo per archiviare il disco del sistema operativo per una macchina virtuale abilitata per Azure. Questa funzionalità è utile per gli ambienti Azure che richiedono un disco SSD a prestazioni più elevate rispetto a un disco rigido standard.

> **Nota:**
>
> I cataloghi persistenti non supportano i dischi del sistema operativo temporanei.

I dischi del sistema operativo temporanei richiedono che lo schema di provisioning utilizzi dischi gestiti e una Raccolta di calcolo di Azure. Per ulteriori informazioni, vedere Raccolta immagini condivise di Azure.

#### Utilizzo di PowerShell per configurare un disco temporaneo

Per configurare un disco del sistema operativo temporaneo di Azure per un catalogo, utilizzare il parametro `UseEphemeralOsDisk` in `Set-ProvScheme`. Impostare il valore del parametro `UseEphemeralOsDisk` su **true**.

> **Nota:**
>
> Per utilizzare questa funzionalità, è necessario abilitare anche i parametri `UseManagedDisks` e `UseSharedImageGallery`.

Ad esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
     CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
     "true" />
4 <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
     true" />
5 </CustomProperties>'
6 <!--NeedCopy-->
```

#### Memorizzazione di un disco del sistema operativo temporaneo

È possibile memorizzare un disco del sistema operativo temporaneo sul disco temporaneo della macchina virtuale o su un disco di risorse. Questa funzionalità consente di utilizzare un disco del sistema operativo temporaneo con una macchina virtuale che non ha una cache o ha una cache insufficiente. Tali macchine virtuali dispongono di un disco temporaneo o di risorse per archiviare un disco del sistema operativo temporaneo, ad esempio `Ddv4`.

Considerare quanto segue:

- Un disco temporaneo viene memorizzato nel disco della cache della macchina virtuale o nel disco temporaneo (risorsa) della macchina virtuale. Il disco della cache è preferibile rispetto al disco temporaneo, a meno che il disco della cache non sia abbastanza grande da ospitare i contenuti del disco del sistema operativo.
- Per gli aggiornamenti, una nuova immagine più grande del disco della cache ma più piccola del disco temporaneo comporta la sostituzione del disco del sistema operativo temporaneo con il disco temporaneo della macchina virtuale.

### Tipologie di archiviazione

Selezionare diversi tipi di archiviazione per le macchine virtuali negli ambienti di Azure che utilizzano MCS. Per le macchine virtuali di destinazione, MCS supporta:

- Disco del sistema operativo: SSD premium, SSD o HDD
- Disco della cache write-back: SSD premium, SSD o HDD

Quando si utilizzano questi tipi di archiviazione, considerare quanto segue:

- Assicurarsi che la macchina virtuale supporti il tipo di archiviazione selezionato.
- Se la configurazione utilizza un disco temporaneo di Azure, non è disponibile l'opzione per l'impostazione del disco della cache write-back.

> **Suggerimento:**
>
> `StorageType` è configurato per un tipo di sistema operativo e un account di archiviazione. `WBCDiskStorageType` è configurato per il tipo di archiviazione della cache write-back. Per un catalogo normale, è necessario `StorageType`. Se `WBCDiskStorageType` non è configurato, `StorageType` viene utilizzato come impostazione predefinita per `WBCDiskStorageType`.

Se WBCDiskStorageType non è configurato, StorageType viene utilizzato come impostazione predefinita per WBCDiskStorageType.

#### Configurazione dei tipi di archiviazione

Per configurare i tipi di archiviazione per le macchine virtuali, utilizzare il parametro `StorageType` in `New-ProvScheme`. Impostare il valore del parametro `StorageType` su uno dei tipi di archiviazione supportati.

Di seguito è riportato un set di esempio del parametro `CustomProperties` in uno schema di provisioning:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </CustomProperties>'
6 <!--NeedCopy-->
```

### Abilita l'archiviazione con ridondanza della zona

È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione del catalogo. Replica il disco gestito di Azure in modo sincrono in più zone di disponibilità, il che consente di effettuare il ripristino dopo che si è verificato un errore in una zona utilizzando la ridondanza di altre.

È possibile specificare **Premium_ZRS** e **StandardSSD_ZRS** nelle proprietà personalizzate del tipo di archiviazione. L'archiviazione ZRS può essere impostata utilizzando le proprietà personalizzate esistenti o tramite il modello **MachineProfile**. L'archiviazione ZRS è supportata anche con il comando `Set-ProvVMUpdateTimeWindow` con i parametri `-StartsNow` e `-DurationInMinutes -1`. È possibile modificare la macchina esistente dall'archiviazione LRS a quella ZRS.

> **Nota:**
>
> - `StartsNow` indica che l'ora di inizio pianificata è l'ora corrente.
> - `DurationInMinutes` con un numero negativo (ad esempio -1) indica che non vi è alcun limite superiore nella finestra oraria della pianificazione.

**Limitazioni:**

- Supportato solo nei dischi gestiti
- Supportato solo se si utilizzano unità a stato solido (SSD) premium e standard
- Non supportato in `StorageTypeAtShutdown`
- Disponibile solo in alcune aree geografiche.
- Le prestazioni di Azure diminuiscono quando si creano dischi ZRS su larga scala. Pertanto, alla prima accensione, accendere le macchine in batch più piccoli (meno di 300 macchine alla volta)

**Imposta l'archiviazione con ridondanza della zona come tipo di archiviazione su disco** È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione iniziale del catalogo oppure aggiornare il tipo di archiviazione in un catalogo esistente.

**Seleziona l'archiviazione con ridondanza della zona utilizzando i comandi PowerShell** Quando si crea un nuovo catalogo in Azure usando il comando `New-ProvScheme` di PowerShell, utilizzare il valore `Standard_ZRS` in `StorageAccountType`.
Ad esempio:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

Quando lo si imposta, questo valore viene convalidato da un'API dinamica che determina se può essere utilizzato correttamente. Le seguenti eccezioni possono verificarsi se l'uso di ZRS non è valido per il proprio catalogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: la proprietà personalizzata StorageTypeAtShutdown non può essere utilizzata con l'archiviazione ZRS.
- **StorageAccountTypeNotSupportedInRegion**: questa eccezione si verifica se si tenta di utilizzare l'archiviazione ZRS in un'area di Azure che non supporta ZRS
- **ZrsRequiresManagedDisks**: è possibile utilizzare l'archiviazione con ridondanza della zona solo con dischi gestiti.

È possibile impostare il tipo di archiviazione su disco utilizzando le seguenti proprietà personalizzate:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante la creazione del catalogo, viene utilizzato il disco del sistema operativo del profilo macchina `StorageType` se non sono impostate le proprietà personalizzate.

### VM riservate di Azure (anteprima)

Le macchine virtuali di Azure con elaborazione riservata garantiscono che il desktop virtuale sia crittografato in memoria e protetto durante l'uso.

È possibile utilizzare MCS per creare un catalogo con macchine virtuali riservate di Azure. È necessario utilizzare il flusso di lavoro del profilo macchina per creare un catalogo di questo tipo. È possibile utilizzare una macchina virtuale e una specifica di modello ARM come input del profilo macchina.

#### Considerazioni importanti per le macchine virtuali riservate

Le considerazioni importanti relative alle dimensioni delle macchine virtuali supportate e alla creazione di un catalogo di macchine con macchine virtuali riservate sono le seguenti:

- Dimensioni di VM supportate: le VM riservate supportano le seguenti dimensioni di VM:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Creare un catalogo di macchine con macchine virtuali riservate.
  - È possibile creare un catalogo di macchine con Azure Confidential VMs utilizzando l'interfaccia Full Configuration e i comandi PowerShell.

- È necessario utilizzare un flusso di lavoro basato sul profilo macchina per creare un catalogo di macchine virtuali riservate di Azure. È possibile utilizzare una macchina virtuale e una specifica di modello come input del profilo macchina.
- L'immagine master e l'input del profilo macchina devono essere entrambi abilitati con lo stesso tipo di sicurezza riservato. I tipi di sicurezza sono:
  * VMGuestStateOnly: VM riservata con solo lo stato di ospite della VM crittografato
  * DiskWithVMGuestState: VM riservata con disco del sistema operativo e stato di ospite della VM crittografati con chiave gestita dalla piattaforma o chiave gestita dal cliente. È possibile crittografare sia il disco del sistema operativo normale che quello temporaneo.
- È possibile ottenere informazioni riservate sulle VM di vari tipi di risorse quali disco gestito, snapshot, immagine di Azure Compute Gallery, VM e specifiche di modello ARM utilizzando il parametro AdditionalData. Ad esempio:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
   \image.folder\username-dev-testing-rg.resourcegroup\
   username-dev-tsvda.vm).AdditionalData
<!--NeedCopy-->
```

  I campi dati aggiuntivi sono:

  * DiskSecurityType
  * ConfidentialVMDiskEncryptionSetId
  * DiskSecurityProfiles

  Per ottenere la proprietà di riservatezza delle dimensioni di una macchina, eseguire il comando seguente: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  Il campo dati aggiuntivo è `ConfidentialComputingType`.
- Non è possibile modificare l'immagine master o il profilo macchina passando dal tipo di protezione riservato a quello non riservato o dal tipo di protezione non riservato a quello riservato.
- Vengono visualizzati i messaggi di errore appropriati per eventuali configurazioni errate.

**Creare un catalogo di macchine con VM riservate**

1. Creare un'immagine master abilitata con una macchina virtuale riservata. Per creare la macchina virtuale master, vedere Guida introduttiva: Distribuire una macchina virtuale riservata con un modello di Resource Manager e Guida introduttiva: Creare una macchina virtuale riservata in AMD nel portale di Azure.

2. Utilizzare la macchina virtuale master come profilo della macchina o creare una specifica del modello di Azure. Per informazioni sulla creazione di una specifica del modello, vedere Creare una specifica del modello di Azure.
3. Creare il catalogo di macchine basato sul profilo macchina utilizzando l'interfaccia Full Configuration o i comandi PowerShell.

> **Nota:**
>
> Assicurarsi che l'immagine master e l'input del profilo della macchina siano entrambi abilitati con lo stesso tipo di sicurezza riservato.

### Azure Marketplace

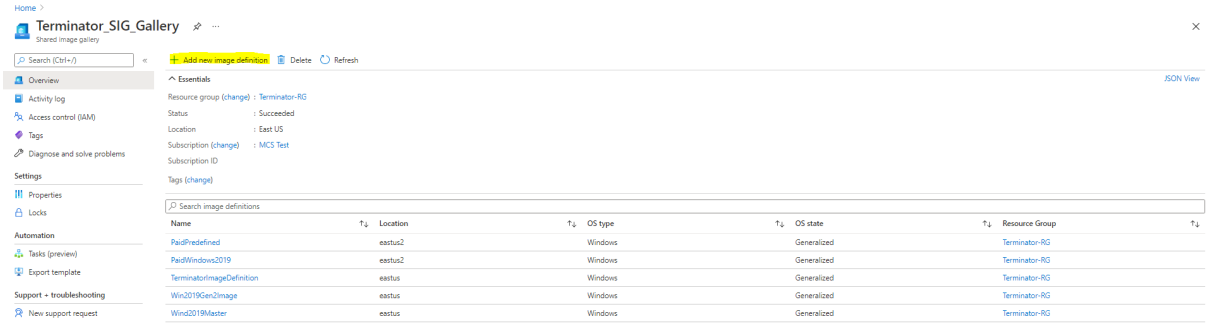
Citrix DaaS supporta l'utilizzo di un'immagine master in Azure che contiene informazioni sul piano per creare un catalogo delle macchine. Per ulteriori informazioni, vedere Microsoft Azure Marketplace.

> **Suggerimento:**
>
> Alcune immagini che si trovano in Azure Marketplace, come l'immagine standard di Windows Server, non aggiungono informazioni sul piano. La funzione di Citrix DaaS è per le immagini a pagamento.

#### Assicurarsi che l'immagine creata nella Raccolta di calcolo di Azure contenga informazioni sul piano di Azure

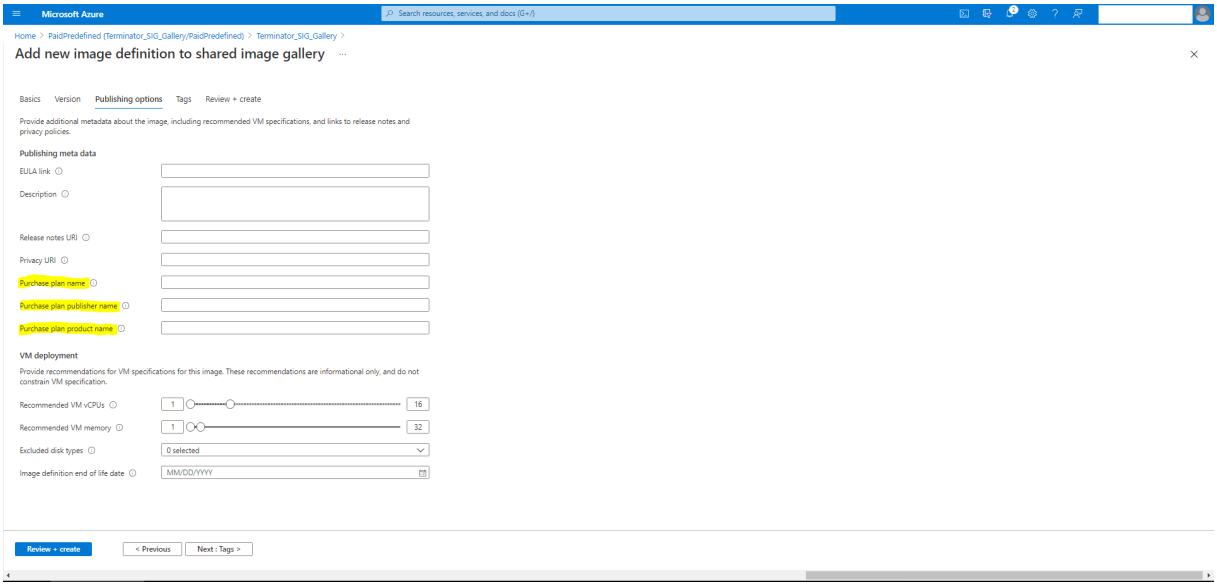
Utilizzare la procedura illustrata in questa sezione per visualizzare le immagini della Raccolta di calcolo di Azure in Citrix Studio. Facoltativamente, queste immagini possono essere utilizzate per un'immagine master. Per inserire l'immagine in una Raccolta di calcolo di Azure, creare una definizione di immagine in una raccolta.



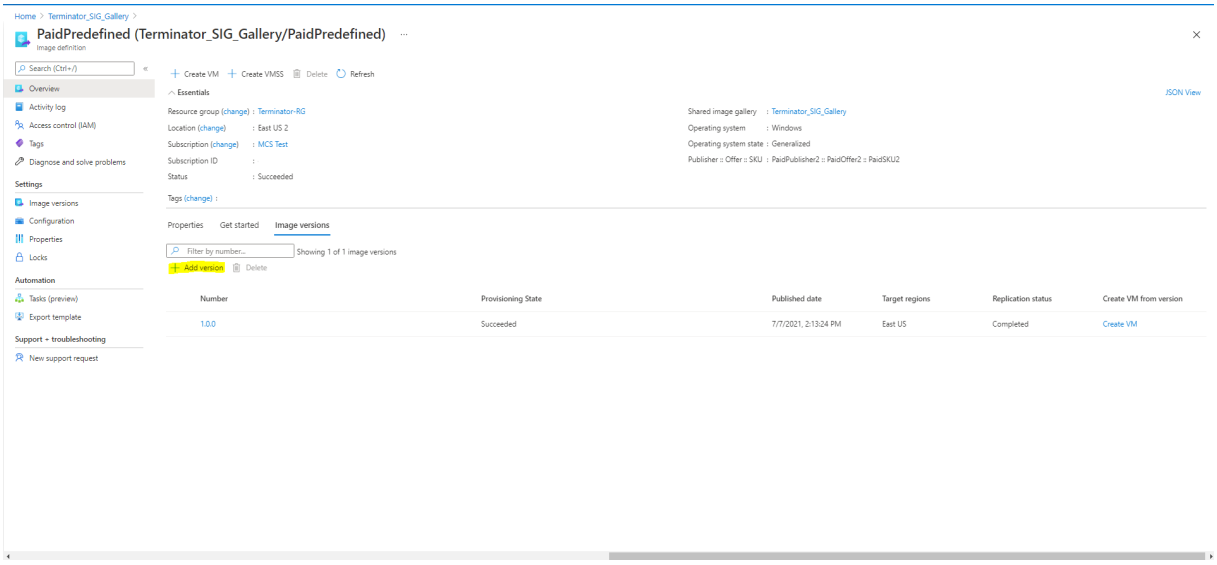

Nella pagina **Publishing options** (Opzioni di pubblicazione), verificare le informazioni sul piano di acquisto.

I campi relativi alle informazioni sul piano di acquisto sono inizialmente vuoti. Compilare questi campi con le informazioni sul piano di acquisto utilizzate per l'immagine. La mancata compilazione delle informazioni sul piano di acquisto può causare la mancata riuscita del processo del catalogo delle macchine.

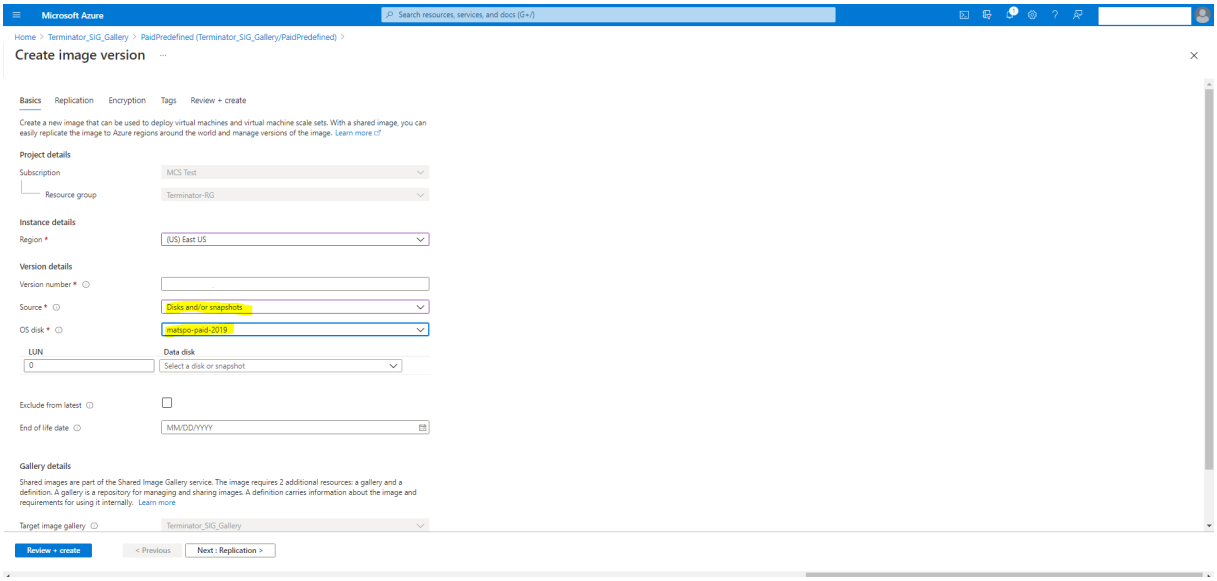



Dopo aver verificato le informazioni sul piano di acquisto, creare una versione immagine all'interno della definizione. Viene utilizzata come immagine master. Fare clic su **Add version** (Aggiungi versione):




Nella sezione **Version details** (Dettagli versione), selezionare la snapshot dell'immagine o il disco gestito come origine:




## Copiare i tag su tutte le risorse

È possibile copiare i tag specificati in un profilo macchina per tutte le risorse, ad esempio più NIC e dischi (disco del sistema operativo, disco di identità e disco della cache di write-back) di una nuova macchina virtuale o di una macchina virtuale esistente inclusa in un catalogo di macchine. L'origine del profilo macchina può essere una VM o una specifica di modello ARM.

> **Nota:**
>
> È necessario aggiungere il criterio sui tag (vedere Assegnare definizioni di criteri per la confor-

> mità dei tag) o aggiungere i tag in un'origine del profilo della macchina per conservare i tag sulle risorse.

#### Prerequisiti

Creare l'origine del profilo macchina (VM o specifica di modello ARM) per avere tag sulle VM, sui dischi e le NIC di quella VM.

- Se si desidera avere una macchina virtuale come input del profilo macchina, applicare i tag sulla macchina virtuale e su tutte le risorse nel portale di Azure. Vedere Applicare i tag con il portale di Azure.
- Se si desidera utilizzare le specifiche di modello ARM come input del profilo macchina, aggiungere il seguente blocco di tag sotto ogni risorsa.

```
1   "tags": {
2
3  "TagC": "Value3"
4   }
5  ,
6  <!--NeedCopy-->
```

> **Nota:**
>
> È possibile avere un massimo di un disco e almeno una NIC nella specifica di modello.

#### Copiare i tag nelle risorse di una macchina virtuale in un nuovo catalogo di macchine

1. Creare un catalogo non persistente o persistente con una macchina virtuale o una specifica di modello ARM come input del profilo macchina.
2. Aggiungere una macchina virtuale al catalogo e accenderla. È necessario vedere che i tag specificati nel profilo della macchina sono stati copiati nelle risorse corrispondenti di quella VM.

   > **Nota:**
   >
   > Viene visualizzato un errore se c'è una mancata corrispondenza tra il numero di NIC fornite nel profilo del computer e il numero di NIC che si desidera che le macchine virtuali utilizzino.

#### Modificare i tag sulle risorse di una macchina virtuale esistente

1. Creare un profilo macchina con i tag su tutte le risorse.
2. Aggiornare il catalogo macchine esistente con il profilo macchina aggiornato. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
<!--NeedCopy-->
```

3. Disattivare la macchina virtuale a cui si intende applicare gli aggiornamenti.
4. Richiedere un aggiornamento pianificato per la macchina virtuale. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
<!--NeedCopy-->
```

5. Accendere la VM.
6. È necessario vedere che i tag specificati nel profilo della macchina sono stati copiati nelle risorse corrispondenti.

> **Nota:**
>
> Viene visualizzato un errore se c'è una mancata corrispondenza tra il numero di NIC fornite nel profilo macchina e il numero di NIC fornite in `Set-ProvScheme`.

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Microsoft Azure.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a Microsoft Azure Resource Manager
- Creare cataloghi di macchine

## Creare un catalogo di Microsoft System Center Virtual Machine Manager

December 21, 2022

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti di virtualizzazione Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Prima di creare un catalogo di VMM, è necessario completare la creazione di una connessione a VMM. Vedere Connessione a Microsoft System Center Virtual Machine Manager.

### Creare una macchina virtuale master

- Installare un VDA nella macchina virtuale master e selezionare l'opzione per ottimizzare il desktop. Questo migliora le prestazioni.
- Creare un'istantanea della macchina virtuale master da utilizzare come backup.
- Creare desktop virtuali.

### MCS su condivisioni di file SMB 3

Per i cataloghi delle macchine creati con MCS su condivisioni file SMB 3 per l'archiviazione delle macchine virtuali, le credenziali devono soddisfare i seguenti requisiti per garantire che le chiamate da Citrix Hypervisor Communications Library (HCL) si connettano correttamente all'archiviazione SMB.

- Le credenziali utente VMM devono includere l'accesso completo in lettura e scrittura all'archiviazione SMB.
- Le operazioni del disco virtuale di archiviazione durante gli eventi del ciclo di vita delle macchine virtuali vengono eseguite tramite il server Hyper-V utilizzando le credenziali utente VMM.

Quando si utilizza VMM 2012 SP1 con Hyper-V su Windows Server 2012: quando si utilizza SMB come archiviazione, abilitare l'Authentication Credential Security Support Provider (CredSSP) da Cloud Connector alle singole macchine Hyper-V. Per ulteriori informazioni, vedere CTX 137465.

Utilizzando una sessione remota standard di PowerShell V3, l'HCL nel Cloud Connector utilizza CredSSP per aprire una connessione alla macchina Hyper-V. Questa funzionalità trasferisce le credenziali utente crittografate con Kerberos alla macchina Hyper-V e i comandi PowerShell nella sessione sulla macchina Hyper-V remota vengono eseguiti con le credenziali fornite (in questo caso, quelle dell'utente VMM), in modo che i comandi di comunicazione all'archiviazione funzionino correttamente.

Le seguenti attività utilizzano script PowerShell che hanno origine nell'HCL. Gli script vengono quindi inviati alla macchina Hyper-V per agire nell'archiviazione SMB 3.0.

**Consolidate master image** (Consolida immagine master): un'immagine master crea un nuovo schema di provisioning MCS (catalogo delle macchine). Questo schema clona e appiattisce la

macchina virtuale master pronta per la creazione di macchine virtuali dal nuovo disco creato (e rimuove la dipendenza dalla macchina virtuale master originale).

ConvertVirtualHardDisk nello spazio dei nomi root\virtualization\v2

Esempio:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

**Create difference disk** (Crea disco di differenza): crea un disco di differenza dall'immagine generata dal consolidamento dell'immagine. Il disco di differenza viene quindi collegato a una nuova macchina virtuale.

CreateVirtualHardDisk nello spazio dei nomi root\virtualization\v2

Esempio:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

**Upload identity disks** (Carica dischi di identità): l'HCL non può caricare direttamente il disco di identità nell'archiviazione SMB. Pertanto, il computer Hyper-V deve caricare e copiare il disco di identità nella posizione di archiviazione. Poiché la macchina Hyper-V non è in grado di leggere il disco dal Cloud Connector, l'HCL deve prima copiare il disco di identità tramite la macchina Hyper-V come segue.

1. L'HCL carica l'identità nel computer Hyper-V tramite la condivisione dell'amministratore.
2. Il computer Hyper-V copia il disco nell'archiviazione SMB tramite uno script PowerShell in esecuzione nella sessione remota di PowerShell.

   Nel computer Hyper-V viene creata una cartella e le autorizzazioni per tale cartella sono bloccate solo per l'utente VMM (tramite la connessione remota PowerShell).
3. L'HCL elimina il file dalla condivisione dell'amministratore.
4. Quando l'HCL completa il caricamento del disco di identità sulla macchina Hyper-V, la sessione remota di PowerShell copia i dischi di identità nell'archiviazione SMB e successivamente li elimina dalla macchina Hyper-V.

La cartella del disco di identità viene ricreata se viene eliminata per renderla disponibile per il riutilizzo.

**Download identity disks** (Scarica dischi di identità): come avviene nel caricamento, i dischi di identità passano attraverso la macchina Hyper-V per giungere all'HCL. Il processo seguente crea una

cartella che dispone solo delle autorizzazioni utente VMM sul server Hyper-V se non esiste.

1. La macchina Hyper-V copia il disco dall'archiviazione SMB all'archiviazione Hyper-V locale tramite uno script PowerShell in esecuzione nella sessione remota di PowerShell V3.
2. L'HCL legge il disco dalla condivisione amministratore del computer Hyper-V in memoria.
3. L'HCL elimina il file dalla condivisione amministratore.

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Microsoft System Center Virtual Machine Manager.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a Microsoft System Center Virtual Machine Manager
- Creare cataloghi di macchine

## Creare un catalogo di Nutanix

August 17, 2023

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti di virtualizzazione Nutanix.

> **Nota:**
>
> Prima di creare un catalogo di Nutanix, è necessario completare la creazione di una connessione a Nutanix. Vedere Connessione a Nutanix.

### Creare un catalogo di macchine utilizzando un'istantanea Nutanix

L'istantanea selezionata è il modello utilizzato per creare le macchine virtuali nel catalogo. Prima di creare il catalogo, creare immagini e istantanee in Nutanix. Per ulteriori informazioni, vedere la documentazione Nutanix.

Nella procedura guidata per la creazione del catalogo:

- Le pagine **Operating System** e **Machine Management** non contengono informazioni specifiche per Nutanix.
- La pagina **Container** o **Cluster and Container** è esclusiva di Nutanix.
  - Se si distribuiscono macchine utilizzando Nutanix AHV XI come risorse, nella pagina **Container** (Contenitore) selezionare un contenitore in cui verranno posizionati i dischi di identità delle macchine virtuali.
  - Se si distribuiscono macchine utilizzando Nutanix AHV Prism Central (PC) come risorse, sarà visualizzata la pagina **Cluster and Container**. Selezionare il cluster da utilizzare per la distribuzione delle macchine virtuali e quindi un contenitore.
- Nella pagina **Master Image** (Immagine master) selezionare l'istantanea dell'immagine. I nomi delle istantanee Acropolis devono avere il prefisso "XD_"per essere utilizzati in Citrix Virtual Apps and Desktops. Utilizzare la console Acropolis per rinominare le istantanee, se necessario. Se si rinominano le istantanee, riavviare la creazione guidata catalogo per visualizzare un elenco aggiornato.
- Nella pagina **Immagine master** (Macchine virtuali) indicare il numero di CPU virtuali e il numero di core per vCPU.
- Nella pagina **NICs** (NIC), selezionare il tipo di NIC per filtrare le reti associate. Questa opzione è disponibile solo per le connessioni Nutanix AHV PC. Esistono due tipi di NIC: **VLAN** e **OVERLAY**. Selezionare una o più delle schede NIC contenute nell'immagine master, quindi selezionare una rete virtuale associata per ciascuna scheda NIC.
- Le pagine **Machine Identities** (Identità macchina), **Domain Credentials** (Credenziali di dominio), **Credenziali di dominio** (Ambiti) e **Summary** (Riepilogo) non contengono informazioni specifiche di Nutanix.

### Limitazione

Quando si crea un catalogo MCS con una connessione host Nutanix (in particolare, i plugin Nutanix AHV 2.7.1 e Nutanix AHV 2.5.1), le dimensioni del disco rigido delle VM fornite vengono visualizzate in modo errato sull'interfaccia **Full Configuration**.

- Plugin Nutanix AHV 2.7.1: la dimensione visualizzata è molto inferiore (1 GB) rispetto alla dimensione di archiviazione reale (50 GB)
- Plugin Nutanix AHV 2.5.1: la dimensione visualizzata è molto inferiore (32 GB) rispetto alla dimensione di archiviazione reale (60 GB)

La dimensione del disco rigido viene visualizzata correttamente sulla console Nutanix. C'è un aggiornamento in sospeso da parte di Nutanix per fornire la dimensione corretta del disco.

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a Nutanix
- Connessione alle soluzioni Nutanix Cloud e dei partner
- Creare cataloghi di macchine

## Creare un catalogo di VMware

June 8, 2023

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine.

> **Nota:**
>
> Prima di creare un catalogo di VMware, è necessario completare la creazione di una connessione a VMware. Vedere Connessione a VMware.

### Creare un catalogo di macchine utilizzando un profilo macchina

È possibile creare un catalogo di macchine MCS utilizzando un profilo macchina. L'origine dell'input del profilo della macchina è un modello VMware. Il profilo della macchina acquisisce le proprietà hardware da un modello VMware e le applica alle macchine virtuali di cui è appena stato effettuato il provisioning nel catalogo.

> **Nota:**
>
> - L'input dell'immagine master (istantanea) e l'input del profilo della macchina (modello VMware) devono essere entrambi abilitati o entrambi disabilitati da vTPM. Questa regola si applica sia a `New-ProvScheme` che a `Set-ProvScheme`.
> - Se l'immagine master è abilitata da vTPM, il modello VMware può provenire solo dalla stessa sorgente VM dell'immagine master.

> • Il criterio di archiviazione crittografata supporta solo la clonazione completa.

Il modello VMware presente nel profilo della macchina deve esistere durante il ciclo di vita del catalogo per consentire il provisioning delle macchine virtuali del catalogo. Senza un modello VMware, non è possibile effettuare il provisioning di nuove VM. Quando un modello VMware viene eliminato, è necessario fornire un nuovo modello utilizzando il comando `Set-ProvScheme`.

- MCS acquisisce le proprietà di un modello VMware. È possibile creare un nuovo modello VMware facendo riferimento alle proprietà archiviate del modello VMware utilizzando il comando `Get-Provscheme`.
- In alternativa, se sono presenti sia il catalogo delle macchine che le VM di cui è stato effettuato il provisioning, è possibile utilizzare anche una macchina con provisioning MCS per creare un nuovo modello VMware.

In base a diversi sistemi operativi, è possibile creare un catalogo macchine con diverse configurazioni:

- Se Windows 11 è installato sull'immagine master, è necessario che vTPM sia abilitato per l'immagine master. Pertanto, il modello VMware, che è un'origine del profilo della macchina, deve avere vTPM collegato.
- Se Windows 10 è installato sull'immagine master senza vTPM collegato, è possibile creare un catalogo di macchine con un modello VMware non vTPM come origine per il profilo della macchina.

Esiste un'altra configurazione in cui è possibile creare un catalogo di macchine utilizzando la modalità di copia completa del disco con un modello di profilo macchina applicato con criteri di archiviazione crittografati.

Per creare un catalogo di macchine utilizzando i comandi di PowerShell con il profilo macchina come input:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire i seguenti comandi:

    - Per creare un catalogo di macchine con il modello VMware allegato a vTPM come fonte per l'input del profilo della macchina e l'immagine master installata da Windows 11:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\\<network name>.
   network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>" -
   ProvisioningType 'MCS'
-Scope @()  -SessionSupport "SingleSession"
-ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Per creare un catalogo di macchine con un modello VMware non vTPM come origine per il profilo della macchina e l'immagine master installata da Windows10:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\\<string>.network
   " }
```

```
8
9   -ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
        -VMMemoryMB 8192
10  -MachineProfile "XDHyp:\HostingUnits<hosting unit name><
        template name>.template"
11  -TenancyType Shared  -FunctionalLevel "L7_20"
12  <!--NeedCopy-->
```

```
1   $catalog = New-BrokerCatalog
2   -AllocationType "Static"
3   -PersistUserChanges  "OnLocal"  -Description "<string>"  -
        IsRemotePC $False
4   -MinimumFunctionalLevel 'L7_9' -Name "<string>" -
        ProvisioningType 'MCS' -Scope @()  -SessionSupport "
        SingleSession" -ZoneUid "<Uid"
5   <!--NeedCopy-->
```

```
1   Set-BrokerCatalog -Name "<string>"
2   -ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
3   <!--NeedCopy-->
```

- Per creare un catalogo macchine utilizzando la modalità di copia completa del disco con modello di profilo macchina applicato con criteri di archiviazione crittografati:

```
1   $identityPool = New-AcctIdentityPool
2   -IdentityPoolName "<string>"
3   -NamingScheme "<string>-###"
4   -NamingSchemeType Numeric
5   -Domain "<domain name>"
6   -ZoneUid "<Uid>"  -Scope @()
7   <!--NeedCopy-->
```

```
1   $provScheme =New-ProvScheme
2   -HostingUnitName "<string>"
3   -IdentityPoolName "<string>" -InitialBatchSizeHint 1
4   -MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
        snapshot name>.snapshot"
5   -NetworkMapping @{
6   "0"="XDHyp:\HostingUnits<hosting unit name>\\<string>.network
        " }
7
8   -ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
        -VMMemoryMB 8192
9   -MachineProfile "XDHyp:\HostingUnits<hosting unit name><
        template name>.template"
10  -TenancyType Shared  -FunctionalLevel "L7_20"
11  -UseFullDiskCloneProvisioning
12  <!--NeedCopy-->
```

```
1   $catalog = New-BrokerCatalog
2   -AllocationType "Static"
3   -PersistUserChanges  "OnLocal"
```

```
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Per aggiornare il profilo di una macchina, utilizzare il comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -
   IdentityPoolName 'name' -MachineProfile 'XDHyp:\
   HostingUnits<hosting unit name><template name>.template
<!--NeedCopy-->
```

### Risoluzione dei problemi

Se il catalogo non viene creato, vedere CTX294978.

### Passaggi successivi

- Se si tratta del primo catalogo che viene creato, si verrà guidati nella creazione di un gruppo di consegna.
- Per esaminare l'intero processo di configurazione, vedere Pianificare e creare una distribuzione.
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di VMware.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a VMware
- Connessione al cloud VMware e alle soluzioni dei partner
- Creare cataloghi di macchine

## Creare cataloghi di diversi tipi di aggiunte

July 6, 2023

Utilizzando MCS, è possibile eseguire il provisioning di macchine come non aggiunte a un dominio, aggiunte ad AD on-premise, aggiunte ad Azure AD o aggiunte ad Azure AD ibrida.

Per informazioni su come configurare le identità delle macchine nell'interfaccia Full Configuration (Configurazione completa), vedere Creare cataloghi delle macchine.

Per informazioni specifiche su come creare cataloghi uniti a identità di macchine, vedere quanto segue:

- Creare cataloghi aggiunti ad Azure Active Directory
- Creare cataloghi compatibili con Microsoft Intune
- Creare cataloghi aggiunti ad Azure Active Directory ibrido
- Creare cataloghi non aggiunti a un dominio

## Creare cataloghi aggiunti ad Azure Active Directory

December 18, 2023

In questo articolo viene descritto come creare cataloghi aggiunti ad Azure Active Directory (AD) utilizzando Citrix DaaS.

Per informazioni su requisiti, limitazioni e considerazioni, vedere Macchine aggiunte ad Azure Active Directory.

Prima di creare il catalogo di macchina, è necessario quanto segue:

1. Nuova posizione risorsa
    - Accedere all'interfaccia utente di amministrazione di Citrix Cloud > menu hamburger in alto a sinistra > **Resource Locations** (Posizioni risorsa).
    - Fare clic su **+ Resource Location** (+ Posizione risorsa).
    - Immettere un nome per la nuova posizione risorsa e fare clic su **Save** (Salva).
2. Creare una connessione host. Per i dettagli, vedere la sezione Creare e gestire connessioni. Quando si distribuiscono macchine in Azure, vedere Connettersi ad Azure Resource Manager.
3. Per eliminare sistematicamente i dispositivi Azure AD obsoleti e consentire ai nuovi dispositivi di essere aggiunti ad Azure AD, è possibile assegnare il ruolo di amministratore dei dispositivi cloud all'entità servizio di provisioning. Se non si eliminano i dispositivi AD di Azure non aggiornati, la macchina virtuale non persistente corrispondente rimane in stato di inizializzazione finché non viene rimossa manualmente dal portale di Azure AD. A tale scopo, abilitare la gestione delle connessioni host dei dispositivi aggiunti ad Azure AD utilizzando l'interfaccia Full Configuration o seguire i seguenti passaggi:

a) Accedere al portale di Azure e passare ad **Azure Active Directory > Ruoli e amministratori**.

b) Cercare il ruolo incorporato di **Cloud Device Administrator** e fai clic su **Aggiungi assegnazioni** per assegnare il ruolo al responsabile del servizio dell'applicazione utilizzata dalla connessione di hosting.

c) Utilizzare l'SDK Citrix Remote PowerShell per eseguire i seguenti comandi per ottenere le `CustomProperties` esistenti della connessione di hosting. La stringa `${ HostingConnectionName }` si riferisce al nome della connessione di hosting.

   i. Aprire una finestra di **PowerShell**.

   ii. Eseguire il comando `asnp citrix*` per caricare i moduli **PowerShell** specifici di Citrix.

   iii. Eseguire il comando che segue per ottenere le proprietà personalizzate esistenti della connessione di hosting.

```
(Get-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
 ).CustomProperties
<!--NeedCopy-->
```

   iv. Copiare CustomProperties dalla connessione a un blocco note e aggiungere l'impostazione della proprietà `<Property xsi:type="StringProperty" Name="AzureAdDeviceManagement"Value="true"/>`.

   v. Nella finestra di **PowerShell** assegnare una variabile alle proprietà personalizzate modificate. Ad esempio, `$UpdatedCustomProperties='<CustomProperties ...</CustomProperties>'`.

   vi. Reimpostare la proprietà personalizzata sulla connessione di hosting:

```
Set-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
  -CustomProperties ${
 UpdatedCustomProperties }
  -ZoneUid ${
 ZoneUid }

<!--NeedCopy-->
```

   vii. Eseguire il comando `(Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName } ).CustomProperties` per verificare le impostazioni delle proprietà personalizzate aggiornate.

È possibile creare cataloghi aggiunti ad Azure AD utilizzando l'interfaccia Full Configuration (Configurazione completa) o **PowerShell**.

### Utilizzare l'interfaccia Full Configuration

Le seguenti informazioni sono un'aggiunta alle linee guida della sezione Creare cataloghi delle macchine. Per creare cataloghi aggiunti ad Azure AD, seguire le linee guida generali in quell'articolo, tenendo conto dei dettagli specifici dei cataloghi aggiunti ad Azure AD.

Nella procedura guidata per la creazione del catalogo:

1. Nella pagina **Master Image** (Immagine master):
   - Selezionare 2106 o successivo come livello funzionale.
   - Selezionare **Use a machine profile** (Usa un profilo macchina) e selezionare il computer appropriato dall'elenco.
2. Nella pagina **Machine Identities** (Identità macchine), selezionare **Azure Active Directory joined** (Aggiunta ad Azure Active Directory). Le macchine create sono di proprietà di un'organizzazione e sono connesse con un account Azure AD appartenente a tale organizzazione. Esistono solo nel cloud.

   > **Nota:**
   >
   > - Il tipo di identità **Azure Active Directory joined** (Aggiunta ad Azure Active Directory) richiede la versione 2106 o successiva come livello di funzionalità minimo per il catalogo.
   > - Le macchine vengono aggiunte al dominio Azure AD associato al tenant a cui è associata la connessione di hosting.

3. Agli utenti deve essere concesso l'accesso esplicito in Azure per accedere alle macchine utilizzando le proprie credenziali AAD. Vedere la sezione Azure Active Directory joined per maggiori dettagli.

### Utilizzare PowerShell

Di seguito sono riportati i passaggi di **PowerShell** equivalenti alle operazioni nell'interfaccia Full Configuration. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

La differenza tra i cataloghi aggiunti ad AD on-premise e quelli aggiunti ad Azure AD sta nella creazione del pool di identità e dello schema di provisioning.

Per creare un pool di identità per i cataloghi aggiunti ad Azure AD:

```
New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
    WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
    NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
    -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
<!--NeedCopy-->
```

Per creare uno schema di provisioning per i cataloghi aggiunti ad Azure AD, il parametro **MachineProfile** è richiesto in New-ProvScheme:

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
    schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.
    w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty
    `" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageType`" Value=`"StandardSSD_LRS`" /><
    Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
    Windows_Server`" /></CustomProperties>" -HostingUnitName "
    AzureResource" -IdentityPoolName "AzureADJoinedCatalog" -
    InitialBatchSizeHint 1 -MachineProfile "XDHyp:\HostingUnits\
    AzureResource\image.folder\azuread-rg.resourcegroup\MasterVDA.vm" -
    MasterImageVM "XDHyp:\HostingUnits\AzureResource\image.folder\
    azuread-rg.resourcegroup\azuread-
    small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
     US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
    azuread-vnet.virtualprivatecloud\Test_VNET.network" }
  -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
     Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
     \AzureResource\serviceoffering.folder\Standard_DS1_v2.
     serviceoffering"
<!--NeedCopy-->
```

Tutti gli altri comandi utilizzati per creare cataloghi aggiunti ad Azure AD sono gli stessi dei tradizionali cataloghi aggiunti ad AD on-premise.

### Visualizzare lo stato del processo di join di Azure AD

Nell'interfaccia Full Configuration (Configurazione completa), lo stato del processo di join di Azure AD è visibile quando le macchine aggiunte ad Azure AD in un gruppo di consegna sono in uno stato di accensione. Per visualizzare lo stato, utilizzare Search (Cerca) per identificare tali macchine e quindi per ogni controllo **Machine Identity** (Identità macchina) nella scheda **Details** (Dettagli) nel riquadro inferiore. In **Machine Identity** (Identità macchina) possono essere visualizzate le seguenti informazioni:

- Aggiunte ad Azure AD
- Not yet joined to Azure AD (Non ancora aggiunta ad Azure AD)

> **Nota:**
>
> Se le macchine non si trovano nello stato Azure AD joined (Aggiunta ad Azure AD), non vengono registrate con il Delivery Controller. Lo stato di registrazione è **Initialization** (Inizializzazione).

Inoltre, utilizzando l'interfaccia Full Configuration (Configurazione completa), è possibile scoprire perché le macchine non sono disponibili. A tale scopo, fare clic su una macchina nel nodo **Search** (Cerca), selezionare **Registration** (Registrazione) nella scheda **Details** (Dettagli) nel riquadro inferiore, quindi leggere la descrizione comando per ulteriori informazioni.

### Gruppo di consegna

Per i dettagli, vedere la sezione Creare gruppi di consegna.

### Abilitare Rendezvous

Una volta creato il gruppo di consegna, è possibile abilitare Rendezvous. Per i dettagli, vedere Rendezvous V2.

### Risoluzione dei problemi

Se l'aggiunta delle macchine ad Azure AD non va a buon fine, procedere come segue:

- Controllare se l'identità gestita assegnata al sistema è abilitata per le macchine. Le macchine di cui è stato eseguito il provisioning con MCS devono avere questa opzione abilitata automaticamente. Il processo di aggiunta ad Azure AD fallisce senza che al sistema venga assegnata un'identità gestita. Se l'identità gestita assegnata al sistema non è abilitata per le macchine di cui è stato eseguito il provisioning con MCS, il motivo possibile è:
  - `IdentityType` del pool di identità associato allo schema di provisioning non è impostato su `AzureAD`. È possibile verificarlo eseguendo `Get-AcctIdentityPool`.
- Controllare lo stato di provisioning dell'estensione **AADLoginForWindows** per le macchine. MCS fa affidamento su questa estensione per aggiungere una macchina virtuale ad Azure AD. Se l'estensione **AADLoginForWindows** non esiste, i possibili motivi sono:
  - `IdentityType` del pool di identità associato allo schema di provisioning non è impostato su `AzureAD`. È possibile verificarlo eseguendo `Get-AcctIdentityPool`.
  - L'installazione dell'estensione **AADLoginForWindows** è bloccata dalla politica di Azure.

- Per risolvere gli errori di assegnazione dell'estensione **AADLoginForWindows**, è possibile controllare i registri in `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` nella macchina di cui è stato eseguito il provisioning con MCS.
- Controllare lo stato di accesso e i registri di debug di Azure AD eseguendo il comando `dsregcmd /status /debug` sulla macchina di cui è stato eseguito il provisioning con MCS.
- Controllare i registri degli eventi di Windows in **Registri applicazioni e servizi > Microsoft > Windows > User Device Registration (Registrazione del dispositivo utente)**.
- Verificare se la gestione dei dispositivi Azure AD è configurata correttamente eseguendo `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }`.

  Assicurarsi che il valore della:

  - proprietà `AzureAdDeviceManagement` in `CustomProperties` sia **true**
  - proprietà `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` nei metadati sia **true**

  Se `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` è **false**, significa che il `ServicePrincipal` dell'applicazione utilizzata dalla connessione di hosting non dispone di autorizzazioni sufficienti per eseguire la gestione dei dispositivi Azure AD. Per risolvere questo problema, assegnare a `ServicePrincipal` il ruolo di **amministratore del dispositivo cloud**.

### Gruppo di sicurezza dinamico di Azure Active Directory

Le regole di gruppo dinamico collocano le VM del catalogo in un gruppo di sicurezza dinamico basato sullo schema di denominazione del catalogo delle macchine.

Se lo schema di denominazione del catalogo delle macchine è Test### (dove # sta per un numero), Citrix crea la regola di appartenenza dinamica *^Test[0-9]{3}$* nel gruppo di sicurezza dinamico. Ora, se il nome della macchina virtuale creata da Citrix è compreso tra Test001 e Test999, la VM è inclusa nel gruppo di sicurezza dinamico.

> **Nota:**
>
> Se il nome della macchina virtuale creata manualmente è compreso tra Test001 e Test999, anche in quel caso la VM è inclusa nel gruppo di sicurezza dinamico. Questa è una delle limitazioni del gruppo di sicurezza dinamico.

La funzionalità dei gruppi di sicurezza dinamici è utile quando si desidera gestire le macchine virtuali tramite Azure Active Directory (Azure AD). È utile anche quando si desidera applicare i criteri di accesso condizionale o distribuire app da Intune filtrando le macchine virtuali con il gruppo di sicurezza dinamico di Azure AD.

È possibile utilizzare i comandi **PowerShell** per:

- Creare un catalogo di macchine con il gruppo di sicurezza dinamico di Azure AD
- Abilitare la funzionalità dei gruppi di sicurezza per un catalogo Azure AD
- Eliminare un catalogo di macchine con il gruppo di sicurezza dei dispositivi aggiunto ad Azure AD

> **Importante:**
>
> - Per creare un catalogo di macchine con il gruppo di sicurezza dinamico di Azure AD, aggiungere macchine al catalogo ed eliminare il catalogo di macchine, è necessario disporre del token di accesso di Azure AD. Per informazioni su come ottenere il token di accesso ad Azure AD, vedere https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/.
> - Per richiedere un token di accesso in Azure AD, Citrix richiede l'autorizzazione **Group.ReadWrite.All** per l'API Microsoft Graph. Un utente di Azure AD che dispone dell'autorizzazione per il consenso di amministratore a livello di tenant può concedere l'autorizzazione **Group.ReadWrite.All** all'API Microsoft Graph. Per informazioni su come concedere il consenso di amministratore a livello di tenant a un'applicazione in Azure Active Directory (Azure AD), vedere il documento Microsoft https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/.

#### Creare un catalogo di macchine con il gruppo di sicurezza dinamico di Azure AD

1. Nell'interfaccia utente di configurazione del catalogo macchine della console basata sul Web, nella pagina **Machine Identities**, selezionare **Azure Active Directory joined**.
2. Accedere ad Azure AD.
3. Ottenere il token di accesso all'API MS Graph. Utilizzare questo token di accesso come valore del parametro `$AzureADAccessToken` quando si eseguono i comandi **PowerShell**.
4. Eseguire il comando seguente per verificare se il nome del gruppo di sicurezza dinamico esiste nel tenant.

```
Get-AcctAzureADSecurityGroup
 –AccessToken  $AzureADAccessToken
 –Name "SecurityGroupName"
<!--NeedCopy-->
```

5. Creare un catalogo di macchine utilizzando l'ID tenant, il token di accesso e il gruppo di sicurezza dinamico. Eseguire il comando seguente per creare un IdentityPool con `IdentityType=AzureAD` e creare un gruppo di sicurezza dinamico in Azure.

```
New-AcctIdentityPool
```

```
-AllowUnicode
-IdentityPoolName "SecurityGroupCatalog"
-NamingScheme "SG-VM-###"
-NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
-WorkgroupMachine
-IdentityType "AzureAD"
-DeviceManagementType "None"
-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupName "SecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

**Abilitare la funzionalità dei gruppi di sicurezza per un catalogo Azure AD**

È possibile abilitare la funzionalità di sicurezza dinamica per un catalogo di Azure AD creato senza abilitare la funzionalità del gruppo di sicurezza dinamico. A questo scopo:

1. Creare manualmente un nuovo gruppo di sicurezza dinamico. È anche possibile riutilizzare un gruppo di sicurezza dinamico esistente.
2. Accedere ad Azure AD e ottenere il token di accesso all'API MS Graph. Utilizzare questo token di accesso come valore del parametro `$AzureADAccessToken` quando si eseguono i comandi **PowerShell**.

   > **Nota:**
   >
   > Per informazioni sulle autorizzazioni richieste dall'utente di Azure AD, vedere https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/.

3. Eseguire il comando seguente per connettere il pool di identità al gruppo di sicurezza dinamico di Azure AD creato.

```
Set-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupNam "ExistingSecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Se si aggiorna lo schema di denominazione, Citrix aggiorna lo schema di denominazione a una nuova regola di appartenenza.  Se si elimina il catalogo, viene eliminata la regola di appartenenza e non il gruppo di sicurezza.

### Eliminare un catalogo di macchine con il gruppo di sicurezza dei dispositivi aggiunto ad Azure AD

Quando si elimina un catalogo di macchine, viene eliminato anche il gruppo di sicurezza dei dispositivi aggiunti ad Azure AD.

Per eliminare il gruppo di sicurezza dinamico di Azure AD, procedere come segue:

1. Accedere ad Azure AD.
2. Ottenere il token di accesso all'API MS Graph. Utilizzare questo token di accesso come valore del parametro `$AzureADAccessToken` quando si eseguono i comandi **PowerShell**.
3. Eseguire il seguente comando:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Creare un gruppo di sicurezza dinamico di Azure AD in un gruppo di sicurezza assegnato ad Azure AD esistente

È possibile creare un gruppo di sicurezza dinamico di Azure AD all'interno di un gruppo di sicurezza assegnato ad Azure AD esistente. È possibile procedere come segue:

- Ottenere informazioni sui gruppi di sicurezza.
- Ottenere tutti i gruppi di sicurezza assegnati ad Azure AD che sono sincronizzati dal server AD locale o i gruppi di sicurezza assegnati a cui è possibile assegnare i ruoli di Azure AD.
- Ottenere tutti i gruppi di sicurezza dinamici di Azure AD.
- Aggiungere il gruppo di sicurezza dinamico di Azure AD come membro del gruppo assegnato ad Azure AD.
- Rimuovere l'appartenenza tra il gruppo di sicurezza dinamico di Azure AD e il gruppo di sicurezza assegnato ad Azure AD quando il gruppo di sicurezza dinamico di Azure AD viene eliminato insieme al catalogo macchine.

È inoltre possibile visualizzare messaggi di errore espliciti in caso di non riuscita di una o più delle operazioni.

**Requisito:**

È necessario disporre del token di accesso all'API MS Graph quando si eseguono i comandi **PowerShell**.

Per ottenere il token di accesso:

1. Aprire Microsoft Graph explorer e accedere ad Azure AD.
2. Assicurarsi di disporre del consenso per le autorizzazioni **Group.ReadWrite.All** e **GroupMember.ReadWrite.All**.
3. Ottenere il token di accesso da Microsoft Graph explorer. Utilizzare questo token di accesso quando si eseguono i comandi **PowerShell**.

Per ottenere informazioni sui gruppi di sicurezza in base all'ID del gruppo:

1. Ottenere il token di accesso.
2. Trovare l'ID dell'oggetto del gruppo nel portale di Azure.
3. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token> -GroupId <GroupUid>
<!--NeedCopy-->
```

Per ottenere i gruppi di sicurezza in base al nome visualizzato del gruppo:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Name <TargetGroupDisplayName>
<!--NeedCopy-->
```

Per ottenere i gruppi di sicurezza il cui nome visualizzato contiene una sottostringa:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-SearchString <displayNameSubString>
<!--NeedCopy-->
```

Per ottenere tutti i gruppi di sicurezza assegnati ad Azure AD sincronizzati dal server AD locale o i gruppi di sicurezza assegnati a cui è possibile assegnare i ruoli di Azure AD:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
<!--NeedCopy-->
```

Per ottenere tutti i gruppi di sicurezza dinamici di Azure AD:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Dynamic true
<!--NeedCopy-->
```

Per ottenere i gruppi di sicurezza assegnati ad Azure AD con il numero massimo di record:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
-MaxRecordCount 10
<!--NeedCopy-->
```

Per aggiungere il gruppo di sicurezza dinamico di Azure AD come membro del gruppo di sicurezza assegnato ad Azure AD:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Add-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
-RefGroupId <DSG-Id>
<!--NeedCopy-->
```

Per ottenere i membri del gruppo di sicurezza assegnati ad Azure AD:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Get-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
<!--NeedCopy-->
```

> **Nota:**
>
> `Get-AcctAzureADSecurityGroupMember` fornisce solo i membri diretti del tipo di gruppo di sicurezza all'interno del gruppo di sicurezza assegnato ad Azure AD.

Per rimuovere l'appartenenza tra il gruppo di sicurezza dinamico di Azure AD e il gruppo di sicurezza assegnato ad Azure AD quando il gruppo di sicurezza dinamico di Azure AD viene eliminato insieme al catalogo macchine:

1. Ottenere il token di accesso.
2. Eseguire il seguente comando **PowerShell** nella console **PowerShell**:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Modificare il nome del gruppo di sicurezza dinamico di Azure AD

È possibile modificare il nome del gruppo di sicurezza dinamico di Azure AD associato a un catalogo di macchine. Questa modifica rende le informazioni sul gruppo di sicurezza archiviate nell'oggetto del pool di identità di Azure AD coerenti con le informazioni archiviate nel portale di Azure.

> **Nota:**
>
> I gruppi di sicurezza dinamici di Azure AD non includono i gruppi di sicurezza sincronizzati da AD locale e altri tipi di gruppi come il gruppo Office 365.

È possibile modificare il nome del gruppo di sicurezza dinamico di Azure AD utilizzando l'interfaccia Full Configuration e i comandi **PowerShell**.

Per modificare il nome del gruppo di sicurezza dinamico di Azure AD utilizzando **PowerShell**:

1. Aprire la finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli **PowerShell** specifici di Citrix.
3. Eseguire il comando `Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]`.

Se il nome del gruppo di sicurezza dinamico di Azure AD non può essere modificato, vengono visualizzati i messaggi di errore appropriati.

## Creare cataloghi compatibili con Microsoft Intune

November 30, 2022

Questo articolo descrive come creare cataloghi compatibili con Microsoft Intune utilizzando Citrix DaaS. È possibile abilitare Microsoft Intune utilizzando l'interfaccia Full Configuration (Configurazione completa) o PowerShell.

Per informazioni su requisiti, limitazioni e considerazioni, vedere Microsoft Intune.

### Utilizzare l'interfaccia Full Configuration

Le seguenti informazioni sono un'aggiunta alle linee guida della sezione Creare cataloghi delle macchine. Questa funzionalità richiede la selezione di **Azure Active Directory joined** (Aggiunta ad Azure Active Directory) in **Machine Identities** (Identità macchine) durante la creazione del catalogo. Seguire le linee guida generali in quell'articolo, tenendo conto dei dettagli specifici di questa funzionalità.

Nella procedura guidata per la creazione del catalogo:

- Nella pagina **Machine Identities** (Identità macchine), selezionare **Azure Active Directory joined** (Aggiunta ad Azure Active Directory) e quindi **Enroll the machines in Microsoft Intune** (Registra le macchine in Microsoft Intune). Se l'opzione è abilitata, registrare le macchine in Microsoft Intune per la gestione.

### Utilizzare PowerShell

Di seguito sono riportati i passaggi di PowerShell equivalenti alle operazioni nell'interfaccia Full Configuration (Configurazione completa).

Per registrare macchine in Microsoft Intune utilizzando l'SDK Remote PowerShell, utilizzare il parametro `DeviceManagementType` in `New-AcctIdentityPool`. Questa funzionalità richiede che il catalogo sia aggiunto ad Azure AD e che Azure AD disponga della licenza Microsoft Intune corretta. Ad esempio:

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
     IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "
     AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -
     NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-
     ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

### Risoluzione dei problemi

Se non è possibile registrare le macchine in Microsoft Intune, procedere come segue:

- Controllare se le macchine di cui è stato eseguito il provisioning con MCS sono aggiunte ad Azure AD. Le macchine non riescono a registrarsi a Microsoft Intune se non sono aggiunte ad Azure AD. Vedere https://docs.citrix.com/it-it/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.html per risolvere i problemi di aggiunta ad Azure AD.

- Controllare se al tenant di Azure AD è assegnata la licenza Intune appropriata. Per informazioni sui requisiti di licenza di Microsoft Intune, vedere https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses.
- Controllare lo stato di provisioning dell'estensione **AADLoginForWindows** per le macchine. MCS si basa su questa estensione per aggiungere una macchina virtuale ad Azure AD ed effettuare la registrazione in Microsoft Intune. Se l'estensione **AADLoginForWindows** non esiste, i possibili motivi sono:
  - `IdentityType` del pool di identità associato allo schema di provisioning non è impostato su `AzureAD` o se `DeviceManagementType` non è impostato su `Intune`. È possibile verificarlo eseguendo `Get-AcctIdentityPool`.
  - L'installazione dell'estensione **AADLoginForWindows** è bloccata dalla politica di Azure.
- Per risolvere gli errori di assegnazione dell'estensione **AADLoginForWindows**, è possibile controllare i registri in `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` nelle macchine di cui è stato eseguito il provisioning con MCS.
- Controllare i registri degli eventi di Windows in **Registri applicazioni e servizi > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.

## Creare cataloghi aggiunti ad Azure Active Directory ibrido

December 5, 2023

In questo articolo viene descritto come creare cataloghi aggiunti ad Azure Active Directory (AD) ibrida utilizzando Citrix DaaS.

È possibile creare cataloghi aggiunti ad Azure AD utilizzando l'interfaccia Full Configuration (Configurazione completa) o PowerShell.

Per informazioni su requisiti, limitazioni e considerazioni, vedere Aggiunto ad Azure Active Directory ibrido.

### Utilizzare l'interfaccia Full Configuration

Le seguenti informazioni sono un'aggiunta alle linee guida della sezione Creare cataloghi delle macchine. Per creare cataloghi aggiunti ad Azure AD ibrido, seguire le linee guida generali in quell'articolo, tenendo conto dei dettagli specifici per i cataloghi aggiunti ad Azure AD ibrido.

Nella procedura guidata per la creazione del catalogo:

- Nella pagina **Machine Identities** (Identità computer), selezionare **Hybrid Azure Active Directory joined** (Aggiunto ad Azure Active Directory ibrido). Le macchine create sono di proprietà di un'organizzazione e hanno effettuato l'accesso con un account Active Directory Domain Services appartenente a tale organizzazione. Esistono nel cloud e on-premise.

> **Nota:**
>
> Se si seleziona **Hybrid Azure Active Directory joined** (Aggiunto ad Azure Active Directory ibrido) come tipo di identità, ogni macchina del catalogo deve disporre di un account computer AD corrispondente.

### Utilizzare PowerShell

Di seguito sono riportati i passaggi di PowerShell equivalenti alle operazioni nell'interfaccia Full Configuration. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

La differenza tra i cataloghi aggiunti ad AD locale e quelli aggiunti ad Azure AD ibrido sta nella creazione del pool di identità e degli account macchina.

Per creare un pool di identità insieme agli account per i cataloghi aggiunti ad Azure AD ibrido:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

> **Nota:**
>
> `$password` è la password corrispondente per un account utente AD con autorizzazioni di scrittura.

Tutti gli altri comandi utilizzati per creare cataloghi aggiunti ad Azure AD ibrido sono gli stessi dei tradizionali cataloghi aggiunti ad AD locale.

### Visualizzare lo stato del processo di join di Azure AD ibrido

Nell'interfaccia Full Configuration (Configurazione completa), lo stato del processo di join di Azure AD ibrida è visibile quando le macchine aggiunte ad Azure AD ibrida in un gruppo di consegna sono in

stato di accensione. Per visualizzare lo stato, utilizzare Search (Cerca) per identificare tali macchine e quindi per ogni controllo **Machine Identity** (Identità macchina) nella scheda **Details** (Dettagli) nel riquadro inferiore. In **Machine Identity** (Identità macchina) possono essere visualizzate le seguenti informazioni:

- Aggiunto ad Azure AD ibrido
- Not yet joined to Azure AD (Non ancora aggiunta ad Azure AD)

> **Nota:**
>
> - Si potrebbe riscontrare un ritardo nell'aggiunta ad Azure AD ibrido alla prima accensione della macchina. Questo è causato dall'intervallo di sincronizzazione dell'identità della macchina predefinita (30 minuti di Azure AD Connect). La macchina si trova nello stato Hybrid Azure AD joined (Aggiunta ad Azure AD ibrido) solo dopo che le identità delle macchine sono state sincronizzate con Azure AD tramite Azure AD Connect
> - Se le macchine non si trovano nello stato Hybrid Azure AD joined (Aggiunta ad Azure AD ibrido), non vengono registrate con il Delivery Controller. Il loro stato di registrazione viene visualizzato come **Initialization** (Inizializzazione).

Inoltre, utilizzando l'interfaccia Full Configuration (Configurazione completa), è possibile scoprire perché le macchine non sono disponibili. A tale scopo, fare clic su una macchina nel nodo **Search** (Cerca), selezionare **Registration** (Registrazione) nella scheda **Details** (Dettagli) nel riquadro inferiore, quindi leggere la descrizione comando per ulteriori informazioni.

### Risoluzione dei problemi

Se l'aggiunta delle macchine ad Azure AD ibrido non va a buon fine, procedere come segue:

- Controllare se l'account della macchina è stato sincronizzato con Azure AD tramite il portale Microsoft Azure AD. Se è sincronizzato, viene visualizzato il messaggio **Not yet joined to Azure AD** (Non ancora aggiunta ad Azure AD), a indicare lo stato della registrazione in sospeso.

  Per sincronizzare gli account delle macchine con Azure AD, assicurarsi che:

  - L'account della macchina si trovi nell'unità organizzativa configurata per la sincronizzazione con Azure AD. Gli account macchina senza l'attributo **userCertificate** non vengono sincronizzati con Azure AD anche se si trovano nell'unità organizzativa configurata per la sincronizzazione.
  - L'attributo **userCertificate** viene inserito nell'account della macchina. Utilizzare Active Directory Explorer per visualizzare l'attributo.
  - Azure AD Connect deve essere stato sincronizzato almeno una volta dopo la creazione dell'account della macchina. In caso contrario, eseguire manualmente il comando `Start-`

`ADSyncSyncCycle -PolicyType Delta` nella console PowerShell della macchina Azure AD Connect per attivare una sincronizzazione immediata.

- Verificare se la coppia di chiavi del dispositivo gestito da Citrix per il join di Azure AD ibrido è stata correttamente inviata alla macchina interrogando il valore di **DeviceKeyPairRestored** in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verificare che il valore sia 1. In caso contrario, i possibili motivi sono:

  - `IdentityType` del pool di identità associato allo schema di provisioning non è impostato su `HybridAzureAD`. È possibile verificarlo eseguendo `Get-AcctIdentityPool`.
  - Il provisioning della macchina non viene eseguito utilizzando lo stesso schema di provisioning del catalogo delle macchine.
  - La macchina non è aggiunta al dominio locale. L'aggiunta a un dominio locale è un prerequisito del join di Azure AD ibrido.

- Controllare i messaggi diagnostici eseguendo il comando `dsregcmd /status /debug` sulla macchina di cui è stato eseguito il provisioning con MCS.

  - Se il join di Azure AD ibrido ha esito positivo, **AzureAdJoined** e **DomainJoined** sono **YES** (Sì) nell'output della riga di comando.
  - In caso contrario, fare riferimento alla documentazione di Microsoft per risolvere i problemi: https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.
  - Se viene visualizzato il messaggio di errore **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** (Messaggio del server: il certificato utente non è trovato sul dispositivo con id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx), eseguire il seguente comando PowerShell per riparare il certificato utente:

    ```
    1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
          UserCertificate
    2  <!--NeedCopy-->
    ```

Per ulteriori informazioni sul problema del certificato utente, vedere CTX566696.

## Creare cataloghi non aggiunti a un dominio

November 16, 2022

Questo articolo descrive come creare cataloghi non aggiunti a un dominio utilizzando Citrix DaaS.

Per informazioni su requisiti, limitazioni e considerazioni, vedere Non-domain-joined.

Prima di creare il catalogo di macchina, è necessario quanto segue:

1. Nuova posizione risorsa
    - Accedere all'interfaccia utente di amministrazione di Citrix Cloud > menu hamburger in alto a sinistra > **Resource Locations** (Posizioni risorsa).
    - Fare clic su **+ Resource Location** (+ Posizione risorsa).
    - Immettere un nome per la nuova posizione risorsa e fare clic su **Save** (Salva).
2. Creare una connessione host. Per i dettagli, vedere la sezione Creare e gestire connessioni.

Utilizzando Citrix DaaS, è possibile creare cataloghi basati su gruppi di lavoro o macchine non aggiunte a un dominio. La creazione di macchine non aggiunte a un dominio dipende dalla modalità di creazione del pool di identità degli account. Il pool di identità degli account è il meccanismo utilizzato da MCS per creare i nomi delle macchine e tenerne traccia durante il provisioning del catalogo.

È possibile creare cataloghi non aggiunti a un dominio utilizzando l'interfaccia Full Configuration (Configurazione completa) o PowerShell.

### Utilizzare l'interfaccia Full Configuration

Le seguenti informazioni sono un'aggiunta alle linee guida della sezione Creare cataloghi delle macchine. Per creare cataloghi non aggiunti a un dominio, seguire le linee guida generali in quell'articolo, tenendo conto dei dettagli specifici dei cataloghi non aggiunti a un dominio.

Nella procedura guidata per la creazione del catalogo:

- Nella pagina **Machine Identities** (Identità computer), selezionare **Non-domain-joined** (Non aggiunta a un dominio). Le macchine create non sono aggiunte a nessun dominio.

> **Nota:**
>
> Il tipo di identità **Non-domain-joined** (Non aggiunte al dominio) richiede la versione 1811 o successiva del VDA come livello di funzionalità minimo per il catalogo. Per renderla disponibile, aggiornare il livello funzionale minimo, se necessario.

### Utilizzare PowerShell

Di seguito sono riportati i passaggi di PowerShell equivalenti alle operazioni nell'interfaccia Full Configuration (Configurazione completa).

È possibile creare un pool di identità per cataloghi non aggiunti a un dominio utilizzando l'SDK Remote PowerShell.

Ad esempio, nelle versioni precedenti tutti i campi di Active Directory sono stati forniti in un'unica istanza:

```
New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -
    IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-##"
    -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local"* -
    Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
<!--NeedCopy-->
```

MCS ora utilizza i nuovi parametri di PowerShell, **WorkgroupMachine** e **IdentityType**, per creare un pool di identità per i cataloghi non aggiunti a un dominio. Utilizzando lo stesso esempio di cui sopra, i parametri eliminano la necessità di specificare tutti i parametri specifici di AD, comprese le credenziali dell'amministratore di dominio:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -
    WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -
    NamingScheme "NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -
    ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
<!--NeedCopy-->
```

Tutti gli altri comandi utilizzati per creare cataloghi non aggiunti a un dominio sono gli stessi dei tradizionali cataloghi aggiunti ad Active Directory on-premise.

## Gestire i cataloghi delle macchine

December 20, 2023

> **Nota:**
>
> In questo articolo viene descritto come gestire i cataloghi utilizzando l'interfaccia Full Configuration (Configurazione completa). Se il catalogo è stato creato utilizzando l'interfaccia Quick Deploy (Distribuzione rapida) e si desidera continuare a utilizzare tale interfaccia per gestire il catalogo, seguire le istruzioni riportate in Gestire i cataloghi in Quick Deploy (Distribuzione rapida).

### Introduzione

È possibile aggiungere o rimuovere macchine da un catalogo delle macchine, rinominare gli account computer Active Directory, modificarne la descrizione o gestirli.

La manutenzione del catalogo può anche includere le attività di verifica che ogni macchina abbia gli ultimi aggiornamenti del sistema operativo, gli aggiornamenti del software antivirus o le modifiche alla configurazione.

- I cataloghi contenenti macchine casuali raggruppate in pool create utilizzando Machine Creation Services (MCS) gestiscono le macchine aggiornando l'immagine utilizzata nel catalogo e quindi aggiornando le macchine. Questo metodo consente di aggiornare un numero elevato di macchine utente in modo efficiente.
- Per i cataloghi contenenti macchine statiche assegnate in modo permanente, è possibile gestire l'immagine o il modello attualmente utilizzato da tali cataloghi, ma solo le macchine aggiunte ai cataloghi successivamente vengono create utilizzando la nuova immagine o modello.
- Per i cataloghi Remote PC Access (Accesso remoto PC), è possibile gestire gli aggiornamenti delle macchine degli utenti al di fuori dell'interfaccia di gestione Full Configuration (Configurazione completa). Eseguire questa attività singolarmente o collettivamente utilizzando strumenti di distribuzione software di terze parti.

Per informazioni sulla creazione e la gestione delle connessioni agli hypervisor host e ai servizi cloud, vedere Connessioni e risorse.

> **Nota:**
>
> MCS non supporta Windows 10 IoT Core e Windows 10 IoT Enterprise. Per ulteriori informazioni, fare riferimento al sito Microsoft.

#### Informazioni sulle istanze persistenti

Quando si aggiorna l'immagine master per un catalogo MCS contenente macchine persistenti, tutte le nuove macchine aggiunte al catalogo utilizzano l'immagine aggiornata. Le macchine esistenti continuano a utilizzare l'immagine master originale. Il processo di aggiornamento di un'immagine viene eseguito allo stesso modo per qualsiasi altro tipo di catalogo. Considerare quanto segue:

- Nel caso dei cataloghi dei dischi persistenti, le macchine preesistenti non vengono aggiornate alla nuova immagine, ma tutte le nuove macchine aggiunte al catalogo utilizzano la nuova immagine.
- Per i cataloghi di dischi non persistenti, l'immagine della macchina viene aggiornata la volta successiva solo se la macchina viene riavviata all'interno di Studio o PowerShell. Se la macchina viene riavviata dall'hypervisor al di fuori di Studio, il disco non viene ripristinato.
- Nel caso dei cataloghi che non persistono, se si desidera utilizzare immagini diverse per macchine diverse, le immagini devono risiedere in cataloghi separati.

### Aggiungere macchine a un catalogo

Prima di iniziare:

- Assicurarsi che l'host di virtualizzazione (hypervisor o fornitore del servizio cloud) disponga di processori, memoria e archiviazione sufficienti per ospitare le macchine aggiuntive.

- Assicurarsi di disporre di un numero sufficiente di account computer Active Directory inutilizzati. Se si utilizzano account esistenti, il numero di computer che è possibile aggiungere è limitato dal numero di account disponibili.
- Se si utilizza l'interfaccia di gestione Full Configuration (Configurazione completa) per creare account computer Active Directory per le macchine aggiuntive, è necessario disporre dell'autorizzazione di amministratore di dominio appropriata.

> **Suggerimento:**
>
> Se l'account Citrix DaaS utilizzato per aggiungere macchine al catalogo delle macchine dispone di autorizzazioni AD limitate, aggiungere tutti i Cloud Connector che si intende utilizzare nella schermata **Log on to...** (Accesso a...).

Per aggiungere macchine a un catalogo:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo delle macchine, quindi selezionare **Add machines** (Aggiungi macchine) nella barra delle azioni.
3. Nella pagina **Virtual Machines** (Macchine virtuali), selezionare il numero di macchine virtuali da aggiungere.
4. Nella pagina **Machine Identities** (Identità macchine), configurare le impostazioni come segue:
   - Selezionare un'identità dall'elenco.
   - Se applicabile, indicare se creare account o utilizzare quelli esistenti e la posizione (dominio) per tali account.

     Se gli account Active Directory esistenti non sono sufficienti per il numero di macchine virtuali che si stanno aggiungendo, selezionare il dominio e il percorso in cui vengono creati gli account.

     Se si utilizzano account Active Directory esistenti, selezionare gli account oppure selezionare **Import** (Importa) e specificare un file .csv contenente i nomi degli account. Assicurarsi che ci siano account sufficienti per tutte le macchine che si stanno aggiungendo. L'interfaccia Full Configuration (Configurazione completa) gestisce questi account. Consentire all'interfaccia di reimpostare le password per tutti gli account o specificare la password dell'account, che deve essere la stessa per tutti gli account.
   - Se questo pool di identità viene utilizzato da altri cataloghi, non è possibile passare a un pool diverso utilizzando Full Configuration. Utilizzare invece il cmdlet **Set-ProvScheme** di PowerShell. Per ulteriori informazioni, vedere la documentazione di Citrix Virtual Apps and Desktops SDK.

- Specificare uno schema di denominazione degli account, utilizzando i marcatori hash per indicare dove compaiono numeri o lettere sequenziali. Ad esempio, uno schema di denominazione PC-Vendite-## (in cui è selezionato 0-9) genera account computer denominati PC-Vendite-01, PC-Vendite-02, PC-Vendite-03 e così via.
- Facoltativamente, è possibile specificare con cosa iniziano i nomi degli account.

  Quando si specifica con cosa iniziano i nomi degli account, tenere presente il seguente scenario: se i numeri o le lettere iniziali sono già in uso, il primo account creato viene denominato utilizzando i numeri o le lettere inutilizzati più vicini di seguito.

5. Nella pagina **Domain Credentials** (Credenziali di dominio), selezionare **Enter credentials** (Immettere le credenziali) e immettere le credenziali utente con autorizzazioni sufficienti per creare account delle macchine.

Le macchine vengono create come processo in background e la creazione di molte macchine può richiedere molto tempo. La creazione della macchina continua anche se si chiude l'interfaccia di gestione Full Configuration (Configurazione completa).

#### Utilizzare i file CSV per aggiungere macchine in blocco a un catalogo

È possibile aggiungere macchine in blocco utilizzando file CSV. La funzionalità è disponibile per tutti i cataloghi ad eccezione dei cataloghi di cui viene eseguito il provisioning tramite MCS.

Per aggiungere macchine in blocco a un catalogo, attenersi alla seguente procedura:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo delle macchine, quindi selezionare **Add Machines** (Aggiungi macchine) nella barra delle azioni. Viene visualizzata la finestra **Add Machines** (Aggiungi macchine).
3. Selezionare **Add CSV File** (Aggiungi file CSV). Viene visualizzata la finestra **Add Machines in Bulk** (Aggiungi macchine in blocco).
4. Selezionare **Download CSV Template** (Scarica modello CSV).
5. Compilare il file del modello.
6. Trascinare o sfogliare il file per caricarlo.
7. Selezionare **Validate** (Convalida) per eseguire controlli di convalida sull'importazione.
8. Selezionare **Import** (Importa) per completare il processo.

#### Considerazioni sull'utilizzo di file CSV per aggiungere macchine

> **Nota:**
>
> - Per gli utenti non Active Directory, è necessario digitare i nomi nel seguente formato: `<identity provider>:<user name>`. Esempio: `AzureAD:username`.
> - I nomi delle VM distinguono tra maiuscole e minuscole. Quando si inseriscono i percorsi delle VM, assicurarsi di aver inserito correttamente i nomi delle VM.

Quando si modifica il file modello CSV, tenere presente quanto segue:

- Questa funzionalità offre una maggiore flessibilità per aggiungere macchine in blocco tramite un file CSV. Nel file è possibile aggiungere solo macchine (da utilizzare con assegnazioni automatiche degli utenti) o aggiungere macchine insieme alle assegnazioni utente. Digitare i dati nel formato seguente:
  - Per le coppie di account macchina e nome utente (samName):
    - Domain\ComputerName1, Domain\Username1
    - Domain\ComputerName2, Domain\Username1;Domain\Username2
    - Dominio\NomeComputer3, AzureAD:nomeutente
  - Solo per gli account macchina:
    - Domain\ComputerName1
    - Domain\ComputerName2
  - Per le coppie di macchine virtuali e nome utente:
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer
  - Solo per le macchine virtuali:
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer

    Ad esempio:
    `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

    dove

    - `xpace-scale` è il NomeConnessione: il nome della connessione che si è inserito in **Full Configuration > Hosting > Add Connections and Resources** (Configurazione completa > Hosting > Aggiungi connessioni e risorse). Per ulteriori informazioni, vedere Creare una connessione e risorse.
    - `East US.region` è il NomeRegione: il nome della regione con estensione `.region`.

        * `wsvdaV3-2.vm` è NomeVM: il nome della macchina virtuale con estensione `.vm`.

- Il numero massimo di macchine che un file può contenere è 1.000. Per importare più di 1.000 macchine, distribuirle su file diversi e quindi importarli uno ad uno. Si consiglia di importare non più di 1.000 macchine. In caso contrario, il completamento della creazione del catalogo può richiedere molto tempo.

È inoltre possibile esportare macchine da un catalogo nella stessa pagina **Add Machines** (Aggiungi macchine). Il file CSV esportato delle macchine può quindi essere utilizzato come modello quando si aggiungono macchine in blocco. Per esportare macchine:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo delle macchine, quindi selezionare **Add Machines** (Aggiungi macchine) nella barra delle azioni. Viene visualizzata la finestra **Add Machines** (Aggiungi macchine).
3. Selezionare **Export to CSV file** (Esporta in file CSV). Viene scaricato un file CSV contenente un elenco delle macchine.
4. Aprire il file CSV per aggiungere o modificare le macchine secondo necessità. Per aggiungere macchine in blocco utilizzando il file CSV salvato, vedere la sezione precedente, Utilizzare i file CSV per aggiungere in blocco macchine a un catalogo.

> **Nota:**
>
> - Questa funzionalità non è disponibile per i cataloghi Remote PC Access (Accesso remoto PC) e di cui viene eseguito il provisioning tramite MCS.
> - L'esportazione e l'importazione di macchine in file CSV sono supportate solo tra cataloghi dello stesso tipo.

### Recuperare gli avvisi e gli errori associati a un catalogo

È possibile visualizzare la cronologia degli errori e degli avvisi per comprendere i problemi del catalogo delle macchine MCS e risolverli.

Utilizzando i comandi PowerShell, è possibile:

- Ottenere un elenco di errori o avvisi
- Cambiare lo stato di avviso da **New** (Nuovo) ad **Acknowledged** (Riconosciuto)
- Eliminare gli errori o gli avvisi

Per eseguire i comandi PowerShell:

1. Aprire una finestra di PowerShell.

2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.

Per ottenere un elenco di errori e avvisi:

Eseguire il comando `Get-ProvOperationEvent`.

- Senza parametri: si ricevono tutti gli errori e gli avvisi
- Con i parametri `LinkedObjectType` e `LinkedObjectUid`: si ricevono tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con il parametro `EventId`: si riceve un errore o un avviso specifico che corrisponde a questo ID evento
- Con il parametro `Filter`: si ricevono errori o avvisi tramite un filtro personalizzato

Per modificare lo stato degli errori o degli avvisi da **New** (Nuovo) ad **Acknowledged** (Riconosciuto):

Eseguire il comando `Confirm-ProvOperationEvent`.

- Con il parametro`EventId`: imposta lo stato di un errore o di un avviso specifico che corrisponde a questo ID evento. È possibile ottenere l'`EventId` di un errore o un avviso specifico come uscita dal comando `Get-ProvOperationEvent`
- Con i parametri `LinkedObjectType` e `LinkedObjectUid`: imposta lo stato di tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con il parametro `All`: imposta lo stato di tutti gli avvisi come **Acknowledged**.

Per eliminare gli errori o gli avvisi:

Eseguire il comando `Remove-ProvOperationEvent`.

- Con il parametro `EventId`: rimuove un errore o un avviso specifico che corrisponde a questo ID evento. È possibile ottenere l'`EventId` di un errore o un avviso specifico come uscita dal comando `Get-ProvOperationEvent`
- Con i parametri `LinkedObjectType` e `LinkedObjectUid`: rimuove tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con il parametro `All`: rimuove tutti gli errori e gli avvisi

Per ulteriori informazioni, vedere Citrix PowerShell SDK.

### Eliminare macchine da un catalogo

Dopo aver eliminato un computer da un catalogo di macchine, gli utenti non possono più accedervi, quindi prima di eliminare un computer, assicurarsi che si verifichino le seguenti condizioni:

- I dati utente sono stati sottoposti a backup o non sono più necessari.
- Tutti gli utenti sono disconnessi. L'attivazione della modalità di manutenzione impedisce la creazione di nuovi collegamenti a una macchina.

- Le macchine sono spente.

Per eliminare macchine da un catalogo:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
3. Selezionare una o più macchine, quindi selezionare **Delete** (Elimina) nella barra delle azioni.
4. Se si stanno eliminando macchine persistenti dal catalogo, scegliere se eliminarle anche dall'hypervisor o dal servizio cloud. Se si decide di eliminarle, indicare se conservare, disabilitare o eliminare i loro account Active Directory.

Quando si eliminano macchine persistenti da un catalogo di Azure Resource Manager, le macchine e i gruppi di risorse associati vengono eliminati da Azure, anche se si decide di conservarli.

Quando si eliminano macchine non persistenti da un catalogo, queste vengono automaticamente eliminate dall'hypervisor o dal servizio cloud.

## Eliminare i computer senza accesso all'hypervisor

Quando si elimina una macchina virtuale o uno schema di provisioning, MCS deve rimuovere i tag dalla macchina virtuale e talvolta anche dal disco di base, in modo che le risorse incluse nelle opzioni di eliminazione non vengano più tracciate o identificate da MCS. Tuttavia, alcune di queste risorse sono accessibili solo tramite hypervisor. Utilizzare l'opzione `PurgeDBOnly` in `Remove-ProvVM` di PowerShell per eliminare oggetti di risorse VM come VM, disco di base, immagine in ACG e così via dal database anche in assenza di accesso tramite hypervisor.

Questa opzione è abilitata su:

- tutti gli hypervisor supportati
- le VM persistenti e non persistenti

### Limiti

Non è possibile utilizzare contemporaneamente i comandi -purgeDBOnly e -ForgetVM.

### Utilizzare il comando PurgeDBOnly

Quando si esegue il comando PowerShell `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM`, l'operazione di eliminazione potrebbe non riuscire nei seguenti scenari:

- La connessione host è in modalità di manutenzione
- Credenziali non valide
- Errore di autenticazione
- Operazione non autorizzata
- Hypervisor non raggiungibile

> **Nota:**
>
> Remove-provVM -ForgetVM interessa solo le VM persistenti. Se una delle macchine virtuali dell'elenco non è persistente, l'operazione non riesce.

Quando l'operazione non riesce perché l'hypervisor non è raggiungibile, viene visualizzato il seguente messaggio:

```
Try to use -PurgeDBOnly option to clean DDC database.
```

Utilizzare l'opzione `-PurgeDBOnly` del comando `Remove-ProvVM` di PowerShell per eliminare i riferimenti di una macchina virtuale dal database MCS. Ad esempio,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

### Modificare un catalogo

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo, quindi selezionare **Edit Machine Catalog** (Modifica catalogo delle macchine) nella barra delle azioni.
3. Nella pagina **Scopes** (Ambiti), modificare gli ambiti.
4. Nella pagina **VDA Upgrade** (Aggiornamento VDA), modificare o selezionare la versione del VDA a cui eseguire l'aggiornamento. Per ulteriori informazioni, vedere Aggiornamento dei VDA.
5. È possibile che vengano visualizzate pagine aggiuntive a seconda del tipo di catalogo.

   Per i cataloghi creati utilizzando un'immagine di Azure Resource Manager, sono visibili le pagine seguenti. Tenere presente che le modifiche apportate si applicano solo alle macchine che verranno aggiunte al catalogo in un secondo momento. Le macchine esistenti rimangono invariate.

   - Nella pagina **Virtual Machines** (Macchine virtuali), modificare le dimensioni delle macchine e le zone di disponibilità in cui si desidera creare macchine.

> **Nota:**
>
> – Sono mostrate solo le dimensioni delle macchine supportate dal catalogo.
> – Se necessario, selezionare **Show only machine sizes used in other machine catalogs** (Mostra solo le dimensioni delle macchine utilizzate in altri cataloghi delle macchine) per filtrare l'elenco delle dimensioni delle macchine.

- Nella pagina **Machine Profile** (Profilo macchina), scegliere se utilizzare o modificare un profilo macchina.
- (Solo quando il catalogo è configurato con un host di gruppo dedicato) Nella pagina **Dedicated host group** (Gruppo di host dedicato), scegliere se modificare un gruppo di host.
- Nella pagina **Storage and License Types** (Tipi di archiviazione e licenza), scegliere se modificare il tipo di archiviazione, il tipo di licenza e le impostazioni di Azure Computer Gallery (disponibile solo quando è in uso il comando **Place prepared image in Azure Gallery** [Inserisci l'immagine preparata nella Raccolta di calcolo di Azure]).

> **Nota:**
>
> Se l'impostazione appena selezionata non supporta le dimensioni correnti della macchina, viene visualizzata una finestra di dialogo di avviso che informa che la modifica dell'impostazione reimposterà le dimensioni della macchina. Se si sceglie di continuare, accanto al menu **Virtual Machines** (Macchine virtuali) viene visualizzato un punto rosso che richiede di selezionare una nuova dimensione della macchina.

Per ulteriori informazioni sulle impostazioni disponibili nelle pagine, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

Per i cataloghi Remote PC Access (Accesso remoto PC), sono visibili le seguenti pagine:

- Nella pagina **Power Management** (Gestione alimentazione), modificare le impostazioni di gestione dell'alimentazione e selezionare una connessione per il risparmio energia.
- Nella pagina **Organizational Units** aggiungere o rimuovere le unità organizzative di Active Directory.

6. Nella pagina **Description** modificare la descrizione del catalogo.
7. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e fare clic su **Save** (Salva) per uscire.

### Rinominare un catalogo

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.

2. Selezionare un catalogo, quindi selezionare **Rename Machine Catalog** (Rinomina catalogo delle macchine) nella barra delle azioni.
3. Immettere il nuovo nome.

### Eliminare un catalogo

Prima di eliminare un catalogo, assicurarsi che si verifichino le seguenti condizioni:

- Tutti gli utenti sono disconnessi e non sono in esecuzione sessioni disconnesse.
- La modalità di manutenzione è attivata per tutte le macchine del catalogo, in modo che non sia possibile effettuare nuove connessioni.
- Tutte le macchine nel catalogo sono spente.
- Il catalogo non è associato a un gruppo di consegna. In altre parole, il gruppo di consegna non contiene macchine del catalogo.

Per eliminare un catalogo:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo, quindi selezionare **Delete Machine Catalog** (Elimina catalogo delle macchine) nella barra delle azioni.
3. Se il catalogo contiene macchine persistenti, indica se eliminare anche quelle macchine dall'hypervisor o dal servizio cloud. Se si decide di farlo, scegliere se conservare, disabilitare o eliminare i loro account computer di Active Directory.
4. Se necessario, selezionare **Hide progress** (Nascondi avanzamento) per eseguire l'eliminazione in background.

> **Nota:**
>
> - Quando si elimina un catalogo di Azure Resource Manager, le macchine e i gruppi di risorse associati vengono eliminati da Azure, anche se si decide di conservarli.
> - Quando si elimina un catalogo contenente macchine non persistenti, tali macchine vengono eliminate dall'hypervisor o dal servizio cloud.
> - Quando l'hypervisor o il servizio cloud non è raggiungibile durante l'eliminazione del catalogo, non riesce sia l'eliminazione del catalogo che quella della macchina virtuale. Se necessario, è possibile scegliere di eliminare i record delle macchine virtuali solo dal database del sito Citrix. A tale scopo, selezionare il catalogo di macchine nel nodo **Machine Catalogs**, quindi eseguire l'eliminazione illustrata nella scheda **Troubleshoot** (Risoluzione dei problemi). Tenere presente che questa azione lascia le macchine virtuali intatte sull'host.

### Gestire gli account computer di Active Directory in un catalogo

Per gestire gli account Active Directory in un catalogo di macchine, è possibile:

- Liberare gli account macchina inutilizzati rimuovendo gli account computer Active Directory dai cataloghi con sistemi operativi a sessione singola e multisessione. Questi account possono quindi essere utilizzati per altre macchine.
- Aggiungere account in modo che quando più computer vengono aggiunti al catalogo, gli account computer siano già presenti. Non utilizzare una barra (/) in un nome di unità organizzativa.

Per gestire gli account Active Directory:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo e quindi selezionare **Manage AD accounts** (Gestisci account AD) nella barra delle azioni.
3. Scegliere se aggiungere o eliminare account computer. Se si aggiungono account, specificare cosa fare con le password degli account: reimpostarle tutte o immettere una password valida per tutti gli account.

   È possibile reimpostare le password se non si conoscono le password dell'account correnti; è necessario disporre dell'autorizzazione per eseguire la reimpostazione delle password. Se si immette una password, la password viene modificata negli account man mano che vengono importati. Se si elimina un account, scegliere se l'account in un'Active Directory deve essere mantenuto, disabilitato o eliminato.

È anche possibile indicare se gli account Active Directory devono essere mantenuti, disabilitati o eliminati quando si rimuovono macchine da un catalogo o si elimina un catalogo.

### Modificare l'immagine master di un catalogo

Consigliamo di salvare copie o snapshot delle immagini prima di modificare l'immagine master di un catalogo. Il database conserva una cronologia delle immagini utilizzate con ogni catalogo delle macchine. Se gli utenti riscontrano problemi relativi alla nuova immagine distribuita sui loro desktop, è possibile ripristinarla alla versione precedente, riducendo al minimo i tempi di inattività degli utenti. Non eliminare, spostare o rinominare le immagini. Altrimenti, non è possibile eseguire il rollback dell'immagine master.

> **Importante:**
>
> Quando si modifica l'immagine master di un catalogo persistente, tenere presente quanto segue:

> solo le macchine aggiunte al catalogo in un secondo momento vengono create utilizzando la nuova immagine. Non implementiamo la nuova immagine nelle macchine esistenti nel catalogo.

Dopo l'aggiornamento, il computer viene riavviato automaticamente.

#### Aggiornare o creare un'immagine

Prima di modificare l'immagine master di un catalogo, preparare una nuova immagine sull'hypervisor host aggiornando un'immagine esistente o creandone una.

1. Nell'hypervisor o nel fornitore di servizi cloud, acquisire una snapshot della macchina virtuale corrente e assegnarle un nome significativo. Questa snapshot può essere utilizzata per ripristinare l'immagine master.
2. Se necessario, avvire l'immagine ed effettuare l'accesso.
3. Installare gli aggiornamenti o apportare le modifiche necessarie all'immagine.
4. Se l'immagine utilizza un vDisk personale, aggiornare l'inventario.
5. Spegnere la macchina virtuale.
6. Acquisire una snapshot della macchina virtuale e assegnarle un nome significativo che venga riconosciuto quando si modifica l'immagine master.

> **Nota:**
>
> Sebbene sia possibile creare una snapshot utilizzando l'interfaccia di gestione, consigliamo di creare la snapshot utilizzando la console di gestione dell'hypervisor, quindi di selezionare tale snapshot nell'interfaccia di gestione Full Configuration (Configurazione completa). Questo consente di fornire un nome e una descrizione significativi anziché un nome generato automaticamente. Per le immagini GPU, è possibile modificare l'immagine solo tramite la console XenServer XenCenter.

#### Cambiare l'immagine master

Per distribuire una nuova immagine master su tutte le macchine di un catalogo:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo, quindi selezionare **Change Master Image** (Cambia immagine master) nella barra delle azioni.
3. Nella pagina **Master Image** (Immagine master), selezionare l'host e l'immagine che si desidera implementare.

> **Suggerimento:**
>
> Per un catalogo creato da MCS, è possibile annotarne l'immagine aggiungendo una nota per l'immagine. Una nota può contenere fino a 500 caratteri. Ogni volta che si modifica l'immagine master, viene creata una voce correlata alla nota se si aggiunge una nota. Se si aggiorna un catalogo senza aggiungere una nota, la voce viene visualizzata come null (-). Per visualizzare la cronologia delle note per l'immagine, selezionare il catalogo, fare clic su **Template Properties** (Proprietà modello) nel riquadro inferiore e quindi fare clic su **View note history** (Visualizza cronologia note).

4. Nella pagina **Rollout Strategy** (Strategia di rollout) scegliere quando le macchine nel catalogo delle macchine devono essere modifcate in base alla nuova immagine: al successivo spegnimento o immediatamente.

   > **Nota:**
   >
   > La pagina **Rollout Strategy** non è disponibile per le VM persistenti perché il rollout è applicabile solo alle VM non persistenti.

5. Verificare le informazioni nella pagina **Summary** (Riepilogo) e quindi selezionare **Finish** (Fine). Ogni macchina si riavvia automaticamente dopo l'aggiornamento.

   Per tenere traccia dello stato di avanzamento dell'aggiornamento, individuare il catalogo in **Machine Catalogs** (Cataloghi delle macchine) per visualizzare la barra di avanzamento in linea e il grafico di avanzamento dettagliato. Nel caso di un catalogo non persistente, tramite la colonna **Image Update** (Aggiornamento immagine), è possibile tenere traccia degli stati di aggiornamento delle immagini tra cui **Fully updated** (Completamente aggiornato), **Partially updated** (Parzialmente aggiornato), **Pending update** (In attesa di aggiornamento) e **Preparing image** (Preparazione immagine).

   > **Suggerimento:**
   >
   > Per visualizzare la colonna **In attesa**, selezionate l'icona **Columns to Display** (Colonne da visualizzare) nella barra delle azioni, selezionare **Machine Catalog > Image Status** (Catalogo macchine > Stato immagine), quindi fare clic su **Save**.

Se si aggiorna un catalogo utilizzando l'SDK PowerShell, è possibile specificare un modello di hypervisor (`VMTemplates`) in alternativa a un'immagine o alla snapshot di un'immagine.

**Strategia di rollout:**

La modifica dell'immagine al successivo arresto avrà effetto immediato su tutte le macchine non attualmente in uso, ovvero le macchine che non hanno una sessione utente attiva. Un sistema in uso riceve l'aggiornamento al termine della sessione attiva corrente.

> **Nota:**
>
> La strategia di rollout è applicabile solo alle macchine virtuali non persistenti.

Considerare quanto segue:

- Le nuove sessioni non possono essere avviate fino al completamento dell'aggiornamento sui computer applicabili.
- Le macchine con sistema operativo a sessione singola vengono immediatamente aggiornate quando la macchina non è in uso o quando gli utenti non hanno effettuato l'accesso.
- In un sistema operativo multisessione, i riavvii non vengono eseguiti automaticamente. Le macchine devono essere spente e riavviate manualmente.

> **Suggerimento:**
>
> Limitare il numero di macchine da riavviare utilizzando le impostazioni avanzate per una connessione host. Utilizzare queste impostazioni per modificare le azioni eseguite in un determinato catalogo. Le impostazioni avanzate variano a seconda dell'hypervisor.

Se si desidera abilitare la pianificazione di riavvio una tantum mediante PowerShell, utilizzare i comandi PowerShell `BrokerCatalogRebootSchedule` per creare, modificare ed eliminare una pianificazione di riavvio:

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`
- `Rename-BrokerCatalogRebootSchedule`

Esempio:

- Per creare un programma di riavvio delle macchine virtuali nel catalogo denominato **BankTellers** a partire dal 3 febbraio 2022, tra le 2:00 e le 4:00.

```
New-BrokerCatalogRebootSchedule -Name BankTellers
-CatalogName BankTellers
-StartDate "2022-02-03"
-StartTime "02:00"
-Enabled $true
-RebootDuration 120
<!--NeedCopy-->
```

- Per creare una pianificazione di riavvio delle macchine virtuali del catalogo con UID 17 a partire dal 3 febbraio 2022, tra l'1:00 e le 5:00. Dieci minuti prima del riavvio, ogni macchina virtuale è impostata per visualizzare una finestra di messaggio con il titolo: "**WARNING: Reboot pending**"

(ATTENZIONE: riavvio in sospeso) e il messaggio: "**Save your work**"(Salvare il lavoro) in ogni sessione utente.

```
New-BrokerCatalogRebootSchedule
-Name 'Update reboot'
-CatalogUid 17
-StartDate "2022-02-03"
-StartTime "01:00" -Enabled $true -RebootDuration 240
-WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
<!--NeedCopy-->
```

- Per rinominare la pianificazione di riavvio del catalogo denominata **Old Name** in **New Name**.

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New
    Name"
<!--NeedCopy-->
```

- Per visualizzare tutte le pianificazioni di riavvio del catalogo con UID 1, quindi rinominare la pianificazione di riavvio del catalogo con l'UID 1 in **Nuovo nome**.

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
   BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Per impostare la pianificazione di riavvio del catalogo denominata **Accounting** in modo da visualizzare una finestra di messaggio con il titolo "**WARNING: Reboot pending e il messaggio Save your work**"(ATTENZIONE: riavvio in sospeso. Salvare il lavoro) dieci minuti prima del riavvio di ciascuna macchina virtuale. Il messaggio viene visualizzato in ogni sessione utente su quella macchina virtuale.

```
Set-BrokerCatalogRebootSchedule -Name Accounting
-WarningMessage "Save your work"
-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
<!--NeedCopy-->
```

- Per visualizzare tutte le pianificazioni di riavvio disattivate e quindi abilitare tutte le pianificazioni di riavvio disattivate.

```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
   BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Per impostare la pianificazione del riavvio del catalogo con UID 17 in modo da visualizzare il messaggio **Rebooting in %m% minutes** (Riavvio in %m% minuti) quindici, dieci e cinque minuti prima del riavvio di ogni macchina virtuale.

```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
   %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
<!--NeedCopy-->
```

- Per configurare il fuso orario per il catalogo denominato **MyCatalog**.

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

#### Rollback dell'immagine master

Dopo aver distribuito un'immagine aggiornata o nuova, è possibile eseguire il rollback. Questo potrebbe essere necessario se si verificano problemi nelle macchine appena aggiornate. Quando si esegue il rollback, le macchine incluse nel catalogo vengono ripristinate all'ultima immagine funzionante. Tutte le nuove funzionalità che richiedono l'immagine più recente non sono più disponibili. Come per il rollout, il rollback di un computer include un riavvio.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare il catalogo, quindi selezionare **Roll Back Master Image** (Esegui il rollback dell'immagine master) nella barra delle azioni.
3. Specificare quando applicare l'immagine precedente alle macchine, come descritto per l'operazione di implementazione.

Il rollback viene applicato solo alle macchine che devono essere ripristinate. Per le macchine che non sono state modificate in base all'immagine nuova o aggiornata (ad esempio, macchine con utenti non scollegati), gli utenti non ricevono messaggi di notifica e non sono costretti a scollegarsi.

Per tenere traccia dell'avanzamento del rollback, individuare il catalogo in **Machine Catalogs** (Cataloghi delle macchine) per visualizzare la barra di avanzamento in linea e il grafico di avanzamento dettagliato.

Non è possibile eseguire il rollback in alcuni scenari, inclusi i seguenti (l'opzione **Roll Back Master Image** non è visibile)

- Non si ha il permesso di eseguire il rollback.
- Il catalogo non è stato creato utilizzando MCS.
- Il catalogo è stato creato utilizzando un'immagine del disco del sistema operativo.
- La snapshot utilizzata per creare il catalogo è danneggiata.
- Le modifiche apportate dall'utente alle macchine nel catalogo non sono persistenti.
- Le macchine nel catalogo sono in esecuzione.

### Modificare il livello funzionale o annullare la modifica

Modificare il livello funzionale del catalogo di macchine dopo l'aggiornamento dei VDA sui computer a una versione più recente. Consigliamo di aggiornare tutti i VDA alla versione più recente per consentire l'accesso a tutte le funzionalità più recenti.

Prima di modificare il livello funzionale di un catalogo di macchine:

- Avviare le macchine aggiornate in modo che si registrino con Citrix DaaS. Ciò consente all'interfaccia di gestione di determinare che le macchine nel catalogo devono essere aggiornate.

Per modificare il livello funzionale di un catalogo:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare il catalogo. La scheda **Details** nel riquadro inferiore visualizza le informazioni sulla versione.
3. Selezionare **Change Functional Level** (Cambia livello funzionale). Se l'interfaccia di gestione rileva che è necessario modificare il livello funzionale il catalogo, viene visualizzato un messaggio. Seguire le istruzioni. Se uno o più macchine non possono essere modificate, viene visualizzato un messaggio che ne spiega il motivo. Per garantire che tutte le macchine funzionino correttamente, consigliamo di risolvere i problemi del computer prima di fare clic su **Change**.

Al termine dell'aggiornamento del catalogo, è possibile ripristinare le versioni VDA precedenti delle macchine selezionando il catalogo e quindi selezionando **Undo Functional Level Change** (Annulla modifica di livello funzionale) nella barra delle azioni.

### Clonare un catalogo

Prima di clonare un catalogo, tenere presente quanto segue:

- Non è possibile modificare le impostazioni associate al sistema operativo e alla gestione della macchina. Il catalogo clonato eredita tali impostazioni dall'originale.
- Il completamento della clonazione di un catalogo può richiedere del tempo. Se necessario, selezionare **Hide progress** (Nascondi avanzamento) per eseguire la clonazione in background.
- Il catalogo clonato eredita il nome dell'originale e ha un suffisso `Copy`. È possibile modificare il nome. Vedere Rinominare un catalogo.
- Al termine della clonazione, accertarsi di assegnare il catalogo clonato a un gruppo di consegna.
- È possibile creare un catalogo vuoto mediante clonazione. Durante la clonazione del catalogo, è possibile impostare il numero di computer su zero per i cataloghi di cui è stato eseguito il provisioning con MCS e non aggiungere macchine per i cataloghi di cui non è stato eseguito il provisioning con MCS.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare un catalogo, quindi selezionare **Clone** (Clona) nella barra delle azioni.
3. Nella finestra **Clone Selected Machine Catalog** (Clona catalogo delle macchine selezionato), visualizzare le impostazioni per il catalogo clonato e configurare le impostazioni a seconda dei casi. Selezionare **Next** (Avanti) per passare alla pagina successiva.

4. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per avviare la clonazione.
5. Se necessario, selezionare **Hide progress** (Nascondi avanzamento) per eseguire la clonazione in background.

## Organizzare i cataloghi utilizzando cartelle

È possibile creare cartelle per organizzare i cataloghi per un facile accesso. Ad esempio, è possibile organizzare i cataloghi per tipo di immagine o per struttura organizzativa.

### Ruoli richiesti

Per impostazione predefinita, è necessario disporre del seguente ruolo integrato per creare e gestire le cartelle del catalogo: amministratore cloud, amministratore completo o amministratore del catalogo delle macchine. Se necessario, è possibile personalizzare i ruoli per la creazione e la gestione delle cartelle del catalogo. Per ulteriori informazioni, consultare Autorizzazioni richieste.

### Creare una cartella del catalogo

Prima di iniziare, pianificare come organizzare i cataloghi. Considerare quanto segue:

- È possibile nidificare le cartelle fino a cinque livelli di profondità (esclusa la cartella principale predefinita).
- Una cartella del catalogo può contenere cataloghi e sottocartelle.
- Tutti i nodi in **Full Configuration** (Configurazione completa) (come i **cataloghi delle macchine** e i **nodi delle applicazioni**) condividono un albero delle cartelle nel backend. Per evitare conflitti di nomi con altri nodi durante la ridenominazione o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in nodi diversi.

Per creare una cartella del catalogo, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella e quindi selezionare **Create Folder** (Crea cartella) nella barra **Actions** (Azioni).
3. Immettere un nome per la nuova cartella, quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> Se si crea una cartella in una posizione non prevista, è possibile trascinarla nella posizione corretta.

### Spostare un catalogo

È possibile spostare un catalogo tra le cartelle. I passaggi dettagliati sono i seguenti:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Visualizzare i cataloghi in base alla cartella. È anche possibile attivare **View all** (Visualizza tutto) sopra la gerarchia delle cartelle per visualizzare tutti i cataloghi contemporaneamente.
3. Fare clic con il pulsante destro del mouse su un catalogo e selezionare **Move Machine Catalog** (Sposta catalogo delle macchine).
4. Selezionare la cartella in cui si desidera spostare il catalogo e quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> È possibile trascinare un catalogo in una cartella.

### Gestire le cartelle di un catalogo

È possibile eliminare, rinominare e spostare le cartelle del catalogo.

È possibile eliminare una cartella solo se tale cartella e le relative sottocartelle non contengono cataloghi.

Per gestire una cartella, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella, quindi selezionare un'azione nella barra **Actions** (Azioni) in base alle esigenze:
   - Per rinominare la cartella, selezionare **Rename Folder** (Rinomina cartella).
   - Per eliminare la cartella, selezionare **Delete Folder** (Elimina cartella).
   - Per spostare la cartella, selezionare **Move Folder** (Sposta cartella).
3. Seguire le istruzioni sullo schermo per completare i passaggi rimanenti.

### Autorizzazioni richieste

Nella tabella seguente sono elencate le autorizzazioni necessarie per eseguire azioni sulle cartelle del catalogo.

| Azione | Autorizzazioni richieste |
| --- | --- |
| Creare cartelle del catalogo | Creare una cartella del catalogo delle macchine |
| Eliminare cartelle del catalogo | Rimuovere una cartella del catalogo delle macchine |
| Spostare le cartelle del catalogo | Spostare una cartella del catalogo delle macchine |
| Rinominare le cartelle del catalogo | Modificare una cartella del catalogo delle macchine |
| Spostare i cataloghi nelle cartelle | Modificare una cartella del catalogo delle macchine e modificare le proprietà del catalogo delle macchine |

### Configurare l'aggiornamento automatico per i VDA

> **Importante:**
>
> - Per garantire un aggiornamento senza problemi, assicurarsi di soddisfare i prerequisiti ed esaminare i problemi noti prima di aggiornare i VDA alle versioni CR o LTSR CU. Vedere Aggiornare i VDA utilizzando l'interfaccia Full Configuration.
> - Quando si aggiornano i VDA LTSR alle versioni LTSR CU (Cumulative Update), assicurarsi che la versione dei VDA Upgrade Agent in esecuzione sui VDA sia la 7.36.0.7 o una versione successiva. Per ulteriori informazioni, vedere Upgrade VDAs using the Full Configuration interface.
> - È possibile passare dal VDA CR al VDA LTSR purché si passi da una versione precedente a una versione successiva. Non è possibile passare da una versione successiva a una versione precedente perché questo è considerato un downgrade. Ad esempio, non è possibile effettuare il downgrade da 2212 CR a 2203 LTSR (qualsiasi CU), ma è possibile eseguire l'upgrade da 2112 CR a 2203 LTSR (qualsiasi CU).
> - È anche possibile aggiornare i VDA utilizzando PowerShell. Vedere Aggiornare i VDA utilizzando PowerShell.

Con questa funzionalità è possibile procedere come segue:

- Aggiornare i VDA in base al catalogo
- Modificare o annullare un aggiornamento VDA pianificato
- Configurare le impostazioni di aggiornamento VDA dopo la creazione del catalogo
- Aggiornare i VDA in base alla singola macchina

> **Nota:**
>
> - Quando si pianificano gli aggiornamenti VDA per un catalogo, possono essere aggiornati solo i VDA nel catalogo in cui è installato l'agente di aggiornamento VDA.
> - L'aggiornamento di un VDA non riesce quando la macchina è in modalità di manutenzione o quando una sessione è in esecuzione sulla macchina.

#### Tipi di macchine supportati

Questa funzionalità si applica ai seguenti tipi di macchine:

- Macchine persistenti fornite da MCS (aggiunte ad AD, aggiunte ad Azure AD e non aggiunte a un dominio). È possibile distribuirle utilizzando **Citrix Machine Creation Services** nella pagina **Machine Management** (Gestione macchine) durante la creazione del catalogo.
- Macchine con Accesso remoto al PC
- Citrix HDX Plus per macchine Windows 365
- Altre macchine persistenti di cui è stato effettuato il provisioning mediante servizi o tecnologie di provisioning non Citrix. È possibile aggiungere tali macchine a DaaS utilizzando **Other service or technology** (Altro servizio o tecnologia) nella pagina **Machine Management** (Gestione macchine) durante la creazione del catalogo.

Per ulteriori informazioni sulle opzioni **Citrix Machine Creation Services** e **Other service or technology** vedere Gestione macchine.

> **Nota:**
>
> Per quanto riguarda le macchine con provisioning effettuato da MCS, sono supportate solo le macchine statiche persistenti. Le macchine casuali non sono supportate anche se sono persistenti.

#### Aggiornare i VDA in base al catalogo

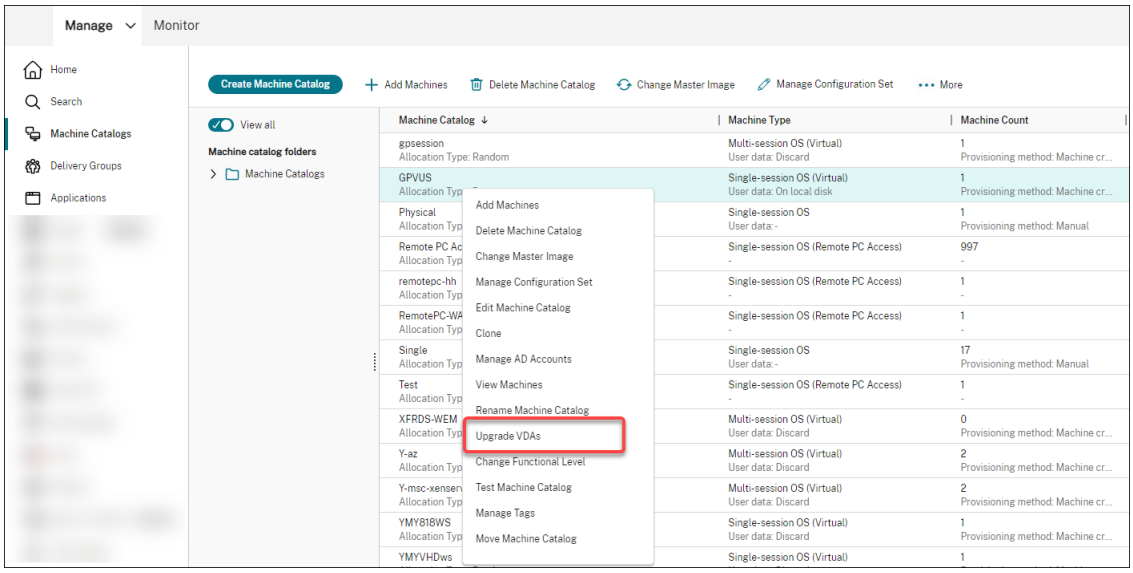
> **Nota:**
>
> Quando si pianificano gli aggiornamenti del VDA per un catalogo, tenere presente che tutte le macchine del catalogo saranno incluse nell'ambito dell'aggiornamento. Pertanto, consigliamo di eseguire il backup di quelle macchine prima di iniziare l'aggiornamento.

Dopo aver abilitato l'aggiornamento VDA per un catalogo, è possibile aggiornare immediatamente i VDA nel catalogo o pianificare gli aggiornamenti per il catalogo. Per farlo, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine).

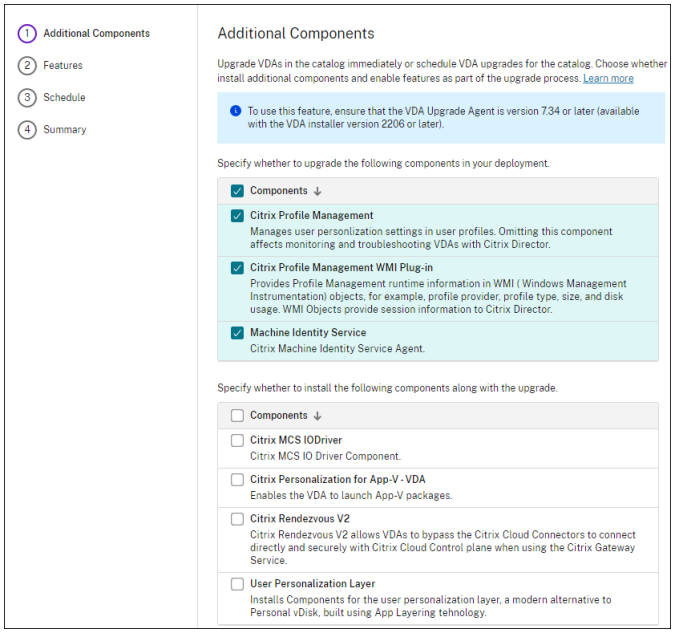
2. Selezionare il catalogo e quindi **Upgrade VDAs** (Aggiorna i VDA) nel menu contestuale o nella barra delle azioni. Fare clic con il pulsante destro del mouse per visualizzare il menu contestuale. Viene visualizzata la finestra di aggiornamento del VDA.




3. Scegliere se aggiornare i componenti aggiuntivi della propria installazione. È anche possibile scegliere di installare determinati componenti oltre all'aggiornamento. Se un componente richiede configurazione, è necessario fare clic sul pulsante **Configure** e configurare le impostazioni del componente per continuare. Dopo la configurazione, è possibile fare clic su **Edit** per modificare la configurazione.

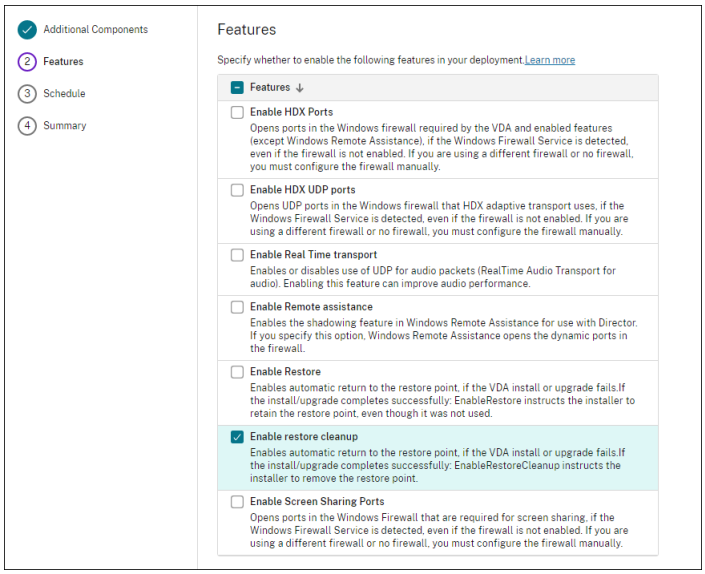
> **Importante:**
>
> - Per utilizzare la funzionalità dei componenti aggiuntivi, assicurarsi che il proprio VDA Upgrade Agent sia la versione 7.34 o successiva, che inclusa nella versione 2206 o successiva del programma di installazione del VDA.
>
> **Nota:**
>
> - Se si decide di non aggiornare un componente, il componente rimane intatto nella distribuzione.
> - Per un elenco completo dei componenti aggiuntivi, vedere Installare i VDA.




4. Fare clic su **Next** (Avanti).
5. Decidere se abilitare una o più delle funzionalità elencate. Fare clic su **Next** (Avanti).

> **Nota:**
>
> Per impostazione predefinita, la casella di controllo **Enable restore cleanup** (Abilita ripristino pulizia) è selezionata. Consigliamo di abilitare la funzione di ripristino. Con la funzionalità abilitata, viene creato un punto di ripristino del sistema prima dell'avvio dell'aggiornamento. Il punto di ripristino viene eliminato installazione del VDA completata. Per ulteriori informazioni, vedere Ripristino in caso di errore di installazione o aggiornamento.



6. Scegliere se aggiornare i VDA immediatamente o a un orario programmato.

    - Per aggiornare immediatamente i VDA, selezionare **Upgrade now** (Esegui l'upgrade ora) e quindi specificare una durata.

      Una durata è il periodo di tempo, espresso in ore, dopo il quale il servizio di aggiornamento VDA interrompe l'avvio di aggiornamenti aggiuntivi. Gli aggiornamenti in corso verranno completati. Durante questo periodo, DaaS inizia ad aggiornare i VDA quando diventano idonei (ad esempio, se non hanno più sessioni attive).

      Maggiore è il numero di VDA da aggiornare, maggiore è la durata. Consigliamo di selezionare un valore elevato (ad esempio 12 ore). Altrimenti, se il numero di VDA è elevato, potrebbero esserci ancora VDA che DaaS non è in grado di aggiornare all'interno di questa finestra.

    - Per pianificare gli aggiornamenti, selezionare **Upgrade later** (Aggiorna in seguito) e quindi specificare quando si desidera che vengano eseguiti gli aggiornamenti.

      È possibile programmare gli aggiornamenti solo per i sette giorni successivi. Gli aggiornamenti pianificati si applicano solo alle macchine attualmente presenti nel catalogo. Se si aggiungono macchine al catalogo in un secondo momento ma si desidera aggiornare anche queste, annullare l'aggiornamento pianificato e quindi ricreare una pianificazione.

7. Fare clic su **Next** (Avanti).
8. Controllare le scelte effettuate nella pagina **Summary**, quindi fare clic su **Finish** per applicare le impostazioni e uscire dalla finestra.

> **Nota:**
>
> - L'opzione **Upgrade VDAs** (Aggiorna VDA) è disponibile solo dopo aver abilitato l'aggiornamento VDA per il catalogo. Per abilitare l'aggiornamento VDA, modificare il catalogo.
> - Tutte le macchine del catalogo vengono messe in modalità di manutenzione mentre vengono implementati gli aggiornamenti. L'avvio degli aggiornamenti può richiedere fino a 30 minuti e verrà eseguito solo durante il periodo di tempo specificato.

Nel nodo **Machine Catalogs** (Cataloghi macchine), la colonna **VDA Upgrade** (Aggiornamento VDA) fornisce informazioni sull'aggiornamento VDA per il catalogo. Possono essere visualizzate le seguenti informazioni:

> **Suggerimento:**
>
> Per visualizzare la colonna **VDA Upgrade** (Aggiornamento VDA), selezionare **Columns to Display** (Colonne da visualizzare) nella barra delle azioni, selezionare **Machine Catalog > VDA Upgrade** (Catalogo delle macchine > Aggiornamento VDA), quindi fare clic su **Save** (Salva).

- **Available** (Disponibile): è disponibile una nuova versione di VDA.

- **Scheduled** (Pianificato): l'aggiornamento VDA è stato pianificato.
- **Not configured** (Non configurato): viene visualizzato quando non è stato abilitato l'aggiornamento VDA per il catalogo.
- **Up to date** (Aggiornato): i VDA del catalogo sono aggiornati.
- **Unknown** (Sconosciuto): impossibile ottenere le informazioni necessarie per l'aggiornamento del VDA. Le ragioni possibili sono molteplici:
  - Il VDA era in uso durante la finestra riservata per l'aggiornamento.
  - Il numero di aggiornamenti in corso ha raggiunto il limite massimo di 500.
  - VDA Upgrade Agent non rispondeva durante la finestra riservata per l'aggiornamento. Assicurarsi che l'agente sia in esecuzione sul VDA e sia in grado di comunicare con Citrix DaaS.
  - Impossibile eseguire i controlli di convalida dell'aggiornamento. Vedere VDA upgrade requirement.

È inoltre possibile visualizzare lo stato degli aggiornamenti VDA per un catalogo. A tale scopo, fare clic sul catalogo e quindi controllare le informazioni **VDA Upgrade State** (Stato dell'aggiornamento VDA) nella scheda **Details** (Dettagli). Possono essere visualizzate le seguenti informazioni:

- **Not scheduled** (Non pianificato): è stato abilitato l'aggiornamento VDA per il catalogo ma non è stato impostato un programma di aggiornamento.
- **Scheduled** (Pianificato): è stata creata una pianificazione di aggiornamento per il catalogo. Ad esempio, se si imposta la pianificazione in modo che inizi alle ore `09:00 PM, December 14, 2030`, le informazioni vengono visualizzate come segue: Scheduled for (Pianificato per le ore) `December 14, 2030 09:00 PM UTC`.
- **In progress** (In corso): gli aggiornamenti VDA sono iniziati.
- **Canceled** (Annullato): l'aggiornamento pianificato è stato annullato.
- **Failed** (Non riuscito): il catalogo contiene una o più macchine i cui aggiornamenti VDA non sono andati a buon fine.
- **Successful** (Operazione completata): tutti i VDA nel catalogo sono stati aggiornati correttamente.

È inoltre possibile risolvere i problemi di aggiornamento VDA con le azioni consigliate per un catalogo. Per farlo, fare clic sul catalogo e andare alla scheda **Troubleshoot** (Risoluzione dei problemi) .

Per eseguire rapidamente il drill-down dei cataloghi con uno stato di aggiornamento VDA specifico, è possibile utilizzare i filtri. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration.

Tenere presente le seguenti considerazioni:

- Il filtro **VDA Upgrade** (Aggiornamento VDA) o **VDA Upgrade State** (Stato dell'aggiornamento VDA) è disponibile per l'uso solo con i seguenti filtri: **Name** (Nome) e **Machine Catalog** (Catalogo delle macchine).

- Quando si utilizza il filtro **VDA Upgrade** (Aggiornamento VDA) o **VDA Upgrade State** (Stato aggiornamento VDA), gli**errori** e gli **avvisi** nell'angolo in alto a destra non sono più disponibili.

#### Modificare o annullare un aggiornamento VDA pianificato

Dopo aver pianificato gli aggiornamenti per un catalogo, è possibile modificare o annullare l'aggiornamento pianificato. Per farlo, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine).
2. Selezionare il catalogo e quindi **Edit Scheduled VDA Upgrade** (Modifica aggiornamento VDA pianificato) nella barra delle azioni. Viene visualizzata la finestra Edit VDA Upgrade (Modifica aggiornamento VDA), che mostra informazioni sulla versione di VDA installata e sulla versione di VDA a cui eseguire l'aggiornamento.
3. Scegliere se modificare o annullare l'aggiornamento pianificato.
    - Per annullare l'aggiornamento, fare clic su **Cancel scheduled upgrade** (Annulla aggiornamento pianificato). Ricorda: l'annullamento dell'aggiornamento pianificato non impone l'interruzione dell'aggiornamento in corso.
4. Fare clic su **Done** (Fine) per uscire dalla finestra.

#### Configurare le impostazioni di aggiornamento VDA modificando un catalogo

Dopo la creazione del catalogo, è possibile configurare le impostazioni di aggiornamento VDA modificando il catalogo. Prima di iniziare a modificare, tenere presente quanto segue:

- Verificare che tutte le macchine presenti nel catalogo si trovino sulla stessa traccia VDA (CR o LTSR). In caso contrario, alcuni aggiornamenti VDA non riusciranno. Ad esempio, se si seleziona **Latest LTSR VDA** (VDA - LTSR più recenti), gli aggiornamenti VDA CR non riusciranno.
- È possibile che siano iniziati gli aggiornamenti di alcune macchine del catalogo. Non è possibile modificare gli aggiornamenti già in corso. Gli aggiornamenti in corso continuano. Quelli che non sono ancora stati avviati eseguiranno l'aggiornamento alla versione specificata.

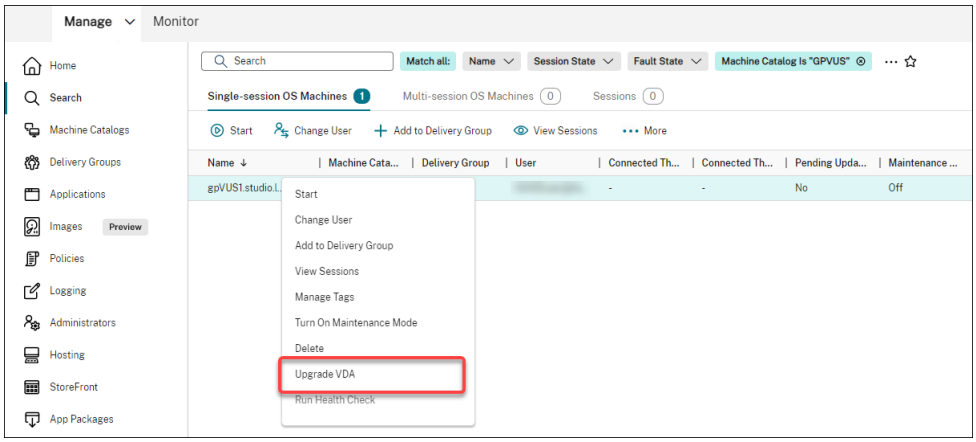
#### Aggiornare i VDA in base alla singola macchina

Dopo aver abilitato l'aggiornamento VDA per un catalogo, è possibile aggiornare i VDA del catalogo uno per uno o in batch. Per farlo, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Search** (Cerca).

2. Selezionare una o più macchine e quindi **Upgrade VDA** (Aggiorna VDA) dal menu contestuale o dalla barra delle azioni. Fare clic con il pulsante destro del mouse per visualizzare il menu contestuale.




> **Nota:**
>
> - Perché l'opzione **Upgrade VDA** (Aggiorna VDA) sia disponibile, assicurarsi di aver abilitato l'aggiornamento VDA per il catalogo in cui risiedono le macchine selezionate e che su tali macchine sia installato l'agente di aggiornamento VDA. Per abilitare l'aggiornamento VDA, modificare il catalogo.
> - Le macchine verranno messe in modalità di manutenzione durante l'implementazione degli aggiornamenti. L'avvio degli aggiornamenti può richiedere fino a 30 minuti.
> - Se la selezione contiene macchine per le quali gli aggiornamenti VDA non sono disponibili o i cui aggiornamenti sono in sospeso (pianificati, in corso o in attesa di aggiornamenti), gli aggiornamenti per quelle macchine verranno saltati.

Nel nodo **Search** (Cerca), è possibile aggiungere la colonna **VDA Upgrade** (Aggiornamento VDA). Per informazioni su come aggiungere una colonna personalizzata, consultare Personalizzare le colonne da visualizzare. La colonna è utile. Fornisce informazioni sull'aggiornamento VDA per la macchina. Possono essere visualizzate le seguenti informazioni:

- **Available** (Disponibile): è disponibile una nuova versione di VDA.
- **Scheduled** (Pianificato): l'aggiornamento VDA è stato pianificato.
- **Not configured** (Non configurato): questa opzione viene visualizzata quando non è stato abilitato l'aggiornamento VDA per la macchina.
- **Up to date** (Aggiornato): il VDA è aggiornato.
- **Unknown** (Sconosciuto): le informazioni sull'aggiornamento VDA non sono ancora disponibili.

È inoltre possibile visualizzare lo stato dell'aggiornamento VDA per una macchina. Per fare ciò, fare clic sulla macchina e quindi controllare le informazioni **VDA Upgrade State** (Stato di aggiornamento VDA) nella scheda **Details** (Dettagli). Possono essere visualizzate le seguenti informazioni:

- **Unknown** (Sconosciuto): impossibile ottenere le informazioni necessarie per l'aggiornamento del VDA. Le ragioni possibili sono molteplici:
  - Il VDA era in uso durante la finestra riservata per l'aggiornamento.
  - Il numero di aggiornamenti in corso ha raggiunto il limite massimo di 500.
  - VDA Upgrade Agent non rispondeva durante la finestra riservata per l'aggiornamento. Assicurarsi che l'agente sia in esecuzione sul VDA e sia in grado di comunicare con Citrix DaaS.
  - Impossibile eseguire i controlli di convalida dell'aggiornamento. Vedere VDA upgrade requirement.
- **Scheduled** (Pianificato): è stata impostata una pianificazione dell'aggiornamento. Ad esempio, se si imposta la pianificazione in modo che inizi alle ore `09:00 PM, December 14, 2030`, le informazioni vengono visualizzate come segue: Scheduled for (Pianificato per le ore) `December 14, 2030 09:00 PM UTC`.
- **Awaiting upgrade** (In attesa di aggiornamento): la macchina viene messa in modalità di manutenzione, in attesa dell'aggiornamento (assicurarsi che gli utenti abbiano effettuato il logout dalla sessione in modo che l'aggiornamento possa procedere).
- **In progress** (In corso): l'aggiornamento VDA è iniziato.
- **Upgrade failed** (Aggiornamento non riuscito): i tentativi di aggiornamento del VDA non sono riusciti.
- **Validation failed** (Convalida non riuscita): i tentativi di convalida delle impostazioni di aggiornamento VDA non sono riusciti.
- **Canceled** (Annullato): l'aggiornamento della macchina è stato annullato.
- **Successful** (Operazione completata): il VDA è stato aggiornato correttamente.

È inoltre possibile risolvere i problemi di aggiornamento VDA con le azioni consigliate per una macchina. Per farlo, fare clic sulla macchina e andare alla scheda **Troubleshoot** (Risoluzione dei problemi).

Per eseguire rapidamente il drill-down su macchine con uno stato di aggiornamento VDA specifico, è possibile utilizzare i filtri. Per ulteriori informazioni, vedere Utilizzare la ricerca nell'interfaccia di gestione Full Configuration. Tenere presente le seguenti considerazioni:

- Il filtro **VDA Upgrade** (Aggiornamento VDA) o **VDA Upgrade State** (Stato dell'aggiornamento VDA) è disponibile per l'uso solo con i seguenti filtri: **Name** (Nome) e **Machine Catalog** (Catalogo delle macchine).
- Quando si utilizza il filtro **VDA Upgrade** (Aggiornamento VDA) o **VDA Upgrade State** (Stato aggiornamento VDA), gli**errori** e gli **avvisi** nell'angolo in alto a destra non sono più disponibili.

**Utilizzare PowerShell per controllare lo stato di aggiornamento dei VDA e la versione VDA**

Utilizzare il comando PowerShell `Get-VusCatalog` per verificare lo stato di aggiornamento dei VDA. Supponiamo che il nome del catalogo sia `wuhanTestMC1`. È possibile digitare quanto segue nel prompt dei comandi:

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`

```
PS C:\Users\hanw> Get-VusCatalog -Name  wuhanTestMC1


CancelledUpgrades           : 0
DurationInHours             : 8
FailedUpgrades              : 0
InProgressUpgrades          : 0
LastStateChangeInUtc        : 4/22/2022 7:52:51 AM
MaxConcurrentUpgrades       : 100
Name                        : wuhanTestMC1
ProvisioningType            : MCS
ScheduledTimeInUtc          : 4/22/2022 7:20:56 AM
SecurityCheckFailedUpgrades : 0
SessionSupport              : SingleSession
StateId                     : UpgradeSuccessful
SuccessfulUpgrades          : 1
TotalMachines               : 1
Uid                         : 12
UpgradeState                : UpgradeAvailable
UpgradeType                 : CR
UpgradeVersion              : 2112.0.0.32068
Uuid                        : 339e7bce-271b-4c37-9a1c-bce287008b65
```

In questo esempio, `UpgradeState` è `UpgradeAvailable`, il che significa che l'aggiornamento VDA è abilitato per il catalogo. `StateId` è `UpgradeSuccessful`, il che significa che il catalogo è stato aggiornato correttamente a 2112.0.0.32068 (`UpgradeVersion`).

Utilizzare il comando PowerShell `Get-BrokerMachine` per ottenere la versione del VDA corrente.

```
SessionProtocol              :
SessionSecureIcaActive       :
SessionSmartAccessTags       :
SessionStartTime             :
SessionState                 :
SessionStateChangeTime       :
SessionSupport               : MultiSession
SessionType                  :
SessionUid                   :
SessionUserName              :
SessionUserSID               :
SessionsEstablished          : 0
SessionsPending              : 0
SummaryState                 : Unregistered
SupportedPowerActions        : {}
Tags                         : {}
UUID                         : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                          : 4
VMToolsState                 : NotPresent
WillShutdownAfterUse         : False
WillShutdownAfterUseReason   : None
WindowsConnectionSetting     : LogonEnabled
ZoneHealthy                  : False
ZoneName                     : My Resource Location
ZoneUid                      : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion                 : 2112.0.0.32068
AllocationType               : Static
ApplicationsInUse            : {}
AssignedClientName           :
AssignedIPAddress            :
AssignedUserSIDs             : {}
AssociatedTenantId           :
AssociatedUserFullNames      : {}
AssociatedUserNames          : {}
AssociatedUserSIDs           : {}
AssociatedUserUPNs           : {}
AzureADJoinedMode            : NotAadJoined
BrowserName                  :
Capabilities                 : {}
CatalogName                  : wuhanTestMC1
CatalogUUID                  : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                   : 12
CbpVersion                   :
ColorDepth                   :
ControllerDNSName            :
DNSName                      : wuhanVUSTest02.WHCloud.Internal
DeliveryType                 :
Description                  :
DesktopConditions            : {}
```

Utilizzare il comando PowerShell `Get-VusAvailableVdaVersion` per ottenere la versione più recente del VDA.

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion

UpgradeType Version
----------- -------
         CR 2203.0.0.33220
       LTSR 2203.0.0.33220
```

### Ripristinare disco del sistema operativo

Utilizzare il comando PowerShell `Reset-ProvVMDisk` per reimpostare il disco del sistema operativo di una macchina virtuale persistente in un catalogo di macchine creato da MCS. Attualmente, questa funzionalità è applicabile agli ambienti di virtualizzazione Azure, Citrix Hypervisor, Google Cloud, SCVMM e VMware.

Per eseguire correttamente il comando PowerShell, assicurarsi che sussistano le seguenti condizioni:

- Le VM di destinazione si trovano in un catalogo MCS persistente.
- Il catalogo macchine MCS funziona correttamente. Ciò implica che lo schema di provisioning e l'host esistono e che lo schema di provisioning contiene le voci corrette.
- L'hypervisor non è in modalità di manutenzione.
- Le VM di destinazione sono spente e in modalità manutenzione.

Effettuare le seguenti operazioni per ripristinare il disco del sistema operativo:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando asnp citrix* per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il comando PowerShell `Reset-ProvVMDisk` in uno dei seguenti modi:

    - Specificare l'elenco delle VM sotto forma di elenco separato da virgole ed eseguire il ripristino su ciascuna VM:

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
        ,"def") -OS
    <!--NeedCopy-->
    ```

    - Specificare l'elenco di VM come output dal comando `Get-ProvVM` ed eseguire il ripristino su ciascuna VM:

    ```
    (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
        "abc" -OS
    <!--NeedCopy-->
    ```

    - Specificare una singola VM per nome:

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
        -OS
    <!--NeedCopy-->
    ```

    - Creare attività di ripristino separate per ciascuna delle VM restituite dal comando `Get-ProvVM`. Questo metodo è meno efficiente perché ogni attività eseguirà gli stessi controlli ridondanti, quali il controllo della capacità dell'hypervisor e il controllo della connessione per ogni VM.

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. Viene visualizzato un prompt di conferma che elenca le VM da reimpostare insieme a un messaggio di avviso che indica che si tratta di un'operazione irreversibile. Se non si fornisce una risposta e si preme **Invio**, non vengono eseguite altre azioni.

   È possibile eseguire il comando PowerShell `-WhatIf` per stampare l'azione che eseguirebbe e uscire senza eseguirla.

   È anche possibile ignorare la richiesta di conferma utilizzando uno dei seguenti metodi:

   - Fornire il parametro `-Force`:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Force
     <!--NeedCopy-->
     ```

   - Fornire il parametro `-Confirm:$false`:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Confirm:$false
     <!--NeedCopy-->
     ```

   - Prima di eseguire `Reset-ProvVMDisk`, modificare `$ConfirmPreference` scegliendo "None":

     ```
     PS C:\Windows\system32> $ConfirmPreference='None'
     PS C:\Windows\system32> $ConfirmPreference
     None
     PS C:\Windows\system32> Reset-ProvVMDisk -
         ProvisioningSchemeName "xxx" -VMName "abc" -OS
     <!--NeedCopy-->
     ```

   > **Nota:**
   >
   > Non togliere le VM dalla modalità di manutenzione né accenderle fino al completamento del processo di ripristino.

5. Eseguire `Get-ProvTask` per ottenere lo stato delle attività restituite dal comando `Reset-ProvVMDisk`.

### Modificare le impostazioni di rete per uno schema di provisioning esistente

È possibile modificare l'impostazione di rete per uno schema di provisioning esistente in modo che le nuove macchine virtuali vengano create nella nuova sottorete. Utilizzare il parametro `-NetworkMapping` nel comando `Set-ProvScheme` per modificare l'impostazione di rete.

Per modificare l'impostazione di rete per uno schema di provisioning esistente, procedere come segue:

1. Nella finestra di PowerShell, eseguire il comando `asnp citrix*` per caricare i moduli di PowerShell.
2. Eseguire `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` per accedere al percorso di rete che si desidera modificare.
3. Assegnare una variabile alla nuova impostazione di rete. Ad esempio:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Eseguire `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Eseguire `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` per verificare la nuova impostazione di rete per lo schema di provisioning esistente.

### Gestire il set di configurazione per un catalogo

Prima di iniziare, assicurarsi di aver configurato la distribuzione del servizio WEM. Per ulteriori informazioni, vedere Introduzione al servizio Workspace Environment Management.

> **Nota:**
>
> Per impostazione predefinita, se si ricopre il ruolo di Cloud Administrator (Amministratore cloud), Full Access Administrator (Amministratore ad accesso completo) o Machine Catalog Administrator (Amministratore del catalogo di macchine), è possibile gestire i set di configurazione per i cataloghi. Se necessario, è possibile consentire ai ruoli di gestire i set di configurazione concedendo loro l'autorizzazione **Manage configuration sets** (Gestione set di configurazione).

#### Associare un catalogo a un set di configurazione

> **Importante:**
>
> Se le istanze di Citrix DaaS e del servizio WEM non risiedono nella stessa regione, non è possibile associare un catalogo a un set di configurazione. In tal caso, eseguire la migrazione del servizio WEM nella stessa area geografica di Citrix DaaS.

Per associare un catalogo a un set di configurazione, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine).
2. Selezionare il catalogo delle macchine e quindi **Manage configuration set** (Gestisci set di configurazione) nella barra delle azioni. Viene visualizzata la finestra **Manage configuration set** (Gestisci set di configurazione).
3. Selezionare un set di configurazione WEM a cui si desidera associare il catalogo.

   > **Nota:**
   >
   > Se il set di configurazione selezionato non contiene impostazioni relative alla configurazione di base di WEM, viene visualizzata l'opzione **Apply basic settings to configuration set** (Applica impostazioni di base al set di configurazione). Si consiglia di selezionare l'opzione per applicare le impostazioni di base al set di configurazione.

4. Fare clic su **Save** (Salva) per salvare la modifica.

#### Passare a un diverso set di configurazione

Per passare a un set di configurazione diverso per un catalogo, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine).
2. Selezionare il catalogo delle macchine e quindi **Manage configuration set** (Gestisci set di configurazione) nella barra delle azioni. Viene visualizzata la finestra **Manage configuration set** (Gestisci set di configurazione).
3. Selezionare un set di configurazione WEM diverso a cui si desidera associare il catalogo.
4. Fare clic su **Save** (Salva) per salvare la modifica.

#### Dissociare un catalogo dal set di configurazione

Per dissociare un catalogo dal set di configurazione, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine).
2. Selezionare il catalogo delle macchine e quindi **Manage configuration set** (Gestisci set di configurazione) nella barra delle azioni. Viene visualizzata la finestra **Manage configuration set** (Gestisci set di configurazione).
3. Fare clic sull'icona X sul lato destro del set di configurazione selezionato.
4. Fare clic su **Save** (Salva) per salvare la modifica.

### Aggiungere descrizioni a un'immagine

È possibile aggiungere descrizioni informative sulle modifiche correlate agli aggiornamenti delle immagini per i cataloghi delle macchine. Utilizzare questa funzionalità per aggiungere una descrizione durante la creazione di un catalogo o quando si aggiorna un'immagine master esistente per un catalogo. È inoltre possibile visualizzare le informazioni per ogni immagine master del catalogo. Questa funzionalità è utile per gli amministratori che desiderano aggiungere etichette descrittive durante l'aggiornamento di un'immagine master utilizzata da un catalogo, ad esempio *Office 365 installato*. Utilizzare i seguenti comandi per aggiungere o visualizzare le descrizioni delle immagini:

- `NewProvScheme`. Un nuovo parametro `masterImageNote` consente di aggiungere una nota a un'immagine. Ad esempio:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName
    XenHu -IdentityPoolName idPool1 -MasterImageVM XDHyp:\HostingUnits\
    XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365 installed"
<!--NeedCopy-->
```

- `Publish-ProvMasterVMImage`. Utilizzare questo parametro per pubblicare la nota. Ad esempio:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -
    MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.
    snapshot -MasterImageNote "Visual Studio 2019 installed"
<!--NeedCopy-->
```

- `Get-ProvSchemeMasterVMImageHistory`. Visualizzare le informazioni per ogni immagine. Ad esempio:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

ProvisioningSchemeName : MyScheme

MasterImageVM : /Base.vm/base.snapshot

Date : 17/05/2021 09:27:50

MasterImageNote : Office365 installed
<!--NeedCopy-->
```

### Riprovare a creare il catalogo

> **Nota:**
>
> Questa funzione si applica solo ai cataloghi MCS.

I cataloghi non riusciti sono contrassegnati da un'icona di errore. Per visualizzare i dettagli, passare alla scheda **Troubleshoot** (Risoluzione problemi) di ogni catalogo. Prima di riprovare a creare il catalogo, tenere presenti le seguenti considerazioni:

- Controllare prima le informazioni sulla risoluzione dei problemi e risolvere i problemi. Le informazioni descrivono i problemi rilevati e forniscono consigli per risolverli.
- Non è possibile modificare le impostazioni associate al sistema operativo e alla gestione della macchina. Il catalogo eredita tali impostazioni dall'originale.
- Il completamento della creazione può richiedere del tempo. Se necessario, selezionare **Hide progress** (Nascondi avanzamento) per eseguire la creazione in background.

Per riprovare a creare un catalogo, procedere come segue:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare il catalogo e passare alla relativa scheda **Troubleshoot**.
3. Fate clic sul collegamento ipertestuale Retry per riprovare a creare il catalogo.
4. Nella procedura guidata visualizzata, modificare le impostazioni se necessario. Se non è necessario apportare modifiche, è possibile andare direttamente alla pagina **Summary** (Riepilogo).
5. Al termine, selezionare **Finish** per iniziare la creazione.

### Convertire un catalogo di macchine non basato su profili macchina in un catalogo di macchine basato su profili macchina

È possibile utilizzare una VM, una specifica di modello (nel caso di Azure) o un modello di avvio (nel caso di AWS) come input del profilo macchina per convertire un catalogo di macchine non basate su profili macchina in un catalogo di macchine basate su profilo macchina. Le nuove macchine virtuali aggiunte al catalogo prendono i valori delle proprietà dal profilo macchina.

> **Nota:**
>
> Non è possibile modificare un catalogo macchine basato su profili macchina esistente per farlo diventare non basato su profili macchina.

A questo scopo:

1. Creare un catalogo di macchine persistente o non persistente con macchine virtuali e senza un profilo macchina.
2. Aprire la finestra di **PowerShell**.

3. Eseguire il comando `Set-ProvScheme` per applicare i valori delle proprietà tratti dal profilo della macchina alle nuove VM aggiunte al catalogo macchine. Ad esempio:

   - Nel caso di Azure:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
      -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
      machineprofile.folder<ResourceGroupName><TemplateSpecName
      ><VersionName>
   <!--NeedCopy-->
   ```

   - Nel caso di AWS:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
      -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
      template>.launchtemplate<launch-template-version>.
      launchtemplateversion"
   <!--NeedCopy-->
   ```

## Ripristinare le informazioni sull'identità degli account computer attivi

È possibile reimpostare le informazioni sull'identità degli account computer attivi che presentano problemi correlati all'identità. È possibile scegliere di reimpostare solo la password della macchina e le chiavi di attendibilità o ripristinare tutta la configurazione del disco di identità. Questa implementazione è applicabile ai cataloghi di macchine di MCS sia persistenti che non persistenti.

> **Nota:**
>
> Attualmente, la funzionalità è supportata solo per gli ambienti di virtualizzazione Azure e VMware.

### Condizioni

Assicurarsi di aver soddisfatto le condizioni seguenti per reimpostare correttamente il disco di identità:

- Spegnere la VM e impostarla in modalità manutenzione
- Non includere il parametro -OS nel comando PowerShell

### Reimpostare il disco di identità

Per reimpostare il disco di identità:

1. Aprire la finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.

3. Reimpostare le informazioni sull'identità.

   - Per reimpostare solo la password della macchina e le chiavi di attendibilità, eseguire i seguenti comandi nel seguente ordine:

     ```
     1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
           PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
           $password -Target IdentityInfo
     2  <!--NeedCopy-->
     ```

     La descrizione dei parametri utilizzati nel comando è la seguente:

     - `IdentityAccountName`: nome dell'account di identità che deve essere riparato.
     - `PrivilegedUserName`: account utente con autorizzazione di scrittura sul provider di identità (AD o AzureAD).
     - `PrivilegedUserPassword`: password relativa a PrivilegedUserName.
     - `Target`: obiettivo dell'azione di riparazione. Può essere IdentityInfo per riparare la password dell'account e/o la chiave di fiducia e UserCertificate per riparare gli attributi del certificato utente delle identità delle macchine aggiunte ad AzureAD ibride.

     ```
     1  Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
           > -Identity -ResetIdentityInfo
     2  <!--NeedCopy-->
     ```

     Il parametro `ResetIdentityInfo` reimposta quanto segue:

     - Password e chiavi di fiducia: se la VM è aggiunta al dominio AD (solo per Citrix DaaS)
     - Solo chiavi di fiducia: se la VM non è aggiunta al dominio AD (solo per Citrix DaaS)
     - Solo password: se la VM è aggiunta al dominio AD (solo per Citrix Virtual Apps and Desktops)

   - Per ripristinare tutta la configurazione del disco di identità, eseguire i seguenti comandi nel seguente ordine:

     ```
     1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
           PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
           $password -Target IdentityInfo
     2  <!--NeedCopy-->
     ```

     ```
     1  Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
           -Identity
     2  <!--NeedCopy-->
     ```

4. Digitare **y** per confermare l'azione. È anche possibile saltare la richiesta di conferma utilizzando il parametro `-Force`. Ad esempio:

   ```
   1  Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
         Identity -Force
   2  <!--NeedCopy-->
   ```

5. Eseguire `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` per verificare l'impostazione aggiornata del disco di identità. Gli attributi del disco di identità (ad esempio `IdentityDiskId`) devono essere aggiornati. `StorageId` e `IdentityDiskIndex` non devono cambiare.

### Modificare la configurazione della cache su un catalogo di macchine esistente

Dopo aver creato un catalogo non persistente con MCSIO abilitato, è possibile utilizzare il comando Set-ProvScheme per modificare i seguenti parametri:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Questa funzionalità è attualmente applicabile a:

- Ambienti GCP e Microsoft Azure e
- un catalogo non persistente con MCSIO abilitato

#### Requisiti

I requisiti per modificare la configurazione della cache sono:

- Aggiornamento alla versione più recente di VDA (2308 o successiva).
- Aver abilitato il parametro `UseWriteBackCache` per il catalogo macchine esistente. Utilizzare `New-ProvScheme` per creare un catalogo di macchine con `UseWriteBackCache` abilitato. Ad esempio:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
    HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
<!--NeedCopy-->
```

#### Modificare la configurazione della cache

Eseguire il comando Set-ProvScheme. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
    ProvisioningSchemeName -WriteBackCacheDisk32 -
    WriteBackCacheMemorySize 128
<!--NeedCopy-->
```

> **Nota:**
>
> - Il valore di `WriteBackCacheDiskSize` deve essere superiore a zero perché è richiesto almeno 1 GB di spazio di archiviazione sul disco cache.
> - Il valore di `WriteBackCacheMemorySize` deve essere inferiore alla dimensione della memoria del catalogo di macchine.
> - Queste modifiche riguardano solo le nuove VM aggiunte al catalogo dopo la modifica. Le VM esistenti non sono interessate da queste modifiche.

### Risoluzione dei problemi

- Per le macchine con stato `Power State Unknown`, vedere CTX131267 per istruzioni.
- Per correggere le macchine virtuali che mostrano continuamente uno stato di alimentazione sconosciuto, vedere Come correggere le macchine virtuali che mostrano continuamente uno stato di alimentazione sconosciuto.
- Se un Cloud Connector non funziona correttamente, le operazioni di provisioning MCS (come gli aggiornamenti del catalogo) richiedono molto più tempo del solito e le prestazioni della console di gestione si riducono in modo significativo.

### Passaggi successivi

Per informazioni sulla gestione di cataloghi di hypervisor specifici, vedere:

- Gestire un catalogo di AWS
- Gestire un catalogo di Citrix Hypervisor
- Gestisci un catalogo di Google Cloud Platform
- Gestire un catalogo di Microsoft Azure
- Gestire un catalogo di Microsoft System Center Virtual Machine Manager
- Gestire un catalogo di VMware

## Gestire un catalogo di AWS

December 18, 2023

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud AWS.

> **Nota:**
>
> Prima di gestire un catalogo di AWS, è necessario completare la creazione di un catalogo di AWS. Vedere Creare un catalogo di AWS.

### Rimuovere i tag

Quando si crea un catalogo o una macchina virtuale, vengono creati tag sulle risorse seguenti:

- Macchina virtuale
- Volume del disco principale
- Volume del disco di identità
- NIC
- Immagine del disco principale (AMI)
- Modello di avvio
- Snapshot dell'AMI o del disco principale

È possibile rimuovere macchine virtuali e cataloghi di macchine dal database Citrix e rimuovere i tag. È possibile usare:

- `Remove-ProvVM` con il parametro `ForgetVM` per rimuovere macchine virtuali e tag da una singola macchina virtuale o un elenco di macchine virtuali da un catalogo di macchine.
- `Remove-ProvScheme` con il parametro `ForgetVM` per rimuovere un catalogo di macchine dal database Citrix e risorse da un catalogo di macchine.

Questa funzionalità è applicabile solo alle macchine virtuali persistenti.

A questo scopo:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Sbloccare le macchine virtuali prima di rimuoverle. Ad esempio:

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
<!--NeedCopy-->
```

4. Eseguire uno dei seguenti comandi per rimuovere le macchine virtuali, il catalogo di macchine e i tag dalle risorse.
   - Eseguire `Remove-ProvVM` con `ForgetVM` per rimuovere le macchine virtuali dal database Citrix e i tag dalle macchine virtuali. Ad esempio:

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
   >" -ForgetVM
<!--NeedCopy-->
```

- Eseguire `Remove-ProvScheme` per rimuovere il catalogo di macchine dal database Citrix e le risorse da un catalogo di macchine. Ad esempio:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
    ForgetVM
<!--NeedCopy-->
```

5. Verificare che la macchina virtuale sia stata rimossa dal Delivery Controller e non dall'hypervisor.

   a) Eseguire `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"`. Questo non deve restituire nulla.

   b) Andare alla console AWS EC2. È necessario visualizzare le macchine virtuali, ma i tag ora sono stati rimossi. I tag delle seguenti risorse vengono rimossi:

      - Macchina virtuale
      - Volume del disco principale
      - Volume del disco di identità
      - NIC

6. Se si rimuove il catalogo delle macchine, verificare che il catalogo sia stato rimosso dal Delivery Controller.

   a) Eseguire `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. Questo deve restituire un errore.

   b) Verificare nella console AWS EC2 che le seguenti risorse siano rimosse.

      - Immagine del disco principale (AMI)
      - Modello di avvio
      - Snapshot dell'AMI o del disco principale

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse sulla piattaforma AWS. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Disco ID | "Name": "VMName_IdentityDisk"<br>"XdConfig": "XdProvisioned=true"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

| Nome della risorsa | Tag |
| --- | --- |
| Immagine | “XdConfig”: “XdProvisioned=true”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| NIC | “Description”: “XD Nic”<br>“XdConfig”: “XdProvisioned=true”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Disco del sistema operativo | “Name”: “VMName_rootDisk”<br>“XdConfig”: “XdProvisioned=true”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>[quando AwsCaptureInstanceProperties = true]<br>“Citrix Resource”: “”<br>[quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true]<br>“CitrixOperationalResource”: “” |
| PrepVM | “Name”: “Preparation - CatalogName - xxxxxxxxxx”<br>“XdConfig”: “XdProvisioned=true”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>[quando AwsCaptureInstanceProperties = true]<br>“Citrix Resource”: “”<br>[quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true]<br>“CitrixOperationalResource”: “” |
| Snapshot pubblicata | “XdConfig”: “XdProvisioned=true” |
| Modello | Se non si tratta di una snapshot per l’AMI Volume Worker, allora “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>[quando AwsCaptureInstanceProperties = true]<br>“XdConfig”: “XdProvisioned=true”<br>[quando AwsCaptureInstanceProperties = true]<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

| Nome della risorsa | Tag |
| --- | --- |
| Macchina virtuale nel catalogo | [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| AMI Volume Worker | “XdConfig”: “XdProvisioned=true” |
| Bootstraper Volume Worker | “Name”: “XenDesktop Temp” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “” |
| Istanza di Volume Worker | “Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true” |

## Ulteriori informazioni

- Connessioni e risorse
- Connessione ad AWS
- Creare cataloghi di macchine
- Creare un catalogo di AWS
- Gestire i cataloghi delle macchine

# Gestire un catalogo di Citrix Hypervisor

December 21, 2022

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione Citrix Hypervisor.

> **Nota:**
>
> Prima di gestire un catalogo di Citrix Hypervisor, è necessario completare la creazione di un catalogo Citrix Hypervisor. Vedere Creare un catalogo di Citrix Hypervisor.

## Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse sulla piattaforma Citrix Hypervisor. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Copia del disco su ogni rete o posizione di archiviazione locale (solo on-premise) | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco ID | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco del sistema operativo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| PrepVM | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig": "XdProvisioned=true" |
| Disco base pubblicato | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Macchina virtuale nel catalogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig": "XdProvisioned=true" |
| Disco WBC | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

## Ulteriori informazioni

- Connessioni e risorse

- Connessione a Citrix Hypervisor
- Creare cataloghi di macchine
- Creare un catalogo di Citrix Hypervisor
- Gestire i cataloghi delle macchine

## Gestisci un catalogo di Google Cloud Platform

July 6, 2023

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti cloud di Google.

> **Nota:**
>
> Prima di gestire un catalogo di Google Cloud Platform, è necessario completare la creazione di un catalogo di Google Cloud Platform. Vedere Creare un catalogo di Google Cloud Platform.

### Aggiungere macchine a un catalogo

Per aggiungere macchine a un catalogo, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare il catalogo delle macchine a cui si desidera aggiungere macchine.
3. Selezionare **Add Machines** (Aggiungi macchine) nella barra delle azioni.
4. Nella pagina **Virtual Machines** (Macchine virtuali), specificare il numero di macchine che si desidera aggiungere e quindi selezionare **Next** (Avanti).
5. Nella pagina **Machine Identities** (Identità macchine), selezionare un account di Active Directory e quindi selezionare **Next** (Avanti).
6. Nella pagina **Domain Credentials** (Credenziali di dominio), selezionare **Enter credentials** (Immetti le credenziali), digitare il nome utente e la password, selezionare **Save** (Salva), quindi selezionare **Next** (Avanti).
7. Nella pagina **Summary** (Riepilogo), confermare le informazioni e quindi selezionare **Finish** (Fine).

### Aggiornare le macchine

Questa funzionalità può essere utile nei casi in cui si desidera aggiornare l'immagine master o il livello funzionale minimo.

Per aggiornare le macchine, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare il catalogo delle macchine che contiene le macchine che si desidera aggiornare.
3. Selezionare **Change Master Image** (Cambia immagine master) nella barra delle azioni.
4. Nella pagina **Master Image** (Immagine master), selezionare una macchina virtuale e il livello funzionale minimo per il catalogo, quindi selezionare **Next** (Avanti).
5. Nella pagina **Rollout Strategy** (Strategia di implementazione), specificare quando si desidera aggiornare le macchine e quindi selezionare **Next** (Avanti).
6. Nella pagina **Summary** (Riepilogo), confermare le informazioni e quindi selezionare **Finish** (Fine).

Per eseguire il rollback di un aggiornamento di una macchina, effettuare le seguenti operazioni:

> **Importante:**
>
> Non rinominare, eliminare o spostare le immagini master, altrimenti non è possibile eseguire il rollback dell'aggiornamento.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
2. Selezionare il catalogo delle macchine in cui si desidera eseguire il rollback dell'aggiornamento della macchina.
3. Seleziona **Roll Back Master Image** (Esegui il rollback dell'aggiornamento della macchina) nella barra delle azioni.
4. Nella pagina **Overview** (Panoramica), confermare le informazioni e quindi selezionare **Next** (Avanti).
5. Nella pagina **Rollout Strategy** (Strategia di implementazione), configurare la strategia di implementazione e quindi selezionare **Next** (Avanti).
6. Nella pagina **Summary** (Riepilogo), confermare le informazioni e quindi selezionare **Finish** (Fine).

### Gestione dell'alimentazione

Citrix DaaS consente la gestione dell'alimentazione delle macchine Google Cloud. Utilizzare il nodo **Search** (Cerca) nel riquadro di navigazione per individuare la macchina di cui si desidera gestire l'alimentazione. Sono disponibili le seguenti azioni per l'alimentazione:

- Delete (Elimina)
- Start (Avvia)
- Restart (Riavvia)
- Force Restart (Forza riavvio)
- Shut Down (Arresta)
- Force Shutdown (Imponi arresto)
- Add to Delivery Group (Aggiungi al gruppo di consegna)
- Manage Tags (Gestisci tag)
- Turn On Maintenance Mode (Attiva la modalità di manutenzione)

È anche possibile gestire l'alimentazione delle macchine Google Cloud utilizzando Autoscale (Scalabilità automatica). A tale scopo, aggiungere le macchine Google Cloud a un gruppo di consegna e abilitare la scalabilità automatica per tale gruppo. Per ulteriori informazioni sulla scalabilità automatica, consultare Scalabilità automatica.

### Aggiornare i computer sottoposti a provisioning utilizzando PowerShell

Il comando `Set-ProvScheme` modifica lo schema di provisioning. Tuttavia, non influisce sulle macchine esistenti. Utilizzando il comando `Set-ProvVMUpdateTimeWindow` di PowerShell, è ora possibile applicare lo schema di provisioning corrente a una macchina o a un set di macchine esistente persistente o non persistente. Attualmente, in GCP, l'aggiornamento delle proprietà supportato da questa funzionalità è il profilo del computer.

È possibile aggiornare:

- Una singola macchina virtuale
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un ID di schema di provisioning
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un nome di uno schema di provisioning

Per aggiornare le macchine virtuali esistenti:

1. Verificare la configurazione delle macchine esistenti. Ad esempio,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aggiornare lo schema di provisioning. Ad esempio,

```
`Set-ProvScheme  –ProvisioningSchemeName "my-catalog"  –
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofileinstance.vm"
<!--NeedCopy-->
```

3. Verifica se la proprietà corrente della VM corrisponde allo schema di provisioning corrente e se c'è qualche azione di aggiornamento in sospeso sulla VM. Ad esempio,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

   È anche possibile trovare macchine con una versione particolare. Ad esempio,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
   VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Aggiornare le macchine esistenti.

   - Per aggiornare tutte le macchine esistenti:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

   - Per aggiornare un elenco di macchine specifiche:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

   - Per aggiornare le macchine in base all'output di `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

   > **Nota:**
   >
   > - `StartsNow` indica che l'ora di inizio pianificata è l'ora corrente.
   > - `DurationInMinutes` con un numero negativo (ad esempio -1) indica che non vi è alcun limite superiore nella finestra oraria della pianificazione.

5. Trovare i computer con un aggiornamento pianificato. Ad esempio,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. Riavviare le macchine. Alla successiva accensione, le modifiche delle proprietà vengono applicate ai computer esistenti. È possibile verificare lo stato aggiornato utilizzando il seguente comando:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

### Modificare le proprietà personalizzate relative al disco di un catalogo esistente

È possibile modificare le seguenti proprietà personalizzate relative al disco di un catalogo esistente e delle VM esistenti del catalogo:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Nota:**
>
> - La proprietà `StorageType` è per il disco del sistema operativo
> - La proprietà `PersistOsDisk` può essere impostata solo per il catalogo non persistente con la cache di write-back abilitata

Questa implementazione consente di selezionare diversi tipi di archiviazione per i diversi dischi anche dopo aver creato un catalogo e quindi equilibra i costi associati ai diversi tipi di archiviazione.

Per fare ciò, utilizzare i comandi PowerShell `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`:

1. Aprire una finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Eseguire `Get-ProvVM -VMName <VM name>` per ottenere le proprietà personalizzate.
4. Modificare la stringa delle proprietà personalizzate.
    a) Copiare le proprietà personalizzate su un file di Blocco note e modificare le proprietà personalizzate.

b) Nella finestra di **PowerShell**, incollare le proprietà personalizzate modificate dal file di Blocco note e assegnare una variabile alle proprietà personalizzate modificate. Ad esempio:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Aggiornare il catalogo esistente. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
   CustomProperties $cp
<!--NeedCopy-->
```

6. Aggiornare le macchine virtuali esistenti. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
   VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Riavviare le macchine virtuali. Alla successiva accensione, le modifiche delle proprietà personalizzate vengono applicate alle macchine virtuali esistenti.

### Proteggersi dall'eliminazione accidentale di macchine

Citrix DaaS consente di proteggere le risorse MCS su Google Cloud per impedirne l'eliminazione accidentale. Configurare la macchina virtuale di cui è stato eseguito il provisioning impostando il flag `deletionProtection` su TRUE.

Per impostazione predefinita, le macchine virtuali di cui è stato eseguito il provisioning tramite MCS o il plug-in Google Cloud vengono create con InstanceProtection abilitato. L'implementazione è applicabile sia ai cataloghi persistenti che a quelli non persistenti. I cataloghi non persistenti vengono aggiornati quando le istanze vengono ricreate dal modello. Per le macchine persistenti esistenti, è possibile impostare il flag nella console di Google Cloud. Per ulteriori informazioni sull'impostazione del flag, consultare il sito della documentazione di Google. Le nuove macchine aggiunte ai cataloghi persistenti vengono create con `deletionProtection` abilitato.

Se si tenta di eliminare un'istanza di una macchina virtuale per la quale è stato impostato il flag `deletionProtection`, la richiesta non riesce. Tuttavia, se viene concessa l'autorizzazione `compute.instances.setDeletionProtection` o il ruolo IAM **Compute Admin**, è possibile reimpostare il flag per consentire l'eliminazione della risorsa.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse sulla piattaforma GCP. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Disco ID | "CitrixResource": "internal"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Immagine | "CitrixResource": "internal"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco del sistema operativo | "CitrixResource": "internal"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| PrepVM | "CitrixResource": "internal"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Snapshot pubblicata | "CitrixResource": "internal" |
| Bucket di archiviazione | "CitrixResource": "internal" |
| Modello | "CitrixResource": "internal" |
| Macchina virtuale nel catalogo | "CitrixResource": "internal"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

| Nome della risorsa | Tag |
| --- | --- |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. Il plug-in aggiunge anche questa etichetta per le macchine virtuali di cui è stato eseguito il provisioning tramite MCS: “citrix-provisioning-scheme-id”: “provSchemeId”. È possibile utilizzare questa etichetta per filtrare in base al catalogo nella console di GCP. |
| Disco WBC | “CitrixResource”: “internal”<br>CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

> **Nota:**
>
> Una macchina virtuale non è visibile nell’inventario Citrix se viene aggiunto un tag **CitrixResource** per identificarla come risorsa creata da MCS. È possibile rimuovere o rinominare il tag per renderlo visibile.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione agli ambienti cloud di Google
- Creare cataloghi di macchine
- Creare un catalogo di Google Cloud Platform
- Gestire i cataloghi delle macchine

## Gestire un catalogo di HPE Moonshot (anteprima)

December 5, 2023

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni riguardano dettagli specifici del catalogo HPE Moonshot.

> **Nota:**
>
> Prima di gestire un catalogo di HPE Moonshot, è necessario completare la creazione di un catalogo di HPE Moonshot.

### Gestione dell'alimentazione

Citrix DaaS consente di gestire l'alimentazione delle macchine HPE Moonshot. Utilizzare il nodo **Search** (Cerca) nel riquadro di navigazione per individuare la macchina di cui si desidera gestire l'alimentazione. Sono disponibili le seguenti azioni per l'alimentazione:

- Start (Avvia)
- Shut Down (Arresta)
- Force Shutdown (Imponi arresto)
- Restart (Riavvia)
- Reset (Reimposta)

> **Nota:**
>
> Le azioni di alimentazione **Suspend** (Sospendi) e **Resume** (Riprendi) non sono supportate.

### Ulteriori informazioni

- Creare e gestire le connessioni
- Connessione a HPE Moonshot
- Creare cataloghi di macchine
- Creare un catalogo di macchine di HPE Moonshot
- Gestire i cataloghi delle macchine

## Gestire un catalogo di Microsoft Azure

December 18, 2023

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Microsoft Azure Resource Manager.

> **Nota:**
>
> Prima di gestire un catalogo di Microsoft Azure, è necessario completare la creazione di un cata-

> logo di Microsoft Azure. Vedere Creare un catalogo di Microsoft Azure.

### Portare il tipo di archiviazione a un livello inferiore quando una VM viene arrestata

È possibile risparmiare sui costi di archiviazione cambiando il tipo di archiviazione di un disco gestito portandolo a un livello inferiore quando si spegne una VM. Per fare ciò, utilizzare la proprietà personalizzata `StorageTypeAtShutdown`.

Il tipo di archiviazione del disco passa a un livello inferiore (come specificato nella proprietà personalizzata `StorageTypeAtShutdown`) quando si arresta la macchina virtuale. Dopo aver acceso la VM, il tipo di archiviazione torna all'originale (come specificato nella proprietà personalizzata `StorageType` o nella proprietà personalizzata `WBCDiskStorageType`).

> **Importante:**
>
> - Il disco non esiste finché la VM non viene accesa almeno una volta. Pertanto, non è possibile modificare il tipo di archiviazione quando si accende la VM per la prima volta.
> - L'avvio di una macchina virtuale potrebbe richiedere un po'più di tempo dopo aver modificato il tipo di archiviazione portandolo a un livello inferiore.

#### Requisiti

- Applicabile a un disco gestito. Ciò implica impostare la proprietà personalizzata `UseManagedDisks` su true.
- Applicabile a un catalogo persistente e non persistente con un disco del sistema operativo persistente. Ciò implica impostare la proprietà personalizzata `persistOsDisk` su true.
- Applicabile a un catalogo non persistente con un disco WBC persistente. Ciò implica impostare la proprietà personalizzata `persistWBC` su true.

#### Restrizione

- Come da Microsoft, è possibile cambiare il tipo di disco solo due volte al giorno. Vedere questo documento Microsoft. Nel caso di Citrix, l'aggiornamento di `StorageType` avviene ogni volta che c'è un'azione Start o Deallocate per la VM. Pertanto, limitare il numero di azioni di alimentazione per VM a due volte al giorno. Ad esempio, un'azione di alimentazione al mattino per avviare la VM e una alla sera per deallocare la VM.

#### Cambiare il tipo di archiviazione portandolo a un livello inferiore

Prima di procedere con i passaggi, vedere Requisiti e Restrizioni.

1. Aggiungere la proprietà personalizzata `StorageTypeAtShutdown`, impostare il valore su Standard_LRS (HDD) e creare un catalogo utilizzando `New-ProvScheme`. Per informazioni sulla creazione di un catalogo utilizzando PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Nota:**
   >
   > Se `StorageTypeAtShutdown` ha un valore diverso da vuoto o Standard_LRS (HDD), l'operazione ha esito negativo.

   Esempio di impostazione di proprietà personalizzate durante la creazione di un catalogo persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS“ />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties> ’
<!--NeedCopy-->
```

   Esempio di impostazione di proprietà personalizzate durante la creazione di un catalogo non persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
```

```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties> '
<!--NeedCopy-->
```

> **Nota:**
>
> Quando si utilizza un profilo macchina, la proprietà personalizzata ha la precedenza sulla proprietà definita in `MachineProfile`.

2. Arrestare la macchina virtuale e controllare il tipo di archiviazione della macchina virtuale nel portale di Azure. Il tipo di archiviazione del disco passa a un livello inferiore, come specificato nella proprietà personalizzata `StorageTypeAtShutdown`.
3. Accendere la VM. Il tipo di archiviazione del disco torna al tipo di archiviazione indicato in:
   - Proprietà personalizzata `StorageType` per il disco del sistema operativo
   - Proprietà personalizzata `WBCDiskStorageType` per il disco WBC solo se specificata in `CustomProperties`. Altrimenti, torna al tipo di archiviazione indicato in `StorageType`.

### Applicare `StorageTypeAtShutdown` a un catalogo esistente

Prima di procedere con i passaggi, vedere Requisiti e Restrizioni.

Utilizzare `Set-ProvScheme` per applicare `StorageTypeAtShutdown`alle nuove macchine virtuali aggiunte a un catalogo esistente.

Esempio di impostazione di proprietà personalizzate durante l'aggiunta di una macchina virtuale a un catalogo esistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
```

```
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties> '

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

### Cambiare il tipo di archiviazione delle VM esistenti a un livello inferiore al momento dell'arresto

Prima di procedere con i passaggi, vedere Requisiti e Restrizioni.

È possibile risparmiare sui costi di archiviazione modificando il tipo di archiviazione delle macchine virtuali esistenti su un livello inferiore quando le macchine virtuali vengono arrestate.

Per modificare il tipo di archiviazione delle macchine esistenti in un catalogo portandolo a un livello inferiore quando le macchine virtuali vengono spente:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Modificare la stringa delle proprietà personalizzate.

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
       Value="Standard_LRS" />
   </CustomProperties>'
   <!--NeedCopy-->
   ```

5. Aggiornare lo schema di provisioning del catalogo esistente. L'aggiornamento si applica alle nuove VM aggiunte dopo l'esecuzione di `Set-ProvScheme`.

   ```
   Set-ProvScheme -ProvisioningSchemeName $CatalogName -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

6. Aggiornare le VM esistenti per abilitarle `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Alla successiva accensione delle macchine, la proprietà `StorageTypeAtShutdown` delle macchine viene aggiornata. Il tipo di archiviazione cambia al successivo arresto.
8. Eseguire il comando seguente per visualizzare il valore `StorageTypeAtShutdown` di ciascuna macchina virtuale di un catalogo:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $\_.VMName; $storageTypeAtShutdown = ($\_.CustomVmData
       | ConvertFrom-Json).StorageTypeAtShutdown.
      DiskStorageAccountType; return New-Object psobject -Property
      @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
      $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

### Aggiornare le macchine di cui è stato eseguito il provisioning allo stato corrente dello schema di provisioning

Il comando `Set-ProvScheme` modifica lo schema di provisioning. Tuttavia, non influisce sulle macchine esistenti. Utilizzando il comando `Set-ProvVMUpdateTimeWindow` di PowerShell, è possibile applicare lo schema di provisioning corrente a una macchina o a un set di macchine esistente persistente o non persistente. È inoltre possibile pianificare una fascia oraria per gli aggiornamenti della configurazione dei computer esistenti forniti da MCS. Eventuali accensioni o riavvii durante la fascia oraria pianificata applicano un aggiornamento pianificato dello schema di provisioning a una macchina. Attualmente, in Azure, è possibile aggiornare `ServiceOffering`, `MachineProfile` e le seguenti proprietà personalizzate:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Nota:**
>
> - È possibile aggiornare `StorageType`, `WBCDiskStorageType` e le proprietà personalizzate `IdentityDiskStorageType` di un catalogo solo usando il disco gestito in ambienti Azure.
> - Se si esegue `Set-ProvVMUpdateTimeWindow` due volte, ha effetto il comando più recente.

È possibile aggiornare:

- Una singola macchina virtuale
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un ID di schema di provisioning
- Un elenco di macchine virtuali specifiche o di tutte le macchine virtuali esistenti associate a un nome di schema di provisioning (nome del catalogo macchine)

Dopo aver apportato le seguenti modifiche allo schema di provisioning, l'istanza della macchina virtuale viene ricreata per i cataloghi persistenti in Azure:

- Cambiare `MachineProfile`
- Rimuovere `LicenseType`
- Rimuovere `DedicatedHostGroupId`

> **Nota:**
>
> Il disco del sistema operativo delle macchine esistenti, insieme a tutti i relativi dati, rimane invariato e al disco viene collegata una nuova VM.

Prima di aggiornare le macchine virtuali esistenti:

1. Verificare la configurazione delle macchine esistenti. Ad esempio,

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Aggiornare lo schema di provisioning. Ad esempio,

   - Con la VM come input del profilo macchina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   virtual-machine>.vm"
<!--NeedCopy-->
```

   - Con le specifiche di modello come input del profilo macchina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    template-spec>.templatespec<template-spec-version>.
    templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

- Con solo questa offerta di servizi:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

3. Verifica se la proprietà corrente della VM corrisponde allo schema di provisioning corrente e se c'è qualche azione di aggiornamento in sospeso sulla VM. Ad esempio,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

È anche possibile trovare macchine con una versione particolare. Ad esempio,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

Per richiedere gli aggiornamenti delle macchine esistenti da applicare al prossimo riavvio:

1. Eseguire i seguenti comandi per aggiornare i computer esistenti e far applicare gli aggiornamenti al successivo riavvio.

- Per aggiornare tutte le macchine esistenti: Ad esempio,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Per aggiornare un elenco di macchine specifiche. Ad esempio,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
    -1
<!--NeedCopy-->
```

- Per aggiornare le macchine in base all'output di Get-ProvVM. Ad esempio,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
```

```
<!--NeedCopy-->
```

**Nota:**

- `StartsNow` indica che l'ora di inizio pianificata è l'ora corrente.
- `DurationInMinutes` con un numero negativo (ad esempio -1) indica che non vi è alcun limite superiore nella finestra oraria della pianificazione.

2. Trovare i computer con un aggiornamento pianificato. Ad esempio,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. Riavviare le macchine. Alla successiva accensione, le modifiche delle proprietà vengono applicate ai computer esistenti. È possibile verificare lo stato aggiornato utilizzando il comando che segue. Ad esempio,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Per pianificare l'aggiornamento di una VM alle impostazioni di provisioning più recenti la prossima volta che verrà avviata nella finestra temporale pianificata:

1. Eseguire i seguenti comandi:

   - Per pianificare un aggiornamento con l'ora di inizio come ora corrente:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

   - Per programmare un aggiornamento durante un fine settimana:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1" -StartTimeInUTC "10/15/2022
    9:00am" -DurationInMinutes (New-TimeSpan -Days 2).
    TotalMinutes
<!--NeedCopy-->
```

**Nota:**

- `VMName` è opzionale. Se non specificato, l'aggiornamento è pianificato per l'intero catalogo.
- Invece di `StartTimeInUTC`, utilizzare `StartsNow` per indicare che l'ora di inizio della pianificazione è l'ora corrente.
- `DurationInMinutes` è opzionale. L'impostazione predefinita è 120 minuti. Un nu-

> mero negativo (ad esempio -1) non indica alcun limite superiore nella finestra oraria della pianificazione.

2. Controllare lo stato dell'aggiornamento.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

3. Accendere la VM. Se si accende il computer dopo la fascia oraria pianificata, l'aggiornamento della configurazione non viene applicato. Se si accende la macchina entro la fascia oraria pianificata,

   - Se la macchina è spenta e
     - non si accende la macchina, l'aggiornamento della configurazione non viene applicato
     - si accende la macchina, viene applicato l'aggiornamento della configurazione
   - Se la macchina è accesa e
     - non si riavvia la macchina, l'aggiornamento della configurazione non viene applicato
     - si riavvia la macchina, viene applicato l'aggiornamento della configurazione

Per annullare l'aggiornamento della configurazione:

È anche possibile annullare un aggiornamento della configurazione di una singola macchina virtuale, di più macchine virtuali o di un intero catalogo. Per annullare un aggiornamento della configurazione:

1. Eseguire `Clear-ProvVMUpdateTimeWindow`. Ad esempio:

   - Per annullare l'aggiornamento della configurazione pianificato per una singola macchina virtuale:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName " my-
    catalog " -VMName " vm1 "
<!--NeedCopy-->
```

   - Per annullare l'aggiornamento della configurazione pianificato per più macchine virtuali:

```
 Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
     catalog" -VMName "vm1","vm2"
<!--NeedCopy-->
```

> **Nota:**
>
> Le macchine virtuali devono appartenere allo stesso catalogo.

### Aggiornare le proprietà delle singole macchine virtuali

È possibile aggiornare le proprietà delle singole macchine virtuali incluse in un catalogo di macchine MCS persistente utilizzando il comando PowerShell `Set-ProvVM`. Tuttavia, gli aggiornamenti non vengono applicati immediatamente. È necessario impostare la finestra temporale utilizzando il comando PowerShell `Set-ProvVMUpdateTimeWindow` per applicare gli aggiornamenti.

Questa implementazione consente di gestire le singole macchine virtuali in modo efficiente senza aggiornare l'intero catalogo di macchine. Attualmente, questa funzionalità è applicabile solo all'ambiente Azure.

Attualmente, le proprietà che è possibile aggiornare sono:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Utilizzando questa funzionalità, è possibile:

- Aggiornare le proprietà di una macchina virtuale
- Conservare le proprietà aggiornate di una macchina virtuale dopo l'aggiornamento del catalogo delle macchine
- Ripristinare gli aggiornamenti di configurazione applicati a una macchina virtuale

Prima di aggiornare le proprietà di una macchina virtuale:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Verificare la configurazione del catalogo di macchine esistente. Ad esempio:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. Verificare la configurazione della macchina virtuale a cui si desidera applicare gli aggiornamenti. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

#### Aggiornare le proprietà di una macchina virtuale

Effettuare le seguenti operazioni per aggiornare le proprietà su una macchina virtuale:

1. Disattivare la macchina virtuale a cui si intende applicare gli aggiornamenti.

2. Aggiornare le proprietà della macchina virtuale. Ad esempio, se si desidera aggiornare la proprietà personalizzata del tipo di archiviazione (`StorageType`) della macchina virtuale, eseguire i comandi seguenti:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

È possibile aggiornare contemporaneamente le proprietà di due macchine virtuali appartenenti a un catalogo di macchine. Ad esempio:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

> **Nota:**
>
> Gli aggiornamenti non vengono applicati immediatamente.

3. Ottenere l'elenco delle proprietà specificate per l'aggiornamento e la versione di configurazione. Ad esempio:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

Controllare il valore della proprietà di `Version` e le proprietà da aggiornare (in questo caso, `StorageType`).

4. Controllare la versione della configurazione. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Controllare il valore della proprietà di `ProvVMConfigurationVersion`. L'aggiornamento non è ancora stato applicato. La VM è ancora nella vecchia configurazione.

5. Richiedere un aggiornamento pianificato. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

Per ulteriori informazioni, vedere Aggiornare le macchine di cui è stato eseguito il provisioning allo stato corrente dello schema di provisioning.

> **Nota:**
>
> Viene inoltre applicato qualsiasi aggiornamento dello schema di provisioning in sospeso.

6. Riavviare la macchina virtuale. Ad esempio:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. Controllare la versione della configurazione. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Controllare il valore della proprietà di `ProvVMConfigurationVersion`. L'aggiornamento viene ora applicato. La VM ora ha la nuova configurazione.

8. Per applicare ulteriori aggiornamenti della configurazione alla macchina virtuale, arrestare la macchina virtuale e ripetere i passaggi.

### Conservare le proprietà aggiornate di una macchina virtuale dopo l'aggiornamento del catalogo delle macchine

Effettuare le seguenti operazioni per mantenere le proprietà aggiornate su una macchina virtuale:

1. Disattivare la macchina virtuale a cui si intende applicare gli aggiornamenti.
2. Aggiornare il catalogo delle macchine. Ad esempio, se si desidera modificare la dimensione della macchina virtuale (`ServiceOffering`) e il tipo di archiviazione (`StorageType`), eseguire i comandi seguenti:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
<!--NeedCopy-->
```

3. Ottenere i dettagli di configurazione del catalogo di macchine. Ad esempio:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

   Ora `ProvisioningSchemeVersion` è incrementato di uno. Vengono inoltre aggiornate le dimensioni e il tipo di archiviazione della VM.

4. Aggiornare le proprietà della macchina virtuale. Ad esempio, fornire un profilo macchina alla macchina virtuale.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```

> **Nota:**
>
> L'input del profilo macchina ha un tag e una dimensione di VM diversa (`ServiceOffering`) specificata.

5. Ottenere l'elenco delle proprietà che la macchina virtuale avrà dopo aver unito gli aggiornamenti di configurazione effettuati sulla macchina virtuale con gli aggiornamenti del catalogo delle macchine. Ad esempio:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

> **Nota:**
>
> Qualsiasi aggiornamento avvenuto sulla macchina virtuale sovrascriverà gli aggiornamenti effettuati sul catalogo delle macchine.

6. Richiedere un aggiornamento pianificato per la macchina virtuale. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Riavviare la macchina virtuale. Ad esempio:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

   La macchina virtuale mantiene le proprie dimensioni aggiornate derivate dal profilo macchina. I valori dei tag specificati nel profilo macchina vengono applicati anche alla macchina virtuale. Tuttavia, il tipo di archiviazione deriva dallo schema di provisioning più recente.

8. Ottenere la versione di configurazione della VM. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   `ProvisioningSchemeVersion` e `ProvVMConfigurationVersion` ora mostrano la versione più recente.

**Ripristinare gli aggiornamenti di configurazione applicati a una macchina virtuale**

1. Dopo aver applicato gli aggiornamenti a una macchina virtuale, arrestare la macchina virtuale.
2. Eseguire il comando seguente per rimuovere gli aggiornamenti applicati alla macchina virtuale. Ad esempio:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

3. Richiedere un aggiornamento pianificato per la macchina virtuale. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Riavviare la macchina virtuale. Ad esempio:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Controllare la versione di configurazione della VM. Ad esempio:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Il valore `ProvVMConfigurationVersion` è ora la versione di configurazione del catalogo macchine.

## Recuperare informazioni per le macchine virtuali di Azure, le snapshot, il disco del sistema operativo e la definizione delle immagini della raccolta

È possibile visualizzare informazioni per una macchina virtuale di Azure, inclusi il disco e il tipo del sistema operativo, la snapshot e la definizione delle immagini della raccolta. Queste informazioni vengono visualizzate per le risorse sull'immagine master quando viene assegnato un catalogo delle macchine. Utilizzare questa funzionalità per visualizzare e selezionare un'immagine Linux o Windows. Una proprietà PowerShell, `TemplateIsWindowsTemplate`, è stata aggiunta al parametro `AdditionDatafield`. Questo campo contiene informazioni specifiche di Azure: tipo di macchina virtuale, disco del sistema operativo, informazioni sulle immagini della raccolta e informazioni sul tipo di sistema operativo. L'impostazione di `TemplateIsWindowsTemplate` su **True** indica che il tipo di sistema operativo è Windows; l'impostazione di `TemplateIsWindowsTemplate` su **False** indica che il tipo di sistema operativo è Linux.

> **Suggerimento:**
>
> Le informazioni visualizzate dalla proprietà PowerShell `TemplateIsWindowsTemplate` derivano dall'API di Azure. A volte, questo campo potrebbe essere vuoto. Ad esempio, una snapshot di un disco di dati non contiene il campo `TemplateIsWindowsTemplate` perché il tipo di sistema operativo non può essere recuperato da una snapshot.

Ad esempio, impostare il parametro `AdditionData` della macchina virtuale di Azure su **True** per il tipo di sistema operativo Windows utilizzando PowerShell:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

### Recuperare informazioni sui nomi delle regioni per macchine virtuali di Azure, dischi gestiti, snapshot, Azure VHD e modelli ARM

È possibile visualizzare informazioni sul nome della regione per una macchina virtuale di Azure, dischi gestiti, snapshot, Azure VHD e modelli ARM. Queste informazioni vengono visualizzate per le risorse sull'immagine master quando viene assegnato un catalogo delle macchine. Una proprietà PowerShell denominata `RegionName` visualizza le informazioni sul nome della regione quando si esegue il comando PowerShell con il parametro `AdditionalData`.

Ad esempio, utilizzare il seguente comando PowerShell per ottenere informazioni su una macchina virtuale in Azure.

```
PS C:\Windows\system32> (get-item XDHyp:\HostingUnits\myAzureNetwork\
    image.folder\hu-dev-testing-rg.resourcegroup\hu-dev-tsvda.vm).
    AdditionalData
Key Value
HardDiskSizeGB 127
ResourceGroupName HU-DEV-TESTING-RG
RegionName East US
TemplateIsWindowsTemplate True
LicenseType
ServiceOfferingDescription Standard_B2ms
ServiceOfferingMemory 8192
```

```
ServiceOfferingCores 2
SupportedMachineGenerations Gen1,Gen2
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SecurityType
SecureBootEnabled
VTpmEnabled
<!--NeedCopy-->
```

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse sulla piattaforma Azure. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Disco ID | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Immagine | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| NIC | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Disco del sistema operativo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| PrepVM | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Snapshot pubblicata | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Gruppo di risorse | "CitrixResource": "Internal" CitrixSchemaVersion: 2.0 "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Account di archiviazione | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

| Nome della risorsa | Tag |
| --- | --- |
| Macchina virtuale nel catalogo | “CitrixResource”: “Internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “Internal” |
| Disco WBC | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “Internal” |

> **Nota:**
>
> Una macchina virtuale non è visibile nell’inventario Citrix se viene aggiunto un tag **CitrixResource** per identificarla come risorsa creata da MCS. È possibile rimuovere o rinominare il tag per renderlo visibile.

### Rimuovere i tag

Quando si crea un catalogo o una macchina virtuale, vengono creati tag sulle risorse seguenti:

- Gruppo di risorse
- Macchina virtuale
- Disco del sistema operativo
- Disco di identità
- Interfaccia di rete
- Account di archiviazione

È possibile rimuovere macchine virtuali e cataloghi di macchine dal database Citrix e rimuovere i tag. È possibile usare:

- `Remove-ProvVM` con il parametro `ForgetVM` per rimuovere macchine virtuali e tag da una singola macchina virtuale o un elenco di macchine virtuali da un catalogo di macchine.
- `Remove-ProvScheme` con il parametro `ForgetVM` per rimuovere un catalogo di macchine dal database Citrix e tag da un intero catalogo di macchine.

Questa funzionalità è applicabile solo alle macchine virtuali persistenti.

A questo scopo:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.

3. Eseguire `Remove-ProvVM` per eliminare le VM dal database Citrix e i tag dalle VM.
   Ad esempio:

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
<!--NeedCopy-->
```

4. Eseguire `Remove-ProvScheme` per eliminare il catalogo macchine dal database Citrix e i tag dai cataloghi di macchine. Ad esempio:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
<!--NeedCopy-->
```

> **Nota:**
>
> Dopo aver utilizzato il parametro `ForgetVM` in `Remove-ProvScheme`, MCS elimina tutte le snapshot, inclusa la snapshot del disco di base, se lo schema di provisioning è presente in Bring your own resource group (BYORG) o nel gruppo di risorse gestito da Citrix.

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a Microsoft Azure
- Creare cataloghi di macchine
- Creare un catalogo di Microsoft Azure
- Gestire i cataloghi delle macchine

## Gestire un catalogo di Microsoft System Center Virtual Machine Manager

December 21, 2022

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti di virtualizzazione Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Prima di gestire un catalogo di VMM, è necessario completare la creazione di un catalogo di VMM. Vedere Creare un catalogo di Microsoft System Center Virtual Machine Manager.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse sulla piattaforma SCVMM. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
| --- | --- |
| Preparare una macchina virtuale | Stringa tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>Immissione della proprietà personalizzata: "XdConfig:"XdProvisioned=True" |
| Macchina virtuale nel catalogo | Stringa tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>Immissione della proprietà personalizzata: "XdConfig:"XdProvisioned=True" |

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a Microsoft System Center Virtual Machine Manager
- Creare cataloghi di macchine
- Creare un catalogo di Microsoft System Center Virtual Machine Manager
- Gestire i cataloghi delle macchine

## Gestire un catalogo di VMware

December 21, 2022

In Gestire i cataloghi delle macchine sono descritte le procedure guidate per la gestione di un catalogo di macchine. Le seguenti informazioni coprono i dettagli specifici degli ambienti di virtualizzazione VMware.

> **Nota:**
>
> Prima di gestire un catalogo di VMware, è necessario completare la creazione di un catalogo di VMware. Vedere Creare un catalogo di VMware.

### Aggiornare l'ID della cartella di un catalogo di macchine

È possibile aggiornare l'ID della cartella di un catalogo di macchine MCS specificando `FolderId` nelle proprietà personalizzate del comando `Set-ProvScheme`. Le macchine virtuali create dopo l'aggiornamento dell'ID della cartella vengono create con questo nuovo ID della cartella. Se questa proprietà non è specificata in `CustomProperties`, le macchine virtuali vengono create nella cartella in cui si trova l'immagine master.

Eseguire la procedura seguente per aggiornare l'ID cartella di un catalogo di macchine.

1. Aprire un browser Web e immettere l'URL del **Web Client vSphere**.
2. Inserire le credenziali e fare clic su **Login** (Accedi).
3. Creare una cartella di posizionamento delle macchine virtuali in **vSphere Web Client**.
4. Aprire una finestra di PowerShell.
5. Eseguire **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
6. Specificare `FolderID` nella casella `CustomProperties` di `Set-ProvScheme`. In questo esempio, il valore dell'ID della cartella è `group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
     f630687372" -CustomProperties "<CustomProperties xmlns=""http
     ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
     http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
     ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
     CustomProperties>"
2 <!--NeedCopy-->
```

7. Aggiungere una macchina virtuale al catalogo delle macchine utilizzando Studio.
8. Controllare la nuova macchina virtuale su vSphere Web Client. La nuova macchina virtuale viene creata nella nuova cartella.

#### Trovare l'ID della cartella in vSphere

Accedere al MOB su qualsiasi sistema server ESXi o vCenter per trovare l'ID della cartella delle VM.

Il MOB (Managed Object Browser) è un'applicazione server basata sul Web disponibile integrata in tutti i sistemi server ESX/ESXi e vCenter. Questa utility vSphere consente di visualizzare informazioni dettagliate su oggetti come VM, datastore e pool di risorse.

1. Aprire un browser Web e immettere `http://x.x.x.x/mob`, dove x.x.x.x è l'indirizzo IP del vCenter Server o dell'host ESX/ESXi. Ad esempio, https://10.60.4.70/mob.
2. Nella pagina **Home** di MOB, fare clic sul valore del **contenuto** della proprietà.
3. Fare clic sul valore di **rootFolder**.

4. Fare clic sul valore di **childEntity**.
5. Fare clic sul valore di **vmFolder**.
6. L'ID della cartella si trova nel valore di **childEntity**.

### Identificare le risorse create da MCS

Di seguito sono riportati i tag che MCS aggiunge alle risorse sulla piattaforma VMware. I tag nella tabella sono rappresentati come "key":"value".

| Nome della risorsa | Tag |
|---|---|
| Preparare una macchina virtuale | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |
| Macchina virtuale nel catalogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |

### Ulteriori informazioni

- Connessioni e risorse
- Connessione a VMware
- Creare cataloghi di macchine
- Creare un catalogo di VMware
- Gestire i cataloghi delle macchine

## Gestione dell'alimentazione

December 5, 2023

Con Citrix DaaS, è possibile gestire l'alimentazione delle VM con provisioning eseguito con MCS su vari hypervisor e servizi cloud supportati. La gestione dell'alimentazione offre:

- Esperienza utente ottimale
- Gestione dei costi e risparmio energetico

Le azioni relative all'alimentazione disponibili sono:

- Start (Avvia)

- Shut down
- Restart (Riavvia)
- Suspend (Sospendi)
- Resume (Riprendi)
- Force Restart (Forza riavvio)
- Force Shutdown (Forza arresto)

> **Nota:**
>
> - In una macchina virtuale non persistente, il ciclo di alimentazione (spegnimento/avvio e riavvio) comporta il ripristino del disco del sistema operativo.
> - Le funzionalità e i comportamenti di gestione dell'alimentazione sono diversi nei diversi hypervisor o servizi cloud.

L'articolo illustra le principali funzionalità di gestione dell'alimentazione associate a determinati hypervisor supportati.

- Gestire l'alimentazione delle VM di AWS
- Gestire l'alimentazione delle VM di Azure

## Gestire l'alimentazione delle VM di AWS

December 5, 2023

Per informazioni sulle autorizzazioni richieste, vedere Informazioni sulle autorizzazioni AWS.

### Ibernazione delle istanze

Il processo di ibernazione memorizza lo stato in memoria dell'istanza, insieme ai relativi indirizzi IP privati ed elastici, consentendole di riprendere esattamente da dove era stata interrotta.

Quando a un'istanza viene richiesto di ibernarsi, scrive lo stato in memoria in un file che si trova nel volume EBS principale e quindi si arresta automaticamente. Un volume Amazon EBS è un dispositivo di archiviazione durevole a livello di blocco che è possibile collegare alle proprie istanze. Dopo aver collegato un volume a un'istanza, è possibile utilizzarlo come si farebbe con un disco rigido fisico. Crittografare il volume EBS principale dell'istanza. La crittografia garantisce una protezione adeguata dei dati sensibili quando vengono copiati dalla memoria al volume EBS. Per informazioni sulla crittografia EBS, vedere Crittografia Amazon EBS.

Di seguito sono elencate le limitazioni dell'ibernazione dell'istanza supportata:

- È supportata una memoria di istanza (RAM) di un massimo di 150 GB
- La modalità di avvio UEFI non è supportata
- Le unità SSD per uso generico e le unità SSD Provisioned IOPS sono supportate solo come tipi di volume EBS.

Di seguito è riportata la capacità di connessione host a livello di hypervisor.

- Hypervisor con funzionalità di sospensione: VMware, Citrix Hypervisor, Hyper-V e GCP
- Hypervisor non compatibili con la sospensione: Nutanix, Azure e AWS

> **Nota:**
>
> - Tutte le funzionalità di sospensione e ibernazione sono denominate sospensione.
> - Per AWS, la funzionalità di sospensione è supportata a livello di macchina ma non a livello di hypervisor.

#### Creare macchine virtuali compatibili con l'ibernazione

Per creare macchine virtuali compatibili con l'ibernazione:

1. Creare una connessione host. Vedere Connessione ad AWS.
2. Avviare un'istanza con EBS principale crittografato e la proprietà **Stop-Hibernate** abilitata. Per ulteriori informazioni su come avviare l'istanza, crittografare il volume EBS principale e abilitare l'ibernazione, vedere https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/. Utilizzare questa istanza come immagine principale per creare un'AMI.
3. Preparare l'immagine principale:
   a) Installare un VDA sull'immagine master. Citrix consiglia di installare la versione più recente per consentire l'accesso alle funzionalità più recenti. La mancata installazione di un VDA nell'immagine master causa l'esito negativo della creazione del catalogo. Per ulteriori informazioni su come installare un VDA, vedere Installare i VDA.
   b) Aggiungere l'immagine master al dominio di cui sono membri le applicazioni e i desktop. Assicurarsi che l'immagine master sia disponibile sull'host in cui vengono create le macchine.
4. Creare un'AMI da quell'istanza. Per informazioni sulla creazione di un'AMI da un'istanza, vedere Creazione AMI da un'istanza Amazon EC2.
5. Creare un catalogo di macchine usando il comando `New-ProvScheme`. Impostare la proprietà personalizzata `AwsCaptureInstanceProperties` su **True**. Per informazioni sull'attivazione delle proprietà delle istanze AWS nell'interfaccia Full Configuration, vedere Applicare le proprietà delle istanze AWS e assegnare tag alle risorse operative nell'interfaccia Full Configuration.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
<!--NeedCopy-->
```

Per informazioni sulla creazione di un catalogo di macchine utilizzando i comandi di PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/.

Le macchine virtuali che possono essere ibernate vengono create se:

- Si seleziona un'AMI creata da un'immagine master con la proprietà **Stop-Hibernate** abilitata.
- La macchina virtuale master è aggiunta al dominio e ha il VDA installato.
- Si seleziona la dimensione corretta della macchina virtuale (offerta di servizi) in grado di gestire l'ibernazione.

Il comando **New-ProvScheme** ha esito negativo con un messaggio di errore appropriato se:

- La macchina virtuale master è abilitata all'ibernazione ma l'offerta di servizi non è in grado di gestire l'ibernazione.
- Se la macchina virtuale master non fa parte del dominio e non ha alcun VDA installato.

#### Stato di ibernazione delle offerte di servizi e dell'AMI

Per ottenere lo stato di ibernazione delle offerte di servizi e dell'AMI (modelli), eseguire i seguenti comandi:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

#### Aggiornare l'offerta di servizi di uno schema di provisioning esistente che supporta l'ibernazione

1. Eseguire il comando `Set-ProvScheme`. Ad esempio,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <
    String>
<!--NeedCopy-->
```

Viene visualizzato un messaggio di eccezione se l'offerta di servizi non è compatibile.

#### Creare un catalogo di macchine con supporto dell'ibernazione

Quando si creano cataloghi di macchine, è possibile utilizzare un profilo macchina che supporti l'ibernazione.

1. Nella procedura guidata di creazione del catalogo, seguire le istruzioni fino alla selezione del profilo macchina.
2. Nella pagina **Machine Template** (Modello di macchina), fare clic su **Select a machine profile** (Selezionare un profilo macchina) e selezionare un profilo macchina.
3. Nella pagina **Virtual Machine**, (Macchina virtuale) fare clic sull'icona **Edit** (Modifica) e selezionare una VM.

   > **Nota:**
   >
   > Se il profilo macchina è abilitato per l'ibernazione, il sistema visualizza solo le VM che possono essere ibernate.

4. Seguire le istruzioni sullo schermo per completare tutte le impostazioni. La pagina **Summary** (Riepilogo) mostra lo stato di ibernazione del catalogo.

   > **Nota:**
   >
   > Nel campo di modifica del catalogo di macchine, quando si cambia il profilo macchina passando a un profilo abilitato all'ibernazione, viene chiesto di riconfigurare le macchine virtuali di conseguenza.

#### Aggiornare il catalogo delle macchine che supporta l'ibernazione

Se si tenta di aggiornare un catalogo macchine esistente con un catalogo macchine che non supporta l'ibernazione, l'aggiornamento non riesce e viene visualizzato un messaggio di errore appropriato.

#### Gestione dell'alimentazione delle macchine virtuali ibernate

È possibile eseguire le seguenti operazioni di gestione dell'alimentazione sulle macchine virtuali ibernate:

1. Sospendere la VM dallo stato di esecuzione.
2. Ripristinare la VM dallo stato sospeso.
3. Riavviare la VM dallo stato sospeso.

Per visualizzare le opzioni di gestione dell'alimentazione, nell'interfaccia **Manage > Full Configuration**, fare clic con il pulsante destro del mouse sulle VM ibernate.

È anche possibile visualizzare lo stato di alimentazione come **Suspending** (Sospensione in corso) e **Suspended** (Sospeso) per ogni VM in base alle operazioni di alimentazione eseguite sulle VM.

## Gestire l'alimentazione delle VM di Azure

December 5, 2023

Per informazioni sulle autorizzazioni richieste, vedere Autorizzazioni Azure richieste.

### Provisioning on demand di Azure

Con il provisioning on demand di Azure, le macchine virtuali vengono create solo quando Citrix Virtual Apps and Desktops avvia un'azione di accensione, dopo il completamento del provisioning.

Quando si utilizza MCS per creare cataloghi delle macchine in Azure Resource Manager, la funzionalità di provisioning on demand di Azure:

- Riduce i costi di archiviazione
- Velocizza la creazione di cataloghi

Quando si crea un catalogo MCS, nel portale di Azure sono visualizzati i gruppi di sicurezza di rete, le interfacce di rete, le immagini di base e i dischi di identità presenti nei gruppi di risorse.

Il portale di Azure non mostra una macchina virtuale finché Citrix Virtual Apps and Desktops non avvia un'azione di accensione per tale macchina. Quindi, lo stato della macchina virtuale nell'interfaccia Full Configuration diventa **On** (Accesa). Esistono due tipi di macchine con le seguenti differenze:

- Per una macchina in pool, il disco del sistema operativo e la cache write-back esistono solo quando esiste la macchina virtuale. Quando si arresta una macchina in pool nella console, la macchina virtuale non è visibile nel portale di Azure. Si ottiene un notevole risparmio sui costi di archiviazione se si spengono regolarmente le macchine (ad esempio, al di fuori dell'orario di lavoro).
- Per una macchina dedicata, il disco del sistema operativo viene creato la prima volta che la macchina virtuale viene accesa. La macchina virtuale presente nel portale di Azure rimane in archivio fino a quando l'identità della macchina non viene eliminata. Quando si arresta una macchina dedicata nella console, la macchina virtuale è ancora visibile nel portale di Azure.

### Conservazione di una macchina virtuale di cui è stato eseguito il provisioning durante il ciclo di alimentazione

Scegliere se conservare una macchina virtuale di cui è stato eseguito il provisioning durante il ciclo di alimentazione. Utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. Questo parametro supporta una proprietà aggiuntiva, `PersistVm`, utilizzata per determinare se una macchina virtuale di cui è stato eseguito il provisioning persiste durante il ciclo di alimentazione. Impostare la proprietà `PersistVm` su **true** per fare in modo che una macchina virtuale persista quando è spenta oppure impostare la proprietà su **false** per assicurare che la macchina virtuale non venga preservata quando è spenta.

> **Nota:**
>
> La proprietà `PersistVm` si applica solo a uno schema di provisioning con le proprietà `CleanOnBoot` e `UseWriteBackCache` abilitato. Se la proprietà `PersistVm` non è specificata per le macchine virtuali non persistenti, vengono eliminate dall'ambiente Azure quando sono spente.

Nell'esempio seguente, il parametro `New-ProvScheme CustomProperties` imposta la proprietà `PersistVm`su **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
   resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

Nell'esempio seguente, il parametro `New-ProvScheme CustomProperties` conserva la cache di write-back impostando `PersistVM` su **true**:

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
```

```
        UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
        StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
        Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
        false`" /><Property xsi:type=`"StringProperty`" Name=`"
        PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
        StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
        type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
        resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
        LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
 -HostingUnitName "demo"
 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"
 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
    resourcegroup\demo-snapshot.snapshot"
 -NetworkMapping @ {
 "0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
    .virtualprivatecloud\default.network" }

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
 -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -UseWriteBackCache
 -WriteBackCacheDiskSize 127
 -WriteBackCacheMemorySize 256
 <!--NeedCopy-->
```

> **Suggerimento:**
>
> La proprietà `PersistVm` determina se conservare una macchina virtuale di cui è stato eseguito il provisioning. La proprietà `PersistOsdisk` determina se mantenere il disco del sistema operativo. Per preservare una macchina virtuale di cui è stato eseguito il provisioning, conservare innanzitutto il disco del sistema operativo. Non è possibile eliminare il disco del sistema operativo senza prima eliminare la macchina virtuale. È possibile utilizzare la proprietà `PersistOsdisk` senza specificare il parametro`PersistVm`.

### Personalizzare il comportamento di accensione in caso di mancata riuscita della modifica del tipo di archiviazione

All'accensione, il tipo di archiviazione di un disco gestito potrebbe non riuscire a passare al tipo desiderato a causa di un errore in Azure. In questi scenari, la VM rimarrebbe disattivata e si riceverebbe un messaggio di errore. Tuttavia, è possibile scegliere di accendere la VM anche quando non può essere ripristinato il tipo di archiviazione configurato oppure scegliere di mantenere spenta la VM.

- Se si configura la proprietà personalizzata `FailSafeStorageType` come **true** (impostazione predefinita) o non la si specifica nei comandi `New-ProvScheme` o `Set-ProvScheme`:

  - All'accensione, la VM si accende con il tipo di archiviazione errato.
  - All'arresto, la VM rimane spenta con il tipo di archiviazione errato.

- Se si configura la proprietà personalizzata `FailSafeStorageType` come **false** nei comandi `New-ProvScheme` o `Set-ProvScheme`:

  - All'accensione, la VM rimane spenta con il tipo di archiviazione errato.
  - All'arresto, la VM rimane spenta con il tipo di archiviazione errato.

Per creare un catalogo di macchine:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Creare un pool di identità se non è già stato creato.
4. Aggiungere la proprietà personalizzata in `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
    \abc.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
     resourcegroup\abc-vnet.virtualprivatecloud\default.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
    serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
     Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. Creare il catalogo di macchine. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Per aggiornare un catalogo di macchine esistente in modo da includere la proprietà personalizzata `FailSafeStorageType`. Questo aggiornamento non influisce sulle macchine virtuali esistenti.

1. Aggiornare la proprietà personalizzata nel comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
    Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
    `" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"false`" />
</CustomProperties>"
<!--NeedCopy-->
```

Per applicare la modifica effettuata in Set-ProvScheme alle macchine virtuali esistenti, eseguire il comando `Request-ProvVMUpdate`.

1. Eseguire il comando Request-ProvVMUpdate. Ad esempio:

```
Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <
    List-Of-Vm-Names>
<!--NeedCopy-->
```

2. Riavviare le macchine virtuali.

### Creare macchine virtuali compatibili con l'ibernazione (anteprima)

Negli ambienti Azure, è possibile creare un catalogo di macchine MCS che supporti l'ibernazione. Utilizzando questa funzionalità, è possibile sospendere una macchina virtuale e riconnettersi allo stato precedente della macchina virtuale quando un utente accede nuovamente.

> **Nota:**
>
> La funzionalità di ibernazione si applica solo ai cataloghi di macchine con sistema operativo a sessione singola (persistenti e non persistenti).

In questa sezione, vedere quanto segue:

- Prerequisiti
- Limiti
- Creare e gestire un catalogo di macchine con funzionalità di ibernazione
- Creare un catalogo di macchine per le VM esistenti compatibili con l'ibernazione
- Abilitare l'ibernazione sulle VM esistenti di cui è stato eseguito il provisioning con MCS
- Controllare la proprietà di ibernazione
- Gestire l'alimentazione delle macchine virtuali (manuale e automatizzata)

### Prerequisiti per utilizzare l'ibernazione

Per utilizzare l'ibernazione, accertarsi di aver completato le seguenti attività:

- Abilitare la funzionalità per la propria sottoscrizione di Azure. Vedere Abilitazione della funzionalità di ibernazione per la sottoscrizione.
- Abilitare i seguenti pulsanti di attivazione/disattivazione in **DaaS > Home > Preview features**:
  - **Eseguire il provisioning di macchine virtuali che possono essere ibernate in Azure**
  - **Supporto di Autoscale per l'ibernazione**
- Installare Azure VM Agent nell'immagine master per Windows e Linux. Il file di paging dell'immagine Windows può trovarsi sul disco temporaneo. MCS imposta la posizione del file di paging sull'unità C: nel disco di base quando nel catalogo macchine è abilitata l'ibernazione.
- MCS imposta automaticamente la proprietà di ibernazione per le risorse generate. Non è necessario configurare le proprietà delle risorse master perché supportino l'ibernazione.
- Nella sottoscrizione utilizzare una dimensione di macchina virtuale che supporti l'ibernazione.
- Creare un profilo macchina compatibile con l'ibernazione (VM o specifica di modello) in modo che le VM ereditino la funzionalità di ibernazione. Per creare la VM, vedere Introduzione all'ibernazione.

  > **Nota:**
  >
  > Secondo Microsoft, è possibile distribuire VM abilitate all'ibernazione da un disco del sistema operativo. Questa funzionalità è attualmente supportata per alcune regioni e sarà presto disponibile per tutte le regioni. Per ulteriori informazioni, vedere Distribuire le macchine virtuali abilitate per l'ibernazione da un disco del sistema operativo.

  Per creare la specifica di modello, procedere come segue:

  1. Aprire il portale di Azure. Scegliere una macchina virtuale di cui si desidera utilizzare la configurazione nel modello. Selezionare **Export template** (Esporta modello) nel riquadro a sinistra.
  2. Deselezionare la casella di controllo **Include parameters**. Copiare il contesto e salvarlo come file JSON, ad esempio `VMExportTemplate.json`.
  3. Verificare che il parametro `hibernationEnabled` sia **`true`** nel modello. Se il parametro non è **`true`**, controllare la configurazione della VM utilizzata. È possibile specificare una dimensione di VM supportata nel file modello. Tuttavia, è possibile specificare le dimensioni della macchina anche durante la creazione del catalogo.
  4. Aggiungere il modello per la risorsa dell'interfaccia di rete al file JSON `VMExportTemplate.json`. Si ottiene così un file modello ARM con due risorse.

5. Selezionare **Azure Portal > Template specs > Import template > Choose local template file** (Portale di Azure > Specifiche del modello > Importa modello > Scegli il file modello locale) per importare questo file modello come specifica di modello ARM.
6. Dopo aver creato la specifica di modello ARM, è possibile utilizzarla come profilo macchina.

> **Nota:**
>
> La sincronizzazione con Citrix Studio potrebbe richiedere alcuni minuti.

Per ulteriori informazioni, vedere il documento Microsoft Prerequisiti per l'uso dell'ibernazione.

#### Limiti

- Sono supportati solo i cataloghi di macchine con sistema operativo a sessione singola (persistenti e non persistenti).
- I dischi temporanei del sistema operativo e le funzionalità di I/O MCS non supportano l'ibernazione di Azure.
- L'ibernazione potrebbe non riuscire durante gli aggiornamenti automatici di Windows.

Per ulteriori informazioni, vedere questo documento Microsoft.

#### Creare e gestire un catalogo di macchine con funzionalità di ibernazione

Per creare macchine virtuali compatibili con l'ibernazione, è possibile creare e gestire un catalogo di macchine che supportano l'ibernazione utilizzando:

- Interfaccia Full Configuration, oppure
- Comandi PowerShell

#### Creare un catalogo di macchine utilizzando l'interfaccia Full Configuration

1. Accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Machine Catalogs** (Cataloghi delle macchine) nel riquadro di sinistra.
3. Selezionare **Create Machine Catalog** (Crea catalogo delle macchine). Si apre la procedura guidata di creazione del catalogo.
4. Nella pagina **Machine Type** (Tipo di macchina), selezionare il tipo di macchina **Tipo di macchina** (Con sistema operativo a sessione singola) per questo catalogo.

5. Nella pagina **Machine Management** (Gestione macchina), selezionare le impostazioni seguenti:
    a) Selezionare **Machines that are power managed (for example, virtual machines or blade PCs)** [Macchine con alimentazione gestita (ad esempio, macchine virtuali o PC blade)].
    b) Selezionare **Citrix Machine Creation Services (MCS)**.
6. Nella pagina **Desktop Experience** (Esperienza desktop), selezionare l'esperienza desktop casuale o statica in base alle esigenze.
7. Nella pagina **Image** (Immagine), selezionare un'immagine master. Selezionare la casella di controllo **Use a machine profile** (Usa un profilo macchina) e selezionare un profilo macchina che supporti l'ibernazione. Fare clic sulla descrizione comando per sapere se un profilo macchina supporta l'ibernazione.
8. Nella pagina **Storage and License Types** (Tipi di archiviazione e licenza), selezionare lo spazio di archiviazione e la licenza da utilizzare per questo catalogo.
9. Nella pagina **Virtual Machines** (Macchine virtuali), selezionare il numero di macchine virtuali, le dimensioni delle macchine virtuali e la zona di disponibilità.

    > **Nota:**
    >
    > Le dimensioni dei computer che supportano l'ibernazione vengono visualizzate solo per la selezione effettuata.

10. Nella pagina **NICs**, aggiungere le NIC che dovranno essere utilizzate dalle macchine virtuali.
11. Nella pagina **Disk Settings** (Impostazioni disco), selezionare il tipo di archiviazione e la dimensione del disco della cache di write-back.
12. Nella pagina **Resource Group** (Gruppo di risorse), seleziona il gruppo di risorse per il provisioning delle VM.
13. Nella pagina **Machine Identities** (Identità macchine), selezionrea **Create new Active Directory accounts** (Crea nuovi account Active Directory). Quindi, specificare uno schema di denominazione degli account.
14. Nella pagina **Domain Credentials** (Credenziali del dominio) fare clic su **Enter credentials** (Inserisci credenziali). Inserire le credenziali del dominio per creare un account nel dominio Active Directory di destinazione.
15. Nella pagina **Summary** (Riepilogo), immettete un nome per il catalogo macchine, quindi fare clic su **Finish** (Fine).

Una volta completata la creazione del catalogo delle macchine MCS, individuare il catalogo nell' elenco dei cataloghi e fare clic sulla scheda **Template Properties** (Proprietà modello). Il valore del parametro **Hibernation** deve essere **Supported**.

Se si intende modificare un catalogo di macchine, tenere presenti le seguenti restrizioni:

- Se il catalogo di macchine corrente supporta l'ibernazione, non è possibile:
  - Cambiare la dimensione della macchina virtuale passando a una dimensione non compatibile con l'ibernazione.
  - Modificare il profilo della macchina impostando un profilo non compatibile con l'ibernazione.
- Se il catalogo di macchine corrente non supporta l'ibernazione, non è possibile:
  - attualmente, modificare il profilo della macchina in uno che supporta l'ibernazione utilizzando l'interfaccia Full Configuration. Tuttavia, è possibile farlo utilizzando i comandi PowerShell. Vedere Abilitare l'ibernazione sulle VM esistenti di cui è stato eseguito il provisioning con MCS.

**Creare un catalogo di macchine per la gestione delle VM esistenti compatibili con l'ibernazione**
Se si dispone già di macchine virtuali compatibili con l'ibernazione e si desidera sospenderle e ripristinarle, creare un catalogo di macchine in cui importare quelle macchine virtuali per gestirne l'alimentazione.

> **Nota:**
>
> È possibile creare un catalogo di macchine con sia VM che supportano l'ibernazione che VM che non la supportano. Tuttavia, se si desidera disporre di funzionalità correlate all'ibernazione, è necessario creare il catalogo delle macchine solo con VM che supportano l'ibernazione.

Per creare un catalogo per le VM esistenti compatibili con l'ibernazione utilizzando l'interfaccia Full Configuration, seguire le istruzioni sullo schermo per completare i passaggi e prestare attenzione alle seguenti impostazioni chiave:

1. Nella pagina **Machine Management** (Gestione macchine) selezionare **Machines that are power managed** (Macchine con alimentazione gestita), quindi selezionare **Other service or technology** (Altro servizio o tecnologia) come modalità di distribuzione delle macchine.
2. Nella pagina **Virtual Machines** (Macchine virtuali), aggiungere o importare solo le VM che supportano l'ibernazione.

**Creare un catalogo di macchine usando i comandi PowerShell** Dopo aver soddisfatto tutti i requisiti per utilizzare l'ibernazione, è possibile creare un catalogo di macchine compatibile con l'ibernazione utilizzando il comando `New-ProvScheme`. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Durante la creazione del catalogo, è possibile verificare se le dimensioni di una macchina virtuale e il profilo macchina supportano o meno l'ibernazione utilizzando i seguenti comandi PowerShell:

- Per la dimensione della VM, eseguire il comando seguente e verificare che la proprietà `supportsHibernation` sia **True**. Ad esempio,

```
Get-ChildItem -AdminAddress "localhost:19097" -LiteralPath @("
    XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder"
    ) | select Name, AdditionalData | ConvertTo-Json
<!--NeedCopy-->
```

- Per il profilo macchina, eseguire il comando seguente e verificre che la proprietà `supportsHibernation` sia **True**. Ad esempio,

```
Get-ChildItem -AdminAddress "localhost:19097" -LiteralPath @("
    XDHyp:\HostingUnits\ <VirtualNetwork> \machineprofile.folder\
    abc.resourcegroup")|select Name, AdditionalData|ConvertTo-Json
<!--NeedCopy-->
```

Se si intende modificare un catalogo di macchine, tenere presenti le seguenti restrizioni:

- Se il catalogo di macchine corrente supporta l'ibernazione, non è possibile:
  - Cambiare la dimensione della macchina virtuale passando a una dimensione non compatibile con l'ibernazione
  - Modificare il profilo della macchina impostando un profilo non compatibile con l'ibernazione.
- Se il catalogo di macchine corrente non supporta l'ibernazione, non è possibile:
  - attualmente, modificare il profilo della macchina in uno che supporta l'ibernazione utilizzando l'interfaccia Full Configuration. Tuttavia, è possibile farlo utilizzando i comandi PowerShell. Vedere Abilitare l'ibernazione sulle VM esistenti di cui è stato eseguito il provisioning con MCS.

Per informazioni su come modificare le dimensioni della macchina virtuale e il profilo macchina di un catalogo utilizzando Remote PowerShell SDK, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

#### Abilitare l'ibernazione sulle VM esistenti di cui è stato eseguito il provisioning con MCS

È possibile abilitare l'ibernazione di Azure sulle seguenti VM esistenti:

- VM Windows con provisioning eseguito con MCS di un catalogo di macchine creato senza un disco temporaneo.
- VM Linux con provisioning eseguito con MCS di un catalogo di macchine creato con e senza un disco temporaneo.

> **Nota:**
>
> - Le VM esistenti con provisioning eseguito con MCS devono avere un agente VM di Azure installato.
> - Attualmente è possibile utilizzare solo il comando PowerShell per abilitare questa funzionalità.

A questo scopo:

1. Aprire una finestra di **PowerShell**.
2. Eseguire `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Verificare la configurazione delle macchine esistenti. Ad esempio:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Abilitare l'ibernazione su questo catalogo di macchine utilizzando il comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
    folder\Standard_D4as_v5.serviceoffering"
<!--NeedCopy-->
```

5. Richiedere l'aggiornamento sulle macchine virtuali esistenti in un catalogo di macchine.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
    String[]
<!--NeedCopy-->
```

6. Riavviare le macchine virtuali per attivare gli aggiornamenti sulle macchine virtuali esistenti. Ad esempio:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

#### Controllare la proprietà di ibernazione

È possibile controllare la proprietà di ibernazione di un catalogo di macchine, di una macchina virtuale e di una macchina broker utilizzando i comandi PowerShell:

- Per verificare la proprietà di ibernazione di uno schema di provisioning, eseguire i seguenti comandi PowerShell. Il parametro `HibernationEnabled` deve essere `True`.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
   VMMetadata -join "" |  ConvertFrom-Json | Select
   HibernationEnabled
<!--NeedCopy-->
```

- Per verificare la proprietà di ibernazione di una VM di provisioning, eseguire i seguenti comandi PowerShell. Il parametro `SupportsHibernation` deve essere `True`.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- Per verificare la capacità di ibernazione di un computer broker, eseguire i seguenti comandi PowerShell. Le azioni relative all'alimentazione **Suspend** (Sospendi) e **Resume** (Riprendi) indicano la capacità di ibernazione.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
<!--NeedCopy-->
```

#### Gestione dell'alimentazione delle VM che supportano l'ibernazione

È possibile eseguire le seguenti operazioni di gestione dell'alimentazione sulle macchine virtuali che supportano l'ibernazione:

- Sospendere la VM dallo stato di esecuzione con il comando **Suspend**.
- Ripristinare la VM dallo stato sospeso con il comando **Resume**
- Forzare lo spegnimento della VM da uno stato sospeso con il comando **Force shut**
- Forzare il riavvio della VM dallo stato sospeso con il comando **Force restart**

Per ulteriori informazioni, vedere quanto segue:

- Suspend
- Resume (Riprendi)

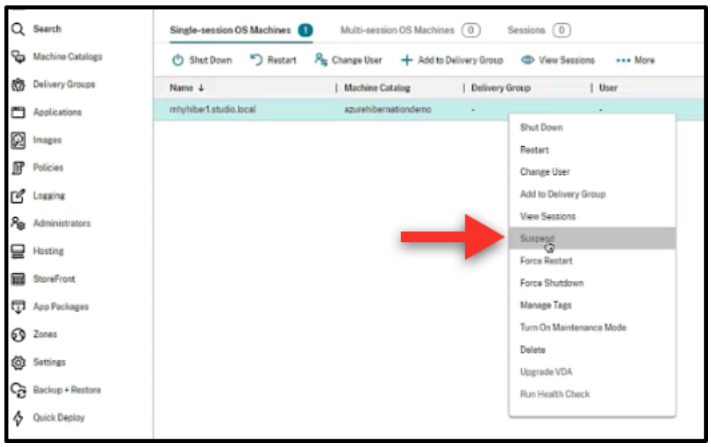
**Suspend** È possibile sospendere una macchina virtuale mediante uno dei seguenti metodi:

- **Manualmente** utilizzando l'interfaccia Full Configuration
- **Automaticamente** mediante il criterio di timeout: per ulteriori informazioni, vedere Impostazioni varie.

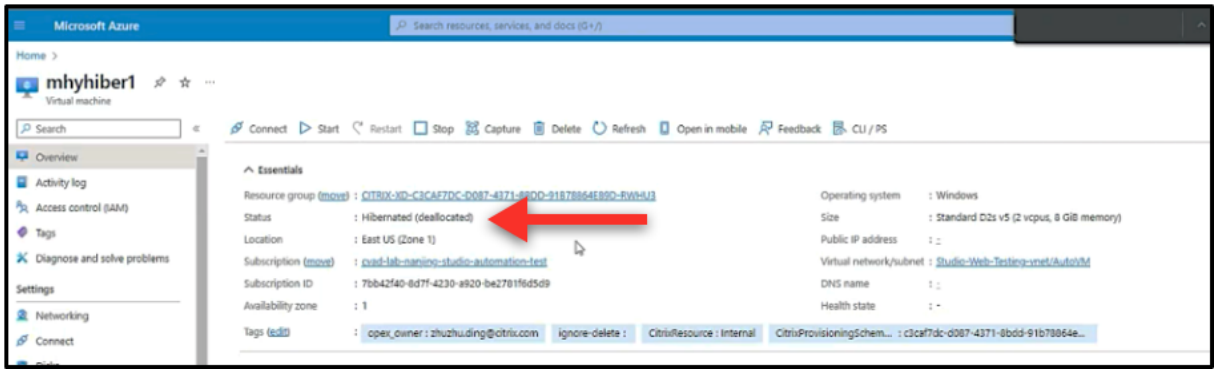
Per sospendere manualmente una macchina virtuale:

1. Fare clic con il pulsante destro del mouse sulla VM e selezionare **Suspend**. Fare clic su **Yes** per confermare l'azione. Lo stato di alimentazione (**Power State**) passa da **Suspending** a **Suspended**.



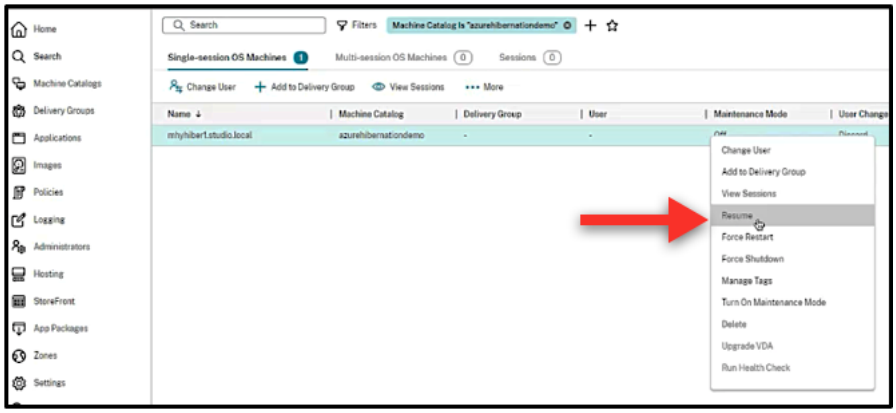

È possibile controllare lo stato della macchina virtuale nel portale Azure.



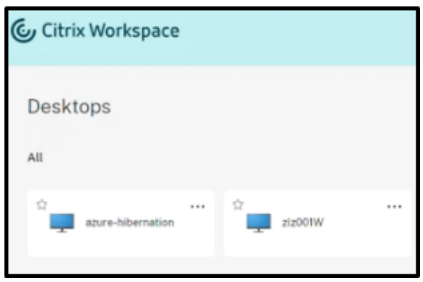

**Resume (Riprendi)** Per far riprendere una macchina virtuale ibernata, utilizzare uno dei seguenti metodi:

- **Manualmente**:
  - Gli amministratori possono far riprendere la macchina virtuale utilizzando l'interfaccia Full Configuration.



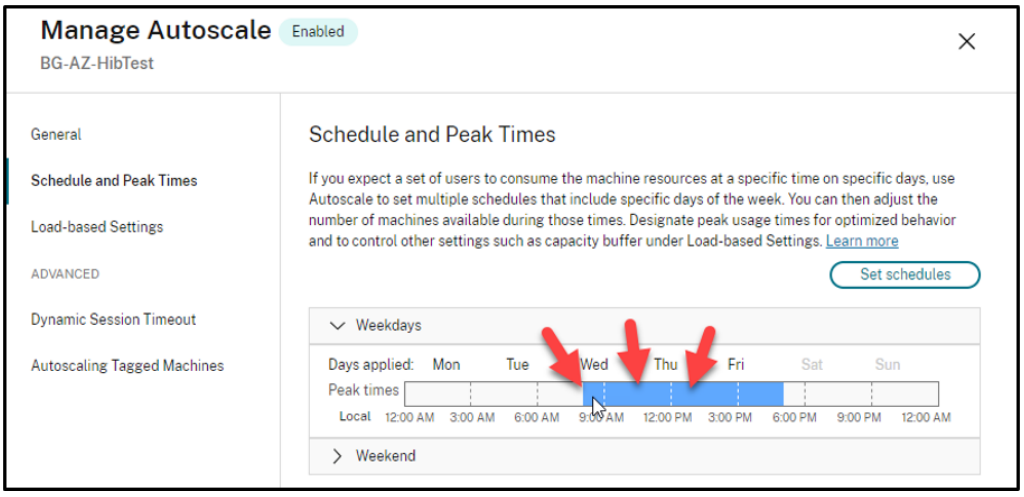

– Gli utenti finali possono avviare la VM utilizzando il menu Citrix Workspace dopo aver fatto clic sull'icona del desktop.




- **Automaticamente**:

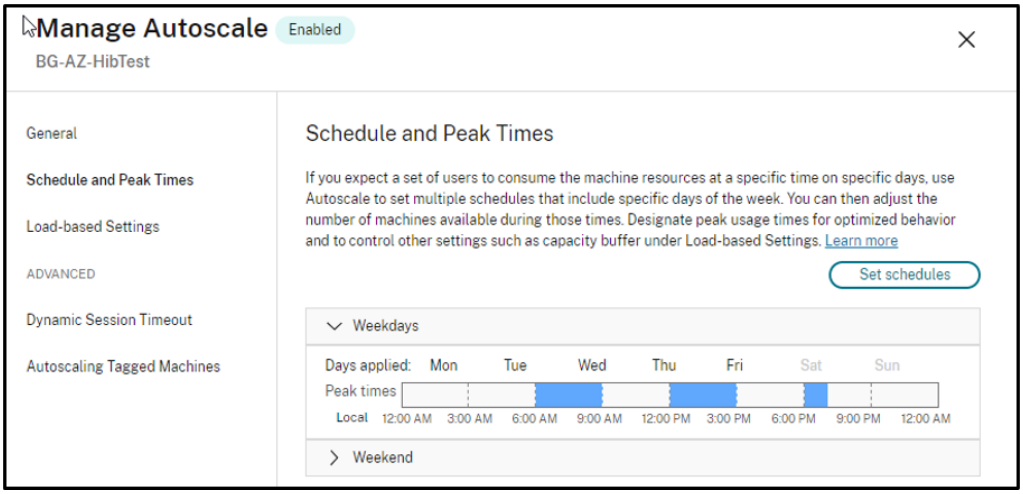
  – Autoscale può accendere automaticamente le macchine ibernate se si configurano correttamente le ore di punta. È possibile impostare le ore di punta a intervalli di 30 minuti facendo clic sulla pianificazione oraria. Ogni riquadro blu rappresenta una fascia oraria contrassegnata come ora di punta. Le ore di punta possono essere fasce orarie consecutive e non consecutive.

    * Fasce orarie consecutive



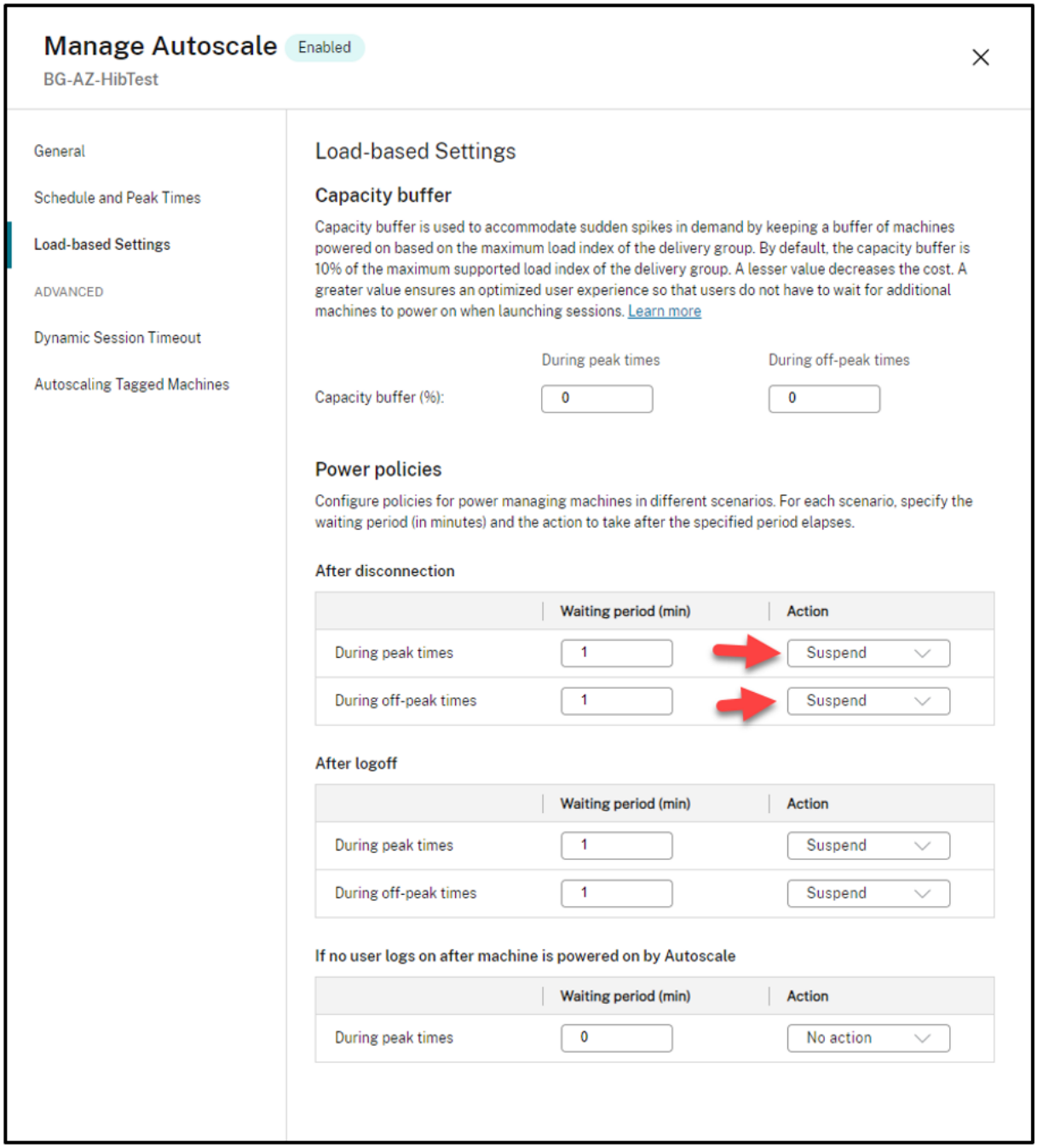

    * Fasce orarie non consecutive




> **Nota:**
>
> In **Manage Autoscale > Load-based Settings**, se l'azione (**Action**) è configurata come **Suspend**, assicurarsi che tutte le VM all'interno di quel gruppo di consegna dispongano della funzionalità di ibernazione. Altrimenti, le macchine virtuali che non possono andare in ibernazione continueranno a funzionare.




## Ulteriori informazioni

Per ulteriori informazioni sull'ibernazione di Citrix Azure, vedere questo articolo della Citrix Tech Zone.

# Criteri di sicurezza

April 14, 2023

Questo articolo descrive le funzionalità di sicurezza su vari hypervisor supportati. Le funzionalità di sicurezza includono:

- Gruppo di sicurezza
- Avvio sicuro
- Funzionalità di crittografia

# Gruppo di sicurezza

April 14, 2023

Il gruppo di sicurezza è un gruppo di regole di sicurezza finalizzate a filtrare il traffico di rete tra una risorsa e l'altra di una rete virtuale. Le regole di sicurezza consentono o negano il traffico di rete in entrata o in uscita da diversi tipi di risorse. Ogni regola specifica le seguenti proprietà:

- Name (Nome): un nome univoco all'interno del gruppo di sicurezza di rete
- Priority (Priorità): le regole vengono elaborate in ordine di priorità, con i numeri più bassi elaborati prima dei numeri più alti, perché i numeri più bassi hanno una priorità più alta
- Source or Destination (Origine o destinazione): qualsiasi numero di indirizzi IP o un singolo indirizzo IP, blocco CIDR (routing interdominio senza classi) (10.0.0.0/24, ad esempio), tag di servizio o gruppo di sicurezza dell'applicazione
- Protocol (Protocollo): i protocolli in base ai quali si aggiungono regole per ogni gruppo di sicurezza
- Direction (Direzione): se la regola si applica al traffico in entrata o in uscita
- Port range (Intervallo di porte): è possibile specificare una singola porta o un intervallo di porte
- Action (Azione): consentire o negare

Per ulteriori informazioni sugli hypervisor supportati, vedere le sezioni seguenti:

- Gruppo di sicurezza in AWS
- Gruppo di sicurezza in Microsoft Azure
- Gruppo di sicurezza in Google Cloud Platform

### Gruppo di sicurezza in AWS

I gruppi di sicurezza agiscono come firewall virtuali che controllano il traffico per le istanze nel VPC. È possibile aggiungere regole ai gruppi di sicurezza che consentono alle istanze nella subnet pubblica di comunicare con le istanze nella subnet privata. Inoltre, questi gruppi di sicurezza potranno anche essere associati a ogni istanza nel VPC. Le regole in entrata controllano il traffico in entrata verso la propria istanza e le regole in uscita controllano il traffico in uscita da essa.

Per ulteriori informazioni sulle impostazioni di rete durante la preparazione delle immagini, vedere Impostazioni di rete durante la preparazione dell'immagine.

Quando si avvia un'istanza, è possibile specificare uno o più gruppi di sicurezza. Per configurare i gruppi di sicurezza, vedere Configurare i gruppi di sicurezza.

### Gruppo di sicurezza in Microsoft Azure

Citrix DaaS supporta i gruppi di sicurezza di rete in Azure. È previsto che i gruppi di sicurezza di rete si associno alle sottoreti. Per ulteriori informazioni, vedere Gruppi di sicurezza di rete.

Per altre informazioni sul gruppo di sicurezza di rete creato durante la preparazione dell'immagine, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager.

### Gruppo di sicurezza in Google Cloud Platform

Durante la preparazione di un catalogo delle macchine, viene preparata un'immagine della macchina che funge da disco di sistema dell'immagine master per il catalogo. Quando si verifica questo processo, il disco viene temporaneamente collegato a una macchina virtuale. Questa macchina virtuale deve essere eseguita in un ambiente isolato che impedisca tutto il traffico di rete in entrata e in uscita. Ciò si ottiene attraverso una coppia di regole firewall "nega tutto". Per ulteriori informazioni, vedere Regole del firewall.

## Avvio sicuro

June 8, 2023

L'avvio sicuro è progettato per garantire che venga utilizzato solo software attendibile per avviare il sistema. Il firmware dispone di un database di certificati attendibili e verifica che l'immagine caricata sia firmata da uno dei certificati attendibili. Se quell'immagine carica altre immagini, anche quell'immagine deve essere verificata allo stesso modo.

vTPM è un'istanza software virtualizzata di un modulo TPM fisico tradizionale. vTPM consente l'attestazione misurando l'intera catena di avvio della macchina virtuale (UEFI, sistema operativo, sistema e driver).

Per ulteriori informazioni sugli hypervisor supportati, vedere le sezioni seguenti:

- Avvio sicuro in Google Cloud Platform
- Avvio sicuro in Microsoft Azure
- Avvio sicuro in VMware

### Avvio sicuro in Google Cloud Platform

È possibile effettuare il provisioning di macchine virtuali schermate su GCP. Una macchina virtuale schermata è rafforzata mediante una serie di controlli di sicurezza che forniscono l'integrità verificabile delle istanze di Compute Engine, utilizzando funzionalità avanzate di sicurezza della piattaforma quali l'avvio sicuro, un modulo di piattaforma attendibile virtuale, firmware UEFI e monitoraggio dell'integrità.

Per ulteriori informazioni sull'uso di PowerShell per creare un catalogo con macchine virtuali schermate, vedere Utilizzo di PowerShell per creare un catalogo con VM schermate.

### Avvio sicuro in Microsoft Azure

In ambienti Azure, è possibile creare cataloghi di macchine abilitati con l'avvio attendibile. Azure offre l'avvio attendibile come modo semplice per migliorare la sicurezza delle macchine virtuali di seconda generazione. L'avvio attendibile protegge da tecniche di attacco avanzate e persistenti. Alla base dell'avvio attendibile c'è l'avvio sicuro della VM. L'avvio attendibile utilizza anche vTPM per eseguire l'attestazione remota tramite il cloud. Viene utilizzato per i controlli dello stato della piattaforma e per prendere decisioni basate sull'attendibilità. È possibile abilitare singolarmente l'avvio sicuro e vTPM. Per ulteriori informazioni sulla creazione di un catalogo di macchine con avvio attendibile, vedere Cataloghi di macchine con avvio attendibile.

### Avvio sicuro in VMware

MCS supporta la creazione di un catalogo di macchine con un modello VMware allegato a vTPM come fonte per l'input del profilo macchina. Se Windows 11 è installato sull'immagine master, è necessario che vTPM sia abilitato per l'immagine master. Pertanto, il modello VMware, che è un'origine del profilo della macchina, deve avere vTPM collegato. Per ulteriori informazioni, vedere Creare un catalogo di macchine utilizzando un profilo macchina.

# Funzionalità di crittografia

June 8, 2023

Le funzionalità di crittografia proteggono il contenuto delle macchine virtuali dagli attacchi di ospiti malintenzionati su un host di macchina virtuale condiviso e dagli attacchi lanciati dal software di controllo dell'hypervisor che gestisce tutte le macchine virtuali presenti sull'host.

Per ulteriori informazioni sugli hypervisor supportati, vedere le sezioni seguenti:

- Funzionalità di crittografia in AWS
- Funzionalità di crittografia in Google Cloud Platform
- Funzionalità di crittografia in Microsoft Azure)

## Funzionalità di crittografia in AWS

Questa sezione descrive le funzionalità di crittografia negli ambienti di virtualizzazione AWS.

### Crittografia automatica

È possibile attivare la crittografia automatica dei nuovi volumi Amazon EBS e delle copie istantanee create nell'account. Per ulteriori informazioni, vedere Crittografia automatica.

## Funzionalità di crittografia in Google Cloud Platform

Questa sezione descrive le funzionalità di crittografia negli ambienti di virtualizzazione di Google Cloud Platform (GCP).

Se si necessita di un maggiore controllo sulle operazioni delle chiavi rispetto a quello consentito dalle chiavi di crittografia gestite da Google, è possibile utilizzare chiavi di crittografia gestite dal cliente. Quando si utilizza una chiave di crittografia gestita dal cliente, un oggetto viene crittografato con la chiave da Cloud Storage nel momento in cui viene archiviato in un bucket e l'oggetto viene decrittografato automaticamente da Cloud Storage quando viene fornito ai richiedenti. Per ulteriori informazioni, vedere Chiavi di crittografia gestite dal cliente.

È possibile utilizzare le chiavi di crittografia gestite dal cliente (CMEK) per i cataloghi MCS. Per ulteriori informazioni, vedere Utilizzo di CMEK (Customer Managed Encryption Keys, chavi di crittografia gestite dal cliente).

### Funzionalità di crittografia in Microsoft Azure

Questa sezione descrive le funzionalità di crittografia negli ambienti di virtualizzazione di Azure.

#### Crittografia lato server di Azure

La maggior parte dei dischi gestiti di Azure è crittografata con la crittografia di Azure Storage, che utilizza la crittografia lato server (SSE) per proteggere i dati dell'utente e aiutarlo a rispettare gli impegni di sicurezza e conformità. Citrix DaaS supporta le chiavi di crittografia gestite dal cliente per i dischi gestiti di Azure tramite Azure Key Vault. Per ulteriori informazioni, vedere Crittografia lato server di Azure.

#### Doppia crittografia di Azure

La doppia crittografia è costituita da crittografia lato piattaforma (impostazione predefinita) e crittografia gestita dal cliente (CMEK). Pertanto, se si è un cliente altamente sensibile alla sicurezza e si nutre preoccupazione per il rischio associato a qualsiasi algoritmo di crittografia, implementazione o chiave compromessa, è possibile optare per questa doppia crittografia. Il sistema operativo persistente e i dischi di dati, le istantanee e le immagini sono tutti crittografati quando inattivi con doppia crittografia. Per ulteriori informazioni, vedere Doppia crittografia su disco gestito.

## Distribuzione rapida

November 21, 2023

### Introduzione

In Citrix DaaS l'interfaccia **Manage > Quick Deploy** (Gestisci > Distribuzione rapida) offre una rapida distribuzione di app e desktop quando si utilizza Microsoft Azure per l'hosting di desktop e app. Questa interfaccia offre una configurazione di base senza funzionalità avanzate.

Utilizzare Quick Deploy (Distribuzione rapida) per:

- Eseguire il provisioning di macchine virtuali e cataloghi che distribuiscono desktop e app ospitati in Microsoft Azure.
- Creare cataloghi Remote PC Access (Accesso remoto PC) per le macchine esistenti.

Con Quick Deploy (Distribuzione rapida) è possibile utilizzare una sottoscrizione Citrix Managed Azure o la propria sottoscrizione di Azure

(sebbene i nomi siano simili, Quick Deploy [Distribuzione rapida] non corrisponde al metodo Quick Create [Creazione rapida] per la creazione di cataloghi nell'interfaccia Quick Deploy [Distribuzione rapida]).

In alternativa a Quick Deploy (Distribuzione rapida), l'interfaccia **Full Configuration** (Configurazione completa) offre funzionalità di configurazione avanzate. Per informazioni sulle opzioni della scheda **Manage** (Gestisci), vedere Management interfaces (Interfacce di gestione).

### Differenze tra le interfacce di gestione

Nella tabella seguente vengono confrontate le interfacce Full Configuration (Configurazione completa) e Quick Deploy (Distribuzione rapida).

| Funzionalità | Distribuzione rapida | Full Configuration (Configurazione completa) |
|---|---|---|
| Distribuzione con Azure | Sì | Sì* |
| Distribuzione utilizzando altri servizi cloud | No | Sì |
| Distribuzione tramite hypervisor locali | No | Sì |
| Immagini preparate da Citrix disponibili | Sì | No |
| Esperienza utente semplificata | Sì | No |

*Quando si utilizza una sottoscrizione Citrix Managed Azure, è necessario utilizzare Quick Deploy (Distribuzione rapida) durante la creazione di un'immagine o di un catalogo.

Se si ha familiarità con l'utilizzo di Full Configuration (Configurazione completa) per creare e gestire cataloghi, Quick Deploy (Distribuzione rapida) presenta le seguenti differenze.

- Terminologia diversa.
  - In Quick Deploy (Distribuzione rapida) è possibile creare un catalogo.
  - In Full Configuration (Configurazione completa) è possibile creare un catalogo delle macchine. In pratica, viene spesso definito semplicemente catalogo.
- Posizione risorsa e Cloud Connector.
  - Quick Deploy (Distribuzione rapida) crea automaticamente una posizione risorsa contenente due Cloud Connector quando si crea il primo catalogo.

  - In Full Configuration (Configurazione completa), la creazione di una posizione risorsa e l'aggiunta di Cloud Connector sono passaggi separati che è necessario completare in Citrix Cloud prima di creare un catalogo.

- Immagini utilizzate per creare cataloghi.
  - Quick Deploy (Distribuzione rapida) offre diverse immagini di macchine Windows e Linux preparate da Citrix. È possibile utilizzare queste immagini per creare cataloghi.

    È inoltre possibile utilizzare queste immagini per creare immagini e quindi personalizzare le nuove immagini in base alle proprie esigenze di distribuzione specifiche. Questa funzionalità è nota come "generatore di immagini". È anche possibile importare immagini dalla propria sottoscrizione di Azure.
  - In Full Configuration (Configurazione completa), è possibile personalizzare le immagini dall'host supportato che si sta utilizzando. Le immagini preparate da Citrix non sono disponibili.

- Visualizzazioni del catalogo:
  - I cataloghi creati in Quick Deploy (Distribuzione rapida) sono visibili nelle visualizzazioni Quick Deploy (Distribuzione rapida) e Full Configuration (Configurazione completa).
  - I cataloghi creati in Full Configuration (Configurazione completa) non sono visibili nella visualizzazione Quick Deploy (Distribuzione rapida).

- Gruppi di consegna:
  - Non si creano gruppi di consegna in Quick Deploy (Distribuzione rapida). In Quick Deploy (Distribuzione rapida) è possibile specificare le macchine, le applicazioni, i desktop e gli utenti (sottoscrittori) nel catalogo.

    Citrix crea automaticamente un gruppo di consegna per ogni catalogo Quick Deploy (Distribuzione rapida), utilizzando lo stesso nome del catalogo. Questa azione avviene dietro le quinte. Non è necessario eseguire alcuna operazione per creare il gruppo di consegna. Il gruppo di consegna viene visualizzato solo nell'interfaccia Full Configuration (Configurazione completa), non in Quick Deploy (Distribuzione rapida).
  - In Full Configuration (Configurazione completa) è possibile creare un gruppo di consegna e indicare quali macchine contiene. Facoltativamente, è possibile specificare anche applicazioni, desktop e utenti È inoltre possibile creare gruppi di applicazioni.

- Layout e interfaccia utente.
  - L'interfaccia Quick Deploy ha un layout e uno stile diversi da quelli di Full Configuration (Configurazione completa). Quick Deploy (Distribuzione rapida) mostra più indicazioni sullo schermo.

Le interfacce non si escludono a vicenda. È possibile utilizzare Quick Deploy (Distribuzione rapida) per creare alcuni cataloghi e quindi utilizzare Full Configuration (Configurazione completa) per creare altri cataloghi.

### Gestire i cataloghi creati nell'interfaccia Quick Deploy (Distribuzione rapida)

Dopo aver creato un catalogo nell'interfaccia Quick Deploy (Distribuzione rapida), è possibile continuare a gestire tale catalogo in tale interfaccia. Per ulteriori informazioni, consultare Gestire i cataloghi in Quick Deploy (Distribuzione rapida). È inoltre possibile utilizzare l'interfaccia Full Configuration (Configurazione completa).

Quando si crea un catalogo in Quick Deploy (Distribuzione rapida), a tale catalogo (oltre al gruppo di consegna e alla connessione di hosting creati automaticamente dietro le quinte) viene assegnato un ambito di `Citrix managed object`. Gli ambiti vengono utilizzati nell'amministrazione delegata per raggruppare gli oggetti.

Cataloghi, gruppi di consegna e connessioni con l'ambito `Citrix managed object` non possono eseguire determinate azioni nell'interfaccia Full Configuration (Configurazione completa) (l'autorizzazione di tali azioni in Full Configuration [Configurazione completa] potrebbe influire negativamente sulla capacità del sistema di supportare sia Quick Deploy [Distribuzione rapida] che Full Configuration [Configurazione completa], pertanto tali azioni sono disabilitate). Nell'interfaccia Full Configuration (Configurazione completa):

- **Catalog** (Catalogo): la maggior parte delle azioni di gestione del catalogo non sono disponibili. Non è possibile eliminare un catalogo.
- **Delivery group** (Gruppo di consegna): sono disponibili la maggior parte delle azioni di gestione del gruppo di consegna. Non è possibile eliminare il gruppo di consegna.
- **Connection** (Connessione): la maggior parte delle azioni di gestione delle connessioni non sono disponibili. Non è possibile eliminare una connessione. Non è possibile creare una connessione basata su una connessione con l'ambito `Citrix managed object`.

Se si crea un catalogo in Quick Deploy (Distribuzione rapida) utilizzando la propria sottoscrizione di Azure (aggiunta a Quick Deploy [Distribuzione rapida]) e si desidera gestire il catalogo (e il relativo gruppo di consegna e connessione) interamente in Full Configuration (Configurazione completa), è possibile *convertire* il catalogo.

- La conversione di un catalogo ne limita la gestione solo all'interfaccia Full Configuration (Configurazione completa). Dopo la conversione di un catalogo, non è più possibile utilizzare l'interfaccia Quick Deploy (Distribuzione rapida) per gestire il catalogo.
- Dopo la conversione di un catalogo, è possibile selezionare le azioni precedentemente non disponibili in Full Configuration (Configurazione completa) (l'ambito `Citrix managed`

`object` viene rimosso dal catalogo convertito, dal gruppo di consegna e dalla connessione di hosting).

- Per convertire un catalogo:

  Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo. Nella scheda **Details** (Dettagli), in **Advanced Settings** (Impostazioni avanzate) selezionare **Convert Catalog** (Converti catalogo). Quando richiesto, confermare la conversione.

- Non è possibile convertire un catalogo creato in Quick Deploy (Distribuzione rapida) utilizzando una sottoscrizione di Citrix Managed Azure.

#### Sostituzione dell'interfaccia precedente Azure Quick Deploy (Distribuzione rapida di Azure)

Quick Deploy (Distribuzione rapida) sostituisce un'interfaccia precedente denominata Azure Quick Deploy (Distribuzione rapida di Azure). La visualizzazione Quick Deploy (Distribuzione rapida) include tutti i cataloghi creati con Azure Quick Deploy (Distribuzione rapida di Azure).

Se si è iniziato a creare un catalogo in Azure Quick Deploy (Distribuzione rapida di Azure), ma l'operazione non è stata completata, tale catalogo viene visualizzato nell'elenco del catalogo Quick Deploy (Distribuzione rapida). Tuttavia, l'unica azione disponibile in Quick Deploy (Distribuzione rapida) è l'eliminazione.

### Requisiti

- Quick Deploy (Distribuzione rapida) supporta solo i carichi di lavoro di Azure. Non è disponibile con altri tipi di host, servizi o hypervisor cloud.
- Quick Deploy (Distribuzione rapida) è disponibile solo nelle edizioni Citrix DaaS per Azure, Premium, Advanced e Workspace Premium Plus.
- È necessario disporre di un account Citrix Cloud e di una sottoscrizione a Citrix DaaS.
- Se è stato ordinato Citrix Managed Azure Consumption Fund, è possibile utilizzare una sottoscrizione a Citrix Managed Azure per la creazione di cataloghi e immagini.

  Se non è stato ordinato il Consumption Fund (o se si preferisce utilizzare la propria sottoscrizione di Azure), è necessario disporre di una sottoscrizione di Azure.

- È necessario disporre delle autorizzazioni appropriate in Citrix DaaS per visualizzare la scheda **Manage** (Gestisci). Per ulteriori informazioni, vedere Amministrazione delegata.

> **Importante:**
>
> Per assicurarsi di ottenere importanti informazioni su Citrix Cloud e sui servizi Citrix a cui si è abbonati, assicurarsi di poter ricevere tutte le notifiche e-mail. Ad esempio, Citrix invia e-mail mensili informative di notifica che descrivono in dettaglio il consumo (utilizzo) di Azure.
>
> Nell'angolo in alto a destra della console Citrix Cloud, espandere il menu a destra del nome del cliente e dei campi OrgID. Selezionare **Impostazioni account**. Nella scheda **Il mio profilo**, selezionare tutte le voci nella sezione **Notifiche tramite e-mail**.

#### Considerazione su Citrix Gateway

Se si utilizza il proprio Citrix Gateway, è necessario che abbia accesso alla VNet specificata nella procedura guidata di creazione del catalogo. Una VPN può fornire tale accesso.

Il servizio Citrix Gateway funziona automaticamente con i cataloghi Quick Deploy (Distribuzione rapida).

### Passaggi successivi

Seguire la guida alla configurazione di Quick Deploy (Distribuzione rapida) in Per iniziare.

Dopo aver configurato la distribuzione utilizzando Quick Deploy (Distribuzione rapida), è possibile continuare a utilizzare tale interfaccia per le seguenti attività di gestione.

- Gestire il catalogo. La gestione del catalogo include l'aggiunta o l'eliminazione di macchine, la gestione delle app e la gestione delle pianificazioni di gestione dell'alimentazione.
- Gestire le immagini. La gestione delle immagini include la preparazione o l'importazione di immagini, l'aggiornamento dei cataloghi con una nuova immagine, la ridenominazione o l'eliminazione di immagini e l'installazione o l'aggiornamento di VDA su un'immagine.
- Aggiungere o rimuovere utenti in un catalogo.
- Gestire le posizioni delle risorse.

## Iniziare a usare Quick Deploy

May 23, 2023

Questo articolo riassume le attività di configurazione per la distribuzione di desktop e app utilizzando l'interfaccia Quick Deploy (Distribuzione rapida) di Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). Si consiglia di esaminare ogni procedura prima di eseguirla effettivamente, in modo da sapere cosa aspettarsi.

Per utilizzare Quick Deploy (Distribuzione rapida) per configurare una distribuzione Remote PC Access (Accesso Remoto PC), vedere Remote PC Access (Accesso remoto PC).

### Riepilogo delle attività di configurazione

Le seguenti sezioni di questo articolo guidano l'utente nelle attività di configurazione:

1. Esaminare e completare le attività necessarie in Requisiti di sistema e preparazione.
2. Impostare una distribuzione rapida Proof of Concept (POC) o una distribuzione di produzione.
3. Fornire l'URL dell'area di lavoro ai propri utenti.

### Requisiti di sistema e preparazione

- Registrarsi a Citrix Cloud e Citrix DaaS.

  Inoltre, se si prevede di utilizzare Citrix Managed Azure, assicurarsi di ordinare il Citrix Azure Consumption Fund (oltre a Citrix DaaS), tramite Citrix o Azure Marketplace.

- **Licenze Windows:** assicurarsi di disporre della licenza appropriata per Servizi Desktop remoto per l'esecuzione di carichi di lavoro di Windows Server o di una licenza per Desktop virtuale Azure per Windows 10. Per ulteriori informazioni, vedere Configurare un server licenze Microsoft RDS.
- Se si prevede di utilizzare una sottoscrizione Citrix Managed Azure e si desidera aggiungere VDA a un dominio utilizzando Criteri di gruppo di Active Directory, è necessario essere un amministratore con l'autorizzazione per eseguire tale azione in Active Directory. Per i dettagli, consultare Customer responsibility (Responsabilità del cliente).
- La configurazione delle connessioni alla rete aziendale on-premise presenta requisiti aggiuntivi.
  - Qualsiasi connessione (peering della rete virtuale di Azure o SD-WAN): requisiti per tutte le connessioni.
  - Connessioni di peering della rete virtuale di Azure: requisiti e preparazione del peering della rete virtuale.
  - Connessioni SD-WAN: requisiti e preparazione della connessione SD-WAN.
- Se si prevede di utilizzare le proprie immagini di Azure durante la creazione di un catalogo, tali immagini devono soddisfare determinati requisiti.
- Requisiti di connettività Internet: requisiti di sistema e connettività.
- Limiti di risorse in una distribuzione Citrix DaaS: limiti.

#### Sistemi operativi supportati

Quando si utilizza Quick Deploy (Distribuzione rapida) con una sottoscrizione Citrix Managed Azure:

- Windows 10 a sessione singola
- Windows 10 multisessione
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux e Ubuntu

Quando si utilizza Quick Deploy (Distribuzione rapida) con una sottoscrizione di Azure gestita dal cliente:

- Windows 10 Enterprise a sessione singola
- Desktop virtuale Windows 10 Enterprise multisessione
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux e Ubuntu

### Configurare una distribuzione rapida Proof of Concept (POC)

Questa procedura richiede una sottoscrizione Citrix Managed Azure.

1. Creare un catalogo utilizzando Quick Create (Creazione rapida).
2. Aggiungere i propri utenti all'Active Directory gestita di Azure.
3. Aggiungere i propri utenti al catalogo.
4. Comunicare agli utenti l'URL di Workspace.

### Configurare una distribuzione di produzione

1. Se si utilizza la propria Active Directory o Azure Active Directory per autenticare gli utenti, connettersi e impostare questo metodo in Citrix Cloud.
2. Se si utilizzano macchine aggiunte a un dominio, verificare di disporre di voci del server DNS valide.
3. Se si utilizza la propria sottoscrizione di Azure (anziché una sottoscrizione Citrix Managed Azure), aggiungere la propria sottoscrizione di Azure.
4. Creare o importare un'immagine. Sebbene sia possibile utilizzare una delle immagini preparate da Citrix così com'è in un catalogo, tali immagini sono destinate principalmente alle distribuzioni Proof of Concept (POC).

5. Se si utilizza una sottoscrizione Citrix Managed Azure e si desidera che gli utenti siano in grado di accedere agli elementi della rete (ad esempio i file server), configurare un peering della rete virtuale di Azure o una connessione Citrix SD-WAN.
6. Creare un catalogo utilizzando Custom Create (Creazione personalizzata).
7. Se si sta creando un catalogo di macchine multisessione, aggiungere app al catalogo, se necessario.
8. Se si utilizza Citrix Managed Azure AD per autenticare gli utenti, aggiungere utenti alla directory.
9. Aggiungere utenti al catalogo.
10. Comunicare agli utenti l'URL di Workspace.

Dopo aver configurato la distribuzione, utilizzare la dashboard **Quick Deploy > Monitor** (Distribuzione rapida > Monitoraggio) per visualizzare l'utilizzo dei desktop, le sessioni e le macchine.

### URL di Workspace

Dopo aver creato i cataloghi e assegnato gli utenti, comunicare agli utenti dove possono trovare i loro desktop e app: l'URL di Workspace. L'URL di Workspace è lo stesso per tutti i cataloghi e gli utenti.

L'URL di Workspace è disponibile in due posizioni:

- Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida) in Citrix DaaS, visualizzare l'URL espandendo **User Access & Authentication** (Accesso e autenticazione utente) sulla destra.
- Dalla console di Citrix Cloud, selezionare **Workspace Configuration** (Configurazione di Workspace) dal menu nell'angolo in alto a sinistra. La **scheda Access** contiene l'URL di Workspace.

Per informazioni sulla personalizzazione dell'URL di Workspace, consultare Personalizzare l'URL di Workspace.

Dopo aver effettuato l'accesso all'URL di Workspace e aver eseguito l'autenticazione, gli utenti possono avviare i desktop e le app.

### Ottenere assistenza

- Consultare l'articolo sulla risoluzione dei problemi.
- Se si riscontrano ancora problemi con Citrix DaaS, aprire un ticket seguendo le istruzioni riportate in Come ottenere assistenza e supporto.

## Creare cataloghi utilizzando Quick Deploy

October 6, 2022

Utilizzare le procedure in questo articolo per creare un catalogo di macchine Microsoft Azure utilizzando l'interfaccia di gestione Quick Deploy (Distribuzione rapida).

Esaminare l'intera procedura prima di creare un catalogo, in modo da sapere cosa aspettarsi.

Per creare un catalogo utilizzando l'interfaccia Full Configuration (Configurazione completa), vedere Creare cataloghi di macchine.

### Tipi di macchine

Un catalogo Quick Deploy (Distribuzione rapida) può contenere uno dei seguenti tipi di macchine:

- **Statico:** il catalogo contiene macchine statiche a sessione singola (note anche come desktop personali, dedicati o persistenti). Statico significa che quando un utente avvia un desktop, quel desktop "appartiene"a quell'utente. Tutte le modifiche apportate dall'utente al desktop vengono mantenute al momento della disconnessione. Successivamente, quando l'utente torna a Citrix Workspace e avvia un desktop, si tratta dello stesso desktop.
- **Casuale:** il catalogo contiene macchine casuali a sessione singola (note anche come desktop non persistenti). Casuale significa che quando un utente avvia un desktop, tutte le modifiche apportate dall'utente a quel desktop vengono eliminate dopo la disconnessione. Successivamente, quando l'utente ritorna a Citrix Workspace e avvia un desktop, potrebbe trattarsi o meno dello stesso desktop.
- **Multisessione:** il catalogo contiene macchine con app e desktop. Più di un utente può accedere a ciascuna di queste macchine contemporaneamente. Gli utenti possono avviare un desktop o le app dalla propria area di lavoro. Le sessioni delle app possono essere condivise. La condivisione delle sessioni non è consentita tra un'app e un desktop.
  - Quando si crea un catalogo multisessione, si seleziona il carico di lavoro: leggero (ad esempio immissione di dati), medio (ad esempio app per ufficio), pesante (ad esempio progettazione) o personalizzato. Ogni opzione rappresenta un numero specifico di macchine e sessioni per macchina, che produce il numero totale di sessioni supportate dal catalogo.
  - Se si seleziona il carico di lavoro personalizzato, è possibile selezionare una delle combinazioni disponibili di CPU, RAM e archiviazione. Digitare il numero di macchine e sessioni per macchina, che genera il numero totale di sessioni supportate dal catalogo.

Quando si distribuiscono desktop, i tipi di macchine statiche e casuali sono talvolta chiamate "tipi di desktop".

### Modi per creare un catalogo utilizzando Quick Deploy (Distribuzione rapida)

Esistono diversi modi per creare e configurare un catalogo:

- **Quick create** (Creazione rapida) è il modo più veloce per iniziare. L'utente fornisce informazioni minime e Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) si occupa di tutto il resto. Un catalogo Quick create (Creazione rapida) è ideale per un ambiente di test o un Proof of Concept (POC).
- **Custom create** (Creazione personalizzata) consente più scelte di configurazione rispetto a Quick create (Creazione rapida). È più adatta a un ambiente di produzione rispetto a un catalogo Quick create (Creazione rapida).
- I cataloghi di **Remote PC Access** (Accesso remoto PC) contengono macchine esistenti (generalmente fisiche) a cui gli utenti accedono in remoto. Per dettagli e istruzioni su questi cataloghi, vedere Remote PC Access (Accesso remoto PC).

Ecco un confronto tra Quick create (Creazione rapida) e Custom create (Creazione personalizzata):

| Quick create (Creazione rapida) | Custom create (Creazione personalizzata) |
|---|---|
| Meno informazioni da fornire. | Più informazioni da fornire. |
| Meno possibilità di scelta per alcune funzionalità. | Più possibilità di scelta per alcune funzionalità. |
| Autenticazione utente di Azure Active Directory gestita da Citrix. | Scelta tra: Azure Active Directory gestita da Citrix o la propria Active Directory/Azure Active Directory. |
| Nessuna connessione alla rete on-premise. | Scelta tra: nessuna connessione alla rete on-premise, peering della rete virtuale di Azure VNet e SD-WAN. |
| Utilizza un'immagine Windows 10 preparata da Citrix. L'immagine contiene un VDA desktop corrente. | Scelta tra: immagini preparate da Citrix, immagini importate da Azure o immagini create in Citrix DaaS da un'immagine preparata o importata da Citrix. |
| Ogni desktop dispone di spazio di archiviazione su disco standard (HDD) di Azure. | Sono disponibili diverse opzioni di archiviazione. |
| Solo desktop statici. | Desktop statici, casuali o multisessione. |
| Non è possibile configurare un programma di gestione dell'alimentazione durante la creazione. La macchina che ospita il desktop si spegne al termine della sessione (è possibile modificare questa impostazione in seguito). | È possibile configurare un programma di gestione dell'alimentazione durante la creazione (una pianificazione di gestione dell'alimentazione Quick Deploy [Distribuzione rapida] è diversa da una pianificazione di gestione dell'alimentazione che è possibile creare utilizzando l'interfaccia di gestione Full Configuration [Configurazione completa]). |

| Quick create (Creazione rapida) | Custom create (Creazione personalizzata) |
| --- | --- |
| È necessario utilizzare una sottoscrizione Citrix Managed Azure. | È possibile utilizzare la sottoscrizione Citrix Managed Azure o la propria sottoscrizione di Azure. |

Per i dettagli sulla procedura, vedere:

- Creare un catalogo Quick Deploy (Distribuzione rapida) utilizzando Quick create (Creazione rapida)
- Creare un catalogo Quick Deploy (Distribuzione rapida) utilizzando Custom create (Creazione personalizzata)

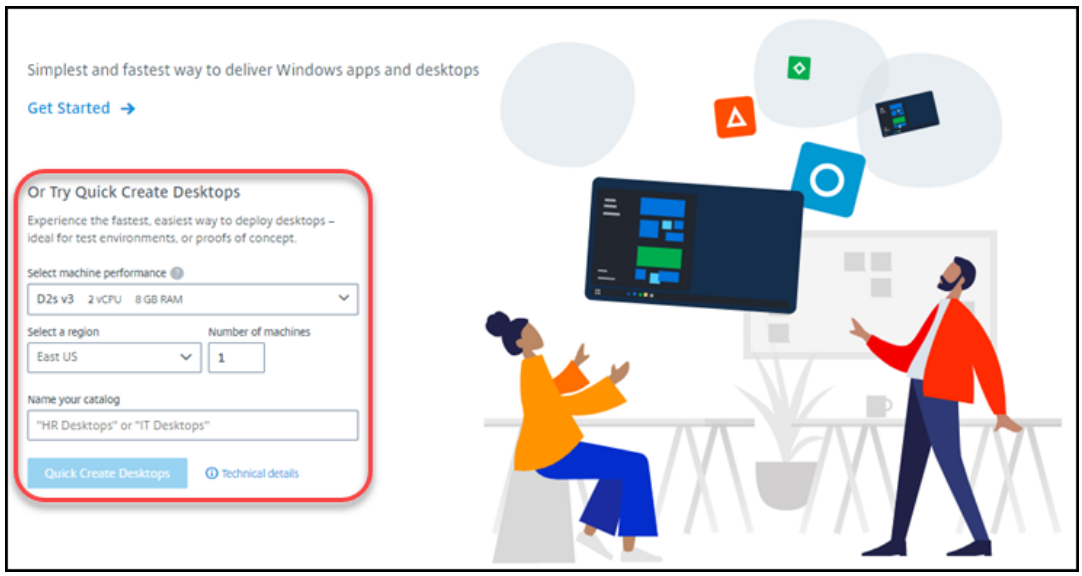
> **Importante:**
>
> Quando si crea un catalogo (o un'immagine) utilizzando una sottoscrizione Citrix Managed Azure per la prima volta, viene richiesto di riconoscere la propria responsabilità per gli addebiti sostenuti e di acconsentirvi. I promemoria di tale consenso possono essere visualizzati anche quando si creano altri cataloghi o immagini utilizzando la sottoscrizione Citrix Managed Azure.

### Creare un catalogo Quick Deploy (Distribuzione rapida) utilizzando Quick create (Creazione rapida)

Il metodo Quick create (Creazione rapida) utilizza una sottoscrizione Citrix Managed Azure e un'immagine Windows 10 preparata da Citrix per creare un catalogo contenente macchine statiche. Le impostazioni di gestione dell'alimentazione utilizzano i valori preimpostati di Cost Saver (Risparmio sui costi). Non è presente alcuna connessione alla rete aziendale. Gli utenti devono essere aggiunti utilizzando Citrix Managed Azure AD.

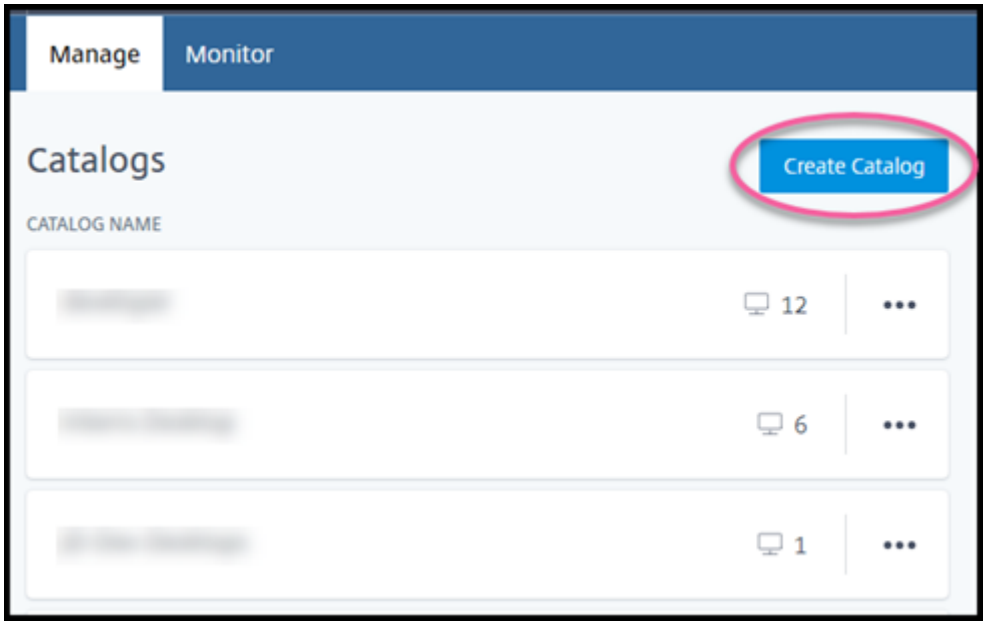
1. Accedere a Citrix Cloud.
2. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
3. Selezionare **Manage > Quick Deploy** (Gestisci > Distribuzione rapida).
4. Se un catalogo non è ancora stato creato, si verrà indirizzati alla pagina **Welcome** (Benvenuto). Scegliere una delle seguenti opzioni:
    - Configurare il catalogo in questa pagina. Continuare con i passaggi da 6 a 10.



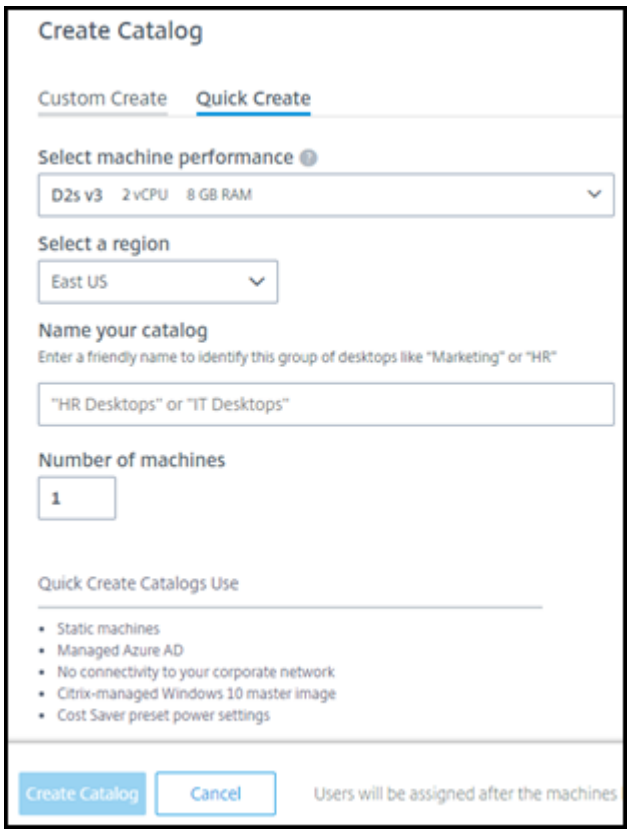

- Selezionare **Get Started** (Inizia). Si verrà indirizzati alla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida). Selezionare **Create Catalog** (Crea catalogo).

5. Se un catalogo è già stato creato (e se ne sta creando un altro), si verrà indirizzati alla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida). Selezionare **Create Catalog** (Crea catalogo).




6. Selezionare **Quick Create** (Creazione rapida) nella parte superiore della pagina, se l'opzione non è già selezionata.




- **Machine performance** (Prestazioni macchina): selezionare il tipo di macchina. Ogni scelta ha una combinazione unica di CPU, RAM e archiviazione. Le macchine con prestazioni più elevate hanno costi mensili più elevati.
- **Region** (Regione): selezionare una regione in cui si desidera creare le macchine. È possibile selezionare una regione vicina ai propri utenti.
- **Name** (Nome): digitare un nome per il catalogo. Questo campo è obbligatorio e non è presente alcun valore predefinito.
- **Number of machines** (Numero di macchine): digitare il numero di macchine desiderato.

7. Al termine, selezionare **Create Catalog** (Crea catalogo). (se si sta creando il primo catalogo dalla pagina **Welcome** [Benvenuto], selezionare **Quick Create Desktops** [Creazione rapida di desktop]).
8. Se questo è il primo catalogo che si sta creando utilizzando una sottoscrizione Citrix Managed Azure, riconoscere la propria responsabilità per gli addebiti correlati quando richiesto.

Durante la creazione del catalogo, il nome del catalogo viene aggiunto all'elenco dei cataloghi, indicandone lo stato di avanzamento durante la creazione.

Inoltre, Citrix DaaS crea automaticamente una posizione risorsa e aggiunge due Citrix Cloud Connector.

Passi successivi:

- È possibile aggiungere utenti alla directory Managed Azure AD durante la creazione del catalogo.
- Dopo aver creato il catalogo, aggiungere utenti al catalogo.

### Creare un catalogo Quick Deploy (Distribuzione rapida) utilizzando Custom create (Creazione personalizzata)

Se si utilizza una sottoscrizione Citrix Managed Azure e si prevede di utilizzare una connessione alle risorse di rete on-premise, creare la connessione di rete prima di creare il catalogo. Per consentire agli utenti di accedere alle risorse on-premise o ad altre risorse di rete, sono necessarie anche le informazioni di Active Directory per quella posizione.

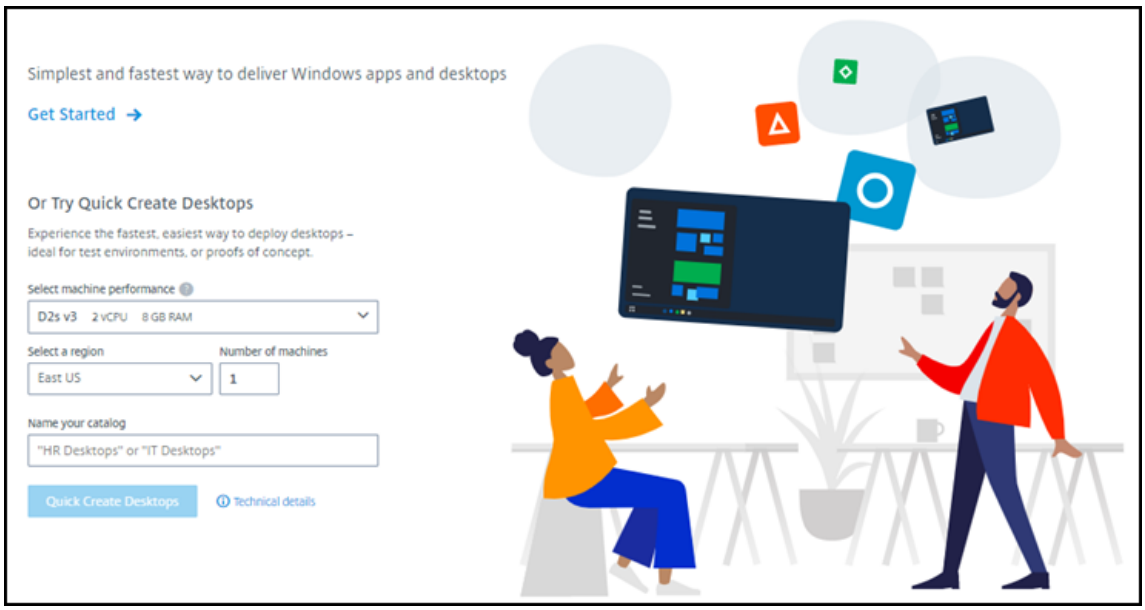
Se non si dispone di una sottoscrizione Citrix Managed Azure, è possibile:

- Ordinare l'Azure Consumption Fund tramite Azure Marketplace, che fornisce una sottoscrizione Citrix Managed Azure.
- Importare (aggiungere) una o più delle proprie sottoscrizioni di Azure a Citrix DaaS prima di creare un catalogo.

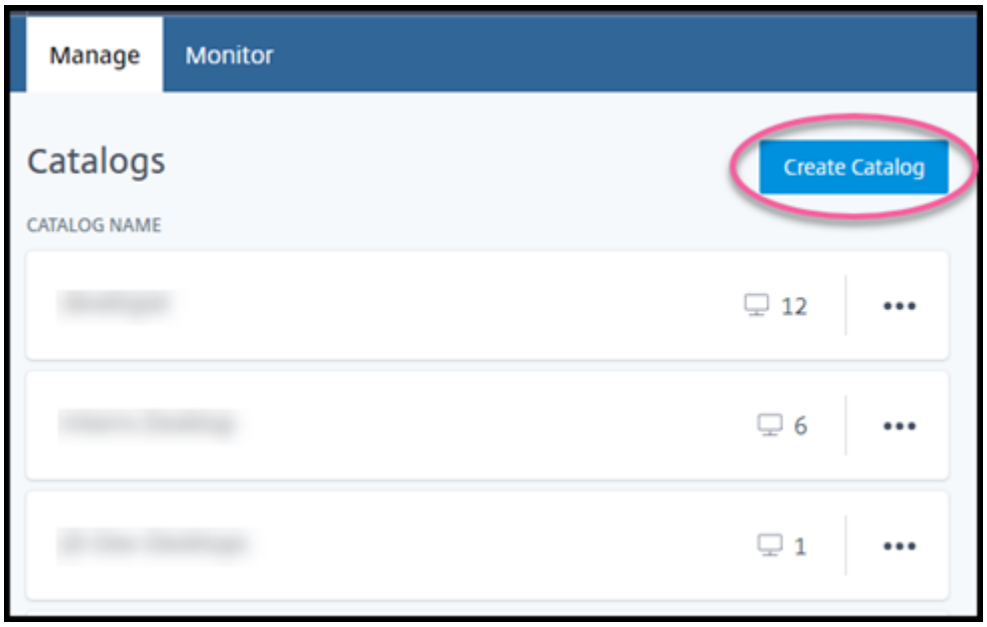
Per creare un catalogo:

1. Accedere a Citrix Cloud.
2. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
3. Selezionare **Manage > Quick Deploy** (Gestisci > Distribuzione rapida).
4. Se un catalogo non è ancora stato creato, si verrà indirizzati alla pagina **Welcome** (Benvenuto). Selezionare **Get Started** (Inizia). Alla fine della pagina introduttiva, si verrà indirizzati alla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida). Selezionare **Create Catalog** (Crea catalogo).

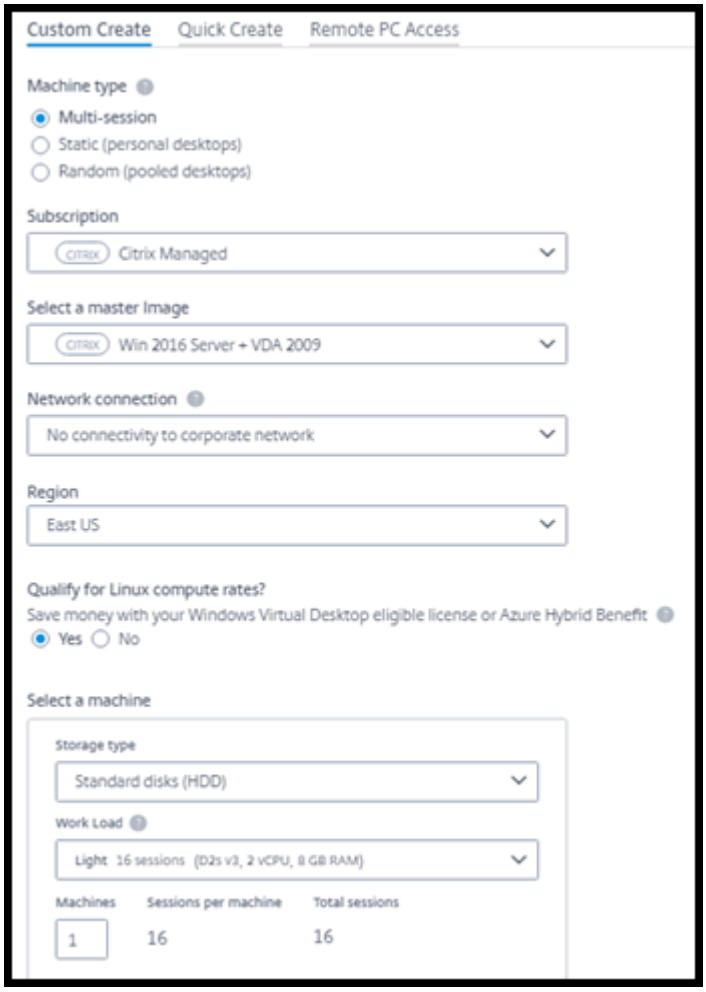



Se un catalogo è già stato creato, si verrà indirizzati alla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida). Selezionare **Create Catalog** (Crea catalogo).




5. Selezionare **Custom Create** (Creazione personalizzata) nella parte superiore della pagina, se non è già selezionata.




6. Compilare i seguenti campi (alcuni campi sono validi solo per determinati tipi di macchine. L'ordine dei campi potrebbe essere diverso).

   - **Machine type** (Tipo di macchina). Selezionare un tipo di macchina. Per i dettagli, vedere Tipi di macchine.
   - **Subscription** (Sottoscrizione). Selezionare una sottoscrizione di Azure.
   - **Master image** (Immagine master): selezionare un'immagine del sistema operativo da utilizzare per le macchine del catalogo.
   - **Network connection** (Connessione di rete): selezionare la connessione di rete da utilizzare per accedere alle risorse della rete.

     Se è stata selezionata una sottoscrizione Citrix Managed Azure, le opzioni disponibili sono:

     - **No Connectivity** (Nessuna connettività): gli utenti non possono accedere a posizioni e risorse sulla rete aziendale on-premise.
     - *Connections* (Connessioni): selezionare una connessione creata in precedenza, ad esempio una connessione di peering della rete virtuale o SD-WAN.

Se è stata selezionata una sottoscrizione di Azure gestita dal cliente, selezionare il gruppo di risorse, la rete virtuale e la subnet appropriati.

- **Region** (Regione): (disponibile solo se è stata selezionata l'opzione **No Connectivity** [Nessuna connettività] in **Network connection** [Connessione di rete]). Selezionare un'area in cui si desidera creare i desktop. È possibile selezionare una regione vicina ai propri utenti.

  Se è stata selezionata una connessione in **Network connection** (Connessione di rete), il catalogo utilizza la regione di quella rete.

- **Qualify for Linux compute rates?** (Qualifica per le tariffe di calcolo Linux?) (disponibile solo se è stata selezionata un'immagine Windows). È possibile risparmiare utilizzando la propria licenza idonea o il Vantaggio Azure Hybrid.

  **Windows Virtual Desktop benefit** (Vantaggio Windows Virtual Desktop): licenze idonee Windows 10 o Windows 7 per utente per:

  - Microsoft 365 E3/ES
  - Vantaggi per l'uso di Microsoft 365 A3/AS/Student
  - Microsoft 365 F3
  - Microsoft 365 Business Premium
  - Windows 10 Enterprise E3/E5
  - Windows 10 Education A3/A5
  - Windows 10 VDA per utente

  Licenza CAL Servizi Desktop remoto per utente o per dispositivo con Software Assurance per carichi di lavoro Windows Server.

  **Azure Hybrid benefit** (Vantaggio Azure Hybrid): licenze Windows Server con Software Assurance attivo o licenze di sottoscrizione idonee equivalenti. Vedere https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Machine** (Macchina):

  - **Storage type** (Tipo di archiviazione): HDD o SSD.
  - **Machine performance** (Prestazioni macchina) (per tipo di macchina **statica** o **casuale**) o **Workload** (Carico di lavoro) (per tipo di macchina multisessione). Le scelte includono solo le opzioni che corrispondono al tipo di generazione (gen1 o gen2) dell'immagine selezionata.

    Se si seleziona il carico di lavoro personalizzato, immettere il numero di macchine e sessioni per macchina nel campo **Machine Performance** (Prestazioni macchina).
  - **Machines** (Macchine). Quante macchine si desiderano in questo catalogo.

- **Machine naming scheme** (Schema di denominazione macchina): vedere Schema di denominazione delle macchine.

- **Name** (Nome): digitare un nome per il catalogo. Questo nome viene visualizzato nella dashboard **Manage** (Gestisci).
- **Power schedule** (Pianificazione alimentazione): per impostazione predefinita, la casella di controllo **I'll configure this later** (Da configurare in seguito) è selezionata. Per i dettagli, vedere Pianificazioni di gestione dell'alimentazione (questa pianificazione di gestione dell'alimentazione è diversa dalle funzionalità di gestione dell'alimentazione disponibili nell'interfaccia di gestione Full Configuration [Configurazione completa] di Citrix DaaS).
- **Join the local Active Directory domain** (Aggiungi al dominio Active Directory locale): (disponibile solo se è stata selezionata una connessione di peering della rete virtuale di Azure in **Network connection** [Connessione di rete]). Selezionare **Yes** (Sì) o **No**. Se si seleziona **Yes** (Sì), immettere:
  - Nome di dominio completo del dominio (ad esempio, Contoso.com).
  - Unità organizzativa: per utilizzare l'unità organizzativa predefinita (Computer), lasciare vuoto questo campo.
  - Nome account Citrix Daas: deve essere un amministratore di dominio o aziendale nel formato nome@dominio o dominio\nome.
  - Password per il nome dell'account Citrix DaaS.
- **Advanced settings** (Impostazioni avanzate): consultare Impostazioni della posizione risorsa durante la creazione di un catalogo.

7. Al termine, selezionare **Create Catalog** (Crea catalogo).
8. Se questo è il primo catalogo che si sta creando utilizzando una sottoscrizione Citrix Managed Azure, riconoscere la propria responsabilità per gli addebiti correlati quando richiesto.

La dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida) indica quando viene creato il catalogo. Inoltre, Citrix DaaS crea automaticamente una posizione risorsa e aggiunge due Citrix Cloud Connector.

Passi successivi:

- Se non lo si è già fatto, configurare il metodo di autenticazione per consentire agli utenti di autenticarsi su Citrix Workspace.
- Dopo aver creato il catalogo, aggiungere utenti al catalogo.
- Se è stato creato un catalogo multisessione, aggiungere le applicazioni (prima o dopo l'aggiunta di utenti).

### Impostazioni della posizione risorsa durante la creazione di un catalogo

Quando si crea un catalogo, è possibile configurare facoltativamente diverse impostazioni della posizione risorsa.

Quando si seleziona **Advanced settings** (Impostazioni avanzate) nella finestra di dialogo di creazione del catalogo, Citrix DaaS recupera le informazioni sulla posizione risorsa.

- Se si dispone già di una posizione risorsa per il dominio e la connessione di rete selezionati per il catalogo, è possibile salvarla perché venga utilizzata dal catalogo che si sta creando.

  Se tale posizione risorsa ha un solo Cloud Connector, ne viene installato un altro automaticamente. Facoltativamente, è possibile specificare le impostazioni avanzate per il Cloud Connector che si sta aggiungendo.
- Se non si dispone di una posizione risorsa impostata per il dominio e la connessione di rete selezionati per il catalogo, viene richiesto di configurarne una.

Configurare le impostazioni avanzate:

- (richieste solo quando la posizione risorsa è già configurata). Un nome per la posizione risorsa.
- Tipo di connettività esterna: tramite il servizio Citrix Gateway o dall'interno della rete aziendale.
- Impostazioni Cloud Connector:
  - (disponibile solo quando si utilizza una sottoscrizione di Azure gestita dal cliente) Machine performance (Prestazioni macchina). Questa selezione viene utilizzata per i Cloud Connector nella posizione risorsa.
  - (disponibile solo quando si utilizza una sottoscrizione di Azure gestita dal cliente) Azure resource group (Gruppo di risorse di Azure). Questa selezione viene utilizzata per i Cloud Connector nella posizione risorsa. L'impostazione predefinita è l'ultimo gruppo di risorse utilizzato dalla posizione risorsa (se applicabile).
  - Unità organizzativa (OU). L'impostazione predefinita è l'ultima unità organizzativa utilizzata dalla posizione risorsa (se applicabile).

Una volta configurate le impostazioni avanzate, selezionare **Save** (Salva) per tornare alla finestra di dialogo di creazione del catalogo.

Dopo aver creato un catalogo, sono disponibili diverse azioni relative alla posizione risorsa. Per i dettagli, consultare Azioni relative alla posizione risorsa.

### Schema di denominazione delle macchine

Per specificare uno schema di denominazione delle macchine durante la creazione di un catalogo, selezionare **Specify machine naming scheme** (Specifica schema di denominazione delle macchine).

Utilizzare da 1 a 4 caratteri jolly (marcatori hash) per indicare dove compaiono numeri o lettere sequenziali nel nome. Regole:

- Lo schema di denominazione deve contenere almeno un carattere jolly, ma non più di quattro caratteri jolly. Tutti i caratteri jolly devono essere uniti.
- Il nome completo, inclusi i caratteri jolly, deve essere compreso tra 2 e 15 caratteri.
- Un nome non può includere spazi vuoti (spazi), barre, barre rovesciate, due punti, asterischi, parentesi uncinate, barre verticali, virgole, tilde, punti esclamativi, simboli di chiocciola, simboli di dollaro, segni di percentuale, accenti circonflessi, parentesi, parentesi graffe o caratteri di sottolineatura.
- Un nome non può iniziare con un punto.
- Un nome non può contenere solo numeri.
- Non utilizzare le seguenti lettere alla fine di un nome: `-GATEWAY`, `-GW` e `-TAC`.

Indicare se i valori sequenziali sono numeri (0-9) o lettere (A-Z).

Ad esempio, uno schema di denominazione `PC-Sales-##` (con **0-9** selezionato) genera account computer denominati `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03` e così via.

Lasciare spazio sufficiente per l'espansione.

- Ad esempio, uno schema di denominazione con 2 caratteri jolly e altri 13 caratteri (ad esempio, `MachineSales-##`) utilizza il numero massimo di caratteri (15).
- Quando il catalogo arriva a contenere 99 macchine, la creazione della macchina successiva non riesce. Citrix DaaS tenta di creare una macchina con tre cifre (100), ma ciò creerebbe un nome con 16 caratteri. Il massimo è 15.
- Quindi, in questo esempio, un nome più breve (ad esempio `PC-Sales-##`) consente di espandersi oltre 99 macchine.

Se non si specifica uno schema di denominazione delle macchine, Citrix DaaS utilizza lo schema di denominazione predefinito `DAS%%%%%-**-###`.

- `%%%%%` = cinque caratteri alfanumerici casuali corrispondenti al prefisso della posizione risorsa
- `**` = due caratteri alfanumerici casuali per il catalogo
- `###` = tre cifre

### Informazioni correlate

- Cataloghi Remote PC Access (Accesso remoto PC)
- Creare un catalogo in una rete che utilizza un server proxy
- Visualizzare le informazioni del catalogo
- Gestire i cataloghi in Quick Deploy (Distribuzione rapida)

# Gestire i cataloghi in Quick Deploy (Distribuzione rapida)

October 6, 2022

In questo articolo vengono descritte le attività di gestione del catalogo che è possibile utilizzare per gestire i cataloghi creati in Quick Deploy (Distribuzione rapida).

Tenere presente che se è stato utilizzato Quick Deploy (Distribuzione rapida) per creare un catalogo e successivamente si utilizza l'interfaccia Full Configuration (Configurazione completa) per eseguire attività di gestione su tale catalogo, non è più possibile utilizzare l'interfaccia Quick Deploy (Distribuzione rapida) per quel catalogo

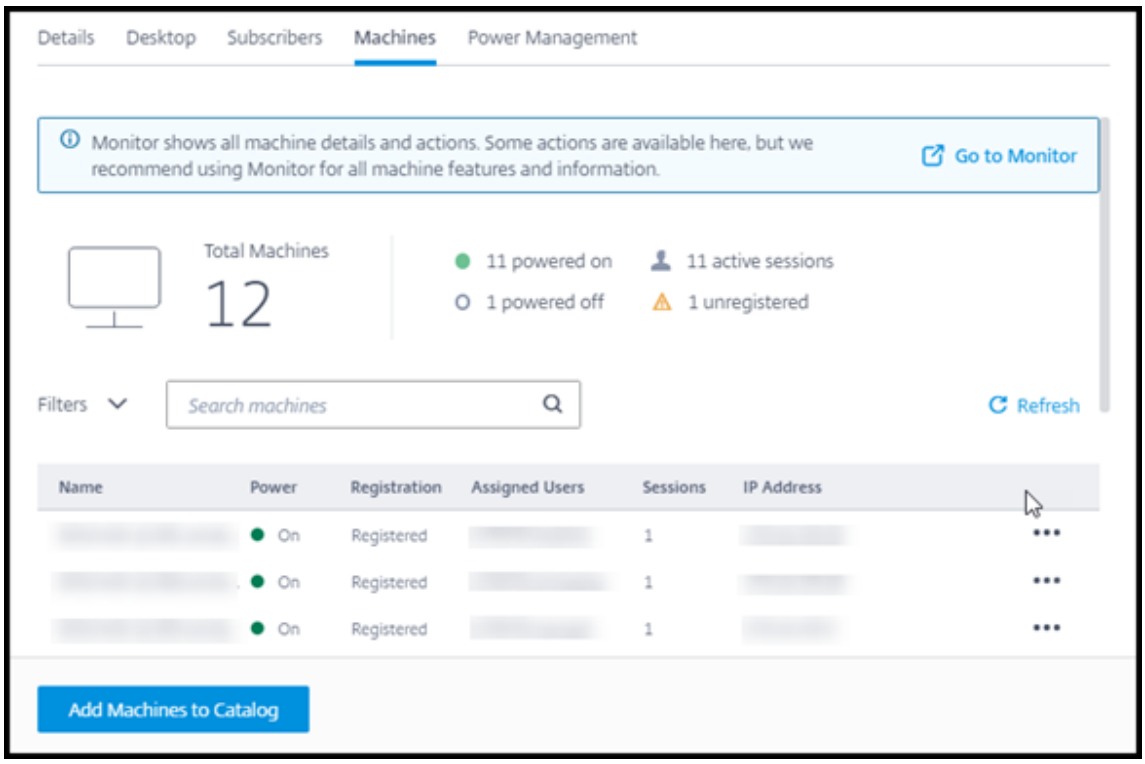
(per informazioni sulla gestione dei cataloghi nell'interfaccia di gestione Full Configuration [Configurazione completa], vedere Gestire i cataloghi delle macchine).

## Aggiungere macchine a un catalogo

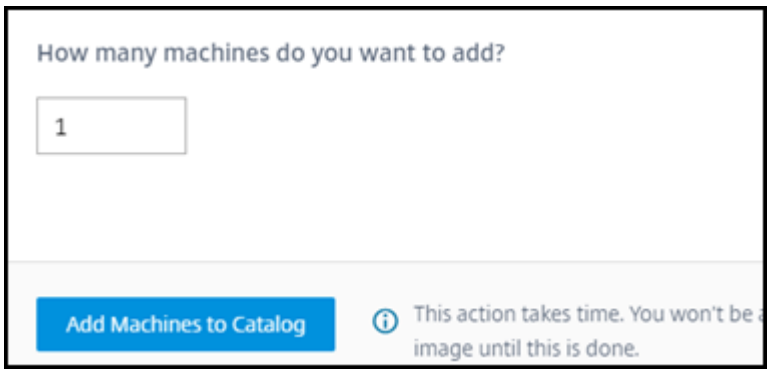
Mentre le macchine vengono aggiunte a un catalogo Quick Deploy (Distribuzione rapida), non è possibile apportare altre modifiche a tale catalogo.

1. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Machines** (Macchine), selezionare **Add Machines to Catalog** (Aggiungi macchine al catalogo).




3. Immettere il numero di macchine che si desidera aggiungere al catalogo.




4. (valido solo se il catalogo è aggiunto a un dominio). Digitare il nome utente e la password per l'account Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops).
5. Selezionare **Add Machines to Catalog** (Aggiungi macchine al catalogo).

Non è possibile ridurre il numero di macchine per un catalogo. Tuttavia, è possibile utilizzare le impostazioni di pianificazione della gestione dell'alimentazione per controllare il numero di macchine accese o eliminare singole macchine dalla scheda **Machines** (Macchine). Vedere Gestire le macchine in un catalogo per informazioni sull'eliminazione delle macchine dalla scheda **Machines** (Macchine).

### Modificare il numero di sessioni per macchina

La modifica del numero di sessioni per macchina multisessione può influire sull'esperienza degli utenti. L'aumento di questo valore può ridurre le risorse di elaborazione allocate alle sessioni simultanee.

Consiglio: osservare i dati di utilizzo per determinare il giusto equilibrio tra esperienza utente e costi.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), selezionare un catalogo contenente macchine multisessione.
2. Nella scheda **Details** (Dettagli), selezionare **Edit** (Modifica) accanto a **Sessions per Machine** (Sessioni per macchina).
3. Immettere un nuovo numero di sessioni per macchina.
4. Selezionare **Update Number of Sessions** (Aggiorna numero di sessioni).
5. Confermare la richiesta.

Questa modifica non influisce sulle sessioni correnti. Quando si modifica il numero massimo di sessioni impostandolo su un valore inferiore alle sessioni attualmente attive di una macchina, il nuovo valore viene implementato attraverso la normale riduzione delle sessioni attive.

Se si verifica un errore prima dell'inizio del processo di aggiornamento, la visualizzazione **Details** (Dettagli) del catalogo mantiene il numero corretto di sessioni. Se si verifica un errore durante il processo di aggiornamento, la visualizzazione indica il numero di sessioni desiderate.

### Gestire le macchine in un catalogo

> **Nota:**
>
> Molte delle azioni disponibili in **Manage > Quick Deploy** (Gestisci > Distribuzione rapida) sono disponibili anche nella scheda **Monitor** (Monitoraggio) in Quick Deploy (Distribuzione rapida).

Per selezionare le azioni da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida):

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi di una voce del catalogo.
2. Nella scheda **Machines** (Macchine), individuare la macchina che si desidera gestire. Nel menu con i puntini di sospensione per quella macchina, selezionare l'azione desiderata:
   - **Restart** (Riavvia): riavvia la macchina selezionata.
   - **Start** (Avvia): avvia la macchina selezionata. Questa azione è disponibile solo se la macchina è spenta.

- **Shutdown** (Arresta): spegne la macchina selezionata. Questa azione è disponibile solo se la macchina è accesa.
- **Turn maintenance mode on/off** (Attiva/disattiva modalità di manutenzione): attiva (se è disattivata) o disattiva (se è attivata) la modalità di manutenzione per la macchina selezionata. Per impostazione predefinita, la modalità di manutenzione è disattivata per una macchina.

  L'attivazione della modalità di manutenzione impedisce la creazione di nuove connessioni a tale macchina. Gli utenti possono connettersi alle sessioni esistenti su tale macchina, ma non possono avviare nuove sessioni su di essa.

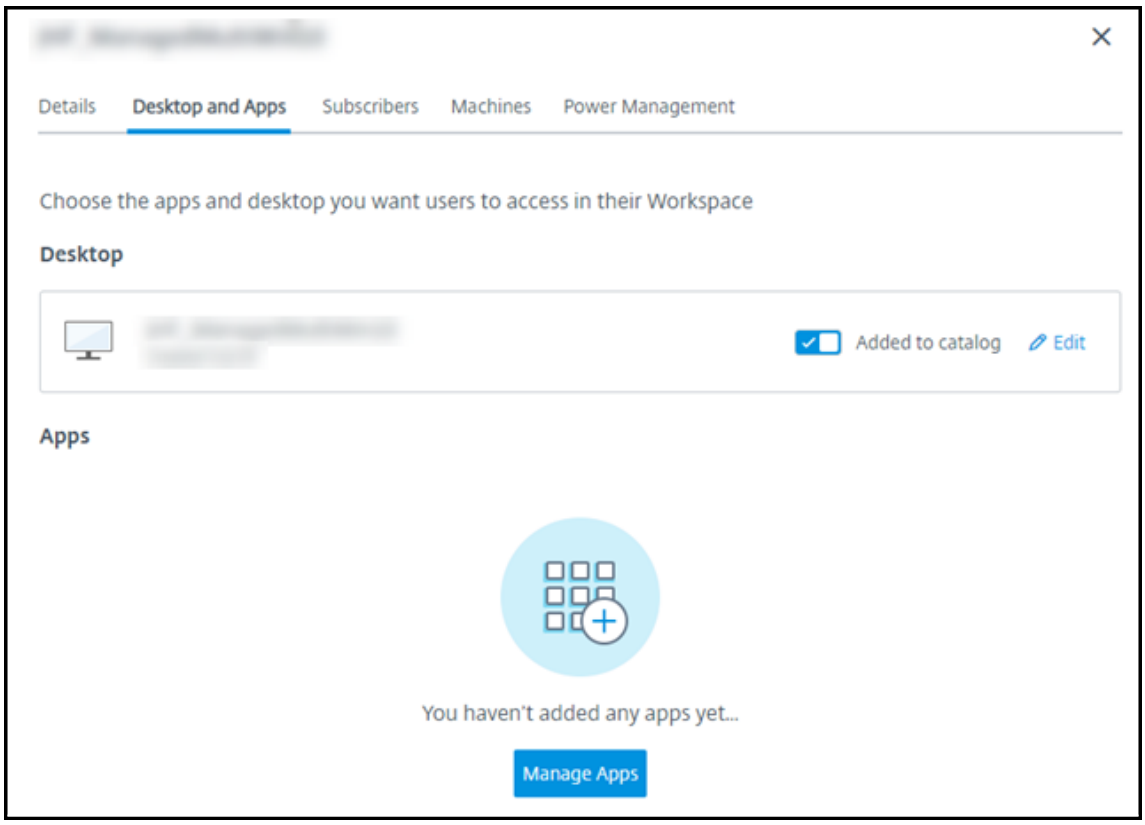
  Si potrebbe voler mettere una macchina in modalità di manutenzione prima di applicare le patch o per la risoluzione dei problemi.
- **Delete** (Elimina): elimina la macchina selezionata. Questa azione è disponibile solo quando il conteggio delle sessioni della macchina è zero. Confermare l'eliminazione.

  Quando una macchina viene eliminata, tutti i dati sulla macchina vengono rimossi.
- **Force restart** (Avvio forzato): forza il riavvio della macchina selezionata. Selezionare questa azione solo se un'azione **Restart** (Riavvia) per la macchina non riesce.

### Aggiungere app a un catalogo

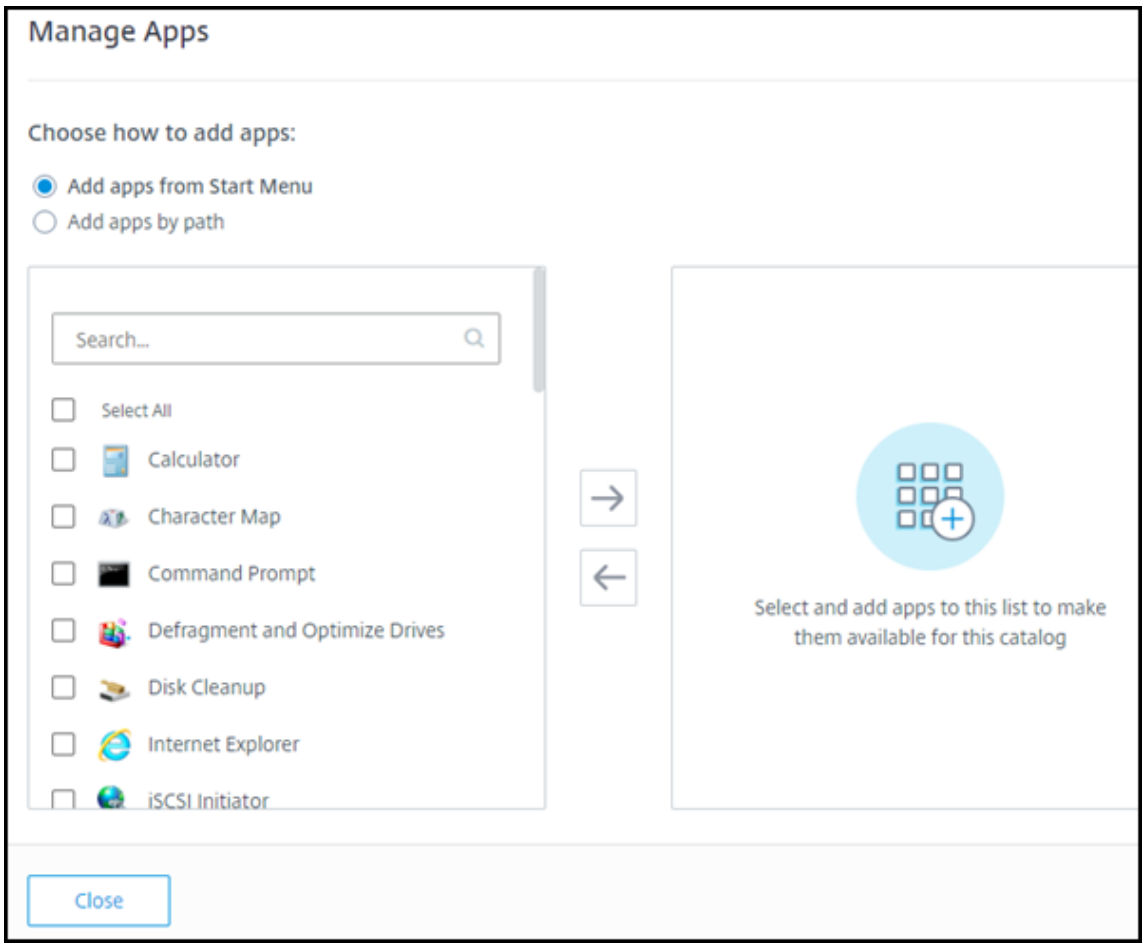
1. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Desktop and Apps** (Desktop e app), selezionare **Manage Apps** (Gestisci app).




3. Selezionare la modalità di aggiunta delle app: dal menu **Start** delle macchine nel catalogo o da un percorso diverso sulle macchine.
4. Per aggiungere app dal menu **Start**:

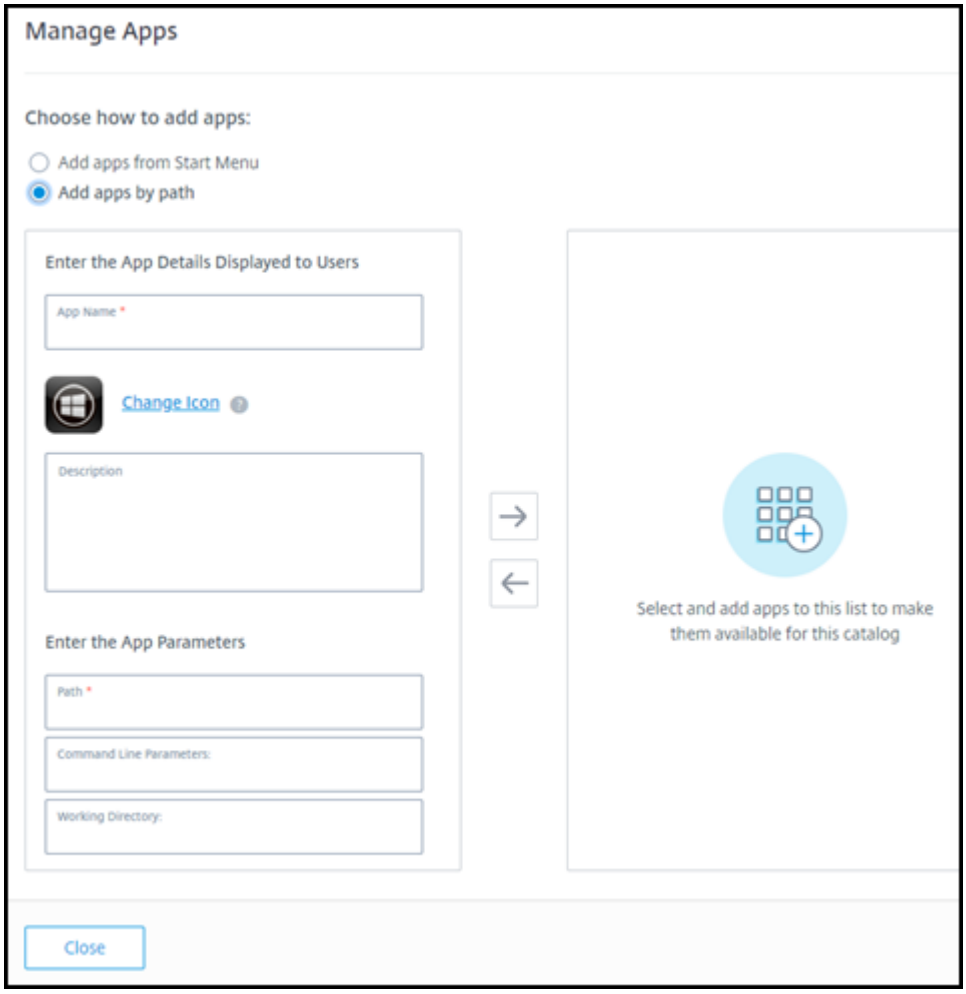
 




- Selezionare le app disponibili nella colonna di sinistra (utilizzare **Search** [Cerca] per personalizzare l'elenco delle app). Selezionare la freccia destra tra le colonne. Le app selezionate vengono spostate nella colonna di destra.
- Allo stesso modo, per rimuovere le app, selezionarle nella colonna di destra. Selezionare la freccia sinistra tra le colonne.
- Se il menu **Start** contiene più di una versione della stessa app, con lo stesso nome, è possibile aggiungerne solo una. Per aggiungere un'altra versione di quell'app, modificare quella versione per cambiarne il nome. È quindi possibile aggiungere quella versione dell'app.

5. Per aggiungere app in base al percorso:




- Immettere il nome dell'app. Questo è il nome che gli utenti vedono in Citrix Workspace.
- L'icona visualizzata è l'icona visualizzata dagli utenti in Citrix Workspace. Per selezionare un'altra icona, selezionare **Change icon** (Cambia icona) e individuare l'icona che si desidera visualizzare.
- (Facoltativo) Immettere una descrizione dell'applicazione.
- Inserire il percorso dell'app. Questo campo è obbligatorio. Facoltativamente, aggiungere i parametri della riga di comando e la directory di lavoro. Per informazioni dettagliate sui parametri della riga di comando, consultare Trasferire i parametri alle applicazioni pubblicate.

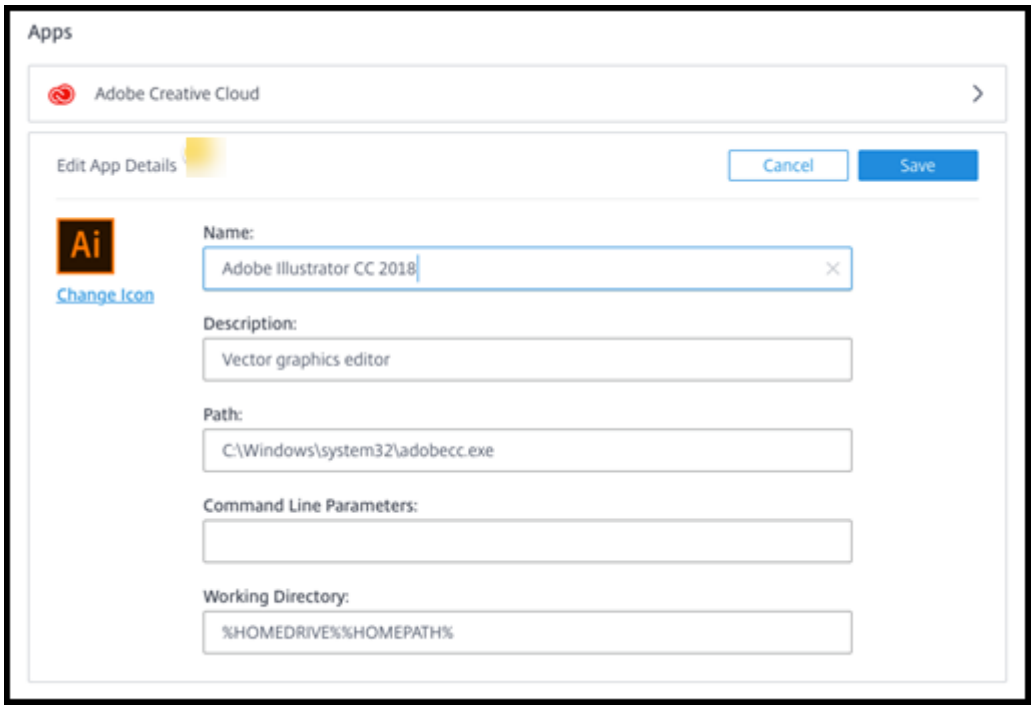
6. Al termine, selezionare **Close** (Chiudi).

Nei VDA Windows Server 2019, alcune icone delle applicazioni potrebbero non essere visualizzate correttamente durante la configurazione e nell'area di lavoro degli utenti. Come soluzione alternativa, dopo la pubblicazione dell'app, modificare l'app e utilizzare la funzione **Change icon** (Cambia icona) per assegnare un'icona diversa che viene visualizzata correttamente.

### Modificare un'app in un catalogo

1. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Desktop and Apps** (Desktop e app), fare clic in un punto qualsiasi della riga contenente l'app che si desidera modificare.
3. Selezionare l'icona della matita.




4. Digitare le modifiche in uno dei seguenti campi:
   - **Nome:** il nome visualizzato dagli utenti in Citrix Workspace.
   - **Descrizione**
   - **Path** (Percorso): il percorso del file eseguibile.
   - **Command line parameters** (Parametri della riga di comando): per i dettagli, consultare Trasferire i parametri alle applicazioni pubblicate.
   - **Directory di lavoro**
5. Per modificare l'icona visualizzata dagli utenti in Citrix Workspace, selezionare **Change icon** (Cambia icona) e individuare l'icona che si desidera visualizzare.
6. Al termine, selezionare **Save** (Salva).

#### Passare parametri alle applicazioni pubblicate

Quando si associa un'applicazione pubblicata a tipi di file, i simboli di percentuale e dell'asterisco (tra virgolette) vengono aggiunti alla fine della riga di comando. Questi simboli fungono da segnaposto per i parametri passati ai dispositivi utente.

- Se un'applicazione pubblicata non viene avviata quando è previsto, verificare che la riga di comando contenga i simboli corretti. Per impostazione predefinita, i parametri forniti dai dispositivi utente vengono convalidati quando vengono aggiunti i simboli.

  Per le applicazioni pubblicate che utilizzano parametri personalizzati forniti dal dispositivo utente, vengono aggiunti i simboli alla riga di comando per ignorare la convalida della riga di comando. Se questi simboli non sono presenti in una riga di comando per l'applicazione, aggiungerli manualmente.

- Se il percorso del file eseguibile include nomi di directory con spazi (ad esempio `"C:\Program Files"`), racchiudere la riga di comando dell'applicazione tra virgolette per indicare che lo spazio appartiene alla riga di comando. Aggiungere virgolette attorno al percorso e un'altra coppia di virgolette attorno ai simboli di percentuale e dell'asterisco. Aggiungere uno spazio tra le virgolette di chiusura per il percorso e le virgolette di apertura per i simboli di percentuale e dell'asterisco.

  Ad esempio, la riga di comando per l'applicazione pubblicata Windows Media Player è: `"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"`

### Rimuovere le app da un catalogo

La rimozione di un'app da un catalogo non rimuove l'app dalle macchine. Impedisce semplicemente che appaia in Citrix Workspace.

1. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Desktop and Apps** (Desktop e app), selezionare l'icona del cestino accanto alle app che si desidera rimuovere.

### Eliminare un catalogo

Quando si elimina un catalogo, tutte le macchine nel catalogo vengono distrutte in modo permanente. L'eliminazione di un catalogo non può essere annullata.

1. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo.

2. Nella scheda **Details** (Dettagli), selezionare **Delete Catalog** (Elimina catalogo).
3. Confermare l'eliminazione.

Per identificare gli account delle macchine Active Directory residui che è necessario eliminare, è possibile scaricare un elenco di nomi di macchine e Cloud Connector.

## Gestire le pianificazioni di gestione dell'alimentazione

Una pianificazione di gestione dell'alimentazione riguarda tutte le macchine in un catalogo. Una pianificazione prevede:

- Esperienza utente ottimale: le macchine sono disponibili per gli utenti quando sono necessarie.
- Sicurezza: le sessioni desktop che rimangono inattive per un intervallo specificato vengono disconnesse, richiedendo agli utenti di avviare una nuova sessione nella propria area di lavoro.
- Gestione dei costi e risparmio energetico: le macchine con desktop che rimangono inattivi vengono spente. Le macchine vengono accese per soddisfare la domanda programmata ed effettiva.

È possibile configurare una pianificazione dell'alimentazione quando si crea un catalogo personalizzato o in un secondo momento. Se non viene selezionata o configurata alcuna pianificazione, una macchina si spegne al termine di una sessione.

Non è possibile selezionare o configurare una pianificazione dell'alimentazione quando si crea un catalogo con Quick Create (Creazione rapida). Per impostazione predefinita, i cataloghi Quick create (Creazione rapida) utilizzano la pianificazione preimpostata Cost Saver (Risparmio sui costi). È possibile selezionare o configurare una pianificazione diversa in un secondo momento per quel catalogo.

La gestione della pianificazione include:

- Conoscenza delle informazioni contenute in una pianificazione
- Creazione di una pianificazione

### Informazioni in una pianificazione

Il diagramma seguente mostra le impostazioni di pianificazione per un catalogo contenente macchine multisessione. Le impostazioni per un catalogo contenente macchine a sessione singola (casuali o statiche) differiscono leggermente.


Una pianificazione di gestione dell'alimentazione contiene le seguenti informazioni.

**Preset schedules (Pianificazioni preimpostate)** Citrix DaaS offre diverse pianificazioni preimpostate. È inoltre possibile configurare e salvare pianificazioni personalizzate. Sebbene sia possibile eliminare i set di impostazioni personalizzati, non è possibile eliminare i set di impostazioni forniti da Citrix.

**Time zone (Fuso orario)** Utilizzato con l'impostazione di accensione delle macchine per stabilire le ore di lavoro e le ore non lavorative, in base al fuso orario selezionato.

Questa impostazione è valida per tutti i tipi di macchine.

**Power on machines: Work hours and after hours (Accensione delle macchine: ore di lavoro e ore non lavorative)** I giorni della settimana e le ore di inizio e fine del giorno che formano l'orario di lavoro. Questo generalmente indica gli intervalli in cui si desidera che le macchine siano accese. Qualsiasi orario al di fuori di tali intervalli è considerato un orario non lavorativo. Diverse impostazioni di pianificazione consentono di inserire valori separati per le ore di lavoro e le ore non lavorative. Si applicano continuamente altre impostazioni.

Questa impostazione è valida per tutti i tipi di macchine.

**Disconnect desktop sessions when idle (Disconnetti le sessioni desktop quando sono inattive)** Il periodo di tempo per cui un desktop può rimanere inattivo (non utilizzato) prima che la sessione venga disconnessa. Dopo la disconnessione di una sessione, l'utente deve accedere a Workspace e avviare nuovamente un desktop. Questa è un'impostazione di sicurezza.

Questa impostazione è valida per tutti i tipi di macchine. Si applica sempre un'unica impostazione.

**Power off idle desktops (Spegni i desktop inattivi)** Il periodo di tempo per cui una macchina può rimanere scollegata prima di essere spenta. Dopo lo spegnimento di una macchina, l'utente deve accedere a Workspace e avviare nuovamente un desktop. Questa è un'impostazione per il risparmio energetico.

Ad esempio, supponiamo che si desideri che i desktop si disconnettano dopo 10 minuti di inattività. Quindi, spegnere le macchine se rimangono scollegate per altri 15 minuti.

Se Tommaso smette di usare il suo desktop e si allontana per una riunione di un'ora, il desktop verrà disconnesso dopo 10 minuti. Dopo altri 15 minuti, la macchina verrà spenta (25 minuti totali).

Dal punto di vista dell'utente, le due impostazioni di inattività (disconnessione e spegnimento) hanno lo stesso effetto. Se Tommaso rimane lontano dal suo desktop per 12 minuti o un'ora, deve riavviare un desktop da Workspace. La differenza tra i due timer influisce sullo stato della macchina virtuale che fornisce il desktop.

Questa impostazione è valida per macchine a sessione singola (statiche o casuali). È possibile immettere valori per le ore lavorative e le ore non lavorative.

**Log off disconnected sessions (Disconnetti le sessioni disconnesse)** Il periodo di tempo per cui una macchina può rimanere disconnessa prima della chiusura della sessione.

Questa impostazione è valida per le macchine multisessione. Si applica sempre un'unica impostazione.

**Power-off delay (Ritardo di spegnimento)** La quantità minima di tempo per cui una macchina deve essere accesa prima di essere idonea allo spegnimento (insieme ad altri criteri). Questa impostazione evita che le macchine si accendano e si spengano a intermittenza durante le richieste di sessione mutevoli.

Questa impostazione è valida per le macchine multisessione e si applica continuamente.

**Minimum running machines (Numero minimo di macchine in esecuzione)** Il numero di macchine che devono rimanere accese, indipendentemente da quanto tempo rimangono inattive o disconnesse.

Questa impostazione è valida per le macchine casuali e multisessione. È possibile immettere valori per le ore lavorative e le ore non lavorative.

**Capacity buffer (Buffer di capacità)** Un buffer di capacità aiuta ad affrontare picchi improvvisi della domanda, mantenendo un buffer di macchine accese. Il buffer viene specificato come percentuale della domanda di sessione corrente. Ad esempio, se ci sono 100 sessioni attive e il buffer di capacità è del 10%, Citrix DaaS fornisce capacità per 110 sessioni. Potrebbe verificarsi un picco della domanda durante l'orario di lavoro o l'aggiunta di nuove macchine al catalogo.

Un valore inferiore riduce il costo. Un valore più elevato aiuta a garantire un'esperienza utente ottimizzata. Quando si avviano le sessioni, gli utenti non devono attendere l'accensione di macchine aggiuntive.

In presenza di una quantità di macchine più che sufficiente per supportare il numero di macchine accese necessarie nel catalogo (incluso il buffer di capacità), le macchine aggiuntive vengono spente. Lo spegnimento potrebbe verificarsi a causa di ore non di punta, disconnessioni delle sessioni o un numero inferiore di macchine nel catalogo. La decisione di spegnere una macchina deve soddisfare i seguenti criteri:

- La macchina è accesa e non è in modalità di manutenzione.
- La macchina è registrata come disponibile o in attesa di registrazione dopo l'accensione.
- La macchina non ha sessioni attive. Le sessioni rimanenti sono terminate (la macchina era inattiva per il periodo di timeout di inattività).
- La macchina è stata accesa per almeno "X"minuti, dove "X"è il ritardo di spegnimento specificato per il catalogo.

  In un catalogo statico, dopo l'assegnazione di tutte le macchine nel catalogo, il buffer di capacità non ha alcun ruolo nell'accensione o nello spegnimento delle macchine.

Questa impostazione è valida per tutti i tipi di macchine. È possibile immettere valori per le ore lavorative e le ore non lavorative.

#### Creare una pianificazione di gestione dell'alimentazione

1. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Power Management** (Gestione dell'alimentazione), determinare se una delle pianificazioni preimpostate (nel menu in alto) soddisfa le proprie esigenze. Selezionare un set di impostazioni predefinito per vedere i valori che utilizza. Se si desidera utilizzare un set di impostazioni predefinito, lasciarlo selezionato.
3. Se si modificano i valori in qualsiasi campo (ad esempio giorni, ore o intervalli), la selezione del set di impostazioni predefinito diventa automaticamente **Custom** (Personalizzata). Un asterisco indica che le impostazioni personalizzate non sono state salvate.
4. Impostare i valori desiderati per la pianificazione personalizzata.
5. Selezionare **Custom** (Personalizzata) in alto, quindi salvare le impostazioni correnti come nuovo set di impostazioni predefinite. Immettere un nome per il nuovo Personalizzato e selezionare il segno di spunta.
6. Al termine, selezionare **Save Changes** (Salva modifiche).

Successivamente, è possibile modificare o eliminare un set di impostazioni predefinite personalizzato utilizzando le icone a forma di matita o cestino nel menu **Presets** (Set di impostazioni predefiniti). Non è possibile modificare o eliminare i set di impostazioni predefiniti comuni.

### Informazioni correlate

- Aggiornare un catalogo con una nuova immagine
- Aggiungere e rimuovere utenti in un catalogo

## Sottoscrizioni di Azure in Quick Deploy

August 17, 2023

### Introduzione

Quando si crea un catalogo o un'immagine in Quick Deploy (Distribuzione rapida), è necessario scegliere tra le sottoscrizioni di Azure disponibili. Quick Deploy (Distribuzione rapida) supporta sia le sottoscrizioni Citrix Managed Azure sia le sottoscrizioni di Azure dell'utente e gestite dai clienti.

- Per utilizzare la propria sottoscrizione di Azure, è innanzitutto necessario importare (aggiungere) una o più di queste sottoscrizioni in Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). Tale azione consente a Citrix DaaS di accedere alle sottoscrizioni di Azure.
- L'utilizzo di una sottoscrizione Citrix Managed Azure non richiede alcuna configurazione della sottoscrizione. Tuttavia, una sottoscrizione Citrix Managed Azure è disponibile solo quando si ordina il Citrix Azure Consumption Fund, in aggiunta a Citrix DaaS.

Alcune funzionalità di Citrix DaaS differiscono a seconda che il catalogo utilizzi una sottoscrizione Citrix Managed Azure o la propria sottoscrizione di Azure.

| Sottoscrizione Citrix Managed Azure | Sottoscrizione di Azure dell'utente |
|---|---|
| Supporta macchine aggiunte a un dominio o non aggiunte a un dominio. | Supporta solo macchine aggiunte a un dominio. |
| Supporta la creazione rapida e la creazione personalizzata di cataloghi. | Supporta solo cataloghi personalizzati. |
| Sempre disponibile durante la creazione di cataloghi e immagini. | È necessario aggiungere la sottoscrizione di Azure a Citrix DaaS prima di creare un catalogo. |
| Per l'autenticazione utente, supporta Citrix Managed Azure Active Directory o Active Directory dell'utente. | È in grado di connettere l'Active Directory dell'utente e Azure Active Directory. |
| Le opzioni di connessione di rete includono **No connectivity** (Nessuna connessione). | Le opzioni di connessione di rete includono solo le proprie reti virtuali. |
| Quando si utilizza il peering della rete virtuale di Azure per connettersi alle risorse, è necessario creare una connessione di peering della rete virtuale in Citrix DaaS. | Selezionare una rete virtuale esistente. |
| Quando si importa un'immagine da Azure, si specifica l'URI dell'immagine. | Quando si importa un'immagine, è possibile selezionare un disco rigido virtuale o selezionare lo spazio di archiviazione nella sottoscrizione di Azure. |
| È in grado di creare una macchina bastion nella sottoscrizione di Azure del cliente per risolvere i problemi delle macchine. | Non è necessario creare una macchina bastion perché è già possibile accedere alle macchine nella propria sottoscrizione. |

### Visualizzare le sottoscrizioni di Azure

Per visualizzare i dettagli delle sottoscrizioni di Azure, da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Cloud Subscriptions** (Sottoscrizioni cloud) a destra. Quindi,

selezionare una sottoscrizione.

- La pagina **Details** (Dettagli) include il numero di macchine, più i numeri e i nomi dei cataloghi e delle immagini che utilizzano la sottoscrizione.
- La pagina **Resource Locations** (Posizioni risorsa) elenca le posizioni risorsa in cui viene utilizzata la sottoscrizione.

## Aggiungere sottoscrizioni di Azure gestite dal cliente

Per utilizzare una sottoscrizione di Azure gestita dal cliente, è necessario aggiungerla a Citrix DaaS prima di creare un catalogo o creare un'immagine che utilizza tale sottoscrizione. Sono disponibili due opzioni per aggiungere le sottoscrizioni di Azure:

- **Se si ha il ruolo di amministratore globale per la directory e si dispone di autorizzazioni di proprietario per la sottoscrizione:** è sufficiente eseguire l'autenticazione nel proprio account Azure.
- **Se non si ha il ruolo di amministratore globale e si dispone di autorizzazioni di proprietario per la sottoscrizione:** prima di aggiungere la sottoscrizione a Citrix DaaS, creare un'app Azure in Azure AD e aggiungere l'app come collaboratore della sottoscrizione. Quando si aggiunge la sottoscrizione a Citrix DaaS, si forniscono le informazioni rilevanti sull'app.

### Aggiungere sottoscrizioni di Azure gestite dal cliente se si ha il ruolo di amministratore globale

Questa attività richiede autorizzazioni di amministratore globale per la directory e autorizzazioni di proprietario per la sottoscrizione.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Cloud Subscriptions** (Sottoscrizioni cloud) sulla destra.
2. Selezionare **Add Azure subscription** (Aggiungi sottoscrizione di Azure).
3. Nella pagina **Add Subscriptions** (Aggiungi sottoscrizioni), selezionare **Add your Azure subscription** (Aggiungi la sottoscrizione di Azure).
4. Selezionare il pulsante che consente a Citrix DaaS di accedere alle sottoscrizioni di Azure per proprio conto.
5. Selezionare **Authenticate Azure Account** (Autentica account Azure). Si verrà reindirizzati alla pagina di accesso di Azure.
6. Inserire le proprie credenziali di Azure.
7. Si ritorna automaticamente a Citrix DaaS. La pagina **Add Subscription** (Aggiungi sottoscrizione) elenca le sottoscrizioni di Azure rilevate. Utilizzare la casella di ricerca per filtrare l'elenco, se necessario. Selezionare una o più sottoscrizioni. Al termine, selezionare **Add Subscriptions** (Aggiungi sottoscrizioni).

8. Confermare di voler aggiungere le sottoscrizioni selezionate.

Le sottoscrizioni di Azure selezionate vengono elencate quando si espande **Subscriptions** (Sottoscrizioni). Le sottoscrizioni aggiunte sono disponibili per la selezione quando si crea un catalogo o un'immagine.

### Aggiungere sottoscrizioni di Azure gestite dal cliente se non si ha il ruolo di amministratore globale

L'aggiunta di una sottoscrizione di Azure quando non si ha il ruolo di amministratore globale è un processo in due parti:

- Prima di aggiungere una sottoscrizione a Citrix DaaS, creare un'app in Azure AD e quindi aggiungere l'app come collaboratore della sottoscrizione.
- Aggiungere la sottoscrizione a Citrix DaaS, utilizzando le informazioni sull'app creata in Azure.

#### Creare un'app in Azure AD e aggiungerla come collaboratore

1. Registrare una nuova applicazione in Azure AD:
    a) Da un browser, andare a https://portal.azure.com.
    b) Nel menu in alto a sinistra, selezionare **Azure Active Directory**.
    c) Nell'elenco **Manage** (Gestisci), selezionare **App registrations** (Registrazioni app).
    d) Selezionare **+ New registration** (+ Nuova registrazione).
    e) Nella pagina **Register an application** (Registra un'applicazione), fornire le seguenti informazioni:
        - **Nome:** immettere il nome della connessione
        - **Tipo di applicazione:** selezionare **Web app / API** (App web/API)
        - **Redirect URI** (URI di reindirizzamento): lasciare il campo vuoto
    f) Selezionare **Create**.
2. Creare la chiave di accesso segreta dell'applicazione e aggiungere l'assegnazione del ruolo:
    a) Dalla procedura precedente, selezionare **App Registration** (Registrazione app) per visualizzare i dettagli.
    b) Prendere nota dell'**Application ID** (ID applicazione) e del **Directory ID** (ID directory). Verranno utilizzati in seguito quando si aggiunge la propria sottoscrizione a Citrix DaaS.
    c) In **Manage** (Gestisci), selezionare **Certificates & secrets** (Certificati e segreti).

d) Nella pagina **Client secrets** (Segreti del client), selezionare **+ New client secret** (+ Nuovo segreto del client).

e) Nella pagina **Add a client secret** (Aggiungi un segreto del client), fornire una descrizione e selezionare un intervallo di scadenza. Quindi, selezionare **Add** (Aggiungi).

f) Prendere nota del valore del segreto del client. Verranno utilizzati in seguito quando si aggiunge la propria sottoscrizione a Citrix DaaS.

g) Selezionare la sottoscrizione di Azure che si desidera collegare (aggiungere) a Citrix DaaS, quindi selezionare **Access control (IAM)** (Controllo dell'accesso [IAM]).

h) Nella casella **Add a role assignment** (Aggiungi un'assegnazione di ruolo), selezionare **Add** (Aggiungi).

i) Nella scheda **Add role assignment** (Aggiungi assegnazione di ruolo), selezionare quanto segue:

- **Role** (Ruolo): collaboratore
- **Assign access to** (Assegna l'accesso a:) utente, gruppo o entità servizio di Azure AD
- **Select** (Seleziona): il nome dell'app Azure creata in precedenza.

j) Selezionare **Save** (Salva).

**Aggiungere la propria sottoscrizione a Citrix DaaS** È necessario l'ID applicazione, l'ID directory e il valore del segreto del client relativi all'app creata in Azure AD.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Cloud Subscriptions** (Sottoscrizioni cloud) sulla destra.
2. Selezionare **Add Azure subscription** (Aggiungi sottoscrizione di Azure).
3. Nella pagina **Add Subscriptions** (Aggiungi sottoscrizioni), selezionare **Add your Azure subscriptions** (Aggiungi le sottoscrizioni di Azure).
4. Selezionare **I have an Azure App with contributor role to the subscription** (Dispongo di un'app di Azure con ruolo di collaboratore per la sottoscrizione).
5. Inserire l'ID tenant (ID directory), l'ID client (ID applicazione) e il segreto del client per l'app creata in Azure.
6. Selezionare **Select your subscription** (Seleziona la sottoscrizione), quindi selezionare la sottoscrizione desiderata.

Successivamente, dalla pagina **Details** (Dettagli) della sottoscrizione nella dashboard di Citrix DaaS, è possibile aggiornare il segreto del client o sostituire l'app Azure dal menu con i puntini di sospensione.

Se Citrix DaaS non riesce ad accedere a una sottoscrizione di Azure dopo che viene aggiunta, non sono consentite diverse azioni delle singole macchine e di gestione dell'alimentazione del catalogo.

Un messaggio fornisce un'opzione per aggiungere nuovamente la sottoscrizione. Se la sottoscrizione è stata originariamente aggiunta utilizzando un'app Azure, è possibile sostituire l'app Azure.

### Aggiungere sottoscrizioni Citrix Managed Azure

Una sottoscrizione Citrix Managed Azure supporta un determinato numero di macchine (in questo contesto, le *macchine* si riferiscono alle macchine virtuali su cui è installato un VDA Citrix. Queste macchine forniscono app e desktop agli utenti. Non sono comprese altre macchine in una posizione risorsa, ad esempio i Cloud Connector).

Se è probabile che la propria sottoscrizione Citrix Managed Azure raggiunga presto il limite e si dispone di licenze Citrix sufficienti, è possibile richiedere un'altra sottoscrizione Citrix Managed Azure. La dashboard contiene una notifica quando si è vicini al limite.

Non è possibile creare un catalogo (o aggiungere macchine a un catalogo) se il numero totale di macchine per tutti i cataloghi che utilizzano la sottoscrizione Citrix Managed Azure supera il limite.

Ad esempio, si supponga un limite ipotetico di 1.000 macchine per sottoscrizione Citrix Managed Azure.

- Supponiamo di avere a disposizione due cataloghi (`Cat1` e `Cat2`) che utilizzano la stessa sottoscrizione Citrix Managed Azure. `Cat1` contiene attualmente 500 macchine e `Cat2` ne ha 250.
- Per pianificare le esigenze di capacità future, si aggiungono 200 macchine a `Cat2`. La sottoscrizione Citrix Managed Azure ora supporta 950 macchine (500 in `Cat 1` e 450 in `Cat 2`). La dashboard indica che la sottoscrizione è vicino al limite.
- Quando sono necessarie altre 75 macchine, non è possibile utilizzare tale sottoscrizione per creare un catalogo con 75 macchine (o aggiungere 75 macchine a un catalogo esistente). Ciò supererebbe il limite della sottoscrizione. Richiedere invece un'altra sottoscrizione Citrix Managed Azure. Quindi, è possibile creare un catalogo utilizzando tale sottoscrizione.

Se si dispone di più di una sottoscrizione Citrix Managed Azure:

- Non viene condiviso nulla tra queste sottoscrizioni.
- Ogni sottoscrizione ha un nome univoco.
- È possibile scegliere tra le sottoscrizioni Citrix Managed Azure (ed eventuali sottoscrizioni di Azure gestite dal cliente che sono state aggiunte) quando:
  - Si crea un catalogo.
  - Si crea o si importa un'immagine.
  - Si crea un peering della rete virtuale o una connessione SD-WAN.

Requisito:

- È necessario disporre di licenze Citrix sufficienti per garantire l'aggiunta di un'altra sottoscrizione Citrix Managed Azure. Utilizzando l'esempio ipotetico precedente, se si dispone di 2.000 licenze Citrix in previsione di distribuire almeno 1.500 macchine tramite le sottoscrizioni Citrix Managed, è possibile aggiungere un'altra sottoscrizione Citrix Managed Azure.

Per aggiungere una sottoscrizione Citrix Managed Azure:

1. Contattare il proprio rappresentante Citrix per richiedere un'altra sottoscrizione Citrix Managed Azure. Si riceverà una notifica quando è possibile procedere.
2. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Cloud Subscriptions** (Sottoscrizioni cloud) sulla destra.
3. Selezionare **Add Azure subscription** (Aggiungi sottoscrizione di Azure).
4. Nella pagina **Add Subscriptions** (Aggiungi sottoscrizioni), selezionare **Add a Citrix Managed Azure subscription** (Aggiungi una sottoscrizione Citrix Managed Azure).
5. Nella pagina **Add a Citrix Managed Subscription** (Aggiungi una sottoscrizione Citrix Managed), selezionare **Add Subscription** (Aggiungi sottoscrizione) nella parte inferiore della pagina.

Se si riceve una notifica che comunica che si è verificato un errore durante la creazione di una sottoscrizione Citrix Managed Azure, contattare il supporto Citrix.

### Rimuovere le sottoscrizioni di Azure

Prima di poter rimuovere una sottoscrizione di Azure, è necessario eliminare tutti i cataloghi e le immagini che la utilizzano.

Se si dispone di una o più sottoscrizioni Citrix Managed Azure, non è possibile rimuoverle tutte. Deve rimanerne almeno una.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Cloud Subscriptions** (Sottoscrizioni cloud) sulla destra.
2. Selezionare la sottoscrizione.
3. Nella scheda **Details** (Dettagli), selezionare **Remove Subscription** (Rimuovi sottoscrizione).
4. Selezionare **Authenticate Azure Account** (Autentica account Azure). Si verrà reindirizzati alla pagina di accesso di Azure.
5. Inserire le proprie credenziali di Azure.
6. Si ritorna automaticamente a Citrix DaaS. Confermare l'eliminazione e quindi selezionare **Yes, Delete Subscription** (Sì, elimina sottoscrizione).

### Aggiornare i segreti del client scaduti

Quando il segreto del client di un abbonamento scade, non è possibile creare cataloghi di macchine per esso e viene visualizzato un avviso nella voce dell'abbonamento. Per risolvere questo problema,

sono disponibili due scelte:

- Aggiornare il segreto del client dell'app Azure in uso
- Passare a un'app Azure con una data di scadenza valida

#### Aggiornare il segreto del client dell'app Azure in uso

Per continuare a usare l'app Azure esistente per accedere alle risorse di Azure, seguire questi passaggi:

1. In Azure, creare un segreto del client per l'app Azure in uso. Prendere nota del nuovo segreto e della data di scadenza per l'uso futuro. Per altre informazioni, vedere Creare un segreto dell'applicazione in Azure.
2. In DaaS, aggiungere le informazioni segrete appena create alla sottoscrizione. I passaggi dettagliati sono i seguenti:

    a) Dalla dashboard **Gestisci > Azure Quick Deploy** in Citrix DaaS per Azure, espandere **Cloud Subscriptions** a destra.
    b) Fare clic sulla sottoscrizione che richiede aggiornamenti del segreto.
    c) Nella pagina della sottoscrizione visualizzata, fare clic sul menu con i puntini di sospensione nel riquadro **Azure App Details** (Dettagli dell'app Azure), quindi selezionare **Update Client Secret** (Aggiorna segreto del client).
    d) Nella pagina **Aggiorna Client Secret**, digitare i dati necessari in **Client Secret** (Segreto client) e **Secret Expiration Date** (Data di scadenza segreto).
    e) Fare clic su **Update Secret** (Aggiorna segreto).

#### Passare a un'app Azure con una data di scadenza valida

Per passare a un'app Azure valida per accedere alle risorse di Azure, ottenere le informazioni necessarie sull'app e aggiungerle alla sottoscrizione utilizzando i seguenti passaggi:

1. In Azure, ottenere un'app Azure valida e annotarne i dettagli. Assicurarsi che alla nuova app Azure sia assegnato il ruolo di *Contributor* (Collaboratore). Per altre informazioni, vedere Creare un'app in Azure AD e aggiungerla come collaboratore.
2. In DaaS, aggiungere i dettagli dell'app Azure alla sottoscrizione. I passaggi dettagliati sono i seguenti:

    a) Dalla dashboard **Gestisci > Azure Quick Deploy** in Citrix DaaS per Azure, espandere **Cloud Subscriptions** a destra.
    b) Fare clic sulla sottoscrizione che richiede aggiornamenti del segreto.

c) Nella pagina della sottoscrizione visualizzata, fare clic sul menu con i puntini di sospensione nel riquadro **Azure App Details** (Dettagli dell'app Azure), quindi selezionare **Replace Azure App** (Sostituisci app Azure).
d) Nella pagina **Replace Azure App**, inserire i dettagli della nuova app Azure nei campi **Directory (tenant) ID** (ID directory [tenant]), **Application (client) ID** (ID applicazione [client]), **Client Secret** (Segreto cliente) e **Secret Expiration Date for the service principal** (Data di scadenza segreto per l'entità di servizio).
e) Fare clic su **Replace App** (Sostituisci app).

## Immagini in Quick Deploy (Distribuzione rapida)

October 6, 2022

Quando si crea un catalogo per distribuire desktop o app, viene utilizzata un'immagine (con altre impostazioni) come modello per la creazione delle macchine.

Quick Deploy (Distribuzione rapida) fornisce una serie di immagini preparate che è possibile scegliere per creare e personalizzare un'immagine in Quick Deploy (Distribuzione rapida). È anche possibile importare (aggiungere) immagini dalla propria sottoscrizione di Azure.

### Immagini preparate da Citrix

Quick Deploy (Distribuzione rapida) fornisce diverse immagini preparate da Citrix:

- Windows 10 Enterprise (sessione singola)
- Desktop virtuale Windows 10 Enterprise (multisessione)
- Desktop virtuale Windows 10 Enterprise (multisessione) con Office 365 ProPlus
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Linux Ubuntu (a sessione singola e multisessione)

Le immagini preparate da Citrix dispongono di un Citrix Virtual Delivery Agent (VDA) e di strumenti per la risoluzione dei problemi installati. Il VDA è il meccanismo di comunicazione tra le macchine degli utenti e l'infrastruttura Citrix Cloud che gestisce Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). Le immagini fornite da Citrix hanno una notazione **CITRIX**.

Le immagini preparate da Citrix non sono disponibili nell'interfaccia Full Configuration (Configurazione completa) di Citrix DaaS.

È anche possibile importare e utilizzare la propria immagine da Azure.

### Modi per utilizzare le immagini in Quick Deploy (Distribuzione rapida)

È possibile:

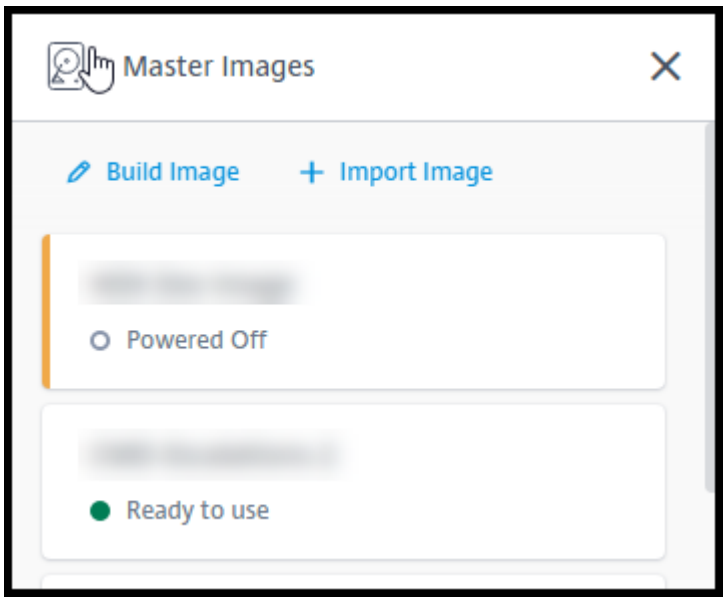
- **Utilizzare un'immagine preparata da Citrix durante la creazione di un catalogo.** Questa scelta è consigliata solo per le distribuzioni Proof of Concept (POC).
- **Utilizzare un'immagine preparata da Citrix per creare un'altra immagine.** Dopo aver creato la nuova immagine, è possibile personalizzarla aggiungendo applicazioni e altro software di cui gli utenti hanno bisogno. Quindi, è possibile usare tale immagine personalizzata quando si crea un catalogo.
- **Importare un'immagine da Azure.** Dopo aver importato un'immagine da Azure, è possibile utilizzarla durante la creazione di un catalogo.

  Oppure è possibile utilizzare quell'immagine per creare una nuova immagine e successivamente personalizzarla aggiungendo app. Quindi, è possibile usare tale immagine personalizzata quando si crea un catalogo.

Quando si crea un catalogo, Citrix DaaS verifica che l'immagine utilizzi un sistema operativo valido e che disponga di un Citrix VDA e di strumenti di risoluzione dei problemi installati (oltre a eseguire altri controlli).

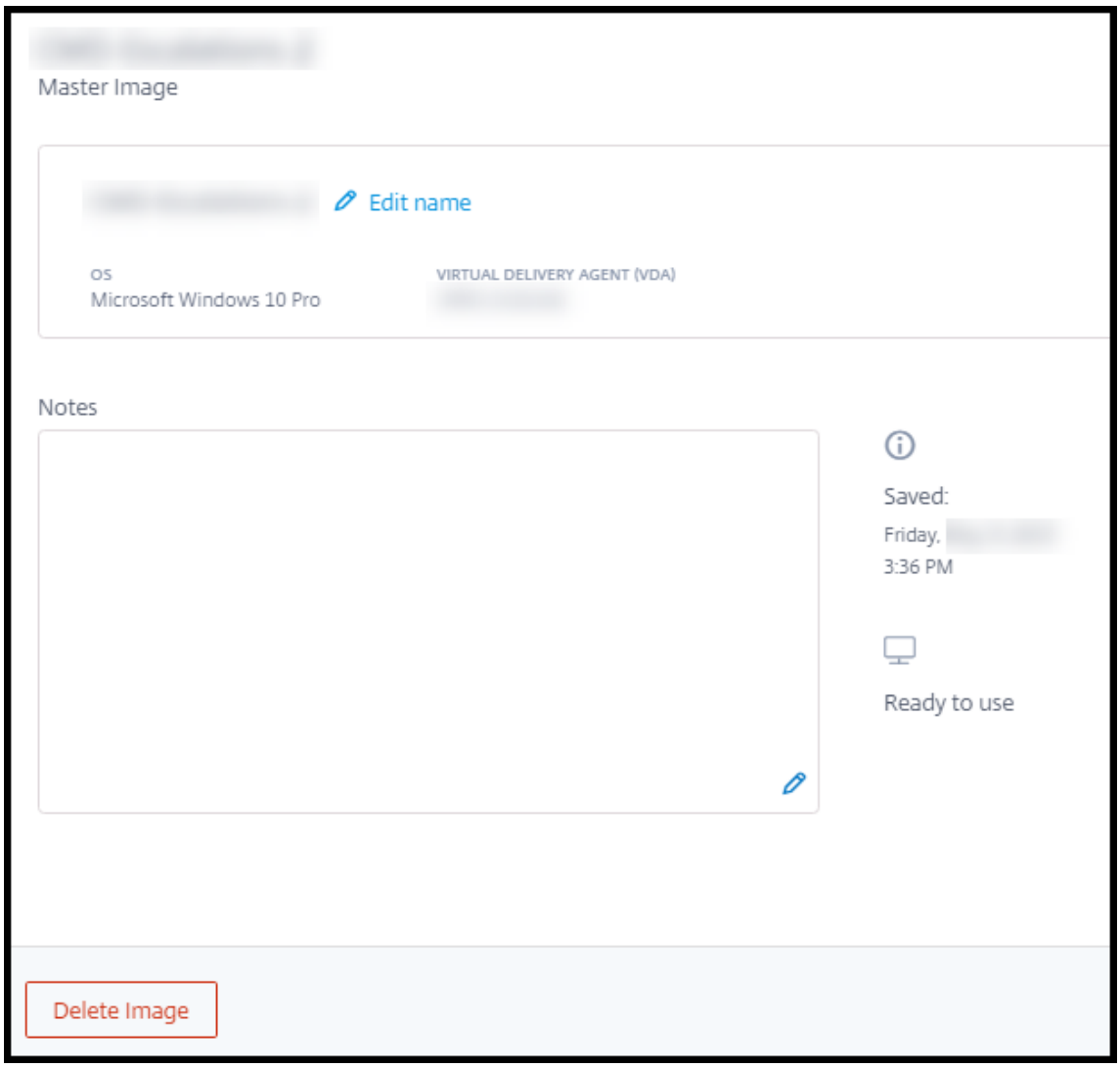
### Visualizzare le informazioni sull'immagine

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Master Images** (Immagini master) sulla destra. La visualizzazione elenca le immagini preparate da Citrix e tutte le immagini importate.



2. Selezionare un'immagine per visualizzarne i dettagli.




Dalla scheda dei dettagli è possibile:

- Cambiare (modificare) il nome dell'immagine.
- Aggiungere e modificare note (disponibile solo per le immagini preparate o importate, non per le immagini preparate da Citrix).
- Eliminare l'immagine.

### Preparare una nuova immagine

La preparazione di una nuova immagine include la creazione dell'immagine e la successiva personalizzazione. Quando si crea un'immagine, viene creata una nuova macchina virtuale per caricare la nuova immagine.

Requisiti:

- Conoscere le caratteristiche prestazionali di cui le macchine hanno bisogno. Ad esempio, l'esecuzione di app CAD potrebbe richiedere CPU, RAM e spazio di archiviazione diversi rispetto ad altre app per ufficio.
- Se si prevede di utilizzare una connessione alle risorse on-premise, configurarla prima di creare l'immagine e il catalogo. Per i dettagli, vedere Connessioni di rete.

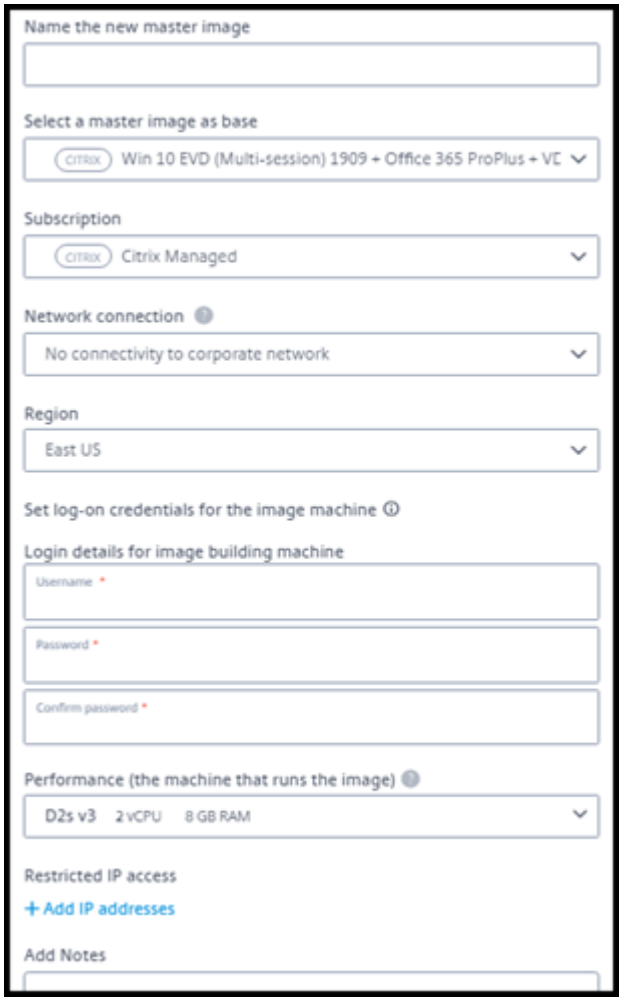
Quando si utilizza un'immagine Ubuntu preparata da Citrix per creare una nuova immagine, viene creata una password root per la nuova immagine. È possibile modificare la password root, ma solo durante il processo di creazione e personalizzazione dell'immagine (non è possibile modificare la password root dopo che l'immagine è stata utilizzata in un catalogo).

- Quando l'immagine viene creata, l'account amministratore specificato (**Dettagli di accesso per la macchina di creazione delle immagini**) viene aggiunto al gruppo `sudoers`.
- Dopo aver eseguito l'RDP sulla macchina contenente la nuova immagine, avviare l'applicazione di terminale e digitare `sudo passwd root`. Quando richiesto, fornire la password specificata durante la creazione dell'immagine. Dopo la verifica, verrà richiesto di inserire una nuova password per l'utente root.

Per creare un'immagine:

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Master Images** (Immagini master) sulla destra.
2. Selezionare **Build Image** (Crea immagine).




3. Immettere valori nei seguenti campi:

   - **Name** (Nome): inserire un nome per la nuova immagine.
   - **Master image** (Immagine master): selezionare un'immagine esistente. Questa è l'immagine di base utilizzata per creare la nuova immagine.
   - **Subscription** (Sottoscrizione): selezionare una sottoscrizione di Azure.
   - **Network connection** (Connessione di rete):
     - Se si utilizza una sottoscrizione Citrix Managed Azure, selezionare **No connectivity** (Nessuna connettività) o una connessione creata in precedenza.
     - Se si utilizza la propria sottoscrizione di Azure gestita dal cliente, selezionare il gruppo di risorse, la rete virtuale e la subnet. Quindi, aggiungere i dettagli del dominio: FQDN, OU, nome account Citrix DaaS e credenziali.
   - **Region** (Regione): (disponibile solo per **No connectivity** [Nessuna connettività]). Selezionare la regione in cui si desidera creare la macchina contenente l'immagine.

- **Logon credentials for image machine** (Credenziali di accesso per la macchina dell'immagine): queste credenziali verranno utilizzate in seguito quando ci si connette (RDP) alla macchina contenente la nuova immagine, in modo da poter installare app e altro software.
- **Machine performance** (Prestazioni della macchina): si tratta di informazioni su CPU, RAM e spazio di archiviazione per la macchina che esegue l'immagine. Selezionare prestazioni della macchina che soddisfino i requisiti delle proprie app.
- **Restricted IP access** (Accesso IP limitato): se si desidera limitare l'accesso a indirizzi specifici, selezionare **Add IP addresses** (Aggiungi indirizzi IP) e quindi immettere uno o più indirizzi. Dopo aver aggiunto gli indirizzi, selezionare **Done** (Fine) per tornare alla scheda **Build Image** (Crea immagine).
- **Notes** (Note): è possibile aggiungere fino a 1024 caratteri di note. Dopo aver creato l'immagine, è possibile aggiornare le note dalla visualizzazione dei dettagli dell'immagine.
- **Local domain join** (Aggiunta a un dominio locale): indicare se si desidera accedere al dominio Active Directory locale.
  - Se si seleziona **Yes** (Sì), immettere l'FDQN, l'OU, il nome account Citrix DaaS e le credenziali.
  - Se si seleziona **No**, immettere le credenziali per la macchina host.

4. Al termine, selezionare **Build Image** (Crea immagine).

La creazione di un'immagine può richiedere fino a 30 minuti. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Master Images** (Immagini master) sulla destra per vedere lo stato corrente (ad esempio `Building image` o `Ready to customize`).

Azione successiva: connettersi a una nuova immagine e personalizzarla.

### Connettersi a una nuova immagine e personalizzarla

Dopo la creazione di una nuova immagine, il relativo nome viene aggiunto all'elenco delle immagini, con uno stato `Ready to customize` (o una formulazione simile). Per personalizzare quell'immagine, è necessario prima scaricare un file RDP. Quando si utilizza quel file per connettersi all'immagine, è possibile aggiungere applicazioni e altro software all'immagine.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Master Images** (Immagini master) sulla destra. Selezionare l'immagine a cui si desidera connettersi.
2. Selezionare **Download RDP file** (Scarica file RDP). Viene scaricato un client RDP.

   La macchina dell'immagine potrebbe spegnersi se non si esegue l'RDP subito dopo averla creata. Ciò consente di risparmiare sui costi. Quando questo accade, selezionare **Power On** (Accendi).

3. Avviare il client RDP scaricato, che tenta automaticamente di connettersi all'indirizzo della macchina contenente la nuova immagine. Quando richiesto, immettere le credenziali specificate durante la creazione dell'immagine.
4. Dopo aver effettuato la connessione alla macchina, aggiungere o rimuovere app, installare gli aggiornamenti e completare qualsiasi altro lavoro di personalizzazione.

   **NON** eseguire il Sysprep dell'immagine.
5. Una volta completata la personalizzazione della nuova immagine, tornare alla finestra di dialogo **Master Images** (Immagini master) e selezionare **Finish build** (Termina creazione). La nuova immagine viene sottoposta automaticamente a test di convalida.

Successivamente, quando si crea un catalogo, la nuova immagine viene inclusa nell'elenco di immagini che è possibile selezionare.

Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), l'immagine visualizzata sulla destra indica quanti cataloghi e macchine utilizzano ciascuna immagine.

> **Nota:**
>
> Dopo aver finalizzato un'immagine, non è possibile modificarla. È necessario creare una nuova immagine (utilizzando facoltativamente l'immagine precedente come punto di partenza) e quindi aggiornare la nuova immagine.

## Importare un'immagine da Azure

Quando si importa un'immagine da Azure che dispone di un VDA Citrix e delle applicazioni necessarie agli utenti, è possibile utilizzarla per creare un catalogo o sostituire l'immagine in un catalogo esistente.

### Requisiti delle immagini importate

> **Nota:**
>
> Citrix DaaS non supporta l'importazione di dischi associati alle macchine virtuali di seconda generazione di Azure.

Citrix esegue test di convalida sull'immagine importata. Assicurarsi che i seguenti requisiti siano soddisfatti quando si prepara l'immagine da importare in Citrix DaaS.

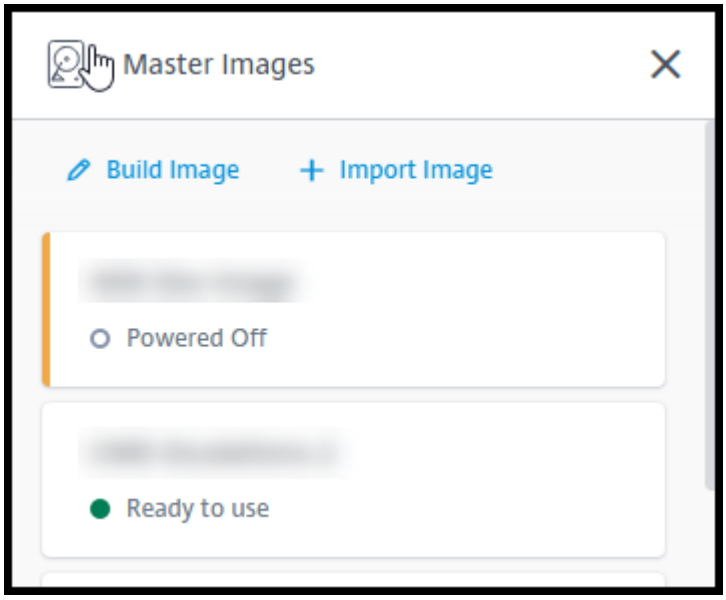
- **Sistema operativo supportato:** l'immagine deve essere un sistema operativo supportato. Per verificare una versione del sistema operativo Windows, eseguire `Get-WmiObject Win32_OperatingSystem`.
- **Generazione supportata:** sono supportate solo le macchine virtuali di prima generazione.

- **Non generalizzata:** l'immagine non deve essere generalizzata.
- **Nessun Delivery Controller configurato:** assicurarsi che nessun Citrix Delivery Controller sia configurato nell'immagine. Assicurarsi che le seguenti chiavi del Registro di sistema vengano eliminate.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **File Personality.ini:** il file `personality.ini` deve esistere nell'unità di sistema.
- **VDA valido:** sull'immagine deve essere installato un VDA Citrix più recente della versione 7.11.
  - Windows: per controllare, utilizzare `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. Per istruzioni sull'installazione, vedere Installare un VDA Windows su un'immagine.
  - Red Hat Enterprise Linux e Ubuntu: per una guida all'installazione, consultare la documentazione del prodotto.
- **Agente della macchina virtuale di Azure:** prima di importare un'immagine, assicurarsi che l'agente della macchina virtuale di Azure sia installato sull'immagine. Per ulteriori informazioni, vedere l'articolo Microsoft Panoramica dell'agente della macchina virtuale di Azure.

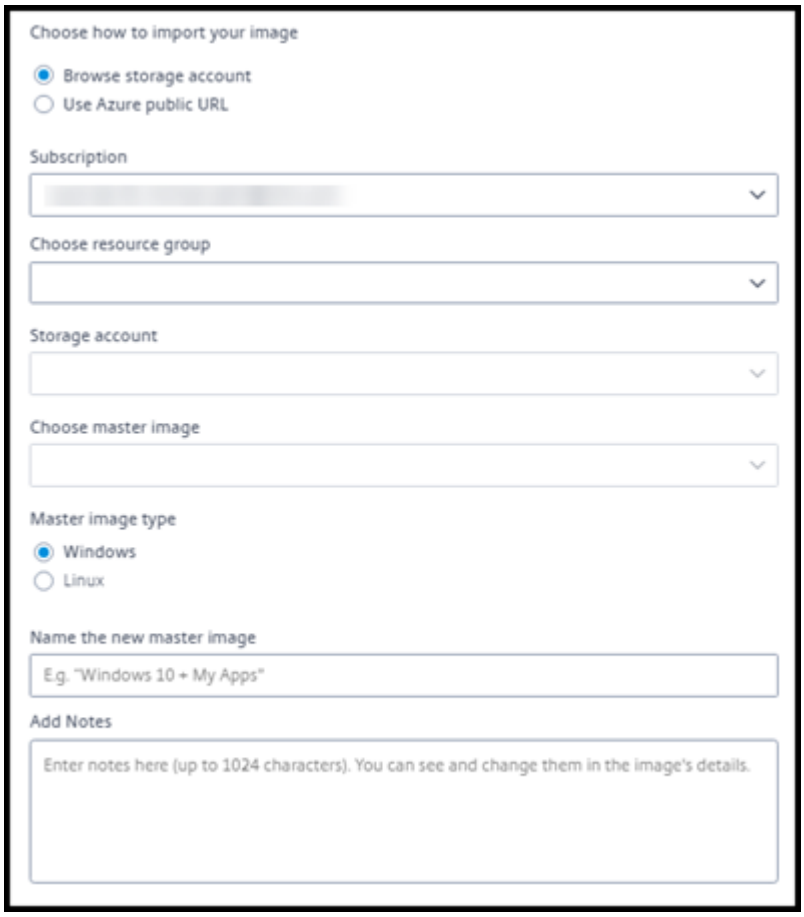
#### Importare l'immagine utilizzando Quick Deploy (Distribuzione rapida)

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Master Images** (Immagini master) sulla destra.



2. Selezionare **Import Image** (Importa immagine).



(Importa immagine)

3. Scegliere come importare l'immagine.

   - Per i dischi gestiti, utilizzare la funzionalità di esportazione per generare un URL SAS. Impostare il tempo di scadenza su 7200 secondi o più.
   - Per i VHD in un account di archiviazione, scegliere una delle seguenti opzioni:
     - Generare un URL SAS per il file VHD.
     - Aggiornare il livello di accesso di un contenitore di archiviazione a blocchi a BLOB o contenitore. Quindi, ottenere l'URL del file.

4. Se è stato selezionato **Browse storage account** (Sfoglia account di archiviazione):

   a) Selezionare in sequenza: sottoscrizione > gruppo di risorse > account di archiviazione > immagine.
   b) Dare un nome all'immagine.

5. Se è stato selezionato **Azure public URL** (URL pubblico di Azure):

   a) Immettere l'URL generato da Azure per il VHD. Per assistenza, selezionare il collegamento al documento Microsoft Scaricare un disco rigido virtuale Windows da Azure.

b) Selezionare una sottoscrizione (un'immagine Linux può essere importata solo se si seleziona una sottoscrizione gestita dal cliente).
c) Dare un nome all'immagine.

6. Al termine, selezionare **Import Image** (Importa immagine).

### Aggiornare un catalogo Quick Deploy (Distribuzione rapida) con una nuova immagine

Il tipo di catalogo determina quali macchine vengono aggiornate quando si aggiorna il catalogo.

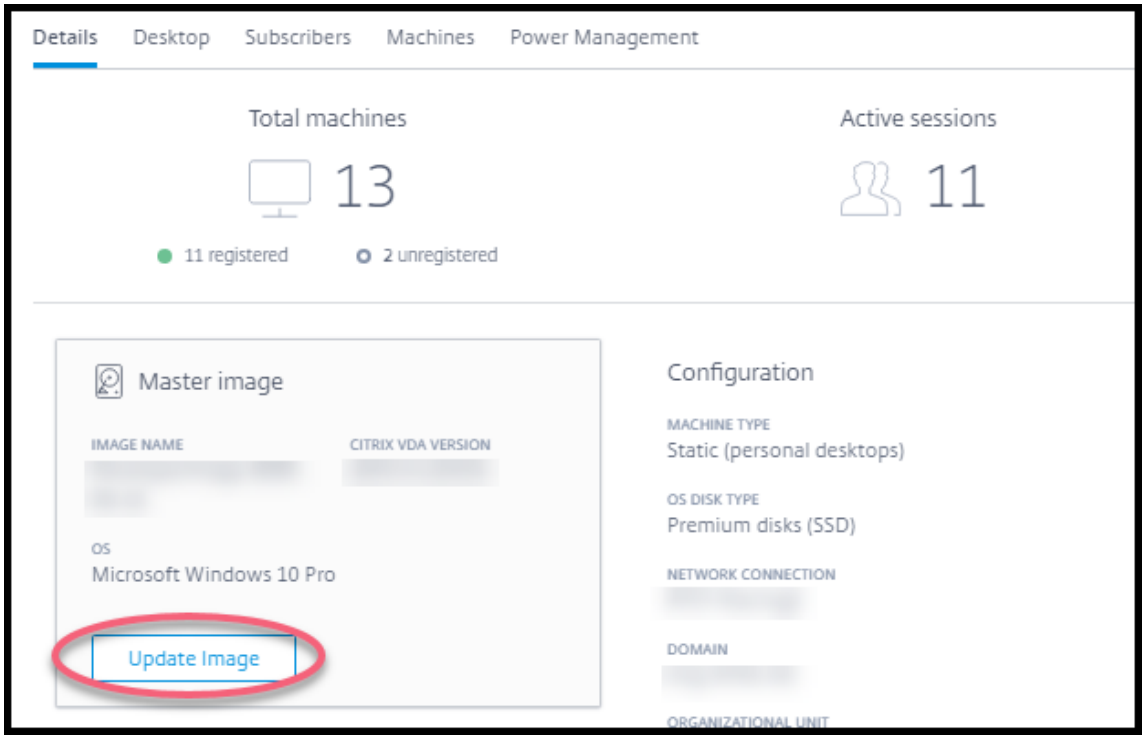
- Per un catalogo casuale, tutte le macchine attualmente presenti nel catalogo vengono aggiornate con l'immagine più recente. Se si aggiungono altri desktop a tale catalogo, si basano sull'immagine più recente.
- Per un catalogo statico, le macchine attualmente presenti nel catalogo non vengono aggiornate con l'immagine più recente. Le macchine attualmente in catalogo continuano a utilizzare l'immagine da cui sono state create. Tuttavia, se si aggiungono altre macchine a quel catalogo, si basano sull'immagine più recente.

È possibile aggiornare un catalogo contenente macchine con immagini gen1 con un'immagine gen2, se le macchine del catalogo supportano gen2. Allo stesso modo, è possibile aggiornare un catalogo contenente macchine gen2 con un'immagine gen1, se le macchine del catalogo supportano gen1.

Per aggiornare un catalogo con una nuova immagine:

1. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), fare clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Details** (Dettagli), selezionare **Update Image** (Aggiorna immagine).




3. Selezionare un'immagine.
4. Per cataloghi casuali o multisessione: selezionare un intervallo di disconnessione. Dopo che Citrix DaaS ha completato l'elaborazione iniziale dell'immagine, le persone in possesso di una sottoscrizione ricevono un avviso che richiede di salvare il lavoro e disconnettersi dai loro desktop. L'intervallo di disconnessione indica il tempo che le persone in possesso di una sottoscrizione hanno a disposizione dopo aver ricevuto il messaggio fino al termine automatico della sessione.
5. Selezionare **Update Image** (Aggiorna immagine).

### Eliminare un'immagine da Quick Deploy (Distribuzione rapida)

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Master Images** (Immagini master) sulla destra.
2. Selezionare l'immagine che si desidera eliminare.
3. Selezionare **Delete Image** (Elimina immagine) nella parte inferiore della scheda. Confermare l'eliminazione.

### Installare un VDA Windows su un'immagine

Utilizzare la procedura seguente per preparare un'immagine Windows che si intende importare in Citrix DaaS.

Per la guida all'installazione di Linux VDA, vedere la documentazione del prodotto Linux VDA.

1. Nell'ambiente Azure, connettersi alla macchina virtuale dell'immagine (se non si è già connessi).
2. È possibile scaricare un VDA utilizzando il link **Downloads** (Download) nella barra di navigazione di Citrix Cloud. Oppure, utilizzare un browser per accedere alla pagina di download di Citrix DaaS.

   Scaricare un VDA sulla macchina virtuale. Esistono pacchetti di download dei VDA separati per un sistema operativo desktop (a sessione singola) e un sistema operativo server (multisessione).
3. Avviare il programma di installazione del VDA facendo doppio clic sul file scaricato. Viene avviata l'installazione guidata.
4. Nella pagina **Environment** (Ambiente), selezionare l'opzione per creare un'immagine utilizzando MCS, quindi selezionare **Next** (Avanti).
5. Nella pagina **Core Components** (Componenti core), selezionare **Next** (Avanti).
6. Nella pagina **Delivery Controller**, selezionare **Let Machine Creation Services do it automatically** (Consenti a Machine Creation Services di eseguire l'operazione automaticamente), quindi selezionare **Next** (Avanti). Confermare la selezione, se richiesto.
7. Lasciare le impostazioni predefinite nelle pagine **Additional Components** (Componenti aggiuntivi), **Features** (Funzionalità) e **Firewall**, a meno che Citrix non abbia fornito indicazioni diverse. Selezionare **Next** (Avanti) in ogni pagina.
8. Nella pagina **Summary** (Riepilogo), selezionare **Install** (Installa). I prerequisiti iniziano a essere installati. Quando viene richiesto il riavvio, procedere.
9. L'installazione del VDA riprende automaticamente. L'installazione dei prerequisiti viene completata e sucessivamente vengono installati i componenti e le funzionalità. Nella pagina **Call Home**, lasciare l'impostazione predefinita (a meno che Citrix non abbia fornito indicazioni diverse). Dopo aver stabilito la connessione, selezionare **Next** (Avanti).
10. Selezionare **Finish** (Fine). La macchina si riavvia automaticamente.
11. Per assicurarsi che la configurazione sia corretta, avviare una o più applicazioni installate sulla macchina virtuale.
12. Spegnere la macchina virtuale. Non eseguire il Sysprep dell'immagine.

Per ulteriori informazioni sull'installazione dei VDA, vedere Installare i VDA.

## Connessioni di rete in Quick Deploy (Distribuzione rapida)

October 6, 2022

## Introduzione

Questo articolo fornisce dettagli su come creare connessioni di rete alle risorse aziendali quando si utilizza una sottoscrizione Citrix Managed Azure.

Quando si utilizza la propria sottoscrizione di Azure gestita dal cliente, non è necessario creare una connessione di rete.

Quando si crea un catalogo Quick Deploy (Distribuzione rapida), si indica se e come gli utenti accedono alle posizioni e alle risorse sulla loro rete aziendale on-premise dai loro desktop e app Citrix. Quando si utilizza una connessione, è necessario creare la connessione prima di creare il catalogo.

Quando si utilizza una sottoscrizione Citrix Managed Azure, le opzioni disponibili sono:

- No connectivity (Nessuna connettività)
- Azure VNet peering (Peering di Azure VNet)
- SD-WAN

Non è possibile modificare il tipo di connessione di un catalogo dopo la creazione del catalogo.

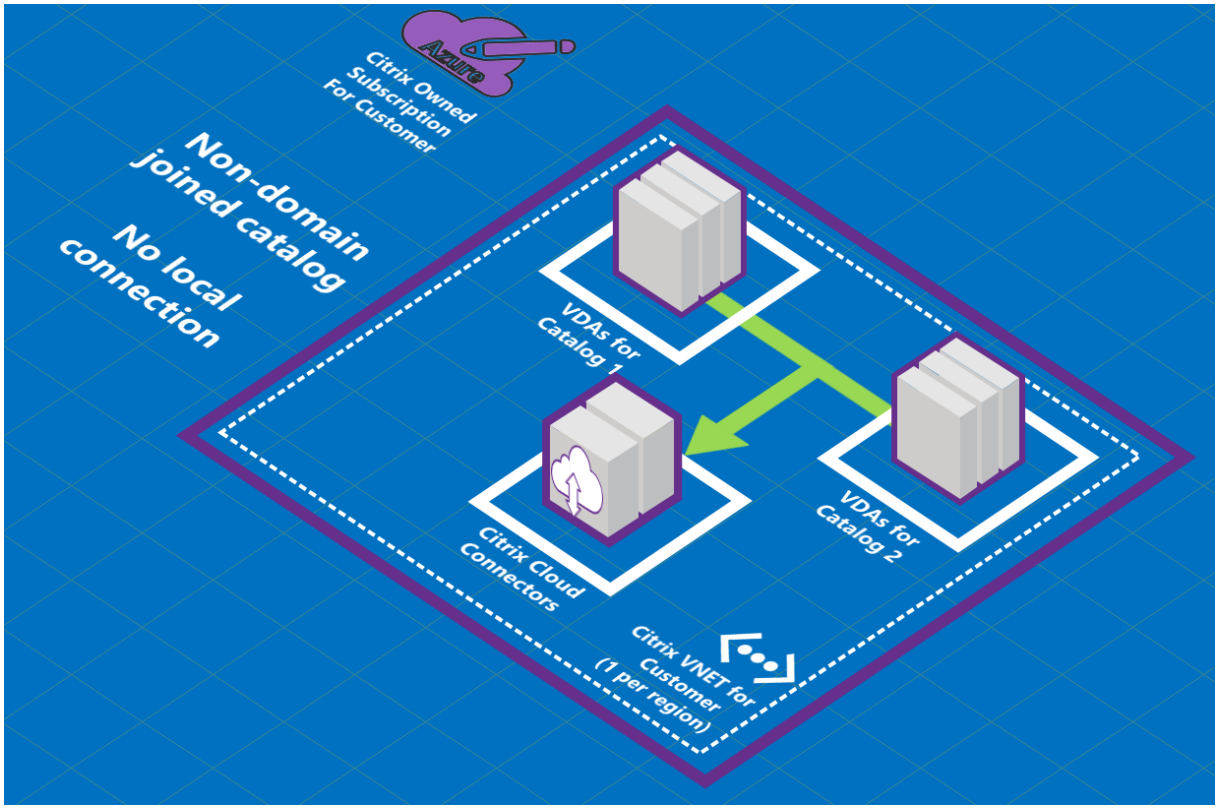
## Requisiti per tutte le connessioni di rete

- Quando si crea una connessione, è necessario disporre di voci del server DNS valide.
- Quando si utilizza Secure DNS o un provider DNS di terze parti, è necessario aggiungere l'intervallo di indirizzi allocato per l'utilizzo da parte di Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) agli indirizzi IP del provider DNS nell'elenco di indirizzi consentiti. Tale intervallo di indirizzi viene specificato quando si crea una connessione.
- Tutte le risorse di servizio che utilizzano la connessione (macchine aggiunte al dominio) devono essere in grado di raggiungere il server NTP (Network Time Protocol) per garantire la sincronizzazione oraria.

## No connectivity (Nessuna connettività)

Quando un catalogo è configurato con **No connectivity** (Nessuna connettività), gli utenti non possono accedere alle risorse sulla propria rete on-premise o su altre reti. Questa è l'unica scelta quando si crea un catalogo utilizzando la creazione rapida.

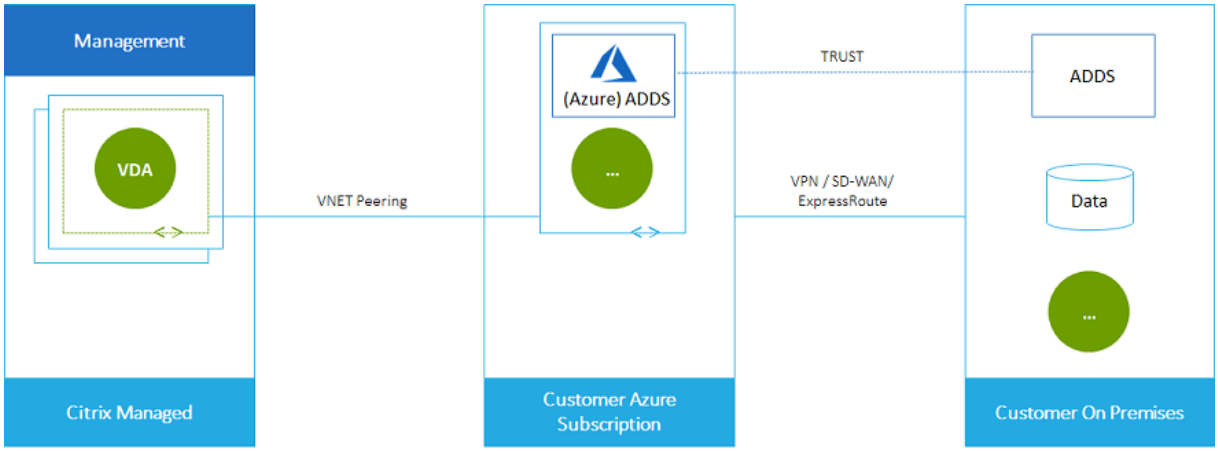
 




### Informazioni sulle connessioni di peering della rete virtuale di Azure

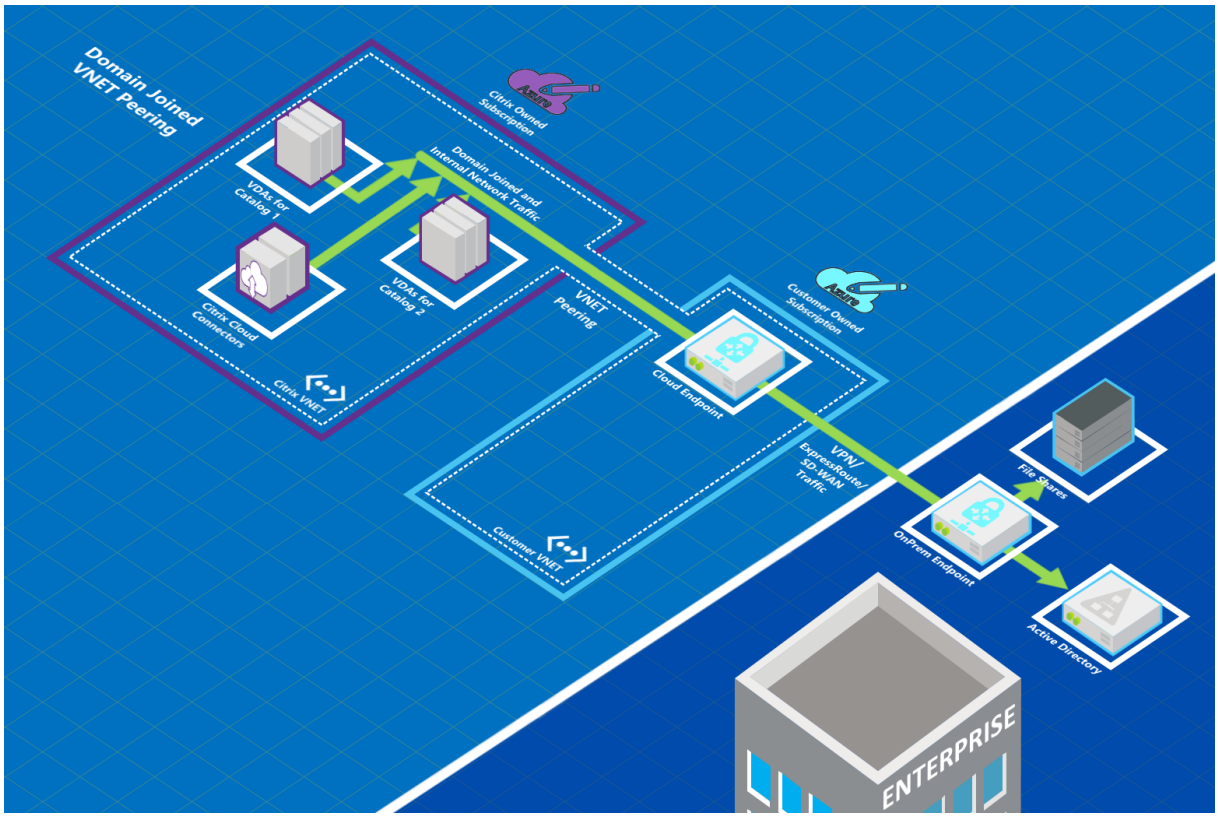
Il peering della rete virtuale connette senza problemi due reti virtuali (VNet) di Azure: la propria e la VNet Citrix DaaS. Il peering consente inoltre agli utenti di accedere a file e altri elementi dalle reti on-premise.

Come illustrato nell'immagine seguente, si crea una connessione utilizzando il peering della rete virtuale di Azure dalla sottoscrizione Citrix Managed Azure alla VNet nella sottoscrizione Azure della propria azienda.



Ecco un'altra illustrazione del peering della rete virtuale.




Gli utenti possono accedere alle proprie risorse di rete (ad esempio i file server) unendosi al dominio locale quando si crea un catalogo (ossia, ci si unisce al dominio AD in cui risiedono le condivisioni di file e altre risorse necessarie). La propria sottoscrizione di Azure si connette a tali risorse (nelle immagini, utilizzando una VPN o Azure ExpressRoute). Quando si crea il catalogo, si forniscono le credenziali del dominio, dell'unità organizzativa e dell'account.

> **Importante:**
>
> - È necessario acquisire ulteriori informazioni sul peering della rete virtuale di Azure prima di utilizzarlo in questo servizio.
> - Creare una connessione di peering della rete virtuale prima di creare un catalogo che la utilizzi.

### Route personalizzate per il peering della rete virtuale di Azure

Le route personalizzate o definite dall'utente sostituiscono le route di sistema predefinite di Azure per indirizzare il traffico tra macchine virtuali in un peering della rete virtuale, reti on-premise e Internet. È possibile utilizzare route personalizzate se ci sono reti a cui si prevede accederanno le risorse Citrix DaaS, ma che non sono collegate direttamente tramite peering della rete virtuale. Ad esempio, è possibile creare una ruote personalizzata che forza il traffico verso Internet o verso una subnet di rete

on-premise attraverso un'appliance di rete.

Per utilizzare route personalizzate:

- È necessario disporre di un gateway di rete virtuale di Azure esistente o di un'appliance di rete come Citrix SD-WAN nell'ambiente Citrix DaaS.
- Quando si aggiungono route personalizzate, è necessario aggiornare le tabelle delle route aziendali con le informazioni della rete virtuale di destinazione di Citrix DaaS per garantire la connettività end-to-end.
- Le route personalizzate vengono visualizzate in Citrix DaaS nell'ordine in cui sono state inserite. Questo ordine di visualizzazione non influisce sull'ordine in cui Azure seleziona le route.

Prima di utilizzare route personalizzate, consultare l'articolo Microsoft Routing del traffico di rete virtuale per informazioni sull'utilizzo di route personalizzate, tipi di hop successivi e su come Azure seleziona le route per il traffico in uscita.

È possibile aggiungere route personalizzate quando si crea una connessione di peering della rete virtuale di Azure o a percorsi esistenti nel proprio ambiente Citrix DaaS. Quando si è pronti per utilizzare route personalizzate con il peering della rete virtuale, fare riferimento alle seguenti sezioni in questo articolo:

- Per route personalizzate con nuovi peering della rete virtuale di Azure: Creare una connessione di peering della rete virtuale di Azure
- Per route personalizzate con peering della rete virtuale di Azure esistenti: Gestire route personalizzate per le connessioni di peering della rete virtuale di Azure esistenti

#### Requisiti e preparazione per il peering della rete virtuale di Azure

- Credenziali per il proprietario di una sottoscrizione di Azure. Deve essere un account Azure Active Directory. Questo servizio non supporta altri tipi di account, ad esempio live.com o account Azure AD esterni (in un tenant diverso).
- Una sottoscrizione di Azure, un gruppo di risorse e una rete virtuale (VNet).
- Configurare le route di rete di Azure in modo che i VDA nella sottoscrizione Citrix Managed Azure possano comunicare con i percorsi di rete.
- Aprire i gruppi di sicurezza della rete Azure dalla propria rete virtuale all'intervallo di indirizzi IP specificato.
- **Active Directory:** per gli scenari aggiunti al dominio, si consiglia di avere un qualche tipo di servizi Active Directory in esecuzione nella rete virtuale con peering. Questi sfruttano le caratteristiche di bassa latenza della tecnologia di peering della rete virtuale di Azure.

Ad esempio, la configurazione potrebbe includere Azure Active Directory Domain Services (AADDS), una macchina virtuale controller di dominio nella rete virtuale o Azure AD Connect nella Active Directory locale.

Dopo aver abilitato AADDS, non è possibile spostare il dominio gestito su una rete virtuale diversa senza eliminare il dominio gestito. Pertanto, è importante selezionare la rete virtuale corretta per abilitare il dominio gestito. Prima di procedere, leggere l'articolo Microsoft Considerazioni sulla progettazione della rete per servizi di dominio Azure AD.

- **Intervallo IP VNet:** quando si crea la connessione, è necessario fornire uno spazio di indirizzi CIDR disponibile (indirizzo IP e prefisso di rete) che sia univoco tra le risorse di rete e le reti virtuali di Azure connesse. Questo è l'intervallo di indirizzi IP assegnato alle macchine virtuali all'interno della rete virtuale con peering di Citrix DaaS.

  Assicurarsi di specificare un intervallo di indirizzi IP che non si sovrapponga agli indirizzi utilizzati nelle reti Azure e on-premise.

  - Ad esempio, se la rete virtuale di Azure ha uno spazio di indirizzi 10.0.0.0 /16, creare la connessione di peering della rete virtuale in Citrix DaaS come 192.168.0.0 /24 o similare.
  - In questo esempio, la creazione di una connessione di peering con un intervallo di indirizzi IP 10.0.0.0 /24 sarebbe considerata un intervallo di indirizzi sovrapposto.

  Se gli indirizzi si sovrappongono, la connessione di peering della rete virtuale potrebbe non essere creata correttamente. Inoltre, non funziona correttamente per le attività di amministrazione del sito.

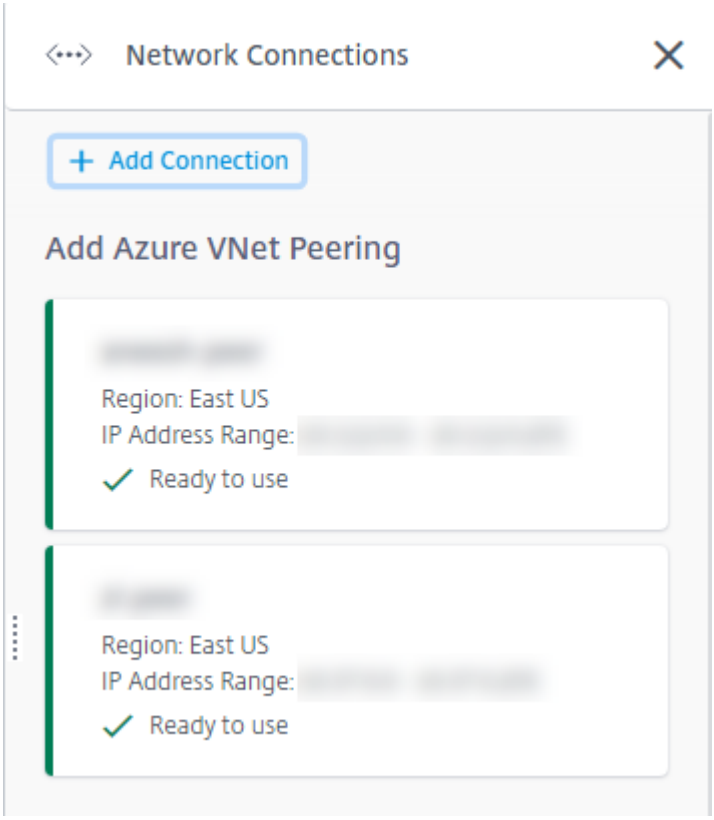
Per informazioni sul peering della rete virtuale, consultare i seguenti articoli Microsoft.

- Peering di rete virtuale
- Gateway VPN di Azure
- Creare una connessione da sito a sito nel portale di Azure
- Domande frequenti sul gateway VPN (cercare "sovrapposizione")

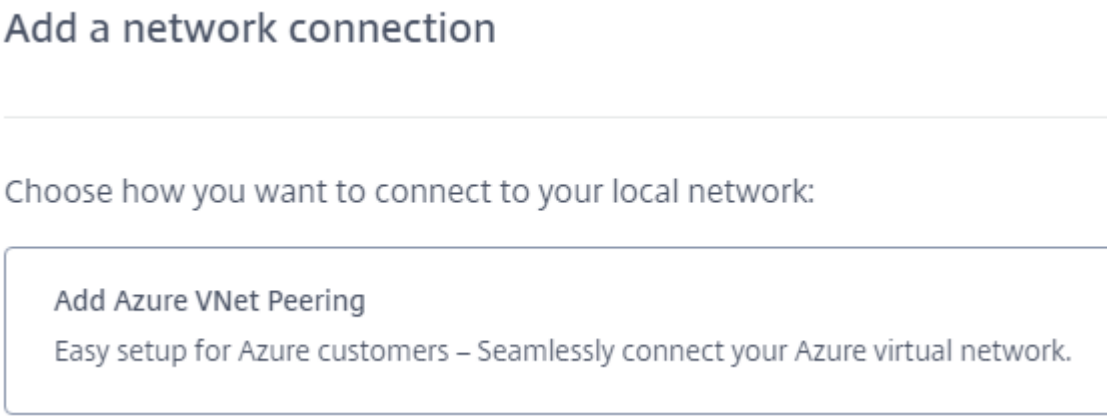
#### Creare una connessione di peering della rete virtuale di Azure

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra. Se sono già impostate delle connessioni, vengono elencate.

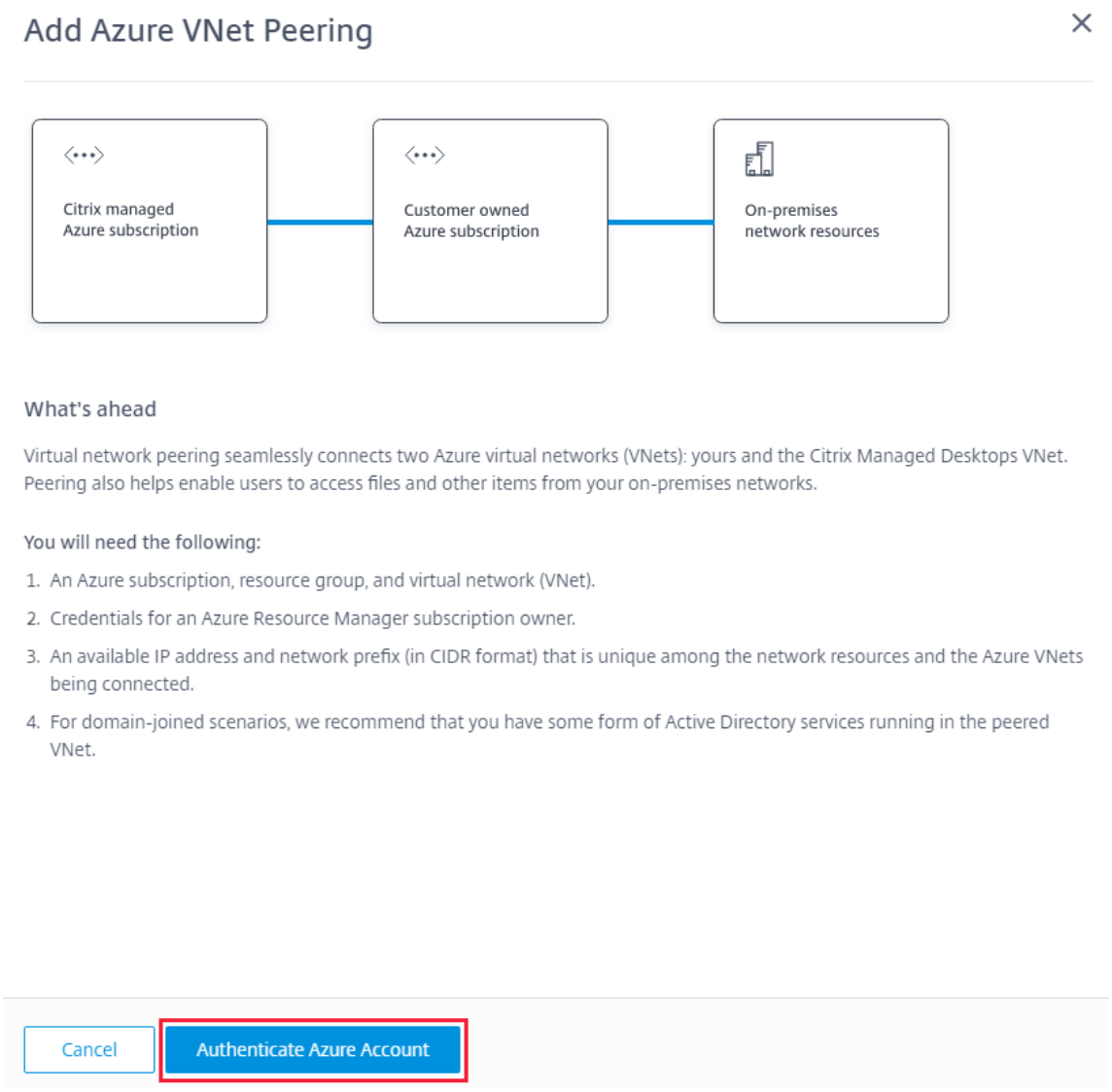



2. Selezionare **Add Connection** (Aggiungi connessione).
3. Fare clic in un punto qualsiasi della casella **Add Azure VNet Peering** (Aggiungi peering della rete virtuale di Azure).



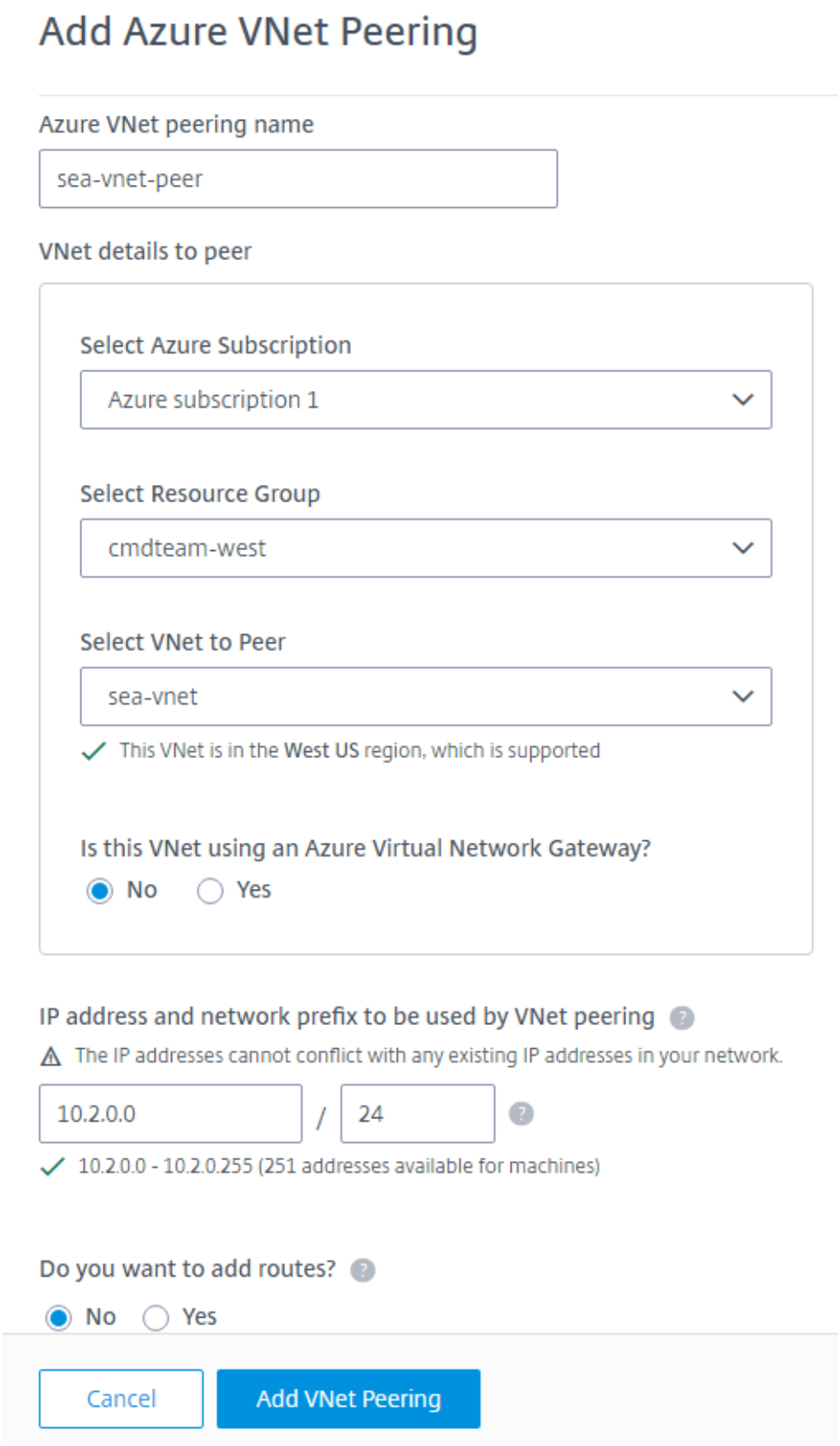

4. Selezionare **Authenticate Azure Account** (Autentica account Azure).




5. Citrix DaaS porta automaticamente alla pagina di accesso di Azure per autenticare le sottoscrizioni di Azure. Dopo aver effettuato l'accesso ad Azure (con le credenziali dell'account amministratore globale) e aver accettato i termini, si ritorna alla finestra di dialogo dei dettagli di creazione della connessione.



6. Digitare un nome per il peer della rete virtuale di Azure.
7. Selezionare la sottoscrizione di Azure, il gruppo di risorse e la rete virtuale di cui eseguire il peering.
8. Indicare se la rete virtuale selezionata utilizza un gateway di rete virtuale di Azure. Per informazioni, vedere l'articolo Microsoft Gateway VPN di Azure.
9. Se si ha risposto **Yes** (Sì) nel passaggio precedente (la rete virtuale utilizza un gateway di rete virtuale di Azure), indicare se si desidera abilitare la propagazione della route del gateway di rete virtuale. Se abilitata, Azure apprende automaticamente (aggiunge) tutte le route tramite il gateway.

   È possibile modificare questa impostazione in un secondo momento nella pagina **Details** (Dettagli) della connessione. Tuttavia, questa modifica può causare modifiche al formato di route e interruzioni del traffico VDA. Inoltre, se si disattiva questa opzione in un secondo momento, è necessario aggiungere manualmente route alle reti che verranno utilizzate dai VDA.
10. Digitare un indirizzo IP e selezionare una network mask. Viene visualizzato l'intervallo di indirizzi da utilizzare, oltre al numero di indirizzi supportati dall'intervallo. Assicurarsi che l'intervallo di indirizzi IP non si sovrapponga agli indirizzi utilizzati nelle reti Azure e on-premise.

    - Ad esempio, se la rete virtuale di Azure ha uno spazio di indirizzi 10.0.0.0 /16, creare la connessione di peering della rete virtuale in Citrix DaaS come 192.168.0.0 /24 o similare.
    - In questo esempio, la creazione di una connessione di peering della rete virtuale con un intervallo di indirizzi IP 10.0.0.0 /24 è considerata un intervallo di indirizzi sovrapposto.

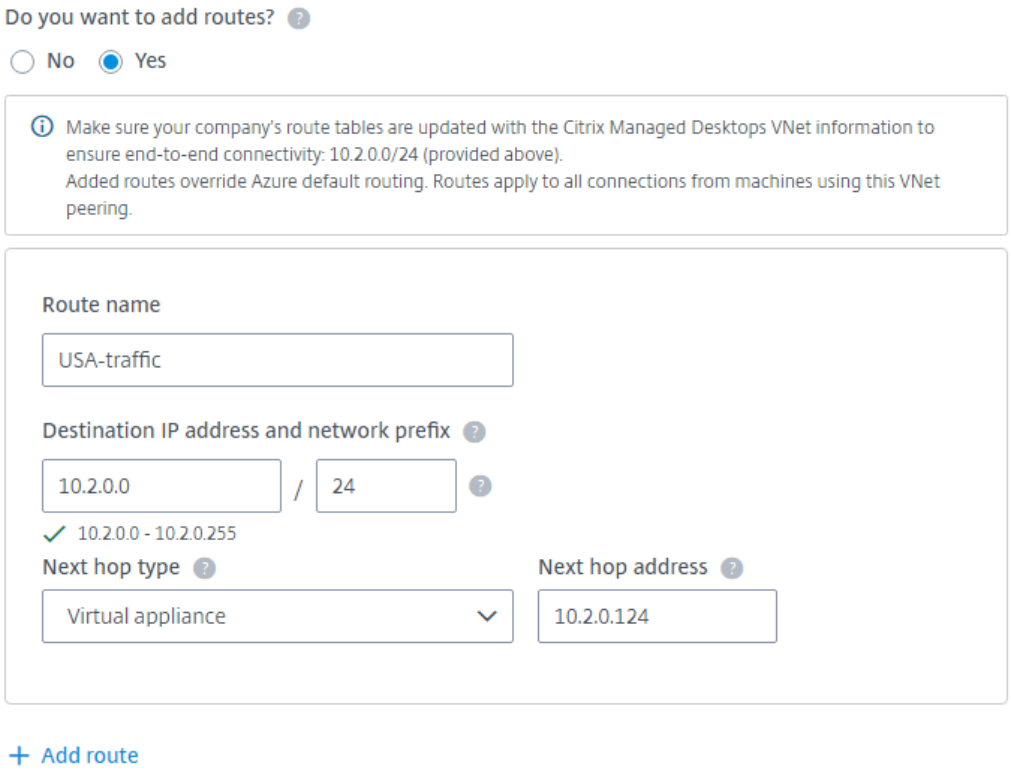
    Se gli indirizzi si sovrappongono, la connessione di peering della rete virtuale potrebbe non essere creata correttamente. Inoltre, non funzionerà correttamente per le attività di amministrazione del sito.
11. Indicare se si desidera aggiungere route personalizzate alla connessione di peering della rete virtuale. Se si seleziona **Yes** (Sì), immettere le seguenti informazioni:

    a) Digitare un nome descrittivo per la route personalizzata.

    b) Immettere l'indirizzo IP di destinazione e il prefisso di rete. Il prefisso di rete deve essere compreso tra 16 e 24.

    c) Selezionare un tipo di hop successivo per il punto in cui si desidera che il traffico venga instradato. Se si seleziona **Virtual appliance** (Appliance virtuale), immettere l'indirizzo IP interno dell'appliance.




Per ulteriori informazioni sui tipi di hop successivi, vedere la sezione Route personalizzate nell'articolo Microsoft *Routing del traffico di rete virtuale*.

d) Per creare un'altra route personalizzata per la connessione, selezionare **Add route** (Aggiungi route).

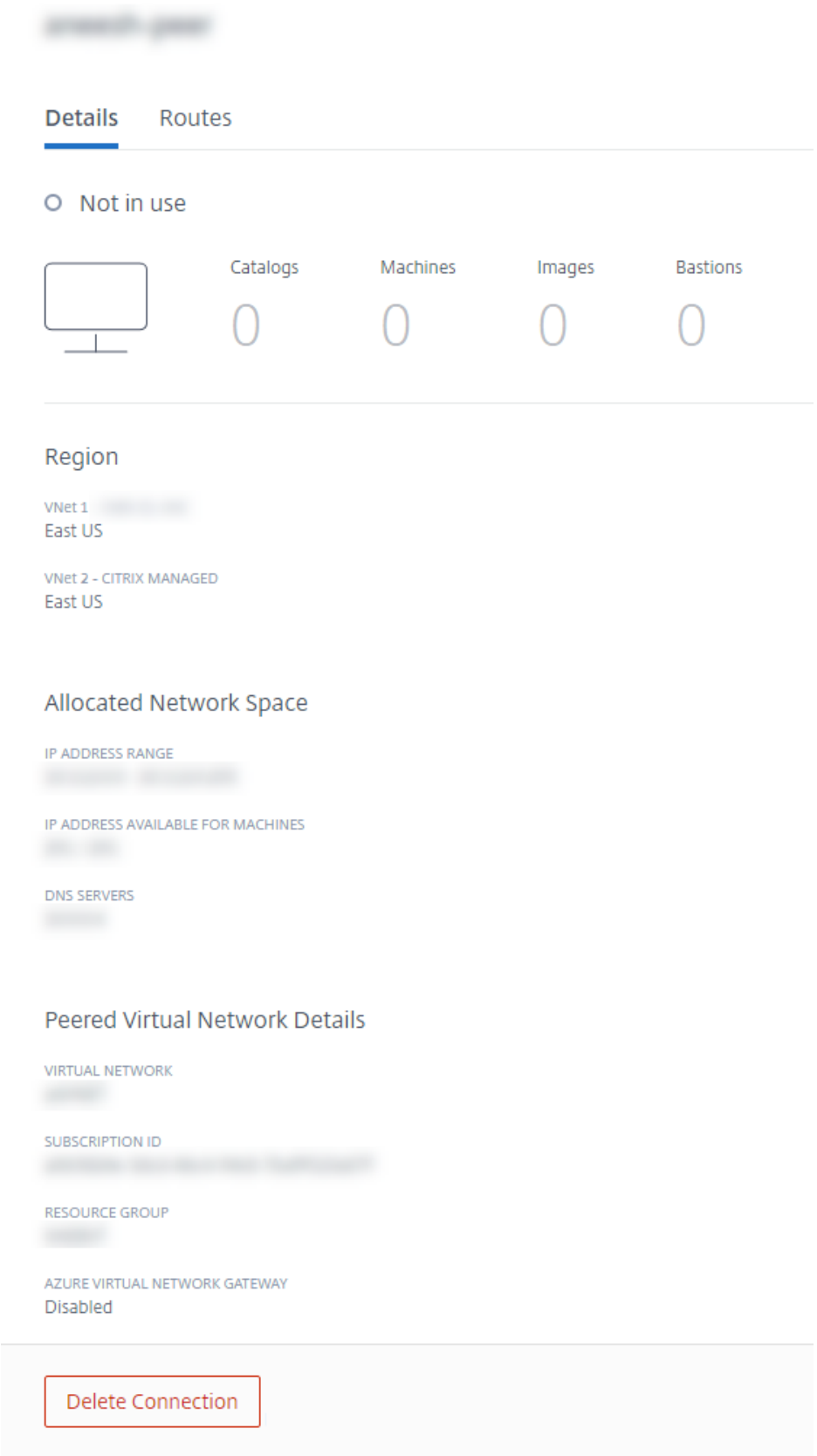
12. Selezionare **Add VNet Peering** (Aggiungi peering della rete virtuale).

Dopo che la connessione è stata creata, viene elencata in **Network Connections > Azure VNet Peers** (Connessioni di rete > Peer della rete virtuale di Azure) sul lato destro della dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida). Quando si crea un catalogo, questa connessione viene inclusa nell'elenco delle connessioni di rete disponibili.

**Visualizzare i dettagli della connessione di peering della rete virtuale di Azure**



1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare la connessione di peering della rete virtuale di Azure che si desidera visualizzare.

I dettagli includono:

- Il numero di cataloghi, macchine, immagini e bastion che utilizzano questa connessione.
- La regione, lo spazio di rete allocato e le reti virtuali con peering.
- Le route attualmente configurate per la connessione di peering della rete virtuale.

#### Gestire route personalizzate per le connessioni peer della rete virtuale di Azure esistenti

È possibile aggiungere nuove route personalizzate a una connessione esistente o modificare route personalizzate esistenti, inclusa la disabilitazione o l'eliminazione di route personalizzate.

> **Importante:**
>
> La modifica, la disattivazione o l'eliminazione di route personalizzate modifica il flusso di traffico della connessione e potrebbe interrompere qualsiasi sessione utente che potrebbe essere attiva.

Per aggiungere una route personalizzata:

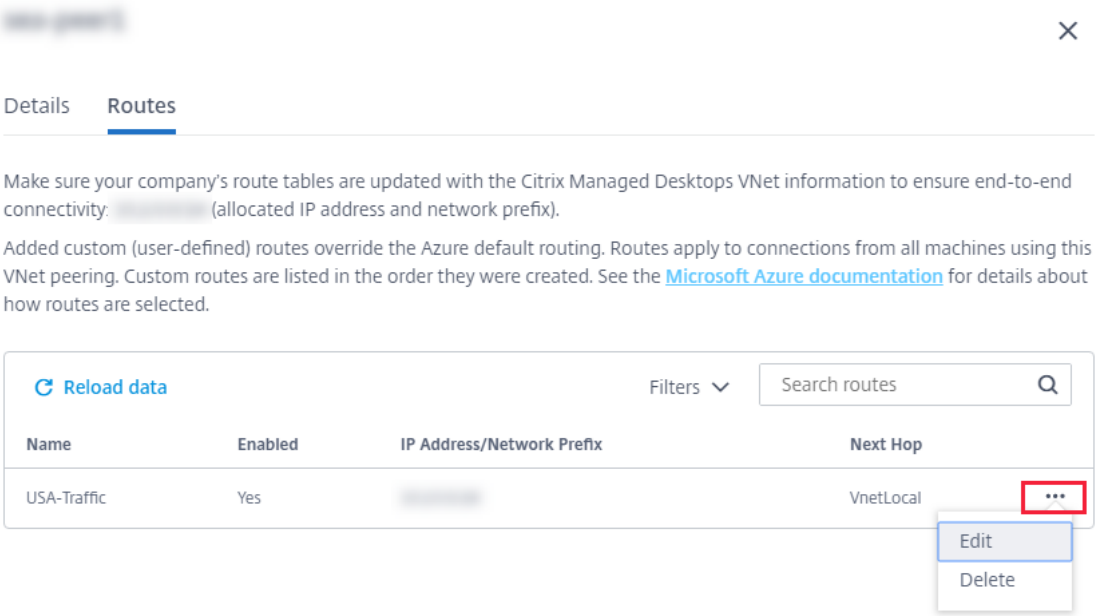
1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare la connessione che si desidera eliminare.
3. Dai dettagli della connessione, selezionare **Routes** (Route) e quindi selezionare **Add Route** (Aggiungi route).
4. Immettere un nome descrittivo, l'indirizzo IP e il prefisso di destinazione e il tipo di hop successivo che si desidera utilizzare. Se si seleziona **Virtual Appliance** (Appliance virtuale) come tipo di hop successivo, immettere l'indirizzo IP interno dell'appliance.
5. Indicare se si desidera abilitare la route personalizzata. Per impostazione predefinita, la route personalizzata è abilitata.
6. Selezionare **Add Route** (Aggiungi route).

Per modificare o disabilitare una route personalizzata:

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare la connessione che si desidera eliminare.
3. Dai dettagli della connessione, selezionare **Routes** (Route) e quindi individuare la route personalizzata che si desidera gestire.

4. Dal menu con i puntini di sospensione, selezionare **Edit** (Modifica).




5. Apportare le modifiche necessarie all'indirizzo IP e al prefisso di destinazione o al tipo di hop successivo, in base alle esigenze.
6. Per abilitare o disabilitare una route personalizzata, in **Enable this route?** (Abilitare questa route?) selezionare **Yes** (Sì) o **No**.
7. Selezionare **Save** (Salva).

Per eliminare una route personalizzata:

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare la connessione che si desidera eliminare.
3. Dai dettagli della connessione, selezionare **Routes** (Route) e quindi individuare la route personalizzata che si desidera gestire.
4. Dal menu con i puntini di sospensione, selezionare **Delete** (Elimina).
5. Selezionare **Deleting a route may disrupt active sessions** (L'eliminazione di una route potrebbe interrompere le sessioni attive) per confermare di aver compreso l'impatto dell'eliminazione della route personalizzata.
6. Selezionare **Delete Route** (Elimina route).

### Eliminare una connessione di peering della rete virtuale di Azure

Prima di poter eliminare una connessione di peering della rete virtuale di Azure, rimuovere tutti i cataloghi associati. Vedere Eliminare un catalogo.

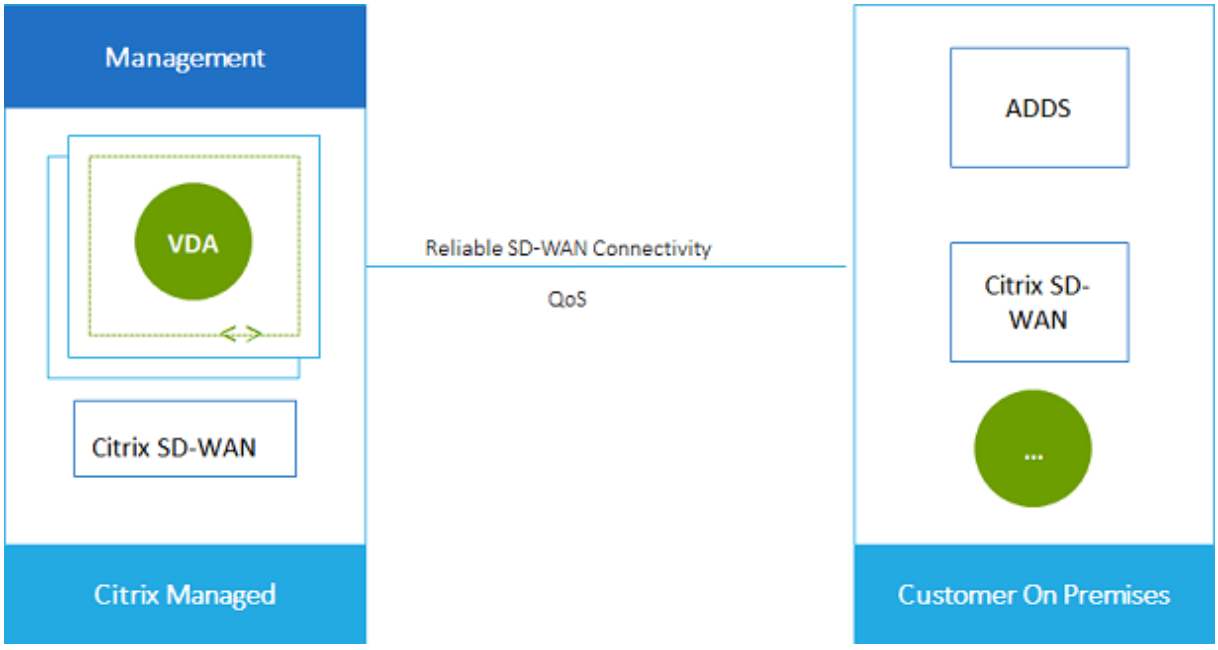
1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare la connessione che si desidera eliminare.
3. Dai dettagli della connessione, selezionare **Delete Connection** (Elimina connessione).

### Informazioni sulle connessioni SD-WAN

Citrix SD-WAN ottimizza tutte le connessioni di rete necessarie a Citrix DaaS. Lavorando insieme alle tecnologie HDX, Citrix SD-WAN fornisce qualità del servizio e affidabilità di connessione per il traffico ICA e Citrix DaaS fuori banda. Citrix SD-WAN supporta le seguenti connessioni di rete:

- Connessione ICA multi-stream tra gli utenti e i loro desktop virtuali
- Accesso a Internet dal desktop virtuale a siti web, app SaaS e altre proprietà cloud
- Accesso dal desktop virtuale a risorse on-premise come Active Directory, file server e server di database
- Traffico in tempo reale/interattivo trasferito su RTP dal motore multimediale nell'app Workspace ai servizi Unified Communications ospitati nel cloud come Microsoft Teams
- Recupero lato client di video da siti come YouTube e Vimeo

Come illustrato nell'immagine seguente, si crea una connessione SD-WAN dalla sottoscrizione Citrix Managed Azure ai propri siti. Durante la creazione della connessione, le appliance VPX SD-WAN vengono create nella sottoscrizione Citrix Managed Azure. Dal punto di vista della SD-WAN, tale posizione viene trattata come una filiale.



### Requisiti e preparazione della connessione SD-WAN

- Se i seguenti requisiti non sono soddisfatti, l'opzione di connessione di rete SD-WAN non è disponibile.
  - Diritti ai servizi Citrix Cloud: Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) e SD-WAN Orchestrator.
  - Una distribuzione SD-WAN installata e configurata. La distribuzione deve includere un Master Control Node (MCN), nel cloud o on-premise, ed essere gestita con SD-WAN Orchestrator.
- Intervallo di indirizzi IP VNet: fornisce uno spazio di indirizzi CIDR disponibile (indirizzo IP e prefisso di rete) univoco tra le risorse di rete che vengono collegate. Questo è l'intervallo di indirizzi IP assegnato alle macchine virtuali all'interno della rete virtuale di Citrix DaaS.

  Assicurarsi di specificare un intervallo di indirizzi IP che non si sovrapponga agli indirizzi utilizzati nelle reti cloud e on-premise.
  - Ad esempio, se la rete ha uno spazio di indirizzi 10.0.0.0 /16, creare la connessione in Citrix DaaS come 192.168.0.0 /24 o similare.
  - In questo esempio, la creazione di una connessione con un intervallo di indirizzi IP 10.0.0.0 /24 verrà considerata un intervallo di indirizzi sovrapposto.

  Se gli indirizzi si sovrappongono, la connessione potrebbe non essere stata creata correttamente. Inoltre, non funziona correttamente per le attività di amministrazione del sito.
- Il processo di configurazione della connessione include attività che l'utente (l'amministratore Citrix DaaS) e l'amministratore di SD-WAN Orchestrator devono completare. Inoltre, per completare le attività, sono necessarie le informazioni fornite dall'amministratore di SD-WAN Orchestrator.

  Prima della creazione effettiva di una connessione, si consiglia di consultare sia le linee guida contenute in questo documento che la documentazione di SD-WAN.

### Creare una connessione SD-WAN

> **Importante:**
>
> Per i dettagli sulla configurazione di SD-WAN, consultare Configurazione di SD-WAN per l'integrazione con Citrix DaaS.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare **Add Connection** (Aggiungi connessione).

3. Nella pagina **Add a network connection** (Aggiungi una connessione di rete), fare clic in un punto qualsiasi della casella SD-WAN.
4. La pagina successiva riassume i passi da intraprendere. Al termine della lettura, selezionare **Start Configuring SD-WAN** (Avvia la configurazione di SD-WAN).
5. Nella pagina **Configure SD-WAN** (Configura SD-WAN), immettere le informazioni fornite dall'amministratore di SD-WAN Orchestrator.

    - **Modalità di distribuzione:** se si seleziona **High availability** (Alta disponibilità), vengono create due appliance VPX (consigliate per gli ambienti di produzione). Se si seleziona **Standalone**, viene creata una sola appliance. Non è possibile modificare questa impostazione in seguito. Per passare alla modalità di distribuzione, è necessario eliminare e ricreare la filiale e tutti i cataloghi associati.
    - **Name** (Nome): digitare un nome per il sito SD-WAN.
    - **Throughput and number of offices** (Throughput e numero di uffici): queste informazioni sono fornite dall'amministratore di SD-WAN Orchestrator.
    - **Region** (Regione): la regione in cui verranno create le appliance VPX.
    - **VDA subnet and SD-WAN subnet** (Subnet VDA e subnet SD-WAN): queste informazioni sono fornite dall'amministratore di SD-WAN Orchestrator. Vedere Requisiti e preparazione della connessione SD-WAN per informazioni su come evitare i conflitti.
6. Al termine, selezionare **Create Branch** (Crea filiale).
7. La pagina successiva riassume cosa cercare nella dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida). Al termine della lettura, selezionare **Got it** (OK).
8. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), la nuova voce SD-WAN in **Network Connections** (Connessioni di rete) mostra lo stato di avanzamento del processo di configurazione. Quando la voce diventa arancione con il messaggio `Awaiting activation by SD-WAN administrator`, avvisare l'amministratore di SD-WAN Orchestrator.
9. Per le attività di amministratore di SD-WAN Orchestrator, vedere la documentazione del prodotto SD-WAN Orchestrator.
10. Al termine delle operazioni dell'amministratore di SD-WAN Orchestrator, la voce SD-WAN in **Network Connections** (Connessioni di rete) diventa verde, con il messaggio `You can create catalogs using this connection`.

#### Visualizzare i dettagli della connessione SD-WAN

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare **SD-WAN** se non è l'unica selezione.

3. Selezionare la connessione che si desidera visualizzare.

La visualizzazione include:

- **Scheda Details (Dettagli):** informazioni specificate durante la configurazione della connessione.
- **Scheda Branch Connectivity (Connettività filiale):** nome, connettività cloud, disponibilità, livello di larghezza di banda, ruolo e posizione per ogni filiale e MCN.

#### Eliminare una connessione SD-WAN

Prima di poter eliminare una connessione SD-WAN, rimuovere tutti i cataloghi associati. Vedere Eliminare un catalogo.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
2. Selezionare SD-WAN se non è l'unica selezione.
3. Selezionare la connessione che si desidera eliminare per espanderne i dettagli.
4. Nella scheda **Details** (Dettagli), selezionare **Delete Connection** (Elimina connessione).
5. Confermare l'eliminazione.

## Utenti e autenticazione in Quick Deploy

October 30, 2023

### Metodi di autenticazione utente

Gli utenti devono autenticarsi quando accedono a Citrix Workspace per avviare il desktop o le app.

Quick Deploy (Distribuzione rapida) supporta i seguenti metodi di autenticazione utente:

- **Managed Azure AD:** Managed Azure AD è un'Azure Active Directory (AAD) fornita e gestita da Citrix. Non è necessario fornire la propria struttura di Active Directory. È sufficiente aggiungere i propri utenti alla directory.
- **Provider di identità**: è possibile utilizzare qualsiasi metodo di autenticazione disponibile in Citrix Cloud.

> **Nota:**
>
> - Le distribuzioni di Remote PC Access (Accesso remoto PC) utilizzano solo Active Directory.

> Per ulteriori informazioni, vedere Remote PC Access (Accesso remoto PC).
>
> - Se si utilizza Azure AD Domain Services: gli UPN di accesso a Workspace devono contenere il nome di dominio specificato durante l'abilitazione di Azure AD Domain Services. Gli accessi non possono utilizzare gli UPN per un dominio personalizzato creato dall'utente, anche se tale dominio personalizzato è designato come primario.

L'impostazione dell'autenticazione utente include le seguenti procedure:

1. Configurare il metodo di autenticazione utente in Citrix Cloud e Workspace Configuration (Configurazione di Workspace).
2. Se si utilizza Managed Azure AD per l'autenticazione utente, aggiungere utenti alla directory.
3. Aggiungere utenti a un catalogo.

### Configurare l'autenticazione utente in Citrix Cloud

Per configurare l'autenticazione utente in Citrix Cloud:

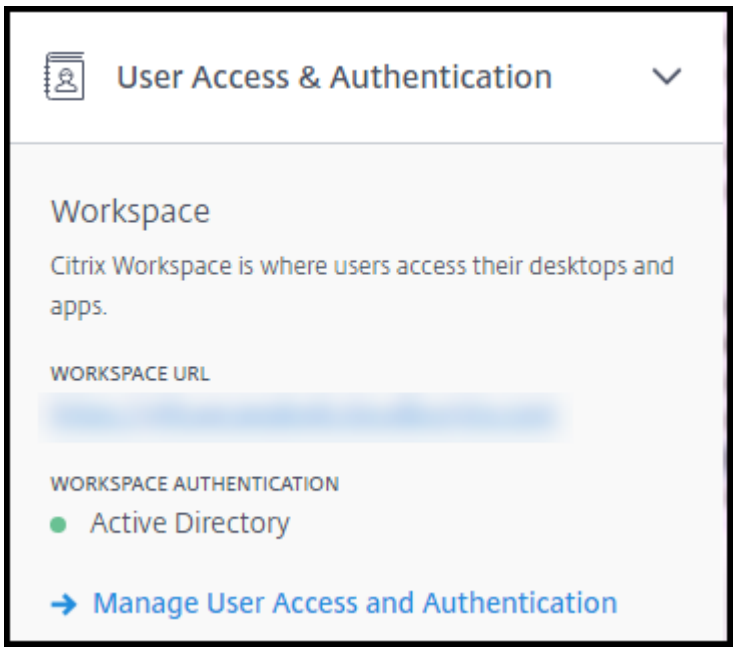
- Connettersi al metodo di autenticazione utente che si desidera utilizzare (in Citrix Cloud, l'utente si "connette"o si "disconnette"da un metodo di autenticazione).
- In Citrix Cloud, impostare l'autenticazione di Workspace per utilizzare il metodo connesso.

> **Nota:**
>
> Il metodo di autenticazione Managed Azure AD è configurato per impostazione predefinita, il che significa che viene automaticamente connesso in Citrix Cloud e l'autenticazione di Workspace viene impostata automaticamente per l'utilizzo di Managed Azure AD per Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). Se si desidera utilizzare questo metodo (e non si è precedentemente configurato un metodo diverso), continuare con Aggiungere ed eliminare utenti in Managed Azure AD.
> Se Managed Azure AD è disconnesso, l'autenticazione di Workspace passerà ad Active Directory. Se si desidera utilizzare un metodo di autenticazione diverso, procedere nel modo seguente.

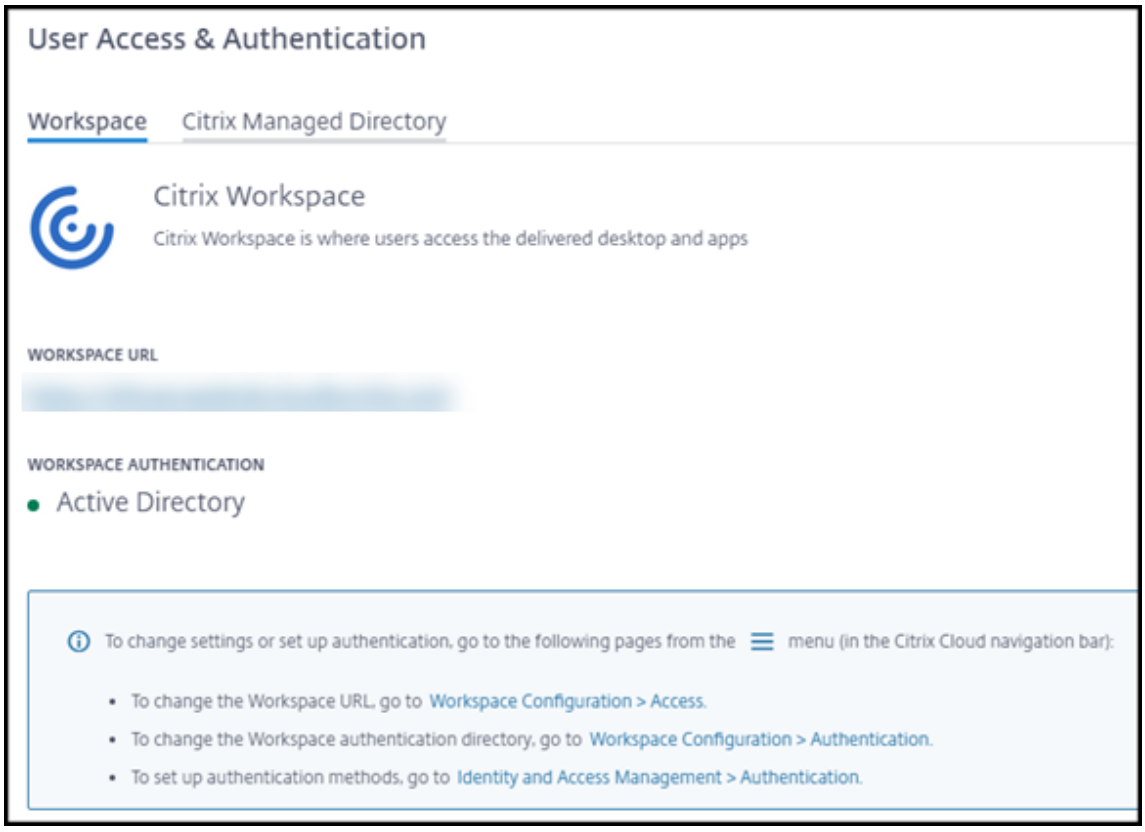
Per modificare il metodo di autenticazione:

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), selezionare **User Access & Authentication** (Accesso utente e autenticazione) a destra.




2. Selezionare **Manage User Access and Authentication** (Gestisci accesso e autenticazione utente). Selezionare la scheda **Workspace**, se non è già selezionata (l'altra scheda indica il metodo di autenticazione utente attualmente configurato).




3. Seguire il link **Per configurare i metodi di autenticazione**. Questo link porta a Citrix Cloud.

Selezionare **Connect** (Connetti) nel menu con i puntini di sospensione per il metodo desiderato.

4. Mentre si è ancora in Citrix Cloud, selezionare **Workspace Configuration** (Configurazione di Workspace) nel menu in alto a sinistra. Nella scheda **Authentication** (Autenticazione), selezionare il metodo desiderato.

Passi successivi:

- Se si utilizza Managed Azure AD, aggiungere utenti alla directory.
- Per tutti i metodi di autenticazione, aggiungere utenti al catalogo.

### Aggiungere ed eliminare utenti in Managed Azure AD

Completare questa procedura solo se si utilizza Managed Azure AD per l'autenticazione utente a Citrix Workspace.

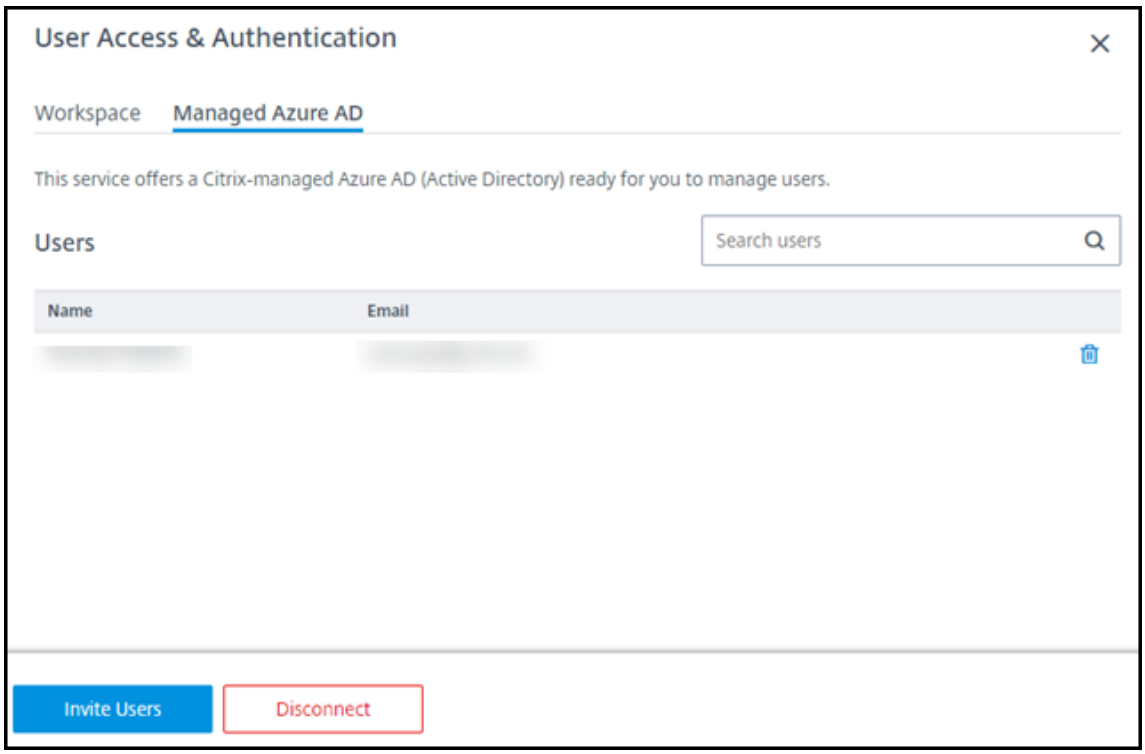
Fornire il nome e gli indirizzi e-mail dei propri utenti. Citrix invia quindi un invito via e-mail a ciascun utente. L'e-mail indica agli utenti di selezionare un link per raggiungere Citrix Managed Azure AD.

- Se l'utente dispone già di un account Microsoft con l'indirizzo e-mail fornito, viene utilizzato questo account.
- Se l'utente non dispone di un account Microsoft con l'indirizzo e-mail, Microsoft crea un account.

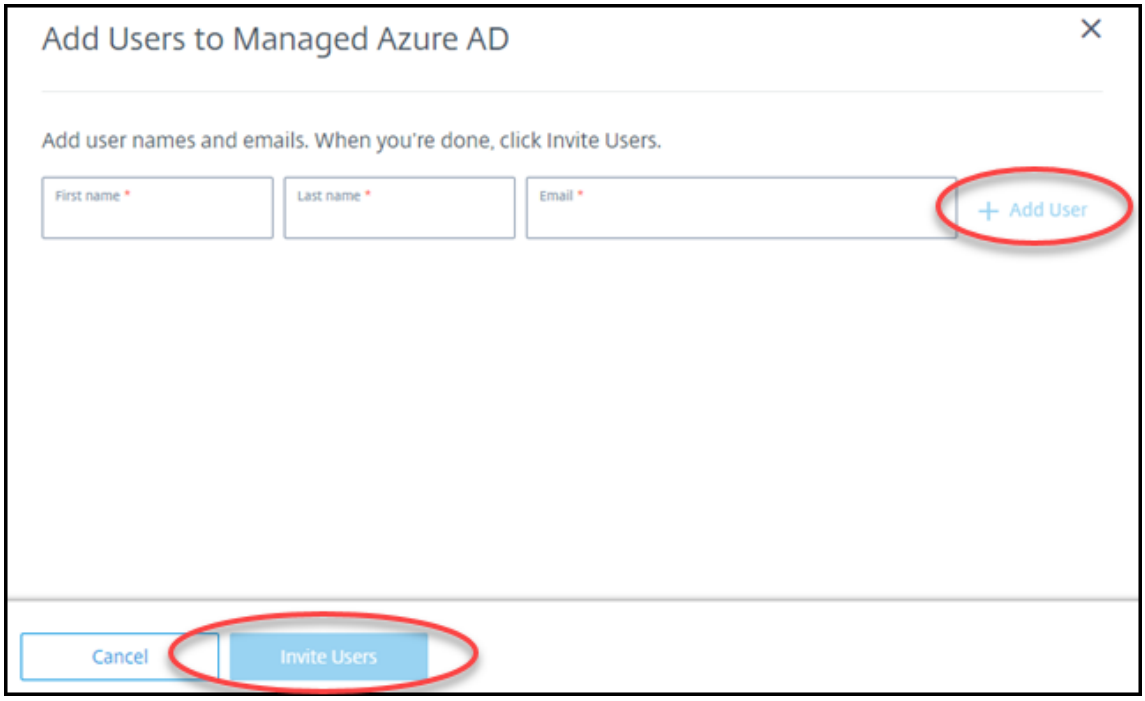
Per aggiungere e invitare utenti a Managed Azure AD:

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **User Access & Authentication** (Accesso utente e autenticazione) a destra. Selezionare **Manage User Access and Authentication** (Gestisci accesso e autenticazione utente).
2. Selezionare la scheda **Managed Azure AD**.
3. Selezionare **Invite Users** (Invita utenti).




4. Digitare il nome e l'indirizzo e-mail di un utente, quindi selezionare **Add User** (Aggiungi utente).




5. Ripetere il passaggio precedente per aggiungere altri utenti.
6. Quando si ha finito di aggiungere le informazioni sull'utente, selezionare **Invite Users** (Invita utenti) nella parte inferiore della scheda.

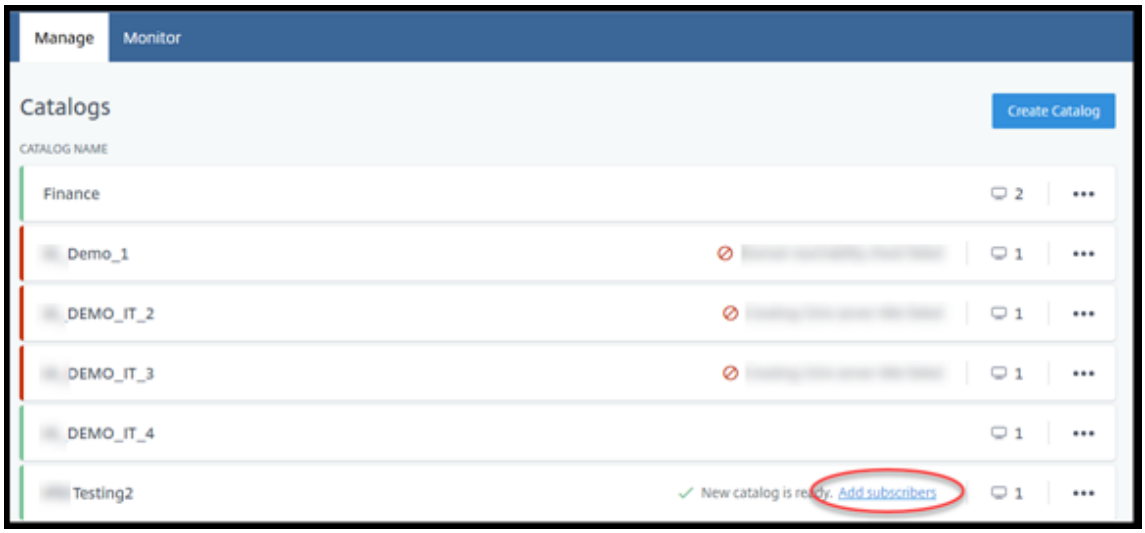
Per eliminare un utente da Managed Azure AD, selezionare l'icona del cestino accanto al nome dell'utente che si desidera eliminare dalla directory. Confermare l'eliminazione.

Passaggio successivo: aggiungere utenti al catalogo

### Aggiungere o rimuovere utenti in un catalogo

Completare questa procedura indipendentemente dal metodo di autenticazione utilizzato.

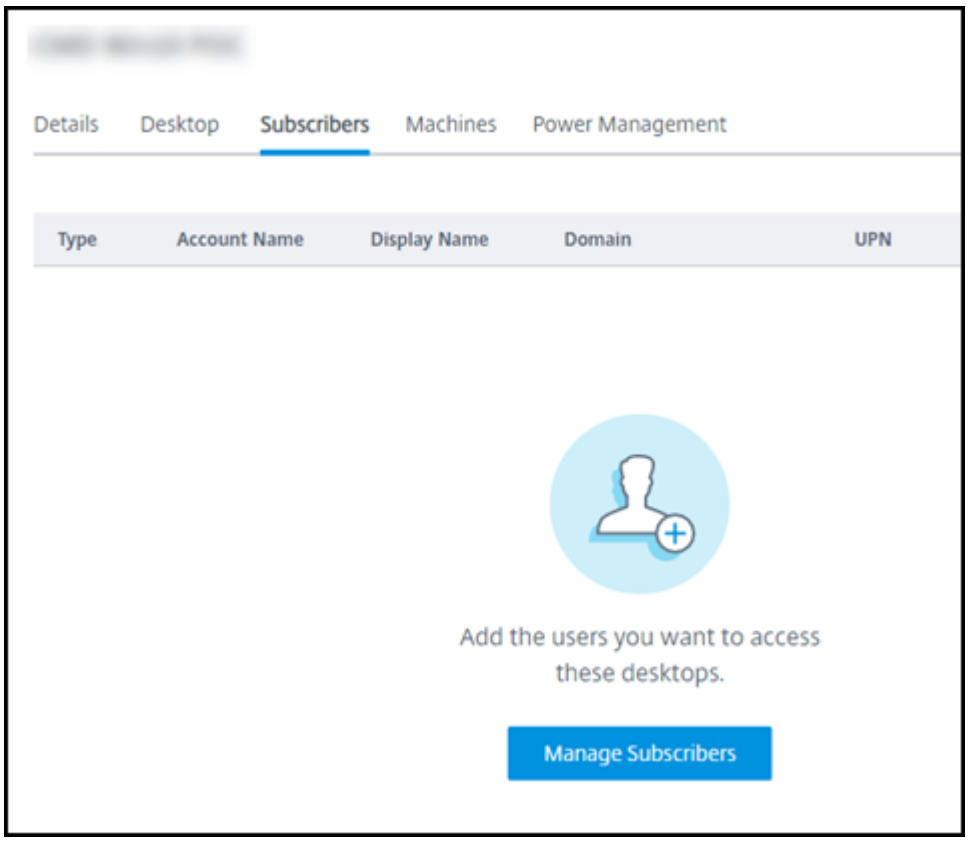
1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), se non è stato aggiunto alcun utente a un catalogo, selezionare **Add subscribers** (Aggiungi sottoscrittori).



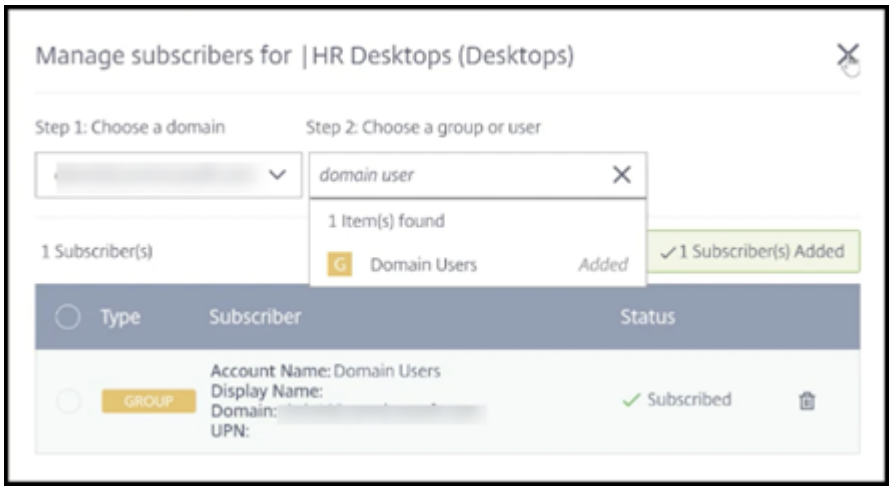

   Per aggiungere utenti a un catalogo che contiene già utenti, fare clic in un punto qualsiasi della voce del catalogo.

2. Nella scheda **Subscribers** (Sottoscrittori), selezionare **Manage Subscribers** (Gestisci sottoscrittori).




3. Selezionare un dominio (se si utilizza Managed Azure AD per l'autenticazione utente, è disponibile una sola voce nel campo del dominio). Quindi, selezionare un utente.




4. Selezionare altri utenti, secondo necessità. Al termine, selezionare la **X** nell'angolo in alto a destra.

Per rimuovere utenti da un catalogo, seguire i passaggi 1 e 2. Nel passaggio 3, selezionare l'icona del cestino accanto al nome che si desidera eliminare (anziché selezionare un dominio e un gruppo/utente). Questa azione rimuove l'utente dal catalogo, non dall'origine (ad esempio Managed Azure AD

o la propria AD o AAD).

Passi successivi:

- Per un catalogo con macchine multisessione, aggiungere le applicazioni, se non lo si è già fatto.
- Per tutti i cataloghi, inviare l'URL di Citrix Workspace ai propri utenti.

### Ulteriori informazioni

Per ulteriori informazioni sull'autenticazione in Citrix Cloud, consultare Gestione delle identità e degli accessi.

## Remote PC Access (Accesso remoto PC) in Quick Deploy (Distribuzione rapida)

February 24, 2023

### Introduzione

Citrix Remote PC Access (Accesso remoto PC) consente agli utenti di utilizzare in remoto macchine fisiche Windows o Linux situate in ufficio. Gli utenti ricevono la migliore esperienza utente utilizzando Citrix HDX per offrire la propria sessione PC da ufficio.

Remote PC Access (Accesso remoto PC) supporta macchine aggiunte a un dominio.

In questo articolo viene descritto come creare una distribuzione Remote PC Access (Accesso remoto PC) utilizzando l'interfaccia Quick Deploy (Distribuzione rapida). Per creare una distribuzione Remote PC Access (Accesso remoto PC) utilizzando l'interfaccia Full Configuration (Configurazione completa), vedere Remote PC Access (Accesso remoto PC).

#### Differenze rispetto alla distribuzione di desktop e app virtuali

Se si ha familiarità con la distribuzione di desktop e app virtuali, la funzionalità Remote PC Access (Accesso remoto PC) presenta diverse differenze:

- Un catalogo Remote PC Access (Accesso remoto PC) in genere contiene macchine fisiche esistenti. Pertanto, non è necessario preparare un'immagine o eseguire il provisioning delle macchine per utilizzare Remote PC Access (Accesso remoto PC). La distribuzione di desktop e app di solito utilizza macchine virtuali (VM) e viene utilizzata un'immagine come modello per il provisioning delle macchine virtuali.

- Quando una macchina in un catalogo casuale in pool Remote PC Access (Accesso remoto PC) viene spenta, non viene ripristinata allo stato originale dell'immagine.
- Per i cataloghi di assegnazione degli utenti statici di Remote PC Access (Accesso remoto PC), l'assegnazione avviene dopo l'accesso di un utente (sulla macchina o tramite RDP). Quando si distribuiscono desktop e app, viene assegnato un utente se è disponibile una macchina.

### Riepilogo dell'installazione e della configurazione

Esaminare questa sezione prima di iniziare le attività.

1. Prima di iniziare:
    a) Esaminare i requisiti e le considerazioni.
    b) Completare le attività di preparazione.
2. Da Citrix Cloud:
    a) Configurare un account Citrix Cloud e fare una sottoscrizione a Citrix DaaS.
    b) Impostare una posizione risorsa in grado di accedere alle risorse di Active Directory. Installare almeno due Cloud Connector nella posizione risorsa. I Cloud Connector comunicano con Citrix Cloud.

    Seguire le linee guida per creare una posizione risorsa e installare Cloud Connector al suo interno. Queste informazioni includono i requisiti di sistema, la preparazione e le procedure.
    c) Connettere Active Directory a Citrix Cloud.
3. Installare un Citrix Virtual Delivery Agent (VDA) su ogni macchina a cui gli utenti accederanno in remoto. I VDA comunicano con Citrix Cloud tramite i Cloud Connector nella posizione risorsa.
4. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida):
    a) Creare un catalogo Remote PC Access (Accesso remoto PC). In questa procedura si specifica la posizione risorsa e si seleziona il metodo di assegnazione degli utenti.
    b) Aggiungere abbonati (utenti) al catalogo, se necessario. Aggiungere utenti a un catalogo se il catalogo utilizza il metodo di assegnazione degli utenti statico con assegnazione automatica o casuale in pool. Non è necessario aggiungere utenti a un catalogo statico preassegnato.
5. Inviare l'URL dell'area di lavoro agli utenti. Dalla propria area di lavoro, gli utenti possono accedere alle loro macchine in ufficio.

## Requisiti e considerazioni

I riferimenti alle macchine in questa sezione si riferiscono alle macchine a cui gli utenti accedono in remoto.

### Aspetti generali

- Le macchine devono eseguire un sistema operativo Windows 10 o Linux (Red Hat Enterprise Linux e Ubuntu) a sessione singola.
- Le macchine devono far parte di un dominio Active Directory Domain Services.
- Se si ha familiarità con l'uso di Remote PC Access (Accesso remoto PC) con Citrix Virtual Apps and Desktops, la funzione Wake-on-LAN (Riattivazione LAN) non è disponibile in Citrix DaaS.

### Rete

- La macchina deve disporre di una connessione di rete attiva. Una connessione cablata è preferibile per una maggiore affidabilità e larghezza di banda.
- Se si utilizza il Wi-Fi:
  - Impostare l'alimentazione in modo che la scheda di rete wireless sia accesa.
  - Configurare la scheda di rete wireless e il profilo di rete per consentire la connessione automatica alla rete wireless prima dell'accesso dell'utente. In caso contrario, il VDA non si registra finché l'utente non esegue l'accesso. La macchina non è disponibile per l'accesso remoto finché un utente non accede.
  - Assicurarsi che i Cloud Connector possano essere raggiunti dalla rete Wi-Fi.

### Dispositivi e periferiche

- I seguenti dispositivi non sono supportati:
  - Switch KVM o altri componenti che possono disconnettere una sessione.
  - PC ibridi, inclusi computer portatili e PC All-in-One e NVIDIA Optimus.
- Collegare la tastiera e il mouse direttamente alla macchina. Il collegamento al monitor o ad altri componenti che possono essere spenti o scollegati può rendere queste periferiche non disponibili. Se è necessario collegare i dispositivi di input a componenti quali monitor, non spegnere tali componenti.
- Per computer portatili e dispositivi Surface Pro: assicurarsi che il computer portatile sia collegato a una fonte di alimentazione anziché andare a batteria. Configurare le opzioni di alimentazione del computer portatile in modo che corrispondano alle opzioni di una macchina desktop. Ad esempio:

- Disattivare la funzionalità di ibernazione.
- Disattivare la funzione di sospensione.
- Impostare l'azione di chiusura del coperchio su **Non intervenire**.
- Impostare l'azione di **pressione del pulsante di accensione** su **Arresta sistema**.
- Disabilitare le funzioni di risparmio energetico della scheda video e della scheda NIC.

Se si utilizza una docking station, è possibile disancorare e reinserire i computer portatili. Quando si disancora il computer portatile, il VDA si registra nuovamente con i Cloud Connector tramite Wi-Fi. Tuttavia, quando si reinserisce il computer portatile, il VDA non passa all'uso della connessione cablata a meno che non si disconnetta la scheda wireless. Alcuni dispositivi offrono una funzionalità integrata di disconnessione della scheda wireless dopo che è stata stabilita una connessione cablata. Gli altri dispositivi richiedono soluzioni personalizzate o utilità di terze parti per disconnettere la scheda wireless. Leggere le considerazioni sulle reti Wi-Fi menzionate in precedenza.

Per abilitare l'inserimento e il disancoraggio per i dispositivi Remote PC Access (Accesso remoto PC):

- In **Start > Impostazioni > Sistema > Alimentazione e sospensione**, impostare **Sospensione** su **Mai**.
- In **Gestione dispositivi > Schede di rete > Scheda Ethernet**, andare a **Risparmio energia** e deselezionare **Consenti al computer di spegnere il dispositivo per risparmiare energia**. Assicurarsi che l'opzione **Consenti al dispositivo di riattivare il computer** sia selezionata.

#### VDA Linux

- Usare Linux VDA su macchine fisiche solo in modalità non 3D. A causa delle limitazioni del driver NVIDIA, la schermata locale del PC non può essere oscurata e visualizza le attività della sessione quando è abilitata la modalità HDX 3D. Visualizzare questa schermata è un rischio per la sicurezza.
- I cataloghi con macchine Linux devono utilizzare il metodo di assegnazione degli utenti statico preassegnato. I cataloghi con macchine Linux non possono utilizzare né i metodi di assegnazione statici autoassegnati né quelli in pool casuali.

#### Considerazioni sull'area di lavoro

- Più utenti con accesso allo stesso PC dell'ufficio vedono la stessa icona in Citrix Workspace. Quando un utente accede a Citrix Workspace, la macchina appare come non disponibile se è già in uso da parte di un altro utente.

### Preparazione

- Decidere come installare il VDA sulle macchine. Sono disponibili diversi metodi:
  - Installare manualmente il VDA su ogni macchina.
  - Eseguire il push dell'installazione del VDA utilizzando Criteri di gruppo, tramite uno script.
  - Eseguire il push dell'installazione del VDA utilizzando uno strumento ESD (Electronic Software Distribution) come Microsoft System Center Configuration Manager (SCCM). Per ulteriori informazioni, vedere Installare i VDA utilizzando SSCM.
- È possibile scoprire ulteriori informazioni sui metodi di assegnazione degli utenti e decidere quale metodo utilizzare. Specificare il metodo durante la creazione di un catalogo Remote PC Access (Accesso remoto PC).
- Decidere in che modo le macchine (o meglio i VDA installati sulle macchine) verranno registrati su Citrix Cloud. Un VDA deve essere registrato per stabilire le comunicazioni con il broker di sessione in Citrix Cloud.

  I VDA si registrano tramite i Cloud Connector nella relativa posizione risorsa. È possibile specificare gli indirizzi dei Cloud Connector quando si installa un VDA o in seguito.

  Per la prima registrazione (iniziale) di un VDA, Citrix consiglia di utilizzare un oggetto Criteri di gruppo (GPO) o un oggetto Criteri di gruppo locale (LGPO) basato su policy. Dopo la registrazione iniziale, Citrix consiglia di utilizzare l'aggiornamento automatico, che è abilitato per impostazione predefinita. Ulteriori informazioni sulla registrazione dei VDA.

### Installare un VDA

Scaricare e installare un VDA su ogni macchina fisica a cui gli utenti accederanno in remoto.

#### Scaricare un VDA

- Per scaricare un VDA Windows:
  1. Utilizzando le credenziali dell'account Citrix Cloud, accedere alla pagina di download di Citrix DaaS.
  2. Scaricare la versione più recente di VDA. Sono disponibili due tipi di pacchetti di installazione. I valori relativi all'anno e al mese nel titolo del VDA variano.
- Per scaricare un VDA Linux per Remote PC Access (Accesso remoto PC), seguire le indicazioni nella documentazione dei VDA Linux.

**Tipi di pacchetti di installazione dei VDA Windows** Il sito di download di Citrix fornisce due tipi di pacchetti di installazione dei VDA Windows che possono essere utilizzati per le macchine Remote PC Access (Accesso remoto PC):

- Programma di installazione di VDA core a sessione singola (la *versione* è *aamm*): `VDAWorkstationCoreSe .exe`

  Il programma di installazione di VDA core a sessione singola è progettato specificamente per Remote PC Access (Accesso remoto PC). È leggero e più facile da distribuire (rispetto ad altri programmi di installazione di VDA) in rete su tutte le macchine. Non include componenti che in genere non sono necessari in queste distribuzioni, come Citrix Profile Management, Machine Identity Service e il livello di personalizzazione degli utenti.

  Tuttavia, se Citrix Profile Management non è installato, le visualizzazioni per Citrix Analytics for Performance e alcuni dettagli della dashboard Monitor (Monitoraggio) non sono disponibili. Per informazioni dettagliate su queste limitazioni, vedere il post del blog Monitorare e risolvere i problemi relativi alle macchine Remote PC Access (Accesso remoto PC).

  Se si desiderano visualizzazioni complete di analisi e monitoraggio, utilizzare il programma di installazione di VDA completo a sessione singola.

- Programma di installazione di VDA completo a sessione singola (la *versione* è *aamm*): `VDAWorkstationSetup_release.exe`

  Sebbene il programma di installazione di VDA completo a sessione singola sia un pacchetto più grande del programma di installazione di VDA core a sessione singola, è possibile personalizzarlo per installare solo i componenti necessari. Ad esempio, è possibile installare i componenti che supportano Profile Management.

**Installare un VDA Windows per Remote PC Access (Accesso remoto PC) in modo interattivo**

1. Fare doppio clic sul file di installazione del VDA scaricato.
2. Nella pagina **Environment** (Ambiente), selezionare **Enable Remote PC Access** (Abilita Accesso remoto PC), quindi fare clic su **Next** (Avanti).
3. Nella pagina **Delivery Controller**, selezionare una delle seguenti opzioni:
   - Se si conoscono gli indirizzi dei Cloud Connector, selezionare **Do it manually** (Esegui l' operazione manualmente). Immettere il nome di dominio completo di un Cloud Connector e fare clic su **Add** (Aggiungi). Ripetere la procedura per gli altri Cloud Connector nella posizione risorsa.
   - Se si conosce la posizione in cui sono stati installati i Cloud Connector nella struttura AD, selezionare **Choose locations from Active Directory** (Scegliere posizioni da Active Direc-

tory), quindi selezionare quella posizione. Ripetere l'operazione per gli altri Cloud Connector.

- Se si desidera specificare gli indirizzi dei Cloud Connector in Citrix Group Policy (Criteri di gruppo Citrix), selezionare **Do it later (Advanced)** (Esegui l'operazione più tardi [Procedura avanzata]), quindi confermare la selezione quando richiesto.

Al termine, fare clic su **Next** (Avanti).

4. Se si utilizza il programma di installazione di VDA completo a sessione singola, nella pagina **Additional Components** (Componenti aggiuntivi) selezionare i componenti che si desidera installare, ad esempio Profile Management (questa pagina non viene visualizzata se si utilizza il programma di installazione di VDA core a sessione singola).
5. Nella pagina **Features** (Funzionalità), fare clic su **Next** (Avanti).
6. Nella pagina **Firewall**, selezionare **Automatically** (Automaticamente) (se non è già selezionato). Quindi, fare clic su **Next** (Avanti).
7. Nella pagina **Summary** (Riepilogo), fare clic su **Install**(Installa).
8. Nella pagina **Diagnose** (Diagnostica), fare clic su **Connect** (Connetti). Assicurarsi che la casella di controllo sia selezionata. Quando richiesto, immettere le credenziali dell'account Citrix. Dopo aver convalidato le credenziali, fare clic su **Next** (Avanti).
9. Nella pagina **Finish** (Fine), fare clic su **Finish** (Fine).

Per informazioni complete sull'installazione, vedere Installare i VDA.

#### Installare un VDA Windows per Remote PC Access (Accesso remoto PC) utilizzando una riga di comando

- Se si utilizza il programma di installazione di VDA core a sessione singola: eseguire `VDAWorkstationCoreSetup.exe` e includere le opzioni `/quiet`, `/enable_hdx_ports` e `/enable_hdx_udp_ports`. Per specificare gli indirizzi dei Cloud Connector, utilizzare l'opzione `/controllers`.

  Ad esempio, il comando seguente installa un VDA core a sessione singola. L'app Citrix Workspace e altri servizi non core non vengono installati. Vengono specificati i nomi di dominio completi di due Cloud Connector e le porte del servizio Windows Firewall verranno aperte automaticamente. L'amministratore gestirà i riavvii.

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
  ```

- Se si utilizza il programma di installazione di VDA completo a sessione singola e si desidera includere Profile Management (o altri componenti opzionali): eseguire `VDAWorkstationSetup.exe` e includere le opzioni `/remotepc` e `/includeadditional`. L'opzione `/remotepc` impedisce l'installazione della maggior parte dei componenti aggiuntivi. L'opzione `/includeadditional` specifica esattamente quali componenti aggiuntivi si desidera installare.

  Ad esempio, il comando seguente impedisce l'installazione di tutti i componenti aggiuntivi facoltativi, ad eccezione di Profile Management.

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional "Citrix User Profile Manager","Citrix User Profile Manager WMI Plugin" /controllers "connector.domain.com" "connector2.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

Per ulteriori informazioni, vedere le opzioni della riga di comando per installare un VDA.

#### Installare un VDA Linux

Seguire le linee guida nella documentazione di Linux per l'installazione interattiva di un VDA Linux o l'utilizzo della riga di comando.

### Creare un catalogo Remote PC Access (Accesso remoto PC)

È necessario che esista una posizione risorsa contenente almeno due Cloud Connector prima di poter creare correttamente un catalogo.

> **Importante:**
>
> Una macchina può appartenere a un solo catalogo alla volta. Questa restrizione non viene applicata quando si specificano le macchine da aggiungere a un catalogo. Tuttavia, ignorare la restrizione può causare problemi in seguito.

1. Accedere a Citrix Cloud.
2. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
3. Se non si è ancora creato alcun catalogo, fare clic su **Get Started** (Inizia) nella pagina **Welcome** (Benvenuto).
4. Selezionare **Manage > Quick Deploy** (Gestisci > Distribuzione rapida).
5. Selezionare **Create Catalog** (Crea catalogo).
6. Nella scheda **Remote PC Access** (Accesso remoto PC), selezionare un metodo per assegnare gli utenti alle macchine.

7. Immettere un nome per il catalogo e selezionare la posizione risorsa creata.
8. Aggiungere le macchine.
9. Fare clic su **Create Catalog** (Crea catalogo).
10. Nella pagina **Your Remote PC Access catalog is being created** (Il catalogo Accesso remoto PC è in fase di creazione), fare clic su **Done** (Fine).
11. Viene visualizzata una voce per il nuovo catalogo nella dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida).

    Dopo aver creato correttamente il catalogo, fare clic su uno dei collegamenti per aggiungere abbonati (utenti) al catalogo. Questo passaggio si applica se il catalogo utilizza il metodo di assegnazione degli utenti statico con assegnazione automatica o in pool casuale non assegnato.

Dopo aver creato un catalogo e aggiunto utenti (se necessario), inviare l'URL di Workspace agli utenti.

### Metodi di assegnazione degli utenti

Il metodo di assegnazione degli utenti scelto durante la creazione di un catalogo indica il modo in cui gli utenti vengono assegnati alle macchine.

- **Assegnazione automatica statica:** l'assegnazione degli utenti si verifica quando un utente accede alla macchina (non utilizzando Citrix, ad esempio, di persona o tramite RDP), dopo l'installazione di un VDA sulla macchina. Successivamente, se altri utenti accedono a quella macchina (non utilizzando Citrix), anche questi utenti vengono assegnati. Solo un utente alla volta può utilizzare la macchina. Questa è una configurazione tipica per gli impiegati o i turnisti che condividono un computer.

  Questo metodo è supportato per le macchine Windows. Non può essere utilizzato con macchine Linux.

- **Preassegnato statico:** gli utenti sono preassegnati alle macchine (di solito questo metodo viene configurato caricando un file CSV contenente la mappatura macchina-utente). Non è necessario che un utente acceda per stabilire l'assegnazione dopo l'installazione del VDA. Inoltre, non è necessario assegnare utenti al catalogo dopo che viene creato. Questo è il metodo migliore per chi lavora in ufficio.

  Questo metodo è supportato per macchine Windows e Linux.

- **In pool casuale non assegnato:** gli utenti vengono assegnati in modo casuale a una macchina disponibile. Solo un utente alla volta può utilizzare la macchina. Questo approccio è ideale per i laboratori informatici nelle scuole.

Questo metodo è supportato per le macchine Windows. Non può essere utilizzato con macchine Linux.

### Metodi per aggiungere macchine a un catalogo

Tenere presente che su ogni macchina deve essere installato un VDA.

Quando si crea o si modifica un catalogo, è possibile aggiungere macchine a un catalogo in tre modi:

- Selezionare gli account delle macchine uno per uno.
- Selezionare le unità organizzative.
- Aggiungere macchine in blocco utilizzando un file CSV. È disponibile un modello da utilizzare per il file CSV.

#### Aggiungere i nomi delle macchine

Questo metodo aggiunge gli account delle macchine uno per uno.

1. Selezionare il dominio.
2. Cercare l'account della macchina.
3. Fare clic su **Add** (Aggiungi).
4. Ripetere l'operazione per aggiungere altre macchine.
5. Al termine dell'aggiunta delle macchine, fare clic su **Done** (Fine).

#### Aggiungere le unità organizzative

Questo metodo aggiunge gli account delle macchine in base all'unità organizzativa in cui risiedono. Quando si selezionano unità organizzative, scegliere unità organizzative di livello inferiore per una maggiore granularità. Se tale granularità non è richiesta, è possibile scegliere unità organizzative di livello superiore.

Ad esempio, nel caso di `Bank`/`Officers`/`Tellers`, selezionare `Tellers` per una maggiore granularità. In caso contrario, è possibile selezionare `Officers` o `Bank` in base alle esigenze.

Lo spostamento o l'eliminazione di unità organizzative dopo che sono state assegnate a un catalogo Remote PC Access (Accesso remoto PC) influisce sulle associazioni dei VDA e causa problemi per le assegnazioni future. Accertarsi che il piano di modifica AD tenga conto degli aggiornamenti delle assegnazioni delle unità organizzative per i cataloghi.

Per aggiungere unità organizzative:

1. Selezionare il dominio.

2. Selezionare le unità organizzative che contengono gli account delle macchine che si desidera aggiungere.
3. Indicare nella casella di controllo se includere le sottocartelle incluse nelle selezioni.
4. Al termine della selezione delle unità organizzative, fare clic su **Done** (Fine).

#### Aggiungere macchine in blocco

1. Fare clic su **Download CSV Template** (Scarica modello CSV).
2. Nel modello, aggiungere le informazioni sugli account delle macchine (fino a 100 voci). Il file CSV può anche contenere i nomi degli utenti assegnati a ciascuna macchina.
3. Salvare il file.
4. Trascinare il file nella pagina **Add machines in bulk** (Aggiungi macchine in blocco) o selezionare il file.
5. Viene visualizzata un'anteprima del contenuto del file. Se non è il file desiderato, è possibile creare un altro file e quindi trascinarlo o selezionarlo.
6. Al termine, fare clic su **Done** (Fine).

### Gestire i cataloghi Remote PC Access (Accesso remoto PC)

Per visualizzare o modificare le informazioni di configurazione di un catalogo Remote PC Access (Accesso remoto PC), selezionare il catalogo dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida) (fare clic su un punto qualsiasi della voce del catalogo).

- Dalla scheda **Details** (Dettagli) è possibile aggiungere o rimuovere macchine.
- Dalla scheda **Subscribers** (Abbonati) è possibile aggiungere o rimuovere utenti.
- Dalla scheda **Machines** (Macchine) è possibile:
  - Aggiungere o rimuovere macchine: pulsante **Add or remove machines** (Aggiungi o rimuovi macchine).
  - Modificare le assegnazioni utente: icona del cestino **Remove assignment** (Rimuovi assegnazione), **Edit machine assignment** (Modifica assegnazione macchina) nel menu con i puntini di sospensione.
  - Controllare quali macchine sono registrate e attivare o disattivare la modalità di manutenzione per le macchine.

## Eseguire il monitoraggio in Quick Deploy (Distribuzione rapida)

October 26, 2022

Dalla dashboard **Monitor** (Monitoraggio), è possibile visualizzare l'utilizzo del desktop, le sessioni e le macchine nella distribuzione Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). È inoltre possibile controllare sessioni, gestire l'alimentazione delle macchine, terminare le applicazioni e i processi in esecuzione.

Per accedere alla dashboard **Monitor** (Monitoraggio):

1. Se non lo si è già fatto, accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), selezionare la scheda **Monitor** (Monitoraggio).

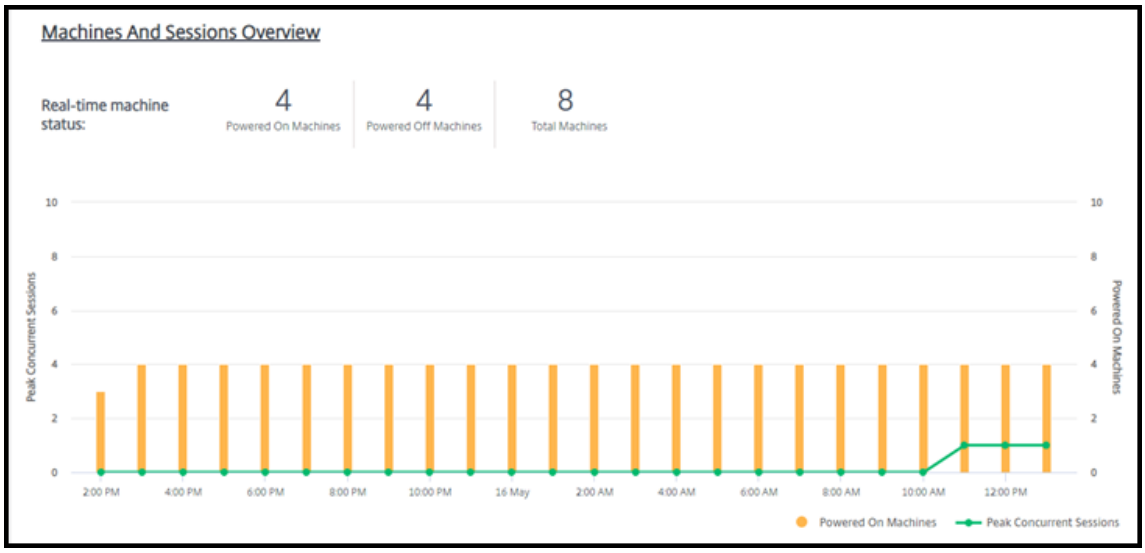
## Monitorare l'utilizzo del desktop

Le visualizzazioni in questa pagina si aggiornano ogni cinque minuti.

- **Machine and Sessions Overview** (Panoramica delle macchine e delle sessioni): è possibile personalizzare la visualizzazione per mostrare informazioni su tutti i cataloghi (impostazione predefinita) o su un catalogo selezionato. È anche possibile personalizzare il periodo di tempo: ultimo giorno, ultima settimana, ultimo mese o ultimi tre mesi.

  I conteggi nella parte superiore della visualizzazione indicano il numero totale di macchine, più il numero di macchine accese e spente. Passare il mouse su un valore per visualizzare quante sono a sessione singola e quante sono multisessione.

  Il grafico sotto i conteggi mostra il numero di macchine accese e le sessioni simultanee di picco in punti regolari durante il periodo di tempo selezionato. Passare il mouse su un punto del grafico per visualizzare i conteggi in quel punto.



- **Top 10s** (I primi 10): per personalizzare la visualizzazione dei primi dieci elementi, selezionare un periodo di tempo: la settimana precedente (impostazione predefinita), il mese precedente o i tre mesi precedenti. È inoltre possibile personalizzare la visualizzazione in modo da visualizzare solo le informazioni sull'attività di macchine a sessione singola, macchine multisessione o applicazioni.
  - **Top 10 Active Users** (Primi 10 utenti attivi): elenca gli utenti che hanno avviato i desktop più frequentemente durante il periodo di tempo. Passando il mouse su una riga vengono visualizzati gli avvii totali.
  - **Top 10 Active Catalogs** (Primi 10 cataloghi attivi): elenca i cataloghi con la durata più lunga durante il periodo di tempo selezionato. La durata è la somma di tutte le sessioni utente di quel catalogo.

#### Rapporto sull'utilizzo del desktop

Per scaricare un rapporto contenente informazioni sugli avvii di macchine nell'ultimo mese, selezionare **Launch Activity** (Attività di avvio). Un messaggio indica che la richiesta è in fase di elaborazione. Il rapporto viene scaricato automaticamente nella posizione di download predefinita sulla macchina locale.

### Filtrare e cercare per monitorare macchine e sessioni

Quando si monitorano le informazioni sulle sessioni e sulle macchine, tutte le macchine o le sessioni vengono visualizzate per impostazione predefinita. È possibile:

- Filtrare la visualizzazione per macchine, sessioni, connessioni o applicazioni.
- Affinare la visualizzazione di sessioni o macchine scegliendo i criteri desiderati, creando un filtro usando le espressioni.
- Salvare i filtri creati per riutilizzarli.

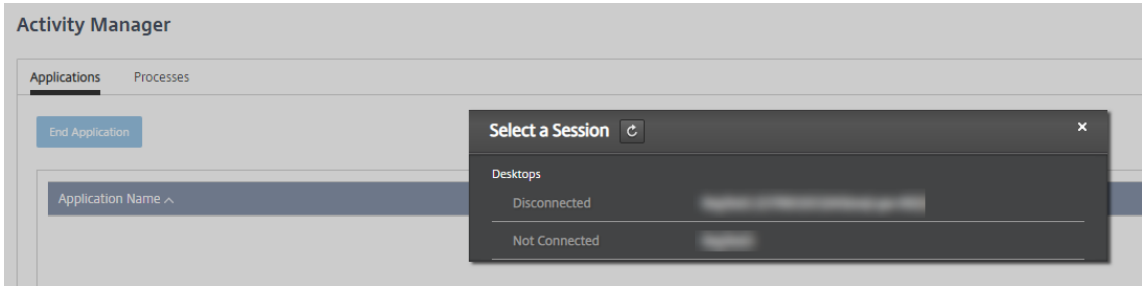
### Controllare le applicazioni di un utente

È possibile visualizzare e gestire applicazioni e processi per un utente che dispone di una sessione in esecuzione o di un desktop assegnato.

1. Dalla dashboard **Monitor** (Monitoraggio) in Citrix DaaS, selezionare **Search** (Cerca) e immettere il nome utente (o i caratteri iniziali del nome utente), la macchina o l'endpoint. Dai risultati della ricerca, selezionare l'elemento che si sta cercando (per comprimere la casella di ricerca senza effettuare una ricerca, selezionare nuovamente **Search** [Cerca]).

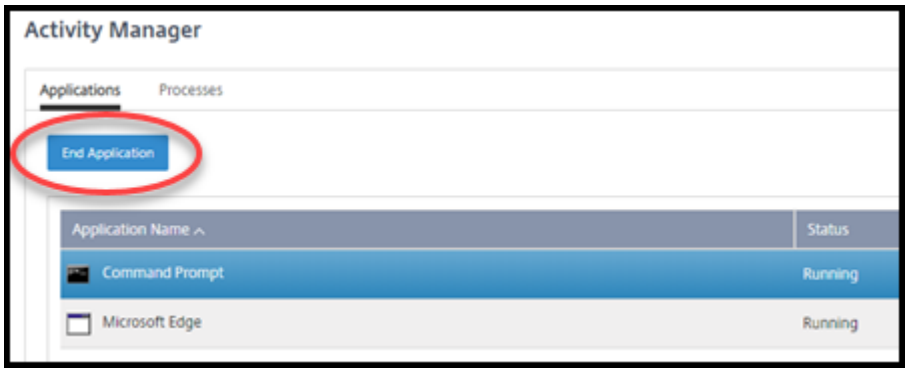
 

2. Selezionare una sessione.




Activity Manager (Gestione attività) elenca le applicazioni e i processi per la sessione dell'utente.

3. Per terminare un'applicazione, nella scheda **Applications** (Applicazioni) in Activity Manager (Gestione attività), selezionare la riga dell'applicazione per selezionare quell'applicazione, quindi selezionare **End Application** (Termina applicazione).




4. Per terminare un processo, nella scheda **Processes** (Processi) in Activity Manager (Gestione attività), selezionare la riga del processo per selezionare quel processo, quindi selezionare **End Process** (Termina processo).
5. Per visualizzare i dettagli della sessione, selezionare **Details** (Dettagli) in alto a destra. Per tornare alla visualizzazione delle applicazioni e dei processi, selezionare Activity Manager (Gestione attività) in alto a destra.
6. Per controllare la sessione, selezionare **Session Control > Log Off** (Controllo sessione > Esci) o **Session Control > Disconnect** (Controllo sessione > Disconnetti).

## Shadowing degli utenti

Utilizzare la funzionalità di shadowing per visualizzare la macchina virtuale o la sessione di un utente o lavorarci direttamente. È possibile utilizzare la funzionalità di shadowing sui VDA Windows e Linux. L'utente deve essere connesso alla macchina di cui si desidera fare lo shadowing. Per verificare la connessione, controllare il nome della macchina elencato nella barra del titolo `User`.

Lo shadowing viene avviato in una nuova scheda del browser. Assicurarsi che il browser consenta i popup dall'URL di Citrix Cloud.

Lo shadowing è supportato solo per gli utenti su macchine aggiunte a un dominio. Per lo shadowing di una macchina non aggiunta a un dominio, è necessario configurare una macchina bastion. Per i dettagli, vedere Accesso bastion.

Lo shadowing deve essere avviato da una macchina sulla stessa rete virtuale delle macchine aggiunte al dominio e soddisfare anche eventuali requisiti di porta.

#### Abilitare lo shadowing

1. Da **Manage > Quick Deploy > Monitor** (Gestisci > Distribuzione rapida > Monitoraggio), andare alla vista **User Details** (Dettagli utente).
2. Selezionare la sessione utente e selezionare **Shadow** (Avvia shadowing) nella vista **Activity Manager** (Gestione attività) o nel riquadro **Session Details** (Dettagli sessione).

#### Shadowing dei VDA Linux

Lo shadowing è disponibile per i VDA Linux versione 7.16 o successive con le distribuzioni Linux RHEL7.3 o Ubuntu versione 16.04.

Monitor (Monitoraggio) utilizza il nome di dominio completo per connettersi al VDA Linux di destinazione. Assicurarsi che il client di Monitor (Monitoraggio) sia in grado di risolvere il nome di dominio completo del VDA Linux.

- Il VDA deve avere i pacchetti `python-websockify` e `x11vnc` installati.
- La connessione `noVNC` al VDA utilizza il protocollo WebSocket. Per impostazione predefinita, viene utilizzato il protocollo WebSocket `ws://`. Per motivi di sicurezza, Citrix consiglia di utilizzare il protocollo `wss://` sicuro. Installare i certificati SSL su ciascun client Monitor (Monitoraggio) e VDA Linux.

Seguire le istruzioni riportate in Shadowing delle sessioni per configurare il VDA Linux per lo shadowing.

1. Dopo aver abilitato lo shadowing, la connessione di shadowing viene inizializzata e sul dispositivo utente viene visualizzato un prompt di conferma.
2. Chiedere all'utente di fare clic su **Yes** (Sì) per avviare la condivisione della macchina o della sessione.
3. L'amministratore può visualizzare solo la sessione di cui viene eseguito lo shadowing.

#### Shadowing di VDA Windows

Lo shadowing delle sessioni di VDA Windows viene eseguito utilizzando l'Assistenza remota di Windows. Abilitare la funzionalità `Use Windows Remote Assistance` durante l'installazione del

VDA.

1. Dopo aver abilitato lo shadowing, la connessione di shadowing viene inizializzata e viene visualizzata una finestra di dialogo che richiede di aprire o salvare il file `.msrc incident`.
2. Aprire il file richiesta di supporto con Remote Assistance Viewer (Visualizzatore di assistenza remota), se non è già selezionato per impostazione predefinita. Sul dispositivo dell'utente viene visualizzato un messaggio di conferma.
3. Chiedere all'utente di fare clic su **Yes** (Sì) per avviare la condivisione della macchina o della sessione.
4. Per un maggiore controllo, chiedere all'utente di condividere il controllo della tastiera e del mouse.

## Monitorare e controllare le sessioni

Le visualizzazioni delle sessioni vengono aggiornate ogni minuto.

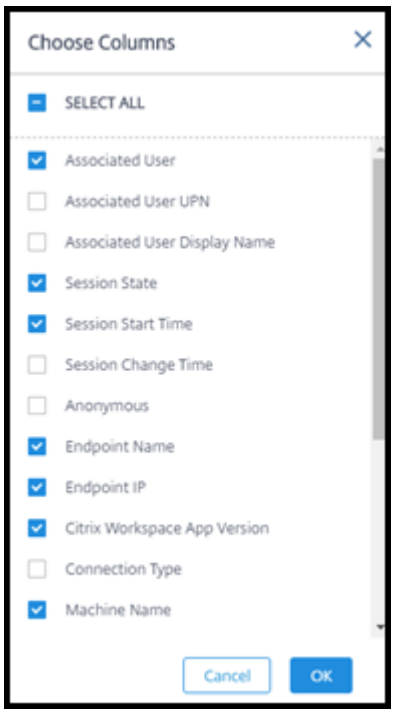
Oltre a visualizzare le sessioni, è possibile disconnettere una o più sessioni o disconnettere gli utenti dalle sessioni.

1. Da **Manage > Quick Deploy > Monitor** (Gestisci > Distribuzione rapida > Monitoraggio), selezionare **Filters** (Filtri).


2. Selezionare la vista **Sessions** (Sessioni).


3. Per personalizzare la visualizzazione, selezionare **Choose Columns** (Scegli colonne) e selezionare le caselle di controllo degli elementi che si desidera visualizzare. Al termine, selezionare **OK**. La visualizzazione delle sessioni si aggiorna automaticamente.




4. Selezionare la casella di controllo a sinistra di ogni sessione che si desidera controllare.
5. Per disconnettersi o disconnettere la sessione, selezionare **Session Control > Log Off** (Controllo sessione > Esci) o **Session Control > Disconnect** (Controllo sessione > Disconnetti).

Tenere presente che la pianificazione della gestione dell'alimentazione per il catalogo può anche controllare la disconnessione delle sessioni e la disconnessione degli utenti dalle sessioni disconnesse.

In alternativa alla procedura precedente è anche possibile **cercare** un utente, selezionare la sessione che si desidera controllare e quindi visualizzare i dettagli della sessione. Le opzioni di uscita e disconnessione sono disponibili anche qui.

#### Rapporto informativo sulla sessione

Per scaricare le informazioni sulla sessione, selezionare **Export** (Esporta) nella visualizzazione delle sessioni. Un messaggio indica che la richiesta è in fase di elaborazione. Il rapporto viene scaricato automaticamente nella posizione di download predefinita sulla macchina locale.

### Monitorare le macchine e controllare l'alimentazione

Le visualizzazioni delle macchine vengono aggiornate ogni minuto.

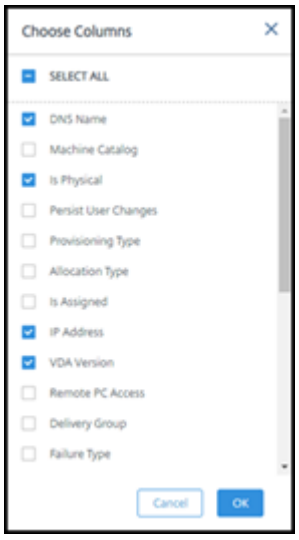
1. Da **Manage > Quick Deploy > Monitor** (Gestisci > Distribuzione rapida > Monitoraggio), selezionare **Filters** (Filtri).

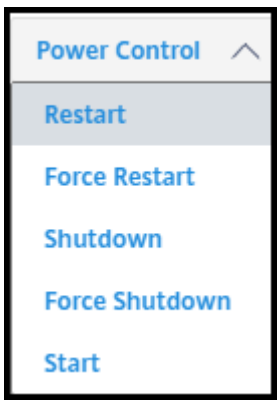
2. Selezionare la vista **Machines** (Macchine).


Per impostazione predefinita, la visualizzazione elenca le macchine con sistema operativo a sessione singola. In alternativa, è possibile visualizzare macchine multisessione.

3. Per personalizzare la visualizzazione, selezionare **Choose Columns** (Scegli colonne) e selezionare le caselle di controllo degli elementi che si desidera visualizzare. Al termine, selezionare **OK**. La visualizzazione delle macchine si aggiorna automaticamente.




4. Per gestire l'alimentazione delle macchine o per attivare o disattivare la modalità di manutenzione, selezionare la casella di controllo a sinistra di ogni macchina che si desidera controllare.
5. Per controllare l'alimentazione delle macchine selezionate, selezionare **Power Control** (Gestione alimentazione) e selezionare un'azione.



6. Per attivare o disattivare la modalità di manutenzione per le macchine selezionate, selezionare **Maintenance Mode > ON** (Modalità di manutenzione > ATTIVATA) o **Maintenance Mode > OFF** (Modalità di manutenzione > DISATTIVATA).

Quando si utilizza la funzionalità di ricerca per trovare e selezionare una macchina, vengono visualizzati i dettagli della macchina, l'utilizzo, l'utilizzo cronologico (degli ultimi sette giorni) e gli IOPS medi.

#### Rapporto informativo sulla macchina

Per scaricare le informazioni sulla sessione, selezionare **Export** (Esporta) nella visualizzazione delle macchine. Un messaggio indica che la richiesta è in fase di elaborazione. Il rapporto viene scaricato automaticamente nella posizione di download predefinita sulla macchina locale.

### Verifica dello stato dell'app e del desktop

Il probe automatizza il processo di controllo dello stato delle app e dei desktop pubblicati. I risultati del controllo dello stato sono disponibili tramite la dashboard **Monitor** (Monitoraggio). Per ulteriori informazioni, vedere:

- Probe delle applicazioni
- Probe dei desktop

## Risoluzione dei problemi in Quick Deploy (Distribuzione rapida)

December 1, 2022

### Introduzione

Le posizioni risorsa contengono le macchine che forniscono desktop e app. Tali macchine vengono create nei cataloghi, quindi i cataloghi sono considerati parte della posizione risorsa. Ogni posizione risorsa contiene anche Cloud Connector. I Cloud Connector consentono a Citrix Cloud di comunicare con la posizione risorsa. In genere, Citrix installa e aggiorna i Cloud Connector.

Facoltativamente, è possibile avviare diverse azioni di Cloud Connector e della posizione risorsa. Vedere:

- Azioni della posizione risorsa
- Impostazioni della posizione risorsa durante la creazione di un catalogo

Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) dispone di strumenti di supporto e risoluzione dei problemi che possono aiutare a risolvere i problemi di configurazione e comunicazione con le macchine che forniscono desktop e app (i VDA). Ad esempio, la creazione di un catalogo potrebbe non riuscire o gli utenti potrebbero non essere in grado di avviare il desktop o le app.

Questa risoluzione dei problemi include ottenere l'accesso alla sottoscrizione Citrix Managed Azure tramite una macchina bastion o un RDP diretto. Dopo aver ottenuto l'accesso alla sottoscrizione, è possibile utilizzare gli strumenti di supporto Citrix per individuare e risolvere i problemi. Per ulteriori informazioni, vedere:

- Risoluzione dei problemi dei VDA tramite macchina bastion o RDP diretto
- Accesso alla macchina bastion
- Accesso RDP diretto

## Risoluzione dei problemi dei VDA tramite macchina bastion o RDP diretto

Le funzionalità di supporto sono destinate alle persone con esperienza nella risoluzione dei problemi Citrix, tra cui:

- Citrix Service Provider (CSP) e altri soggetti con conoscenze tecniche ed esperienza nella risoluzione dei problemi con i prodotti Citrix DaaS.
- Personale di assistenza Citrix.

Se non si ha familiarità o dimestichezza con la risoluzione dei problemi dei componenti Citrix, è possibile chiedere aiuto all'assistenza Citrix. I rappresentanti dell'assistenza Citrix potrebbero chiedere di impostare uno dei metodi di accesso descritti in questa sezione. Tuttavia, i rappresentanti di Citrix eseguono l'effettiva risoluzione dei problemi, utilizzando gli strumenti e le tecnologie Citrix.

> **Importante:**
>
> Queste funzionalità di supporto sono valide solo per le macchine aggiunte a un dominio. Se le macchine nei propri cataloghi non fanno parte di un dominio, si verrà guidati a richiedere aiuto per la risoluzione dei problemi all'assistenza Citrix.

### Metodi di accesso

Questi metodi di accesso sono validi solo per la sottoscrizione Citrix Managed Azure. Per ulteriori informazioni, consultare Sottoscrizioni di Azure.

Vengono forniti due metodi di accesso a scopi di supporto.

- Accedere alle proprie risorse tramite una macchina bastion nella sottoscrizione Citrix Managed Azure dedicata del cliente. La macchina bastion è un unico punto di accesso che consente l'

accesso alle macchine nella sottoscrizione. Fornisce una connessione sicura a tali risorse consentendo il traffico remoto da indirizzi IP in un intervallo specificato.

I passaggi di questo metodo includono:

- Creare la macchina bastion
- Scaricare un agente RDP
- RDP alla macchina bastion
- Connettersi dalla macchina bastion alle altre macchine Citrix nel proprio abbonamento

La macchina bastion è destinata all'uso a breve termine. Questo metodo è destinato a problemi che riguardano la creazione di cataloghi o macchine di immagini.

- Accesso RDP diretto alle macchine nella sottoscrizione Citrix Managed Azure dedicata del cliente. Per consentire il traffico RDP, la porta 3389 deve essere definita nel Gruppo di sicurezza di rete.

  Questo metodo è destinato a problemi del catalogo diversi dalla creazione, ad esempio utenti che non sono in grado di avviare i propri desktop.

Tenere presente che, in alternativa a questi due metodi di accesso, è possibile contattare il supporto Citrix per ricevere assistenza.

### Accesso alla macchina bastion

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Troubleshoot & Support** (Risoluzione dei problemi e supporto) sulla destra.
2. Fare clic su **View troubleshooting options** (Visualizza opzioni di risoluzione dei problemi).
3. Nella pagina **Troubleshoot** (Risoluzione dei problemi), selezionare uno dei primi due tipi di problemi, quindi fare clic su **Use our troubleshooting machine** (Usa la nostra macchina per la risoluzione dei problemi).
4. Nella pagina **Troubleshoot with Bastion Machine** (Risoluzione dei problemi con la macchina bastion), selezionare il catalogo.
   - Se le macchine nel catalogo selezionato non sono aggiunte a un dominio, viene richiesto di contattare il supporto Citrix.
   - Se è già stata creata una macchina bastion con accesso RDP alla connessione di rete del catalogo selezionato, andare al passaggio 8.
5. Viene visualizzato l'intervallo di accesso RDP. Se si desidera limitare l'accesso RDP a un intervallo più piccolo di quello consentito dalla connessione di rete, selezionare la casella di controllo **Restrict RDP access to only computers in IP address range** (Limita l'accesso RDP solo ai computer nell'intervallo di indirizzi IP) e quindi immettere l'intervallo desiderato.

6. Digitare un nome utente e una password da utilizzare per accedere quando si esegue l'RDP alla macchina bastion. Requisiti della password.

   Non utilizzare caratteri Unicode nel nome utente.

7. Fare clic su **Create Bastion Machine** (Crea macchina bastion).

   Quando la macchina bastion viene creata correttamente, il titolo della pagina cambia in **Bastion –*connection*** (Bastion —connessione).

   Se la creazione della macchina bastion non riesce (o se si verificano problemi durante il funzionamento), fare clic su **Delete** (Elimina) nella parte inferiore della pagina di notifica degli errori. Provare a creare nuovamente la macchina bastion.

   È possibile modificare la limitazione dell'intervallo RDP dopo la creazione della macchina bastion. Fare clic su **Edit** (Modifica). Immettere il nuovo valore e quindi fare clic sul segno di spunta per salvare la modifica (fare clic su **X** per annullare la modifica).

8. Fare clic su **Download RDP File** (Scarica file RDP).
9. RDP alla macchina bastion, utilizzando le credenziali specificate durante la creazione della macchina bastion (l'indirizzo della macchina bastion è incorporato nel file RDP scaricato).
10. Connettersi dalla macchina bastion alle altre macchine Citrix nella sottoscrizione. È quindi possibile raccogliere i registri ed eseguire la diagnostica.

Le macchine bastion vengono accese al momento della creazione. Per risparmiare sui costi, le macchine vengono spente automaticamente se rimangono inattive dopo l'avvio. Le macchine vengono eliminate automaticamente dopo diverse ore.

È possibile gestire o eliminare una macchina bastion utilizzando i pulsanti in fondo alla pagina. Se si sceglie di eliminare una macchina bastion, è necessario riconoscere che tutte le sessioni attive sulla macchina termineranno automaticamente. Inoltre, tutti i dati e i file salvati sulla macchina verranno eliminati.

### Accesso RDP diretto

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Troubleshoot & Support** (Risoluzione dei problemi e supporto) sulla destra.
2. Fare clic su **View troubleshooting options** (Visualizza opzioni di risoluzione dei problemi).
3. Nella pagina **Troubleshoot** (Risoluzione dei problemi), selezionare **Other catalog issue** (Altro problema relativo al catalogo).
4. Nella pagina **Troubleshoot with RDP Access** (Risolvi i problemi tramite l'accesso RDP), selezionare il catalogo.

Se RDP è già stato abilitato nella connessione di rete del catalogo selezionato, andare al passaggio 7.

5. Viene visualizzato l'intervallo di accesso RDP. Se si desidera limitare l'accesso RDP a un intervallo inferiore a quello consentito dalla connessione di rete, selezionare la casella di controllo **Restrict RDP access to only computers in IP address range** (Limita l'accesso RDP solo ai computer nell'intervallo di indirizzi IP) e quindi immettere l'intervallo desiderato.
6. Fare clic su **Enable RDP Access** (Abilita accesso RDP).

   Quando l'accesso RDP viene abilitato correttamente, il titolo della pagina cambia in **RDP Access –*connection*** (Accesso RDP - connessione).

   Se l'accesso RDP non è stato abilitato correttamente, fare clic su **Retry Enabling RDP** (Riprova ad abilitare RDP) nella parte inferiore della pagina di notifica degli errori.
7. Connettersi alle macchine utilizzando le credenziali di amministratore di Active Directory. È quindi possibile raccogliere i registri ed eseguire la diagnostica.

### Ottenere assistenza

Se i problemi persistono, aprire un ticket seguendo le istruzioni in Come ottenere assistenza e supporto.

## Gudia di Quick Deploy (Distribuzione rapida)

September 12, 2023

### Schede del catalogo nella dashboard di Quick Deploy (Distribuzione rapida)

Dalla dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida) in Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops), fare clic in un punto qualsiasi della voce del catalogo. Le seguenti schede contengono informazioni sul catalogo:

- **Details** (Dettagli): elenca le informazioni specificate al momento della creazione del catalogo (o della modifica più recente). Contiene inoltre informazioni sull'immagine utilizzata per creare il catalogo.

  Da questa scheda è possibile:

  - Cambiare l'immagine utilizzata nel catalogo.
  - Eliminare il catalogo.

  - Accedere alla pagina contenente i dettagli per la posizione risorsa utilizzata dal catalogo.

- **Desktop:** disponibile solo per i cataloghi contenenti macchine a sessione singola (statiche o casuali). Da questa scheda è possibile modificare il nome e la descrizione del catalogo.
- **Desktop and Apps** (Desktop e app): la scheda **Desktop and Apps** (Desktop e app) è disponibile solo per i cataloghi contenenti macchine multisessione. Da questa scheda è possibile:
  - Aggiungere, modificareo rimuovere le applicazioni a cui gli utenti del catalogo possono accedere in Citrix Workspace.
  - Modificare il nome e la descrizione del catalogo.
- **Subscribers** (Sottoscrittori): elenca tutti gli utenti, inclusi il tipo (utente o gruppo), il nome dell'account, il nome visualizzato, il dominio Active Directory e il nome dell'entità utente.

  Da questa scheda è possibile aggiungere o rimuovere utenti per un catalogo.
- **Machines** (Macchine): mostra il numero totale di macchine nel catalogo, più il numero di macchine registrate, macchine non registrate e macchine con modalità di manutenzione attivata.

  Per ogni macchina nel catalogo, la visualizzazione include il nome di ogni macchina, lo stato di alimentazione (acceso/spento), lo stato di registrazione (registrato/non registrato), gli utenti assegnati, il numero di sessioni (0/1) e lo stato della modalità di manutenzione (un'icona che indica se è attivata o disattivata).

  Da questa scheda è possibile:

  - Aggiungere o eliminare una macchina
  - Avviare, riavviare, arrestare una macchina o forzarne il riavvio
  - Attivare o disattivare la modalità di manutenzione di una macchina

  Per i dettagli, consultare Gestire i cataloghi. Molte delle azioni della macchina sono disponibili anche nella scheda **Monitor** (Monitoraggio) della dashboard di Quick Deploy (Distribuzione rapida). Vedere Monitorare le macchine e controllarne l'alimentazione.
- **Power Management** (Gestione dell'alimentazione): consente di gestire l'accensione e lo spegnimento delle macchine nel catalogo. Una pianificazione indica anche quando le macchine inattive vengono disconnesse.

  È possibile configurare una pianificazione dell'alimentazione quando si crea un catalogo personalizzato o in un secondo momento. Se non viene impostata esplicitamente alcuna pianificazione, una macchina si spegne al termine di una sessione.

  Quando si crea un catalogo utilizzando la creazione rapida, non è possibile selezionare o configurare una pianificazione dell'alimentazione. Per impostazione predefinita, i cataloghi Quick create (Creazione rapida) utilizzano la pianificazione preimpostata Cost Saver (Risparmio sui

costi). Tuttavia, è possibile modificare il catalogo in un secondo momento e cambiare la pianificazione.

Per i dettagli, vedere Gestire le pianificazioni di gestione dell'alimentazione.

### Server DNS

Questa sezione si applica a tutte le distribuzioni che contengono macchine aggiunte a un dominio. È possibile ignorare questa sezione se si utilizzano solo macchine non aggiunte a un dominio.

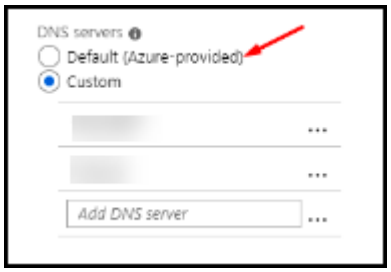
1. Prima di creare un catalogo aggiunto a un dominio (o una connessione, se si utilizza una sottoscrizione Citrix Managed Azure), verificare se sono presenti voci del server DNS in grado di risolvere i nomi di dominio pubblici e privati.

   Quando Citrix DaaS crea un catalogo o una connessione, cerca almeno una voce del server DNS valida. Se non vengono trovate voci valide, l'operazione di creazione non riesce.

   Dove controllare:

   - Se si utilizza la propria sottoscrizione di Azure, controllare la voce **Server DNS** in Azure.
   - Se si utilizza una sottoscrizione Citrix Managed Azure e si sta creando una connessione di peering della rete virtuale di Azure, controllare la voce **Server DNS** nella rete virtuale di Azure di cui si sta eseguendo il peering.
   - Se si utilizza una sottoscrizione Citrix Managed Azure e si crea una connessione SD-WAN, controllare le voci DNS in SD-WAN Orchestrator.

2. In Azure, l'impostazione **Personalizzata** deve contenere almeno una voce valida. Questo servizio non può essere utilizzato con l'**impostazione Predefinita (fornita da Azure)**.

   - Se l'impostazione **Predefinita (fornita da Azure)** è abilitata, modificare l'impostazione su **Personalizzata**e aggiungere almeno una voce del server DNS.
   - Se sono già presenti voci del server DNS in **Personalizzata**, verificare che le voci che si desidera utilizzare con questo servizio possano risolvere i nomi IP di dominio pubblici e privati.
   - Se non si dispone di server DNS in grado di risolvere i nomi di dominio, Citrix consiglia di aggiungere un server DNS fornito da Azure con tali funzionalità.

3. Se si modificano delle voci del server DNS, riavviare tutte le macchine connesse alla rete virtuale. Il riavvio assegna le nuove impostazioni del server DNS (le macchine virtuali continuano a utilizzare le impostazioni DNS correnti fino al riavvio).

   Se si desidera modificare gli indirizzi DNS in un secondo momento, dopo la creazione di una connessione:

- Quando si utilizza la propria sottoscrizione di Azure, è possibile modificarli in Azure (come descritto nei passaggi precedenti). In alternativa, è possibile modificarli in questo servizio.
- Quando si utilizza una sottoscrizione Citrix Managed Azure, questo servizio non sincronizza le modifiche degli indirizzi DNS apportate in Azure. Tuttavia, è possibile modificare le impostazioni DNS per la connessione in questo servizio.

Tenere presente che la modifica degli indirizzi dei server DNS può potenzialmente causare problemi di connettività per le macchine nei cataloghi che utilizzano tale connessione.

#### Aggiunta di server DNS tramite questo servizio

Prima di aggiungere un indirizzo del server DNS a una connessione, assicurarsi che il server DNS sia in grado di risolvere i nomi di dominio pubblici e interni. Citrix consiglia di testare la connettività a un server DNS prima di aggiungerlo.

1. Per aggiungere, modificare o rimuovere un indirizzo del server DNS durante la creazione di una connessione, selezionare **Edit DNS servers** (Modifica server DNS) nella pagina **Add** *connection type* (Aggiungi tipo di connessione). Oppure, se un messaggio indica che non sono stati trovati indirizzi di server DNS, selezionare **Add DNS Servers** (Aggiungi server DNS). Continuare con il passaggio 3.
2. Per aggiungere, modificare o rimuovere un indirizzo del server DNS per una connessione esistente:

   a) Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Network Connections** (Connessioni di rete) sulla destra.
   b) Selezionare la connessione che si desidera modificare.
   c) Selezionare **Edit DNS servers** (Modifica server DNS).

3. Aggiungere, modificare o rimuovere indirizzi.

   a) Per aggiungere un indirizzo, selezionare **Add DNS server** (Aggiungi server DNS) e quindi inserire l'indirizzo IP.
   b) Per modificare un indirizzo, fare clic all'interno del campo dell'indirizzo e modificare i numeri.

c) Per rimuovere un indirizzo, selezionare l'icona del cestino accanto alla voce dell'indirizzo. Non è possibile rimuovere tutti gli indirizzi del server DNS. La connessione deve averne almeno uno.

4. Al termine, selezionare **Confirm Changes** (Conferma modifiche) nella parte inferiore della pagina.
5. Riavviare tutte le macchine che utilizzano tale connessione. Il riavvio assegna le nuove impostazioni del server DNS (le macchine virtuali continuano a utilizzare le impostazioni DNS correnti fino al riavvio).

## Criteri

### Impostare criteri di gruppo per macchine non aggiunte a un dominio

1. Eseguire l'RDP alla macchina utilizzata per l'immagine.
2. Installare Citrix Group Policy Management:

   a) Andare a CTX220345. Scaricare l'allegato.
   b) Fare doppio clic sul file scaricato. Nella cartella `Group Policy Templates 1912 > Group Policy Management`, fare doppio clic su `CitrixGroupPolicyManagement_x64.msi`.

3. Utilizzando il comando **Esegui**, avviare `gpedit.msc` per aprire l'Editor Criteri di gruppo.
4. In `User Configuration Citrix Policies > Unfiltered`, selezionare **Modifica criterio**.

   Se la console Gestione Criteri di gruppo restituisce un errore (come descritto in CTX225742), installare Microsoft Visual C++ 2015 Runtime (o una versione successiva di tale runtime).

5. Abilitare le impostazioni dei criteri secondo necessità. Ad esempio:

   - Quando si lavora in **Configurazione computer** o **Configurazione utente** (a seconda di cosa si desidera configurare), nella scheda **Settings** (Impostazioni), in `Category > ICA / Printing`, selezionare **Auto-create PDF Universal Printer** (Crea automaticamente stampante universale PDF) e impostare l'opzione su `Enabled`.
   - Se si desidera che gli utenti connessi siano amministratori del proprio desktop, aggiungere il gruppo **Interactive User** (Utente interattivo) al gruppo di amministratori incluso.

6. Al termine, salvare l'immagine.
7. Aggiornare il catalogo esistente o creare un nuovo catalogo utilizzando la nuova immagine.

#### Impostare criteri di gruppo per le macchine aggiunte al dominio

1. Verificare che la funzionalità Gestione Criteri di gruppo sia installata.
    - In una macchina Windows multisessione, aggiungere la funzionalità Gestione Criteri di gruppo, utilizzando lo strumento Windows per aggiungere ruoli e funzionalità (ad esempio **Aggiungi ruoli e funzionalità**).
    - Su una macchina Windows a sessione singola, installare gli Strumenti di amministrazione remota del server per il sistema operativo appropriato (questa installazione richiede un account amministratore di dominio). Dopo l'installazione, la console Gestione Criteri di gruppo è disponibile dal menu **Start**.
2. Scaricare e installare il pacchetto Citrix Group Policy management (Gestione Criteri di gruppo Citrix) dalla pagina di download di Citrix, quindi configurare le impostazioni dei criteri secondo necessità. Seguire la procedura descritta in Impostare criteri di gruppo per le macchine non aggiunte a un dominio, dal passaggio 2 alla fine.

Consultare gli articoli di riferimento sulle impostazioni dei criteri per scoprire cosa è disponibile. Tutte le funzionalità dei criteri sono disponibili dall'interfaccia Full Configuration (Configurazione completa) di Citrix DaaS.

### Azioni della posizione risorsa

Citrix crea automaticamente una posizione risorsa e due Cloud Connector quando si crea il primo catalogo per la pubblicazione di desktop e app. È possibile specificare alcune informazioni relative alla posizione risorsa quando si crea un catalogo. Consultare Impostazioni della posizione risorsa durante la creazione di un catalogo.

Per Remote PC Access (Accesso remoto PC), è possibile creare la posizione risorsa e i Cloud Connector.

Questa sezione descrive le azioni disponibili dopo la creazione di una posizione risorsa.

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Cloud Subscriptions** (Sottoscrizioni cloud) sulla destra.
2. Selezionare la sottoscrizione.
    - La scheda **Details** (Dettagli) mostra il numero e i nomi dei cataloghi e delle immagini nella sottoscrizione. Indica inoltre il numero di macchine in grado di fornire desktop o app. Tale conteggio non include le macchine utilizzate per altri scopi, come immagini, Cloud Connector o server di licenze RDS.

- La scheda **Resource Locations** (Posizioni risorse) elenca ciascuna posizione risorsa. Ogni voce di posizione risorsa include lo stato e l'indirizzo di ogni Cloud Connector nella posizione risorsa.

Il menu con i puntini di sospensione nella voce di una posizione risorsa contiene le seguenti azioni.

#### Run Health Check (Esegui controllo di integrità)

Selezionando **Run Health Check** (Esegui controllo di integrità) viene avviato immediatamente il controllo della connettività. Se il controllo non riesce, lo stato di Cloud Connector risulta sconosciuto, perché non comunica con Citrix Cloud. Potrebbe essere utile riavviare il Cloud Connector.

#### Restart Connectors (Riavvia Connector)

Citrix consiglia di riavviare un solo Cloud Connector alla volta. Il riavvio mette offline il Cloud Connector e interrompe l'accesso degli utenti e la connettività della macchina.

Selezionare la casella di controllo relativa al Cloud Connector che si desidera riavviare. Selezionare **Restart** (Riavvia).

#### Add Connectors (Aggiungi Connector)

L'aggiunta di un Cloud Connector richiede in genere 20 minuti per essere completata.

Fornire le seguenti informazioni:

- Quanti Cloud Connector aggiungere.
- Credenziali dell'account del servizio di dominio, utilizzate per collegare le macchine Cloud Connector al dominio.
- Prestazioni della macchina.
- Gruppo di risorse di Azure. L'impostazione predefinita è l'ultimo gruppo di risorse utilizzato dalla posizione risorsa.
- Unità organizzativa (OU). L'impostazione predefinita è l'ultima unità organizzativa utilizzata dalla posizione risorsa.
- Se la rete richiede un server proxy per la connettività Internet. Se si indica **Yes** (Sì), fornire il nome di dominio completo o l'indirizzo IP del server proxy e il numero di porta.

Al termine, selezionare **Add Connectors** (Aggiungi Connector).

#### Delete Connectors (Elimina Connector)

Se un Cloud Connector non è in grado di comunicare con Citrix Cloud e il riavvio non risolve il problema, il supporto Citrix consiglia di eliminare il Cloud Connector.

Selezionare la casella di controllo relativa al Cloud Connector che si desidera eliminare. Quindi, selezionare **Delete** (Elimina). Quando richiesto, confermare l'eliminazione.

È anche possibile eliminare un Cloud Connector disponibile. Tuttavia, se eliminando quel Cloud Connector rimangono meno di due Cloud Connector disponibili nella posizione risorsa, non è consentito eliminare il Cloud Connector selezionato.

#### Select Update Time (Seleziona ora di aggiornamento)

Citrix fornisce automaticamente gli aggiornamenti software per i Cloud Connector. Durante un aggiornamento, un Cloud Connector viene portato offline e aggiornato, mentre gli altri Cloud Connector rimangono in servizio. Al termine del primo aggiornamento, un altro Cloud Connector viene portato offline e aggiornato. Questo processo continua fino all'aggiornamento di tutti i Cloud Connector nella posizione risorsa. Il momento migliore per avviare gli aggiornamenti è in genere al di fuori del normale orario di lavoro.

Scegliere l'ora di inizio degli aggiornamenti o indicare che si desidera che gli aggiornamenti vengano avviati quando ne è disponibile uno. Al termine, selezionare **Save** (Salva).

#### Rename (Rinomina)

Immettere il nuovo nome per la posizione risorsa. Selezionare **Save** (Salva).

#### Configure Connectivity (Configura connettività)

Indicare se gli utenti possono accedere a desktop e app tramite il servizio Citrix Gateway o solo dall'interno della rete aziendale.

### Profile Management

Profile Management garantisce che le impostazioni personali vengano applicate alle applicazioni virtuali degli utenti, indipendentemente dalla posizione del dispositivo utente.

La configurazione di Profile Management è facoltativa.

È possibile abilitare Profile Management con il servizio di ottimizzazione dei profili. Questo servizio fornisce un modo affidabile per gestire queste impostazioni in Windows. La gestione dei profili garantisce un'esperienza coerente mantenendo un unico profilo che segue l'utente. Consolida automaticamente e ottimizza i profili utente per ridurre al minimo i requisiti di gestione e archiviazione. Il servizio di ottimizzazione dei profili richiede un'amministrazione, un supporto e un'infrastruttura minimi. Inoltre, l'ottimizzazione del profilo offre agli utenti un'esperienza di accesso e disconnessione migliorata.

Il servizio di ottimizzazione dei profili richiede una condivisione file in cui persistono tutte le impostazioni personali. L'utente gestisce i file server. Si consiglia di configurare la connettività di rete per consentire l'accesso a questi file server. È necessario specificare la condivisione file come percorso UNC. Il percorso può contenere variabili di ambiente di sistema, attributi utente di Active Directory o variabili Profile Management. Per ulteriori informazioni sul formato della stringa di testo UNC, consultare Specificare il percorso dell'archivio utente.

Quando si abilita Profile Management, prendere in considerazione l'ulteriore ottimizzazione del profilo utente configurando il reindirizzamento delle cartelle per ridurre al minimo gli effetti delle dimensioni del profilo utente. L'applicazione del reindirizzamento delle cartelle è complementare alla soluzione Profile Management. Per ulteriori informazioni, consultare Reindirizzamento delle cartelle Microsoft.

### Configurare il server di licenze Servizi Desktop remoto Microsoft per i carichi di lavoro di Windows Server

Questo servizio consente di accedere alle funzionalità di sessione remota di Windows Server quando viene consegnato un carico di lavoro di Windows Server, ad esempio Windows 2016. Questa operazione richiede in genere una licenza di accesso client (CAL) di Servizi Desktop remoto. La macchina Windows in cui è installato il VDA Citrix deve essere in grado di contattare un server licenze Servizi Desktop remoto per richiedere licenze CAL di Servizi Desktop remoto.

Installare e attivare il server licenze. Per ulteriori informazioni, vedere il documento Microsoft Attivare il server licenze di Servizi Desktop remoto. Per gli ambienti Proof of Concept (POC), è possibile utilizzare il periodo di prova fornito da Microsoft.

Con questo metodo, è possibile fare in modo che Citrix DaaS applichi le impostazioni del server licenze. È possibile configurare il server licenze e la modalità per utente nella console di Servizi Desktop remoto sull'immagine. È inoltre possibile configurare il server licenze utilizzando le impostazioni di Criteri di gruppo Microsoft. Per ulteriori informazioni, vedere il documento Microsoft Concedere licenze CAL (Client Access License) per la distribuzione di Servizi Desktop remoto.

Per configurare il server licenze di Servizi Desktop remoto utilizzando le impostazioni di Criteri di gruppo

1. Installare un server licenze di Servizi Desktop remoto in una delle macchine virtuali disponibili. La macchina virtuale deve essere sempre disponibile. I carichi di lavoro Citrix DaaS devono essere in grado di raggiungere questo server licenze.
2. Specificare l'indirizzo del server licenze e la modalità di licenza per utente utilizzando Criteri di gruppo Microsoft. Per ulteriori informazioni, vedere il documento Microsoft che spiega come specificare la modalità gestione licenze Desktop remoto per un server Host sessione Desktop remoto.

I carichi di lavoro di Windows 10 richiedono l'adeguata attivazione della licenza di Windows 10. Si consiglia di seguire la documentazione Microsoft per attivare i carichi di lavoro di Windows 10.

### Utilizzo dell'impegno di consumo

> **Nota:**
>
> Questa funzionalità è disponibile in anteprima.

Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), selezionare la scheda **General** (Generali). Il valore **Consumption** (Consumo) indica il consumo utilizzato nel mese di calendario corrente. Tale valore include gli impegni mensili e a termine.

Quando si seleziona **General** (Generali), la scheda **Notifications** (Notifiche) include:

- Consumo totale utilizzato per il mese (mensile e a termine).
- Numero di unità di impegno di consumo mensile.
- Percentuale dell'impegno di consumo a termine.

I valori e le barre di avanzamento possono avvisare di eccedenze di utilizzo potenziali o effettive.

La visualizzazione dei dati effettivi può richiedere 24 ore. I dati di utilizzo e fatturazione sono considerati finali 72 ore dopo la fine di un mese di calendario.

Per ulteriori informazioni sull'utilizzo, consultare Monitorare le licenze e l'utilizzo attivo.

Facoltativamente, è possibile richiedere che le notifiche vengano visualizzate nella dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida) quando l'utilizzo del consumo (per impegni mensili, a termine o entrambi) raggiunge un livello specificato. Per impostazione predefinita, le notifiche sono disabilitate.

1. Nella scheda **Notifications** (Notifiche), selezionare **Edit Notification Preferences** (Modifica preferenze di notifica).
2. Per abilitare le notifiche, fare clic sul dispositivo di scorrimento in modo da visualizzare il segno di spunta.
3. Immettere un valore. Ripetere l'operazione per l'altro tipo di consumo, se necessario.
4. Selezionare **Save** (Salva).

Per disabilitare le notifiche, fare clic sul dispositivo di scorrimento in modo che il segno di spunta non venga più visualizzato, quindi selezionare **Save** (Salva).

### Monitorare l'utilizzo delle licenze Citrix

Per visualizzare le informazioni sull'utilizzo delle licenze Citrix, seguire le linee guida in Monitorare le licenze e l'utilizzo attivo. È possibile visualizzare:

- Riepilogo delle licenze
- Report sull'utilizzo
- Trend di utilizzo e attività delle licenze
- Utenti con licenza

È anche possibile rilasciare licenze.

### Bilanciamento del carico

Il bilanciamento del carico si applica alle macchine multisessione, non alle macchine a sessione singola.

> **Importante:**
>
> La modifica del metodo di bilanciamento del carico influisce su tutti i cataloghi della distribuzione. Ciò include tutti i cataloghi creati utilizzando qualsiasi tipo di host supportato, basato su cloud e on-premise, indipendentemente dall'interfaccia utilizzata per crearli (ad esempio Full Configuration [Configurazione completa] o Quick Deploy [Distribuzione rapida]).
>
> Assicurarsi di aver configurato i limiti massimi di sessione per tutti i cataloghi prima di procedere.
>
> - In Quick Deploy (Distribuzione rapida), tale impostazione si trova nella scheda **Details** (Dettagli) di ogni catalogo.
> - In Full Configuration (Configurazione completa), vedere Bilanciare il carico delle macchine.

Il bilanciamento del carico misura il carico della macchina e determina quale macchina multisessione selezionare per una sessione utente in entrata nelle condizioni correnti. Questa selezione si basa sul metodo di bilanciamento del carico configurato.

Sono disponibili due metodi di bilanciamento del carico da configurare: orizzontale o verticale. Il metodo si applica a tutti i cataloghi multisessione (e quindi a tutte le macchine multisessione) nella distribuzione Citrix DaaS.

- **Bilanciamento del carico orizzontale:** una sessione utente in entrata viene assegnata alla macchina accesa disponibile con il carico inferiore.

Esempio semplice: si dispone di due macchine configurate per 10 sessioni ciascuna. La prima macchina gestisce cinque sessioni simultanee. La seconda macchina ne gestisce cinque.

Il bilanciamento del carico orizzontale offre elevate prestazioni per l'utente, ma può aumentare i costi man mano che più macchine vengono mantenute accese e occupate.

Questo metodo è abilitato per impostazione predefinita.

- **Bilanciamento del carico verticale:** una sessione utente in entrata viene assegnata alla macchina accesa con l'indice di carico più elevato. Citrix DaaS calcola e quindi assegna un indice di carico per ogni macchina multisessione. Il calcolo considera fattori quali CPU, memoria e concorrenza.

  Questo metodo satura le macchine esistenti prima di passare a nuove macchine. Man mano che gli utenti si disconnettono e liberano capacità sulle macchine esistenti, viene assegnato un nuovo carico a tali macchine.

  Esempio semplice: si dispone di due macchine configurate per 10 sessioni ciascuna. La prima macchina gestisce le prime 10 sessioni simultanee. La seconda macchina gestisce l'undicesima sessione.

  Con il bilanciamento del carico verticale, le sessioni massimizzano la capacità della macchina accesa, il che può far risparmiare sui costi della macchina.

Per configurare il metodo di bilanciamento del carico:

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **General** (Generali) a destra.
2. In **Global Settings** (Impostazioni globali), selezionare **View All** (Visualizza tutto).
3. Nella pagina **Global Settings** (Impostazioni globali), in **Multi-Session Catalog Load Balancing** (Bilanciamento del carico del catalogo multisessione) scegliere il metodo di bilanciamento del carico.
4. Selezionare **Confirm** (Conferma).

### Creare un catalogo in una rete che utilizza un server proxy

Seguire questa procedura se la rete richiede un server proxy per la connettività Internet e se si sta utilizzando la propria sottoscrizione di Azure (l'utilizzo di una sottoscrizione Citrix Managed Azure con una rete che richiede un server proxy non è supportato).

1. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), avviare il processo di creazione del catalogo fornendo le informazioni richieste e selezionando **Create Catalog** (Crea catalogo) nella parte inferiore della pagina.

2. La creazione del catalogo non riesce a causa del requisito del proxy. Tuttavia, viene creata una posizione risorsa. Il nome della posizione risorsa inizia con "DAS", a meno che non sia stato fornito un nome per la posizione risorsa durante la creazione del catalogo. Nella dashboard **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), espandere **Cloud Subscriptions** (Sottoscrizioni cloud) a destra. Nella scheda **Resource Locations** (Posizioni risorse), controllare se la nuova posizione risorsa creata contiene dei Cloud Connector. In caso affermativo, eliminarli.
3. In Azure, creare due macchine virtuali (vedere Requisiti di sistema di Cloud Connector). Aggiungere queste macchine al dominio.
4. Dalla console Citrix Cloud, installare un Cloud Connector su ogni macchina virtuale. Assicurarsi che i Cloud Connector si trovino nella stessa posizione risorsa creata in precedenza. Seguire le linee guida in:
   - Configurazione proxy e firewall di Cloud Connector
   - Requisiti di sistema e connettività
5. Da **Manage > Quick Deploy** (Gestisci > Distribuzione rapida), ripetere il processo di creazione del catalogo. Quando il catalogo viene creato, utilizzare la posizione risorsa e i Cloud Connector creati nei passaggi precedenti.

### Ottenere assistenza

- Consultare Risoluzione dei problemi.
- Se si ha bisogno di ulteriore assistenza con Citrix DaaS, aprire un ticket seguendo le indicazioni riportate in Come ottenere assistenza e supporto.

## Creare gruppi di consegna

December 18, 2023

### Introduzione

Un gruppo di consegna è una raccolta di macchine selezionate da uno o più cataloghi di macchine. Nel gruppo di consegna è anche specificato quali utenti possono utilizzare tali macchine, oltre alle applicazioni e ai desktop disponibili per tali utenti.

La creazione di un gruppo di consegna rappresenta il passaggio successivo per configurare la distribuzione dopo la creazione di un catalogo delle macchine. In seguito è possibile modificare le im-

postazioni iniziali nel primo gruppo di consegna e creare altri gruppi di consegna. Esistono anche funzionalità e impostazioni che è possibile configurare solo quando si modifica un gruppo di consegna, non quando lo si crea.

Prima di creare un gruppo di consegna:

- Consultare questa sezione per conoscere le scelte da fare e le informazioni da fornire.
- Assicurarsi di aver creato una connessione all'hypervisor, al servizio cloud o ad altre risorse che ospitano le macchine.
- Assicurarsi di aver creato un catalogo delle macchine contenente macchine virtuali o fisiche.

Per avviare la procedura guidata per la creazione del gruppo di consegna:

1. Accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Selezionare **Manage** (Gestisci).
3. Se questo è il primo gruppo di consegna creato, la console guida l'utente alla selezione corretta (ad esempio "Set up delivery groups to be displayed as services"[Imposta gruppi di consegna da visualizzare come servizi]). La procedura guidata per la creazione del gruppo di consegna si apre e illustra il processo.
4. Se è già stato creato un gruppo di consegna e si desidera crearne un altro, attenersi alla seguente procedura:
    a) Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
    b) Per organizzare i gruppi di consegna utilizzando le cartelle, creare cartelle nella cartella predefinita **Delivery Groups**. Per ulteriori informazioni, vedere Create a group folder.
    c) Selezionare la cartella in cui si desidera creare il gruppo, quindi fare clic su **Create Delivery Group** (Crea gruppo di consegna). Si apre la procedura guidata per la creazione del gruppo.

La procedura guidata comprende le pagine descritte nella sezione seguente. Le pagine della procedura guidata visualizzate potrebbero essere diverse a seconda delle selezioni effettuate.

### Passaggio 1. Macchine

Selezionare un catalogo delle macchine e selezionare il numero di macchine di quel catalogo che si desidera utilizzare.

Buono a sapersi:

- Almeno una macchina di un catalogo selezionato deve rimanere inutilizzata.

- È possibile specificare un catalogo in più gruppi di consegna. Tuttavia, una macchina può essere utilizzata in un solo gruppo di consegna.
- Un gruppo di consegna può utilizzare macchine di più di un catalogo. Tuttavia, tali cataloghi devono contenere gli stessi tipi di macchine (sistema operativo multisessione, sistema operativo a sessione singola o accesso remoto al PC). In altre parole, non è possibile combinare tipi di macchina diversi in uno stesso gruppo di consegna. Analogamente, se la distribuzione contiene cataloghi di macchine Windows e cataloghi di macchine Linux, un gruppo di consegna può contenere macchine dell'uno o dell'altro tipo ma non di entrambi.
- Un gruppo di consegna MCS può aggiungere solo un catalogo di tipo MCS.
- Citrix consiglia di installare o aggiornare tutti i VDA alla versione più recente, quindi di eseguire il comando **Change functional level** (Cambia livello funzionale) per i cataloghi delle macchine e i gruppi di consegna in base alle esigenze. Quando si crea un gruppo di consegna, se si selezionano macchine con versioni VDA diverse installate, il gruppo di consegna è compatibile con la versione VDA meno recente. Ad esempio, se su una delle macchine è installato un VDA versione 7.1 e su altre macchine è installata la versione corrente, tutte le macchine del gruppo possono utilizzare solo le funzionalità supportate in VDA 7.1. Ciò significa che alcune funzionalità che richiedono versioni più recenti del VDA potrebbero non essere disponibili in tale gruppo di consegna.
- Vengono eseguiti i seguenti controlli di compatibilità:
  - MinimumFunctionalLevel deve essere compatibile
  - SessionSupport deve essere compatibile
  - AllocationType deve essere compatibile per SingleSession
  - ProvisioningType deve essere compatibile
  - PersistChanges deve essere compatibile per MCS e Citrix Provisioning
  - Il catalogo RemotePC è compatibile solo con il catalogo RemotePC
  - Controllo relativo ad AppDisk

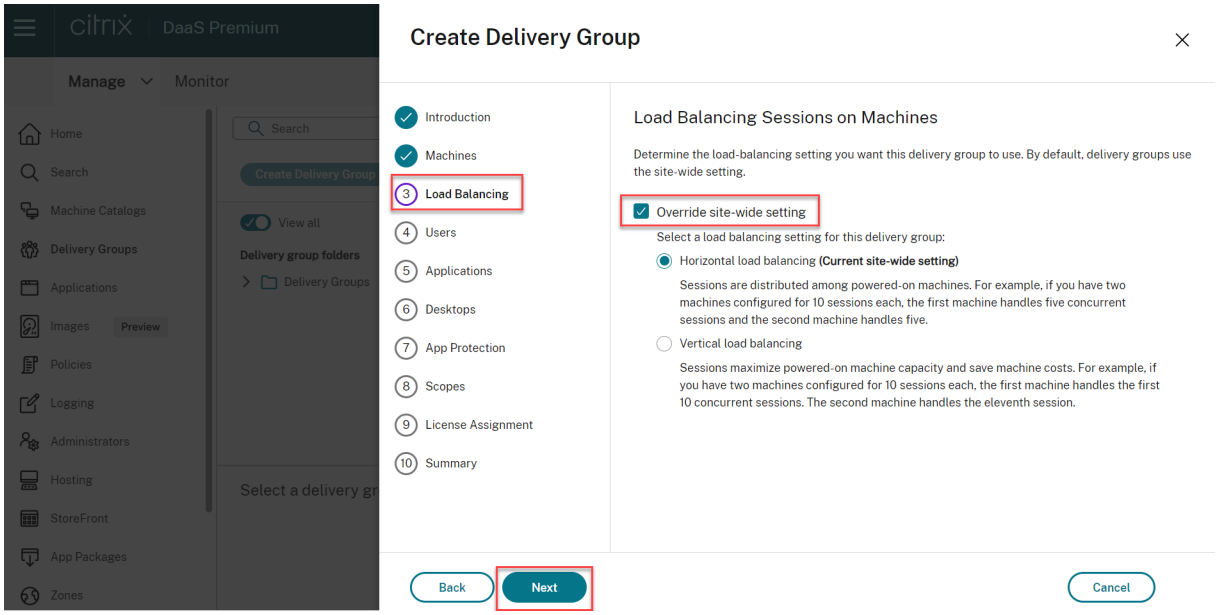
### Passaggio 2. Bilanciamento del carico (anteprima)

Per configurare le impostazioni di bilanciamento del carico durante la creazione di un gruppo di consegna:

1. Accedere a DaaS Premium.
2. Nel riquadro di navigazione a sinistra, fare clic su **Delivery Groups** (Gruppi di consegna).
3. Nella pagina **Delivery Groups**, fare clic su **Create Delivery Group** (Crea gruppo di consegna).
4. Nella procedura guidata **Create Delivery Group**, fare clic su **Next** (Avanti). Si apre la procedura guidata **Machines**.

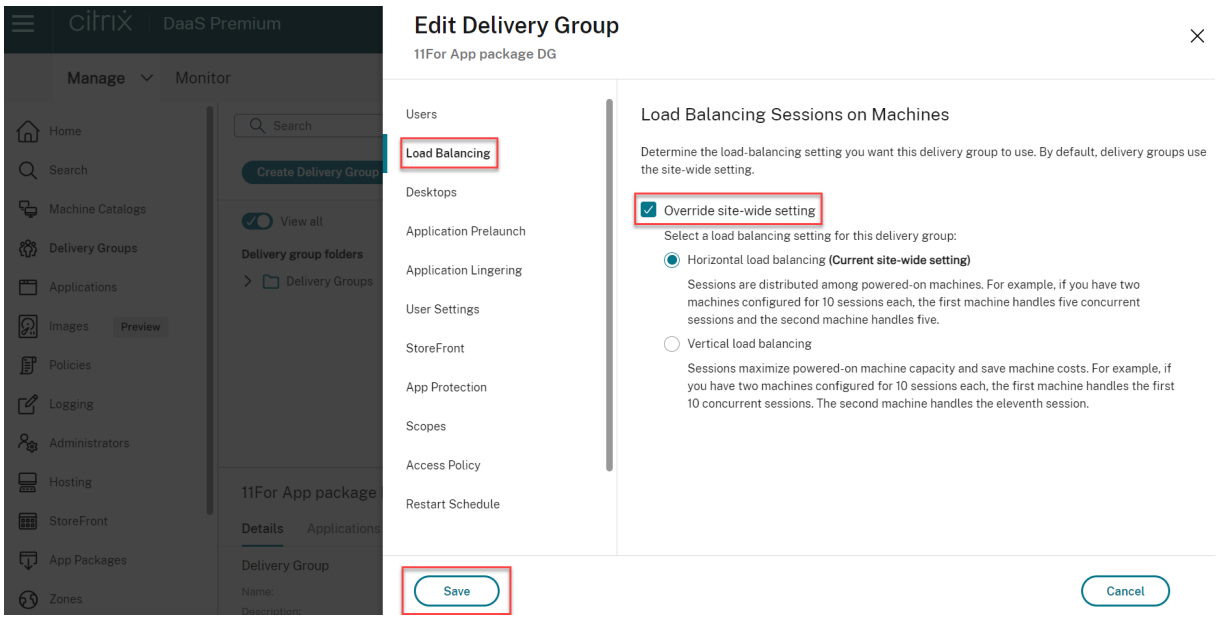
5. Nella procedura guidata **Machines**, selezionare un catalogo macchine richiesto e fare clic su **Next**. Si apre la procedura guidata **Load Balancing** (Bilanciamento del carico).
6. Nella procedura guidata **Load Balancing**, selezionare la casella di controllo **Override site-wide setting** (Ignora impostazione a livello di sito).
7. Selezionare l'opzione **Horizontal load balancing** (Bilanciamento del carico orizzontale) o **Vertical load balancing option** (Bilanciamento del carico verticale) come richiesto e fare clic su **Next**.




Per configurare le impostazioni di bilanciamento del carico durante la modifica di un gruppo di consegna esistente:

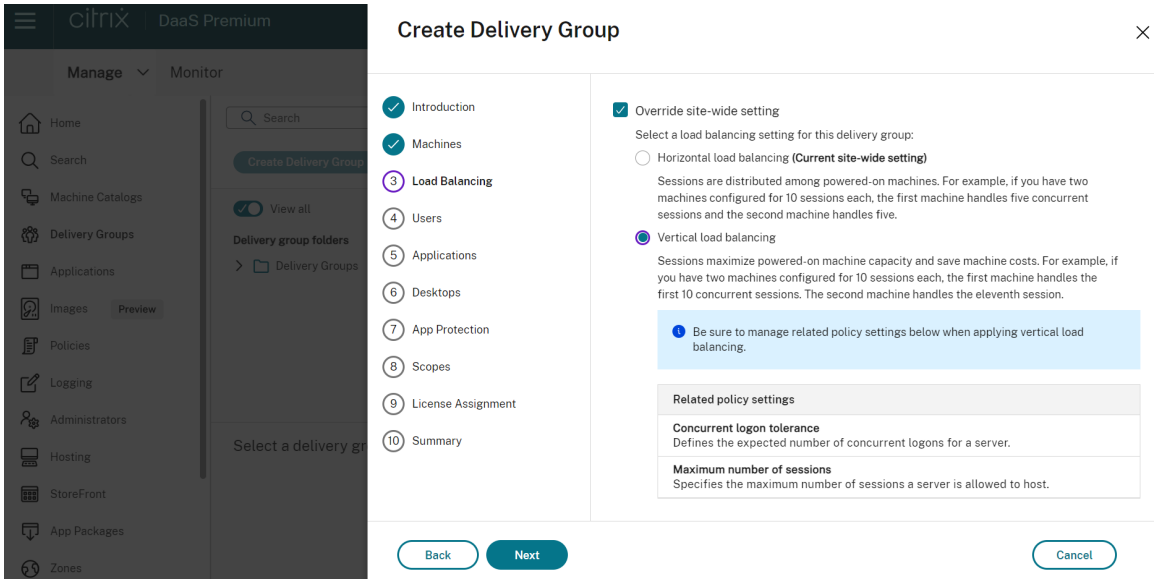
1. Accedere a DaaS Premium.
2. Nel riquadro di navigazione a sinistra, fare clic su **Delivery Groups** (Gruppi di consegna).
3. Selezionare un **gruppo di consegna** dall'elenco e fare clic su **Edit** (Modifica). Si apre la procedura guidata **Edit Delivery Group** (Modifica gruppo di consegna).
4. Nella pagina **Edit Delivery Group**, fare clic su **Load Balancing**.
5. Selezionare la casella di controllo **Override site-wide setting** (Ignora impostazione a livello di sito).
6. Selezionare l'opzione **Horizontal load balancing** (Bilanciamento del carico orizzontale) o **Vertical load balancing** (Bilanciamentodel carico verticale) come richiesto e fate clic su **Save**.




**Nota:**

Quando viene applicata l'impostazione Vertical load balancing, assicurarsi che i criteri **Concurrent logon tolerance** (Tolleranza di accesso simultaneo) e **Maximum number of sessions** (Numero massimo di sessioni) siano configurati in modo appropriato.




Per ulteriori informazioni sul bilanciamento del carico a livello di sito e a livello di gruppo di consegna, vedere Bilanciare il carico delle macchine.

### Passaggio 3. Tipo di consegna

Questa pagina viene visualizzata solo se è stato scelto un catalogo delle macchine contenente macchine statiche (assegnate) con sistema operativo a sessione singola. Scegliere **Applications** (Applicazioni) o **Desktops** (Desktop). Non è possibile abilitare entrambi.

Se sono state selezionate macchine da un catalogo per sistema operativo multi-sessione o di macchine con sistema operativo a sessione singola casuale (in pool), si presume che il tipo di consegna sia applicazioni e desktop. È possibile distribuire applicazioni, desktop o entrambi.

### Passaggio 4. AppDisks

Ignorare questa pagina. Selezionare **Next** (Avanti).

### Passaggio 5. Utenti

Specificare gli utenti e i gruppi di utenti che possono utilizzare le applicazioni e i desktop del gruppo di consegna.

#### Dove vengono specificati gli elenchi degli utenti

Gli elenchi degli utenti vengono specificati quando si crea o si modifica quanto segue:

- Elenco di accesso utente di una distribuzione, che non è configurato tramite questa console. Per impostazione predefinita, la regola dei criteri di autorizzazione applicazione include tutti gli utenti. Per ulteriori informazioni, vedere i cmdlet `BrokerAppEntitlementPolicyRule` dell'SDK di PowerShell.
- Gruppi di consegna.
- Applicazioni.

> **Nota:**
>
> Quando si specifica un elenco di utenti, è possibile selezionare gli account utente da uno dei seguenti provider di identità a cui è connesso l'account Citrix Cloud: Active Directory, Azure Active Directory o Okta.

L'elenco degli utenti che possono accedere a un'applicazione è formato dall'intersezione degli elenchi di utenti di cui sopra.

**Utenti autenticati e non autenticati**

Esistono due tipi di utenti: autenticati e non autenticati (quelli non autenticati sono anche detti anonimi). È possibile configurare uno o entrambi i tipi in un gruppo di consegna.

- **Authenticated** (Autenticati): per accedere alle applicazioni e ai desktop, gli utenti e i membri del gruppo specificati per nome devono presentare credenziali quali smart card o nome utente e password per l'app StoreFront o Citrix Workspace. Per i gruppi di consegna contenenti macchine con sistema operativo a sessione singola, è possibile importare i dati utente (un elenco di utenti) in un secondo momento modificando il gruppo di consegna.
- **Non autenticati (anonimi):** per i gruppi di consegna contenenti macchine con sistema operativo multi-sessione, è possibile consentire agli utenti di accedere alle applicazioni e ai desktop senza presentare le credenziali all'app StoreFront o Citrix Workspace. Ad esempio, nei chioschi, l'applicazione potrebbe richiedere le credenziali, ma il portale di accesso Citrix e gli strumenti non lo fanno. Viene creato un gruppo di utenti anonimi quando si installa il primo Delivery Controller.

  Per concedere l'accesso agli utenti non autenticati, ogni macchina del gruppo di consegna deve disporre di un VDA con sistema operativo multisessione installato. Quando sono abilitati gli utenti non autenticati, è necessario disporre di un archivio StoreFront non autenticato.

  Gli account utente non autenticati vengono creati su richiesta all'avvio di una sessione e sono denominati AnonXYZ, in cui XYZ è un valore univoco a tre cifre.

  Le sessioni utente non autenticate hanno un timeout di inattività predefinito di 10 minuti e vengono disconnesse automaticamente quando il client si disconnette. La riconnessione, il roaming tra i client e il controllo Workspace non sono supportati.

Nella tabella seguente vengono descritte le scelte effettuate nella pagina **Users**:

| Abilitare l'accesso per | Aggiungere/assegnare utenti e gruppi di utenti? | Attivare la casella di controllo "Give access to unauthenticated users" (Concedi accesso a utenti non autenticati)? |
|---|---|---|
| Solo utenti autenticati | Sì | No |
| Solo utenti non autenticati | No | Sì |
| Utenti autenticati e non autenticati | Sì | Sì |

#### Limitazione dell'accesso di utenti o gruppi

È anche possibile limitare l'uso di un gruppo di consegna aggiungendo utenti o gruppi di utenti all'elenco **Allow list**. Solo gli utenti inclusi nell'elenco **Allow list** possono accedere alle app e ai desktop del gruppo di consegna. È anche possibile aggiungere utenti e gruppi di utenti a un elenco di blocco facendo clic su **Add block list** (Aggiungi elenco di blocco), per impedire agli utenti di utilizzare le app e desktop del gruppo di consegna selezionato. Un elenco di blocco è significativo solo quando viene utilizzato per bloccare utenti contenuti nell'elenco degli utenti consentiti.

### Passaggio 6. Applicazioni

Buono a sapersi:

- Non è possibile aggiungere applicazioni ai gruppi di consegna Accesso remoto PC.
- Per impostazione predefinita, le nuove applicazioni aggiunte vengono inserite in una cartella denominata Applications. È possibile specificare una cartella diversa. Per ulteriori informazioni, vedere l'articolo Applicazioni.
- È possibile modificare le proprietà di un'applicazione quando la si aggiunge a un gruppo di consegna o in un secondo momento. Per ulteriori informazioni, vedere l'articolo Applicazioni.
- Se si tenta di aggiungere un'applicazione e in quella cartella ne esiste già una con lo stesso nome, verrà richiesto di rinominare l'applicazione che si sta aggiungendo. Se si rifiuta, all'applicazione viene aggiunto un suffisso che la rende univoca all'interno di quella cartella di applicazioni.
- Quando si aggiunge un'applicazione a più di un gruppo di consegna, può verificarsi un problema di visibilità se non si dispone dell'autorizzazione a visualizzare l'applicazione in tutti questi gruppi di consegna. In questi casi, vedere un amministratore con autorizzazioni più ampie o estendere il proprio ambito per includere tutti i gruppi di consegna a cui è stata aggiunta l'applicazione.
- Se si pubblicano due applicazioni con lo stesso nome per gli stessi utenti, modificare la proprietà Application name (for user) [Nome applicazione (per utente)]. In caso contrario, gli utenti vedranno nomi duplicati nell'app Citrix Workspace.

Selezionare il menu **Add** (Aggiungi) per visualizzare le origini dell'applicazione.

- **From Start menu** (Dal menu Start): applicazioni individuate in una macchina creata dall'immagine nel catalogo selezionato. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco di applicazioni rilevate; selezionare quelle che si desidera aggiungere e quindi selezionare **OK**.
- **Manually defined** (Definizione manuale): applicazioni situate nella distribuzione o in un altro punto della rete. Quando si seleziona questa origine, viene avviata una nuova pagina in cui

si digita il percorso dell'eseguibile, della directory di lavoro, degli argomenti della riga di comando facoltativi e dei nomi visualizzati per amministratori e utenti. Dopo aver inserito queste informazioni, selezionare **OK**.

- **Existing** (Esistenti): applicazioni precedentemente aggiunte alla distribuzione, forse in un altro gruppo di consegna. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco di applicazioni rilevate; selezionare quelle che si desidera aggiungere e quindi selezionare **OK**.
- **App-V**: applicazioni contenute in pacchetti App-V. Quando si seleziona questa origine, viene avviata una nuova pagina in cui si seleziona il server App-V o la libreria di applicazioni. Selezionare le applicazioni che si desidera aggiungere dalla visualizzazione risultante, quindi selezionare **OK**.

Se l'origine di un'applicazione o un'applicazione non è disponibile o valida, questa non è visibile o non è selezionabile. Ad esempio, l'origine **Existing** (Esistenti) non è disponibile se alla distribuzione non sono state aggiunte applicazioni. Oppure un'applicazione potrebbe non essere compatibile con i tipi di sessione supportati sulle macchine del catalogo selezionato.

### Passaggio 7. App Protection

Le seguenti informazioni sono supplementari all'articolo App Protection nella documentazione di Citrix Virtual Apps and Desktops. Per utilizzare la protezione delle app in un'implementazione Citrix DaaS, seguire le linee guida generali offerte in quell'articolo, tenendo conto dei dettagli di cui sotto.

- È necessario disporre di un abbonamento Citrix Cloud valido e di diritti di protezione delle app validi. Per acquistare la funzione di protezione delle app, contattare il proprio rappresentante commerciale Citrix.
- La protezione delle app richiede l'attendibilità XML. Per abilitare l'attendibilità XML, andare a **Settings > Enable XML trust** (Impostazioni > Abilita attendibilità XML).
- Per quanto riguarda anti-screen-capturing:
  - Su Windows e macOS, solo la finestra del contenuto protetto è vuota. La protezione delle app è attiva quando una finestra protetta non è ridotta a icona.
  - Nel sistema operativo Linux, l'intera acquisizione è vuota. La protezione delle app è attiva indipendentemente dal fatto che una finestra protetta sia ridotta a icona o meno.

### Passaggio 8. Desktop (o regole di assegnazione dei desktop)

Il titolo di questa pagina dipende dal catalogo delle macchine scelto in precedenza nella procedura guidata:

- Se si sceglie un catalogo contenente macchine in pool, questa pagina si intitola **Desktops**.
- Se è stato scelto un catalogo contenente macchine assegnate e si è specificato "Desktops"nella pagina **Delivery Type** (Tipo di consegna), questa pagina si intitola **Desktop Assignment Rules** (Regole di assegnazione desktop).
- Se si sceglie un catalogo contenente macchine assegnate e si era specificato "Applications"nella pagina **Delivery Type**, questa pagina si intitola **Applications** (Applicazioni).

Selezionare **Add** (Aggiungi). Nella finestra di dialogo:

- Nei campi **Display name** (Nome visualizzato) e **Description** (Descrizione), digitare le informazioni da visualizzare nell'app Citrix Workspace.
- Per aggiungere una restrizione tag a un desktop, selezionare **Restrict launches to machines with this tag** (Limita avvii alle macchine con questo tag), quindi selezionare il tag dal menu.
- Utilizzando i pulsanti di opzione è possibile selezionare:
  - **Allow everyone with access to this delivery group to use a desktop** (Consenti a tutti coloro che hanno accesso a questo gruppo di consegna di utilizzare un desktop). Tutti gli utenti del gruppo di consegna possono avviare un desktop (per gruppi con macchine in pool) o ricevere una macchina quando avviano il desktop (per gruppi con macchine assegnate).
  - **Restrict desktop use** (Limita l'uso del desktop): l'uso del desktop viene limitato aggiungendo utenti e gruppi di utenti all'elenco **Allow**. Solo gli utenti presenti nell'elenco **Allow** possono accedere a un desktop. È anche possibile aggiungere utenti e gruppi di utenti a un elenco di blocco facendo clic su **Add block list** (Aggiungi elenco di blocco), per impedire agli utenti di utilizzare i desktop del gruppo di consegna selezionato. Un elenco di blocco è significativo solo quando viene utilizzato per bloccare utenti contenuti nell'elenco degli utenti consentiti.
- Se il gruppo contiene macchine assegnate, specificare il numero massimo di desktop per utente. Questo deve essere un valore pari a uno o maggiore di uno.
- Attivare o disattivare il desktop (per le macchine in pool) o la regola di assegnazione desktop (per le macchine assegnate). La disattivazione di un desktop interrompe la distribuzione del desktop. La disattivazione di una regola di assegnazione desktop interrompe l'assegnazione automatica del desktop agli utenti.
- Al termine, selezionare **OK**.

### Passaggio 9 Assegnazione licenza

Determina la licenza che si desidera venga utilizzata dal gruppo di consegna. Per impostazione predefinita, il gruppo di consegna utilizza la licenza del sito. Per ulteriori informazioni, vedere Licenze multi-tipo.

### Passaggio 10. Riepilogo

Inserire un nome per il gruppo di consegna. È inoltre possibile (facoltativamente) immettere una descrizione, che viene visualizzata nell'app Workspace e nell'interfaccia di gestione Full Configuration (Configurazione completa).

Esaminare le informazioni di riepilogo e quindi selezionare **Finish** (Fine). Se non è stata selezionata alcuna applicazione o non è stato specificato alcun desktop da distribuire, viene chiesto se si desidera continuare.

### Ulteriori informazioni

- Gestire i gruppi di consegna
- Applicazioni

## Gestire i gruppi di consegna

November 21, 2023

### Introduzione

In questo articolo vengono descritte le procedure per la gestione dei gruppi di consegna dalla console di gestione. Oltre a modificare le impostazioni specificate durante la creazione del gruppo, è possibile configurare altre impostazioni non disponibili quando si crea un gruppo di consegna.

Le procedure sono organizzate per categorie: generali, utenti, macchine e sessioni. Alcune attività riguardano più di una categoria. Ad esempio l'opzione "Prevent users from connecting to machines" (Impedisci agli utenti di connettersi alle macchine) è descritta nella categoria macchine, ma influisce anche sugli utenti. Se non si riesce a trovare un'attività in una categoria, controllare in una categoria correlata.

Altri articoli contengono anche informazioni correlate:

- L'articolo Applicazioni contiene informazioni sulla gestione delle applicazioni nei gruppi di consegna.
- La gestione dei gruppi di consegna richiede le autorizzazioni predefinite dell'amministratore del gruppo di consegna. Per ulteriori informazioni, vedere Amministrazione delegata.

## Aspetti generali

- Modificare il tipo di consegna
- Modificare gli indirizzi StoreFront
- Cambiare il livello funzionale
- Gestire i gruppi di consegna di Remote PC Access
- Modificare la licenza per un gruppo di consegna
- Organizzare i gruppi di consegna utilizzando le cartelle
- Gestire la protezione delle app

### Modificare il tipo di consegna di un gruppo di consegna

Il tipo di consegna indica ciò che il gruppo può fornire: applicazioni, desktop o entrambi.

Prima di cambiare un tipo di **applicazione** nel tipo **Desktops** (Desktop), eliminare tutte le applicazioni dal gruppo.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Delivery Type** (Tipo di spedizione) selezionare il tipo di consegna desiderato.
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. Oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

### Modificare gli indirizzi StoreFront

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **StoreFront**, indicare se si desidera specificare un indirizzo del server StoreFront in un secondo momento (**Manually** [Manualmente]) oppure selezionare **Add new** (Aggiungi nuovo) per specificare i server StoreFront che si desidera utilizzare (**Automatically** [Automaticamente]).
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. Oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

È inoltre possibile specificare gli indirizzi del server StoreFront selezionando **StoreFront** nel riquadro di sinistra della console.

### Cambiare il livello funzionale

Modificare il livello funzionale del gruppo di consegna dopo aver aggiornato i VDA sulle relative macchine e i cataloghi delle macchine contenenti le macchine utilizzate nel gruppo di consegna.

Prima di iniziare:

- Se si utilizza Citrix Provisioning (in precedenza Provisioning Services), aggiornare la versione VDA nella console Citrix Provisioning.
- Avviare le macchine contenenti il VDA aggiornato in modo che possano registrarsi con Citrix DaaS. Questo processo indica alla console ciò che deve essere modificato nel gruppo di consegna.
- Se si continua a utilizzare versioni precedenti dei VDA, le funzionalità più recenti del prodotto potrebbero non essere disponibili. Per ulteriori informazioni, vedere la documentazione di aggiornamento.

Per modificare il livello funzionale di un gruppo di consegna:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Change Functional Level** (Cambia livello funzionale) nella barra delle azioni. L'azione **Change Functional Level** (Cambia livello funzionale) viene visualizzata solo se vengono rilevati VDA aggiornati.

Viene indicato quali macchine, se presenti, non possono passare a quel determinato livello funzionale e perché. È quindi possibile annullare l'azione di modifica, risolvere i problemi della macchina e quindi eseguire nuovamente l'azione di modifica.

Una volta completato la modifica, è possibile ripristinare le macchine ai loro stati precedenti. Selezionare il gruppo di consegna, quindi selezionare **Undo Functional Level Change** (Annulla modifica livello funzionale) nella barra delle azioni.

### Gestire i gruppi di consegna di Remote PC Access

Se una macchina contenuta in un catalogo delle macchine Accesso remoto PC non è assegnata a un utente, viene temporaneamente assegnata a un gruppo di consegna associato a tale catalogo. Questa assegnazione temporanea consente di assegnare la macchina a un utente in un secondo momento.

L'associazione fra catalogo macchine e gruppo di consegna ha un valore di priorità. La priorità determina a quale gruppo di consegna è assegnata la macchina quando si registra nel sistema o quando un utente necessita di un'assegnazione macchina: più basso è il valore, maggiore è la priorità. Se un catalogo di macchine Accesso remoto PC dispone di più assegnazioni di gruppi di consegna, il software seleziona quella con la priorità più alta. Utilizzare l'SDK di PowerShell per impostare questo valore di priorità.

Quando vengono creati per la prima volta, i cataloghi di macchine Remote PC Access (Accesso remoto PC) vengono associati a un gruppo di consegna. Questa associazione significa che gli account delle macchine o le unità organizzative aggiunti al catalogo in un secondo momento possono essere aggiunti al gruppo di consegna. Questa associazione può essere disattivata o attivata.

Per aggiungere o rimuovere un'associazione di catalogo macchine di Accesso remoto PC con un gruppo di consegna:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo Accesso remoto PC.
3. Nella sezione **Details** (Dettagli), fare clic sulla scheda **Machine Catalogs** (Cataloghi macchine) e quindi selezionare un catalogo di Accesso remoto PC.
4. Per aggiungere o ripristinare un'associazione, selezionare **Add Desktops** (Aggiungi desktop). Per rimuovere un'associazione, selezionare **Remove Association** (Rimuovi associazione).

#### Modificare la licenza per un gruppo di consegna

Per modificare il diritto alla licenza per un gruppo di consegna, effettuare le seguenti operazioni:

1. Selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro di spostamento.
2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **License Assignment** (Assegnazione licenza), selezionare la licenza che si desidera venga utilizzata dal gruppo.
4. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, fare clic su **Save** (Salva) per applicare le modifiche e chiudere la finestra.

Per ulteriori informazioni sui diritti a livello di gruppo di consegna, consultare Multi-type licensing (Licenze multi-tipo).

#### Organizzare i gruppi di consegna utilizzando le cartelle

È possibile creare cartelle per organizzare i gruppi di consegna per un facile accesso.

**Ruoli richiesti** Per impostazione predefinita, è necessario disporre del seguente ruolo integrato per creare e gestire le cartelle del gruppo di consegna: Cloud Administrator (amministratore cloud), Full Administrator (amministratore completo) o Delivery Group Administrator (amministratore del gruppo di consegna). Se necessario, è possibile personalizzare i ruoli per la creazione e la gestione delle cartelle del gruppo di consegna. Per ulteriori informazioni, consultare Autorizzazioni richieste.

**Creare una cartella del gruppo di consegna** Prima di iniziare, pianificare come organizzare i gruppi di consegna. Considerare quanto segue:

- È possibile nidificare le cartelle fino a cinque livelli (esclusa la cartella principale predefinita).
- Una cartella può contenere gruppi di consegna e sottocartelle.
- Tutti i nodi in **Full Configuration** (Configurazione completa) (come i **cataloghi delle macchine**, i nodi delle **applicazioni** e dei **gruppi di consegna**) condividono un albero delle cartelle nel back-end. Per evitare conflitti di nomi con altri nodi durante la ridenominazione o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in nodi diversi.

Per creare una cartella del gruppo di consegna, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella e quindi selezionare **Create Folder** (Crea cartella) nella barra **Actions** (Azioni).
3. Immettere un nome per la nuova cartella, quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> Se si crea una cartella in una posizione non prevista, è possibile trascinarla nella posizione corretta.

### Spostare un gruppo di consegna

È possibile spostare un gruppo di consegna da una cartella all'altra. I passaggi dettagliati sono i seguenti:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Visualizzare i gruppi per cartella. È anche possibile attivare **View all** (Visualizza tutto) sopra la gerarchia delle cartelle per visualizzare tutti i gruppi contemporaneamente.
3. Fare clic con il pulsante destro del mouse su un gruppo, quindi selezionare **Move Delivery Group** (Sposta gruppo di consegna).
4. Selezionare la cartella in cui si desidera spostare il gruppo e quindi fare clic su **Done** (Fine).

> **Suggerimento:**
>
> È possibile trascinare un gruppo in una cartella.

### Gestire le cartelle dei gruppi di consegna

È possibile eliminare, rinominare e spostare le cartelle dei gruppi di consegna.

Tenere presente che è possibile eliminare una cartella solo se essa e le relative sottocartelle non contengono gruppi di consegna.

Per gestire una cartella, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, selezionare una cartella, quindi selezionare un'azione nella barra **Actions** (Azioni) in base alle esigenze:
   - Per rinominare la cartella, selezionare **Rename Folder** (Rinomina cartella).
   - Per eliminare la cartella, selezionare **Delete Folder** (Elimina cartella).
   - Per spostare la cartella, selezionare **Move Folder** (Sposta cartella).
3. Seguire le istruzioni sullo schermo per completare i passaggi rimanenti.

**Autorizzazioni richieste** Nella tabella seguente sono elencate le autorizzazioni necessarie per eseguire azioni sulle cartelle dei gruppi di consegna.

| Azione | Autorizzazioni richieste |
|---|---|
| Creare cartelle dei gruppi di consegna | Creazione di cartella del gruppo di consegna |
| Eliminare le cartelle dei gruppi di consegna | Rimozione della cartella del gruppo di consegna |
| Spostare le cartelle dei gruppi di consegna | Spostamento cartella del gruppo di consegna |
| Ridenominare le cartelle dei gruppi di consegna | Modifica della cartella del gruppo di consegna |
| Spostare i gruppi di consegna nelle cartelle | Modifica della cartella del gruppo di consegna e modifica delle proprietà del gruppo di consegna |

### Gestire la protezione delle app

Le seguenti informazioni sono supplementari all'articolo App Protection nella documentazione di Citrix Virtual Apps and Desktops. Per utilizzare la protezione delle app in un'implementazione Citrix DaaS, seguire le linee guida generali offerte in quell'articolo, tenendo conto dei dettagli di cui sotto.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.

2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Manage app protection**, è possibile abilitare l'**Anti-keylogging e l'Anti-Screen-Capturing**.

- È necessario disporre di un abbonamento Citrix Cloud valido e di diritti di protezione delle app validi. Per acquistare la funzione di protezione delle app, contattare il proprio rappresentante commerciale Citrix.
- La protezione delle app richiede l'attendibilità XML. Per abilitare l'attendibilità XML, andare a **Settings > Enable XML trust** (Impostazioni > Abilita attendibilità XML).
- Per quanto riguarda anti-screen-capturing:
  - Su Windows e macOS, solo la finestra del contenuto protetto è vuota. La protezione delle app è attiva quando una finestra protetta non è ridotta a icona.
  - Nel sistema operativo Linux, l'intera acquisizione è vuota. La protezione delle app è attiva indipendentemente dal fatto che una finestra protetta sia ridotta a icona o meno.

## Utenti

> **Nota:**
>
> L'opzione **Leave user management to Citrix Cloud** (Lascia la gestione degli utenti a Citrix Cloud) è stata rimossa. Per quanto riguarda i gruppi di consegna in cui le assegnazioni degli utenti sono state gestite tramite Citrix Cloud, continuare a gestirle all'interno della libreria Citrix Cloud.

Questo argomento copre le seguenti sezioni:

- Modificare le impostazioni utente
- Aggiungere o rimuovere utenti

### Modificare le impostazioni utente in un gruppo di consegna

Il nome di questa pagina viene visualizzato come **User Settings** (Impostazioni utente) o **Basic Settings** (Impostazioni di base).

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **User Settings** (Impostazioni utente), modificare una qualsiasi delle impostazioni nella tabella seguente.

4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. Oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

| Impostazione | Descrizione |
|---|---|
| Descrizione | Testo utilizzato da Citrix Workspace (o StoreFront) e visualizzato dagli utenti. |
| Enable delivery group (Abilita gruppo di consegna) | Indica se il gruppo di consegna è abilitato. |
| Time zone (Fuso orario) | Il fuso orario in cui devono risiedere le macchine di questo gruppo di consegna. L'opzione elenca i fusi orari supportati dal sito. **Nota:** la modifica del fuso orario su un gruppo di consegna potrebbe provocare il riavvio delle macchine del gruppo. Per evitare ciò, modificare le impostazioni del fuso orario solo al di fuori degli orari di produzione. |
| Enable Secure ICA | Protegge le comunicazioni da e verso le macchine del gruppo di consegna utilizzando SecureICA, che crittografa il protocollo ICA. Il livello predefinito è 128 bit. Il livello può essere modificato utilizzando l'SDK. Citrix consiglia di utilizzare più metodi di crittografia come la crittografia TLS durante l'attraversamento di reti pubbliche. Inoltre, SecureICA non controlla l'integrità dei dati. |
| Numero massimo di desktop per utente | Quanti desktop può avere un utente. |

#### Aggiungere o rimuovere utenti in un gruppo di consegna

Per informazioni dettagliate sugli utenti, vedere Utenti.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
3. Nella pagina **Users** (Utenti):
   - Per aggiungere utenti, selezionare **Add** (Aggiungi) e specificare gli utenti da aggiungere.

- Per rimuovere utenti, selezionare uno o più utenti, quindi selezionare **Remove** (Rimuovi).
- Selezionare o deselezionare la casella di controllo per consentire l'accesso agli utenti non autenticati.

4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. Oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

**Gestire le assegnazioni degli utenti** Per gestire le assegnazioni degli utenti:

1. In **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna).
2. Selezionare un gruppo, quindi selezionare **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
3. Nella pagina **Machine Allocation** (Allocazione macchine), aggiungere o rimuovere utenti. Per aggiungere utenti, selezionarli o immettere un elenco di nomi utente separato da punti e virgole.

Quando si immettono i nomi utente, considerare quanto segue:

- Se gli utenti si trovano in Active Directory, immettere direttamente i nomi. In caso contrario, inserire i nomi in questo formato: `<identity provider>:<user name>`. Esempio: `AzureAD:username`.

## Macchine

- Modificare le assegnazioni delle macchine agli utenti
- Aggiornare una macchina
- Aggiungere, modificare o rimuovere una restrizione di tag per un desktop
- Rimuovere una macchina
- Limitare l'accesso alle macchine
- Impedire agli utenti di connettersi a una macchina (modalità manutenzione)
- Arrestare e riavviare le macchine
- Creare e gestire pianificazioni di riavvio per le macchine
- Caricare macchine gestite
- Gestire la scalabilità automatica

Oltre alle funzionalità descritte in questo articolo, vedere Scalabilità automatica per informazioni sulla gestione proattiva dell'alimentazione delle macchine.

### Modificare le assegnazioni delle macchine agli utenti di un gruppo di consegna

È possibile modificare le assegnazioni delle macchine con sistema operativo a sessione singola con provisioning MCS. Non è possibile modificare le assegnazioni per macchine con sistema operativo

multisessione o macchine con provisioning fornito da Citrix Provisioning.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Machine Allocation** (Allocazione macchine), specificare i nuovi utenti.
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. Oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

#### Aggiornare una macchina di un gruppo di consegna

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
3. Selezionare una macchina e quindi selezionare **Update Machines** (Aggiorna macchine) nella barra delle azioni.

Per scegliere un'immagine master diversa, selezionare **Master image** (Immagine master), quindi selezionare una snapshot.

Per applicare le modifiche e notificarlo agli utenti della macchina, selezionare **Rollout notification to end-users** (Notifica rollout agli utenti finali). Quindi specificare:

- Quando aggiornare l'immagine: ora o al successivo riavvio
- Il tempo di distribuzione del riavvio (il tempo totale per iniziare ad aggiornare tutte le macchine del gruppo)
- Indica se gli utenti vengono avvisati del riavvio
- Il messaggio che ricevono gli utenti

#### Aggiungere, modificare o rimuovere una restrizione di tag per un desktop

L'aggiunta, la modifica e la rimozione di restrizioni ai tag possono avere effetti imprevisti sui desktop di cui si considera l'avvio. Leggere le considerazioni e le avvertenze in Tag.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Desktops** (Desktop) selezionare il desktop e selezionare **Modifica**.
4. Per aggiungere una restrizione tag, selezionare **Restrict launches to machines with the tag** (Limita avvii alle macchine con il tag), quindi selezionare il tag.

5. Per modificare o rimuovere una restrizione tag, effettuare le seguenti operazioni:
    - Selezionare un tag diverso.
    - Rimuovere la restrizione tag deselezionando **Restrict launches to machines with this tag** (Limita avvii alle macchine con il tag).
6. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. Oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

#### Rimuovere una macchina da un gruppo di consegna

La rimozione di una macchina la elimina da un gruppo di consegna. Non la elimina dal catalogo macchine utilizzato dal gruppo di consegna. Pertanto, tale macchina è disponibile per l'assegnazione a un altro gruppo di consegna.

Le macchine devono essere spente prima di poter essere rimosse. Per impedire temporaneamente agli utenti di connettersi a una macchina durante la rimozione, mettere la macchina in modalità di manutenzione prima di spegnerla.

Le macchine potrebbero contenere dati personali, quindi prestare attenzione prima di allocare la macchina a un altro utente. Considerare la possibilità di ricreare l'immagine della macchina.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
3. Assicurarsi che la macchina sia spenta.
4. Selezionare la macchina, quindi selezionare **Remove from Delivery Group** (Rimuovi dal gruppo di consegna) nella barra delle azioni.

È inoltre possibile rimuovere una macchina da un gruppo di consegna tramite la connessione utilizzata dalla macchina.

#### Limitare l'accesso alle macchine di un gruppo di consegna

Qualsiasi modifica apportata per limitare l'accesso alle macchine di un gruppo di consegna sostituisce le impostazioni precedenti, indipendentemente dal metodo utilizzato. È possibile effettuare le seguenti operazioni:

- **Restrict access for administrators using delegated administration scopes** (Limita l'accesso per gli amministratori utilizzando ambiti di amministrazione delegata): creare e assegnare un ambito che consente agli amministratori di accedere a tutte le applicazioni e un altro ambito

che consente l'accesso solo a determinate applicazioni. Per ulteriori informazioni, vedere Amministrazione delegata.

- **Limitare l'accesso agli utenti tramite espressioni dei criteri SmartAccess:** utilizzare le espressioni dei criteri per filtrare le connessioni degli utenti effettuate tramite Citrix Gateway.

  1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
  2. Selezionare un gruppo e quindi fare clic su **Edit** (Modifica) nella barra delle azioni.
  3. Nella pagina **Access Policy** (Criteri di accesso), selezionare **Connections through Citrix Gateway** (Connessioni tramite Citrix Gateway).
  4. Per scegliere un sottoinsieme di tali connessioni, selezionare **Connections meeting any of the following filters** (Connessioni che soddisfano uno dei seguenti filtri). Definire quindi il sito Citrix Gateway e aggiungere, modificare o rimuovere le espressioni dei criteri SmartAccess per gli scenari di accesso utente consentiti. Per ulteriori informazioni, vedere la documentazione di Citrix Gateway.
  5. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, selezionare **Save** (Salva) per applicare le modifiche e chiudere la finestra.

- **Limitare l'accesso per gli utenti tramite filtri di esclusione:** utilizzare i filtri di esclusione per i criteri di accesso impostati nell'SDK. I criteri di accesso vengono applicati ai gruppi di consegna per affinare le connessioni. Ad esempio, è possibile limitare l'accesso alla macchina a un sottoinsieme di utenti ed è possibile specificare i dispositivi utente consentiti. I filtri di esclusione affinano ulteriormente i criteri di accesso. Ad esempio, per motivi di sicurezza, è possibile negare l'accesso a un sottoinsieme di utenti o dispositivi. Per impostazione predefinita, i filtri di esclusione sono disabilitati.

  Ad esempio, per prevenire l'accesso da un laboratorio didattico su una subnet della rete aziendale a un determinato gruppo di consegna, indipendentemente da chi sta utilizzando le macchine nel laboratorio, utilizzare il comando: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

  È possibile utilizzare il carattere jolly asterisco (*) per far corrispondere tutti i tag che iniziano con la stessa espressione dei criteri. Ad esempio, se si aggiunge il tag `VPDesktops_Direct` a una macchina e `VPDesktops_Test` a un altro, impostando il tag nello script `Set-BrokerAccessPolicy` a `VPDesktops_*` si applica il filtro a entrambe le macchine.

  Se si è connessi tramite un browser Web o con la funzionalità di esperienza utente dell'app Citrix Workspace abilitata nello store, non è possibile utilizzare un filtro di esclusione dei nomi client.

### Impedire agli utenti di connettersi a una macchina (modalità di manutenzione) in un gruppo di consegna

Quando è necessario impedire temporaneamente che vengano effettuate nuove connessioni alle macchine, è possibile attivare la modalità di manutenzione per una o tutte le macchine di un gruppo di consegna. Questa operazione può essere effettuata prima di applicare patch o di utilizzare gli strumenti di gestione.

- Quando una macchina con sistema operativo multisessione è in modalità di manutenzione, gli utenti possono connettersi a sessioni esistenti, ma non possono avviare nuove sessioni.
- Quando una macchina con sistema operativo a sessione singola (o un PC che utilizza Accesso remoto PC) è in modalità di manutenzione, gli utenti non possono connettersi o riconnettersi. Le connessioni correnti permangono finché non si disconnettono o si scollegano.

Per attivare o disattivare la modalità di manutenzione:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo.
3. Per attivare la modalità di manutenzione per tutte la macchine del gruppo di consegna, selezionare **Turn On Maintenance Mode** (Attiva modalità di manutenzione) nella barra delle azioni.

   Per attivare la modalità di manutenzione per una macchina, selezionare **View Machines** (Visualizza macchine) nella barra delle azioni. Selezionare una macchina, quindi selezionare **Turn On Maintenance Mode** (Abilita modalità di manutenzione) nella barra delle azioni.
4. Per disattivare la modalità di manutenzione per una o tutte le macchine di un gruppo di consegna, seguire le istruzioni precedenti, ma selezionare **Turn Off Maintenance Mode** (Disabilita modalità di manutenzione) nella barra delle azioni.

Le impostazioni di Connessione desktop remoto di Windows influiscono anche sul fatto che una macchina con sistema operativo multisessione possa essere o meno in modalità di manutenzione. La modalità di manutenzione è attiva quando si verifica una delle seguenti condizioni:

- La modalità di manutenzione è impostata su attivata, come descritto in precedenza.
- RDC è impostato su **Don't allow connections to this computer** (Non consentire connessioni al computer).
- RDC è impostato su **Don't allow connections to this computer** (Non consentire connessioni a questo computer) e la modalità di accesso utente Configurazione host remoto corrisponde a **Allow reconnections, but prevent new logons** (Consenti riconnessioni, ma impedisci nuovi accessi) o **Allow reconnections, but prevent new logons until the server is restarted** (Consenti riconnessioni, ma impedisci nuovi accessi fino al riavvio del server).

È inoltre possibile attivare o disattivare la modalità manutenzione per:

- Una connessione che influisce sulle macchine che la utilizzano.
- Un catalogo di macchine, che influisce sulle macchine che contiene.

#### Arrestare e riavviare le macchine di un gruppo di consegna

Questa procedura non è supportata per le macchine Remote PC Access (Accesso remoto PC).

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
3. Selezionare la macchina e quindi selezionare una delle seguenti azioni nella barra delle azioni:

   > **Nota:**
   >
   > - Le seguenti azioni sono valide solo per le macchine con gestione dell'alimentazione.
   > - Alcune opzioni potrebbero non essere disponibili, a seconda dello stato della macchina.

   - **Force shut down** (Spegnimento forzato): spegne forzatamente la macchina e aggiorna l'elenco delle macchine.
   - **Restart** (Riavvio): richiede al sistema operativo di arrestare e quindi riavviare la macchina. Se il sistema operativo non è in grado di eseguire la procedura, la macchina rimane nello stato corrente.
   - **Force restart** (Forza riavvio): chiude forzatamente la sessione del sistema operativo e riavvia la macchina.
   - **Suspend** (Sospendi): mette in pausa la macchina senza arrestarla e aggiorna l'elenco delle macchine.
   - **Shut down** (Arresto): richiede l'arresto del sistema operativo.

Per le azioni non forzate, se la macchina non chiude la sessione entro 10 minuti, viene spenta. Se Windows tenta di installare aggiornamenti durante la chiusura, c'è il rischio che la macchina venga spenta prima del completamento degli aggiornamenti.

#### Creare e gestire pianificazioni di riavvio per le macchine di un gruppo di consegna

> **Nota:**
>
> - Quando una pianificazione di riavvio viene applicata a un gruppo di consegna con AutoScale abilitato, le relative macchine vengono semplicemente spente e AutoScale

> provvederà ad accenderle.
> - Quando le pianificazioni di riavvio vengono applicate a macchine a sessione singola casuali, tali macchine vengono spente anziché riavviate, per risparmiare sui costi. Si consiglia di utilizzare AutoScale per accendere le macchine.
> - La modifica del fuso orario su un gruppo di consegna potrebbe provocare il riavvio delle macchine del gruppo. Per evitare ciò, modificare le impostazioni del fuso orario solo al di fuori degli orari di produzione.

Una pianificazione di riavvio specifica quando le macchine di un gruppo di consegna vengono periodicamente riavviate. È possibile creare una o più pianificazioni per un gruppo di consegna. Una pianificazione può influire su:

- Tutte le macchine del gruppo.
- Una o più macchine (ma non tutte) del gruppo. Le macchine sono identificate da un tag applicato alla macchina. Questa operazione è chiamata restrizione tag, perché il tag limita un'azione solo agli elementi che hanno il tag (in questo caso le macchine).

Ad esempio, supponiamo che tutte le macchine si trovino in un unico gruppo di consegna. Si desidera che ogni macchina venga riavviata una volta alla settimana e che le macchine utilizzate dal team di contabilità vengano riavviate quotidianamente. A tale scopo, impostare una pianificazione per tutte le macchine e un'altra pianificazione solo per le macchine del team contabilità.

Una pianificazione include il giorno e l'ora di inizio del riavvio e la relativa durata. La durata è "Start all affected machines at the same time"(Avvia contemporaneamente tutte le macchine interessate) o un intervallo probabilmente necessario per riavviare tutte le macchine interessate.

È possibile attivare o disattivare una pianificazione. La disattivazione di una pianificazione può essere utile durante i test, durante intervalli speciali o durante la preparazione delle pianificazioni prima di averne bisogno.

Non è possibile utilizzare pianificazioni per l'accensione o l'arresto automatico dalla console di gestione, solo per il riavvio.

**Sovrapposizione delle pianificazioni** Più pianificazioni possono sovrapporsi. Nell'esempio precedente, entrambe le pianificazioni influenzano le macchine del team di contabilità. Quelle macchine potrebbero essere riavviate due volte alla domenica. Il codice di pianificazione è progettato per evitare di riavviare la stessa macchina più spesso del previsto, ma non può essere garantito.

- Se le pianificazioni coincidono esattamente con i tempi di inizio e durata, è più probabile che le macchine vengano riavviate una sola volta.
- Più le pianificazioni differiscono nei tempi di inizio e durata, più è probabile che si verifichino più riavvii.

- Il numero di macchine interessate da una pianificazione influisce anche sulla possibilità di sovrapposizione. Nell'esempio, la pianificazione settimanale che interessa tutti i computer potrebbe avviare il riavvio più velocemente della pianificazione giornaliera per le macchine del team di contabilità, a seconda della durata specificata per ciascuna.

Per un'analisi approfondita delle pianificazioni di riavvio, vedere Elementi interni della pianificazione del riavvio.

#### Visualizzare le pianificazioni di riavvio

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Selezionare la pagina **Restart Schedule** (Pianificazione riavvii).

La pagina **Restart Schedule** contiene le seguenti informazioni per ogni pianificazione configurata:

- Nome della pianificazione.
- Eventuale limitazione tag utilizzata.
- Quante volte si verifica il riavvio della macchina.
- Se gli utenti della macchina ricevono una notifica o meno.
- Se la pianificazione è abilitata o meno. La disattivazione di una pianificazione può essere utile durante i test, durante intervalli speciali o durante la preparazione delle pianificazioni prima di averne bisogno.

**Aggiungere (applicare) tag** Quando si configura una pianificazione di riavvio che utilizza una restrizione tag, assicurarsi che il tag sia stato aggiunto (applicato) alle macchine interessate dalla pianificazione. Nell'esempio precedente, ciascuna delle macchine utilizzate dal team di contabilità ha un tag applicato. Per ulteriori informazioni, vedere Tag.

Sebbene sia possibile applicare più tag a una macchina, una pianificazione di riavvio può specificare un solo tag.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare il gruppo contenente le macchine che la programmazione deve controllare.
3. Selezionare **View Machines** (Visualizza macchine), quindi selezionare le macchine a cui si desidera aggiungere un tag.
4. Selezionare **Manage Tags** (Gestisci tag) nella barra delle azioni.
5. Se il tag esiste, attivare la casella di controllo accanto al nome del tag. Se il tag non esiste, selezionare **Create** (Crea) e quindi specificare il nome del tag. Dopo aver creato il tag, attivare la casella di controllo accanto al nome del tag appena creato.
6. Selezionare **Save** (Salva) nella finestra di dialogo **Manage Tags** (Gestisci tag).

**Creare una pianificazione di riavvio**

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Restart Schedule** (Pianificazione riavvio), selezionare **Add** (Aggiungi).
4. Nella pagina **Add Restart Schedule** (Aggiungi pianificazione di riavvio):
    - Per abilitare la pianificazione, selezionare **Yes** (Sì). Per disabilitare la pianificazione, selezionare **No**.
    - Digitare un nome e una descrizione della pianificazione.
    - Per **Restrict to tag** (Limita ai tag), applicare una restrizione per il tag.
    - Per **Include machines in maintenance mode** (Includi macchine in modalità di manutenzione), scegliere se includere in questo programma di riavvio le macchine in modalità di manutenzione. Se invece si desidera utilizzare PowerShell, vedere Riavvii pianificati per le macchine in modalità di manutenzione.
    - Per **Restart frequency** (Frequenza di riavvio), selezionare la frequenza di riavvio: giornaliera, settimanale, mensile o una volta. Se si seleziona **Weekly** (Settimanale) o **Monthly** (Mensile), è possibile specificare uno o più giorni specifici.
    - Per **Repeats every** (Si ripete ogni), specificare la frequenza con cui si desidera eseguire la pianificazione.
    - Per **Start date** (Data di inizio), specificare una data di inizio per la prima occorrenza della pianificazione.
    - Per **Begin restart at** (Inizia il riavvio alle ore) specificare, in formato orologio 24 ore, l'ora della giornata in cui iniziare il riavvio.
    - In **Restart duration** (Durata del riavvio):
        - Se non si desidera utilizzare il riavvio naturale, selezionare **Restart all machines at the same time** (Riavvia tutti i computer contemporaneamente) o **Restart all machines within a time period** (Riavvia tutti i computer entro un periodo di tempo).
        - Se si desidera utilizzare il riavvio naturale, selezionare **Restart all machines after draining all sessions** (Riavviare tutti i computer dopo aver esaurito tutte le sessioni).

          All'avvio di una pianificazione di riavvio configurata per utilizzare il riavvio naturale:

            * Tutti i computer inattivi appartenenti al gruppo di consegna vengono riavviati immediatamente.
            * Ogni macchina appartenente al gruppo di consegna che abbia una o più sessioni attive viene riavviata quando tutte le sessioni vengono scollegate.

> **Nota:**
>
> È possibile utilizzare questa opzione per le macchine con alimentazione gestita e anche per le macchine con alimentazione non gestita.

- In **Send notification to users** (Invia notifica agli utenti), scegliere se visualizzare un messaggio di notifica sulle macchine interessate prima dell'inizio del riavvio. Per impostazione predefinita, non viene visualizzato alcun messaggio.
- Se si sceglie di visualizzare un messaggio 15 minuti prima dell'inizio del riavvio, è possibile scegliere (in **Notification frequency** [Frequenza di notifica]) di ripetere il messaggio ogni cinque minuti dopo il messaggio iniziale. Per impostazione predefinita, il messaggio non si ripete.
- Immettere il titolo e il testo della notifica. Non è presente testo predefinito.

  Se si desidera che il messaggio includa un conto alla rovescia per il riavvio, includere la variabile **%m%**. A meno che non si scelga di riavviare tutte le macchine contemporaneamente, il messaggio viene visualizzato su ogni macchina all'ora appropriata prima del riavvio.

5. Fare clic su **Done** (Fine) per applicare le modifiche e chiudere la finestra **Add Restart Schedule** (Aggiungi pianificazione di riavvio).
6. Fare clic su **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra **Edit Delivery Group** (Modifica gruppo di consegna). In alternativa, fare clic su **Save** (Salva) per applicare le modifiche e chiudere la finestra.

**Eseguire immediatamente un programma di riavvio** Una pianificazione di riavvio specifica quando le macchine di un gruppo di consegna vengono riavviate regolarmente. È inoltre possibile eseguire immediatamente una pianificazione di riavvio per riavviare le macchine in tale pianificazione.

Per eseguire immediatamente un pianificazione di riavvio, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare il gruppo di consegna applicabile, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Restart Schedule** (Riavvia pianificazione), selezionare una pianificazione che si desidera eseguire e quindi selezionare **Run schedule now** (Esegui pianificazione ora).

> **Nota:**
>
> - Non è possibile eseguire immediatamente una pianificazione se è configurata con l'impostazione **Restart all machines after draining sessions** (Riavvia tutte le macchine

> dopo aver svuotato le sessioni).
> - Ora è possibile applicare **Run schedule now** (Esegui pianificazione ora) solo a una sola pianificazione alla volta.
> - Dopo aver modificato una pianificazione, l'opzione **Run schedule now** (Esegui pianificazione ora) non è più disponibile. Selezionare **Apply** (Applica) per renderla disponibile.

#### Modificare, rimuovere, abilitare o disattivare una pianificazione di riavvio

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Restart Schedule** (Pianificazione di riavvio) selezionare la casella di controllo relativa a una pianificazione.

    - Per modificare una pianificazione, selezionare **Edit** (Modifica). Aggiornare la configurazione della pianificazione, utilizzando le linee guida in Creare una pianificazione di riavvio.
    - Per abilitare o disabilitare una pianificazione, selezionare **Edit** (Modifica). Selezionare o deselezionare la casella di controllo **Enable restart schedule** (Abilita pianificazione riavvio).
    - Per rimuovere una pianificazione, selezionare **Remove** (Rimuovi). Confermare la rimozione. La rimozione di una pianificazione non influisce sui tag applicati alle macchine interessate.

#### Riavvii pianificati ritardati a causa di un'interruzione del database

> **Nota:**
>
> Questa funzionalità è disponibile solo in PowerShell.

Se si verifica un'interruzione del database del sito prima dell'inizio di un riavvio pianificato per le macchine (VDA) di un gruppo di consegna, i riavvii iniziano al termine dell'interruzione. Questa azione può avere risultati imprevisti.

Ad esempio, supponiamo di aver programmato il riavvio di un gruppo di consegna durante le ore fuori produzione (a partire dalle 03:00). Un'ora prima dell'inizio del riavvio pianificato (02:00) si verifica un'interruzione del database del sito. L'interruzione dura sei ore (fino alle 8 del mattino). La pianificazione di riavvio inizia quando viene ripristinata la connessione tra il Delivery Controller e il database del sito. Il riavvio del VDA inizia ora cinque ore dopo la pianificazione originale. Questa azione potrebbe comportare il riavvio dei VDA durante le ore di produzione.

Per evitare questa situazione, è possibile utilizzare il parametro `MaxOvertimeStartMins` per i cmdlet `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. Il valore speci-

fica il numero massimo di minuti dopo l'ora di inizio pianificata in cui una pianificazione di riavvio può iniziare.

- Se la connessione al database viene ripristinata entro quell'ora (ora pianificata + `MaxOvertimeStartMins` ), inizia il riavvio del VDA.
- Se la connessione al database non viene ripristinata entro quell'ora, i riavvii del VDA non vengono avviati.
- Se questo parametro viene omesso o ha un valore zero, il riavvio pianificato inizia quando viene ripristinata la connessione al database, indipendentemente dalla durata dell'interruzione.

Per ulteriori informazioni, vedere la Guida del cmdlet. Questa funzionalità è disponibile solo in PowerShell.

**Riavvii programmati per macchine in modalità manutenzione** Per indicare se una pianificazione di riavvio influisce sulle macchine in modalità di manutenzione, utilizzare l'opzione `IgnoreMaintenanceMode` con i cmdlet `BrokerRebootScheduleV2`.

Ad esempio, il cmdlet seguente crea una pianificazione che riavvia sia le macchine in modalità di manutenzione che quelle che non sono in modalità di manutenzione.

```
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

Il cmdlet seguente modifica una pianificazione di riavvio esistente.

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Per ulteriori informazioni, vedere la Guida del cmdlet.

#### Caricare macchine gestite nei gruppi di consegna

È possibile caricare solo le macchine gestite con sistema operativo multisessione.

La gestione del carico misura il carico del server e determina quale server selezionare nelle condizioni ambientali correnti. Questa selezione si basa su:

- **Stato della modalità di manutenzione server:** un sistema operativo multisessione viene preso in considerazione per il bilanciamento del carico solo quando la modalità di manutenzione è disattivata.
- **Indice di carico server:** determina la probabilità di ricevere connessioni di un server che distribuisce macchine con sistema operativo multisessione. L'indice è una combinazione di strumenti di valutazione del carico: il numero di sessioni e le impostazioni per le metriche delle

prestazioni come CPU, disco e utilizzo della memoria. Gli strumenti di valutazione del carico sono specificati nelle impostazioni dei criteri di gestione del carico.

Un indice di caricamento server pari a 10000 indica che il server è completamente caricato. Se non sono disponibili altri server, gli utenti potrebbero ricevere un messaggio che indica che il desktop o l'applicazione non è disponibile quando avviano una sessione.

È possibile monitorare l'indice di carico in Director (Monitor), in una ricerca dell'interfaccia di gestione Full Configuration (Configurazione completa) e nell'SDK.

Nelle visualizzazioni della console, per visualizzare la colonna **Server Load Index** (che è nascosta per impostazione predefinita), selezionare una macchina, fare clic con il pulsante destro del mouse su un'intestazione di colonna e quindi selezionare **Select Column**. Nella **categoria Machine**, selezionare **Load Index**.

Nell'SDK utilizzare il cmdlet `Get-BrokerMachine`. Per ulteriori informazioni, vedere CTX202150.

- **Concurrent logon tolerance policy setting** (Impostazione dei criteri di tolleranza di accesso simultaneo): il numero massimo di richieste simultanee di accesso al server. (questa impostazione equivale alla limitazione del carico nelle versioni XenApp 6.x).

  Quando l'impostazione di tolleranza di accesso simultaneo di tutti i server è pari o superiore all'impostazione, la richiesta di accesso successiva viene assegnata al server con meno accessi in sospeso. Se questi criteri sono soddisfatti da più di un server, viene selezionato il server con l'indice di carico più basso.

#### Gestire la scalabilità automatica

Per impostazione predefinita, la scalabilità automatica è disabilitata per i gruppi di consegna. Per gestire la scalabilità automatica per un gruppo di consegna (se applicabile), effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Manage Autoscale** (Gestisci scalabilità automatica) nella barra delle azioni. Viene visualizzata la finestra **Manage Autoscale** (Gestisci scalabilità automatica).
3. Configurare le impostazioni in base alle esigenze. Per informazioni sulle impostazioni di scalabilità automatica, consultare Scalabilità automatica.
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra. In alternativa, selezionare **Save** (Salva) per applicare le modifiche e chiudere la finestra.

## Sessioni

- Scollegare o disconnettere una sessione o inviare un messaggio agli utenti
- Configurare il pre-lancio e la persistenza della sessione
- Configurare il roaming di sessione
- Controllare la riconnessione della sessione quando è disconnessa dalla macchina in modalità di manutenzione

### Scollegare o disconnettere una sessione o inviare un messaggio agli utenti del gruppo di consegna

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
3. Per disconnettere un utente da una sessione, selezionare la sessione o il desktop, quindi selezionare **Log off** (Disconnetti) nella barra delle azioni. La sessione si chiude e la macchina diventa disponibile per altri utenti, a meno che non sia allocata a un utente specifico.
4. Per disconnettere una sessione, selezionare la sessione o il desktop, quindi selezionare **Disconnect** (Disconnetti) nella barra delle azioni. Le applicazioni continuano a essere eseguite e la macchina rimane allocata a quell'utente. L'utente può riconnettersi alla stessa macchina.
5. Per inviare un messaggio agli utenti, selezionare la sessione, la macchina o l'utente, quindi selezionare **Send message** (Invia messaggio) nella barra delle azioni. Inserire il messaggio.

### Configurare il pre-avvio della sessione e la permanenza della sessione in un gruppo di consegna

Queste funzionalità sono supportate solo su sistemi operativi multisessione.

Le funzionalità di pre-avvio della sessione e di persistenza della sessione consentono a utenti specifici di accedere rapidamente alle applicazioni, come segue:

- Avviando le sessioni prima che vengano richieste (pre-avvio della sessione)
- Mantenendo attive le sessioni dell'applicazione dopo che un utente ha chiuso tutte le applicazioni (persistenza della sessione)

Per impostazione predefinita, il pre-avvio della sessione e la permanenza della sessione non vengono utilizzati. Una sessione viene avviata (viene lanciata) quando un utente avvia un'applicazione e rimane attiva fino alla chiusura dell'ultima applicazione aperta nella sessione.

Considerazioni:

- Il gruppo di consegna deve supportare le applicazioni e le macchine devono eseguire un VDA per il sistema operativo multisessione, versione minima 7.6.
- Queste funzionalità sono supportate solo quando si utilizza l'app Citrix Workspace per Windows e richiedono anche una configurazione aggiuntiva dell'app Citrix Workspace. Per istruzioni, cercare il pre-avvio della sessione nella documentazione del prodotto per la propria versione dell'app Citrix Workspace per Windows.
- L'app Citrix Workspace per HTML5 non è supportata.
- Quando si utilizza il pre-avvio della sessione, se la macchina di un utente viene messa in modalità di sospensione o ibernazione, il pre-avvio non funziona (indipendentemente dalle impostazioni di pre-avvio della sessione). Gli utenti possono bloccare le loro macchine/sessioni. Tuttavia, se un utente si disconnette dall'app Citrix Workspace, la sessione viene terminata e il pre-avvio non è più applicabile.
- Quando si utilizza il pre-avvio della sessione, le macchine client fisiche non possono utilizzare le funzioni di gestione dell'alimentazione di sospensione o ibernazione. Gli utenti di macchine client possono bloccare le proprie sessioni, ma non devono scollegarsi.
- Il pre-avvio e la permanenza delle sessioni consumano una licenza per utilizzo simultaneo, ma solo quando sono connesse. Se si utilizza una licenza utente/dispositivo, la licenza dura 90 giorni. Le sessioni pre-avviate e in periodo di permanenza inutilizzate si disconnettono dopo 15 minuti per impostazione predefinita. Questo valore può essere configurato in PowerShell (cmdlet `New`/`Set-BrokerSessionPreLaunch`).
- Un'attenta pianificazione e il monitoraggio dei modelli di attività degli utenti sono essenziali per personalizzare queste funzionalità in modo che si completino. La configurazione ottimale trova un equilibrio fra i vantaggi della disponibilità delle applicazioni precedenti per gli utenti e il costo di mantenimento delle licenze in uso e dell'allocazione delle risorse.
- È inoltre possibile configurare il pre-avvio della sessione per un'ora pianificata nell'app Citrix Workspace.

**Per quanto tempo rimangono attive le sessioni pre-avviate e in periodo di permanenza se sono inutilizzate** Esistono diversi modi per specificare per quanto tempo una sessione inutilizzata debba rimanere attiva se l'utente non avvia un'applicazione: un timeout configurato e le soglie di caricamento del server. È possibile configurarli tutti. L'evento che si verifica prima causa la fine della sessione inutilizzata.

- **Timeout:** un timeout configurato specifica il numero di minuti, ore o giorni in cui una sessione pre-avviata o in periodo di permanenza inutilizzata rimane attiva. Se si configura un timeout troppo breve, le sessioni pre-avviate terminano prima che diano all'utente il vantaggio di un accesso più rapido alle applicazioni. Se si configura un timeout troppo lungo, potrebbero essere negate connessioni utente in ingresso perché il server non dispone di risorse sufficienti.

  È possibile abilitare questo timeout solo dall'SDK (cmdlet `New`/`Set-BrokerSessionPreLaunch`

), non dalla console di gestione. Se si disattiva il timeout, questo non viene visualizzato nella visualizzazione della console per tale gruppo di consegna né nelle pagine **Edit Delivery Group** (Modifica gruppo di consegna).

- **Soglie:** la fine automatica delle sessioni pre-avviate e in periodo di permanenza in base al carico del server garantisce che le sessioni rimangano aperte il più a lungo possibile, supponendo che siano disponibili risorse server. Le sessioni pre-avviate e in periodo di permanenza inutilizzate non causano rifiuti delle connessioni, perché vengono terminate automaticamente quando sono necessarie risorse per nuove sessioni utente.

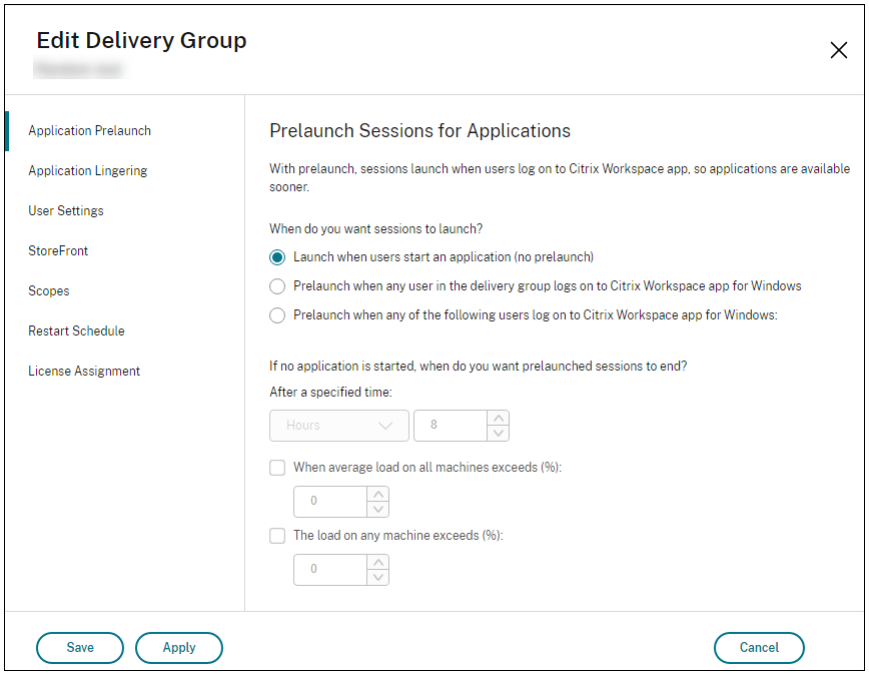
  È possibile configurare due soglie: il carico percentuale medio di tutti i server del gruppo di consegna e il carico percentuale massimo di un singolo server del gruppo. Quando viene superata una soglia, vengono terminate le sessioni che sono in stato di pre-avvio o di permanenza da più tempo. Le sessioni vengono terminate una per una a intervalli di un minuto fino a quando il carico scende al di sotto della soglia. Quando la soglia è stata superata, non vengono avviate nuove sessioni di pre-avvio.

I server con VDA non registrati con un controller e i server in modalità di manutenzione sono considerati a pieno carico. Un'interruzione non pianificata causa il completamento automatico delle sessioni in pre-avvio e in periodo di permanenza per liberare capacità.

**Per abilitare il pre-avvio della sessione**

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Application Prelaunch** (Pre-avvio applicazioni), abilitare il pre-avvio della sessione scegliendo quando si avviano le sessioni:
   - Quando un utente avvia un'applicazione. Questa è l'impostazione predefinita. Il pre-avvio della sessione è disabilitato.
   - Quando qualsiasi utente del gruppo di consegna accede all'app Citrix Workspace per Windows.
   - Quando chiunque in un elenco di utenti e gruppi di utenti accede all'app Citrix Workspace per Windows. Assicurarsi di specificare anche utenti o gruppi di utenti se si sceglie questa opzione.




4. Una sessione pre-avviata viene sostituita con una sessione normale quando l'utente avvia un' applicazione. Se l'utente non avvia un'applicazione (la sessione pre-avviata non è utilizzata), le impostazioni seguenti influiscono sul tempo in cui la sessione rimane attiva.

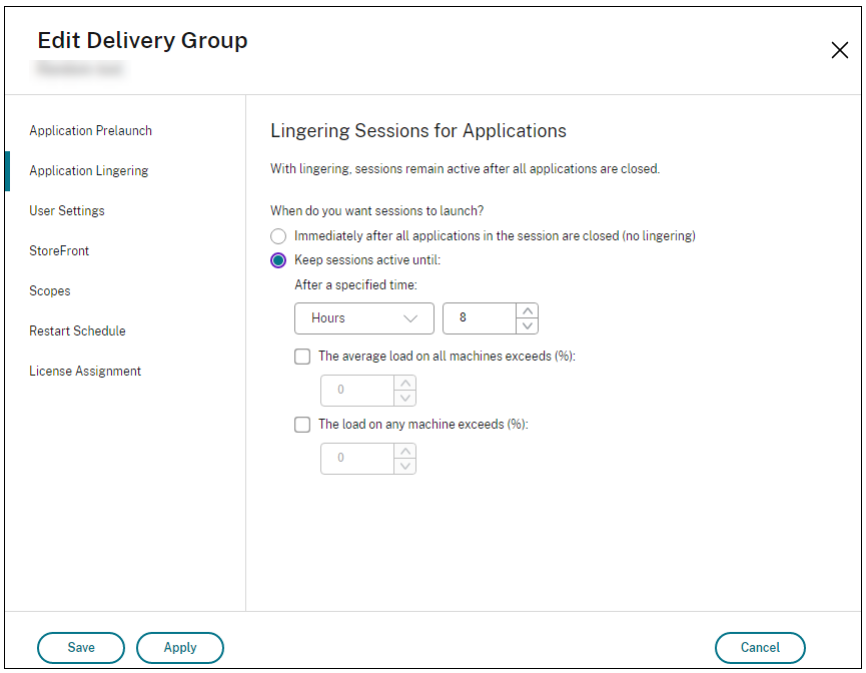
    - Al termine di un intervallo di tempo specificato. È possibile modificare l'intervallo di tempo (1-99 giorni, 1-2376 ore o 1-142.560 minuti).
    - Quando il carico medio di tutte le macchine del gruppo di consegna supera una percentuale specificata (1-99%).
    - Quando il carico di qualsiasi macchina del gruppo di consegna supera una percentuale specificata (1-99%).

    Riepilogo: una sessione pre-avviata rimane attiva fino a quando non si verifica uno dei seguenti eventi: un utente avvia un'applicazione, il tempo specificato è trascorso o viene superata una soglia di carico specificata.

**Per attivare la permanenza della sessione**

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit** (Modifica) nella barra delle azioni.
3. Nella pagina **Application Lingering** (Permanenza applicazione), attivare la permanenza della sessione selezionando **Keep sessions active until** (Mantieni sessioni attive fino a).




4. Diverse impostazioni influiscono sul tempo in cui una sessione persistente rimane attiva se l'utente non avvia un'altra applicazione.

   - Al termine di un intervallo di tempo specificato. È possibile modificare l'intervallo di tempo: 1-99 giorni, 1-2376 ore o 1-142.560 minuti.
   - Quando il carico medio su tutte le macchine del gruppo di consegna supera una percentuale specificata: 1- 99%.
   - Quando il carico di qualsiasi macchina del gruppo di consegna supera una percentuale specificata: 1-99%.

   Riepilogo: una sessione in periodo di persistenza rimane attiva fino a quando non si verifica uno dei seguenti eventi: un utente avvia un'applicazione, il tempo specificato è trascorso o viene superata una soglia di carico specificata.

### Configurare il roaming di sessione

Per impostazione predefinita, il roaming delle sessioni è abilitato per i gruppi di consegna. Le sessioni sono in roaming fra i dispositivi client con l'utente. Quando l'utente avvia una sessione e si sposta su un altro dispositivo, viene utilizzata la stessa sessione e le applicazioni sono disponibili simultaneamente su entrambi i dispositivi. È possibile visualizzare le applicazioni su più dispositivi. Seguono le applicazioni, indipendentemente dal dispositivo o dall'esistenza di sessioni correnti. Spesso seguono anche stampanti e altre risorse assegnate all'applicazione. In alternativa, è anche possibile usare PowerShell. Per ulteriori informazioni, vedere Roaming di sessione.

**Configurare il roaming di sessione per le applicazioni** Per configurare il roaming di sessione per le applicazioni, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
3. Nella pagina **Users** (Utenti), abilitare il roaming delle sessioni selezionando la casella di controllo **Sessions roam with users as they move between devices** (Sessioni in roaming con gli utenti mentre si spostano da un dispositivo all'altro).
    - Quando è abilitato, se un utente avvia una sessione di un'applicazione e si sposta su un altro dispositivo, la stessa sessione è in esecuzione e disponibile su entrambi i dispositivi. Quando è disabilitato, la sessione non è più accessibile da dispositivi diversi.
4. Selezionare **OK** per applicare le modifiche e chiudere la finestra.

**Configurare il roaming di sessione per i desktop** Per configurare il roaming di sessione per un desktop, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.
2. Selezionare un gruppo, quindi selezionare **Edit Delivery Group** (Modifica gruppo di consegna) nella barra delle azioni.
3. Nella pagina **Desktops** (Desktop) selezionare il desktop e selezionare **Modifica**.
4. Abilitare il roaming della sessione selezionando la casella di controllo **Session roaming** (Roaming della sessione).
    - Quando è abilitato, se un utente avvia il desktop e si sposta su un altro dispositivo, la stessa sessione è in esecuzione e le applicazioni sono disponibili su entrambi i dispositivi. Quando è disabilitato, la sessione non è più accessibile da dispositivi diversi.
5. Selezionare **OK** per applicare le modifiche e chiudere la finestra.

### Controllare la riconnessione della sessione quando è disconnessa dalla macchina in modalità di manutenzione

> **Nota:**
>
> Questa funzionalità è disponibile solo in PowerShell.

È possibile controllare se le sessioni disconnesse su macchine in modalità di manutenzione possono riconnettersi alle macchine nel gruppo di consegna.

Prima della fine di maggio 2021, la riconnessione non era consentita per le sessioni desktop a sessione singola in pool che si erano disconnesse dalle macchine in modalità di manutenzione. Ora è possibile configurare un gruppo di consegna per consentire o vietare le riconnessioni (indipendentemente dal tipo di sessione) dopo la disconnessione da una macchina in modalità di manutenzione.

Durante la creazione o la modifica di un gruppo di consegna (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), utilizzare il parametro `-AllowReconnectInMaintenanceMode <boolean>` per consentire o vietare le riconconnessioni per le macchine scollegate da una macchina in modalità di manutenzione.

- Se è impostato su true, le sessioni possono riconnettersi alle macchine del gruppo.
- Se è impostato su false, le sessioni non possono riconnettersi alle macchine del gruppo.

Valori predefiniti:

- Sessione singola: Disabled (Disattivato)
- Multisessione: Enabled (Abilitato)

### Risoluzione dei problemi

- I VDA che non sono registrati con un Delivery Controller non vengono presi in considerazione quando si avviano sessioni mediate. Ciò si traduce in un sottoutilizzo di risorse altrimenti disponibili. Esistono vari motivi per cui un VDA potrebbe non essere registrato, molti dei quali sono risolvibili da un amministratore. La visualizzazione dei dettagli fornisce informazioni sulla risoluzione dei problemi nella creazione guidata del catalogo e dopo aver aggiunto un catalogo a un gruppo di consegna.

  Dopo aver creato un gruppo di consegna, il relativo riquadro dei dettagli indica il numero di macchine che si prevede siano registrate, ma non lo sono. Ad esempio, una o più macchine sono accese e non in modalità manutenzione, ma non sono attualmente registrate presso un Controller. Quando si visualizza una macchina non registrata che dovrebbe esserlo, vedere la scheda **Troubleshoot** (Risoluzione dei problemi) nel riquadro dei dettagli per individuare le possibili cause e leggere le azioni correttive consigliate.

  Per i messaggi sul livello di funzionalità, vedere Versioni e livelli funzionali di VDA.

  Per informazioni sulla risoluzione dei problemi relativi alla registrazione di VDA, vedere CTX136668.

- Nella visualizzazione di un gruppo di consegna, la **versione VDA installata** nel riquadro dei dettagli potrebbe differire dalla versione effettiva installata sulle macchine. La visualizzazione Programmi e funzionalità di Windows della macchina mostra la versione VDA effettiva.

- Per le macchine con **stato di alimentazione sconosciuto**, vedere CTX131267 per informazioni.

# Creare gruppi di applicazioni

August 17, 2023

## Introduzione

I gruppi di applicazioni consentono di gestire raccolte di applicazioni. È possibile creare gruppi di applicazioni per applicazioni condivise tra gruppi di consegna diversi o utilizzate da un sottoinsieme di utenti all'interno di gruppi di consegna. I gruppi di applicazioni sono facoltativi. Offrono un'alternativa all'aggiunta delle stesse applicazioni a più gruppi di consegna. I gruppi di consegna possono essere associati a più di un gruppo di applicazioni e un gruppo di applicazioni può essere associato a più di un gruppo di consegna.

L'uso di gruppi di applicazioni offre vantaggi in termini di gestione delle applicazioni e di controllo delle risorse rispetto all'uso di più gruppi di consegna.

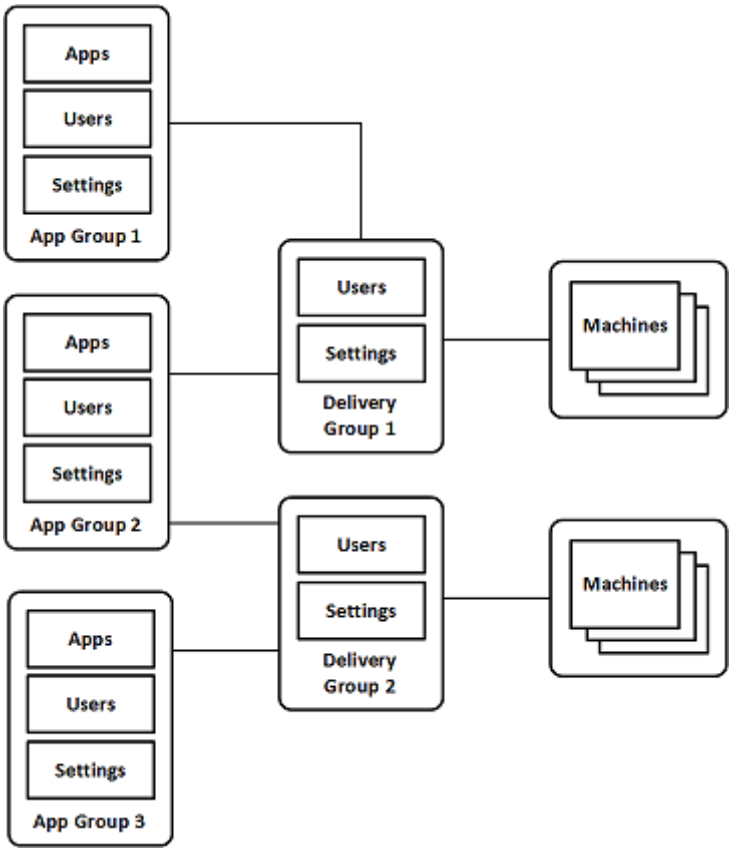
- Il raggruppamento logico delle applicazioni e le relative impostazioni consente di gestire tali applicazioni come un'unica unità. Ad esempio, non è necessario aggiungere (pubblicare) la stessa applicazione nei singoli gruppi di consegna uno alla volta.
- La condivisione della sessione tra gruppi di applicazioni consente di ridurre il consumo di risorse. In altri casi, può essere utile disabilitare la condivisione della sessione tra gruppi di applicazioni.
- È possibile utilizzare la funzione di restrizione tag per pubblicare applicazioni tratte da un gruppo di applicazioni, considerando solo un sottoinsieme di macchine in gruppi di consegna selezionati. Con le restrizioni tag, è possibile utilizzare le macchine esistenti per più di un'attività di pubblicazione, risparmiando i costi associati alla distribuzione e alla gestione di macchine aggiuntive. Una restrizione tag può essere spiegata come una suddivisione (o la creazione di partizioni) delle macchine che fanno parte di un gruppo di consegna. L'utilizzo di un gruppo di applicazioni o di desktop con una restrizione tag può essere utile per isolare e risolvere i problemi di un sottoinsieme di macchine in un gruppo di consegna.

## Configurazioni di esempio

### Esempio 1

L'immagine seguente mostra una distribuzione che include gruppi di applicazioni:




In questa configurazione, le applicazioni vengono aggiunte ai gruppi di applicazioni, non ai gruppi di consegna. I gruppi di consegna specificano quali macchine vengono utilizzate (anche se è visibile, le macchine sono in cataloghi di macchine).

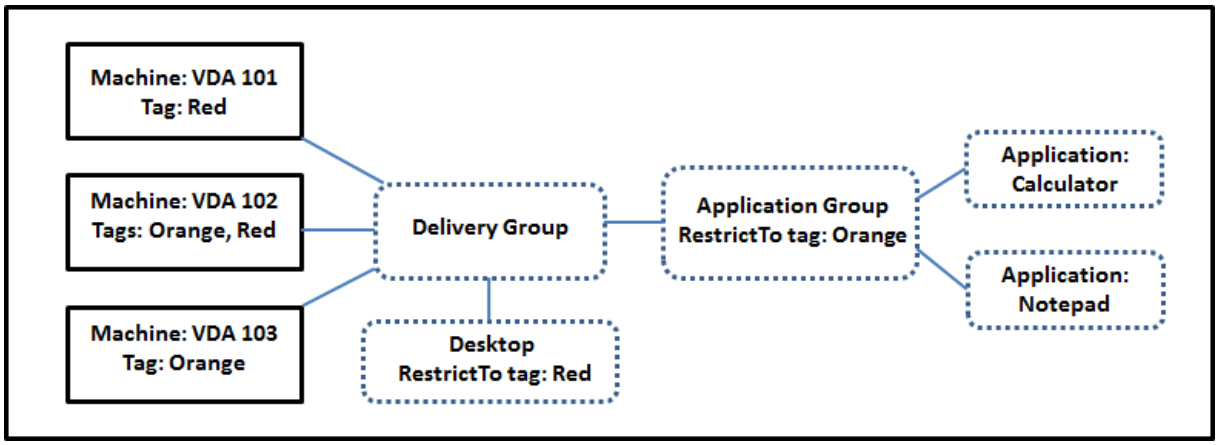
Il gruppo di applicazioni 1 è associato al gruppo di consegna 1. Gli utenti specificati nel gruppo di applicazioni 1 possono accedere alle applicazioni del gruppo di applicazioni 1, purché siano presenti anche nell'elenco di utenti per il gruppo di consegna 1. Questo approccio segue le indicazioni secondo cui l'elenco di utenti di un gruppo di applicazioni è un sottoinsieme (una restrizione) degli elenchi di utenti dei gruppi di consegna associati. Le impostazioni del gruppo di applicazioni 1 (ad esempio la condivisione della sessione dell'applicazione tra gruppi di applicazioni, i gruppi di consegna associati) si applicano alle applicazioni e agli utenti di tale gruppo. Le impostazioni del gruppo di consegna 1 (come il supporto degli utenti anonimi) si applicano agli utenti dei gruppi di applicazioni 1 e 2, poiché tali gruppi di applicazioni sono stati associati a tale gruppo di consegna.

Il gruppo di applicazioni 2 è associato a due gruppi di consegna: 1 e 2. A ciascuno di questi gruppi di consegna può essere assegnata una priorità nel gruppo di applicazioni 2, che indica l'ordine in cui i gruppi di consegna verranno controllati all'avvio di un'applicazione. Per i gruppi di consegna con priorità uguale si applica il bilanciamento del carico. Gli utenti specificati nel gruppo di applicazioni 2 possono accedere alle applicazioni del gruppo di applicazioni 2, purché siano presenti anche negli elenchi di utenti per il gruppo di consegna 1 e il gruppo di consegna 2.

**Esempio 2**

Questo semplice layout utilizza restrizioni tag per limitare quali macchine vengono considerate per determinati lanci di desktop e applicazioni. Il sito dispone di un gruppo di consegna condiviso, un desktop pubblicato e un gruppo di applicazioni configurato con due applicazioni.




Sono stati aggiunti tag a ciascuna delle tre macchine (VDA 101-103).

Il gruppo di applicazioni è stato creato con la restrizione dei tag "arancione", quindi ciascuna delle sue applicazioni (Calcolatrice e Blocco note) può essere avviata solo sulle macchine di quel gruppo di consegna che hanno il tag "arancione": VDA 102 e 103.

Per esempi e indicazioni più completi sull'utilizzo delle restrizioni tag nei gruppi di applicazioni (e per i desktop), vedere Tag.

## Guida e considerazioni

Citrix consiglia di aggiungere le applicazioni a gruppi di applicazioni o a gruppi di consegna, ma non a entrambi. In caso contrario, la complessità aggiuntiva di avere applicazioni in due tipi di gruppo può rendere più difficile la gestione.

Per impostazione predefinita, un gruppo di applicazioni è abilitato. Dopo aver creato un gruppo di applicazioni, è possibile modificare il gruppo per cambiare questa impostazione. Vedere Gestire i gruppi di applicazioni.

Per impostazione predefinita, la condivisione della sessione dell'applicazione tra gruppi di applicazioni è abilitata. Vedere Condivisione della sessione tra gruppi di applicazioni.

Citrix consiglia di aggiornare i gruppi di consegna alla versione corrente. Ciò richiede:

1. L'aggiornamento dei VDA sulle macchine utilizzate nel gruppo di consegna.
2. Passare a un livello di funzionalità superiore per i cataloghi di macchine contenenti quelle macchine

3. Passare a un livello di funzionalità superiore per il gruppo di consegna.

Per ulteriori informazioni, vedere Gestire i gruppi di consegna.

Per utilizzare i gruppi di applicazioni, la versione minima dei componenti principali è la 7.9.

La creazione di gruppi di applicazioni richiede l'autorizzazione di amministrazione delegata del ruolo predefinito di Amministratore gruppo di consegna. Per ulteriori informazioni, vedere Amministrazione delegata.

Questo articolo si riferisce all'"associazione"di un'applicazione a più gruppi di applicazioni per differenziare tale azione dall'aggiunta di una nuova istanza dell'applicazione da un'origine disponibile. Analogamente, i gruppi di consegna sono associati ai gruppi di applicazioni (e viceversa), anziché essere aggiunte o componenti l'uno dell'altro.

## Condividere la sessione con gruppi di applicazioni

Quando la condivisione della sessione dell'applicazione è abilitata, tutte le applicazioni vengono avviate nella stessa sessione dell'applicazione. Ciò consente di risparmiare i costi associati all'avvio di più sessioni dell'applicazione e consente l'utilizzo di funzionalità dell'applicazione che comportano l'uso degli Appunti, ad esempio le operazioni di copia e incolla. Tuttavia, in alcune situazioni si potrebbe voler disattivare la condivisione della sessione.

Quando si utilizzano i gruppi di applicazioni, è possibile configurare la condivisione della sessione dell'applicazione nei tre modi seguenti che estendono il comportamento standard di condivisione della sessione che è disponibile quando si utilizzano solo gruppi di consegna:

- Condivisione della sessione abilitata tra gruppi di applicazioni.
- Condivisione della sessione abilitata solo tra applicazioni nello stesso gruppo di applicazioni.
- Condivisione della sessione disabilitata.

### Condivisione della sessione tra gruppi di applicazioni

È possibile abilitare la condivisione della sessione dell'applicazione tra gruppi di applicazioni oppure disabilitarla per limitare la condivisione della sessione dell'applicazione solo alle applicazioni dello stesso gruppo di applicazioni.

- **È utile un esempio di quando si abilita la condivisione della sessione tra gruppi di applicazioni:**

  Il gruppo di applicazioni 1 contiene applicazioni di Microsoft Office quali Word ed Excel. Il gruppo di applicazioni 2 contiene altre applicazioni quali Blocco note e Calcolatrice, ed entrambi i gruppi di applicazioni sono collegati allo stesso gruppo di consegna. Un utente che ha accesso a entrambi i gruppi di applicazioni inizia una sessione di applicazione avviando

Word e quindi avvia Blocco note. Se la sessione esistente dell'utente che esegue Word è adatta all'esecuzione di Blocco note, questo viene avviato all'interno della sessione esistente. Se Blocco note non può essere eseguito dalla sessione esistente, ad esempio se la restrizione tag esclude la macchina su cui è in esecuzione la sessione, viene creata una nuova sessione su una macchine adatta anziché utilizzare la condivisione della sessione.

- **È utile un esempio di quando si disabilita la condivisione della sessione tra gruppi di applicazioni:**

  Si dispone di un insieme di applicazioni che non interagiscono bene con altre applicazioni installate sulle stesse macchine, ad esempio due versioni diverse della stessa suite software o due versioni diverse dello stesso browser Web. Si preferisce non consentire a un utente di avviare entrambe le versioni nella stessa sessione.

  Si crea un gruppo di applicazioni per ogni versione della suite software e si aggiungono le applicazioni di ciascuna versione della suite software al gruppo di applicazioni corrispondente. Se la condivisione di sessioni tra gruppi è disabilitata per ciascuno di questi gruppi di applicazioni, un utente specificato in tali gruppi può eseguire applicazioni della stessa versione nella stessa sessione e può comunque eseguire altre applicazioni contemporaneamente, ma non nella stessa sessione. Se l'utente avvia una delle applicazioni con versioni diverse (che si trovano in un gruppo di applicazioni diverso) o avvia un'applicazione che non è contenuta in un gruppo di applicazioni, l'applicazione viene avviata in una nuova sessione.

Questa funzionalità di condivisione della sessione tra gruppi di applicazioni non è una funzione sandboxing di protezione. Non è infallibile e non può impedire agli utenti di avviare applicazioni nelle loro sessioni tramite altri mezzi (ad esempio tramite Esplora risorse).

Se una macchina ha raggiunto la sua capacità massima, non vengono avviate nuove sessioni su di essa. Le nuove applicazioni vengono avviate nelle sessioni esistenti sulla macchina in base alle esigenze utilizzando la condivisione delle sessioni (a condizione che ciò sia conforme alle restrizioni di condivisione delle sessioni descritte qui).

È possibile rendere solo le sessioni preavviate disponibili ai gruppi di applicazioni nei quali è consentita la condivisione della sessione dell'applicazione. Le sessioni che utilizzano la funzione di permanenza della sessione sono disponibili per tutti i gruppi di applicazioni. Queste funzionalità devono essere abilitate e configurate in ciascuno dei gruppi di consegna associati al gruppo di applicazioni. Non è possibile configurarli nei gruppi di applicazioni.

Per impostazione predefinita, la condivisione della sessione dell'applicazione tra gruppi di applicazioni è abilitata quando si crea un gruppo di applicazioni. Non è possibile modificare questa impostazione quando si crea il gruppo. Dopo aver creato un gruppo di applicazioni, è possibile modificare il gruppo per cambiare questa impostazione. Vedere Gestire i gruppi di applicazioni.

#### Disabilitare la condivisione della sessione all'interno di un gruppo di applicazioni

È possibile impedire la condivisione della sessione tra applicazioni che si trovano nello stesso gruppo di applicazioni.

- **È utile osservare l'esempio di quando si disabilita la condivisione della sessione all'interno dei gruppi di applicazioni:**

  Si desidera che gli utenti accedano a più sessioni a schermo intero simultanee di un'applicazione su monitor separati.

  È possibile creare un gruppo di applicazioni e aggiungervi le applicazioni. Se la condivisione delle sessioni è vietata tra le applicazioni di quel gruppo di applicazioni, quando un utente specificato in tale gruppo avvia un'applicazione e successivamente un'altra, le applicazioni vengono avviate in sessioni separate e l'utente può spostare ciascuna su un monitor separato.

Per impostazione predefinita, la condivisione della sessione delle applicazioni è abilitata quando si crea un gruppo di applicazioni. Non è possibile modificare questa impostazione quando si crea il gruppo. Dopo aver creato un gruppo di applicazioni, è possibile modificare il gruppo per cambiare questa impostazione. Vedere Gestire i gruppi di applicazioni.

### Creare un gruppo di applicazioni

Utilizzare il processo di creazione di un gruppo di applicazioni per creare categorie di applicazioni nell'app Citrix Workspace. Le categorie di applicazioni consentono di gestire raccolte di applicazioni in Citrix Workspace.

Per creare un gruppo di applicazioni:

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Per organizzare i gruppi di applicazioni utilizzando le cartelle, create cartelle nella cartella principale **Application Groups** (Gruppi di applicazioni).
3. Selezionare la cartella in cui si desidera creare il gruppo, quindi fare clic su **Create Application Group** (Crea gruppo di applicazioni). La procedura guidata per la creazione del gruppo viene avviata con una **pagina introduttiva**. È possibile rimuovere la pagina dai lanci futuri di questa procedura guidata.
4. Seguire la procedura guidata per configurare le impostazioni nelle pagine descritte di seguito. Al termine di ogni pagina, selezionare **Next** (Avanti) fino a raggiungere la pagina **Summary** (Riepilogo).

**Passaggio 1. Gruppi di consegna**

La pagina **Delivery Groups** elenca tutti i gruppi di consegna, con il numero di macchine contenuto da ciascuno gruppo.

- L'elenco **Compatible Delivery Groups** (Gruppi di consegna compatibili) contiene i gruppi di consegna che è possibile selezionare. I gruppi di consegna compatibili contengono macchine casuali (non assegnate in modo permanente o statico) con sistema operativo server o desktop.
- L'elenco **Incompatible Delivery Groups** (Gruppi di consegna non compatibili) contiene gruppi di consegna che non è possibile selezionare. Ogni voce contiene la spiegazione del perché non è compatibile, ad esempio perché contiene macchine assegnate staticamente.

Un gruppo di applicazioni può essere associato a gruppi di consegna contenenti macchine condivise (non private) in grado di distribuire applicazioni.

È inoltre possibile selezionare gruppi di consegna contenenti macchine condivise che consegnano solo desktop, se sono soddisfatte entrambe le seguenti condizioni:

- Il gruppo di consegna contiene macchine condivise ed è stato creato con una versione di XenDesktop precedente alla 7.9.
- Si ha l'autorizzazione Edit Delivery Group (Modifica gruppo di consegna).

Il tipo di gruppo di consegna viene automaticamente convertito in "desktop e applicazioni"quando viene eseguito il commit della procedura guidata di creazione del gruppo.

Sebbene sia possibile creare un gruppo di applicazioni a cui non sono associati gruppi di consegna (ad esempio per organizzare le applicazioni o come archiviazione delle applicazioni non attualmente utilizzate), il gruppo di applicazioni non può essere utilizzato per consegnare le applicazioni finché non specifica almeno un gruppo di consegna. Inoltre, non è possibile aggiungere applicazioni al gruppo di applicazioni dal menu di origine **From Start** (Dall'inizio) se non sono specificati gruppi di consegna.

I gruppi di consegna selezionati specificano le macchine che verranno utilizzate per consegnare le applicazioni. Selezionare le caselle di controllo accanto ai gruppi di consegna che si desidera associare al gruppo di applicazioni.

Per aggiungere una restrizione tag, selezionare **Restrict launches to machines with the tag** (Limita gli avvii alle machine con il tag), quindi selezionare il tag dall'elenco a discesa.

**Passaggio 2. Utenti**

Specificare chi può utilizzare le applicazioni nel gruppo di applicazioni. È possibile accettare tutti gli utenti e i gruppi di utenti presenti nei gruppi di consegna selezionati nella pagina precedente oppure selezionare utenti e gruppi di utenti specifici da quei gruppi di consegna. Se si limita l'uso a utenti specificati, solo gli utenti specificati nel gruppo di consegna e nel gruppo di applicazioni possono

accedere alle applicazioni di questo gruppo. In sostanza, l'elenco utenti specificato nel gruppo di applicazioni fornisce un filtro per gli elenchi di utenti dei gruppi di consegna.

L'attivazione o la disabilitazione dell'utilizzo delle applicazioni da parte di utenti non autenticati è disponibile solo nei gruppi di consegna e non nei gruppi di applicazioni.

Per informazioni sulla posizione in cui vengono specificati gli elenchi di utenti in una distribuzione, vedere Dove vengono specificati gli elenchi di utenti.

#### Passaggio 3. Applicazioni

Buono a sapersi:

- Per impostazione predefinita, le nuove applicazioni aggiunte vengono inserite in una cartella denominata **Applications**. È possibile specificare una cartella diversa. Se si tenta di aggiungere un'applicazione e in quella cartella ne esiste già una con lo stesso nome, verrà richiesto di rinominare l'applicazione che si sta aggiungendo. Se si accetta il nome univoco suggerito, l'applicazione viene aggiunta con il nuovo nome. In caso contrario, è necessario rinominarlo prima di poterlo aggiungere. Per ulteriori informazioni, vedere Gestire le cartelle delle applicazioni.
- È possibile modificare le proprietà (impostazioni) di un'applicazione al momento dell'aggiunta o in un secondo momento. Vedere Modificare le proprietà dell'applicazione. Se si pubblicano due applicazioni con lo stesso nome per gli stessi utenti, modificare la proprietà **Application name (for user)** [Nome applicazione (per utente)] nell'interfaccia di gestione Full Configuration (Configurazione completa). In caso contrario, gli utenti vedranno nomi duplicati nell'app Citrix Workspace.
- Quando si aggiunge un'applicazione a più gruppi di applicazioni, può verificarsi un problema di visibilità se non si dispone di autorizzazioni sufficienti a visualizzare l'applicazione in tutti questi gruppi. In questi casi, vedere un amministratore con autorizzazioni di livello superiore o estendere il proprio ambito in modo da includere tutti i gruppi a cui è stata aggiunta l'applicazione.

Selezionare l'elenco a discesa **Add** (Aggiungi) per visualizzare le origini dell'applicazione.

- **Menu From Start:** applicazioni che vengono individuate su una macchina nei gruppi di consegna selezionati. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco delle applicazioni individuate. Selezionare le caselle di controllo delle applicazioni da aggiungere e quindi selezionare **OK**.

  Questa origine non può essere selezionata se è stata selezionata una delle seguenti opzioni:

  - Gruppi di applicazioni a cui non sono associati gruppi di consegna.
  - Gruppi di applicazioni a cui sono associati gruppi di consegna che non contengono macchine.

  - Un gruppo di consegna che non contiene macchine.

- **Manually defined** (Definizione manuale): applicazioni situate nel sito o in un altro punto della rete. Quando si seleziona questa origine, viene avviata una nuova pagina in cui si digita il percorso dell'eseguibile, della directory di lavoro, degli argomenti della riga di comando facoltativi e dei nomi visualizzati per amministratori e utenti. Dopo aver inserito queste informazioni, selezionare **OK**.
- **Existing** (Esistenti): applicazioni precedentemente aggiunte al sito. Quando si seleziona questa origine, viene avviata una nuova pagina con un elenco delle applicazioni individuate. Selezionare le caselle di controllo delle applicazioni da aggiungere e quindi selezionare **OK**. Non è possibile selezionare questa origine se il sito non dispone di applicazioni.
- **App-V**: applicazioni contenute in pacchetti App-V. Quando si seleziona questa origine, viene avviata una nuova pagina in cui si seleziona **App-V server** o **Application Library**. Nella schermata risultante, selezionare le caselle di controllo delle applicazioni da aggiungere e quindi selezionare **OK**. Per ulteriori informazioni, vedere applications.Distribuire e rendere disponibili applicazioni App-V. Questa origine non può essere selezionata (o potrebbe non essere visualizzata) se App-V non è configurato per il sito.

  > **Nota:**
  >
  > Nei VDA versione 2003 e successive, la pubblicazione di pacchetti App-V dagli URL HTTP non è supportata. Non è possibile selezionare tali applicazioni dall'elenco.

Come già osservato, alcune voci del menu a discesa **Add** (Aggiungi) non sono selezionabili se non esiste un'origine valida di quel tipo. Le origini non compatibili non sono elencate (ad esempio, non è possibile aggiungere gruppi di applicazioni ai gruppi di applicazioni, quindi quell'origine non è elencata quando si crea un gruppo di applicazioni).

#### Passaggio 4. Ambiti

Questa pagina viene visualizzata solo se in precedenza è stato creato un ambito personalizzato. Per impostazione predefinita, è selezionato l'ambito **All**. Per ulteriori informazioni, vedere Amministrazione delegata.

#### Passaggio 5. Riepilogo

Immettere un nome per il gruppo di applicazioni. È inoltre possibile (facoltativamente) inserire una descrizione.

Esaminare le informazioni di riepilogo e quindi selezionare **Finish** (Fine).

# Gestire i gruppi di applicazioni

January 31, 2023

## Introduzione

In questo articolo viene descritto come gestire i gruppi di applicazioni creati.

Vedere Applications (Applicazioni) per informazioni sulla gestione delle applicazioni nei gruppi di applicazioni o nei gruppi di consegna, comprese le procedure seguenti:

- Aggiungere o rimuovere applicazioni in un gruppo di applicazioni.
- Modificare le associazioni dei gruppi di applicazioni.

La gestione dei gruppi di applicazioni richiede le autorizzazioni di amministrazione delegate del ruolo predefinito Amministratore gruppo di consegna. Per ulteriori informazioni, vedere Amministrazione delegata.

## Attivare o disattivare un gruppo di applicazioni

Quando un gruppo di applicazioni è abilitato, può consegnare le applicazioni che sono state aggiunte ad esso. La disattivazione di un gruppo di applicazioni disabilita tutte le applicazioni del gruppo. Tuttavia, se tali applicazioni sono associate anche ad altri gruppi di applicazioni abilitati, possono essere recapitate da tali altri gruppi. Allo stesso modo, se l'applicazione è stata aggiunta in modo esplicito ai gruppi di consegna associati al gruppo di applicazioni (oltre a essere stata aggiunta al gruppo di applicazioni), la disattivazione del gruppo di applicazioni non influisce sulle applicazioni che fanno parte di tali gruppi di consegna.

Un gruppo di applicazioni è abilitato quando lo si crea. Non è possibile modificare questa impostazione quando si crea il gruppo.

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Nella pagina **Settings** (Impostazioni), selezionare o deselezionare la casella di controllo **Enable Application Group** (Abilita gruppo di applicazioni).
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure **OK** per applicare le modifiche e chiudere la finestra.

### Attivare o disattivare la condivisione della sessione delle applicazioni tra gruppi di applicazioni

La condivisione della sessione tra gruppi di applicazioni è abilitata quando si crea un gruppo di applicazioni. Non è possibile modificare questa impostazione quando si crea il gruppo. Per ulteriori informazioni, vedere Condivisione della sessione tra gruppi di applicazioni.

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Nella pagina **Settings** selezionare o deselezionare la casella di controllo **Enable application session sharing between Application Groups** (Abilita condivisione della sessione delle applicazioni tra gruppi di applicazioni).
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure **OK** per applicare le modifiche e chiudere la finestra.

### Disabilitare la condivisione della sessione delle applicazioni all'interno di un gruppo di applicazioni

La condivisione della sessione tra applicazioni nello stesso gruppo di applicazioni è abilitata per impostazione predefinita quando si crea un gruppo di applicazioni. Se si disattiva la condivisione della sessione delle applicazioni tra gruppi di applicazioni, la condivisione della sessione tra applicazioni che appartengono allo stesso gruppo di applicazioni rimane abilitata.

È possibile utilizzare PowerShell SDK per configurare gruppi di applicazioni con la condivisione della sessione delle applicazioni disabilitata tra le applicazioni in essi contenute. In alcune circostanze questo può essere auspicabile. Ad esempio, si potrebbe avere necessità che gli utenti avviino le applicazioni non integrate in finestre di applicazione a schermo intero su monitor separati.

Quando si disattiva la condivisione della sessione delle applicazioni all'interno di un gruppo di applicazioni, ciascuna applicazione del gruppo viene avviata in una nuova sessione dell'applicazione. Se è disponibile una sessione disconnessa adatta che esegue la stessa applicazione, questa viene riconnessa. Ad esempio, se si avvia Blocco note e c'è una sessione disconnessa con Blocco note in esecuzione, viene ricollegata tale sessione anziché crearne una nuova. Se sono disponibili più sessioni disconnesse adatte, una delle sessioni viene scelta come quella a cui riconnettersi, in modo casuale ma deterministico. Se la situazione si ripresenta nelle stesse circostanze, viene scelta la stessa sessione, ma in altri casi la sessione non è necessariamente prevedibile.

È possibile utilizzare PowerShell SDK per disattivare la condivisione della sessione dell'applicazione

per tutte le applicazioni di un gruppo di applicazioni esistente oppure per creare un gruppo di applicazioni con la condivisione della sessione delle applicazioni disabilitata.

#### Esempi di cmdlet PowerShell

Per disabilitare la condivisione delle sessioni, utilizzare i cmdlet Broker PowerShell New-BrokerApplicationGroup o Set-BrokerApplicationGroup con il parametro SessionSharingEnabled impostato su False e il parametro SingleAppPerSession impostato su True.

- Ad esempio, per creare un gruppo di applicazioni con la condivisione della sessione delle applicazioni disabilitata per tutte le applicazioni del gruppo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Ad esempio, per disabilitare la condivisione della sessione delle applicazioni tra tutte le applicazioni di un gruppo di applicazioni esistente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

#### Considerazioni

- Per attivare la proprietà `SingleAppPerSession`, è necessario impostare la proprietà `SessionSharingEnabled` su False. Le due proprietà non devono essere abilitate contemporaneamente. Il parametro `SessionSharingEnabled` si riferisce alla condivisione della sessione tra gruppi di applicazioni.
- La condivisione della sessione delle applicazioni funziona solo per le applicazioni che sono associate a gruppi di applicazioni ma non a gruppi di consegna. Tutte le applicazioni associate direttamente a un gruppo di consegna condividono le sessioni per impostazione predefinita.
- Se un'applicazione è assegnata a più gruppi di applicazioni, assicurarsi che non vi siano impostazioni in conflitto tra i gruppi. Ad esempio, se per un gruppo l'opzione è impostata su True e per un altro è impostata su False, il risultato è un comportamento imprevedibile.

### Rinominare un gruppo di applicazioni

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni e quindi selezionare **Rename Application Group** (Rinomina gruppo di applicazioni) nella barra delle azioni.
3. Specificare il nuovo nome univoco e quindi selezionare **OK**.

### Aggiungere, rimuovere o modificare la priorità delle associazioni dei gruppi di consegna con un gruppo di applicazioni

Un gruppo di applicazioni può essere associato a gruppi di consegna contenenti macchine condivise (non private) in grado di distribuire applicazioni.

È inoltre possibile selezionare gruppi di consegna contenenti macchine condivise che consegnano solo desktop, se sono soddisfatte entrambe le seguenti condizioni:

- Il gruppo di consegna contiene macchine condivise ed è stato creato con una versione precedente alla 7.9.
- Si ha l'autorizzazione Edit Delivery Group (Modifica gruppo di consegna).

Il tipo di gruppo di consegna viene automaticamente convertito in "desktop e applicazioni"quando viene eseguito il commit della finestra di dialogo **Edit Application Group** (Modifica gruppo di applicazioni).

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Delivery Groups** (Gruppi di consegna).
4. Per aggiungere gruppi di consegna, selezionare **Add** (Aggiungi). Selezionare le caselle di controllo dei gruppi di consegna disponibili (i gruppi di consegna non compatibili non possono essere selezionati). Al termine delle selezioni, scegliere **OK**.
5. Per rimuovere i gruppi di consegna, selezionare le caselle di controllo dei gruppi da rimuovere e quindi selezionare **Remove** (Rimuovi). Confermare l'eliminazione quando richiesto.
6. Per modificare la priorità dei gruppi di consegna, selezionare la casella di controllo del gruppo di consegna e quindi selezionare **Edit Priority** (Modifica priorità). Immettere la priorità (0 = massima), quindi selezionare **OK**.
7. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure **OK** per applicare le modifiche e chiudere la finestra.

### Aggiungere, modificare o rimuovere una restrizione tag in un gruppo di applicazioni

L'aggiunta, la modifica e la rimozione di restrizioni tag può avere effetti imprevisti su quali macchine vengono considerate per il lancio delle applicazioni. Leggere le considerazioni e le avvertenze in Tag.

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups**

(Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Delivery Groups** (Gruppi di consegna).
4. Per aggiungere una restrizione tag, selezionare **Restrict launches to machines with the tag** (Limita avvii alle macchine con il tag), quindi selezionare il tag dal menu.
5. Per modificare o rimuovere una restrizione tag, selezionare un tag diverso dal menu o rimuovere completamente la restrizione tag deselezionando **Restrict launches to machines with this tag** (Limita avvii alle macchine con questo tag).
6. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure **OK** per applicare le modifiche e chiudere la finestra.

### Aggiungere o rimuovere utenti in un gruppo di applicazioni

Per informazioni dettagliate sugli utenti, vedere Creare gruppi di applicazioni.

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Users**. Indicare se si desidera consentire di utilizzare le applicazioni incluse nel gruppo di applicazioni a tutti gli utenti dei gruppi di consegna associati oppure solo utenti e gruppi specifici. Per aggiungere utenti, selezionare **Add** (Aggiungi) e specificare gli utenti da aggiungere. Per rimuovere utenti, selezionare uno o più utenti, quindi selezionare **Remove** (Rimuovi).
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure **OK** per applicare le modifiche e chiudere la finestra.

### Aggiungere, modificare o rimuovere l'icona di un'applicazione in un gruppo di applicazioni

Per aggiungere, modificare o rimuovere l'icona di un'applicazione, attenersi alla seguente procedura.

1. Nel riquadro di navigazione, selezionare **Applications** (Applicazioni).
2. Nella scheda **All Applications** (Tutte le applicazioni), selezionare un'applicazione e quindi scegliere **Properties** (Proprietà).

Per apportare modifiche a livello di gruppo di applicazioni, passare alla scheda **Application Groups** (Gruppi di applicazioni), selezionare un'applicazione in un gruppo e quindi scegliere **Properties** (Proprietà).

3. Selezionare la pagina **Delivery** (Consegna), quindi selezionare **Change** (Modifica). Viene visualizzata la finestra **Select icon** (Seleziona icona).
4. Nella finestra **Select icon** (Seleziona icona), effettuare una delle seguenti operazioni:
   - Per aggiungere un'icona, selezionare **Add** (Aggiungi), quindi selezionare l'icona.
   - Per rimuovere un'icona, selezionarla e quindi selezionare **Remove** (Rimuovi).
   - Per modificare un'icona, selezionarla per l'applicazione.

   > **Importante:**
   >
   > - Non è possibile aggiungere un'icona di dimensioni superiori a 200 KB.
   > - È possibile aggiungere solo file con estensione .icon.
   > - Non è possibile rimuovere le icone incorporate.
   > - Non è possibile rimuovere l'icona di un'applicazione in uso.

5. Selezionare **OK** per applicare le modifiche e chiudere la finestra.

### Modificare gli ambiti in un gruppo di applicazioni

È possibile modificare un ambito solo se lo si è creato (non è possibile modificare l'ambito All). Per ulteriori informazioni, vedere Amministrazione delegata.

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni nel riquadro centrale, quindi selezionare **Edit Application Group** (Modifica gruppo di applicazioni) nella barra delle azioni.
3. Selezionare la pagina **Scopes** (Ambiti). Selezionare o deselezionare la casella di controllo accanto agli ambiti che si desidera modificare.
4. Selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure **OK** per applicare le modifiche e chiudere la finestra.

### Eliminare un gruppo di applicazioni

Un'applicazione deve essere associata ad almeno un gruppo di consegna o un gruppo di applicazioni. Se dopo l'eliminazione di un gruppo di applicazioni una o più applicazioni non appartengono più a un gruppo, viene visualizzato un avviso che informa che l'eliminazione di tale gruppo rimuove anche tali applicazioni. È quindi possibile confermare o annullare l'eliminazione.

L'eliminazione di un'applicazione non la elimina dall'origine da cui proveniva originariamente. Tuttavia, se si desidera renderla nuovamente disponibile, è necessario aggiungerla di nuovo.

1. Da **Manage > Full Configuration** (Gestione > Configurazione completa), selezionare **Applications** (Applicazioni) nel riquadro di sinistra, quindi selezionare la scheda **Application Groups** (Gruppi di applicazioni).
2. Selezionare un gruppo di applicazioni e quindi selezionare **Delete Group** (Elimina gruppo) nella barra delle azioni.
3. Confermare l'eliminazione quando richiesto.

## Organizzare i gruppi di applicazioni utilizzando le cartelle

È possibile creare cartelle per organizzare i gruppi di applicazioni per un facile accesso.

### Ruoli richiesti

Per impostazione predefinita, è necessario avere uno dei seguenti ruoli predefiniti per creare e gestire cartelle per i gruppi di applicazioni:

- Cloud Administrator (Amministratore cloud)
- Full Administrator (Amministratore completo)
- Application Group Administrator (Amministratore del gruppo di applicazioni)

È possibile delegare le azioni di gestione ad altri utenti creando ruoli personalizzati. Nella tabella seguente sono elencate le autorizzazioni richieste per ogni azione.

| Azione | Autorizzazioni richieste |
|---|---|
| Creare cartelle per gruppi di applicazioni | Create Application Group Folder |
| Eliminare le cartelle dei gruppi di applicazioni | Remove Application Group Folder |
| Spostare le cartelle dei gruppi di applicazioni | Move Application Group Folder |
| Rinominare le cartelle dei gruppi di applicazioni | Edit Application Group Folder |
| Spostare i gruppi di applicazioni nelle cartelle | Edit Application Group Folder, Edit Application Group Properties |

Per ulteriori informazioni, vedere Creare e gestire ruoli.

### Creare e gestire le cartelle

È possibile utilizzare la barra Actions o il menu di scelta rapida per creare e gestire le cartelle dei gruppi di applicazioni. Inoltre, è possibile trascinare un gruppo di applicazioni o una cartella nella posizione desiderata nell'albero delle cartelle.

Buono a sapersi:

- È possibile nidificare le cartelle fino a cinque livelli (esclusa la cartella principale predefinita).
- Una cartella può contenere gruppi di applicazioni e sottocartelle. È possibile eliminare una cartella solo se essa e le relative sottocartelle non contengono gruppi di applicazioni.
- Tutte le risorse presenti in Full Configuration (quali cataloghi di macchine, gruppi di consegna, applicazioni e gruppi di applicazioni) condividono un albero di cartelle nel back-end. Per evitare conflitti di nomi con altre cartelle di risorse durante la ridenominazione o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in alberi di cartelle diversi.

## Accesso remoto al PC

July 28, 2023

> **Nota:**
>
> In questo articolo viene descritto come configurare Remote PC Access (Accesso remoto PC) utilizzando l'interfaccia Full Configuration (Configurazione completa). Se si utilizza l'interfaccia Quick Deploy (Distribuzione rapida), seguire le istruzioni riportate in Remote PC Access (Accesso remoto PC) in Quick Deploy (Distribuzione rapida).

Accesso remoto PC è una funzionalità di Citrix Virtual Apps and Desktops che consente alle organizzazioni di consentire ai dipendenti di accedere facilmente alle risorse aziendali in remoto in modo sicuro. La piattaforma Citrix rende possibile questo accesso sicuro offrendo agli utenti l'accesso ai PC fisici dell'ufficio. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Accesso remoto PC elimina la necessità di introdurre e fornire altri strumenti per il telelavoro. Ad esempio, desktop o applicazioni virtuali e la relativa infrastruttura associata.

Accesso remoto PC utilizza gli stessi componenti Citrix Virtual Apps and Desktops che forniscono desktop e applicazioni virtuali. Di conseguenza, i requisiti e il processo di distribuzione e configurazione di Accesso remoto PC sono gli stessi richiesti per la distribuzione di Citrix Virtual Apps and Desktops per la distribuzione di risorse virtuali. Questa uniformità offre un'esperienza amministrativa coerente e

unificata. Gli utenti ricevono la migliore esperienza utente utilizzando Citrix HDX per offrire la propria sessione PC da ufficio.

La funzionalità è costituita da un catalogo delle macchine di tipo **Remote PC Access** (Accesso remoto PC) che fornisce le seguenti funzionalità:

- Possibilità di aggiungere macchine specificando le OE. Questa capacità facilita l'aggiunta di PC in blocco.
- Possibilità di aggiungere macchine utilizzando file CSV. Questa capacità facilita l'aggiunta di PC in blocco in scenari con limitazioni della struttura dell'unità organizzativa.
- Assegnazione automatica degli utenti in base all'utente che accede al PC Windows dell'ufficio. Supportiamo le assegnazioni di utenti singoli e più utenti. Per impostazione predefinita, Citrix DaaS assegna automaticamente più utenti alla successiva macchina non assegnata. Per limitare l'assegnazione automatica a un singolo utente, accedere a Web Studio, passare a **Full Configuration > Settings** e disattivare l'impostazione **Enable automatic assignment of multiple users for Remote PC Access** (Abilita l'assegnazione automatica di più utenti per l'accesso remoto al PC).

Citrix Virtual Apps and Desktops può gestire più casi d'uso per PC fisici utilizzando altri tipi di cataloghi di macchine. Questi casi d'uso includono:

- PC Linux fisici
- PC fisici in pool (ovvero assegnati in modo casuale, non dedicati)

> **Note:**
>
> Per i dettagli sulle versioni del sistema operativo supportate, vedere i requisiti di sistema per il VDA per il sistema operativo a sessione singola e Linux VDA.
>
> Per le distribuzioni locali, Remote PC Access (Accesso remoto PC) è valido solo per le licenze Advanced o Premium di Citrix DaaS. Le sessioni consumano licenze allo stesso modo delle altre sessioni di Citrix Virtual Desktops. Per Citrix Cloud, Remote PC Access (Accesso remoto PC) è valido per Citrix DaaS e Workspace Premium Plus.

### Considerazioni

Anche se tutte le considerazioni e i requisiti tecnici e che si applicano a Citrix Virtual Apps and Desktops e Citrix DaaS in generale si applicano anche a Remote PC Access (Accesso remoto PC), alcuni potrebbero essere più rilevanti o applicabili esclusivamente al caso di utilizzo fisico del PC.

> **Importante:**
>
> I sistemi fisici Windows 11 (e alcuni che eseguono Windows 10) includono funzionalità di sicurezza basate sulla virtualizzazione che fanno sì che il software VDA li rilevi erroneamente

> come macchine virtuali. Per mitigare questo problema, sono disponibili le seguenti opzioni:
>
> - Utilizzare l'opzione "/physicalmachine"insieme all'opzione "/remotepc"nell'ambito dell' installazione del VDA mediante la riga di comando
> - Se l'opzione sopra indicata non è stata utilizzata, dopo l'installazione del VDA aggiungere il seguente valore di registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
> - Nome: ForceEnableRemotePC
> - Tipo: DWORD
> - Dati: 1

### Considerazioni sulla distribuzione

Durante la pianificazione della distribuzione di Accesso remoto PC, prendere alcune decisioni generali.

- È possibile aggiungere Remote PC Access (Accesso remoto PC) a una distribuzione esistente di Citrix Virtual Apps and Desktops e Citrix DaaS. Prima di scegliere questa opzione, considerare quanto segue:
  - I Delivery Controller o i Cloud Connector correnti sono adeguatamente dimensionati per supportare il carico aggiuntivo associato ai VDA di Accesso remoto PC?
  - I database del sito locali e i server di database sono adeguatamente dimensionati per supportare il carico aggiuntivo associato ai VDA di Accesso remoto PC?
  - I VDA esistenti e i nuovi VDA di Accesso remoto PC supereranno il numero massimo di VDA supportati per sito?
- È necessario distribuire il VDA sui PC dell'ufficio tramite un processo automatizzato. Di seguito sono riportate due opzioni disponibili:
  - Strumenti di distribuzione elettronica del software (ESD) come SCCM: installare i VDA utilizzando SCCM.
  - Script di distribuzione: installare i VDA utilizzando gli script.
- Vedere le Considerazioni sulla sicurezza di Remote PC Access (Accesso remoto PC).

### Considerazioni sul catalogo di macchine

Il tipo di catalogo di macchine richiesto dipende dal caso d'uso:

- Catalogo macchine Accesso remoto PC
  - PC dedicati Windows/Linux

  - PC multiutente dedicati Windows/Linux. Questo caso d'uso si applica ai PC fisici dell'ufficio a cui più utenti possono accedere da remoto in turni diversi.
  - PC Windows/Linux in pool. Questo caso d'uso si applica ai PC fisici a cui possono accedere più utenti casuali, come i laboratori informatici.

Una volta identificato il tipo di catalogo di macchine, considerare quanto segue:

- Una macchina può essere assegnata a un solo catalogo di macchine alla volta.
- Per facilitare l'amministrazione delegata, è consigliabile creare cataloghi di macchine in base alla posizione geografica, al reparto o a qualsiasi altro raggruppamento che faciliti la delega dell'amministrazione di ciascun catalogo agli amministratori appropriati.
- Quando si scelgono le unità organizzative (OU) in cui risiedono gli account macchina, selezionare quelle di livello inferiore per una maggiore granularità. Se tale granularità non è richiesta, è possibile scegliere OU di livello superiore. Ad esempio, nel caso di banca/funzionari/cassieri, selezionare i **Tellers** (Cassieri) per una maggiore granularità. In caso contrario, è possibile selezionare **Officers** (Funzionari) o **Bank** (banca) in base a quanto è richiesto.
- Lo spostamento o l'eliminazione di unità organizzative dopo l'assegnazione a un catalogo di macchine Accesso remoto PC influisce sulle associazioni VDA e causa problemi per le assegnazioni future. Pertanto, assicurarsi di pianificare di conseguenza in modo che gli aggiornamenti delle assegnazioni alle unità organizzative dei cataloghi di macchine siano contabilizzati nel piano di modifica di Active Directory.
- È possibile scegliere le OU per aggiungere macchine al catalogo delle macchine in blocco. In alcuni scenari, non è facile farlo a causa delle restrizioni della struttura dell'unità organizzativa. Invece, è possibile aggiungere macchine in blocco utilizzando file CSV. Questa funzionalità offre una maggiore flessibilità per l'aggiunta di macchine in blocco. È possibile aggiungere solo macchine (da utilizzare con assegnazioni automatiche degli utenti) o aggiungere macchine insieme alle assegnazioni utente.
- La funzione Wake on LAN integrata è disponibile solo con il catalogo di macchine di tipo **Accesso remoto PC**.

### Considerazioni su Linux VDA

Queste considerazioni sono specifiche per Linux VDA:

- La funzionalità Physical monitor blanking for Remote PC Access VDAs (Oscurazione fisica del monitor per i VDA di accesso remoto al PC) è disponibile, ma non per tutte le distribuzioni Linux. Per le distribuzioni Linux non supportate, utilizzare il Linux VDA su macchine fisiche solo in modalità non 3D. A causa delle limitazioni del driver NVIDIA, la schermata locale del PC non può essere oscurata e visualizza le attività della sessione quando è abilitata la modalità HDX 3D. Visualizzare questa schermata è un rischio per la sicurezza.

- Consigliamo di utilizzare cataloghi di macchine del tipo con sistema operativo a sessione singola per le macchine Linux fisiche.

### Requisiti tecnici e considerazioni

Questa sezione contiene i requisiti tecnici e le considerazioni per i PC fisici.

- I seguenti dispositivi non sono supportati:
  - Switch KVM o altri componenti che possono disconnettere una sessione.
  - PC ibridi, inclusi computer portatili e PC All-in-One e NVIDIA Optimus.
  - Macchine a doppio avvio.
- Collegare la tastiera e il mouse direttamente al PC. Il collegamento al monitor o ad altri componenti che possono essere spenti o scollegati può rendere queste periferiche non disponibili. Se è necessario collegare i dispositivi di input a componenti quali monitor, non spegnere tali componenti.
- I PC devono far parte di un dominio di Servizi di dominio Active Directory.
- L'avvio sicuro è supportato solo su Windows 10.
- Il PC deve disporre di una connessione di rete attiva. Una connessione cablata è preferibile per una maggiore affidabilità e larghezza di banda.
- Se si utilizza il Wi-Fi, effettuare le seguenti operazioni:
  1. Impostare l'alimentazione in modo che la scheda di rete wireless sia accesa.
  2. Configurare la scheda di rete wireless e il profilo di rete per consentire la connessione automatica alla rete wireless prima dell'accesso dell'utente. In caso contrario, il VDA non si registra finché l'utente non esegue l'accesso. Il PC non è disponibile per l'accesso remoto fino a quando un utente non ha effettuato l'accesso.
  3. Assicurarsi che i Delivery Controller o i connettori cloud possano essere raggiunti dalla rete Wi-Fi.
- È possibile utilizzare Accesso remoto PC sui computer portatili. Assicurarsi che il computer portatile sia collegato a una fonte di alimentazione anziché funzionare a batteria. Configurare le opzioni di alimentazione del laptop in modo che corrispondano alle opzioni di un PC desktop. Ad esempio:
  1. Disattivare la funzionalità di ibernazione.
  2. Disattivare la funzione di sospensione.
  3. Impostare l'azione di chiusura del coperchio su **Non intervenire**.
  4. Impostare l'azione di pressione del pulsante di accensione su **Arresta sistema**.
  5. Disabilitare le funzioni di risparmio energetico della scheda video e della scheda NIC.

- Accesso remoto PC è supportato sui dispositivi Surface Pro con Windows 10. Seguire le stesse linee guida per i computer portatili citati sopra.
- Se si utilizza una docking station, è possibile disancorare e reinserire i computer portatili. Quando si disancora il computer portatile, il VDA si registra nuovamente nei Delivery Controller o nei connettori cloud tramite Wi-Fi. Tuttavia, quando si reinserisce il computer portatile, il VDA non passa all'uso della connessione cablata a meno che non si disconnetta la scheda wireless. Alcuni dispositivi offrono una funzionalità integrata di disconnessione della scheda wireless dopo che è stata stabilita una connessione cablata. Gli altri dispositivi richiedono soluzioni personalizzate o utilità di terze parti per disconnettere la scheda wireless. Leggere le considerazioni sulle reti Wi-Fi menzionate in precedenza.

  Eseguire le seguenti operazioni per abilitare l'inserimento e il disancoraggio per i dispositivi di Accesso remoto PC:

  1. Nel menu **Start**, selezionare **Impostazioni > Sistema > Alimentazione e sospensione** e impostare **Sospensione** su **Mai**.
  2. In **Gestione periferiche > Schede di rete > Adattatore Ethernet** andare su **Risparmio energia** e deselezionare **Consenti al computer di spegnere il dispositivo per risparmiare energia**. Assicurarsi che l'opzione **Consenti al dispositivo di riattivare il computer** sia selezionata.

- Più utenti con accesso allo stesso PC dell'ufficio vedono la stessa icona in Citrix Workspace. Quando un utente accede a Citrix Workspace, tale risorsa appare come non disponibile se già in uso da parte di un altro utente.
- Installare l'app Citrix Workspace su ciascun dispositivo client (ad esempio, un PC di casa) che accede al PC dell'ufficio.

### Sequenza di configurazione

Questa sezione contiene una panoramica su come configurare Accesso remoto PC quando si utilizza il catalogo di macchine di **Accesso remoto PC**. Per informazioni su come creare altri tipi di cataloghi delle macchine, vedere Creare cataloghi delle macchine.

1. Solo sito locale: per utilizzare la funzionalità di riattivazione LAN integrata, configurare i prerequisiti descritti in Riattivazione LAN.
2. Se è stato creato un nuovo sito Citrix Virtual Apps and Desktops per l'accesso remoto PC:

   a) Selezionare il tipo di sito **Remote PC Access** (Accesso remoto PC).
   b) Nella pagina **Risparmio energia** scegliere di attivare o disattivare la gestione del risparmio energia per il catalogo di macchine Accesso remoto PC predefinito. È possibile modificare

questa impostazione in un secondo momento modificando le proprietà del catalogo macchine. Per informazioni dettagliate sulla configurazione della riattivazione LAN, vedere Riattivazione LAN.

c) Completare le informazioni nelle pagine **Users** e **Machine Accounts**.

Completando questa procedura viene creato un catalogo delle macchine denominato **Remote PC Access Machines** (Macchine di Accesso remoto PC) e un gruppo di consegna denominato **Remote PC Access Desktops** (Desktop di Accesso remoto PC).

3. Se si aggiungono elementi a un sito Citrix Virtual Apps and Desktops esistente:

   a) Creare un catalogo macchine di tipo **Accesso remoto PC** (pagina Operating System della procedura guidata). Per informazioni dettagliate su come creare un catalogo delle macchine, vedere Creare cataloghi delle macchine. Assicurarsi di assegnare l'unità organizzativa corretta in modo che i PC di destinazione siano resi disponibili per l'utilizzo con Accesso remoto PC.

   b) Creare un gruppo di consegna per fornire agli utenti l'accesso ai PC inclusi nel catalogo delle macchine. Per informazioni dettagliate su come creare un gruppo di consegna, vedere Creare gruppi di consegna. Assicurarsi di assegnare il gruppo di consegna a un gruppo di Active Directory che contiene gli utenti che richiedono l'accesso ai propri PC.

4. Distribuire il VDA nei PC dell'ufficio.

   - Si consiglia di utilizzare il programma di installazione VDA core del sistema operativo a sessione singola (`VDAWorkstationCoreSetup.exe`).
   - È inoltre possibile utilizzare il programma di installazione VDA completo per sessione singola (`VDAWorkstationSetup.exe`) con l'opzione `/remotepc /physicalmachine`, che ottiene lo stesso risultato dell'utilizzo del programma di installazione VDA principale.
   - È possibile abilitare Assistenza remota di Windows per consentire ai team dell'help desk di fornire supporto remoto tramite Citrix Director. A tale scopo, utilizzare l'opzione `/enable_remote_assistance`. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.
   - Per poter visualizzare le informazioni sulla durata dell'accesso in Director, è necessario utilizzare il programma di installazione VDA completo per sessione singola e includere il componente **Citrix User Profile Management WMI Plugin**. Includere questo componente utilizzando l'opzione `/includeadditional`. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.
   - Per informazioni sulla distribuzione di VDA utilizzando SCCM, vedere Installare i VDA utilizzando SCCM.
   - Per informazioni sulla distribuzione di VDA tramite script di distribuzione, vedere Installare i VDA utilizzando gli script.

Dopo aver completato i passaggi da 2 a 4, gli utenti vengono assegnati automaticamente ai propri computer quando effettuano l'accesso locale sui PC.

5. Chiedere agli utenti di scaricare e installare l'app Citrix Workspace su ciascun dispositivo client utilizzato per accedere al PC dell'ufficio in remoto. L'app Citrix Workspace è disponibile dal sito di download Citrix o negli store delle applicazioni per i dispositivi mobili supportati.

## Funzionalità gestite tramite il Registro di sistema

> **Attenzione:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

### Modalità sospensione (versione minima 7.16)

Per consentire a un computer Accesso remoto PC di passare a uno stato di sospensione, aggiungere questa impostazione del Registro di sistema sul VDA e quindi riavviare il computer. Dopo il riavvio, vengono rispettate le impostazioni di risparmio energetico del sistema operativo. La macchina entra in modalità di sospensione dopo al termine del periodo di inattività preconfigurato. Dopo che si è svegliata, la macchina si registra nuovamente nel Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Dati: 1

### Gestione delle sessioni

Per impostazione predefinita, la sessione di un utente remoto viene disconnessa automaticamente quando un utente locale avvia una sessione su tale computer (premendo CTRL+ALT+CANC). Per evitare questa azione automatica, aggiungere la seguente voce del Registro di sistema nel PC dell'ufficio e quindi riavviare il computer.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD

- Dati: 1

Per impostazione predefinita, l'utente remoto ha la preferenza rispetto all'utente locale quando il messaggio di connessione non viene riconosciuto entro il periodo di timeout. Per configurare il comportamento, utilizzare questa impostazione:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Dati:
  - 1 - L'utente remoto ha sempre la preferenza se non risponde all'interfaccia utente di messaggistica nel periodo di timeout specificato. Questo comportamento è l'impostazione predefinita se questa impostazione non viene configurata.
  - 2 - L'utente locale ha la preferenza.

Il timeout per l'applicazione della modalità Accesso remoto PC è di 30 secondi per impostazione predefinita. È possibile configurare questo timeout, ma si consiglia di non impostarlo a meno di 30 secondi. Per configurare il timeout, utilizzare questa impostazione del Registro di sistema:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dati: numero di secondi al timeout in valori decimali

Quando un utente desidera ottenere forzatamente l'accesso alla console: l'utente locale può premere Ctrl+Alt+Canc due volte in un intervallo di 10 secondi per ottenere il controllo locale su una sessione remota e forzare un evento di disconnessione.

Dopo la modifica del Registro di sistema e il riavvio del computer, se un utente locale preme Ctrl+Alt+Canc per accedere al PC mentre è utilizzato da un utente remoto, l'utente remoto riceve un messaggio di richiesta. Il messaggio di richiesta chiede se consentire o negare la connessione dell'utente locale. Consentendo la connessione, viene disconnessa la sessione dell'utente remoto.

### Riattivare su LAN

Accesso remoto PC supporta la funzione di riattivazione su LAN, che offre agli utenti la possibilità di accendere i PC fisici da remoto. Questa funzionalità consente agli utenti di mantenere spenti i PC dell'ufficio quando non sono in uso per risparmiare sui costi energetici. Consente inoltre l'accesso remoto quando una macchina è stata spenta inavvertitamente.

Con la funzione di riattivazione su LAN, i Magic Packet vengono inviati direttamente dal VDA in esecuzione sul PC alla sottorete in cui risiede il PC quando viene richiesto dal controller di consegna. Ciò

consente alla funzionalità di agire senza dipendere da componenti aggiuntivi dell'infrastruttura o da soluzioni di terze parti per la distribuzione di Magic Packet.

La funzione di riattivazione su LAN è diversa dalla funzione di riattivazione su LAN basata su SCCM precedente. La funzione di riattivazione su LAN integrata con SCCM è un'opzione alternativa di riattivazione su LAN per l'accesso remoto PC disponibile solo con Citrix Virtual Apps and Desktops locali. Per informazioni sulla riattivazione LAN basata su SCCM, vedere Riattivazione LAN - integrata con SCCM.

#### Requisiti di sistema

Di seguito sono riportati i requisiti di sistema per l'utilizzo della funzione di riattivazione su LAN:

- Piano di controllo:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 o versioni successive
- PC fisici:
  - VDA versione 2009 o successiva
  - Windows 10 o Windows 11. Per i dettagli relativi al supporto, vedere i requisiti di sistema del VDA.
  - Riattivazione su LAN abilitata in BIOS/UEFI
  - Riattivazione su LAN abilitata nelle proprietà della scheda di rete all'interno della configurazione di Windows

#### Configurare la riattivazione su LAN

Per configurare la riattivazione LAN, è possibile utilizzare l'interfaccia di gestione Full Configuration (Configurazione completa) o PowerShell.

**Configurare la riattivazione LAN nell'interfaccia Full Configuration (Configurazione completa)**
Per creare la connessione di Riattivazione LAN:

1. Andare al nodo **Hosting** a sinistra.
2. Selezionare **Add Connection and Resources** (Aggiungi connessione e risorse).
3. Nella pagina **Connection** (Connessione) della procedura guidata, fornire quanto segue:
   a) Tipo di connessione: Riattivazione LAN del PC remoto
   b) Nome della zona: selezionare la zona in cui risiede il catalogo Remote PC Access (Accesso remoto PC)

c) Nome connessione: inserire un nome per la connessione Riattivazione LAN

4. Completare i passaggi rimanenti nella procedura guidata Add Connection and Resources (Aggiungi connessione e risorse).

Per aggiungere la connessione Riattivazione LAN a un catalogo delle macchine Remote PC Access (Accesso remoto PC):

1. Se si sta creando un nuovo catalogo delle macchine Remote PC Access (Accesso remoto PC), è possibile aggiungere la connessione nella pagina **Machine Type** (Tipo di macchina) della procedura guidata di configurazione del catalogo delle macchine utilizzando l'elenco a discesa.
2. Se si desidera aggiungere la connessione Riattivazione LAN a un catalogo delle macchine esistente:

   a) Andare al nodo **Machine Catalogs** (Cataloghi delle macchine) a sinistra.
   b) Selezionare il catalogo delle macchine Remote PC Access (Accesso remoto PC) appropriato.
   c) Fare clic con il pulsante destro del mouse sul catalogo delle macchine o selezionare il menu **More** (Altro) in alto.
   d) Selezionare **Edit Machine Catalog** (Modifica catalogo delle macchine).
   e) Nella pagina **Power Management** (Gestione alimentazione), selezionare **Yes** (Sì).
   f) Selezionare la connessione appropriata dall'elenco a discesa.
   g) Selezionare **Save** (Salva).

> **Nota:**
>
> La configurazione di Riattivazione LAN tramite l'interfaccia Full Configuration (Configurazione completa) è disponibile solo con Citrix DaaS al momento.

**Configurare la riattivazione LAN tramite PowerShell** Per configurare la Riattivazione LAN tramite PowerShell:

1. Creare il catalogo di macchine Accesso remoto PC se non è già disponibile.
2. Creare la connessione host di riattivazione LAN se è già disponibile.
3. Recuperare l'identificatore univoco della connessione host di Riattivazione LAN.
4. Associare la connessione host di riattivazione su LAN a un catalogo di macchine.

Per creare la connessione host di riattivazione su LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

```

```
# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
        $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

Quando la connessione host è pronta, eseguire i seguenti comandi per recuperare l'identificatore univoco della connessione host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Dopo aver recuperato l'identificatore univoco della connessione, eseguire i comandi seguenti per associare la connessione al catalogo del computer Accesso remoto PC:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

#### Considerazioni di progettazione

Quando si prevede di utilizzare la riattivazione su LAN con Accesso remoto PC, considerare quanto segue:

- Più cataloghi di macchine possono utilizzare la stessa connessione host di riattivazione su LAN.
- Perché un PC possa riattivare un altro PC, entrambi i PC devono trovarsi nella stessa sottorete e utilizzare la stessa connessione host di riattivazione su LAN. Non importa se i PC si trovano nello stesso catalogo di macchine o cataloghi diversi.

- Le connessioni host vengono assegnate a zone specifiche. Se la distribuzione contiene più di una zona, è necessaria una connessione host di riattivazione su LAN in ciascuna zona. Lo stesso vale per i cataloghi di macchine.
- I Magic Packet vengono trasmessi utilizzando l'indirizzo di trasmissione globale 255.255.255.255. Assicurarsi che l'indirizzo non sia bloccato.
- Deve essere presente almeno un PC acceso nella sottorete, per ciascuna connessione di riattivazione su LAN, per poter riattivare le macchine in quella sottorete.

#### Considerazioni operative

Di seguito sono riportate considerazioni sull'impiego della funzione di riattivazione su LAN:

- Il VDA deve registrarsi almeno una volta prima che il PC possa essere riattivato utilizzando la funzione di riattivazione su LAN integrata.
- La funzione di riattivazione su LAN può essere utilizzata solo per riattivare i PC. Non supporta altre azioni di alimentazione, ad esempio il riavvio o l'arresto.
- I Magic Packet vengono inviati in uno di due modi:
  1. Quando un utente tenta di avviare una sessione sul proprio PC e il VDA non è registrato
  2. Quando un amministratore invia manualmente un comando di accensione dall'interfaccia Full Configuration (Configurazione completa) o da PowerShell
- Poiché il Delivery Controller non è a conoscenza dello stato di alimentazione di un PC, l'interfaccia Full Configuration (Configurazione completa) visualizza **Not Supported** (Non supportato) nello stato di alimentazione. Il controller di consegna utilizza lo stato di registrazione del VDA per determinare se un PC è acceso o spento.

### Risoluzione dei problemi

#### Lo schermo nero del monitor non funziona

Se il monitor locale del PC Windows non ha lo schermo nero mentre è attiva una sessione HDX (il monitor locale mostra ciò che sta accadendo nella sessione), ciò è probabilmente dovuto a problemi del driver del fornitore della GPU. Per risolvere il problema, assegnare al driver di visualizzazione indiretta Citrix (IDD) una priorità maggiore rispetto al driver del fornitore della scheda grafica impostando il seguente valore del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dati: 3

Per ulteriori informazioni sulle priorità della scheda video e sulla creazione del monitor, vedere l'articolo del Knowledge Center CTX237608.

### La sessione si disconnette quando si seleziona Ctrl+Alt+Canc nel computer in cui è attivata la notifica di gestione della sessione

La notifica di gestione della sessione controllata dal valore del Registro di sistema **SasNotification** funziona solo quando la modalità Accesso remoto PC è attivata sul VDA. Se il PC fisico ha il ruolo di Hyper-V o qualsiasi funzionalità di sicurezza basata sulla virtualizzazione abilitata, il PC si segnala come macchina virtuale. Se il VDA rileva che è in esecuzione su una macchina virtuale, disattiva automaticamente la modalità Accesso remoto PC. Per attivare la modalità Accesso remoto PC, aggiungere il seguente valore del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dati: 1

Riavviare il PC affinché l'impostazione abbia effetto.

### Informazioni diagnostiche

Le informazioni diagnostiche su Accesso remoto PC vengono scritte nel registro eventi applicazioni di Windows. I messaggi informativi non vengono limitati. I messaggi di errore vengono limitati eliminando i messaggi duplicati.

- 3300 (informativo): Macchina aggiunta al catalogo
- 3301 (informativo): Macchina aggiunta al gruppo di consegna
- 3302 (informativo): Macchina assegnata all'utente
- 3303 (errore): Eccezione

### Gestione dell'alimentazione

Se è attivata la gestione dell'alimentazione per Accesso remoto PC, le trasmissioni dirette dalla sottorete potrebbero non riuscire ad avviare i computer che si trovano in una sottorete diversa dal controller. Se è necessaria la gestione dell'alimentazione tra sottoreti che utilizzano trasmissioni dirette da sottoreti e il supporto AMT non è disponibile, provare il proxy di riattivazione o il metodo Unicast. Verificare che tali impostazioni siano abilitate nelle proprietà avanzate per la connessione di gestione dell'alimentazione.

#### La sessione remota attiva registra gli input del touchscreen locale

Quando il VDA abilita la modalità Accesso remoto PC, il computer ignora l'input del touchscreen locale durante una sessione attiva. Se il PC fisico ha il ruolo di Hyper-V o qualsiasi funzionalità di sicurezza basata sulla virtualizzazione abilitata, il PC si segnala come macchina virtuale. Se il VDA rileva che è in esecuzione su una macchina virtuale, disattiva automaticamente la modalità Accesso remoto PC. Per attivare la modalità Accesso remoto PC, aggiungere la seguente impostazione del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dati: 1

Riavviare il PC affinché l'impostazione abbia effetto.

### Altre risorse

Di seguito sono elencate altre risorse per Accesso remoto PC:

- Guida alla progettazione della soluzione: decisioni sulla progettazione di Remote PC Access (Accesso remoto PC).
- Esempi di architetture di Remote PC Access (Accesso remoto PC): architettura di riferimento per la soluzione Citrix Remote PC Access (Accesso remoto PC).

## Rimuovere componenti

February 24, 2023

Per rimuovere componenti installati (come i VDA), Citrix consiglia di utilizzare la funzionalità di Windows per la rimozione o la modifica dei programmi. In alternativa, è possibile rimuovere i componenti utilizzando la riga di comando o uno script.

Quando si rimuovono i componenti, i prerequisiti non vengono rimossi e le impostazioni del firewall non vengono modificate.

Quando si rimuove un VDA, la macchina si riavvia automaticamente dopo la rimozione, per impostazione predefinita.

### Rimuovere i componenti utilizzando la funzionalità di Windows per rimuovere o modificare programmi

Dalla funzionalità di Windows per la rimozione o la modifica di programmi:

- Per rimuovere un VDA, selezionare **Citrix Virtual Delivery Agent** <*versione*>, quindi fare clic con il pulsante destro del mouse e selezionare **Uninstall** (Disinstalla). Il programma di installazione si avvia ed è possibile selezionare i componenti da rimuovere.
- Per rimuovere Universal Print Server, selezionare **Citrix Universal Print Server**, quindi fare clic con il pulsante destro del mouse e selezionare **Uninstall**(Disinstalla).

### Rimuovere un VDA utilizzando la riga di comando

Eseguire il comando utilizzato per installare il VDA: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` o `VDAWorkstationCoreSetup.exe`. Vedere Installare utilizzando la riga di comando per le descrizioni della sintassi.

- Per rimuovere solo il VDA o solo l'app Citrix Workspace, utilizzare le opzioni `/remove` e `/components`.
- Per rimuovere il VDA e l'app Citrix Workspace, utilizzare l'opzione `/removeall`.

Ad esempio, il comando seguente rimuove il VDA e l'app Citrix Workspace da una macchina con sistema operativo multisessione.

```
VDAServerSetup.exe /removeall
```

Ad esempio, il comando seguente rimuove il VDA ma non l'app Citrix Workspace per Windows (se installata) da una macchina con sistema operativo a sessione singola.

```
VDAWorkstationSetup.exe /remove /components vda
```

È inoltre possibile rimuovere un VDA utilizzando uno script fornito da Citrix. Vedere Rimuovere i VDA utilizzando lo script.

## Livello di personalizzazione utente

June 8, 2023

La funzionalità del livello di personalizzazione utente di Citrix Virtual Apps and Desktops estende le funzionalità dei cataloghi di macchine non persistenti per preservare i dati degli utenti e le applicazioni installate localmente in tutte le sessioni. Basata sulla tecnologia sottostante Citrix App Layering, la funzionalità di livello di personalizzazione utente supporta Citrix Provisioning and Machine Creation Services (MCS) in un catalogo di macchine non persistenti.

Installare i componenti del livello di personalizzazione utente insieme al Virtual Delivery Agent all'interno dell'immagine master. Un file VHD memorizza localmente le applicazioni installate dall'utente. Il disco rigido virtuale montato sull'immagine funge da disco rigido virtuale dell'utente.

> **Importante:**
>
> È possibile distribuire livelli di personalizzazione utente in App Citrix Virtual Apps and Desktops o livelli utente App Layering abilitati in un modello di immagine, non in entrambi. Non installare la funzionalità del livello di personalizzazione utente in un livello all'interno di App Layering.

Questa funzionalità sostituisce Personal vDisk (PvD), fornendo allo stesso tempo un'esperienza di lavoro persistente per gli utenti in un ambiente desktop non persistente in pool.

Per distribuire la funzionalità del livello di personalizzazione utente, installarla e configurarla seguendo i passaggi descritti nell'articolo. Fino a quel momento la funzione non è disponibile.

## Supporto delle applicazioni

A parte le seguenti eccezioni, tutte le applicazioni installate da un utente localmente sul desktop sono supportate nel livello di personalizzazione utente.

### Eccezioni

Le seguenti applicazioni fanno eccezione e non sono supportate nel livello di personalizzazione utente:

- Applicazioni aziendali, ad esempio MS Office e Visual Studio.
- Applicazioni che modificano lo stack di rete o l'hardware. Esempio: un client VPN.
- Applicazioni che dispongono di driver a livello di avvio. Esempio: un programma antivirus.
- Applicazioni con driver che utilizzano l'archivio driver. Esempio: un driver di stampante.

  > **Nota:**
  >
  > È possibile rendere disponibili le stampanti utilizzando Oggetti Criteri di gruppo di Windows.

*Non* consentire agli utenti di installare applicazioni non supportate localmente. Piuttosto, installare queste applicazioni direttamente sull'immagine master.

**Applicazioni che richiedono un account utente locale o amministratore**

Quando un utente installa un'applicazione localmente, l'app entra nel livello utente. Se l'utente aggiunge o modifica un utente o un gruppo locale, le modifiche non persistono oltre la sessione.

> **Importante:**
>
> Aggiungere qualsiasi utente o gruppo locale richiesto nell'immagine master.

## Requisiti

La funzionalità del livello di personalizzazione utente richiede i seguenti componenti:

- Citrix Virtual Apps and Desktops 7 1909 o versioni successive
- Virtual Delivery Agent (VDA), versione 1912 o successiva
- Citrix Provisioning, versione 1909 o successiva
- Condivisione file di Windows (SMB) o File di Azure con autenticazione AD locale abilitata

È possibile distribuire la funzionalità di livello di personalizzazione utente nelle seguenti versioni di Windows quando il sistema operativo viene distribuito come singola sessione. Il supporto è limitato a un singolo utente in una singola sessione.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, versione 1607 o successiva
- Windows 10 multisessione (File di Azure supportato)
- Windows Server 2016 (File di Azure supportato)
- Windows Server 2019 (File di Azure supportato)

Per Citrix Virtual Apps and Desktops 7, l'uso di File di Azure con livelli di personalizzazione utente è supportato nei client Windows Server 2019, Windows Server 2016v e Windows 10.

> **Nota:**
>
> se si utilizza un sistema operativo server, è supportato solo Server VDI. Per i dettagli sulla distribuzione, vedere l'articolo VDI del server.
>
> Il livello di personalizzazione utente supporta un solo utente alla volta per macchina e quindi il computer si deve riavviare per reimpostare i dischi. Non è possibile utilizzare il livello di personalizzazione utente con sistemi operativi server multisessione, ma solo con sistemi server a sessione singola. Il livello di personalizzazione utente funziona solo con desktop non persistenti.

Disinstallare la funzionalità del livello di personalizzazione utente, se installata. Riavviare l'immagine master prima di installare l'ultima versione.

## Configurare la condivisione di file

La funzionalità del livello di personalizzazione utente richiede l'archiviazione SMB (Server Message Block) di Windows. Per creare una condivisione file Windows, attenersi alla procedura usuale per il sistema operativo Windows in uso.

Per informazioni dettagliate sull'utilizzo dei File di Azure con cataloghi basati su Azure, consultare Configurare l'archiviazione di File di Azure per i livelli di personalizzazione utente.

## Consigli

Seguire i suggerimenti riportati in questa sezione per una distribuzione corretta del livello di personalizzazione utente.

### Microsoft System Center Configuration Manager (SCCM)

Se si utilizza SCCM con la funzionalità del livello di personalizzazione utente, seguire le linee guida Microsoft per la preparazione dell'immagine in un ambiente VDI. Per ulteriori informazioni, fare riferimento a questo articolo di Microsoft TechNet.

### Dimensione del livello utente

Un livello utente è un disco con thin-provisioning che si espande man mano che viene utilizzato lo spazio sul disco. La dimensione predefinita consentita per un livello utente è 10 GB, il minimo consigliato.

> **Nota:**
>
> Durante l'installazione, se il valore è impostato su zero (0), la dimensione del livello utente predefinita è impostata su 10 GB.

Se si desidera modificare la dimensione del livello utente, è possibile immettere un valore diverso per il criterio **User Layer Size** di Studio. Vedere **Passaggio 5: Creare criteri personalizzati per i gruppi di consegna**, in **Facoltativo: fare clic su Seleziona accanto a Dimensione livello utente in GB.**

### Strumenti per sovrascrivere la dimensione del livello utente (facoltativo)

È possibile ignorare la dimensione del livello utente utilizzando uno strumento di Windows per definire una quota sulla condivisione file a livello utente.

Utilizzare uno dei seguenti strumenti di quota Microsoft per impostare una quota rigida nella directory del livello utente denominata **Users** (Utenti):

- Gestione risorse file server (FSRM)
- Gestione quote

> **Nota:**
>
> L'aumento della quota influisce sui nuovi livelli utente ed espande quelli esistenti. La diminuzione della quota influisce solo sui nuovi livelli utente. I livelli utente esistenti non diminuiscono mai di dimensioni.

### Distribuire un livello di personalizzazione utente

Quando si distribuisce la funzionalità di personalizzazione utente, è possibile definirne i criteri in Studio. Assegnare quindi i criteri al gruppo di consegna associato al catalogo macchine in cui viene distribuita la funzionalità.

Se si lascia l'immagine master senza configurazione del livello di personalizzazione utente, i servizi rimangono inattivi e non interferiscono con le attività di creazione.

Se si impostano i criteri nell'immagine master, i servizi tentano di eseguire e montare un livello utente all'interno dell'immagine master. L'immagine master mostrerebbe comportamenti inaspettati e instabilità.

Per distribuire la funzionalità del livello di personalizzazione utente, completare i passaggi seguenti nell'ordine seguente:

- Passaggio 1: verificare la disponibilità di un ambiente Citrix Virtual Apps and Desktops.
- Passaggio 2: Preparare l'immagine master.
- Passaggio 3: Creare un catalogo macchine.
- Passaggio 4: Creare un gruppo di consegna.
- Passaggio 5: Creare criteri personalizzati per il gruppo di consegna.

> **Nota:**
>
> l'accesso per la prima volta dopo l'aggiornamento di Windows 10 sull'immagine richiede più tempo del solito. Il livello dell'utente deve essere aggiornato per la nuova versione di Windows 10, il che aumenta il tempo di accesso.

#### Passaggio 1: Verificare che sia disponibile un ambiente Citrix Virtual Apps and Desktops

Assicurarsi che il proprio ambiente Citrix Virtual Apps and Desktops sia disponibile per l'utilizzo con questa nuova funzionalità. Per informazioni dettagliate sull'installazione, vedere Installare e configurare Citrix Virtual Apps and Desktops.

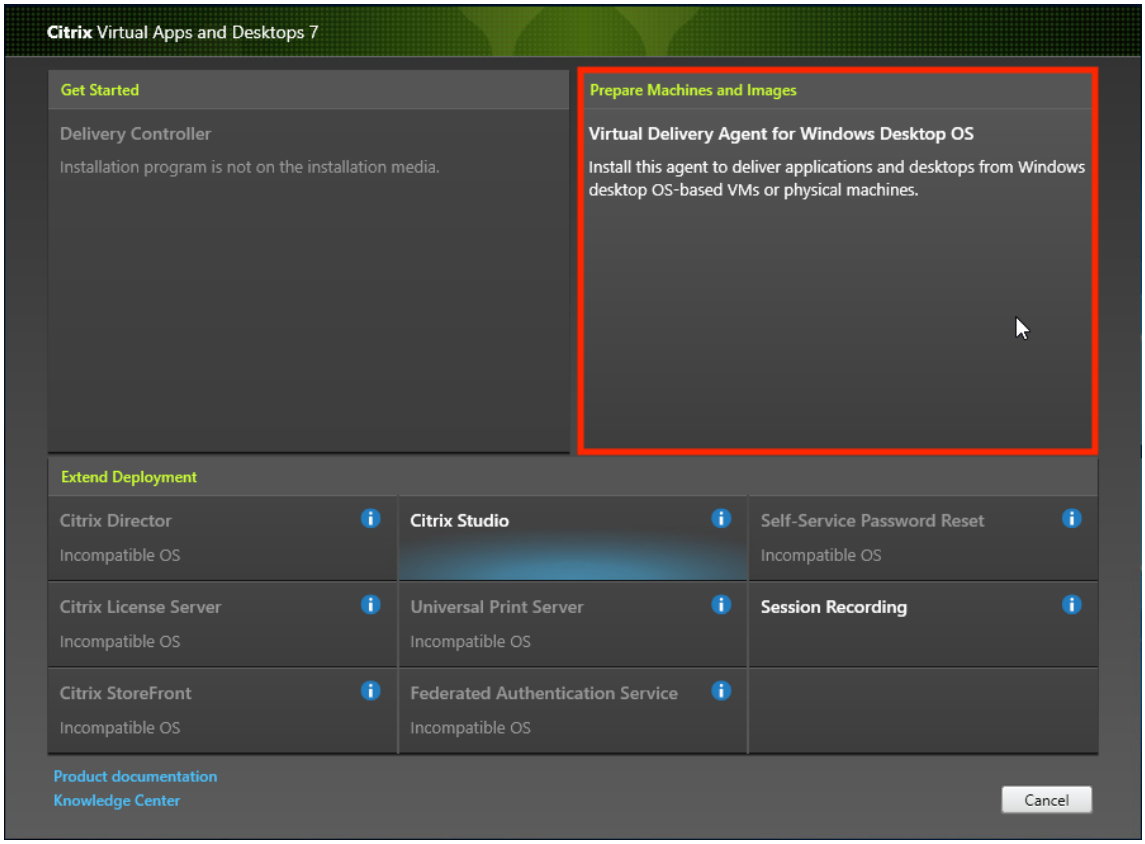
 

### Passaggio 2: Preparare l'immagine master

Per preparare l'immagine master:

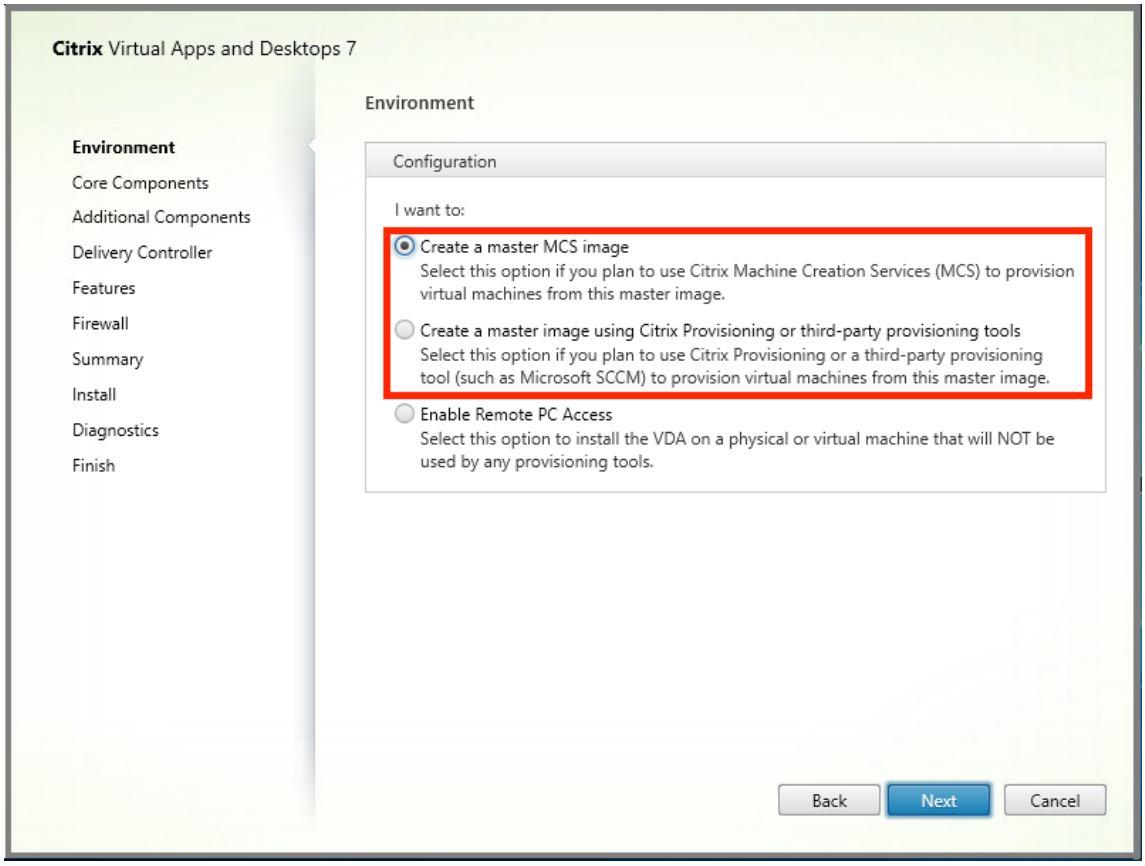
1. Individuare l'immagine master. Installare le applicazioni aziendali dell'organizzazione e tutte le altre app che gli utenti generalmente trovano utili.
2. Se si sta distribuendo Server VDI, attenersi alla procedura descritta nell'articolo Server VDI. Assicurarsi di includere il componente facoltativo, il **livello di personalizzazione utente**. Per i dettagli, vedere le Opzioni della riga di comando per l'installazione di un VDA.
3. Se si utilizza Windows 10, installare Virtual Delivery Agent (VDA) 1912 o versione successiva. Se è già installata una versione precedente del VDA, disinstallare prima la versione precedente. Quando si installa la nuova versione, assicurarsi di selezionare e installare il componente opzionale, **Citrix User Personalization Layer**, come segue:

    a) Fare clic sul riquadro **Virtual Delivery Agent for Windows Desktop OS**:




    a) **Environment** (Ambiente): selezionare **Create a master MCS image** (Creare un'immagine MCS master) o **Create a master image using Citrix Provisioning or third-party provisioning tools** (Creare un'immagine master utilizzando Citrix Provisioning o strumenti di provisioning di terze parti).

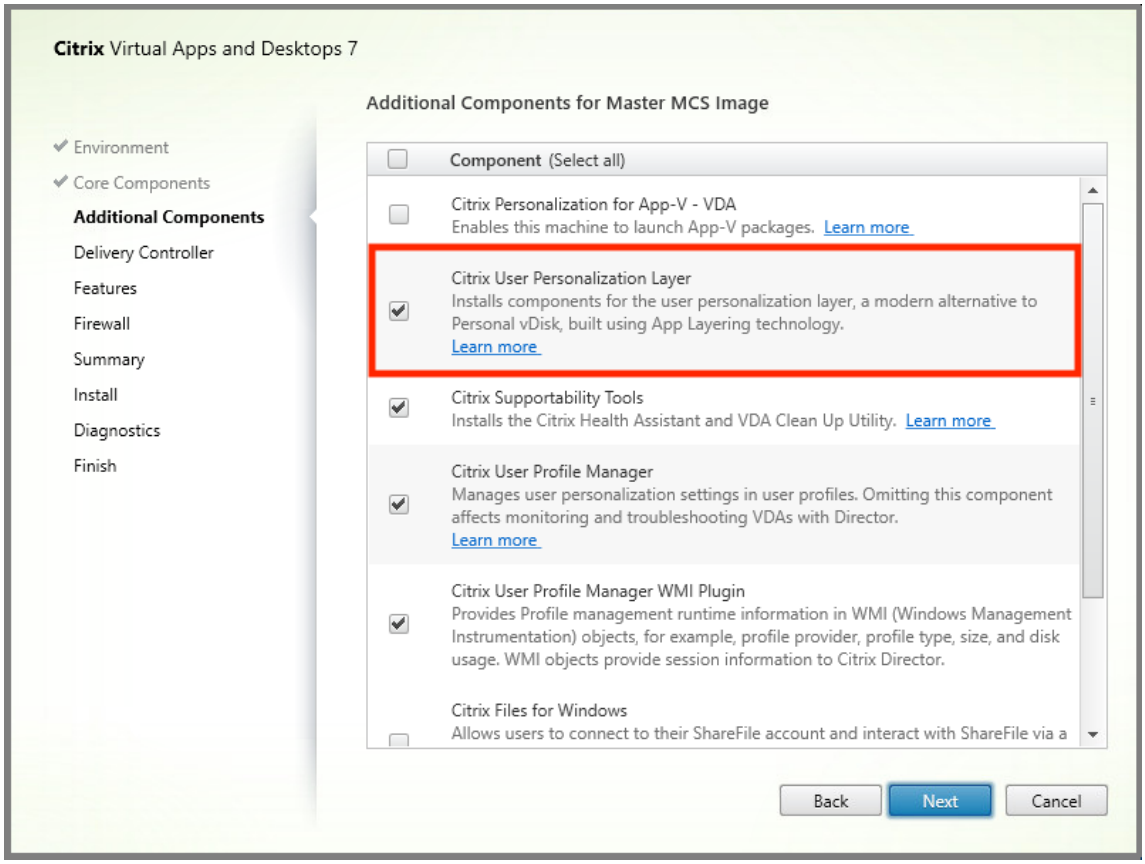
 




a) **Core components** (Componenti principali): fare clic su **Next**.

b) **Additional components** (Componenti aggiuntivi): inserire un segno di spunta in **Citrix User Personalization Layer**.




a) Fare clic sulle schermate di installazione rimanenti, configurando il VDA in base alle esigenze, e fare clic su **Install**. L'immagine si riavvia una o più volte durante l'installazione.

4. Lasciare disabilitata l'opzione **Windows updates**. Il programma di installazione del livello di personalizzazione utente disattiva gli aggiornamenti di Windows nell'immagine. Lasciare disabilitati gli aggiornamenti.

L'immagine è pronta per essere caricata in Studio.

> **Nota:**
>
> se si desidera semplicemente aggiornare il livello di personalizzazione utente (UPL), è possibile farlo con una versione più recente di UPL e il pacchetto autonomo. Non è necessario aggiornare il VDA.

### Passaggio 3: Creare un catalogo macchine

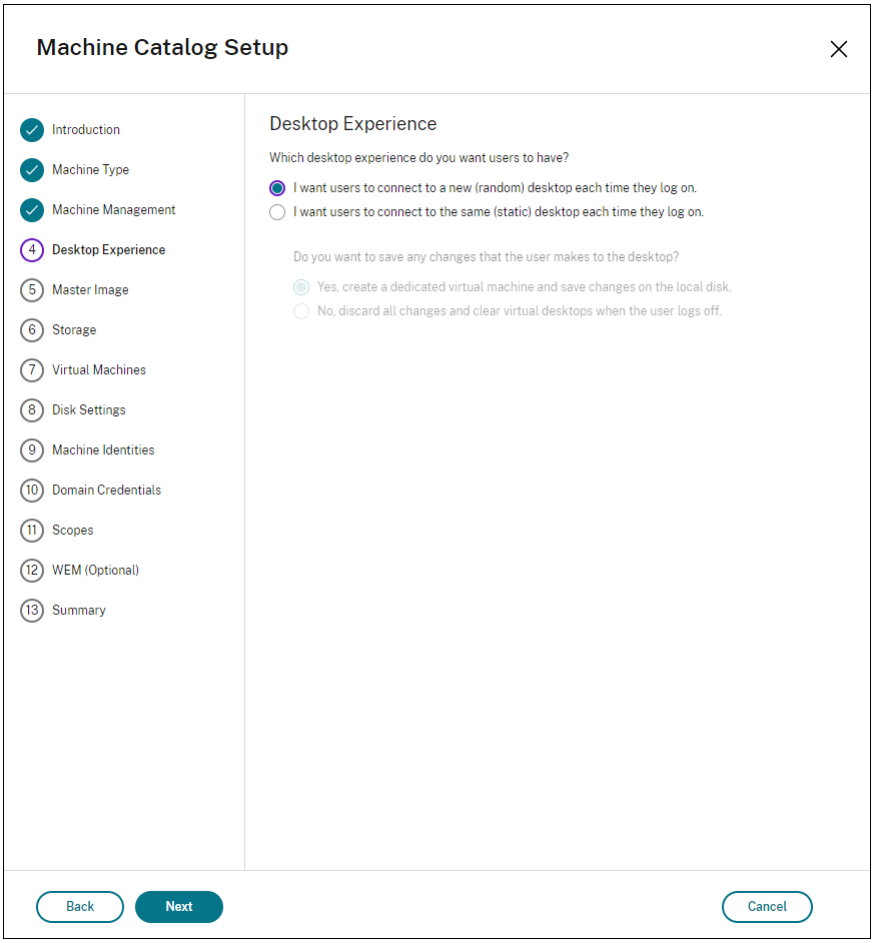
In Studio, attenersi alla procedura per creare un catalogo di macchine. Utilizzare le seguenti opzioni durante la creazione del catalogo:

1. Selezionare **Operating System** (Sistema operativo) e impostarlo su **Single session OS** (Sistema operativo a sessione singola).

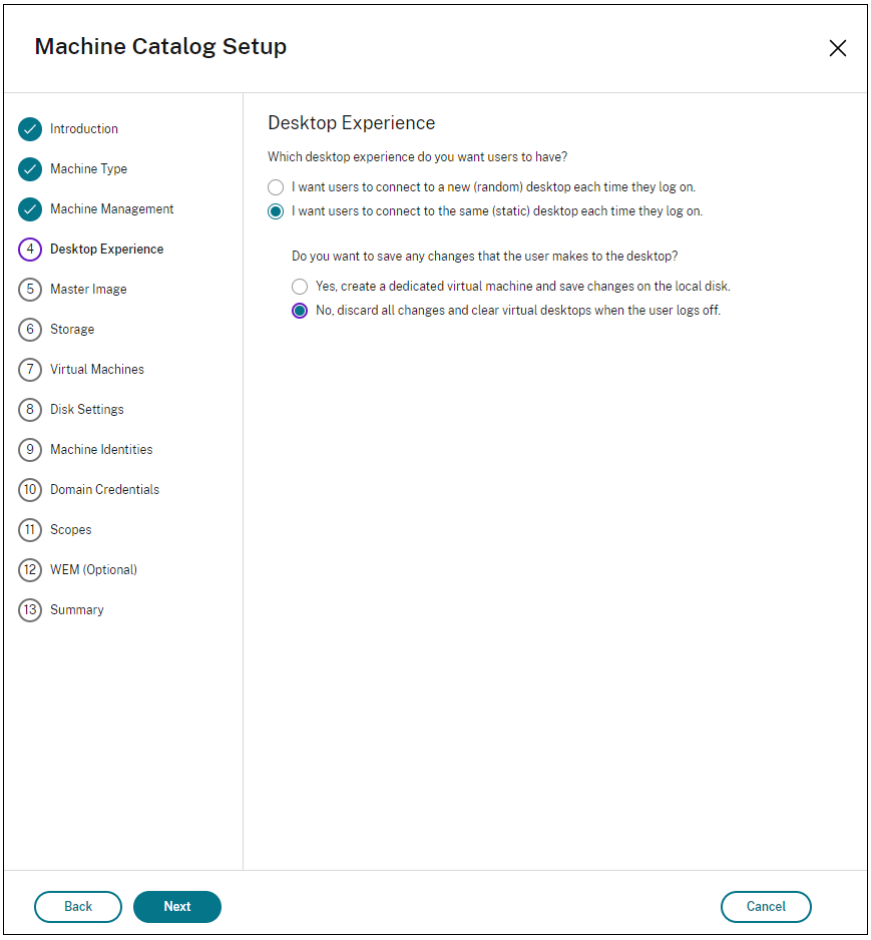
2. Selezionare **Machine Management** (Gestione macchine) e impostarlo su **Machines that are power managed** (Macchine con alimentazione gestita). Ad esempio, macchine virtuali o PC blade.
3. Selezionare **Desktop Experience** (Esperienza desktop) e impostarla sul tipo di catalogo **in pool casuale** o **in pool statico**, come negli esempi seguenti:

   - **In pool casuale:**




   - **In pool statico:** se si seleziona l'esperienza in pool statico, configurare i desktop in modo da eliminare tutte le modifiche e cancellare i desktop virtuali quando l'utente si scollega, come mostrato nello screenshot seguente:




> **Nota:**
>
> Il livello di personalizzazione utente non supporta i cataloghi in pool statico configurati per utilizzare Citrix Personal vDisk o assegnati come macchine virtuali dedicate.

4. Se si utilizza MCS, selezionare **Immagine master** e l'istantanea per l'immagine creata nella sezione precedente.
5. Configurare le rimanenti proprietà del catalogo in base alle esigenze dell'ambiente.

### Passaggio 4: Creare un gruppo di consegna

Creare e configurare un **gruppo di consegna**, comprendente i computer del catalogo macchine creato. Per ulteriori informazioni, vedere Creare gruppi di consegna.

### Passaggio 5: Creare criteri personalizzati per i gruppi di consegna

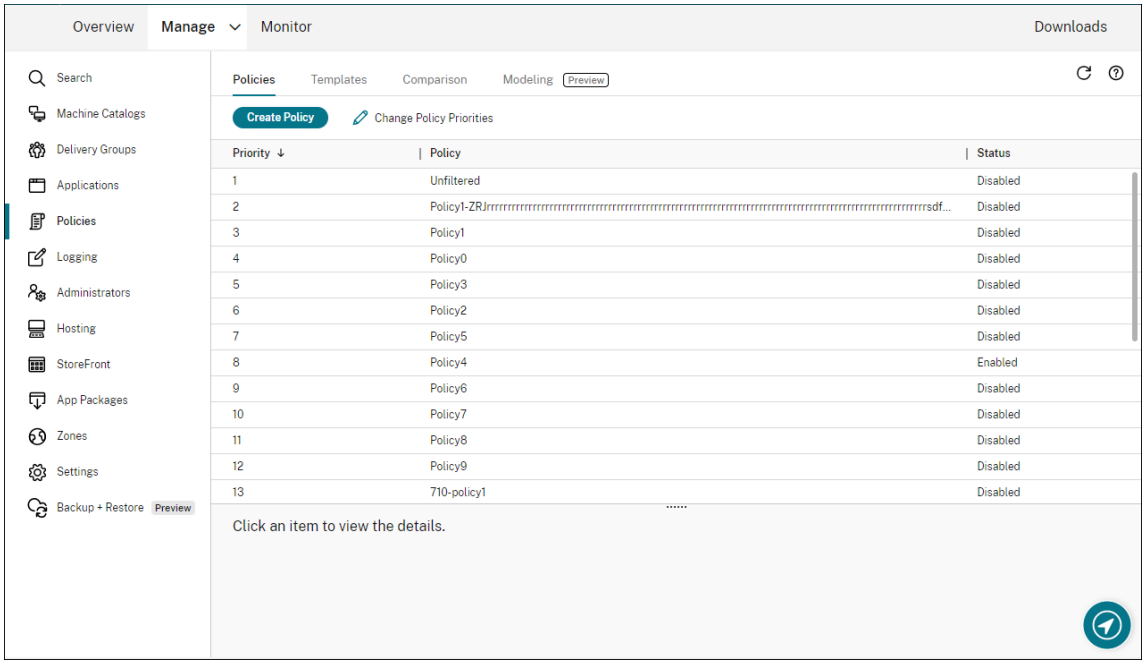
Per abilitare il montaggio dei livelli utente all'interno di Virtual Delivery Agent, utilizzare i parametri di configurazione per specificare:

- In quale posizione sulla rete accedere ai livelli utente.
- Fino a che dimensione consentire ai dischi del livello utente di ingrandirsi.

Definire i parametri come criteri Citrix personalizzati in Web Studio e assegnarli al gruppo di consegna.

1. Accedere a Web Studio e selezionare **Policies** nel riquadro a sinistra:




2. Selezionare **Create Policy** (Crea criterio) nella barra delle azioni. Viene visualizzata la finestra Create Policy (Crea criterio).
3. Digitare "user layer"(livello utente) nel campo di ricerca. Nell'elenco dei criteri disponibili vengono visualizzati i tre criteri seguenti:
   - Esclusioni a livello utente
   - User Layer Repository Path (Percorso del repository del livello utente)
   - User Layer Size GB (Dimensione livello utente GB)

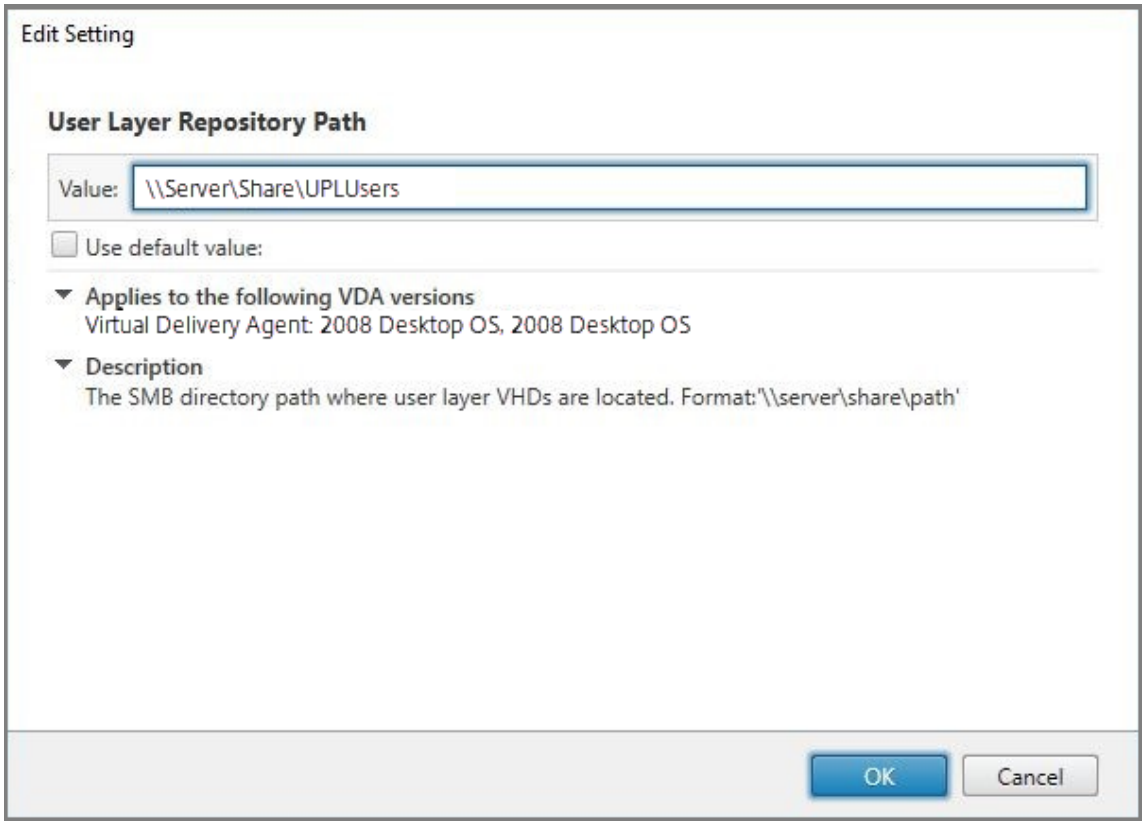
   > **Nota:**
   >
   > L'aumento delle dimensioni influisce sui nuovi livelli utente ed espande i livelli utente esistenti. La riduzione delle dimensioni influisce solo sui nuovi livelli utente. I livelli utente esistenti non diminuiscono mai di dimensioni.

4. Selezionare la casella di controllo accanto a **User Layer Repository Path** (Percorso del repository del livello utente) e fare clic su **Edit** (Modifica). Viene visualizzata la finestra Edit Setting (Modifica impostazione).

5. Immettere un percorso nel campo **Value** e fare clic su **Save**:

   - **Formato del percorso:** `\\server-name-or-address\share-name\folder`
   - **Esempio di percorso:** `\\Server\Share\UPLUsers`
   - **Esempio di percorsi risultanti:** per un utente chiamato **Alex** in **CoolCompanyDomain**, il percorso sarebbe: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

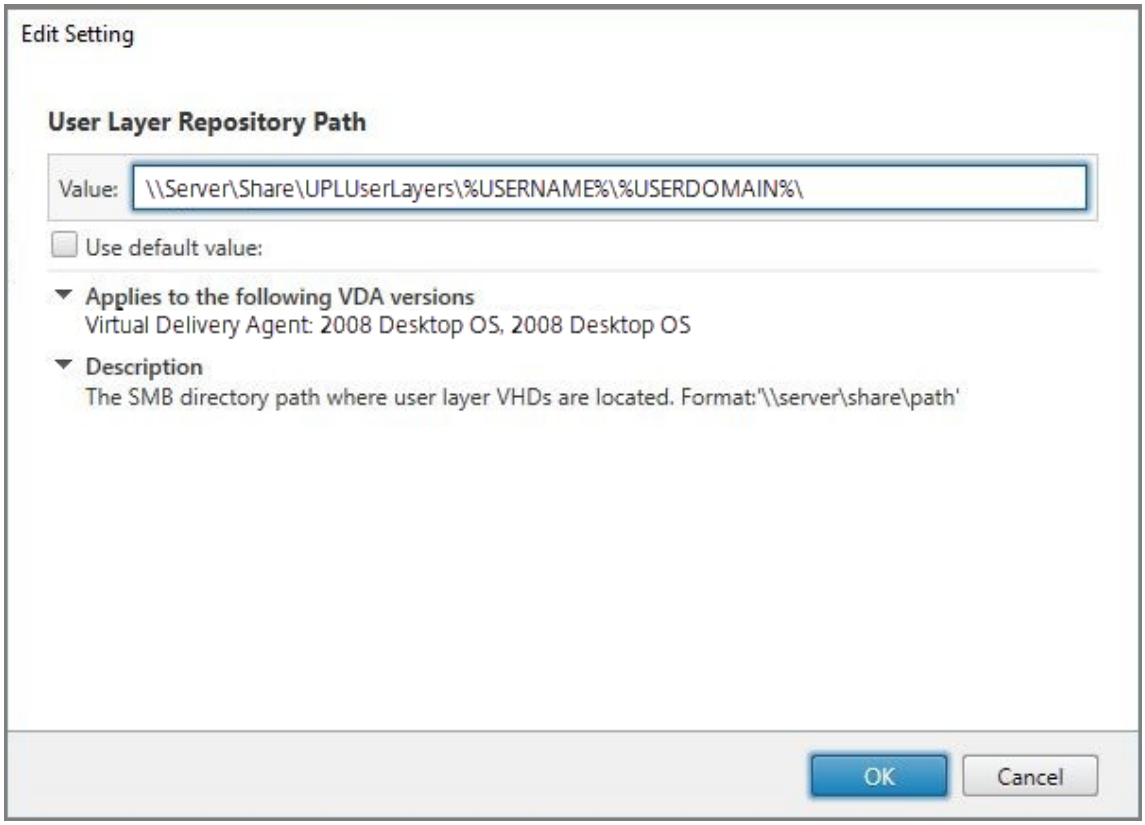



È possibile personalizzare il percorso utilizzando le variabili %USERNAME% e %USERDOMAIN%, le variabili di ambiente della macchina e gli attributi di Active Directory (AD). Quando sono espanse, queste variabili danno luogo a percorsi espliciti.

Esempio di variabili di ambiente:

- **Formato del percorso:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Esempio di percorso:** `\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%`
- **Esempio di percorsi risultanti:** per un utente chiamato **Alex** in **CoolCompanyDomain**, il percorso sarebbe: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

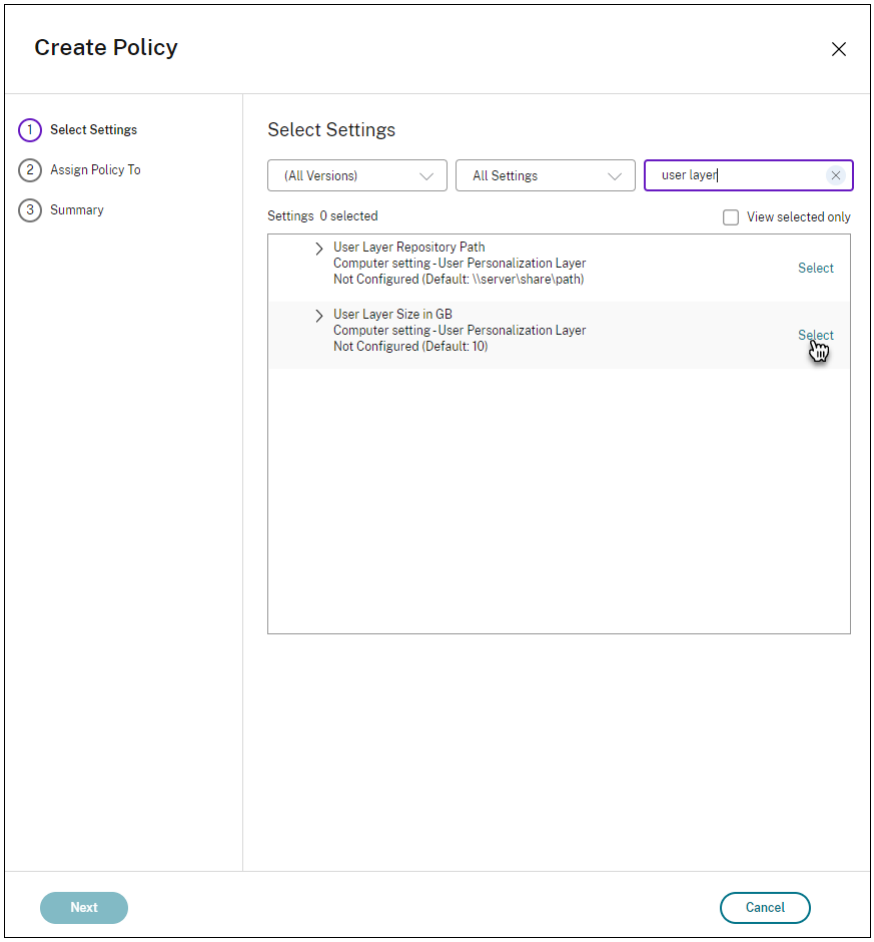



Esempio di attributi AD personalizzati:

- Formato del percorso: `\\Server-name-or-address\share-name\AD-attribute`
- Esempio di percorso: `\\Server\share\\#sAMAccountName#`
- Esempio di percorsi risultanti: `\\Server\share\JohnSmith` (se #sAMAccount-Name# si risolve in JohnSmith per l'utente corrente)

6. Facoltativo: selezionare la casella di controllo accanto a **User Layer Size in GB** (Dimensione del livello utente in GB) e fare clic su **Edit** (Modifica):

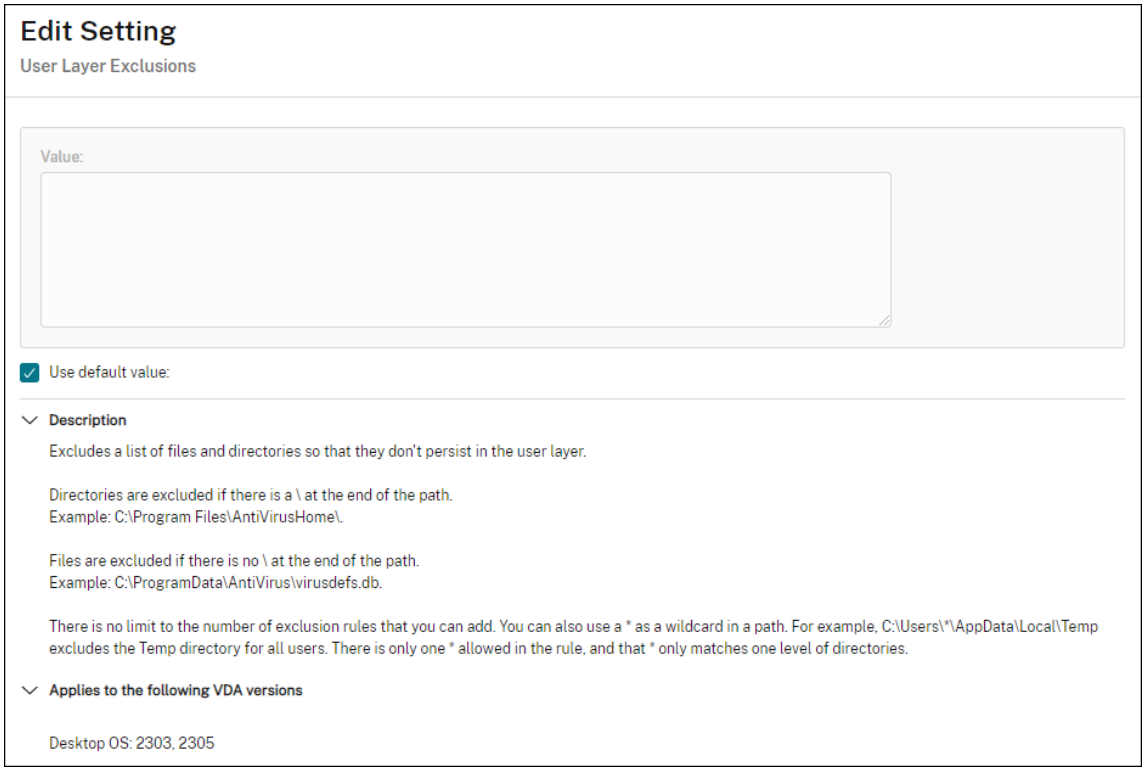



(Percorso del repository del livello utente)

Viene visualizzata la finestra Edit Settingsi.

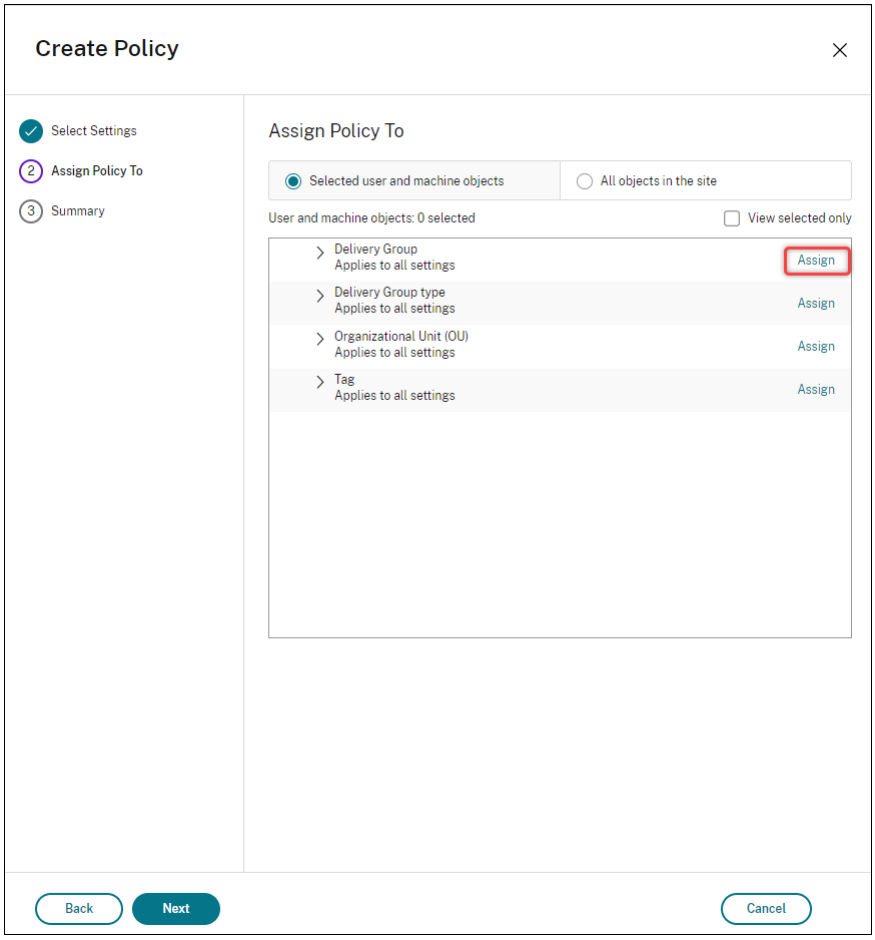
7. Facoltativo: modificare il valore predefinito di **10 GB** alla dimensione massima che ogni livello utente può raggiungere. Fare clic su **Salva**.
8. Facoltativo: selezionare la casella di controllo accanto a **User Layer Exclusions** (Esclusioni a livello utente) e fare clic su **Edit** (Modifica).



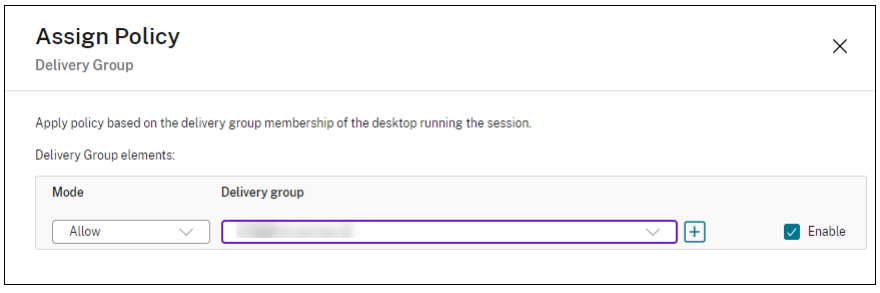

9. Facoltativo: specificare i file e le cartelle da escludere, quindi fare clic su **Save**. Per ulteriori informazioni, vedere la documentazione di Citrix App Layering.
10. Fare clic su **Next** per configurare utenti e macchine a cui effettuare l'assegnazione. Fare clic sul collegamento **Delivery Group Assign** (Assegna a gruppo di consegna) evidenziato in questa immagine:



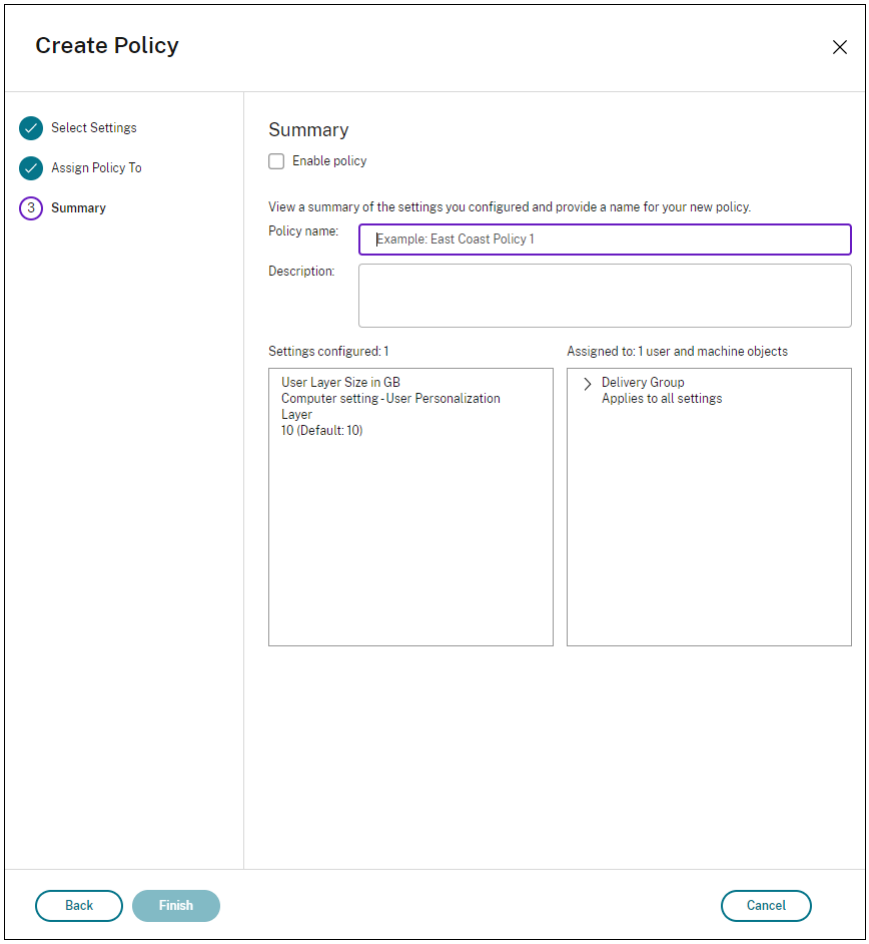

(Percorso del repository del livello utente)

11. Nel menu **Delivery Group** selezionare il gruppo di consegna creato nella sezione precedente. Fare clic su **OK**.




12. Immettere un nome per il criterio. Fare clic sulla casella di controllo per attivare il criterio e quindi fare clic su **Finish**.




### Configurare le impostazioni di protezione nella cartella del livello utente

In qualità di amministratore di dominio, è possibile specificare più di una posizione di archiviazione per i livelli utente. Creare una sottocartella `\Users` per ciascun percorso di archiviazione (inclusa la posizione predefinita). Proteggere ogni posizione utilizzando le seguenti impostazioni.

| Nome impostazione | Valore | Si applica a |
|---|---|---|
| Proprietario autore | Modifica | Solo sottocartelle e file |
| Diritti del proprietario | Modifica | Solo sottocartelle e file |
| Utenti o gruppo | Crea cartella/Aggiunta dati; Visita cartella/Esegui file; Elenca cartella/Leggi dati; Leggi attributi | Solo cartella selezionata |
| Sistema | Controllo completo | Cartella selezionata, sottocartelle e file relativi |

| Nome impostazione | Valore | Si applica a |
| --- | --- | --- |
| Amministratori di dominio e gruppo di amministrazione selezionato | Controllo completo | Cartella selezionata, sottocartelle e file relativi |

### Messaggi del livello utente

Quando un utente non è in grado di accedere al livello utente, riceve uno di questi messaggi di notifica.

- **Livello utente in uso**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- **Livello utente non disponibile**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- **Il sistema non ripristinato dopo lo scollegamento dell'utente**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

### File di registro da utilizzare per la risoluzione dei problemi

Il file di registro ulayersvc.log contiene l'output del software del livello di personalizzazione utente in cui vengono registrate le modifiche.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

### Limiti

Tenere presenti le seguenti limitazioni durante l'installazione e l'utilizzo della funzionalità di livello di personalizzazione utente.

- *Non* tentare di distribuire il software del livello di personalizzazione utente su un livello all'interno di App Layering. Distribuire i livelli di personalizzazione degli utenti in Citrix Virtual Apps and Desktops oppure abilitare i livelli utente in un modello di immagine App Layering, non entrambe le cose. Entrambi i processi producono i livelli utente necessari.
- *Non* configurare la funzionalità di livello di personalizzazione utente con i cataloghi di macchine persistenti.
- *Non* utilizzare gli host di sessione.
- *Non* aggiornare il catalogo macchine con un'immagine che esegue una nuova installazione del sistema operativo (anche la stessa versione di Windows 10). La procedura consigliata consiste nell'applicare aggiornamenti al sistema operativo all'interno della stessa immagine master utilizzata durante la creazione del catalogo macchine.
- *Non* utilizzare driver di avvio, né altre personalizzazioni di avvio anticipato.
- *Non* eseguire la migrazione dei dati PvD alla funzionalità del livello di personalizzazione utente.
- *Non* eseguire la migrazione dei livelli utente esistenti dal prodotto App Layering completo alla funzionalità del livello di personalizzazione utente.
- *Non* modificare il percorso SMB del livello utente per accedere ai livelli utente creati utilizzando un'immagine del sistema operativo master diversa.
- Quando un utente si disconnette da una sessione e quindi effettua nuovamente l'accesso, la nuova sessione viene eseguita su un computer diverso all'interno del pool. In un ambiente VDI, Microsoft Software Center vede un'applicazione come **Installed** nel primo computer, ma **Unavailable** (Non disponibile) sul secondo computer.

  Per scoprire lo stato effettivo dell'applicazione, istruire l'utente a selezionare l'applicazione nel Software Center e fare clic su **Install**. SCCM aggiorna quindi lo stato al valore effettivo.
- Software Center si arresta occasionalmente immediatamente dopo l'avvio all'interno di un VDA con la funzionalità di livello di personalizzazione utente abilitata. Per evitare questo problema, seguire i consigli di Microsoft per l'implementazione di SCCM in un ambiente VDI XenDesktop. Assicurarsi inoltre che il servizio `ccmexec` sia in esecuzione prima di avviare Software Center.
- Nei criteri di gruppo (impostazioni computer), le impostazioni dei livelli utente sostituiscono le impostazioni applicate all'immagine master. Pertanto, le modifiche apportate nelle impostazioni computer utilizzando un oggetto criteri di gruppo non sono sempre presenti per l'utente al successivo accesso alla sessione.

  Per risolvere questo problema, creare uno script di accesso utente che invia il comando:

  ```
  gpupdate /force
  ```

  Ad esempio, un cliente imposta il seguente comando per l'esecuzione ad ogni accesso utente:

```
gpudate /Target:Computer /force
```

Per ottenere risultati ottimali, applicare le modifiche delle impostazioni computer direttamente al livello utente, dopo che l'utente ha effettuato l'accesso.

- Un account utente di dominio non deve essere l'ultimo utente ad aver effettuato l'accesso a un'immagine master. Altrimenti le macchine fornite in provisioning da quell'immagine avranno problemi.
- I certificati personalizzati non persistono quando UPL è abilitato in un ambiente Azure AD puro, a causa di un problema sottostante di Windows in esecuzione su Azure. Se Microsoft risolve questo problema in un miglioramento futuro, aggiorneremo questo articolo.

## Aggiornare i VDA

July 28, 2023

### Introduzione

Citrix mantiene tutti i componenti di Citrix DaaS (in precedenza chiamato Citrix Virtual Apps and Desktops) della distribuzione dell'utente, ad eccezione dei VDA.

Prima di iniziare un aggiornamento di VDA:

- Leggere l'intero articolo, in modo da sapere cosa aspettarsi.
- Esaminare la policy del ciclo di vita per Citrix DaaS.

Per aggiornare un VDA, scaricare un programma di installazione VDA ed eseguirlo sulla macchina o sull'immagine. È possibile utilizzare l'interfaccia grafica o la riga di comando del programma di installazione. Per informazioni, vedere:

- Programmi di installazione dei VDA
- Installare i VDA utilizzando l'interfaccia grafica
- Installare i VDA utilizzando la riga di comando

Se il VDA è stato originariamente installato utilizzando `VDAWorkstationCoreSetup.exe`:

- Questa configurazione viene mantenuta se si aggiorna il VDA con l'ultima versione dello stesso programma di installazione.
- Se si esegue `VDAWorkstationSetup.exe` su quella macchina, è possibile abilitare le funzionalità non supportate in `VDAWorkstationCoreSetup.exe`. Tenere presente che alcune di queste funzionalità potrebbero essere abilitate per impostazione predefinita nel programma

di installazione di `VDAWorkstationSetup.exe`. È inoltre possibile installare l'app Citrix Workspace.

> **Nota:**
>
> Quando si aggiorna un VDA alla versione 7.17 o a una versione successiva supportata, si verifica un riavvio durante l'aggiornamento. Questo riavvio non può essere evitato. L'aggiornamento riprende automaticamente dopo il riavvio (a meno che non venga specificato `/noresume` nella riga di comando).

Dopo aver aggiornato i VDA, aggiornare le immagini e i cataloghi che utilizzano quei VDA.

### Aggiornare i vDA utilizzando l'interfaccia Full Configuration

> **Importante:**
>
> - Come best practice, si consiglia di testare accuratamente gli aggiornamenti dei VDA prima di passare alla produzione.
> - È possibile passare dal VDA CR al VDA LTSR purché si passi da una versione precedente a una versione successiva. Non è possibile passare da una versione successiva a una versione precedente perché questo è considerato un downgrade. Ad esempio, non è possibile effettuare il downgrade da 2212 CR a 2203 LTSR (qualsiasi CU), ma è possibile eseguire l'upgrade da 2112 CR a 2203 LTSR (qualsiasi CU).
> - Gli aggiornamenti su richiesta (quali gli aggiornamenti rapidi e le patch tra le versioni principali) non sono supportati.

Utilizzando l'interfaccia Full Configuration, è possibile aggiornare i VDA in base ai cataloghi o alle macchine. È possibile aggiornarli immediatamente o a un orario pianificato.

Per ulteriori informazioni sul servizio di aggiornamento VDA, vedere Tech Brief: Citrix VDA Upgrade service. L'articolo contiene una panoramica del servizio, informazioni dettagliate su come funziona e altre risorse utili.

#### Prerequisiti

- Piano di controllo: Citrix DaaS
- Tipo di VDA: VDA con sistema operativo a sessione singola o multisessione
- Versione VDA: 2109 o successiva o 2203 LTSR o successiva

  > **Nota:**

> Consigliamo di utilizzare il VDA CR più recente o il più recente VDA LTSR CU.

- Tipo di provisioning: macchine persistenti (quali le macchine con provisioning MCS, macchine Accesso remoto PC, Citrix HDXPlus per Windows 365). Vedere Tipi di macchine supportati.
- I VDA devono avere VDA Upgrade Agent installato e il servizio deve essere in esecuzione.
- Si deve disporre delle autorizzazioni per aggiornare i VDA.
- L'aggiornamento del VDA deve essere configurato con il corretto tracciamento CR o LTSR in Full Configuration.
- I VDA non devono essere in uso (gli utenti devono scollegarsi).

  > **Nota:**
  >
  > Gli aggiornamenti vengono ignorati per tutti i VDA in uso o in stato disconnesso. È consigliabile pianificare una finestra di aggiornamento e richiedere agli utenti di scollegarsi dai VDA.

- I VDA non devono essere in modalità di manutenzione (un VDA può essere messo in modalità di manutenzione da un amministratore o può anche essere messo automaticamente in modalità di manutenzione se ha superato il numero massimo di tentativi di registrazione consentiti).
- Gli URL pertinenti devono essere stati aggiunti all'elenco degli indirizzi consentiti se il filtro URL è attivo. Vedere VDA upgrade requirement.
- I VDA devono appartenere a un gruppo di consegna ed essere registrati in DaaS.
- Il livello di funzionalità è impostato correttamente in modo che la funzione di aggiornamento del VDA sia disponibile per l'uso. Vedere Versioni e livelli funzionali dei VDA.
- Il VDA di destinazione supporta il sistema operativo del VDA corrente.

**Problemi noti**

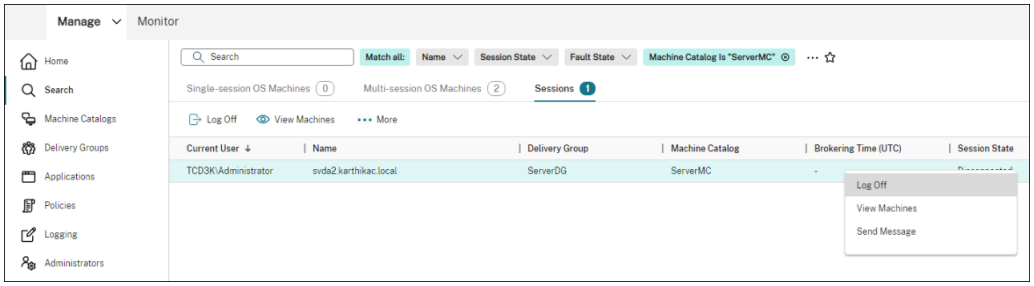
**Problema 1: aggiornamento dei VDA LTSR alle versioni LTSR Cumulative Update (CU) non riuscito** I tentativi di aggiornamento dei VDA LTSR alle versioni LTSR CU (Cumulative Update) potrebbero fallire. Sebbene il processo di aggiornamento sembri essere completato correttamente in Full Configuration, la versione installata del VDA non cambia e lo stato torna a **Upgrade Available** dopo un minuto o due. Il problema si verifica con i VDA su cui è installata la versione 7.35.0.7 o precedente di VDA Upgrade Agent.

Per risolvere il problema, accedere al VDA e aggiornare VDA Upgrade Agent alla versione 7.37.0.7 o a una versione successiva (utilizzando il programma di installazione VDA versione 2303 o successiva). A partire dalla versione 7.37.0.7, VDA Upgrade Agent supporta l'aggiornamento automatico in modo che gli agenti delle versioni precedenti in esecuzione sui VDA possano automaticamente aggiornarsi

alla versione più recente. Con questa funzione di aggiornamento automatico, il servizio di aggiornamento VDA verifica la versione del VDA riportata dall'agente e quindi pianifica gli aggiornamenti entro un'ora per aggiornare automaticamente l'agente alla versione più recente. Questa funzione di aggiornamento automatico alleggerisce il carico di manutenzione dell'amministratore.

Affinché l'agente presente sul VDA si aggiorni automaticamente, accertarsi di aver scollegato le sessioni in modo che il servizio di aggiornamento del VDA possa avviare gli aggiornamenti automatici. È possibile scollegare le sessioni in Full Configuration.




Se l'agente non si aggiorna automaticamente, accedere al VDA e aggiornare l'agente manualmente come segue:

1. Per visualizzare l'agente di aggiornamento VDA in Pannello di controllo > Disinstalla o modifica programma, eseguire il cmdlet seguente.

```
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $\_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent
     Service - x64'  }
 ).GetValue('SystemComponent')
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $\_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent
     Service - x64'  }
 ) | Set-ItemProperty -Name SystemComponent -Value 0
<!--NeedCopy-->
```

2. Installare la versione più recente di VDA Upgrade Agent. Per eseguire l'installazione automatica, utilizzare il seguente cmdlet:

   - `msiexec /i CitrixUpgradeAgent_x64.msi /q`

È possibile identificare la versione di VDA Upgrade Agent utilizzando il cmdlet o uno script. Vedere Risoluzione dei problemi.

**Problema 2: proxy non supportato** Attualmente, il VDA Upgrade Agent non supporta le configurazioni proxy. Questa limitazione può causare problemi di connettività quando l'agente tenta di stabilire connessioni tramite un server proxy.

È possibile applicare una soluzione alternativa per risolvere il problema. Effettuare le operazioni seguenti:

1. Individuare il file di configurazione dell'agente di aggiornamento VDA all'indirizzo: `C:\Program Files\Citrix\CitrixUpgradeAgent\Citrix.UpdateServices.UpdateAgent.exe.config`.
2. Aprire il file di configurazione utilizzando un editor di testo.
3. Aggiungere le seguenti righe alla fine del file, sostituendo `ProxyServerName` con il nome effettivo del server proxy:

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://PROXYSERVER:PORT" usesystemdefault
       ="false" />
  </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

4. Riavviare il servizio Citrix VDA Upgrade Agent per applicare la configurazione aggiornata.

#### Flusso di lavoro generale

Di seguito è riportato un flusso di lavoro generale per aggiornare i VDA utilizzando l'interfaccia Full Configuration:

1. Abilitare l'aggiornamento VDA per un catalogo.
   - È possibile abilitare l'aggiornamento VDA durante la creazione di un catalogo.
   - È possibile abilitare l'aggiornamento VDA durante la modifica di un catalogo.
2. Aggiornare i VDA in base ai cataloghi o alle macchine. Per ulteriori informazioni, vedere Configurare l'aggiornamento automatico per i VDA.

   > **Nota:**
   >
   > Quando si pianificano gli aggiornamenti del VDA per un catalogo, tenere presente che tutte le macchine del catalogo saranno incluse nell'ambito dell'aggiornamento. Pertanto, consigliamo di eseguire il backup di quelle macchine prima di iniziare l'aggiornamento.

#### Risoluzione dei problemi

Se si riscontrano errori di aggiornamento, è possibile utilizzare i seguenti registri per risolvere autonomamente i problemi oppure fornire i registri quando si contatta il supporto tecnico Citrix per ricevere assistenza.

- Registri dell'installazione iniziale del VDA in `%temp%/Citrix/XenDesktop Installer`
- Registri di aggiornamento in `C:\Windows\Temp\Citrix\XenDesktop Installer`

Per controllare le versioni di VDA Upgrade Agent, utilizzare il seguente cmdlet: `Get-VusComponentVersion -ComponentType VUS` Elenca tutti i VDA e le relative versioni di VDA Upgrade Agent.

Per ottenere i nomi dei VDA, utilizzare il seguente cmdlet: `Get-BrokerMachine -UUID "<version number>"`, dove `<version number>` è la versione di VDA Upgrade Agent ottenuta dal cmdlet `Get-VusComponentVersion`.

Per controllare le versioni di VDA Upgrade Agent a livello di catalogo, è possibile utilizzare il seguente script:

> **Nota:**
>
> Lo script è inteso come esempio e potrebbe essere necessario adattarlo all'ambiente specifico. Si consiglia di verificare accuratamente lo script prima di utilizzarlo in un ambiente di produzione.

```
Param(
    [Parameter (Mandatory=$true)]
    [string] $CatalogName
)

try
{

    $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-
       Object -Property UUID

    if($Uuids -eq $null)
    {

        throw "Cannot find CatalogName "+$CatalogName
     }

    Write-Output("Catalog Name passed is "+$CatalogName)

   foreach($Uuid in $Uuids)
    {

        $compVersion = Get-VusComponentVersion -MachineId $machine.UUID
            -ComponentType VUS
        $Machine = Get-BrokerMachine -UUID $compVersion.MachineId
        Write-Output("MachineName: "+$Machine.MachineName+", Machine
           UUID:"+$machine.MachineId+", VUA Version:"+$compVersion.
           Version)
     }

 }

```

```
catch
{

    Write-Output("Exception Occured")
    Write-Host $_
 }

<!--NeedCopy-->
```

**Registri relativi al VDA Upgrade Agent** È inoltre possibile raccogliere i registri relativi al VDA Upgrade Agent. I registri che si possono raccogliere includono:

- **Tracce Citrix Diagnostic Facility (CDF)**.
- **Registri eventi di Windows**. Informazioni scritte nel registro eventi di Windows. Visualizzare i registri in **Event Viewer > Applications and Services Logs > Citrix VDA Upgrade Agent Service** (Visualizzatore eventi > Registri applicazioni e servizi > Citrix VDA Upgrade Agent Service).

Se necessario, è possibile modificare il file di configurazione di VDA Upgrade Agent in modo che i registri vengano scritti continuamente su un file. Per abilitare la registrazione su un file, effettuare le seguenti operazioni:

1. Passare alla cartella `C:\Program Files\Citrix\CitrixUpgradeAgent`.
2. Aprire il file `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Cambiare il valore di `LogToFile` portandolo a `1`.
4. Riavviare il servizio Citrix VDA Upgrade Agent. Questo crea un file di registro in: `C:\ProgramData\Citrix\Update Services\Logs`.

> **Nota:**
>
> - Se si abilita la registrazione su un file, i registri vengono scritti in modo continuo, consumando potenzialmente spazio di archiviazione. Ricordare di disattivare la registrazione dopo la risoluzione del problema. Per disabilitare la registrazione, impostare prima `LogToFile` su `0` e poi riavviare il servizio Citrix VDA Upgrade Agent.
> - Quando `LogToFile=1` è impostato, i registri vengono scritti solo nel file. Non appariranno nelle tracce del CDF.

**Risoluzione degli errori di download degli aggiornamenti VDA** Seguire i passaggi seguenti per individuare e risolvere gli errori di download relativi alla funzionalità di aggiornamento del VDA:

1. Assicurarsi che gli URL pertinenti siano stati aggiunti all'elenco degli indirizzi consentiti se il filtro URL è attivo. Vedere VDA upgrade requirement.

2. Dopo aver aggiunto gli URL necessari all'elenco dei permessi, provare a riprogrammare l'aggiornamento del VDA.

È possibile abilitare il tracciamento CDF o impostare `LogToFile` su 1 per acquisire registri dettagliati per l'analisi. Se il problema di download persiste, controllare gli errori. Se viene visualizzato il seguente messaggio di errore "Download Failed: This access control list is not in canonical form and therefore cannot be modified"(Download non riuscito: questo elenco di controllo degli accessi non è in forma canonica e pertanto non può essere modificata), significa che le autorizzazioni sulla cartella `C:/ProgramData/Citrix/UpgradeServices/Downloads/VDA` non sono corrette. Per risolvere il problema, effettuare una delle seguenti operazioni:

- **Opzione 1**: reimpostare gli elenchi di controllo degli accessi (ACL) sulla cartella utilizzando il seguente comando. (Il comando reimposta gli ACL con gli ACL ereditati predefiniti per tutti i file corrispondenti)

  - `icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA"/reset /T /C /L /Q`

- **Opzione 2**: eliminare la cartella VDA in Downloads e quindi pianificare l'aggiornamento del VDA.

**Risolvere gli errori di convalida dell'aggiornamento del VDA** Seguire i passaggi seguenti per individuare e risolvere gli errori di download relativi alla funzionalità di aggiornamento del VDA:

1. Assicurarsi che gli URL pertinenti siano stati aggiunti all'elenco degli URL consentiti se è attivo il filtro URL, in particolare gli URL Certificate Revocation List (CRL) o Online Certificate Status Protocol (OCSP) necessari per il controllo della revoca. Vedere VDA upgrade requirement.
2. Dopo aver aggiunto gli URL necessari all'elenco dei permessi, provare a riprogrammare l'aggiornamento del VDA.

Suggeriamo di abilitare il tracciamento CDF o di impostare `LogToFile` su 1 per acquisire registri dettagliati per l'analisi. I registri possono includere i seguenti errori:

- RevocationStatusUnknown
- La funzione di revoca non è stata in grado di verificare lo stato della revoca del certificato.
- La funzione di revoca non è stata in grado di verificare la revoca perché il server di revoca era offline.

Il VDA Upgrade Agent fa affidamento sulle chiamate di sistema Windows per convalidare i certificati ed eseguire i controlli di revoca. Gli errori sopra riportati indicano che l'agente non è in grado di stabilire una connessione agli URL CRL od OCSP.

Tenere presente che il VDA Upgrade Agent attualmente non supporta le impostazioni proxy. Le chiamate CRL e OCSP in uscita effettuate da CryptoAPI non tengono conto delle configurazioni proxy, il che può causare errori.

Se l'ambiente dispone di una configurazione proxy, è possibile configurare il proxy di sistema sul VDA per facilitare le chiamate CRL in uscita. Seguire i passaggi seguenti per configurare il proxy di sistema:

```
netsh winhttp import proxy source=ie

Or

netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
<!--NeedCopy-->
```

### Aggiornare i VDA utilizzando PowerShell

È possibile configurare gli aggiornamenti dei VDA utilizzando l'SDK Remote PowerShell. Per ulteriori informazioni sull'SDK Remote PowerShell, vedere SDK Remote PowerShell per Citrix DaaS.

Di seguito sono riportati i cmdlet di PowerShell:

- **Get-VusCatalog**

  Utilizzare questo cmdlet per ottenere dettagli su un catalogo quali `Name`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR), `Upgrade scheduled` e `StateId` (stato di `Upgrade scheduled`).

- **Get-VusMachine**

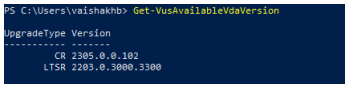
  Utilizzare questo cmdlet per ottenere dettagli di una macchina quali `MachineName`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR) e `StateId` (stato di `Upgrade scheduled`).

- **Get-VusComponentVersion**

  Utilizzare questo cmdlet per verificare se i VDA hanno segnalato le versioni dei componenti. Utilizzare `MachineId` per filtrare i VDA. `MachineId` è l'UUID di `Get-BrokerMachine`.

- **Get-VusAvailableVdaVersion**

  Utilizzare questo cmdlet per controllare l'ultima versione CR/LTSR rilasciata tramite il VDA Update Service.

- **Set-VusCatalogUpgradeType**

Utilizzare questo cmdlet per impostare il tipo di aggiornamento di un catalogo su CR o LTSR. Il tipo di aggiornamento può essere impostato solo a livello di catalogo macchine.

- **New-VusMachineUpgrade**

  Utilizzare questo cmdlet per configurare gli aggiornamenti dei VDA a livello di computer.

- **New-VusCatalogSchedule**

  Utilizzare questo cmdlet per pianificare gli aggiornamenti dei VDA a livello di catalogo macchine.

#### Esempi di cmdlet a livello di macchina

- Impostare il tipo di aggiornamento.

  Esempio:

  ```
  - Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType
    LTSR
  ```

- Utilizzare `Get-VusMachine` per controllare l'`UpgradeState` delle macchine di un catalogo.

  Esempio:

  ```
  - Get-VusMachine -CatalogName test-catalog
  ```

```
PS C:\Users> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  :
LastStateChange  :
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    :
SessionSupport   : SingleSession
StateId          :
StatusMessage    :
UpgradeState     : UpgradeAvailable
UpgradeType      : LTSR
UpgradeVersion   :

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  :
LastStateChange  :
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    :
SessionSupport   : SingleSession
StateId          :
StatusMessage    :
UpgradeState     : UpgradeAvailable
UpgradeType      : LTSR
UpgradeVersion   :
```

Se si nota che `UpgradeState` è `Unknown`, una possibile ragione è che il Citrix VDA Upgrade Agent installato sul VDA non ha segnalato la versione al VDA Update Service. È possibile utilizzare il cmdlet `Get-VusComponentVersion` per verificare se il VDA ha segnalato versioni dei componenti.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Se non viene visualizzato alcun risultato, verificare quanto segue:

- Il VDA fa parte di un catalogo e di un gruppo di distribuzione.
- Il VDA Upgrade Agent è installato sul VDA ed è in esecuzione. Se necessario, provare a riavviare l'agente.

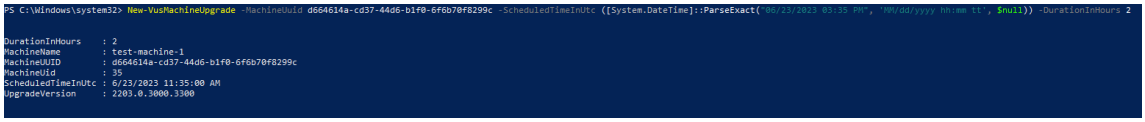
**Nota**: se non rimangono risultati, raccogliere le tracce di Citrix Diagnostic Facility durante il riavvio del VDA Upgrade Agent e risolvere i problemi.

- Pianificare gli aggiornamenti dei VDA. Prima di iniziare, tenere presente quanto segue:
  - `DurationInHours`: consente di fornire la durata in ore del processo di aggiornamento. I VDA verranno messi in modalità di manutenzione. Il programma di installazione del VDA verrà scaricato e verrà eseguito l'aggiornamento. Fornire una durata maggiore se ci sono molti VDA da aggiornare.
  - `UpgradeNow`: utilizzare questo interruttore per pianificare immediatamente un aggiornamento o un set `ScheduledTimeInUtc`.
  - `ScheduledTimeInUtc`: consente di pianificare un aggiornamento per una data e un'ora specifiche.

  Esempio:

  - `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

  È possibile utilizzare `MachineUuid`, `MachineUid` e `MachineName` per pianificare l'aggiornamento del VDA.




- Verificare lo stato dell'aggiornamento.

  Esempio:
  - `Get-VusMachine -MachineName test-machine-1`

```
PS C:\Windows\system32> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 2
LastStateChange  : 6/23/2023 11:47:35 AM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 11:35:00 AM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

```
PS C:\Users\vaishakhb> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

**Esempi di cmdlet a livello di catalogo**

- Impostare il tipo di aggiornamento a livello di catalogo macchine.

  Esempio:

  ```
  - Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType
    LTSR
  ```

- Utilizzare `Get-VusCatalog` per controllare il valore `UpgradeState` delle macchine in un catalogo:

  Esempio:

  ```
  -Get-VusCatalog -Name test-catalog
  ```

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades           :
DurationInHours             :
FailedUpgrades              :
InProgressUpgrades          :
LastStateChangeInUtc        :
MaxConcurrentUpgrades       :
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          :
SecurityCheckFailedUpgrades :
SessionSupport              : SingleSession
StateId                     :
SuccessfulUpgrades          :
TotalMachines               :
Uid                         : 30
UpgradeState                : UpgradeAvailable
UpgradeType                 : LTSR
UpgradeVersion              :
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

Se si nota che `UpgradeState` è `Unknown`, una possibile ragione è che il Citrix VDA Upgrade Agent installato sul VDA non ha segnalato la versione al VDA Update Service. È possibile utilizzare il cmdlet `Get-VusComponentVersion` per verificare se il VDA ha segnalato versioni dei componenti.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Se non viene visualizzato alcun risultato, verificare quanto segue:

- Il VDA fa parte di un catalogo e di un gruppo di distribuzione.
- Il VDA Upgrade Agent è installato sul VDA ed è in esecuzione. Se necessario, provare a riavviare l'agente.

**Nota**: se non rimangono risultati, raccogliere le tracce di Citrix Diagnostic Facility durante il riavvio del VDA Upgrade Agent e risolvere i problemi.

- Pianificare gli aggiornamenti dei VDA. Prima di iniziare, tenere presente quanto segue:
  - `DurationInHours`: consente di fornire la durata in ore del processo di aggiornamento. I VDA del catalogo verranno messi in modalità di manutenzione. Verrà scaricato il programma di installazione del VDA e sarà eseguito l'aggiornamento su ciascun VDA. Fornire

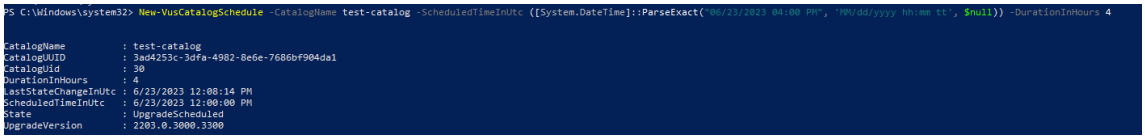
 

una durata maggiore se il catalogo contiene molti VDA.
- `UpgradeNow`: utilizzare questo interruttore per pianificare immediatamente un aggiornamento o un set `ScheduledTimeInUtc`.
- `ScheduledTimeInUtc`: consente di pianificare un aggiornamento per una data e un'ora specifiche.

Esempio:

- `New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 4`

È possibile utilizzare `CatalogName`, `Uid` e `Uuid` per pianificare l'aggiornamento.




- Verificare lo stato dell'aggiornamento. Utilizzare il cmdlet `Get-VusCatalog` o `Get-VusMachine` per controllare periodicamente lo stato di aggiornamento del VDA. Utilizzare `MachineUuid`, `MachineUid` e `MachineName` per filtrare i VDA.

  Esempio:
  - `Get-VusCatalog -Name test-catalog`

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades           : 0
DurationInHours             : 4
FailedUpgrades              : 0
InProgressUpgrades          : 0
LastStateChangeInUtc        : 6/23/2023 12:08:43 PM
MaxConcurrentUpgrades       : 100
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          : 6/23/2023 12:00:00 PM
SecurityCheckFailedUpgrades : 0
SessionSupport              : SingleSession
StateId                     : UpgradeInProgress
SuccessfulUpgrades          : 0
TotalMachines               : 2
Uid                         : 30
UpgradeState                : UpgradeScheduled
UpgradeType                 : LTSR
UpgradeVersion              : 2203.0.3000.3300
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

  Utilizzare `Get-VusMachine` per visualizzare lo stato di aggiornamento del VDA di ogni macchina in un catalogo.

```
PS C:\Users\vaishakhb> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:17:33 PM
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

### Se sui VDA è installato Personal vDisk

Se il componente Personal vDisk (PvD) è stato installato su un VDA, tale VDA non può essere aggiornato alla versione 1912 LTSR o successiva fino a quando non viene rimosso tale componente.

Questa istruzione si applica anche se non PvD non è stato mai usato. Ecco come il componente PvD potrebbe essere stato installato nelle versioni precedenti:

- Nell'interfaccia grafica del programma di installazione VDA, PvD era un'opzione nella pagina **Componenti aggiuntivi**. Nelle versioni 7.15 LTSR e 7.x precedenti questa opzione era attivata per impostazione predefinita. Quindi, se sono state accettate le impostazioni predefinite (o se l'opzione è stata abilitata esplicitamente in qualsiasi versione), PvD è stato installato.
- Sulla riga di comando, l'opzione `/baseimage` ha installato PvD. Se è stata specificata questa opzione o è stato utilizzato uno script che la conteneva, è stato installato PvD.

#### Cosa fare

Se il programma di installazione dei VDA non rileva i componenti AppDisks o PvD nel VDA attualmente installato, l'aggiornamento procede come di consueto.

Se il programma di installazione rileva il componente PvD nel VDA attualmente installato:

- **Interfaccia grafica**: l'aggiornamento va in pausa. Viene visualizzato un messaggio in cui si chiede se si desidera rimuovere automaticamente il componente non supportato. Quando si fa clic su **OK**, il componente viene rimosso automaticamente e l'aggiornamento procede.
- **CLI:** il comando ha esito negativo se il programma di installazione rileva il componente PvD. Per evitare errori di comando, includere la seguente opzione nel comando: `/remove_pvd_ack`.

Se si desidera continuare a utilizzare PvD sui computer Windows 10 (1607 e versioni precedenti, senza aggiornamenti), VDA 7.15 LTSR è l'ultima versione supportata. Tenere presente che il programma di supporto esteso per XenApp e XenDesktop 7.15 LTSR non si applica ai VDA utilizzati con Citrix DaaS. Per ulteriori informazioni, vedere la Extended Support Customer Guide nel Citrix Support Knowledge Center.

### Sistemi operativi precedenti

Nell'articolo Requisiti di sistema sono elencati i sistemi operativi Windows supportati per i VDA della versione corrente.

- Per i VDA LTSR, vedere l'articolo sui requisiti di sistema per la propria versione LTSR.
- Per i VDA Linux, vedere la documentazione di Linux Virtual Delivery Agent.

Per le macchine Windows con sistemi operativi che non sono più supportati per l'installazione del VDA più recente, sono disponibili le seguenti opzioni.

Per gli ambienti non WVD:

- Creare una nuova immagine della macchina in una versione di Windows supportata, quindi installare il nuovo VDA.
- Se la creazione di una nuova immagine della macchina non è un'opzione valida, ma si desidera aggiornare il sistema operativo, disinstallare il VDA prima di aggiornare il sistema operativo. In caso contrario, il VDA sarà in uno stato non supportato. Dopo aver aggiornato il sistema operativo, installare il nuovo VDA.
- Se sulla macchina è installata la versione 7.15 LTSR (e si tenta di installare una versione più recente), un messaggio informa che si sta utilizzando l'ultima versione supportata.
- Se sulla macchina è installata una versione precedente alla 7.15 LTSR, un messaggio guida l'utente a CTX139030 per informazioni. È possibile scaricare i VDA 7.15 LTSR dal sito Web Citrix.

## Migrare la configurazione a Citrix Cloud

November 21, 2023

### Perché utilizzare Automated Configuration

Gli amministratori IT responsabili di ambienti grandi o complessi spesso considerano le migrazioni un processo noioso. Spesso finiscono per scriversi da soli gli strumenti per svolgere con successo questo compito poiché tende a essere specifico per i loro casi d'uso

Citrix vuole contribuire a semplificare questo processo automatizzando il processo di migrazione mediante lo strumento Automated Configuration. Gli amministratori possono facilmente testare le configurazioni attuali in Citrix Cloud e sfruttare i vantaggi offerti da Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops), mantenendo *intatti*gli ambienti attuali. Inoltre, non vi è alcun impatto sull'utente finale, poiché Automated Configuration funziona perfettamente in background. Tali vantaggi includono una riduzione del sovraccarico amministrativo quando Citrix gestisce parte del back-end e del piano di controllo, aggiornamenti automatici e personalizzabili dei componenti Citrix Cloud e altri.

Citrix utilizza la configurazione standard del settore come codice per offrire un meccanismo che aiuta ad automatizzare i processi di migrazione. Automated Configuration rileva ed esporta uno o più siti locali come raccolta di file di configurazione. La configurazione di questi file può quindi essere importata in Citrix DaaS.

Automated Configuration consente inoltre agli amministratori di unire più siti locali in un unico sito, evitando conflitti di nomi. Gli amministratori possono stabilire se le risorse debbano essere controllate dalla configurazione locale o cloud.

Automated Configuration non è solo uno strumento di migrazione una tantum, ma può anche automatizzare la configurazione quotidiana in Citrix Cloud. Lo spostamento della configurazione Citrix DaaS può essere utile per molte ragioni:

- Sincronizzazione del sito dalla fase di test o di staging alla fase di produzione
- Effettuare il backup e ripristinare la configurazione
- Raggiungere i limiti delle risorse
- Migrare da una regione all'altra

Il seguente video di *2 minuti* fornisce una panoramica rapida di Automated Configuration.

Si tratta di un video incorporato. Fare clic sul collegamento per guardare il video

Per ulteriori informazioni su Automated Configuration, vedere Proof of Concept: Automated Configuration Tool in Tech Zone.

Per uno sguardo più approfondito sullo spostamento della distribuzione e sulla preparazione della configurazione locale per la migrazione, vedere l'articolo Deployment Guide: Migrating Citrix Virtual Apps and Desktops from on-premises to Citrix Cloud in Tech Zone.

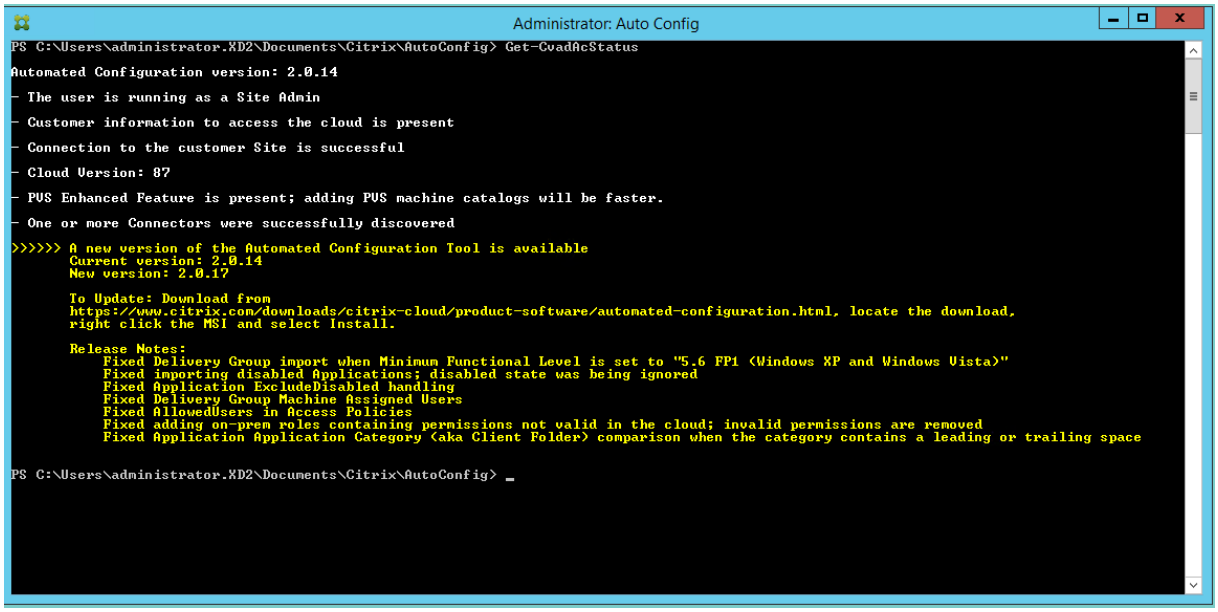
### Scaricare Automated Configuration

Scaricare e installare lo strumento Automated Configuration da Citrix Downloads.

> **Importante:**
>
> Per evitare errori di funzionamento, utilizzare sempre l'ultima versione disponibile di Automated Configuration.

### Aggiornamento di Automated Configuration

Quando si eseguono cmdlet che accedono al cloud in Automated Configuration, lo strumento avvisa l'utente quando è disponibile per il download una versione più recente.




È possibile assicurarsi di avere la versione più recente attenendosi alla seguente procedura:

1. Fare doppio clic sull'icona **Auto Config**. Viene visualizzata una finestra di PowerShell.
2. Eseguire il seguente comando per verificare il numero di versione.

   ```
   Get-CvadAcStatus
   ```

3. Controllare la versione dello strumento rispetto alla versione elencata nell'avviso o su Citrix Downloads. L'ultima versione dello strumento si trova lì.
4. Scaricare e installare l'ultima versione dello strumento. *Non* è necessario disinstallare la versione precedente per aggiornare Automated Configuration.

> **Nota:**
>
> L'avviso viene visualizzato ogni volta che si esegue un cmdlet che accede al cloud. Per ulteriori informazioni sui cmdlet, vedere Automated Configuration tool cmdlets.

### Limitazioni note

- I cataloghi di macchine forniti tramite Machine Creation Services hanno considerazioni speciali. Per ulteriori informazioni su MCS, vedere Understanding migrating Machine Creation Services provisioned catalogs.

### Oggetti di migrazione supportati

Automated Configuration supporta lo spostamento della configurazione dei seguenti componenti:

- Tag
- Amministrazione delegata
  - Ambiti
  - Ruoli
- Connessioni host
  - Un unico pool di risorse
  - Ambiti di amministrazione
- Cataloghi di macchine
  - Ambiti di amministrazione
  - Macchine
  - Accesso remoto al PC, fisico, in pool, con provisioning, MCS, assegnato
- StoreFronts
- Gruppi di consegna
  - Criteri di accesso
  - Associazione di ambiti di amministrazione
  - Criteri di accesso alle applicazioni
  - Criteri di assegnazione
  - Criteri di autorizzazione/desktop
  - Pianificazioni dell'alimentazione
  - Permanenza della sessione
  - Prelavancio della sessione
  - Pianificazioni di riavvio

  - Tag
- Gruppi di applicazioni
  - Associazione di ambiti di amministrazione
  - Gruppi di consegna
  - Utenti e gruppi
- Applicazioni
  - Cartelle delle applicazioni
  - Icone
  - Applicazioni
  - FDA configurati da broker
  - Tag
- Criteri di gruppo
- Preferenze dell'area utente

### Ordine di migrazione dei componenti

I componenti e le relative dipendenze sono elencati qui. Le dipendenze di un componente devono essere presenti prima di poter essere importate o unite. Se manca una dipendenza, è possibile che il comando di importazione o unione non riesca. La sezione **Fixups** del file di registro mostra le dipendenze mancanti in caso di errore di importazione o unione.

1. Tag
   - Nessuna pre-dipendenza
2. Amministrazione delegata
   - Nessuna pre-dipendenza
3. Connessioni host
   - Informazioni sulla sicurezza in CvadAcSecurity.yml
4. Cataloghi di macchine
   - Macchine presenti in Active Directory
   - Connessioni host
   - Tag
5. StoreFronts
6. Gruppi di consegna
   - Macchine presenti in Active Directory

- Utenti presenti in Active Directory
- Cataloghi di macchine
- Tag

7. Gruppi di applicazioni
    - Gruppi di consegna
    - Tag
8. Applicazioni
    - Gruppi di consegna
    - Gruppi di applicazioni
    - Tag
9. Criteri di gruppo
    - Gruppi di consegna
    - Tag
10. Preferenze dell'area utente

## Prerequisiti comuni

Di seguito sono riportati alcuni prerequisiti comuni necessari per il corretto funzionamento di Automated Configuration. Questi prerequisiti vengono utilizzati sia nelle migrazioni da locale a cloud che da cloud a cloud.

### Generazione dell'ID cliente, dell'ID client e della chiave segreta

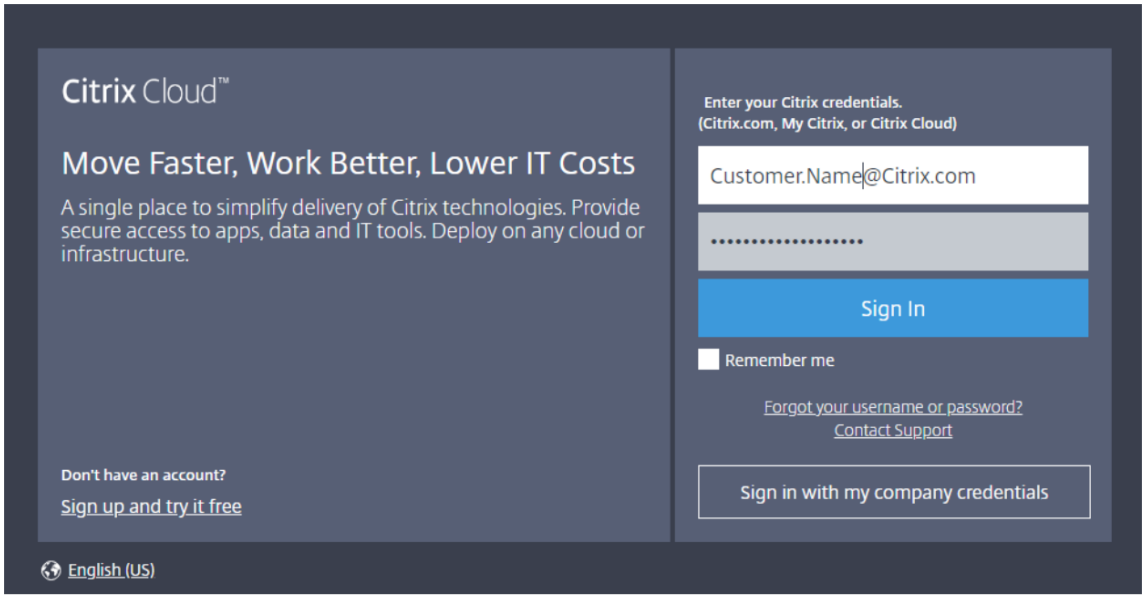
Prima di iniziare la migrazione utilizzando Automated Configuration, è necessario disporre dell'ID cliente Citrix Cloud e creare un ID client e una chiave segreta per importare la configurazione in Citrix Cloud. Tutti i cmdlet che accedono al cloud richiedono questi valori.

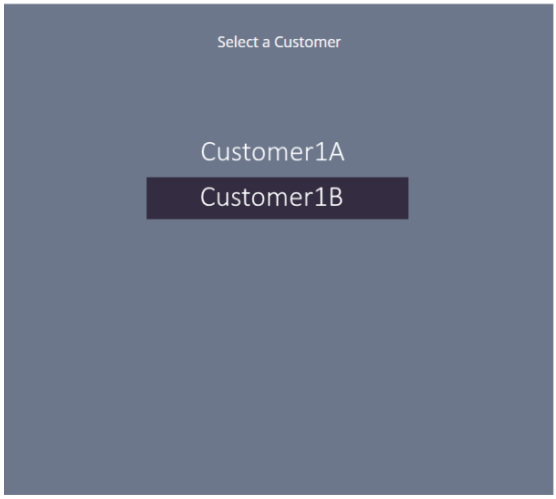
I passaggi seguenti consentono di recuperare l'ID cliente e creare l'ID client e la chiave segreta.

Per recuperare l'**ID cliente**:

1. Accedere al proprio account Citrix Cloud e selezionare il cliente.

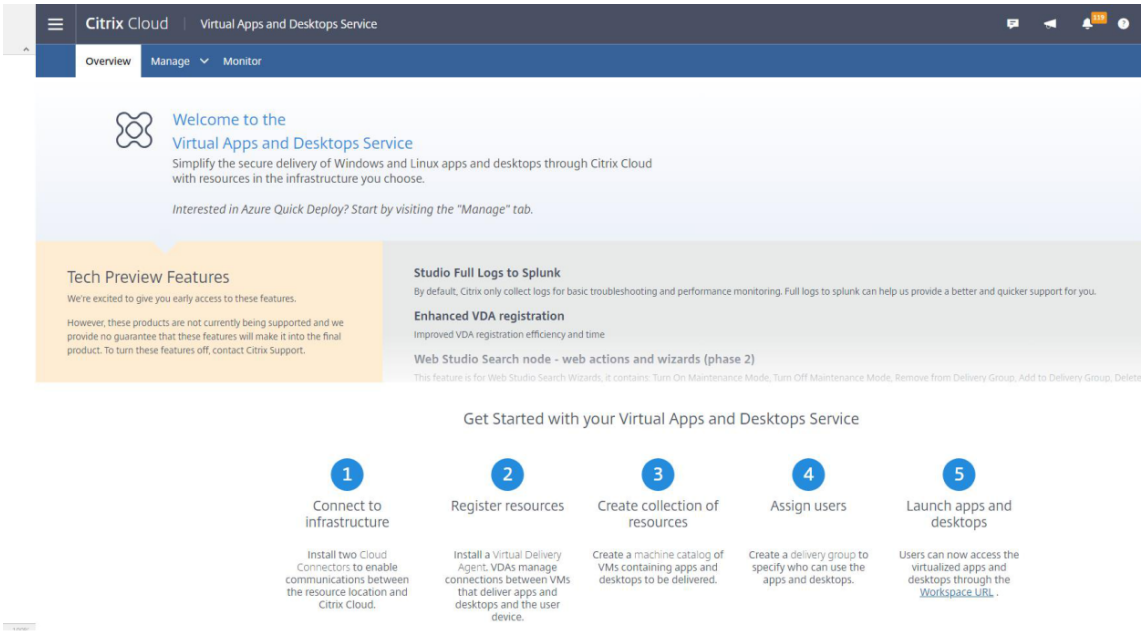
 

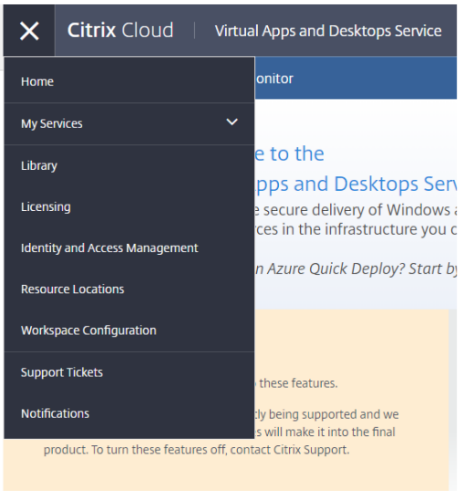


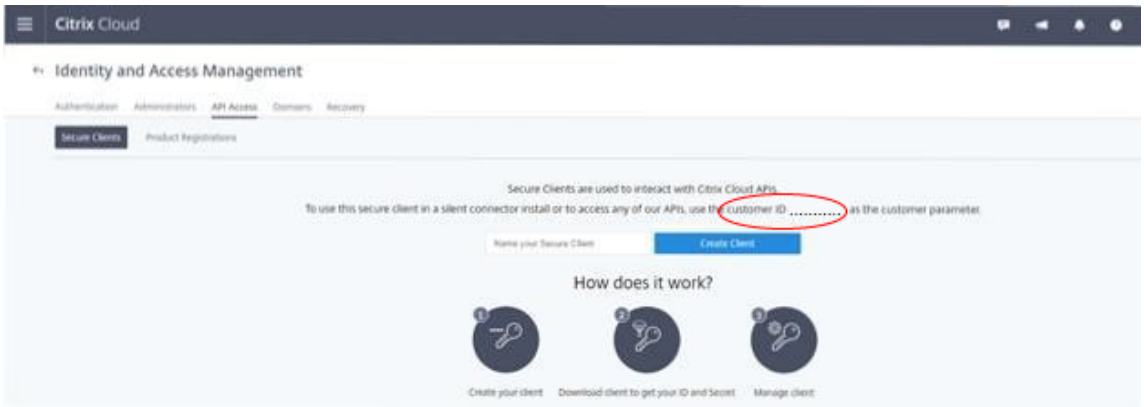

2. Fare clic sul menu a forma di hamburger, quindi selezionare **Identity and Access Management** (Gestione identità e accessi) nel menu a discesa.



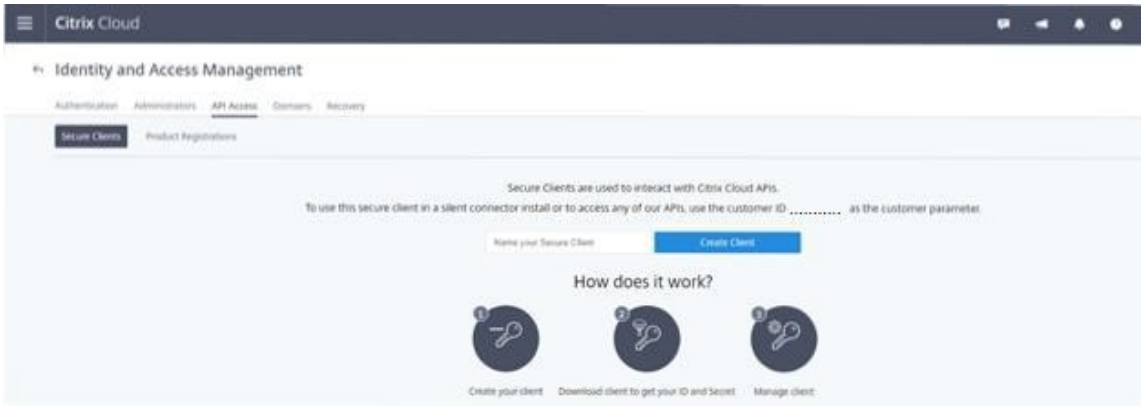

3. L'**ID cliente** si trova nella pagina **Gestione identità e accessi** .



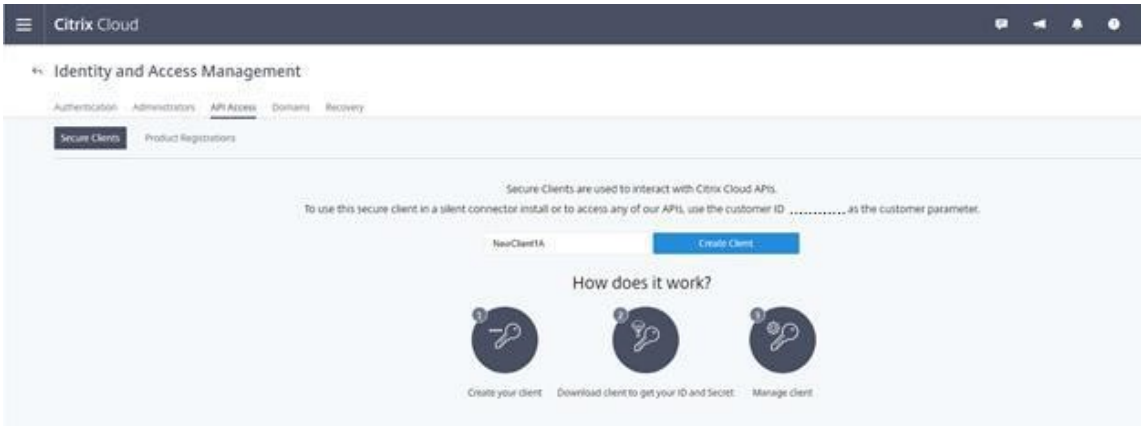

 

Per recuperare l'**ID client** e la **chiave segreta**:

1. Nella pagina **Identity and Access Management**, fare clic sulla scheda **API Access**.

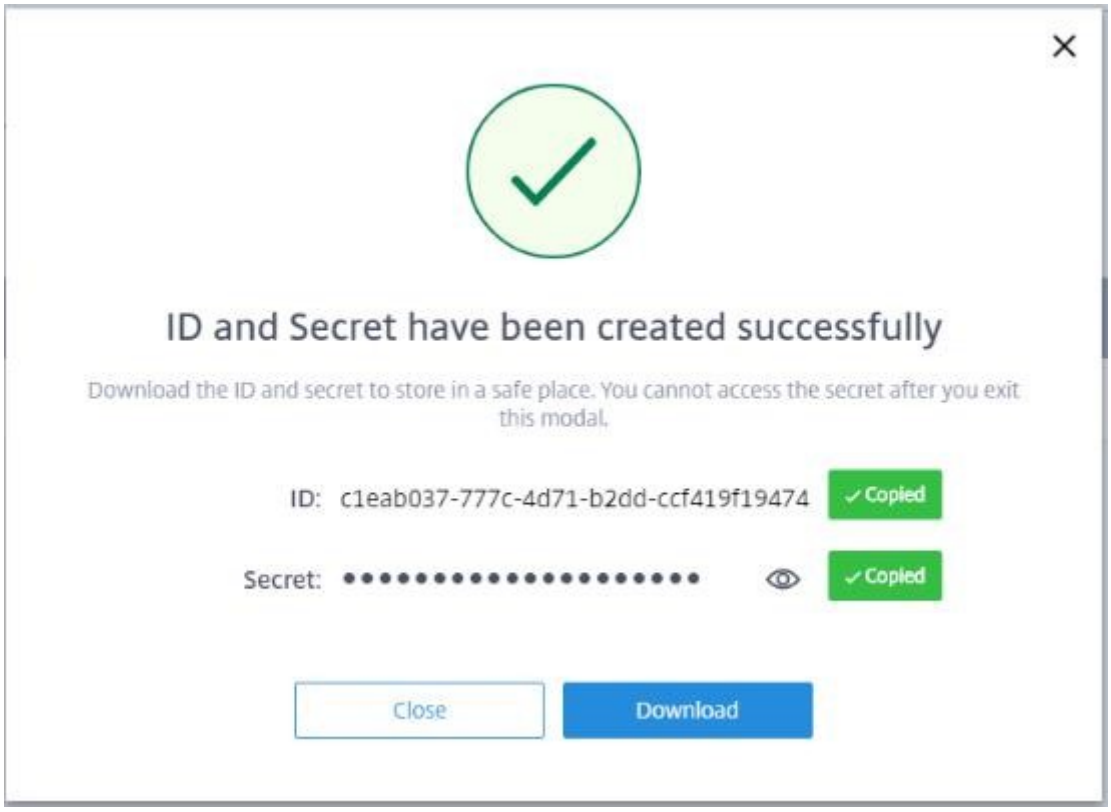



2. Inserire un nome nella casella. Questo nome viene utilizzato per distinguere tra più ID client e chiavi segrete. Fare clic su **Create client** per creare l'ID client e la chiave segreta.

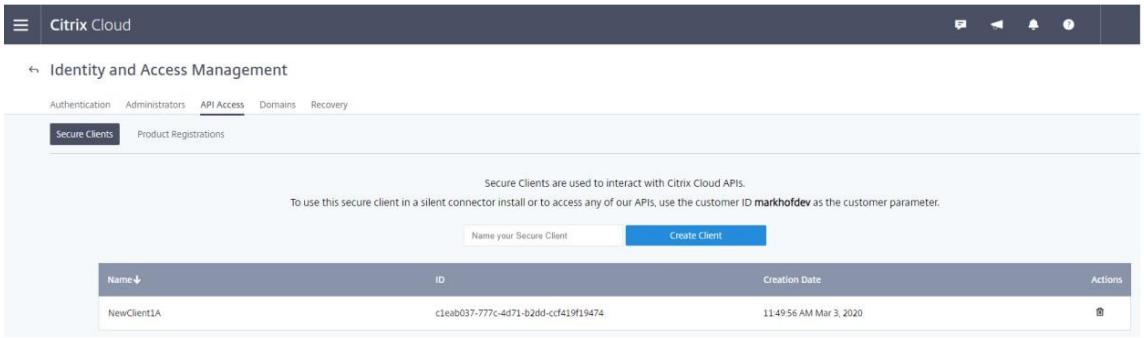



3. La seguente finestra di dialogo viene visualizzata dopo aver creato correttamente l'ID client e la chiave segreta. Fare attenzione a copiare entrambi i valori in una posizione sicura e scaricare il file .csv contenente queste informazioni. Il file .csv può essere utilizzato per creare il file CustomerInfo.yml.




4. L'ID client e la chiave segreta sono stati creati correttamente.




Mettere questi valori in una posizione sicura e condividerli solo con membri dell'azienda fidati che hanno bisogno di accedere allo strumento o accedere alle API Rest del cloud. L'ID client e la chiave segreta non scadono. Se sono compromessi, rimuoverli immediatamente utilizzando l'icona **Cestino** e crearne di nuovi.

> **Nota:**
>
> La chiave segreta non può essere recuperata se viene persa o dimenticata; è necessario creare un nuovo ID client e una chiave segreta.

### Compilare il file di informazioni sul cliente

L'utilizzo del file CustomerInfo.yml elimina la necessità di fornire i parametri delle informazioni sui clienti con l'esecuzione di ogni cmdlet. È possibile sovrascrivere qualsiasi informazione sul cliente utilizzando i parametri del cmdlet.

Creare il file CustomerInfo.yml utilizzando il cmdlet `New-CvadAcCustomerInfoFile`.

> **Importante:**
>
> Non modificare manualmente il file CustomerInfo.yml. Ciò potrebbe causare errori di formattazione involontari.

`New-CvadAcCustomerInfoFile` ha i seguenti parametri richiesti.

- CustomerId: ID cliente.
- ClientID: ID cliente creato su Citrix Cloud.
- Segreto: il segreto del cliente creato su Citrix Cloud.

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6
-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

È inoltre possibile creare CustomerInfo.yml utilizzando il parametro `SecurityCsvFileSpec` che punta al file security.csv scaricato. È inoltre necessario specificare il CustomerId.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name
\downloads/security.csv -CustomerId markhof123
```

Aggiornare il file CustomerInfo.yml utilizzando il cmdlet `Set-CvadAcCustomerInfoFile`. Questo cmdlet modifica solo l'ID client.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

Di seguito è riportato un esempio di file CustomerInfo.yml.

```
# Created/Updated on 2020/01/29 16:46:47
CustomerId: 'markhof123'
ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'
Secret: 'TwBLaaabbbaaaaaaaaaaw=='
Environment: Production
AltRootUrl: ''
StopOnError: False
AlternateFolder: ''
Locale: 'en-us'
Editor: 'C:\Program Files\Notepad++\notepad++.exe'
Confirm: True
DisplayLog: True
```

### Compilare il file di mappatura delle zone

Una zona locale è equivalente alla posizione di una risorsa cloud. A differenza di altri componenti del sito, non è possibile importare automaticamente l'area locale nel cloud. Questa deve essere invece mappata manualmente utilizzando il file ZoneMapping.yml. È possibile che si verifichino errori di importazione se il nome della zona non è associato a un nome di posizione risorsa esistente.

Per i siti locali con una sola zona e per i siti cloud che hanno una sola risorsa, lo strumento Automated Configuration crea l'associazione corretta, eliminando la necessità di gestire manualmente il file ZoneMapping.yml.

Per i siti locali con più zone o i siti cloud con più posizioni di risorse, il file ZoneMapping.yml deve essere aggiornato manualmente per riflettere la corretta mappatura delle zone locali alle posizioni delle risorse cloud. Questa operazione deve essere eseguita prima di tentare qualsiasi operazione di importazione nel cloud.

Il file ZoneMapping.yml si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*. Il contenuto del file.yml è un dizionario con il nome della zona come chiave e il nome della posizione della risorsa come valore.

Ad esempio, un sito Citrix Virtual Apps and Desktops on-premise con una zona primaria denominata "Zone-1"e una zona secondaria denominata "Zone-2"viene migrato a una distribuzione Citrix DaaS con due posizioni risorse cloud appena create denominate "Cloud-RL-1"e "Cloud-RL-2". In questo caso, ZoneMapping.yml verrà configurato come segue:

```
1               Zone-1: Cloud-RL-1
2
3               Zone-2: Cloud-RL-2
```

> **Nota:**
>
> Tra i due punti e il nome della posizione della risorsa deve essere presente uno spazio. Se vengono utilizzati spazi nel nome della zona o della posizione della risorsa, racchiudere il nome tra virgolette.

### Connessioni host

Le connessioni host e gli hypervisor associati possono essere esportati e importati utilizzando Automated Configuration.

L'aggiunta di un hypervisor a una connessione host richiede informazioni di sicurezza specifiche per il tipo di hypervisor. Queste informazioni non possono essere esportate dal sito locale per motivi di sicurezza. È necessario fornire manualmente le informazioni in modo che Automated Configuration possa importare correttamente le connessioni host e gli hypervisor nel sito cloud.

Il processo di esportazione crea il file CvadAcSecurity.yml nel percorso *%HOMEPATH%\Documents\Citrix\AutoConfig* contenente segnaposto per ogni elemento di protezione necessario per il tipo di hypervisor specifico. È necessario aggiornare il file CvadAcSecurity.yml prima di importarlo nel sito cloud. Gli aggiornamenti dell'amministratore vengono mantenuti su più esportazioni con nuovi segnaposto di sicurezza aggiunti secondo necessità. Gli elementi di sicurezza non vengono mai rimossi. Per ulteriori informazioni, vedere Manually update the CvadAcSecurity.yml file

```
            HostConn1:
            ConnectionType: XenServer
            UserName: root
            PasswordKey: rootPassword
            HostCon2:
            ConnectionType: AWS
            ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH
            SecretKey: TwBLaaaaaaaaaaaaaaaaw==
            Region: East
```

**Informazioni sulla sicurezza per ciascun hypervisor** Di seguito sono elencate le informazioni di sicurezza necessarie per ciascun tipo di hypervisor.

- XenServer, Hyper-V, VMware
  - Nome utente
  - Password in chiaro
- Microsoft Azure
  - ID sottoscrizione
  - ID applicazione
  - Segreto applicazione
- Amazon Web Services
  - ID account di servizio
  - Segreto applicazione
  - Regione

**Considerazioni speciali sulla sicurezza** Tutte le informazioni di sicurezza vengono inserite come testo non crittografato. Se il testo non crittografato non è consigliato, le connessioni host e gli hypervisor associati possono essere creati manualmente utilizzando l'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa). Le connessioni host e i nomi degli hypervisor devono corrispondere esattamente alle controparti locali in modo che i cataloghi di macchine che utilizzano le connessioni host possano essere importati correttamente.

### Attivare i siti

Il Delivery Controller nei siti on-premise e cloud controlla le risorse come i desktop di intermediazione, le applicazioni e il riavvio delle macchine. I problemi si verificano quando un insieme comune di risorse è controllato da due o più siti. Una situazione del genere può verificarsi durante la migrazione da un sito locale a un sito cloud. È possibile per i Delivery Controller on-premise e cloud gestire lo stesso set di risorse. Tale duplice gestione può comportare l'indisponibilità e l'ingestibilità delle risorse e può essere difficile da diagnosticare.

L'attivazione del sito consente di controllare dove è controllato il sito attivo.

L'attivazione del sito viene gestita utilizzando la modalità di manutenzione del gruppo di consegna. I gruppi di consegna vengono messi in modalità di manutenzione quando il sito è inattivo. La modalità di manutenzione viene rimossa dai gruppi di consegna per i siti attivi.

L'attivazione del sito non influisce sulla registrazione dei VDA o dei cataloghi delle macchine, né la gestisce.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

Tutti i cmdlet supportano `IncludeByName` e i `ExcludeByName` filtri. Questo parametro consente di selezionare quali gruppi di consegna possono modificare la modalità di manutenzione. I gruppi di consegna possono essere modificati in modo selettivo secondo necessità.

#### Importazione e trasferimento del controllo sul cloud

Di seguito è riportata una descrizione di alto livello su come importare e trasferire il controllo dal sito locale al sito cloud.

1. Esportare e importare il sito locale nel cloud. Accertarsi che il parametro `–SiteActive` non sia presente in nessuno dei cmdlet di importazione. Il sito locale è attivo e il sito cloud è inattivo. Per impostazione predefinita, i gruppi di distribuzione del sito cloud sono in modalità di manutenzione.
2. Verificare il contenuto e la configurazione del cloud.
3. Al di fuori delle ore di lavoro, impostare il sito locale su inattivo. Il parametro `–SiteActive` deve essere assente. Tutti i gruppi di consegna in loco sono in modalità di manutenzione.
    - `Set-CvadAcSiteActiveStateOnPrem`
4. Impostare il sito cloud su attivo. Il parametro `–SiteActive` deve essere presente. Nessun gruppo di distribuzione del sito cloud è in modalità di manutenzione.
    - `Set-CvadAcSiteActiveStateCloud –SiteActive`
5. Verificare che il sito cloud sia attivo e che il sito locale sia inattivo.

#### Trasferire di nuovo il controllo sul sito locale

Per trasferire il controllo dal sito cloud al sito locale:

1. Al di fuori delle ore di lavoro, impostare il sito cloud su inattivo. Tutti i gruppi di distribuzione del sito cloud sono in modalità di manutenzione.
   - `Set-CvadAcSiteActiveStateCloud`
2. Impostare il sito locale su attivo. Nessun gruppo di consegna locale è in modalità di manutenzione.
   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

#### Informazioni aggiuntive sull'attivazione del sito

- Se non è prevista la gestione dell'alimentazione per le macchine e non ci sono pianificazioni di riavvio (il che di solito significa che non ci sono nemmeno connessioni host), tutti i gruppi di consegna cloud possono essere importati come attivi. Aggiungere `-SiteActive` a `Merge-CvadAcToSite`/`Import-CvadAcToSite` o eseguire `Set-CvadAcSiteActiveStateCloud -SiteActive` dopo l'importazione.
- Se è prevista la gestione dell'alimentazione delle macchine o vi sono pianificazioni di riavvio, è necessario un processo diverso. Ad esempio, quando si passa da on-premise a cloud in questa situazione, impostare il sito on-premise su inattivo utilizzando `Set-CvadAcSiteActiveStateOnPrem`. Quindi, impostare il sito cloud su attivo utilizzando `Set-CvadAcSiteActiveStateCloud -SiteActive`.
- I cmdlet `Set-CvadAcSiteActiveStateOnPrem` e `Set-CvadAcSiteActiveStateCloud` vengono utilizzati anche per invertire il processo. Ad esempio, eseguire `Set-CvadAcSiteActiveState` senza il parametro `-SiteActive`, quindi eseguire `Set-CvadAcSiteActiveStateOnPrem` con il parametro `-SiteActive`.

### Informazioni sulla migrazione dei cataloghi con provisioning di Machine Creation Services

> **Nota:**
>
> Questa funzione è disponibile solo nelle versioni 3.0 e successive. Controllare la versione in uso utilizzando `Get-CvadAcStatus` in Automated Configuration.

I cataloghi di Machine Creation Services (MCS) creano due diversi tipi di cataloghi:

- Quando le modifiche apportate a una macchina vengono perse/ripristinate (comunemente nel sistema operativo del server, in cui vengono pubblicate le applicazioni), si tratta di un caso d'uso VDI/multisessione in pool

- Quando le modifiche apportate a una macchina vengono conservate durante il riavvio (comunemente nel sistema operativo del client con un utente dedicato); si tratta di un caso d'uso VDI statico

Il tipo di catalogo può essere confermato nel nodo catalogo in Citrix Studio e osservando il valore "Dati utente:"del catalogo.

> **Nota:**
>
> Non è possibile eseguire il backup di MCS dal cloud utilizzando Automated Configuration.

#### Cataloghi VDI/multisessione in pool

I cataloghi con "Dati utente: Discard"sono cataloghi VDI raggruppati e possono solo migrare l'immagine e la configurazione principali. Le macchine virtuali presenti in questi cataloghi non vengono migrate. Questo perché il ciclo di vita della macchina virtuale viene mantenuto dal sito da cui si sta importando, il che significa che ogni volta che i computer vengono accesi, il suo stato potrebbe cambiare. Ciò rende impossibile l'importazione poiché i dati di importazione per le macchine virtuali perdono rapidamente la sincronizzazione.

Quando si esegue la migrazione di questi cataloghi utilizzando lo strumento, vengono creati i metadati del catalogo e viene avviata la creazione dell'immagine principale, ma non vengono importate macchine.

Poiché la creazione di questo processo richiede più tempo maggiori sono le dimensioni dell'immagine principale, il comando di importazione all'interno dello strumento avvia solo la creazione del catalogo MCS e non attende il completamento. Una volta completata l'importazione, monitorare l'avanzamento della creazione del catalogo utilizzando l'interfaccia di gestione Full Configuration (Configurazione completa) nella distribuzione cloud.

Una volta creata l'immagine principale, è possibile eseguire il provisioning delle macchine. È necessario tenere conto delle considerazioni sulla capacità in quanto l'utilizzo locale potrebbe consumare capacità.

Tutti gli altri oggetti (gruppi di consegna/applicazioni/criteri e così via) che utilizzano quel catalogo possono essere importati e non devono attendere la creazione dell'immagine principale. Al termine della creazione del catalogo, è possibile aggiungere macchine al catalogo importato e quindi gli utenti possono avviare le proprie risorse.

> **Nota:**
>
> Utilizzare gli stessi comandi disponibili nello strumento per effettuare la migrazione dei cataloghi e di tutti gli altri oggetti.

### Cataloghi VDI statici

> **Nota:**
>
> Poiché questa operazione comporta l'importazione di dettagli di basso livello archiviati nel database, questo processo deve essere eseguito da una macchina che abbia accesso al database.

I cataloghi VDI statici eseguono la migrazione dell'immagine principale, delle configurazioni e di tutte le macchine virtuali. A differenza di quanto avviene nel caso d'uso dei VDI in pool, non è necessario creare immagini.

I VDA devono essere puntati sul connettore affinché possano registrarsi nel cloud.

Fare riferimento alla sezione Attivare i siti per rendere attivo il sito cloud, in modo che la pianificazione del riavvio, la gestione dell'alimentazione e altri elementi siano controllati dal cloud.

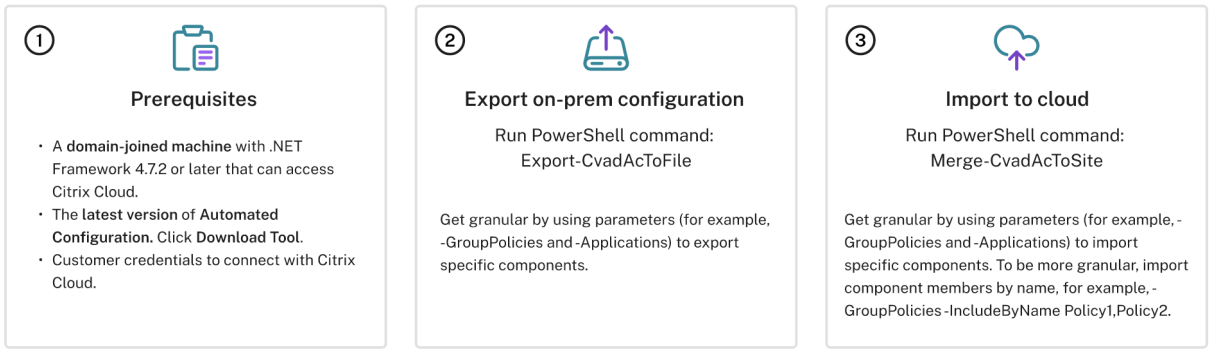
Una volta completata la migrazione, se si desidera eliminare questo catalogo dal sito locale, è necessario scegliere di lasciare la macchina virtuale e l'account AD. In caso contrario, vengono eliminati e il sito cloud rimarrebbe puntato sulla macchina virtuale eliminata.

## Migrazione da on-premise al cloud

October 30, 2023

Automated Configuration (Configurazione automatica) consente di automatizzare lo spostamento della configurazione on-premise su un sito cloud.

L'immagine seguente è una visione di alto livello di ciò che Automated Configuration (Configurazione automatica) può fare per migrare la configurazione al cloud.




### Prerequisiti per la migrazione della configurazione

Per *esportare* la configurazione da Citrix Virtual Apps and Desktops, è necessario:

- Citrix Virtual Apps and Desktops: versione attuale e rispettivo predecessore immediato o Citrix Virtual Apps and Desktops, XenApp e XenDesktop LTSR: tutte le versioni
- Un computer aggiunto al dominio con .NET Framework 4.7.2 o versione successiva e SDK Citrix PowerShell. Questo viene installato automaticamente sul Delivery Controller (per l'esecuzione su una macchina diversa dal Delivery Controller on-premise, è necessario installare Citrix Studio, poiché Studio installa gli snap-in PowerShell corretti. Il programma di installazione di Studio si trova sul supporto di installazione di Citrix Virtual Apps and Desktops).

Per *importare* la configurazione nel servizio Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops), è necessario quanto segue:

- Una macchina con accesso a Citrix Cloud. Non è necessario che sia un Delivery Controller o una macchina aggiunta al dominio.
- Citrix DaaS con il provisioning effettuato.
- Una posizione risorsa attiva con Connector installato e aggiunto al dominio nello stesso dominio della configurazione on-premise.
- La connettività ai siti che accedono a Citrix Cloud deve essere consentita e disponibile. Per ulteriori informazioni, vedere Requisiti di sistema e connettività.

> **Nota:**
>
> Automated Configuration (Configurazione automatica) non può essere installata su un sistema Cloud Connector. Se si esegue Automated Configuration su un server diverso dal Delivery Controller, è necessario utilizzare il parametro -AdminAddress e specificare il nome DNS o l'indirizzo IP del Delivery Controller. Ad esempio, `Export-CvadAcToFile -AdminAddress 192.168.0.10`

### Esportazione della configurazione on-premise di Citrix Virtual Apps and Desktops

> **Importante:**
>
> - È necessario disporre del file CustomerInfo.yml con il proprio ID cliente, dell'ID client e delle informazioni sulla chiave segreta incluse. Per ulteriori informazioni su come recuperare il proprio ID cliente, l'ID client e la chiave segreta, vedere Generare l'ID cliente, l'ID client e la chiave segreta. Per informazioni su come aggiungere queste informazioni al file CustomerInfo.yml, vedere Inserimento di dati nel file di informazioni dei clienti.
> - Il file ZoneMapping.yml deve includere informazioni che mappano la zona on-premise alle posizioni risorsa nel cloud. Per ulteriori informazioni su come mappare le zone, vedere Inserimento di dati nel file di mappatura delle zone.
> - Se si dispone di connessioni host, è necessario inserire le informazioni corrispondenti nel file CvadAcSecurity.yml.

1. Installare Automated Configuration (Configurazione automatica).

2. Fare doppio clic sull'icona **Auto Config**. Viene visualizzata una finestra di PowerShell.
3. Eseguire il comando seguente per esportare tutti i componenti. L'esportazione della configurazione on-premise *non* la modifica in alcun modo.

   ```
   Export-CvadAcToFile
   ```

Dopo aver eseguito qualsiasi cmdlet per la prima volta, viene creata una cartella di esportazione con i file di configurazione .yml e i log. La cartella si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*. Ogni esportazione successiva crea una sottocartella. La cartella principale *%HOMEPATH%\Documents\Citrix\AutoCo* contiene sempre i file esportati dall'esportazione più recente.

> **Nota:**
>
> Se Automated Configuration (Configurazione automatica) non è installato sul Delivery Controller, eseguire `import-module Citrix.AutoConfig.Commands` prima di utilizzare lo strumento tramite PowerShell. Questo passaggio non è necessario se si apre Automated Configuration (Configurazione automatica) utilizzando l'icona **Auto Config** (Configurazione automatica).

In caso di errori o eccezioni, vedere la sezione **Fixups** (Correzioni) nel file di log.

## Importare la configurazione in Citrix DaaS

> **Importante:**
>
> - È necessario disporre del file CustomerInfo.yml con il proprio ID cliente, dell'ID client e delle informazioni sulla chiave segreta incluse. Per ulteriori informazioni su come recuperare il proprio ID cliente, l'ID client e la chiave segreta, vedere Generare l'ID cliente, l'ID client e la chiave segreta. Per informazioni su come aggiungere queste informazioni al file CustomerInfo.yml, vedere Inserimento di dati nel file di informazioni dei clienti.
> - Il file ZoneMapping.yml deve includere informazioni che mappano la zona on-premise alle posizioni delle risorse nel cloud. Per ulteriori informazioni su come mappare le zone, vedere Inserimento di dati nel file di mappatura delle zone.
> - Se si dispone di connessioni host, è necessario inserire le informazioni corrispondenti nel file CvadAcSecurity.yml.

### Eseguire un'importazione

1. Fare doppio clic sull'icona **Auto Config**. Viene visualizzata una finestra di PowerShell.
2. Eseguire il comando seguente per importare tutti i componenti.

   ```
   Merge-CvadAcToSite
   ```

Verificare lo stato previsto con il nuovo stato corrente. Diverse opzioni di importazione controllano se i risultati dell'importazione sono identici o un sottoinsieme del sito on-premise.

Dopo aver eseguito il cmdlet, viene creata una cartella di esportazione con i file di configurazione .yml e i log. La cartella si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

In caso di errori o eccezioni, vedere la sezione **Fixups** (Correzioni) nel file di log.

> **Nota:**
>
> Se Automated Configuration (Configurazione automatica) non è installato sul Delivery Controller, eseguire `import-module Citrix.AutoConfig.Commands` prima di utilizzare lo strumento tramite PowerShell. Questo passaggio non è necessario se si apre Automated Configuration (Configurazione automatica) utilizzando l'icona **Auto Config** (Configurazione automatica).

Per ripristinare la configurazione originale di Citrix DaaS, consultate Eseguire il backup della configurazione Citrix DaaS.

### Operazione di importazione in dettaglio

Il processo di importazione è progettato per eseguire con precisione gli aggiornamenti, eseguire solo gli aggiornamenti necessari e verificare che tutti gli aggiornamenti siano stati effettuati correttamente. Di seguito sono riportati i passaggi da seguire in tutte le operazioni di importazione.

1. Leggere il file .yml esportato (stato previsto).
2. Leggere il cloud (stato attuale).
3. Eseguire il backup dello stato di pre-importazione del cloud in file .yml (il pre-backup può essere ripristinato, se necessario).
4. Valutare le differenze tra lo stato previsto e quello attuale. Questo determina quali aggiornamenti effettuare.
5. Effettuare gli aggiornamenti.
6. Leggere nuovamente il cloud (nuovo stato attuale).
7. Eseguire il backup dello stato post-importazione del cloud in file .yml (il post-backup può essere ripristinato, se necessario).
8. Confrontare il nuovo stato attuale con lo stato previsto.
9. Segnalare i risultati del confronto.

### Migrazione granulare

> **Importante:**
>
> Per ulteriori informazioni sull'ordine di migrazione dei componenti, vedere Ordine di migrazione dei componenti.

È possibile migrare in modo selettivo solo i componenti o anche solo i nomi dei componenti.

- I parametri dei componenti supportati includono `MachineCatalogs`, `Tags` e altri ancora.
- I parametri del nome dei componenti supportati includono `IncludeByName`, `ExcludeByName` e altri ancora.

Per ulteriori informazioni sui parametri e su come utilizzarli, vedere Parametri di migrazione granulare.

### Attivare i siti

L'attivazione del sito consente di controllare quale sito è attivo e controlla le risorse. Per ulteriori informazioni, vedere Attivare i siti.

## Unire più siti in un unico sito

October 30, 2023

Il supporto multi-sito per Automated Configuration (Configurazione automatica) fornisce un metodo per unire più siti on-premise in un unico sito cloud.

Il supporto multi-sito aggiunge prefissi e suffissi univoci ai nomi dei componenti in base al sito on-premise, garantendo l'univocità dei nomi dopo l'unione di più siti on-premise in un unico sito cloud.

I prefissi e i suffissi possono essere assegnati per ciascuno dei seguenti componenti in base al sito on-premise.

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`

- HostConnection
- MachineCatalog
- StoreFront
- Tag

Le cartelle delle applicazioni supportano i prefissi, i suffissi e il rerooting. Il rerooting aggiunge una cartella aggiuntiva di primo livello alla struttura di cartelle esistente di un'applicazione.

### Regole per prefissi e suffissi

1. I prefissi e i suffissi non possono contenere nessuno dei seguenti caratteri speciali: `\ , / ; : # . * ? = < > | ( )"' { } [ ]`
2. I prefissi e i suffissi possono contenere spazi finali ma non spazi iniziali.
3. I prefissi e i suffissi devono essere racchiusi tra virgolette doppie per contenere spazi finali.
4. I prefissi e i suffissi vengono applicati al momento dell'importazione, dell'unione e dell'aggiunta. I file .yml di origine non vengono mai modificati.
5. Il processo relativo ai prefissi e ai suffissi aggiunge automaticamente prefissi o suffissi ai nomi dei componenti dipendenti, se applicabile. Ad esempio, se i nomi dei cataloghi delle macchine hanno il prefisso "Est", anche i gruppi di consegna a cui fanno riferimento hanno il prefisso "Est".
6. Se il nome di un componente inizia già con il prefisso o il suffisso, non viene aggiunto alcun prefisso o suffisso. I nomi dei componenti non possono contenere prefissi o suffissi doppi identici.
7. I prefissi e i suffissi possono essere utilizzati singolarmente o in combinazione.
8. L'uso di un prefisso o di un suffisso su un componente è facoltativo.

> **Nota:**
>
> L'interfaccia Full Configuration (Configurazione completa) visualizza i componenti in ordine alfabetico.

#### Raggruppare per sito

Utilizzare i prefissi per raggruppare visivamente i componenti di un singolo sito. Ogni sito è elencato nel proprio gruppo con prefissi in ordine alfabetico, che controllano l'ordinamento dei diversi gruppi del sito.

#### Raggruppare per nome

Utilizzare i suffissi per raggruppare visivamente componenti di più siti con nomi simili. I componenti con nomi simili provenienti da siti diversi si alternano visivamente.

#### File SiteMerging.yml

L'aggiunta di prefissi ai siti inizia con il file SiteMerging.yml, che contiene la mappatura dei prefissi e dei suffissi dei siti per uno o più siti on-premise. È possibile gestire il file SiteMerging.yml manualmente oppure utilizzando i cmdlet disponibili elencati nella sezione Unione di più cmdlet di siti on-premise.

#### Esportazione, importazione, unione e aggiunta

L'unione non può iniziare finché non si è esportato un sito on-premise. Per esportare un sito on-premise, vedere Migrazione da on-premise a cloud.

#### Cartella di destinazione dell'esportazione centrale

I metodi descritti in questa sezione collocano più esportazioni di siti in una posizione centrale di condivisione file. Il file SiteMerging.yml, il file CustomerInfo.yml e tutti i file di esportazione risiedono in tale posizione di condivisione file, consentendo di eseguire l'importazione da un'unica posizione indipendente dai siti on-premise.

Le operazioni di accesso al cloud non fanno mai riferimento ai siti on-premise o ad Active Directory, consentendo quindi di eseguire operazioni di accesso al cloud da qualsiasi luogo.

### Condivisione diretta dei file

Le operazioni di esportazione, importazione, unione e novità/aggiunta forniscono un parametro per la destinazione o l'origine di una cartella diversa dalla cartella predefinita, *%HOMEPATH%\Documents\Citrix\AutoConfig*. Gli esempi seguenti utilizzano una condivisione file centrale situata in `\\share.central.net`, a cui l'amministratore ha già accesso, avendo fornito le credenziali necessarie.

Per indirizzare l'esportazione in una cartella specifica del sito, utilizzare il parametro `–TargetFolder` :

Dal DDC Est:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteEast
```

Dal DDC Ovest:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteWest
```

Una volta completate le esportazioni, creare i file CustomerInfo.yml e SiteMerging.yml e inserirli in `\\share.central.net\AutoConfig`.

> **Nota:**
>
> Non utilizzare il parametro `SiteRootFolder` durante la creazione del file SiteMerging.yml quando si utilizza questo metodo di riferimento per la condivisione diretta di file.

Per importare, unire o aggiungere dalla condivisione diretta di file, è necessario decidere da quale macchina si desidera eseguire l'operazione di accesso al cloud. Le opzioni includono:

- Uno dei DDC on-premise in cui lo strumento è già installato.
- La macchina che ospita la condivisione file.
- Una macchina diversa.

Automated Configuration (Configurazione automatica) deve essere installato sulla macchina che accede al cloud. Non vengono utilizzati né l'SDK PowerShell on-premise, né il DDC né Active Directory, quindi i requisiti di esecuzione per l'accesso al cloud sono più semplici dei requisiti di esportazione.

Per unire il DDC Est al cloud:

```
Merge-CvadAcToSite –SiteName East –SourceFolder \\share.central.
net\AutoConfig\SiteEast -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

Per unire il DDC Ovest al cloud:

```
Merge-CvadAcToSite –SiteName West –SourceFolder \\share.central.
net\AutoConfig\SiteWest -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

Di seguito è riportato un esempio di file SiteMerging.yml utilizzato nell'esempio precedente.

```
1     East:
2       SiteRootFolder: "" # Important: leave this empty
3       AdminScopePrefix: "East_"
4       AdminRolePrefix: "East_"
5       ApplicationAdminPrefix: "East_"
6       ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
7       ApplicationFolderRoot: "East"
8       ApplicationGroupPrefix: "East_"
9       ApplicationUserPrefix: "East_"
10      DeliveryGroupPrefix: "East_"
11      GroupPolicyPrefix: "East_"
12      HostConnectionPrefix: "East_"
13      MachineCatalogPrefix: "East_"
```

```
14        StoreFrontPrefix: "East_"
15        TagPrefix: "East_"
16        AdminScopeSuffix: "_east"
17        AdminRoleSuffix: "_east"
18        ApplicationAdminSuffix: "_east"
19        ApplicationFolderSuffix: "_east"
20        ApplicationGroupSuffix: "_east"
21        ApplicationUserSuffix: "_east"
22        DeliveryGroupSuffix: "_east"
23        GroupPolicySuffix: "_east"
24        HostConnectionSuffix: "_east"
25        MachineCatalogSuffix: "_east"
26        StoreFrontSuffix: "_east"
27        TagSuffix: "_east"
28      West:
29        SiteRootFolder: "" # Important: leave this empty
30        AdminScopePrefix: "Western "
31        AdminRolePrefix: "Western "
32        ApplicationAdminPrefix: "Western "
33        ApplicationFolderPrefix: "" # Note that a new parent root folder
              is used instead
34        ApplicationFolderRoot: "Western"
35        ApplicationGroupPrefix: "Western "
36        ApplicationUserPrefix: "Western "
37        DeliveryGroupPrefix: "Western "
38        GroupPolicyPrefix: "Western "
39        HostConnectionPrefix: "Western "
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        TagSuffix: ""
```

### Riferimento alla condivisione file utilizzando SiteMerging.yml

Questo metodo utilizza il membro `SiteRootFolder` del set di prefissi del sito. Sebbene sia più complesso del metodo di condivisione diretta dei file, questo metodo riduce le probabilità di indirizzare la cartella sbagliata durante l'esportazione, l'importazione, l'unione o l'aggiunta.

Per prima cosa, impostare `SiteRootFolder` per ogni sito nel file SiteMerging.yml. È necessario eseguire questa operazione nella posizione condivisa.

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \\share.
central.net\AutoConfig\SiteEast -TargetFolder \\share.central.net\
AutoConfig

New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest -
TargetFolder \\share.central.net\AutoConfig
```

In questo esempio, Est è una specifica di cartella completa e Ovest è una specifica di cartella relativa.

Per indirizzare l'esportazione a una cartella specifica del sito utilizzando il file SiteMerging.yml:

Dal DDC Est:

```
mkdir \\share.central.net\AutoConfig\SiteEast

Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Dal DDC Ovest:

```
mkdir \\share.central.net\AutoConfig\SiteWest

Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Il cmdlet di esportazione utilizza la posizione della cartella CustomerInfo.yml per individuare il file SiteMerging.yml. Nel caso di Est, `SiteRootFolder` è completo. È utilizzato così com'è. Nel caso di Ovest, `SiteRootFolder` non è completo. È combinato con la posizione della cartella CustomerInfo.yml per recuperare una posizione di cartella completa per Ovest.

Per unire il DDC Est al cloud:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Per unire il DDC Ovest al cloud:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Di seguito è riportato un esempio di file SiteMerging.yml utilizzato nell'esempio precedente.

```
1       East:
2       SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"
3       AdminScopePrefix: "East_"
4       AdminRolePrefix: "East_"
5       ApplicationAdminPrefix: "East_"
6       ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
7       ApplicationFolderRoot: "East"
8       ApplicationGroupPrefix: "East_"
9       ApplicationUserPrefix: "East_"
```

```
10        DeliveryGroupPrefix: "East_"
11        GroupPolicyPrefix: "East_"
12        HostConnectionPrefix: "East_"
13        MachineCatalogPrefix: "East_"
14        StoreFrontPrefix: "East_"
15        TagPrefix: "East_"
16        AdminScopeSuffix: "_east"
17        AdminRoleSuffix: "_east"
18        ApplicationAdminSuffix: "_east"
19        ApplicationFolderSuffix: "_east"
20        ApplicationGroupSuffix: "_east"
21        ApplicationUserSuffix: "_east"
22        DeliveryGroupSuffix: "_east"
23        GroupPolicySuffix: "_east"
24        HostConnectionSuffix: "_east"
25        MachineCatalogSuffix: "_east"
26        StoreFrontSuffix: "_east"
27        TagSuffix: "_east"
28      West:
29        SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
30        AdminScopePrefix: "Western "
31        AdminRolePrefix: "Western "
32        ApplicationAdminPrefix: "Western "
33        ApplicationFolderPrefix: "" # Note that a new parent root folder
              is used instead
34        ApplicationFolderRoot: "Western"
35        ApplicationGroupPrefix: "Western "
36        ApplicationUserPrefix: "Western "
37        DeliveryGroupPrefix: "Western "
38        GroupPolicyPrefix: "Western "
39        HostConnectionPrefix: "Western "
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        TagSuffix: ""
```

Se non viene utilizzato un metodo di condivisione file centrale e l'importazione, l'unione o l'aggiunta vengono eseguite dai singoli DDC, creare e replicare il file SiteMerging.yml su ogni DDC che viene migrato nel cloud. Il percorso predefinito è *%HOMEPATH%\Documents\Citrix\AutoConfig*. È necessario specificare il parametro `–SiteName` per selezionare i prefissi del sito corretti.

### Unire i siti

Citrix consiglia di eseguire le operazioni cloud in passaggi e di eseguire una revisione completa di ogni risultato prima di eseguire la successiva operazione cloud. Ad esempio, se si uniscono tre siti in un unico sito cloud:

1. Unire il sito iniziale al cloud utilizzando il valore `SiteName` appropriato.
2. Esaminare i risultati nell'interfaccia di gestione Full Configuration (Configurazione completa).
3. Se i risultati non sono corretti, determinare il problema e la relativa causa, correggerlo e quindi eseguire nuovamente l'unione. Se necessario, rimuovere i componenti cloud e iniziare da zero utilizzando `Remove-CvadAcFromSite` per il componente e i membri selezionati. Se i risultati sono corretti, continuare.
4. Se l'unione iniziale è corretta, unire il secondo sito al singolo sito cloud.
5. Ripetere i passaggi 2 e 3.
6. Se la seconda unione è corretta, unire il terzo sito al singolo sito cloud.
7. Ripetere i passaggi 2 e 3.
8. Esaminare le risorse dal punto di vista dell'utente e verificare che la visualizzazione sia nello stato desiderato.

#### Rimuovere un componente utilizzando il prefisso del sito

È possibile rimuovere in modo selettivo i componenti di un sito utilizzando il prefisso sul parametro `–IncludeByName` del cmdlet `Remove-CvadAcFromSite`. Nell'esempio seguente, i gruppi di consegna del DDC Ovest non sono corretti. Per rimuovere i gruppi di consegna solo per il sito Ovest:

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”
```

Per rimuovere tutti i componenti Ovest, eseguire i seguenti cmdlet in ordine.

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “Western *”
Remove-CvadAcFromSite –Applications –IncludeByName “Western *”
Remove-CvadAcFromSite – ApplicationGroups –IncludeByName “Western *”
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”
Remove-CvadAcFromSite –MachineCatalogs –IncludeByName “Western *”
Remove-CvadAcFromSite –HostConnections –IncludeByName “Western *”
Remove-CvadAcFromSite –Tags –IncludeByName “Western *”
```

Per rimuovere i criteri di gruppo dei componenti Est, utilizzare il suffisso:

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “*_east”
```

# Migrazione dal cloud al cloud

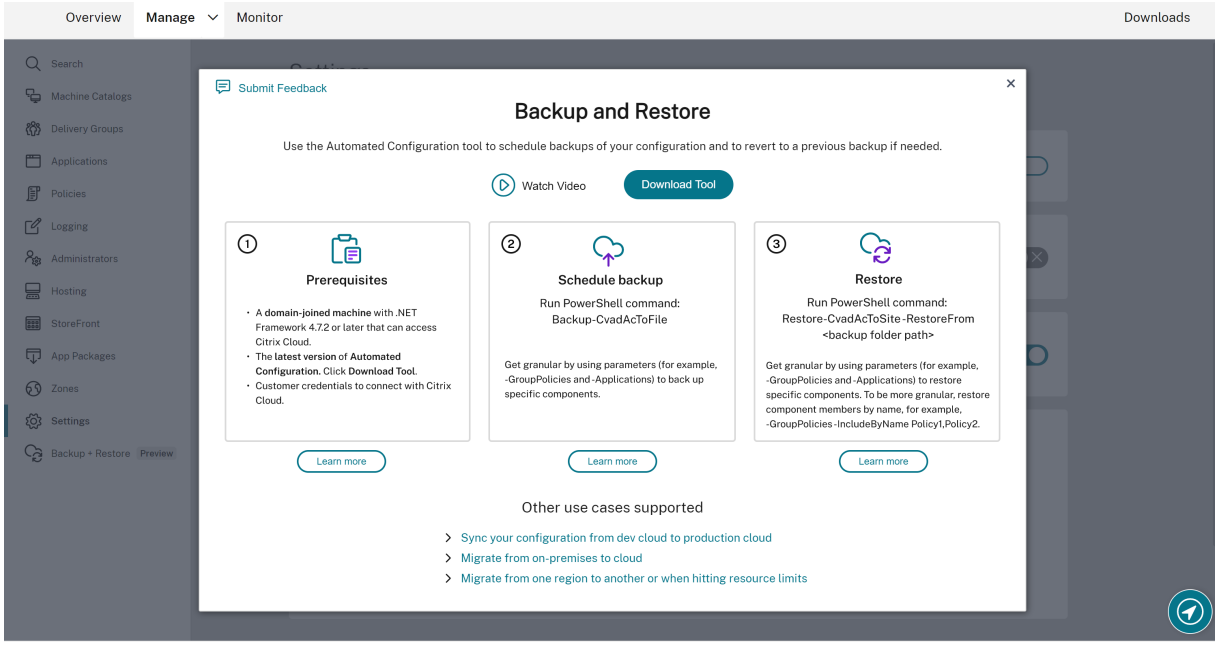
October 6, 2022

Automated Configuration (Configurazione automatica) consente di automatizzare lo spostamento della configurazione cloud su un altro sito cloud o di ripristinare il proprio sito cloud.

L'utilizzo di Automated Configuration (Configurazione automatica) può risolvere molti casi d'uso:

- Sincronizzazione del sito dalla fase di test o di staging alla fase di produzione
- Effettuare il backup e ripristinare la configurazione
- Raggiungere i limiti delle risorse
- Migrare da una regione all'altra

In Full Configuration (Configurazione completa) su Citrix Cloud, vedere il nodo Backup and Restore (Backup e ripristino) per informazioni su Automated Configuration (Configurazione automatica) e su come può essere utilizzata per migrare la configurazione dal cloud al cloud.




## Prerequisiti per la migrazione della configurazione

Per eseguire il backup e il ripristino della configurazione, è necessario:

- Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops) con il provisioning eseguito.
- Una posizione risorsa attiva con Connector installato.
- La connettività ai siti che accedono a Citrix Cloud deve essere consentita e disponibile. Per ulteriori informazioni, vedere Requisiti di sistema e connettività.

> **Nota:**
>
> Non è possibile eseguire il backup di MCS dal cloud utilizzando Automated Configuration.

### Eseguire il backup della configurazione Citrix DaaS

> **Importante:**
>
> - È necessario disporre del file CustomerInfo.yml con il proprio ID cliente, dell'ID client e delle informazioni sulla chiave segreta incluse. Per ulteriori informazioni su come recuperare il proprio ID cliente, l'ID client e la chiave segreta, vedere Generare l'ID cliente, l'ID client e la chiave segreta. Per informazioni su come aggiungere queste informazioni al file CustomerInfo.yml, vedere Inserimento di dati nel file di informazioni dei clienti.
> - Il file ZoneMapping.yml deve includere informazioni che mappano le posizioni risorsa nel cloud. Per ulteriori informazioni su come mappare le zone, vedere Inserimento di dati nel file di mappatura delle zone.
> - Se si dispone di connessioni host, è necessario inserire le informazioni corrispondenti nel file CvadAcSecurity.yml.

1. Installare Automated Configuration (Configurazione automatica).

   > **Nota:**
   >
   > Per la migrazione da cloud a cloud, Automated Configuration (Configurazione automatica) può essere installata su una macchina con accesso a Internet a cui l'amministratore ha accesso diretto.

2. Fare doppio clic sull'icona **Auto Config**. Viene visualizzata una finestra di PowerShell.
3. Utilizzare il comando seguente per eseguire un backup.

   ```
   Backup-CvadAcToFile
   ```

Dopo aver eseguito qualsiasi cmdlet per la prima volta, viene creata una cartella di esportazione con i file di configurazione .yml e i log. La cartella si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

In caso di errori o eccezioni, vedere la sezione **Fixups** (Correzioni) nel file di log.

### Ripristinare la configurazione su Citrix DaaS

1. Fare doppio clic sull'icona **Auto Config**. Viene visualizzata una finestra di PowerShell.
2. Utilizzare il comando seguente per eseguire un ripristino.

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```

Verificare lo stato previsto con il nuovo stato corrente.

Dopo aver eseguito il cmdlet, viene creata una cartella di esportazione con i file di configurazione .yml e i log. La cartella si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

In caso di errori o eccezioni, vedere la sezione **Fixups** (Correzioni) nel file di log.

Il processo di backup e ripristino protegge da modifiche o danneggiamenti involontari della configurazione del sito cloud. Mentre Automated Configuration (Configurazione automatica) esegue backup ogni volta che viene apportata una modifica, questo backup riflette lo stato della configurazione del sito cloud prima delle modifiche. Per proteggersi è necessario eseguire periodicamente il backup della configurazione del sito cloud e salvarlo in un luogo sicuro. Se si verifica una modifica o un danneggiamento indesiderati, il backup può essere utilizzato per correggere la modifica o il danneggiamento a livello di configurazione del sito completo o granulare.

## Migrazione granulare

> **Importante:**
>
> Per ulteriori informazioni sull'ordine di migrazione dei componenti, vedere Ordine di migrazione dei componenti.

### Ripristino di interi componenti

Il ripristino di un componente comporta la selezione di uno o più parametri del componente.

Per ripristinare l'intero gruppo di consegna e i componenti del catalogo delle macchine, seguire questo esempio:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

### Ripristino dei membri dei componenti

Il ripristino di uno o più membri dei componenti utilizza la funzionalità `IncludeByName`. Il cmdlet `Restore` viene richiamato con il parametro `RestoreFolder` insieme al singolo componente selezionato e all'elenco di inclusione.

Per ripristinare due criteri di gruppo da un backup, seguire questo esempio:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss

-GroupPolicies -IncludeByName Policy1,Policy2

-DeliveryGroups -MachineCatalogs
```

#### Ripristino dell'intera configurazione del sito cloud

Ripristinare la configurazione completa del sito cloud significa selezionare tutti i componenti da ripristinare.

Per ripristinare l'intera configurazione del sito cloud, seguire questo esempio:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

### Attivare i siti

L'attivazione del sito consente di controllare quale sito è attivo e controlla le risorse. Per ulteriori informazioni, vedere Attivare i siti.

## Cmdlet dello strumento Automated Configuration

October 30, 2023

Questa pagina elenca tutti i cmdlet e i parametri supportati dallo strumento.

Tutti i cmdlet accettano parametri con uno dei seguenti tipi.

- Stringa
- Elenco di stringhe
- Booleano: `$true` o `$false`
- SwitchParameter: presenza del parametro significa `$true`; assenza del parametro significa `$false`

> **Nota:**
>
> SwitchParameter è il metodo preferito per le selezioni true o false, ma le variabili booleane sono ancora utilizzate nello strumento a causa di problemi legacy.

La tabella seguente è un riepilogo di tutti i cmdlet. Vedere ogni singola sezione per scoprire quali parametri sono supportati da ciascun cmdlet.

| Categoria | Cmdlet | Descrizione |
|---|---|---|
| Migrazione da on-premise al cloud | `Export-CvadAcToFile` | Esportare file on-premise in file YAML. |

| Categoria | Cmdlet | Descrizione |
| --- | --- | --- |
| | | `Import-CvadAcToSite`<br>`Merge-CvadAcToSite`<br>`New-CvadAcToSite`<br>`Sync-CvadAcToSite`<br>*Migrazione granulare* Per i componenti, utilizzare i parametri con i comandi indicati sopra. Esempi: `MachineCatalogs`, `Tags`. Per i nomi dei componenti, utilizzare i parametri con i comandi indicati sopra. Esempi: `IncludeByName`, `ExcludeByName`. |
| Cmdlet da cloud a cloud | `Backup-CvadAcToFile` | Esegue il backup di tutta la configurazione dal sito cloud.<br>`Restore-CvadAcToSite`<br>`Remove-CvadAcFromSite`<br>*Migrazione granulare* Per i componenti, utilizzare i parametri con i comandi indicati sopra. Esempi: `MachineCatalogs`, `Tags`. Per i nomi dei componenti, utilizzare i parametri con i comandi indicati sopra. Esempi: `IncludeByName`, `ExcludeByName`. |
| Altri cmdlet di base | `Compare-CvadAcToSite` | Confronta i file .yml on-premise con la configurazione cloud. |
| Cmdlet relativi ai prerequisiti | `New-CvadAcCustomerInfoFile` | Creare un file di informazioni dei clienti. |

| Categoria | Cmdlet | Descrizione |
| --- | --- | --- |
| | | Set-CvadAcCustomerInfoFile |
| Cmdlet per assistenza e risoluzione dei problemi | New-CvadAcZipInfoForSupport | Comprime tutti i file di log e i file .yml in un unico file zip da inviare a Citrix per assistenza. |
| | | Get-CvadAcStatus |
| | | Test-CvadAcConnectionWithSite |
| | | Find-CvadAcConnector |
| | | Get-CvadAcCustomerSites |
| | | New-CvadAcTemplateToFile |
| | | Show-CvadAcDocument |
| | | Find-CvadAcInFile |
| Cmdlet per l'attivazione del sito | Set-CvadAcSiteActiveStateOnPrem | Imposta lo stato del sito on-premise su attivo o inattivo. |
| | | Set-CvadAcSiteActiveStateCloud |
| Unione di più cmdlet di siti on-premise | New-CvadAcSiteMergingInfo | Crea un set di informazioni prefisso/suffisso per l'unione dei siti. |
| | | Set-CvadAcSiteMergingInfo |
| | | Remove-CvadAcSiteMergingInfo |

Per ulteriori informazioni sui parametri e su come utilizzarli, vedere Parametri di migrazione granulare.

### Cmdlet di base

#### Cmdlet da on-premise a cloud

- `Export-CvadAcToFile` - Esporta file on-premise in file YAML.

  Esporta la configurazione dalla configurazione on-premise. Questa è l'operazione di esportazione predefinita per Automated Configuration. Non vengono apportate modifiche alla configurazione del sito on-premise. I file esportati vengono inseriti nella directory *%HOMEPATH%\Documents\Citrix\AutoConfig* in una sottocartella dal nome univoco **Export** (Esporta). La cartella *%HOMEPATH%\Documents\Citrix\AutoConfig* contiene sempre l'ultima configurazione del sito on-premise esportata.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti | | Elenco di stringhe |
| `TargetFolder` | Specifica la cartella di destinazione dell'esportazione. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `AdminAddress` | Specifica l'indirizzo DNS o IP del Delivery Controller quando l'esportazione non viene eseguita sul Delivery Controller. | | Stringa |
| `CheckUserAndMachines` | Verifica se gli utenti e le macchine si trovano in Active Directory. Gli utenti e le macchine che non si trovano in Active Directory potrebbero causare errori di importazione. | | `$true` o `$false` |
| `ZipResults` | Comprime il backup dei file YAML in un unico file zip. Il file si trova nella stessa cartella dei file YAML di cui è stato eseguito il backup e ha lo stesso nome della cartella. | | SwitchParameter |

  Restituisce:

  - Vedere Valori restituiti dai cmdlet

Esistono tre modi per importare dati nel cloud. L'esecuzione di cmdlet specifici può produrre una delle tre combinazioni di azioni seguenti sul sito cloud:

- Add (Aggiungi), Update (Aggiorna) e Delete (Elimina)
- Solo Add (Aggiungi) e Update (Aggiorna)
- Solo Add (Aggiungi)

| Cmdlet | Add (Aggiungi) | Aggiornamento | Delete (Elimina) |
|---|---|---|---|
| Import (Importa) | X | X | X |
| Merge (Unisci) | X | X | |
| New (Nuovo) | X | | |

- `Import-CvadAcToSite` - Importare file YAML nel cloud. Supporta operazioni di creazione, aggiornamento ed eliminazione.

  Importa tutti i file on-premise nel cloud. Questo comando garantisce che lo stato finale del cloud sia identico allo stato on-premise. Questa opzione elimina tutte le modifiche esistenti nel cloud. I file di configurazione del sito importati provengono da *%HOMEPATH%\Documents\Citrix\AutoConfig*. *Da usare con cautela.*

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti. | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti. | | Elenco di stringhe |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud. | | SwitchParameters |
| `SourceFolder` | Identifica una cartella principale sostitutiva per *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `Merge` | Se impostato su `$true`, aggiunge componenti solo al sito cloud. I componenti non vengono rimossi. Impostare su `$false` per rimuovere i componenti. | | `$true` o `$false` |
| `AddOnly` | Se impostato su `$true`, aggiunge solo nuovi componenti, non aggiorna né elimina i componenti esistenti. Impostare su `$false` per consentire aggiornamenti ed eliminazioni. `Merge` viene ignorato quando questo parametro è `$true`. | | `$true` o `$false` |
| `MergePolicies` | Unire impostazioni e filtri dei criteri. L'unione avviene solo quando un criterio importato esiste già nel DDC cloud. Il risultato dell'unione dei criteri è che i criteri DDC cloud contengono le impostazioni e i filtri già presenti, in aggiunta a eventuali nuovi filtri e impostazioni importati. Tenere presente che quando si verificano conflitti tra impostazioni e filtri, i valori importati hanno la precedenza. | | SwitchParameter |
| `OnErrorAction` | Vedere OnErrorAction parameter. | | Stringa |

Restituisce:

- Vedere Valori restituiti dai cmdlet

- `Merge-CvadAcToSite` - Importare file YAML nel cloud. Supporta operazioni di creazione e aggiornamento.

  Unisce i file on-premise nel cloud, ma *non* elimina alcun componente nel cloud o nel sito on-premise. In questo modo vengono conservate le modifiche già apportate nel cloud. Se in Citrix Cloud esiste un componente con lo stesso nome, questo comando può modificare quel componente. Questa è l'operazione di importazione predefinita per Automated Configuration. I file di configurazione del sito uniti provengono da *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti. | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti. | | Elenco di stringhe |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud. | | SwitchParameters |
| `SourceFolder` | Identifica una cartella principale sostitutiva per *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |
| `Merge` | Se impostato su `$true`, aggiunge componenti solo al sito cloud. I componenti non vengono rimossi. Impostare su `$false` per rimuovere i componenti. | | `$true` o `$false` |
| `AddOnly` | Se impostato su `$true`, aggiunge solo nuovi componenti, non aggiorna né elimina i componenti esistenti. Impostare su `$false` per consentire aggiornamenti ed eliminazioni. `Merge` viene ignorato quando questo parametro è `$true`. | | `$true` o `$false` |
| `MergePolicies` | Unire impostazioni e filtri dei criteri. L'unione avviene solo quando un criterio importato esiste già nel DDC cloud. Il risultato dell'unione dei criteri è che i criteri DDC cloud contengono le impostazioni e i filtri già presenti, in aggiunta a eventuali nuovi filtri e impostazioni importati. Tenere presente che quando si verificano conflitti tra impostazioni e filtri, i valori importati hanno la precedenza. | | SwitchParameter |
| `OnErrorAction` | Vedere OnErrorAction parameter. | | Stringa |

Restituisce:

  - Vedere Valori restituiti dai cmdlet

- `New-CvadAcToSite` - Importare file YAML nel cloud. Supporta operazioni di creazione e aggiornamento.

  Importa la configurazione del sito on-premise nel cloud ma aggiunge solo nuovi componenti. I componenti esistenti del sito cloud non vengono né aggiornati né eliminati. Utilizzare questo comando se i componenti esistenti del sito cloud devono rimanere invariati.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti. | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti. | | Elenco di stringhe |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud. | | SwitchParameters |
| `SourceFolder` | Identifica una cartella principale sostitutiva per *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |
| `OnErrorAction` | Vedere OnErrorAction parameter. | | Stringa |

  Restituisce:

  - Vedere Valori restituiti dai cmdlet

- `Sync-CvadAcToSite` - Esportare e importare in un unico passaggio.

  Sync esegue sia l'esportazione che l'importazione in un unico passaggio. Utilizzare il parametro `SourceTargetFolder` per specificare la cartella di destinazione di esportazione/importazione.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti | | Elenco di stringhe |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud | | SwitchParameters |
| `SourceTargetFolder` | Specifica la cartella di destinazione per l'esportazione/importazione. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `AdminAddress` | Specifica l'indirizzo DNS o IP del Delivery Controller quando l'esportazione non viene eseguita sul Delivery Controller. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |
| `Merge` | Se impostato su `$true`, aggiunge componenti solo al sito cloud. I componenti non vengono rimossi. Impostare su `$false` per rimuovere i componenti. | | `$true` o `$false` |
| `AddOnly` | Se impostato su `$true`, aggiunge solo nuovi componenti, non aggiorna né elimina i componenti esistenti. Impostare su `$false` per consentire aggiornamenti ed eliminazioni. `Merge` viene ignorato quando questo parametro è `$true`. | | `$true` o `$false` |
| `MergePolicies` | Unire impostazioni e filtri dei criteri. L'unione avviene solo quando un criterio importato esiste già nel DDC cloud. Il risultato dell'unione dei criteri è che i criteri DDC cloud contengono le impostazioni e i filtri già presenti, in aggiunta a eventuali nuovi filtri e impostazioni importati. Tenere presente che quando si verificano conflitti tra impostazioni e filtri, i valori importati hanno la precedenza. | | SwitchParameter |

Restituisce:

- Vedere Valori restituiti dai cmdlet

**Cmdlet da cloud a cloud**

- `Backup-CvadAcToFile` - Esegue il backup di tutta la configurazione dal sito cloud.

  Esporta la configurazione cloud in file .yml. Questo backup può essere utilizzato in un processo di backup e ripristino per ripristinare i componenti persi.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti | | SwitchParameters |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud | | SwitchParameters |
| `TargetFolder` | Specifica la cartella di destinazione dell'esportazione. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |
| `ZipResults` | Comprime il backup dei file YAML in un unico file zip. Il file si trova nella stessa cartella dei file YAML di cui è stato eseguito il backup e ha lo stesso nome della cartella. | | SwitchParameter |

  Restituisce:

  - Vedere Valori restituiti dai cmdlet

- `Restore-CvadAcToSite` - Ripristina i file YAML di backup nel sito cloud. Questo sito cloud può essere uguale o diverso dal sito cloud di origine.

  Ripristina il sito cloud alla configurazione precedente. I file importati provengono dalla cartella specificata utilizzando il parametro `-RestoreFolder`, che identifica la cartella contenente i file .yml da ripristinare nel sito cloud. Questa deve essere una specifica di cartella completa.

Questo cmdlet può essere utilizzato per ripristinare la configurazione precedente o per eseguire il backup e il ripristino del sito cloud. Questo comando può aggiungere, eliminare e aggiornare il sito cloud.

Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti. | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti. | | Elenco di stringhe |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud. | | SwitchParameters |
| `RestoreFolder` | Identifica la cartella contenente i file .yml da ripristinare nel sito cloud. Questa deve essere una specifica di cartella completa. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |
| `Merge` | Se impostato su `$true`, aggiunge componenti solo al sito cloud. I componenti non vengono rimossi. Impostare su `$false` per rimuovere i componenti. | | `$true` o `$false` |
| `AddOnly` | Se impostato su `$true`, aggiunge solo nuovi componenti, non aggiorna né elimina i componenti esistenti. Impostare su `$false` per consentire aggiornamenti ed eliminazioni. `Merge` viene ignorato quando questo parametro è `$true`. | | `$true` o `$false` |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `MergePolicies` | Unire impostazioni e filtri dei criteri. L'unione avviene solo quando un criterio importato esiste già nel DDC cloud. Il risultato dell'unione dei criteri è che i criteri DDC cloud contengono le impostazioni e i filtri già presenti, in aggiunta a eventuali nuovi filtri e impostazioni importati. Tenere presente che quando si verificano conflitti tra impostazioni e filtri, i valori importati hanno la precedenza. | | SwitchParameter |
| `OnErrorAction` | Vedere OnErrorAction parameter. | | Stringa |

Restituisce:

- Vedere Valori restituiti dai cmdlet

- `Remove-CvadAcFromSite` - Rimuovere i membri dei componenti dal cloud.

  Può reimpostare l'intero sito o rimuovere elementi membri da un componente (ad esempio, la rimozione di un catalogo delle macchine dall'elenco dei cataloghi). Questo può essere utilizzato in abbinamento al parametro `IncludeByName` per rimuovere in modo selettivo membri specifici.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti | | Elenco di stringhe |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud | | SwitchParameters |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |

Restituisce:

- Vedere Valori restituiti dai cmdlet

**Altri cmdlet di base**

- `Compare-CvadAcToSite` - Confronta i file .yml locali con la configurazione cloud, producendo un report delle modifiche apportate da un cmdlet `Import`, `Merge` o `Restore`.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti. | | SwitchParameters |
| Filtraggio per nomi di oggetti | Vedere Filtraggio per nomi di oggetti. | | Elenco di stringhe |
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud. | | SwitchParameters |
| `SourceFolder` | Identifica una cartella principale sostitutiva per *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Stringa |
| `Locale` | Specifica la lingua del testo umanamente leggibile che può essere esportato. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true` o `$false` |
| `Merge` | Se impostato su `$true`, aggiunge componenti solo al sito cloud. I componenti non vengono rimossi. Impostare su `$false` per rimuovere i componenti. | | `$true` o `$false` |
| `AddOnly` | Se impostato su `$true`, aggiunge solo nuovi componenti, non aggiorna né elimina i componenti esistenti. Impostare su `$false` per consentire aggiornamenti ed eliminazioni. `Merge` viene ignorato quando questo parametro è `$true`. | | `$true` o `$false` |
| `OnErrorAction` | Vedere OnErrorAction parameter. | | Stringa |

  Restituisce:

  - Vedere Valori restituiti dai cmdlet

## Parametri di migrazione granulare

### Migrazione per componenti

I seguenti componenti possono essere specificati con i cmdlet che li supportano. L'opzione `All` viene selezionata automaticamente quando non vengono specificati parametri dei componenti. Per evitare errori, si consiglia di migrare i componenti nel seguente ordine:

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

### Filtraggio per nomi di oggetti

**Migrazione per nomi di componenti** I parametri `IncludeByName` e `ExcludeByName` consentono di includere ed escludere i membri dei componenti nei cmdlet in base al nome. È possibile scegliere un solo componente (ad esempio gruppi di consegna) alla volta in uno qualsiasi dei cmdlet supportati. Se un membro del componente si trova in entrambe le aree, l'esclusione sostituisce qualsiasi altro parametro e nell'elenco di correzione del log viene inserita una voce che identifica il nome del componente e del membro esclusi.

`IncludeByName` e `ExcludeByName` utilizzano un elenco di nomi dei membri dei componenti. Qualsiasi nome può contenere uno o più caratteri jolly. Sono supportati due tipi di caratteri jolly. L'elenco dei nomi dei membri dei componenti deve essere racchiuso tra virgolette singole quando il nome di un membro contiene caratteri speciali.

- * Corrisponde a un numero qualsiasi di caratteri
- ? Corrisponde a un singolo carattere

`IncludeByName` e `ExcludeByName` possono anche accettare un file contenente un elenco di membri in cui ogni membro può essere esplicito o contenere caratteri jolly. Ogni riga del file può contenere un membro. Gli spazi iniziali e finali vengono tagliati dal nome del membro. Il nome del

file deve essere preceduto dal segno @ ed essere racchiuso tra virgolette singole (un requisito di PowerShell in modo che @ non venga reinterpretato). È possibile elencare più file oltre ad associarli con i nomi dei membri.

Un esempio di unione di tutti i gruppi di consegna i cui nomi iniziano con `DgSite1` e contengono `Home2` sarebbe:

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

**Per nome del gruppo di consegna** `ByDeliveryGroupName` filtra in base al nome del gruppo di consegna per applicazioni e gruppi di applicazioni. Questo parametro è sempre un elenco di inclusione che identifica i membri da includere in base alla loro associazione al gruppo di consegna.

`ByDeliveryGroupName` contiene un elenco dei nomi dei gruppi di consegna. Qualsiasi nome può contenere uno o più caratteri jolly. Sono supportati due tipi di caratteri jolly.

- * corrisponde a un numero qualsiasi di caratteri
- ? corrisponde a un singolo carattere

L'esempio seguente unisce tutte le applicazioni che fanno riferimento a tutti i nomi dei gruppi di consegna che iniziano con `EastDg`.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

**Esclusione degli elementi disabilitati** `ExcludeDisabled` filtra dalle operazioni di importazione tutte le applicazioni e i gruppi di applicazioni disabilitati. Il valore predefinito di `ExcludeDisabled` è **`false`**, il che significa che tutte le applicazioni e i gruppi di applicazioni vengono importati indipendentemente dal loro stato abilitato.

**Per nome macchina** `ByMachineName` filtra i cataloghi delle macchine e i gruppi di consegna in base al nome della macchina. Questo parametro è sempre un elenco di inclusione che identifica i membri da includere in base all'associazione del nome della macchina.

`ByMachineName` accetta un elenco di nomi di macchine in cui qualsiasi nome può contenere uno o più caratteri jolly. Sono supportati due tipi di caratteri jolly.

- * corrisponde a un numero qualsiasi di caratteri
- ? corrisponde a un singolo carattere

Quando si importa o si esporta utilizzando `ByMachineName` e il filtro del nome di una macchina non restituisce macchine nel catalogo delle macchine o nel gruppo di consegna, il catalogo delle macchine o il gruppo di consegna viene escluso dall'esportazione o dall'importazione.

> **Nota:**
>
> L'utilizzo di `ByMachineName` in qualsiasi cmdlet di tipo importazione fa sì che `MergeMachines` sia impostato su `$true`.

**Unione di macchine** `MergeMachines`, se impostato su `$true`, indica all'operazione di importazione di aggiungere macchine solo al catalogo delle macchine o al gruppo di consegna. Le macchine non vengono rimosse, consentendo operazioni di aggiunta incrementali.

L'impostazione predefinita di `MergeMachines` è false, il che significa che le macchine vengono rimosse se non sono presenti nel file .yml del catalogo delle macchine o del gruppo di consegna. `MergeMachines` è impostato su `$true` quando `ByMachineName` viene utilizzato, ma può essere sovrascritto impostando `MergeMachines` su false.

### Cmdlet relativi ai prerequisiti

- `New-CvadAcCustomerInfoFile` - Creare un file di informazioni dei clienti. Per impostazione predefinita, il file di informazioni dei clienti si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `CustomerId` | ID del cliente. | x | Stringa |
| `ClientId` | ID client del cliente creato su Citrix Cloud. I valori CustomerId e Secret devono essere specificati quando si utilizza questo parametro. | A seconda delle condizioni | Stringa |
| `Secret` | Chiave segreta del cliente creata su Citrix Cloud. I valori CustomerId e ClientId devono essere specificati quando si utilizza questo parametro. | A seconda delle condizioni | Stringa |
| `Environment` | Ambiente Production, ProductionGov o ProductionJP. | | Enumerazione |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `LogFileName` | Cambia il prefisso del file di log da CitrixLog a un altro valore. | | Stringa |
| `AltRootUrl` | Da usare solo sotto la direzione di Citrix. | | Stringa |
| `StopOnError` | Interrompe l'operazione al primo errore. | | `$true` o `$false` |
| `TargetFolder` | Utilizzare la cartella specificata come cartella principale anziché *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Stringa |
| `Locale` | Utilizzare le impostazioni internazionali specificate anziché le impostazioni internazionali del sistema su cui viene eseguito lo strumento. | | Stringa |
| `Editor` | Utilizzare l'editor specificato per visualizzare il log al completamento di ogni cmdlet. Notepad.exe è l'editor predefinito. Questo parametro deve includere le specifiche di file complete per l'editor e l'editor deve acquisire la specifica del file di log come unico parametro. | | Stringa |
| `SecurityCsvFileSpec` | La specifica di file completa che punta al file SecurityClient.csv scaricato da Citrix Identity and Access Management. Il valore CustomerId deve essere specificato quando si utilizza questo parametro. | | Stringa |

Restituisce:

- Vedere Valori restituiti dai cmdlet

- `Set-CvadAcCustomerInfoFile` - Aggiornare un file di informazioni dei clienti esistente. Vengono modificati solo i parametri specificati dal cmdlet. Tutti i valori dei parametri non specificati nel file CustomerInfo.yml sono invariati.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `CustomerId` | ID del cliente. | | Stringa |
| `ClientId` | ID client del cliente creato su Citrix Cloud. | | Stringa |
| `Secret` | Chiave segreta del cliente creata su Citrix Cloud. | | Stringa |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `Environment` | Ambiente Production, ProductionGov o ProductionJP. | | Enumerazione |
| `LogFileName` | Cambia il prefisso del file di log da CitrixLog a un altro valore. | | Stringa |
| `StopOnError` | Interrompe l'operazione al primo errore. | | `$true` o `$false` |
| `TargetFolder` | Utilizzare la cartella specificata come cartella principale anziché *%HOMEPATH%\Documents\Citrix\AutoConfig*. | | Stringa |
| `Locale` | Utilizzare le impostazioni internazionali specificate anziché le impostazioni internazionali del sistema su cui viene eseguito lo strumento. | | Stringa |
| `Editor` | Utilizzare l'editor specificato per visualizzare il log al completamento di ogni cmdlet. Notepad.exe è l'editor predefinito. Questo parametro deve includere le specifiche di file complete per l'editor e l'editor deve acquisire la specifica del file di log come unico parametro. | | Stringa |
| `SecurityCsvFileSpec` | La specifica di file completa che punta al file SecurityClient.csv scaricato da Citrix Identity and Access Management. Il valore CustomerId deve essere specificato quando si utilizza questo parametro. | | Stringa |

Restituisce:

- Vedere Valori restituiti dai cmdlet

**Parametri relativi ai prerequisiti**

Insieme ai parametri di accesso al cloud, è possibile utilizzare i seguenti parametri con i cmdlet relativi ai prerequisiti:

- `Environment` - Ambiente Production o ProductionGov.
- `LogFileName` - Cambiare il prefisso del file di log da CitrixLog a un altro valore.
- `StopOnError` - Interrompe l'operazione al primo errore.
- `AlternateRootFolder` - Utilizzare la cartella specificata come cartella principale anziché *%HOMEPATH%\Documents\Citrix\AutoConfig*

- `Locale` - Utilizzare le impostazioni internazionali specificate anziché le impostazioni internazionali del sistema su cui viene eseguito lo strumento.
- `Editor` - Utilizzare l'editor specificato per visualizzare il log al completamento di ogni cmdlet. Notepad.exe è l'editor predefinito. Questo parametro deve includere le specifiche di file complete per l'editor e l'editor deve acquisire la specifica del file di log come unico parametro.

### Cmdlet per assistenza e risoluzione dei problemi

- `New-CvadAcZipInfoForSupport` - Comprime tutti i file di log e i file .yml in un unico file zip da inviare a Citrix per assistenza. Le informazioni sensibili dei clienti (CustomerInfo.yml e CvadAcSecurity.yml) non sono incluse nel file zip. Anche il file Icon.yml è escluso a causa delle sue dimensioni. Il file zip viene inserito in *%HOMEPATH%\Documents\Citrix\AutoConfig* e denominato *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, in base alla data e all'ora. Questo file zip può anche fungere da backup.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `TargetFolder` | Specifica una cartella di destinazione per creare e salvare il file zip. | | Stringa |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |

  Restituisce:

  - Il file zip con nome e posizione del file zip viene visualizzato nel prompt dei comandi.

- `Get-CvadAcStatus` - Da utilizzare per testare la connettività e garantire che tutti i prerequisiti siano soddisfatti. Restituisce informazioni sullo strumento come il numero di versione e la connettività con il cloud e lo stato del connettore.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud | | SwitchParameters |
| `SiteId` | Identifica il sito a cui connettersi. | | Stringa |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `AdminAddress` | Questo è l'indirizzo DNS o IP del Delivery Controller on-premise utilizzato per verificare il livello di accesso degli amministratori. Questo è necessario se lo strumento non viene eseguito su un Delivery Controller. | | Stringa |

Restituisce:

- Visualizza i risultati per ogni elemento.

- `Test-CvadAcConnectionWithSite` - Testare la connessione con il sito cloud per verificare che la connessione della comunicazione funzioni. Questo cmdlet utilizza i parametri di accesso al cloud o il file CustomerInfo.yml per specificare le informazioni di connessione del cliente.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud | | SwitchParameters |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |

Restituisce:

- I risultati del test vengono visualizzati sulla riga di comando.

- `Find-CvadAcConnector` - Individua i connettori esistenti e ne determina lo stato di funzionamento. Questo cmdlet utilizza le informazioni del file CustomerInfo.yml o il parametro ID cliente per individuare i connettori del cliente.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `CustomerInfoFileSpec` | La specifica del file che punta a un file di informazioni dei clienti per sovrascrivere la posizione e il nome predefiniti. Questo parametro viene ignorato quando viene fornito il parametro `CustomerId`. | | Stringa |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `CustomerId` | L'ID del cliente. Questo parametro sostituisce lo stesso valore nel file CustomerInfo.yml. | | Stringa |

Restituisce:

- I risultati sono mostrati sulla riga di comando.

- `Get-CvadAcCustomerSites` - Restituisce l'elenco di tutte le sedi dei clienti. Questo cmdlet utilizza i parametri di accesso al cloud o il file CustomerInfo.yml per specificare le informazioni di connessione del cliente.

  Parametri:

  - Vedere Parametri di accesso al cloud

  Restituisce:

  - Visualizza un elenco di ID delle sedi dei clienti trovate.

- `New-CvadAcTemplateToFile` - Crea un file modello per i componenti selezionati, che consente di creare manualmente un file di importazione.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti | | SwitchParameters |
| `TargetFolder` | Specifica la cartella di destinazione dell'esportazione. | | Stringa |

  Restituisce:

  - Vedere Valori restituiti dai cmdlet

- `Show-CvadAcDocument` - Visualizza questa documentazione nel browser predefinito.

  Parametri:

  - None (Nessuno).

  Restituisce:

  - Visualizza questa pagina Web nel browser Web predefinito.

- `Find-CvadAcInFile` - La funzionalità Find in file (Trova nei file) esegue ricerche nei file YAML dei componenti e cerca membri corrispondenti a uno o più nomi che possono contenere caratteri jolly. Il risultato è un report dei membri trovati. Find in file (Trova nei file) può cercare solo un componente alla volta. Find in file (Trova nei file) cerca tutti i file YAML nella cartella corrente e in tutte le sottocartelle. Utilizzare `FindSourceFolder` per limitare il numero di file da cercare.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Migrazione per componenti | Vedere Migrazione per componenti. Nota: il valore `-All` non è valido. | | SwitchParameters |
| `IncludeByName` | Un elenco che specifica i nomi dei gruppi di consegna da includere quando si imposta lo stato attivo del sito su attivo. I caratteri jolly * e ? sono supportati nei nomi. | | Elenco di stringhe |
| `Unique` | Segnala solo membri trovati in modo univoco. | | SwitchParameter |
| `IncludeYaml` | Includi il file YAML specifico per i membri. | | SwitchParameter |
| `FindSourceFolder` | La cartella in cui viene avviata la ricerca. | | Stringa |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | SwitchParameter |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |

  Risultato:

  - Crea un report contenente i membri trovati per il componente specificato.

### Cmdlet per l'attivazione del sito

Per ulteriori informazioni sull'attivazione dei siti e sull'utilizzo di questi cmdlet, vedere Attivazione dei siti.

- `Set-CvadAcSiteActiveStateOnPrem` - Imposta lo stato del sito on-premise su attivo o inattivo.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud | | SwitchParameters |
| `SiteActive` | Se presente, imposta il sito on-premise su attivo rimuovendo la modalità di manutenzione da tutti i gruppi di consegna. Quando questo parametro non è presente, la modalità di manutenzione è impostata su tutti i gruppi di consegna. | | SwitchParameter |
| `IncludeByName` | Un elenco che specifica i nomi dei gruppi di consegna da includere quando si imposta lo stato attivo del sito su attivo. I caratteri jolly * e ? sono supportati nei nomi. | | Elenco di stringhe |
| `ExcludeByName` | Un elenco che specifica i nomi dei gruppi di consegna da escludere quando si imposta lo stato attivo del sito su attivo. I caratteri jolly * e ? sono supportati nei nomi. | | Elenco di stringhe |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true or $false` |

Restituisce:

- Vedere Valori restituiti dai cmdlet

- `Set-CvadAcSiteActiveStateCloud` - Imposta lo stato del sito cloud su attivo o inattivo.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Parametri di accesso al cloud | Vedere Parametri di accesso al cloud | | SwitchParameters |
| `SiteActive` | Se presente, imposta il sito cloud su attivo rimuovendo la modalità di manutenzione da tutti i gruppi di consegna. Quando questo parametro non è presente, la modalità di manutenzione è impostata su tutti i gruppi di consegna. | | SwitchParameter |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `IncludeByName` | Un elenco che specifica i nomi dei gruppi di consegna da includere quando si imposta lo stato attivo del sito su attivo. I caratteri jolly * e ? sono supportati nei nomi. | | Elenco di stringhe |
| `ExcludeByName` | Un elenco che specifica i nomi dei gruppi di consegna da escludere quando si imposta lo stato attivo del sito su attivo. I caratteri jolly * e ? sono supportati nei nomi. | | Elenco di stringhe |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |
| `DisplayLog` | Visualizza il file di log al completamento del cmdlet. Impostare su `$false` per eliminare la visualizzazione del log. | | `$true or $false` |

Restituisce:

- Vedere Valori restituiti dai cmdlet

### Unione di più cmdlet di siti on-premise

Per ulteriori informazioni sull'unione dei siti e sull'utilizzo di questi cmdlet, vedere Unire più siti in un unico sito.

- `New-CvadAcSiteMergingInfo` - Crea un set di informazioni sul prefisso/suffisso per l'unione dei siti. Non è necessario conoscere tutti i prefissi o i suffissi all'inizio. Possono essere aggiornati con `Set-CvadAcSiteMergingInfo` o modificando manualmente il file SiteMerging.yml.
  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `SiteName` | Il nome utilizzato per identificare l'insieme di prefissi/suffissi per un sito specifico. Può corrispondere al nome del sito effettivo, ma non è necessario. | x | Stringa |

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| Parametri di unione dei siti | Vedere Parametri di unione dei siti | | SwitchParameters |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |

Restituisce:

- Nessuna

- `Set-CvadAcSiteMergingInfo` - Aggiorna un set di informazioni prefisso/suffisso esistente per l'unione dei siti.

  Parametri:

| Nome | Descrizione | Obbligatorio? | Tipo |
|---|---|---|---|
| `SiteName` | Il nome utilizzato per identificare l'insieme di prefissi/suffissi per un sito specifico. Può corrispondere al nome del sito effettivo, ma non è necessario. | x | Stringa |
| Parametri di unione dei siti | Vedere Parametri di unione dei siti | | SwitchParameters |
| `Quiet` | Eliminare la registrazione nella console. | | SwitchParameter |

  Restituisce:

  - Nessuna

- `Remove-CvadAcSiteMergingInfo` - Rimuove un set di informazioni prefisso/suffisso esistente per l'unione dei siti.

  Parametri:

  - `SiteName` - Identifica l'insieme di prefissi e suffissi del sito. Questa è una stringa ed è obbligatoria.

  Restituisce:

  - Nessuna

**Parametri di unione dei siti**

I seguenti parametri possono essere utilizzati per l'esecuzione dei cmdlet di unione dei siti. Tutti i parametri elencati sono stringhe.

- `SiteName` - Il nome utilizzato per identificare l'insieme di prefissi/suffissi per un sito specifico. Può corrispondere al nome del sito effettivo, ma non è necessario. SiteName è un parametro obbligatorio.
- `AdminScopedPrefix` - Il prefisso da applicare agli ambiti dell'amministratore.
- `ApplicationPrefix` - Il prefisso da applicare alle applicazioni.
- `ApplicationFolderPrefix` - Il prefisso da applicare alle cartelle delle applicazioni; `ApplicationFolderPrefix` può essere combinato con `ApplicationFolderRoot`.
- `ApplicationFolderRoot` - La nuova cartella principale per le cartelle delle applicazioni. Questo crea una gerarchia di cartelle aggiuntiva. `ApplicationFolderRoot` può essere combinato con `ApplicationFolderPrefix`.
- `ApplicationGroupPrefix` - Il prefisso per i gruppi di applicazioni.
- `ApplicationUserPrefix` - Il prefisso da applicare al nome dell'applicazione visualizzato dall'utente.
- `ApplicationAdminPrefix` - Il prefisso da applicare al nome dell'applicazione visualizzato dall'amministratore.
- `DeliveryGroupPrefix` - Il prefisso da applicare ai gruppi di consegna.
- `GroupPolicyPrefix` - Il prefisso da applicare ai nomi dei criteri.
- `HostConnectionPrefix` - Il prefisso da applicare alle connessioni host.
- `MachineCatalogPrefix` - Il prefisso da applicare ai cataloghi delle macchine.
- `StoreFrontPrefix` - Il prefisso da applicare ai nomi StoreFront.
- `TagPrefix` - Il prefisso da applicare ai tag.
- `AdminScopedSuffix` - Il suffisso da applicare agli ambiti dell'amministratore.
- `ApplicationSuffix` - Il suffisso da applicare alle applicazioni.
- `ApplicationFolderSuffix` - Il suffisso da applicare alle cartelle delle applicazioni; `ApplicationFolderSuffix` può essere combinato con `ApplicationFolderRoot`.
- `ApplicationGroupSuffix` - Il suffisso per i gruppi di applicazioni.
- `ApplicationUserSuffix` - Il suffisso da applicare al nome dell'applicazione visualizzato dall'utente.
- `ApplicationAdminSuffix` - Il suffisso da applicare al nome dell'applicazione visualizzato dall'amministratore.
- `DeliveryGroupSuffix` - Il suffisso da applicare ai gruppi di consegna.
- `GroupPolicySuffix` - Il suffisso da applicare ai nomi dei criteri.
- `HostConnectionSuffix` - Il suffisso da applicare alle connessioni host.
- `MachineCatalogSuffix` - Il suffisso da applicare ai cataloghi delle macchine.
- `StoreFrontSuffix` - Il suffisso da applicare ai nomi StoreFront.

- `TagSuffix` - Il suffisso da applicare ai tag.
- `SiteRootFolder` - Il nome completo della cartella da utilizzare per le esportazioni e le importazioni; può essere una cartella locale o una condivisione file.

### Parametri generici

#### Parametri di accesso al cloud

Tutti i cmdlet che accedono al cloud supportano i seguenti parametri aggiuntivi.

> **Nota:**
>
> CustomerID, ClientID e Secret possono essere inseriti nel file CustomerInfo.yml o specificati con il cmdlet utilizzando i seguenti parametri. Quando vengono specificati in entrambe le posizioni, i parametri del cmdlet hanno la precedenza.

- `CustomerId` - L'ID cliente utilizzato nelle API Rest, necessario per accedere a tutte le API Rest. L'ID cliente si trova in Citrix Cloud.
- `ClientId` - Il clientID creato sul sito Web Citrix Cloud Identity and Access Management. È necessaria per ottenere il token di connessione richiesto per l'autenticazione per tutte le API Rest.
- `Secret` - La chiave segreta creata sul sito Web Citrix Cloud Identity and Access Management. È necessaria per ottenere il token di connessione richiesto per l'autenticazione per tutte le API Rest.
- `CustomerInfoFileSpec` - La specifica del file che punta a un file di informazioni dei clienti per sovrascrivere la posizione e il nome predefiniti.

#### Parametri della modalità di migrazione

I cmdlet che modificano la configurazione del sito cloud (`Import`, `Restore`,`Merge`, `New` e `Sync`) supportano i seguenti parametri aggiuntivi per fornire ulteriore flessibilità.

- `CheckMode` - Esegue l'operazione di importazione ma *non* apporta modifiche. Tutte le modifiche previste vengono segnalate prima del completamento dell'importazione. È possibile utilizzare questo comando per verificare l'importazione prima che venga eseguita.
- `BackupFirst` - Esegue il backup dei contenuti cloud in file .yml prima di modificare la configurazione cloud. Questo parametro è abilitato per impostazione predefinita.
- `Confirm` - Se è impostato su true, chiede agli utenti di confermare che desiderano apportare modifiche alla configurazione del sito cloud. Il cmdlet `Remove` mostra un prompt a causa della sua natura distruttiva. Impostare questo parametro su false se non si desidera alcun prompt, ad esempio nel caso di esecuzione all'interno di script automatici. `Confirm` è impostato su true per impostazione predefinita.

- `SecurityFileFolder` - Questa è la cartella completa contenente il file CustomerInfo.yml che potrebbe puntare a una cartella locale o a una cartella di una condivisione di rete a cui potrebbe essere applicato il controllo dell'autenticazione. Lo strumento non richiederà le credenziali; l'accesso alla risorsa controllata deve essere ottenuto prima di eseguire lo strumento.
- `SiteName` - Specifica il prefisso e il suffisso per l'unione dei siti da utilizzare durante l'importazione.
- `SiteActive` - Specifica se il sito importato è attivo o inattivo. Per impostazione predefinita, questo parametro è impostato su `$false`, il che indica che il sito importato è inattivo.

#### Parametri di visualizzazione del log

I cmdlet `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare` e `Remove` visualizzano il file di log al termine dell'operazione. È possibile impedire la visualizzazione impostando il parametro `-DisplayLog` su `$false`. Notepad.exe viene utilizzato per impostazione predefinita per visualizzare il file di log. È possibile specificare un editor diverso nel file CustomerInfo.yml.

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

### Valori restituiti dai cmdlet

#### ActionResult

Tutti i cmdlet restituiscono il valore seguente.

```
1            public class ActionResult
2            {
3
4                public bool                          Overall_Success;
5                public Dictionary<string, string>   Individual_Success;
6                public object                        CustomResult;
7             }
```

`Overall_Success` restituisce un singolo valore booleano che mostra la corretta esecuzione del cmdlet in tutti i componenti selezionati: true significa che l'operazione è riuscita e false che non è riuscita.

`Individual_Success` restituisce uno o tre valori per ogni componente principale. Il risultato di un componente può essere Success (Operazione riuscita), Failure (Operazione non riuscita) o Skipped (Saltato). Skipped (Saltato) indica che il componente non è stato selezionato per l'esecuzione dal cmdlet.

`CustomResult` è specifico del cmdlet.

**CustomResult**

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File` e `Remove` riportano le seguenti informazioni personalizzate sui risultati a una singola istanza di `EvaluationResultData`.

> **Nota:**
>
> I cmdlet `Export` e `Template` non restituiscono un risultato personalizzato.

```
public class EvaluationResultData
{

    public Dictionary<string, Dictionary<string,
       ActionResultValues >> EvaluationResults;
    public int                  Added;
    public int                  Updated;
    public int                  Deleted;
    public int                  NoChange;
    public int                  TotalChanged;
    public EvaluationResults     OverallResult;
    public string               CloudBackupFolder;
    public string               SourceBackupFolder;
 }

Where:
public enum ActionResultValues
{

    Add,
    Update,
    Delete,
    Identical,
    DoNothing
 }

public enum EvaluationResults
{

    Success,
    Failure,
    Skipped
 }
```

`EvaluationResults` visualizza un elenco con una voce per ogni componente selezionato. La chiave è il nome del componente e il valore è un elenco di ogni membro del componente e l'azione intrapresa su tale membro del componente. Le azioni possono essere uno qualsiasi dei valori `ActionResultValues`.

`Added`, `Updated`, `Deleted` e `NoChange` indicano il numero totale di membri dei componenti aggiunti, aggiornati, eliminati o nessuna azione intrapresa, in quell'ordine.

`TotalChanged` è la somma di `Added`, `Updated` e `Deleted`.

`OverallResult` è un singolo valore booleano che indica il risultato del cmdlet. Il valore true indica la riuscita delle operazioni per tutti i componenti e false indica un errore nell'elaborazione di uno o più componenti.

`CloudBackupFolder` è la specifica di file completa del backup della configurazione del sito cloud prima che il cmdlet esegua qualsiasi azione di modifica del cloud.

`SourceBackupFolder` è la specifica di file completa del backup del file di origine effettuato dopo il completamento del cmdlet. Per impostazione predefinita, questi file si trovano in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

### Guida di PowerShell

La guida di PowerShell è disponibile per ogni cmdlet. Tutti i parametri sono documentati con ogni cmdlet insieme a una breve spiegazione del cmdlet. Per accedere alla guida di qualsiasi cmdlet, digitare `Get-Help` davanti al cmdlet.

```
Get-Help Import-CvadAcToSite
```

## Risoluzione dei problemi relativi ad Automated configuration (Configurazione automatica) e informazioni aggiuntive

December 21, 2022

> **Importante:**
>
> Per i messaggi di errore che si verificano comunemente nella Configurazione automatica e le soluzioni corrispondenti, vedere le *domande frequenti sulla risoluzione dei problemi* nell'articolo del Knowledge Center CTX277730.

### Errori dello strumento di configurazione automatica

Le operazioni dello strumento di configurazione automatica possono talvolta produrre errori. Quando ciò accade, possono verificarsi errori durante l'elaborazione di componenti come cataloghi di macchine, gruppi di consegna o criteri di gruppo, ad esempio. L'uso di `OnErrorAction` e dei parametri di continuazione consente di rilevare gli errori durante l'elaborazione, risolverli e riprendere da dove si era interrotto.

Il valore predefinito di `OnErrorAction` è `StopCompEnd`. Quando si verifica un errore, lo strumento termina l'elaborazione del componente corrente. Non vengono elaborati componenti aggiuntivi e gli errori non si ripercuotono sui componenti dipendenti a valle. Dopo aver risolto gli errori, è possibile eseguire nuovamente i cmdlet con qualsiasi parametro di continuazione applicato.

#### Parametro OnErrorAction

È possibile definire i valori del parametro `OnErrorAction` nei cmdlet di migrazione per controllare come lo strumento risponde agli errori rilevati durante l'elaborazione dei componenti.

Questa tabella mostra i valori dei parametri e le relative descrizioni:

| Valore | Descrizione |
|---|---|
| `Continue` | Tenta di elaborare il maggior numero possibile di componenti. |
| `Pause` | Si interrompe al termine dell'elaborazione e richiede di continuare o interrompere. |
| `StopCompEnd` | Tenta di elaborare quanto più possibile il componente. Si arresta dopo che il componente è finito. (Impostazione predefinita) |
| `StopImmediately` | L'elaborazione si interrompe quando viene rilevato un errore. |

#### Cmdlet di migrazione

È possibile applicare il parametro `OnErrorAction` ai seguenti cmdlet di migrazione:

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

Esempio: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

#### Parametri di ripresa

Questi parametri definiscono il modo in cui lo strumento riprende a funzionare dopo la pausa o l'interruzione di un'operazione a causa di un errore.

È possibile applicare ai cmdlet di migrazione parametri di ripresa che includono uno dei seguenti valori del parametro `OnErrorAction`:

- `Pause`
- `StopCompEnd`
- `StopImmediately`

Questa tabella mostra i valori dei parametri e le relative descrizioni:

| Valore | Descrizione |
|---|---|
| `-AllRemaining` | Richiede un componente iniziale. L'elaborazione inizia dal componente iniziale ed elabora tutti i componenti rimanenti. Vengono elaborati più componenti. |
| `-Resume` | Utilizza il componente di CurrentComponent.txt come punto di partenza. Tutto il resto è impostato su true. Vengono elaborati più componenti. |
| `-Repeat` | Utilizza il componente di CurrentComponent.txt come punto di partenza. Tutto il resto è impostato su false. Viene elaborato un solo componente. |

L'ultimo componente elaborato viene archiviato nel file CurrentComponent.txt nella cartella Auto-Config. La modifica di questo file non è consigliata.
Se si specifica `-Resume` o `-Repeat` e CurrentComponent.txt è mancante o non valido, l'elaborazione si interrompe e viene richiesto di selezionare un componente.

#### Impostare OnErrorAction nel file CustomerInfo.yml

È inoltre possibile impostare i valori `OnErrorAction` nel file CustomerInfo.yml. Impostare i valori utilizzando i seguenti cmdlet:

- Per un nuovo file: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- Per un file esistente: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

## Log

L'esecuzione di qualsiasi cmdlet genera un file di log creato e una voce nel file di log principale della cronologia. Tutti i file di log delle operazioni vengono inseriti in una cartella di backup. Tutti i nomi dei file di log iniziano con `CitrixLog`, quindi mostrano l'operazione di configurazione automatica e la data e l'ora dell'esecuzione del cmdlet. I log non vengono eliminati automaticamente.

Il log principale della cronologia si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*, nel file chiamato **History.Log**. Ogni esecuzione di cmdlet produce una voce di log principale contenente la data, l'operazione, il risultato, il backup e le posizioni dei file di log dell'esecuzione.

È inoltre possibile utilizzare il cmdlet `New-CvadAcZipInfoForSupport` per raccogliere i log da inviare a Citrix per assistenza. Questo cmdlet comprime tutti i file di log e i file .yml in un unico file zip. Le informazioni sensibili dei clienti (CustomerInfo.yml e CvadAcSecurity.yml) non sono incluse nel file zip. Anche il file Icon.yml è escluso a causa delle sue dimensioni. Il file zip viene inserito in *%HOMEPATH%\Documents\Citrix\AutoConfig* e denominato *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, in base alla data e all'ora. Questo file zip può anche fungere da backup.

Ogni file di log include quanto segue:

- Il nome dell'operazione e se la modalità di controllo è abilitata
- La data e l'ora di inizio e fine
- Voci multiple per le azioni di ciascun componente e le notifiche di successo/errore
- Riepilogo delle azioni intraprese, inclusi vari conteggi di oggetti creati
- Correzioni consigliate ove applicabile
- Posizione della cartella di backup, ove applicabile
- Posizione del log principale
- Durata

## File diagnostici

I file diagnostici aiutano a individuare e risolvere i problemi. I seguenti file vengono creati quando viene eseguita la relativa operazione. Si trovano nella sottocartella specifica dell'azione in *%HOMEPATH%\Documents\Citrix\AutoConfig*. Includere questi file quando si forniscono informazioni per il supporto alla risoluzione dei problemi.

### Esportazione

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

Questo file conta tutte le chiamate dell'SDK Broker PowerShell effettuate per esportare la configurazione del sito nei file.

**Import (Importa), Merge (Unisci), Restore (Ripristina), Sync (Sincronizza), Backup (Esegui il backup), Compare (Confronta)**

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

Questo file documenta ogni chiamata API Rest e le informazioni correlate.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

In questo file è presente tutto il contenuto dell'API Rest `Add`, `Update` e `Delete`.

### Problemi derivanti dalle dipendenze

Le importazioni e le unioni potrebbero non riuscire a causa di dipendenze mancanti. Alcuni problemi comuni sono:

1. In Criteri di gruppo mancano dei filtri del gruppo di consegna. Le cause comuni sono gruppi di consegna che non sono stati importati.
2. Le applicazioni non riescono a essere importate o unite. La causa comune è la mancanza di gruppi di consegna o gruppi di applicazioni che non sono stati importati.
3. Nei gruppi di applicazioni manca un RestrictToTag. Le cause comuni sono i tag che non sono stati importati.
4. Le connessioni host non vanno a buon fine. La causa abituale è la mancanza di informazioni di sicurezza nel file CvadAcSecurity.yml.
5. I cataloghi delle macchine non funzionano. La causa abituale sono le connessioni host che non sono state importate.
6. Macchine mancanti nei cataloghi delle macchine e nei gruppi di consegna. La causa abituale sono le macchine che non sono state trovate in Active Directory.
7. Utenti mancanti nei gruppi di consegna. La causa abituale sono gli utenti che non sono stati trovati in Active Directory.

### Consigli

- Non eseguire più di un'istanza di Automated configuration (Configurazione automatica) alla volta. L'esecuzione di più istanze simultanee produce risultati imprevedibili nel sito cloud. Se questo si verifica, eseguire nuovamente un'istanza di Automated configuration (Configurazione automatica) per portare il sito allo stato previsto.
- Non elaborare o modificare i dati nella scheda Manage (Gestisci) in Full Configuration (Configurazione completa) durante l'esecuzione di Automated configuration (Configurazione automatica).

- Verificare sempre visivamente i risultati di Merge (unisci)/Import (importa)/Restore (ripristina) in Full Configuration (Configurazione completa) per garantire che il sito cloud soddisfi le aspettative.

## Cartelle

### Posizione predefinita della cartella principale

Tutte le operazioni dello strumento Automated configuration (Configurazione automatica) avvengono nella cartella principale o nelle sottocartelle al suo interno. La cartella principale si trova in *%HOMEPATH%\Documents\Citrix\AutoConfig*.

### Esportazione

Tutti i file esportati vengono collocati in due cartelle, offrendo facilità d'uso e una cronologia delle esportazioni. Le esportazioni vengono sempre inserite nella cartella principale. Le copie vengono inserite in una sottocartella denominata **Export** (Esporta) con la data e l'ora dell'esportazione.

La cartella principale contiene sempre la configurazione del sito on-premise esportata più recente. Ogni sottocartella **Export** (Esporta) contiene l'esportazione effettuata nella data e ora indicate, che mantiene una cronologia delle esportazioni. È possibile utilizzare qualsiasi sottocartella **Export** (Esporta) per configurare il sito cloud. Automated configuration (Configurazione automatica) non elimina o modifica le sottocartelle di esportazione esistenti.

### Import (Importa)/Merge (Unisci)/Sync (Sincronizza)/Compare (Confronta)

Le operazioni `Import`, `Merge` e `Compare` provenienti sempre da file che si trovano nella cartella principale. Ogni operazione comporta la creazione di una sottocartella in cui vengono copiati i file nella cartella principale, fornendo una cronologia dei file sorgente modificati del sito cloud.

### Restore (Ripristina)

L'operazione `Restore` utilizza una sottocartella esistente per configurare il sito cloud. La cartella di origine è specificata nel parametro `-RestoreFolder` richiesto. A differenza di altri comandi, non viene creata nessuna nuova sottocartella perché l'operazione `Restore` utilizza una sottocartella esistente. La cartella di ripristino può essere la cartella principale ma deve comunque essere specificata nel parametro `-RestoreFolder`.

### Backup

Automated Configuration (Configurazione automatica) inizializza, aggiorna ed esegue il backup di una configurazione del sito cloud. Se vengono utilizzate per un certo tempo, molte configurazioni diverse possono cambiare sul sito cloud. Per facilitare l'uso a lungo termine e preservare le modifiche alla cronologia, Automated Configuration (Configurazione automatica) utilizza uno schema di conservazione per salvare la cronologia delle modifiche e fornire un metodo per ripristinare gli stati precedenti.

I backup della configurazione del sito cloud vengono sempre eseguiti in una sottocartella denominata **Backup** con i dati e l'ora del backup. Automated Configuration (Configurazione automatica) non elimina o modifica le sottocartelle di esportazione esistenti.

È possibile utilizzare i backup per ripristinare componenti specifici o l'intera configurazione. Per ripristinare l'intero gruppo di consegna e i componenti del catalogo delle macchine, utilizzare il cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **Nota:**
>
> Le informazioni sul file di backup nel cmdlet precedente si basano sui backup dell'utente.

Per ripristinare l'intera configurazione del sito cloud, utilizzare il cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

> **Nota:**
>
> Le informazioni sul file di backup nel cmdlet precedente si basano sui backup dell'utente.

#### Modifica della cartella principale predefinita

Le operazioni `Export`, `Import`, `Merge`, `Sync` e `Compare` possono modificare la cartella principale predefinita utilizzando il parametro `–AlternateFolder`. La creazione e la gestione delle sottocartelle per ciascuna operazione rimangono le stesse descritte in precedenza.

#### File copiati nelle sottocartelle

Tutti i file con estensione ".yml"vengono copiati nelle sottocartelle delle operazioni, ad eccezione dei seguenti:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

#### Backup automatizzati di siti cloud in modalità provvisoria

Viene eseguito un backup della configurazione corrente del sito cloud prima di eseguire operazioni che modificano la configurazione. Questo include i parametri `Import`, `Merge`, `Sync` e `Restore`. Il backup si trova sempre in una sottocartella sotto la sottocartella operativa.

Nel caso di `Restore`, la cartella di backup è una sottocartella della cartella specificata nel parametro `-RestoreFolder`.

### Automazione

I cmdlet dello strumento Automated configuration (Configurazione automatica) possono essere eseguiti negli script di automazione senza l'intervento dell'amministratore eliminando i prompt e la visualizzazione dei risultati dei log al completamento del cmdlet. È inoltre possibile impostare i parametri in modo che facciano lo stesso utilizzando il file CustomerInfo.yml.

Aggiungere il seguente parametro ai cmdlet che modificano il cloud per impedire la visualizzazione dei prompt.

```
-Confirm $false
```

Aggiungere il seguente parametro ai cmdlet per impedire la visualizzazione del log al completamento del cmdlet.

```
-DisplayLog $false
```

Aggiungere il seguente parametro ai cmdlet per impedire la registrazione nella finestra di comando PowerShell.

```
-Quiet
```

Come metodo alternativo, i seguenti parametri possono essere inseriti nel file CustomerInfo.yml.

```
Confirm: False
```

```
DisplayLog: False
```

### Esportazione da PC diversi dal Delivery Controller

Lo strumento Automated configuration (Configurazione automatica) utilizza più SDK Citrix PowerShell per esportare la configurazione del sito on-premise in file. Questi SDK vengono installati au-

tomaticamente sul Delivery Controller, consentendo allo strumento di funzionare sul Delivery Controller senza azioni aggiuntive. Quando viene eseguito su macchine diverse dai Delivery Controller, è necessario installare il set di SDK Citrix PowerShell richiesto dallo strumento. Questo set di SDK fa parte di Citrix Studio, che può essere installato dal supporto di installazione Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Automated configuration (Configurazione automatica) non può essere eseguito su Cloud Connector.

### Passaggio a Citrix Cloud Government e Japan Control Plane

Gli ambienti Citrix Cloud Government e Japan Control Plane utilizzano punti di accesso diversi per autenticare e allocare i token di accesso. Questo requisito unico si applica a qualsiasi strumento di Automated configuration (Configurazione automatica) che accede al cloud. Effettuare i seguenti passaggi per utilizzare Automated configuration (Configurazione automatica) in questi ambienti.

1. Nella cartella *%HOMEPATH%\Documents\Citrix\AutoConfig*, modificare CustomerInfo.yml.
2. Aggiungere una delle seguenti righe, a seconda dell'ambiente a cui si desidera connettersi, a CustomerInfo.yml (o modificarla, se già presente).

   ```
   Environment: 'ProductionGov'
   ```

   o

   ```
   Environment: 'ProductionJP'
   ```

Automated Configuration (Configurazione automatica) può ora essere utilizzata in questi ambienti.

### Raccolta dati Citrix Cloud

Per informazioni sulle informazioni raccolte da Citrix Cloud, vedere Gestione dei log e dei contenuti dei clienti di Citrix Cloud Services.

### Risorse aggiuntive

#### Forum di discussione

Visitare il forum di discussione Citrix per Automated Configuration (Configurazione automatica).

### Video

Guardare Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops su YouTube.

### Formazione

Il Cloud Learning Center contiene guide video dettagliate per la creazione di una distribuzione di servizi, incluse le attività descritte in questo articolo. Vedere Migrazione di Citrix Virtual Apps and Desktops a Citrix Cloud Learning Path.

## Esegue la migrazione dei carichi di lavoro da una posizione risorsa a un'altra utilizzando Image Portability Service

December 5, 2023

Image Portability Service semplifica la gestione delle immagini su più piattaforme. Le API REST di Citrix Virtual Apps and Desktops possono essere utilizzate per automatizzare l'amministrazione delle risorse all'interno di un sito Citrix Virtual Apps and Desktops.

Il flusso di lavoro di Image Portability inizia quando si utilizza Citrix Cloud per avviare la migrazione di un'immagine dalla posizione locale alla sottoscrizione nel cloud pubblico. Dopo aver preparato l'immagine, Image Portability Service aiuta a trasferire l'immagine nella sottoscrizione nel cloud pubblico e a prepararla per l'esecuzione. Infine, Citrix Provisioning o Machine Creation Services esegue il provisioning dell'immagine nella sottoscrizione nel cloud pubblico.

### Componenti

I componenti di Image Portability Service includono:

- Servizi Citrix Cloud
- Citrix Credential Wallet
- Citrix Connector Appliance
- VM di Compositing Engine
- Script di esempio di PowerShell

### Servizi Citrix Cloud

L'API Citrix Cloud Services è un servizio API REST che interagisce con Image Portability Service. Utilizzando il servizio REST API, è possibile creare e monitorare i processi di Image Portability. Ad esempio, si effettua una chiamata API per avviare un processo di Image Portability, ad esempio per esportare un disco, e quindi per effettuare chiamate per ottenere lo stato del processo.

### Citrix Credentials Wallet

Il servizio Citrix Credentials Wallet gestisce in modo sicuro le credenziali di sistema, consentendo a Image Portability Service di interagire con le risorse. Ad esempio, quando si esporta un disco da vSphere a una condivisione SMB, Image Portability Service richiede le credenziali per aprire una connessione alla condivisione SMB per scrivere il disco. Se le credenziali sono memorizzate nel Credential Wallet, Image Portability Service può recuperare e utilizzare tali credenziali.

Questo servizio dà la possibilità di gestire completamente le proprie credenziali. L'API dei servizi cloud funge da punto di accesso, offrendo la possibilità di creare, aggiornare ed eliminare le credenziali.

### Compositing Engine

Il Compositing Engine esegue la maggior parte del lavoro in Image Portability Service. Il Compositing Engine (CE) è una singola macchina virtuale creata all'inizio di un processo di esportazione o preparazione di Image Portability. Queste VM vengono create nello stesso ambiente in cui si svolge il lavoro. Ad esempio, quando si esporta un disco da vSphere, il CE viene creato sul server vSphere. Allo stesso modo, quando si esegue un processo di preparazione in Azure, AWS o Google Cloud, il CE viene creato rispettivamente in Azure, AWS o Google. Il CE monta il disco su se stesso e quindi esegue le necessarie manipolazioni del disco. Al termine del processo di preparazione o esportazione, la macchina virtuale CE e tutti i suoi componenti vengono eliminati.

### Connector Appliance

Il Connector Appliance, su cui è in esecuzione il software del provider per gestire le risorse IPS, viene eseguito nel tuo ambiente (sia in locale che nella sottoscrizione di Azure, AWS o Google Cloud) e funge da controller per i singoli processi. Riceve le istruzioni di processo dal servizio cloud e crea e gestisce le VM di Compositing Engine. La macchina virtuale Connector Appliance funge da unico punto di comunicazione sicuro tra i servizi cloud e gli ambienti. Distribuire uno o più Connector Appliance in ciascuna delle proprie posizioni di risorse (locale, Azure, AWS o Google Cloud). Un Connector Appliance viene distribuito in ogni posizione di risorse per motivi di sicurezza. Collocando Connector Appliance e Compositing Engine, il livello di sicurezza dell'implementazione aumenta notevolmente,

poiché tutti i componenti e le comunicazioni vengono mantenuti all'interno della propria posizione delle risorse.

### Moduli PowerShell

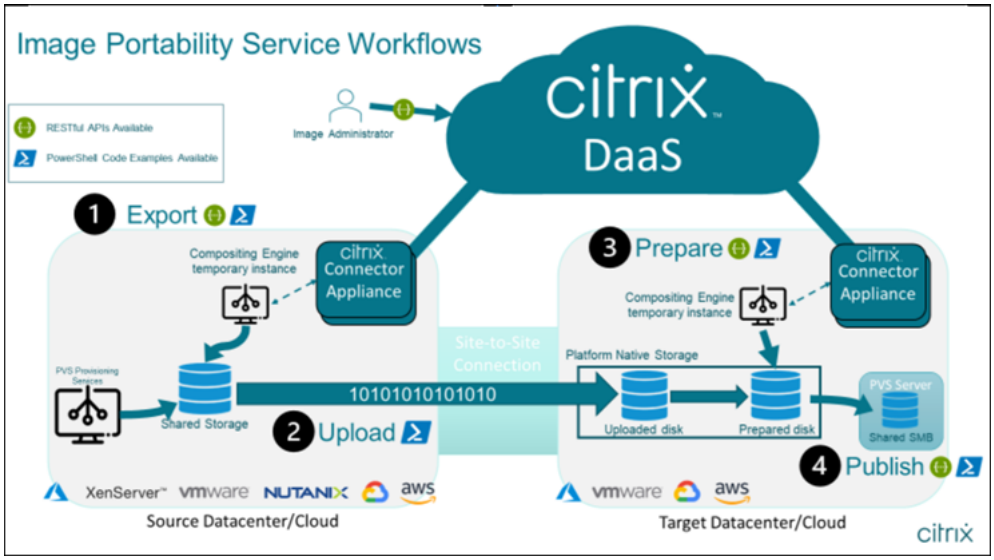
Forniamo una raccolta di moduli PowerShell da utilizzare all'interno degli script come punto di partenza per sviluppare la propria automazione personalizzata. I moduli forniti sono supportati così come sono, ma è possibile modificarli se ciò è necessario per la distribuzione.

L'automazione di PowerShell utilizza i parametri di configurazione forniti per comporre una chiamata REST al servizio API Citrix Cloud per avviare il processo e quindi fornire aggiornamenti periodici man mano che il processo procede.

Se si desidera sviluppare la propria soluzione di automazione, è possibile effettuare chiamate al servizio cloud direttamente utilizzando il linguaggio di programmazione preferito. Consultare il portale API per informazioni dettagliate sulla configurazione e l'utilizzo degli endpoint REST e dei moduli PowerShell di Image Portability Service.

## Flussi di lavoro

Image Portability Service utilizza un flusso di lavoro in più fasi per preparare un'immagine del catalogo principale da una posizione di risorse locale per la sottoscrizione al cloud pubblico. Il servizio esporta l'immagine dalla piattaforma hypervisor locale perché la si possa caricare nella propria sottoscrizione al cloud pubblico (la nostra utility di caricamento PowerShell fornita può aiutare ad automatizzare questa operazione). Quindi, Image Portability prepara l'immagine per renderla compatibile con la piattaforma cloud pubblica in uso. Infine, l'immagine è pubblicata e pronta per essere distribuita come nuovo catalogo di macchine all'interno della posizione delle risorse cloud.



Questi flussi di lavoro di alto livello si basano sulla configurazione di provisioning di origine e destinazione dell'immagine (Machine Creation o Citrix Provisioning). Il flusso di lavoro scelto determina quali passaggi del processo di Image Portability sono necessari.

Fare riferimento alla tabella seguente per comprendere quali processi sono necessari per ciascuno dei flussi di lavoro IPS supportati.

| Flusso di lavoro (da origine a destinazione) | Esportazione | Caricamento | Preparazione | Pubblicazione |
|---|---|---|---|---|
| Da MCS a MCS | Y | Y | Y | N |
| Da PVS a MCS* | N | Y | Y | N |
| Da PVS a PVS su Azure/Google Cloud* | N | Y | Y | Y |
| Da MCS a PVS su Azure/Google Cloud | Y | Y | Y | Y |

*Si suppone che si disponga dell'immagine originale come Citrix Provisioning vDisk e che non sia necessario esportarla direttamente dall'hypervisor della piattaforma di origine.

## Requisiti

Per iniziare a utilizzare Image Portability, è necessario soddisfare i seguenti requisiti.

### Un'immagine del catalogo macchine Citrix

IPS richiede l'utilizzo di immagini con una delle seguenti configurazioni testate:

- Windows Server 2016, 2019 e 2022H2
- Windows 10 o 11
- Provisioning tramite Machine Creation Services o Citrix Provisioning
- VDA Citrix Virtual Apps and Desktops versione 1912CU6, 1912CU7, 2203CU1, 2203CU2, 2212, 2303 o 2305
- Servizi Desktop remoto abilitati per l'accesso alla console in Azure

Il servizio di portabilità delle immagini supporta i seguenti hypervisor e piattaforme cloud:

**Piattaforme di origine:**

- VMware vSphere 7.0 e 8.0
- Citrix Hypervisor/XenServer 8.2
- Nutanix Prism Element 3.x
- Microsoft Azure
- Google Cloud Platform

**Piattaforme di destinazione:**

- VMware vSphere 8.0
- Microsoft Azure
- AWS
- Google Cloud Platform

#### Un Citrix Connector Appliance

È necessario che un Citrix Connector Appliance sia installato e configurato in ogni posizione delle risorse in cui si intende utilizzare Image Portability. Ad esempio, se si utilizza la portabilità delle immagini per spostare un'immagine da vSphere ad Azure, AWS e Google Cloud, occorrono almeno quattro Citrix Connector Appliance:

Per istruzioni dettagliate, vedere Distribuire Connector Appliances.

#### Una condivisione di file SMB (Windows)

È necessaria una **condivisione di file SMB** di Windows per l'archiviazione temporanea dei dati durante i processi di esportazione ospitati nella posizione delle risorse locale in cui si utilizza Image Portability Service. Assicurarsi che lo spazio libero disponibile sulla condivisione sia almeno il doppio delle dimensioni configurate del file system dell'immagine.

#### Una macchina per l'esecuzione di script PowerShell

Assicurarsi che la macchina che esegue gli script PowerShell abbia le seguenti caratteristiche:

- PowerShell versione 5.1.

- Una connessione di rete veloce alla condivisione di file SMB. Può essere la stessa macchina che ospita la condivisione di file.
- Una connessione di rete veloce alle piattaforme cloud pubbliche in cui si prevede di utilizzare la funzionalità Image Portability. Ad esempio, Azure, AWS o Google Cloud.

  Vedere la sezione Preparare una macchina per PowerShell per i dettagli di come scaricare e configurare i moduli di Image Portability dalla PowerShell Gallery.

#### Il proprio ID cliente Citrix Cloud

Assicurarsi di avere una sottoscrizione Citrix DaaSvalida.

Per continuare, è necessario accedere a Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops). Se non si dispone dell'accesso, contattare il rappresentante Citrix.

Per istruzioni su come creare e configurare un client API da utilizzare con la portabilità delle immagini, consultare la documentazione sulla procedura introduttiva dell'API.

#### Autorizzazioni e configurazione richieste per Azure

Affinché il servizio di portabilità delle immagini esegua azioni nella propria risorsa Azure, è necessario concedere all'entità servizio di Azure utilizzata da Image Portability Service le autorizzazioni per determinate funzionalità di Azure. Per l'elenco dettagliato, vedere Autorizzazioni richieste per Microsoft Azure.

È possibile assegnare il ruolo **Contributor** all'entità del servizio nella risorsa associata. In alternativa, per assegnare le autorizzazioni minime richieste, è possibile creare ruoli personalizzati con le autorizzazioni richieste e assegnarli all'entità servizio con ambito corrispondente alle risorse appropriate.

Per informazioni sulla configurazione dei ruoli di sicurezza per l'entità servizio di Azure e per la creazione di ruoli personalizzati, vedere la documentazione di Azure.

#### Autorizzazioni e configurazione richieste da Google Cloud

Affinché il servizio di portabilità delle immagini esegua azioni nel progetto Google Cloud, concedere le autorizzazioni per determinate funzionalità all'entità servizio Google Cloud utilizzato da Image Portability Service.

Per l'elenco dettagliato, vedere Autorizzazioni richieste da Google Cloud.

È possibile assegnare queste autorizzazioni utilizzando i seguenti ruoli:

- Editor Cloud Build

- Amministratore Compute
- Amministratore archiviazione
- Utente account di servizio

Per ulteriori informazioni sulla configurazione delle autorizzazioni degli account di servizio, vedere ladocumentazione di Google Cloud.

#### Autorizzazioni e configurazione richieste per Amazon Web Services

Per eseguire i flussi di lavoro del servizio di portabilità delle immagini con un account Amazon Web Services (AWS), la rispettiva identità di Identity and Access Management (IAM) deve disporre delle autorizzazioni corrette.

Per un elenco dettagliato, vedere Autorizzazioni richieste da AWS.

### Configurare Image Portability Service

Per configurare Image Portability Service:

- Distribuire Connector Appliances
- Preparare una macchina per PowerShell
- Aggiungere credenziali a Credential Wallet

#### Distribuire Connector Appliances

Per la portabilità delle immagini è necessario che i Citrix Connector Appliance creino processi di Image Portability. I Connector Appliance aiutano a proteggere le interazioni con gli ambienti cloud pubblici e locali. I Connector Appliance inviano comunicazioni di ritorno a Image Portability Service per creare report sullo stato del processo e sullo stato generale di integrità del servizio.

Per distribuire e configurare Connector Appliance nel tuo ambiente, seguire la procedura descritta in Connector Appliance per servizi cloud.

Prendere nota della configurazione hardware richiesta e dell'accesso alla porta di rete per l'appliance quando si pianifica la distribuzione.

Quando l'appliance viene distribuita e registrata, i componenti necessari per abilitare Image Portability vengono installati automaticamente.

#### Preparare una macchina per PowerShell

Per aiutarti a iniziare a utilizzare Image Portability, abbiamo creato moduli PowerShell personalizzabili utilizzabili con il servizio.

Le sezioni seguenti descrivono come preparare una macchina per l'esecuzione degli script PowerShell. Questi script sono solo alcuni esempi. È possibile modificarli o migliorarli in base alle proprie esigenze.

> **Nota:**
>
> Dopo l'installazione iniziale, utilizzare **Update-Module** per aggiornare il modulo PowerShell.

**Requisiti di PowerShell** Per utilizzare gli script PowerShell, è necessario quanto segue:

- Un computer Windows per eseguire gli script PowerShell che gestiscono i processi di portabilità delle immagini. La macchina:
  - Dispone dell'ultima versione di PowerShell.
  - Dispone di una connessione di rete da 10 Gb/s o superiore alla condivisione di file SMB locale e di una connessione veloce al cloud pubblico (Azure, AWS o Google Cloud, ad esempio).
  - Può essere la stessa macchina che ospita la condivisione di file.
  - È un computer che esegue Windows 10, Windows Server 2019 o Windows Server 2022, con le ultime patch Microsoft.
  - Può connettersi alla Microsoft PowerShell Gallery per scaricare le librerie PowerShell richieste.

A seconda della versione di Windows, potrebbe essere necessario disabilitare il supporto TLS 1.0/1.1. Per ulteriori informazioni, fare riferimento alla documentazione di supporto TLS di Microsoft PowerShell Gallery.

Per impostazione predefinita, PowerShell non esegue automaticamente l'autenticazione tramite un server proxy. Assicurarsi di aver configurato la sessione PowerShell per utilizzare il server proxy come richiesto da Microsoft e dalle best practice del fornitore di proxy.

Se durante l'esecuzione degli script PowerShell vengono visualizzati errori relativi a una versione mancante o precedente di PowerShellGet, è necessario installare la versione più recente come segue:

```
1 Install-Module -Name PowerShellGet -Force -Scope CurrentUser -
     AllowClobber
2 <!--NeedCopy-->
```

**Installare le librerie e i moduli** Image Portability Service attinge alle librerie della Microsoft PowerShell Gallery per gestire le operazioni di portabilità.

> **Importante:**
>
> Dopo l'installazione iniziale, utilizzare **Update-Module** per installare le nuove versioni.

1. Eseguire il seguente comando PowerShell per scaricare i moduli più recenti:

```
Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Scope CurrentUser
<!--NeedCopy-->
```

   - Per modificare la variabile di ambiente PATH:

     Premere **Y** e **Invio** per accettare.
   - Per installare il provider NuGet:

     Premere **Y** e **Invio** per accettare.
   - Se si ricevono informazioni su un repository non attendibile:

     Premere **A** (Sì a tutti) e **Invio** per continuare.

2. Verificare che tutti i moduli necessari siano stati scaricati eseguendo il comando:

```
Get-InstalledModule -Name Citrix.*
<!--NeedCopy-->
```

   Questo comando restituisce un output simile al seguente:

| Nome | Repository | Descrizione |
|---|---|---|
| Citrix.Image.Uploader | PSGallery | Comandi per caricare un VHD(x) in un account di archiviazione di Azure, AWS o GCP e ottenere informazioni su un VHD(x) |
| Citrix.Workloads.Portability | PSGallery | Cmdlet autonomo per il processo di immagine di Citrix Image Portability Service |

**Aggiornare i moduli alla versione più recente** Eseguire il seguente comando per aggiornare lo script alla versione più recente.

```
Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Force
<!--NeedCopy-->
```

**Eseguire l'SDK Remote PowerShell di Citrix Virtual Apps and Desktops** Image Portability Service richiede che l'SDK Remote PowerShell di Citrix Virtual Apps and Desktops crei e gestisca i processi di portabilità all'interno di Citrix Cloud.

Scaricare e installare l'SDK Remote PowerShell sul proprio computer.

**Installare componenti di terze parti specifici della piattaforma** Il modulo PowerShell Image Portability Service non installa dipendenze di terze parti. Pertanto, è possibile limitare l'installazione solo alle piattaforme a cui ci si rivolge. Se si utilizza una delle seguenti piattaforme, seguire le istruzioni pertinenti per l'installazione delle dipendenze della piattaforma:

**VMware** Se si stanno creando processi di portabilità delle immagini che comunicano con l'ambiente VMware, eseguire il seguente comando per installare i moduli VMware PowerShell richiesti.

```
Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -
    Force -SkipPublisherCheck
<!--NeedCopy-->
```

**Amazon Web Services** Se si stanno creando processi di Image Portability in Azure, scaricare e installare l'interfaccia della riga di comando AWS, quindi eseguire questi comandi per installare i moduli di AWS PowerShell richiesti:

```
Install-Module -Name AWS.Tools.Installer
Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
<!--NeedCopy-->
```

**Azure** Se si stanno creando processi di Image Portability in Azure, scaricare e installare le utilità della riga di comando di Azure, quindi eseguire questi comandi per installare i moduli di Azure PowerShell richiesti:

```
Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber -
    Force
Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
<!--NeedCopy-->
```

**Google Cloud** Se si stanno creando lavori di portabilità delle immagini in Google Cloud, scaricare e installare Google Cloud SDK sul proprio computer.

**Disinstallare script e moduli** Eseguire i seguenti comandi per disinstallare i moduli utilizzati dal software Image Portability.

> **Nota:**
>
> Gli script e i componenti di terze parti non vengono rimossi automaticamente durante la disinstallazione dei moduli IPS.

Per disinstallare i moduli:

```
Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images.Uploader" | Uninstall-Module
<!--NeedCopy-->
```

### Aggiungere credenziali a Credential Wallet

Per gli scenari di automazione end-to-end, è possibile configurare Image Portability Service per l'autenticazione in modo non interattivo con Citrix Cloud, il cloud pubblico e le risorse locali. Inoltre, Image Portability Service utilizza le credenziali archiviate nel Citrix Credential Wallet ogni volta che le nostre API eseguono l'autenticazione diretta con le risorse cloud locali e pubbliche. L'impostazione delle credenziali come descritto in questa sezione è un passaggio obbligatorio per l'esecuzione di processi di esportazione, preparazione e pubblicazione.

Quando si eseguono i processi, Image Portability Service richiede l'accesso a risorse di cui si ha il controllo. Ad esempio, affinché Image Portability Service esporti un disco da un server vSphere a una condivisione SMB, il servizio richiede l'accesso a entrambi i sistemi. Per proteggere queste informazioni sull'account, Image Portability Service utilizza il servizio Citrix Credential Wallet. Questo servizio memorizza le credenziali nel portafoglio con un nome definito dall'utente. Quando si desidera eseguire un processo, è necessario fornire il nome della credenziale da utilizzare. Inoltre, queste credenziali possono essere aggiornate o eliminate dal portafoglio in qualsiasi momento.

Vengono spesso archiviate credenziali per queste piattaforme:

- Microsoft Azure
- AWS
- Google Cloud
- Condivisione SMB
- VMware vSphere
- Nutanix AHV
- XenServer

Per gestire le credenziali, fare riferimento alla sezione Image Portability Service APIs and Credentials Management del Developer API Portal.

### Utilizzare Image Portability Service

La preparazione delle immagini nelle posizioni di risorse locali nell'abbonamento al cloud pubblico richiede la creazione di processi di Image Portability all'interno di Citrix Cloud. È possibile creare un processo per effettuare chiamate API dirette al servizio all'interno dello script o del programma, oppure utilizzando i moduli PowerShell di esempio che abbiamo sviluppato per automatizzare le chiamate API. Fare riferimento a Image Portability Service Developer API Portal per informazioni sull'utilizzo delle API REST e dei moduli PowerShell per creare processi IPS.

#### Pubblicare cataloghi di macchine utilizzando Citrix Provisioning

Image Portability Service (IPS) viene utilizzato con Machine Creation Services (MCS) in Azure, AWS e Google Cloud o con Citrix Provisioning (PVS) in Azure o Google Cloud. È possibile combinare le soluzioni PowerShell e REST descritte in questa guida con gli strumenti della piattaforma, le API della piattaforma o gli SDK di Citrix DaaS per creare un flusso di lavoro end-to-end senza interruzioni e automatizzato per la creazione di un catalogo di macchine basato sull'immagine preparata. A seconda della piattaforma cloud scelta, possono essere necessari passaggi intermedi tra il completamento di un processo di preparazione IPS e la creazione di un catalogo o l'assegnazione a un target PVS.

**AWS** IPS prepara i lavori su AWS e produce un volume. I Machine Creation Services richiedono un'Amazon Machine Image (AMI) durante la creazione del catalogo. Per generare un'AMI dall'immagine migrata, è prima necessario creare un'istantanea dell'immagine dal volume risultante, quindi creare un'AMI basata su quell'istantanea. Questa operazione può essere eseguita con l'interfaccia della riga di comando (CLI) di AWS:

```
> aws ec2 create-snapshot --volume-id <VolumeId>
> aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
    root-device-name '/dev/sda1 --boot-mode uefi --ena-support --
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
 SnapshotId=<SnapshotID> }
 '
<!--NeedCopy-->
```

<VolumeId> è l'output del processo di preparazione IPS. L'AMI risultante può essere utilizzata come immagine master MCS.

È disponibile uno script di esempio di PowerShell per automatizzare questa parte del flusso di lavoro nel modulo Citrix.Workloads.Portability come script denominato New-ImsAwsImage.ps1.

**Azure** In Azure, IPS produce dischi gestiti che sono direttamente utilizzabili come immagini master MCS. Per assegnare l'immagine risultante ai target PVS, IPS fornisce un'operazione di "pubblicazione" per copiare il disco gestito in un file VHD(x) nello store PVS.

**Google Cloud** Gli IPS preparano i lavori su Google Cloud e producono un disco. MCS richiede un modello di istanza Google Cloud. Il processo per la creazione di un modello di istanza MCS da un disco è descritto in dettaglio in Preparare un'istanza di macchina virtuale master e un disco persistente.

Per i target PVS su Google Cloud, IPS fornisce un'operazione di "pubblicazione"per copiare il disco in un file VHD(x) nello store PVS.

#### Automatizzare la configurazione VDA

Quando si prepara un'immagine gestita da Citrix che ha avuto origine in locale, è possibile riconfigurare il VDA all'interno dell'immagine per supportare l'ambiente di destinazione per il quale l'immagine viene preparata. Image Portability Service può applicare le modifiche alla configurazione VDA in tempo reale durante la fase di preparazione del flusso di lavoro. Esistono tre parametri di configurazione che definiscono il funzionamento del VDA nell'immagine migrata: **InstallMisa**, **InstallPvs** e **XdReconfigure**. Definire questi parametri durante la creazione di processi IPS come segue:

```
InstallMisa = $true
<!--NeedCopy-->
```

La configurazione di **InstallMisa** su **true** consente a Image Portability Service di installare tutti i componenti VDA mancanti necessari per il provisioning dell'immagine utilizzando MCS.

La configurazione di **InstallMisa** su **true** richiede anche la configurazione di **CloudProvisioningType** su **Mcs**.

```
InstallPvs = '2206'
<!--NeedCopy-->
```

La versione del server PVS con cui viene utilizzata l'immagine: (string, default $null). Ad esempio: 2206, 7.33 o 2203cu1 (richiesto se il tipo di provisioning è PVS).

Impostare **InstallPvs** sulla versione del server PVS in cui viene distribuita l'immagine. Quando **InstallPvs** è impostato, Image Portability Service installa automaticamente la versione specificata del software del dispositivo di destinazione PVS contenuto nell'immagine durante i processi di preparazione. IPS supporta le due build più recenti (versione base o aggiornamenti cumulativi) delle ultime due Long-Term Service Release (LTSR) e le versioni correnti (CR).

La configurazione di **InstallPvs** richiede inoltre che **CloudProvisioningType** sia configurato su **Pvs**.

Sia per **InstallMisa** che per **InstallPvs**, tenere presente quanto segue:

- Solo le recenti versioni LTSR e CR del VDA supportano questa funzionalità.
- Se i componenti necessari sono già presenti per il VDA installato, non vengono apportate modifiche, anche se i parametri sono configurati.

- Per le versioni supportate di VDA, Image Portability installa la versione appropriata dei componenti richiesti, anche se non sono presenti i componenti VDA necessari.
- Per le versioni non supportate del VDA, la riconfigurazione non riesce e viene registrato un messaggio se non sono presenti i componenti VDA necessari. Il processo di preparazione viene completato anche se la riconfigurazione VDA non è stata completata.

**XdReconfigure** richiede uno dei seguenti valori: **controllers** o **site_guid**. Ecco alcuni esempi di parametri di configurazione che utilizzano ciascun valore:

Utilizzando **controller**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'controllers'
        ParameterValue = 'comma-separated-list-of-your-cloud-connectors
           -fqdns'
     }

)
<!--NeedCopy-->
```

dove **ParameterValue** è l'elenco dei nomi di dominio completo dei nuovi DDC a cui si desidera puntare il VDA. È possibile specificare più DDC in un formato separato da virgole.

Utilizzando **site_guid**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'site_guid'
        ParameterValue = 'active-directory-site-guid'
     }

)
<!--NeedCopy-->
```

**XdReconfigure** accetta anche i valori supportati quando si esegue il programma di installazione dalla riga di comando VDA con lo switch di installazione **/reconfigure**, ad esempio **XenDesktopVdaSetup.exe /reconfigure**. Alcuni esempi di questi valori sono **wem_agent_port**, **wem_cached_data_sync_port**, **wem_cloud_connectors** o **wem_server**. Per un elenco completo delle opzioni della riga di comando di riconfigurazione VDA, legere la documentazione dei VDA Citrix DaaS.

> **Nota:**
>
> È possibile utilizzare `-DryRun` durante l'esecuzione dei comandi per convalidare la configurazione e le impostazioni di rete del dispositivo connettore.

## Riferimenti

Questa sezione fornisce informazioni tecniche di riferimento, basate su ciò che occorre.

### Autorizzazioni richieste dai servizi di Image Portability Services

Questa sezione descrive in dettaglio le autorizzazioni richieste da Image Portability Service su ciascuna delle piattaforme cloud e locali supportate.

**Autorizzazioni richieste da Connector Appliance** Connector Appliance deve accedere ai seguenti URL per preparare le immagini nell'Image Portability Service:

```
*.layering.cloud.com
credentialwallet.citrixworkspaceapi.net
graph.microsoft.com
login.microsoftonline.com
management.azure.com
*.blob.storage.azure.net
<!--NeedCopy-->
```

**Autorizzazioni richieste da VMware vCenter** Le seguenti autorizzazioni vCenter sono necessarie per eseguire il processo di esportazione del disco IPS in un ambiente VMware. Queste autorizzazioni sono disponibili in **Roles** (Ruoli) nella sezione **Access Control** (Controllo accessi) del pannello di amministrazione di vCenter.

```
- Cryptographic operations
    - Direct Access

- Datastore
    - Allocate space
    - Browse datastore
    - Low level file operations
    - Remove file

- Folder
    - Create folder
    - Delete folder

- Network
    - Assign network

- Resource
    - Assign virtual machine to resource pool

- Virtual machine
    - Change Configuration
        - Add existing disk
```

```
23          - Add new disk
24          - Remove disk
25
26      - Edit Inventory
27          - Create from existing
28          - Create new
29          - Remove
30
31      - Interaction
32          - Power off
33          - Power on
34  <!--NeedCopy-->
```

**Autorizzazioni richieste per Microsoft Azure** Image Portability richiede che l'account del servizio Azure disponga delle seguenti autorizzazioni.

Quando viene specificato il gruppo di risorse da utilizzare per il Compositing Engine (ovvero nella proprietà *resourceGroup* in una richiesta REST o nel parametro *-AzureVmResourceGroup* quando si utilizzano i comandi PowerShell Citrix.Workloads.Portability), sono necessarie le seguenti autorizzazioni nell'ambito del gruppo di risorse.

```
1  Microsoft.Compute/disks/beginGetAccess/action
2  Microsoft.Compute/disks/endGetAccess/action
3  Microsoft.Compute/disks/delete
4  Microsoft.Compute/disks/read
5  Microsoft.Compute/disks/write
6  Microsoft.Compute/virtualMachines/delete
7  Microsoft.Compute/virtualMachines/powerOff/action
8  Microsoft.Compute/virtualMachines/read
9  Microsoft.Compute/virtualMachines/write
10 Microsoft.Network/networkInterfaces/delete
11 Microsoft.Network/networkInterfaces/join/action
12 Microsoft.Network/networkInterfaces/read
13 Microsoft.Network/networkInterfaces/write
14 Microsoft.Network/networkSecurityGroups/delete
15 Microsoft.Network/networkSecurityGroups/join/action
16 Microsoft.Network/networkSecurityGroups/read
17 Microsoft.Network/networkSecurityGroups/write
18 Microsoft.Resources/deployments/operationStatuses/read
19 Microsoft.Resources/deployments/read
20 Microsoft.Resources/deployments/write
21 Microsoft.Resources/subscriptions/resourcegroups/read
22 <!--NeedCopy-->
```

Quando il gruppo di risorse da utilizzare per il Compositing Engine non viene specificato, sono necessarie le seguenti autorizzazioni nell'ambito della sottoscrizione.

```
1  Microsoft.Compute/disks/beginGetAccess/action
2  Microsoft.Compute/disks/endGetAccess/action
3  Microsoft.Compute/disks/read
```

```
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Authorization/roleAssignments/read
Microsoft.Authorization/roleDefinitions/read
<!--NeedCopy-->
```

Le seguenti autorizzazioni sono necessarie nell'ambito del gruppo di risorse di destinazione specificato (ovvero il gruppo di risorse specificato nella proprietà *targetDiskResourceGroupName* in una richiesta REST o nel parametro *-TargetResourceGroup* quando si utilizza PowerShell).

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/snapshots/delete
Microsoft.Compute/snapshots/read
Microsoft.Compute/snapshots/write
<!--NeedCopy-->
```

Le seguenti autorizzazioni sono necessarie nell'ambito del gruppo di risorse di rete virtuale specificato (ovvero il gruppo di risorse specificato nella proprietà *virtualNetworkResourceGroupName* in una richiesta REST o nel parametro *-AzureVirtualNetworkResourceGroupName* quando si utilizza PowerShell).

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
<!--NeedCopy-->
```

> **Importante:**
>
> L'opzione `ceVmSku` per i processi "prepare"e ' "prepareAndPublish" 'controlla il tipo di macchina virtuale di Azure a cui è adatto il disco gestito risultante. È necessario selezionare un ceVmSku con la stessa famiglia e versione delle VM di cui si intende effettuare il provisioning dall'immagine di output. Il valore predefinito di `Standard_D2S_v3` è adatto all'esecuzione su tutte le macchine della famiglia v3 D. Con gli SKU di macchine virtuali v4 e più recenti, Microsoft ha reso opzionale il disco di risorse temporaneo collegato alle macchine virtuali. Ciò

> influisce sul corretto posizionamento dei file di paging. Se si intende utilizzare uno SKU VM *senza* un disco di risorse temporaneo per le macchine di cui si esegue il provisioning utilizzando l'immagine di output, è necessario assicurarsi che neanche il proprio ceVmSku abbia un disco di risorse temporaneo. Se il ceVmSku è di tipo dotato di un disco di risorse temporaneo, IPS sposta il file di paging di Windows su quel disco. Se si utilizza un disco preparato in questo modo su uno SKU che non dispone di un disco di risorse temporanee, viene visualizzata una finestra di avviso a ogni accesso. Se il ceVmSku non dispone di un disco temporaneo, il file di paging viene configurato nel volume principale del sistema. Ciò potrebbe comportare costi di I/O non intenzionali se si utilizza un'immagine preparata in questo modo su uno SKU che include un disco di risorse temporaneo.

**Autorizzazioni richieste da Google Cloud** Image Portability richiede che l'account del servizio Google Cloud disponga delle seguenti autorizzazioni:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.stop
compute.instances.updateDisplayDevice
compute.networks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
iam.serviceAccounts.get
iam.serviceAccounts.list
resourcemanager.projects.get
storage.buckets.create
```

```
storage.buckets.delete
storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

**Autorizzazioni richieste da AWS** Image Portability richiede di allegare all'utente Identity and Access Management (IAM) un documento di criteri JSON con la seguente configurazione:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ec2:CreateTags",
                "ec2:CreateImage",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:RebootInstances",
                "ec2:RegisterImage",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> **Nota:**
>
> Se necessario, potrebbe essere utile ridurre ulteriormente l'ambito della risorsa.

**Autorizzazioni necessarie per Nutanix AHV** Per usufruire della portabilità delle immagini è necessario essere amministratore del cluster nella configurazione Nutanix AHV.

**Autorizzazioni richieste per XenServer** Image Portability richiede almeno il ruolo di "mministratore VM"per il pool in cui si trova l'host XenServer.

**Rete** Image Portability Service (IPS) crea una macchina virtuale di lavoro chiamata Compositing Engine (CE) per eseguire operazioni sulle immagini. Tutte le Connector Appliance che si trovano nella posizione risorsa/zona associata devono essere in grado di comunicare tramite HTTPS con la CE. Tutte le comunicazioni tra una Connector Appliance (CA) e la CE vengono avviate dalla CA con una singola eccezione per vSphere in cui esiste una comunicazione HTTPS bidirezionale tra CE e CA.

Negli ambienti cloud (Azure, AWS, Google Cloud) la CE viene creata con un indirizzo IP privato. Quindi la CE deve trovarsi sulla stessa rete virtuale della CA o su una rete virtuale raggiungibile dalla CA.

Inoltre, per i processi che coinvolgono file su una condivisione SMB (ad esempio, processi di esportazione), la CE deve trovarsi su una rete con connettività alla condivisione SMB.

Vedere la documentazione dell'API Image Portability Service per dettagli su come specificare la rete da utilizzare per la CE in ciascuna piattaforma supportata.

Per i processi di "preparazione", il sistema operativo contenuto nell'immagine viene avviato (sulla CE) per eseguire operazioni di specializzazione e di altro tipo. Se l'immagine contiene agenti di gestione o di sicurezza che telefonano a un server di controllo, questi processi possono interferire con il processo di preparazione.

Se viene specificata l'opzione di annullamento dell'accesso al dominio, la connettività di rete può influire sui risultati. Se la VM del motore di composizione può raggiungere il controller di dominio Active Directory tramite la rete, l'annullamento dell'accesso rimuove l'account computer dal dominio. Questo interrompe l'appartenenza al dominio della VM di origine da cui è stata estratta l'immagine.

Pertanto, si consiglia di isolare la rete fornita per l'operazione da altre risorse di rete. Questa operazione può essere eseguita mediante l'isolamento della sottorete o con le regole del firewall. Vedere Isolamento della rete per i dettagli.

In alcuni ambienti hypervisor locali, l'hypervisor può essere configurato con un certificato del server TLS, che non è considerato attendibile dal set di autorità di certificazione root attendibili della CA o non corrisponde al nome host del server. In tali situazioni, **IPS fornisce proprietà di richiesta di processo** che possono essere utilizzate per risolvere il problema. Vedere Certificati TLS per i dettagli.

**Proxy di rete** Se il traffico di rete tra la CA e Internet attraversa un proxy che esegue l'introspezione TLS, potrebbe essere necessario aggiungere l'autorità di certificazione radice del proxy (ovvero il cer-

tificato che il proxy utilizza per firmare i certificati TLS che genera) al set di autorità di certificazione root della CA. Per ulteriori informazioni, vedere Registrare il Connector Appliance con Citrix Cloud.

**Isolamento della rete**

- Azure

  In Azure, per impostazione predefinita, la CE viene creata con un gruppo di sicurezza di rete (NSG) collegato alla relativa NIC se l'entità servizio di Azure usata nell'operazione dispone delle autorizzazioni Azure necessarie [1].

  Questo NSG è configurato per bloccare tutto il traffico in entrata/uscita dal CE con le seguenti eccezioni:

  - SMB (porta 445) in uscita
  - HTTPS (porta 443) in entrata
  - quello richiesto per i servizi interni di Azure

  L'uso di NSG può essere forzato impostando la proprietà *networkIsolation* nella richiesta di processo su *true*. In questo caso il processo ha esito negativo se l'entità principale del servizio utilizzata nell'operazione non dispone delle autorizzazioni necessarie. L'uso di NSG può essere disabilitato impostando la proprietà *NetworkIsolation* su *false*.

- AWS

In AWS, per ottenere l'isolamento della rete della CE, è possibile creare uno o più gruppi di sicurezza di rete che bloccano tutto il traffico indesiderato e quindi, nella richiesta di processo, assegnare i gruppi di sicurezza all'istanza della CE utilizzando il parametro di richiesta *securityGroupIds* che accetta come valore un elenco di ID del gruppo di sicurezza.

- Google Cloud

In Google Cloud per ottenere l'isolamento della rete della CE, è possibile creare regole firewall che bloccano tutto il traffico indesiderato e quindi applicare tali regole alla CE tramite tag di rete. IPS crea la CE con il *Compositing Engine* dei tag di rete ed è possibile assegnarle altri tag di rete utilizzando il parametro di richiesta di processo *networkTags* che accetta un elenco di tag come valore.

**Certificati TLS** Se il certificato del server dell'hypervisor è firmato da un'autorità non considerata attendibile dalla CA, è possibile utilizzare due approcci alternativi per risolvere il problema.

1. Specificare nella richiesta di lavoro un ulteriore certificato dell'autorità di certificazione radice da utilizzare nella verifica del certificato. Questo certificato deve essere l'autorità di certificazione radice utilizzata per firmare il certificato del server dell'hypervisor.

2. Specificare nella richiesta di lavoro l'impronta digitale SHA-1 del certificato del server dell'hypervisor. In questo caso la convalida del certificato viene effettuata verificando che l'impronta digitale SHA-1 del certificato restituito dall'hypervisor corrisponda a quella fornita nella richiesta di lavoro. Tenere presente che questo metodo potrebbe non funzionare se è presente un proxy di intercettazione TLS tra CE e l'hypervisor.

I parametri delle richieste di processo relative a quanto sopra, indicati rispettivamente di seguito per ciascuna piattaforma, sono:

- vSphere
    1. vCenterSslCaCertificate
    2. vCenterSslFingerprint
- Nutanix
    1. prismSslCaCertificate
    2. prismSslFingerprint
- XenServer
    1. xenSslCaCertificate
    2. xenSslFingerprint

Vedere la documentazione dell'API di Image Portability Service per ulteriori dettagli.

Possono verificarsi errori di convalida dei certificati anche in caso di mancata corrispondenza tra il nome host del server hypervisor e il nome host contenuto nel relativo certificato. In questo caso la corrispondenza del nome host può essere disabilitata impostando il seguente parametro su *true* nella richiesta di lavoro:

- vSphere
    - vCenterSslNoCheckHostname
- Nutanix
    - prismSslNoCheckHostname
- XenServer
    - xenSslNoCheckHostname

### Documentazione correlata

- Documentazione dell'API Image Portability Service
- Connector Appliance per servizi cloud

- Documentazione di Google Cloud
- Account del servizio Google Cloud
- Registrazione e autenticazione delle app Microsoft Azure

1. If per l'operazione viene utilizzato un gruppo di risorse esplicito, le seguenti autorizzazioni nell'ambito del gruppo di risorse:
   - Microsoft.Network/networkSecurityGroups/join/action
   - Microsoft.Network/networkSecurityGroups/read
   - Microsoft.Network/networkSecurityGroups/write

   Otherwise the following permissions at the scope of the subscription if no explicit resource group is being used:

   - Microsoft.Network/networkSecurityGroups/delete
   - Microsoft.Network/networkSecurityGroups/join/action
   - Microsoft.Network/networkSecurityGroups/read
   - Microsoft.Network/networkSecurityGroups/write

## Stampa

October 6, 2022

La gestione delle stampanti nell'ambiente è un processo multistadio:

1. Acquisire familiarità con i concetti di stampa, se non la si ha già.
2. Pianificare l'architettura di stampa. Ciò include l'analisi delle esigenze aziendali, dell'infrastruttura di stampa esistente, del modo in cui gli utenti e le applicazioni interagiscono con la stampa oggi e di quale modello di gestione della stampa si applica meglio all'ambiente in uso.
3. Configurare l'ambiente di stampa selezionando un metodo di provisioning della stampante e quindi creando criteri per la distribuzione del progetto di stampa. Aggiornare i criteri quando vengono aggiunti nuovi dipendenti o server.
4. Verificare una configurazione di stampa pilota prima di distribuirla agli utenti.
5. Effettuare la manutenzione dell'ambiente di stampa Citrix gestendo i driver della stampante e ottimizzando le prestazioni di stampa.
6. Risolvere i problemi che potrebbero sorgere.

Per informazioni complete sulla stampa in un ambiente Citrix DaaS (in precedenza chiamato servzio Citrix Virtual Apps and Desktops), iniziare da Print (Stampa). Da questo articolo, si può passare a:

- Esempi di configurazione di stampa

- Procedure consigliate
- Criteri di stampa e preferenze
- Provisioning delle stampanti
- Mantenere l'ambiente di stampa

### Installare il componente Universal Print Server sui server di stampa

1. Verificare che su ogni server di stampa sia installato Microsoft Virtual C++ Runtime 2017, a 32 bit e a 64 bit.
2. Accedere alla pagina di download di Citrix Universal Print Server e fare clic su **Download File** (Scarica file).
3. Eseguire uno dei seguenti comandi su ciascun server di stampa:
    - Per un sistema operativo a 32 bit: **UpsServer_x86.msi**.
    - Per un sistema operativo a 64 bit: **UpsServer_x64.msi**.

Dopo aver installato Universal Print Server, configurarlo utilizzando le istruzioni fornite in Provisioning delle stampanti.

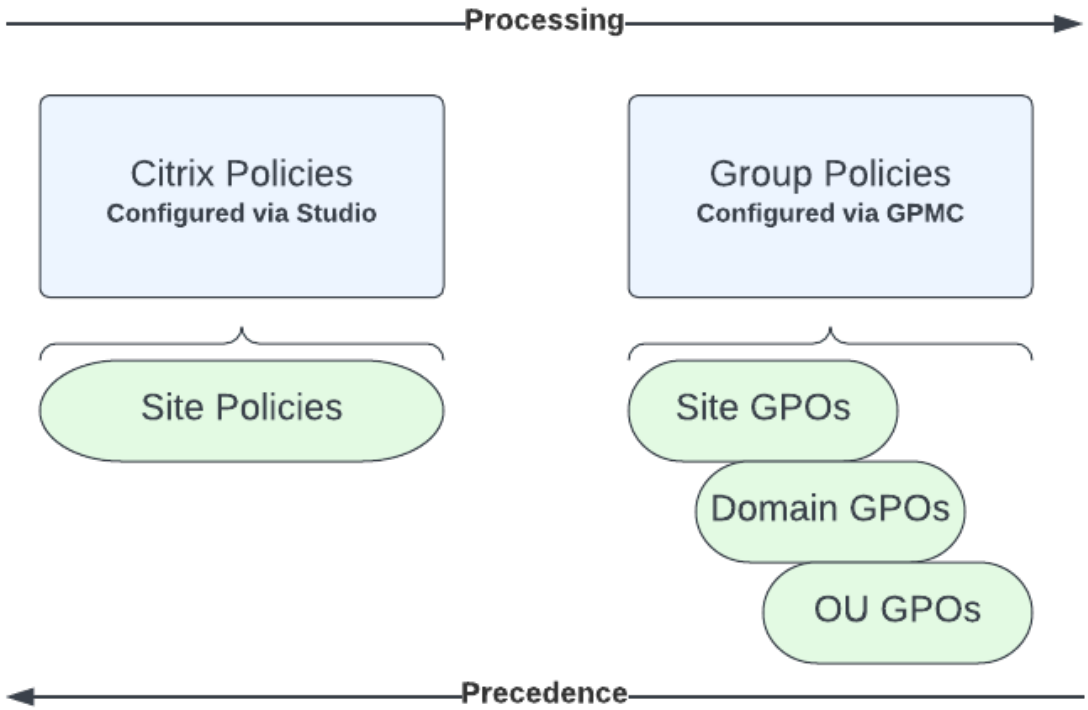
## Criteri

April 14, 2023

I criteri sono una raccolta di impostazioni che definiscono la modalità di gestione delle sessioni, della larghezza di banda e della sicurezza per un gruppo di utenti, di dispositivi o di tipi di connessione.

È possibile applicare le impostazioni dei criteri ai VDA o agli utenti. È possibile modificare le impostazioni in Web Studio o negli oggetti dei criteri di gruppo (GPO) di Active Directory. È possibile specificare filtri (assegnazioni di oggetti) per i criteri. Se non si assegnano criteri specifici ai filtri, le impostazioni vengono applicate a tutte le sessioni utente.




È possibile applicare criteri a diversi livelli della rete. Le impostazioni dei criteri posizionate a livello di oggetto Criteri di gruppo unità organizzativa hanno la precedenza più alta sulla rete. I criteri a livello di oggetto Criteri di gruppo di dominio sostituiscono i criteri a livello di oggetto Criteri di gruppo del sito. I criteri a livello di oggetto Criteri di gruppo del sito ignorano eventuali criteri in conflitto a livello di Criteri locali di Microsoft e Citrix.

Tutti i criteri del sito Citrix vengono creati e gestiti nella console Citrix Studio e memorizzati nel database del sito. I criteri di gruppo vengono creati e gestiti tramite la Console Gestione Criteri di gruppo Microsoft (GPMC) e archiviati nell'Active Directory. I criteri locali Microsoft vengono creati nel sistema operativo Windows e vengono memorizzati nel Registro di sistema.

Web Studio utilizza una Modellazione guidata per aiutare gli amministratori a confrontare le impostazioni di configurazione all'interno di modelli e criteri per aiutare a eliminare le impostazioni in conflitto e ridondanti.

Le impostazioni vengono unite in base alla priorità e alla loro condizione. Qualsiasi impostazione disabilitata sostituisce un'impostazione abilitata a livello inferiore. Le impostazioni dei criteri non configurati vengono ignorate e non sostituiscono le impostazioni di livello inferiore.

I criteri di Web Studio possono inoltre avere conflitti con i criteri di gruppo in Active Directory e potrebbero sovrascriversi reciprocamente a seconda della situazione.

Tutti i criteri vengono elaborati nel seguente ordine:

1. Dall'app Citrix Workspace, l'utente finale accede a un VDA utilizzando le credenziali di dominio.
2. I criteri Citrix vengono elaborati per l'utente finale e per il VDA
3. I criteri vengono applicati nel seguente ordine:
    a) Criteri locali
    b) Criteri del sito
    c) Criteri di dominio
    d) Criteri OU (unità organizzativa)

> **Nota:**
>
> - È possibile che non siano presenti tutti i criteri ai quattro livelli. Per la maggior parte dei clienti, vengono utilizzati solo i criteri del sito. I criteri locali richiedono all'utente di accedere al VDA per modificare i criteri. Pertanto, questi criteri non vengono quasi mai utilizzati.
> - Non è supportata la combinazione di criteri Windows e Citrix nello stesso oggetto Criteri di gruppo.

Per informazioni complete sui criteri Citrix, vedere le pagine seguenti:

- Lavorare con i criteri
- Modelli di criteri
- Creare criteri
- Assegnare priorità ai criteri, modellarli, confrontarli e risolverne i problemi
- Impostazioni dei criteri predefinite
- Riferimento alle impostazioni dei criteri

> **Nota:**
>
> i riferimenti alle impostazioni dei criteri per Citrix DaaS sono gli stessi delle impostazioni dei criteri per Citrix Virtual Apps and Desktops. Pertanto, è possibile fare riferimento anche alla sezione Riferimento alle impostazioni dei criteri nella documentazione di Citrix Virtual Apps and Desktops per Citrix DaaS.

## Lavorare con i criteri

May 23, 2023

Configurare i criteri Citrix per controllare l'accesso degli utenti e gli ambienti delle sessioni. I criteri Citrix sono il metodo più efficiente per controllare le impostazioni relative a connessione, sicurezza e

larghezza di banda. È possibile creare criteri per gruppi specifici di utenti, dispositivi o tipi di connessione. Ogni criterio può contenere più impostazioni.

### Strumenti per lavorare con i criteri Citrix

- Studio: i criteri creati utilizzando Studio vengono archiviati nel database del sito e gli aggiornamenti vengono inviati al VDA in uno dei seguenti casi:
  - Quando quel VDA si registra con Controller
  - Quando un utente avvia una sessione
- Console di gestione dei criteri di gruppo: se l'ambiente di rete utilizza Active Directory e si dispone dell'autorizzazione per gestire i criteri di gruppo, è possibile utilizzare la Group Policy Management Console (GPMC) per creare e modificare i criteri per il sito. Nella console, è possibile configurare gli oggetti Criteri di gruppo (GPO) con le impostazioni e i filtri desiderati. Questi criteri avranno la priorità rispetto ai criteri configurati in Studio. Per ulteriori informazioni, vedere CTX238166.

### Ordine di elaborazione e precedenza dei criteri

Le impostazioni dei criteri di gruppo vengono elaborate nell'ordine seguente:

1. Citrix DaaS Site GPO (archiviato nel database del sito)
2. Oggetti Criteri di gruppo a livello di dominio
3. Unità organizzative

Tuttavia, se vengono applicate impostazioni diverse per lo stesso criterio in due GPO, le impostazioni dei criteri elaborate per ultime sovrascrivono quelle elaborate in precedenza. Questa configurazione implica che le impostazioni dei criteri hanno la precedenza nell'ordine seguente:

1. Unità organizzative
2. Oggetti Criteri di gruppo a livello di dominio
3. GPO del sito Citrix DaaS (archiviato nel database del sito)

Quando si utilizzano più criteri, è possibile assegnare priorità ai criteri che contengono impostazioni in conflitto. Per ulteriori informazioni, vedere Assegnare priorità ai criteri, modellarli, confrontarli e risolverne i problemi.

### Flusso di lavoro per i criteri Citrix

Il processo di configurazione dei criteri è il seguente:

1. Creare il criterio.
2. Configurare le impostazioni dei criteri.
3. Assegnare il criterio agli oggetti macchina e utente.
4. Assegnare una priorità al criterio.
5. Verificare il criterio effettivo eseguendo la Modellazione guidata Criteri di gruppo Citrix.

> **Nota:**
>
> Per aprire la Modellazione guidata Criteri di gruppo Citrix, andare alla scheda **Policies > Modeling** (Criteri > Modellazione) e quindi fare clic su **Launch Modeling Wizard** (Avvia Modellazione guidata) nel riquadro **Actions** (Azioni). La scheda **Modeling** è disponibile in Web Studio ospitato in Citrix Cloud su richiesta del cliente.

### Esplorare i criteri e le impostazioni Citrix

Le impostazioni dei criteri vengono ordinate in categorie in base alla funzione o alla funzionalità a cui si riferiscono. Ad esempio, la sezione Profile Management include le impostazioni dei criteri per la gestione dei profili.

- Le impostazioni del computer (impostazioni dei criteri applicabili alle macchine) definiscono il comportamento dei desktop virtuali e vengono applicate all'avvio di un desktop virtuale. Queste impostazioni si applicano anche quando non sono presenti sessioni utente attive sul desktop virtuale.
- Le impostazioni utente definiscono l'esperienza dell'utente. Le impostazioni utente vengono applicate quando un utente si connette o si riconnette.

Per accedere ai criteri, alle impostazioni o ai modelli, selezionare **Policies** (Criteri) nel riquadro di navigazione di Web Studio.

- Nella scheda **Policies** (Criteri) sono elencati tutti i criteri. Quando si seleziona un criterio, le schede in basso visualizzano:
  - Overview (Panoramica): elenca nome, priorità, stato attivato/disattivato e descrizione
  - Settings (Impostazioni): elenca tutte le impostazioni configurate
  - Assigned To (Assegnato a): indica il gruppo di consegna. È possibile modificare o rimuovere le impostazioni di "Assigned To". Applicare il criterio in base all'appartenenza al gruppo di consegna del desktop che esegue la sessione. Per ulteriori informazioni, vedere Creare criteri.
- Nella scheda **Templates** (Modelli) sono elencati i modelli forniti da Citrix e quelli personalizzati che sono stati creati. Quando si seleziona un modello, le schede in basso visualizzano:

  - Descrizione (perché potrebbe essere utile usare il modello);
  - Impostazioni (elenco delle impostazioni configurate). Per ulteriori informazioni, vedere Modelli di criteri.
  - La scheda **Comparison** (Confronto) consente di confrontare le impostazioni di un criterio o di un modello con quelle di altri criteri o modelli. Ad esempio, si potrebbe voler verificare i valori delle impostazioni per garantire la conformità alle procedure consigliate. Per ulteriori informazioni, vedere Assegnare priorità ai criteri, modellarli, confrontarli e risolverne i problemi.
  - Dalla scheda **Modeling** (Modellazione), è possibile simulare gli scenari di connessione con i criteri Citrix. Per ulteriori informazioni, vedere Assegnare priorità ai criteri, modellarli, confrontarli e risolverne i problemi.

  Per cercare un'impostazione in un criterio o in un modello:

  1. Selezionare il criterio o il modello.
  2. Selezionare la scheda **Edit policy** (Modifica criterio) o **Edit Template** (Modifica modello).
  3. Nella pagina **Select Settings** (Seleziona impostazioni), iniziare a digitare il nome dell'impostazione.

  È possibile restringere l'ambito di ricerca selezionando:

  - Una categoria (ad esempio la larghezza di banda)
  - La casella di controllo **View selected only** (Visualizza solo selezionati)
  - Per cercare solo le impostazioni che sono state aggiunte al criterio selezionato.

- Per cercare un'impostazione all'interno di un criterio:

  1. Selezionare il criterio.
  2. Selezionare la scheda **Settings** (Impostazioni) e digitare il nome dell'impostazione.

Una volta creato, un criterio è indipendente dal modello utilizzato. È possibile utilizzare il campo **Description** (Descrizione) di un nuovo criterio per tenere traccia del modello di origine utilizzato.

## Modelli di criteri

November 16, 2022

I modelli sono un'origine per la creazione di criteri da un punto di partenza predefinito. I modelli Citrix integrati, ottimizzati per ambienti specifici o condizioni di rete, possono essere utilizzati come:

- Fonte per la creazione di criteri e modelli personalizzati da condividere tra siti.

- Un riferimento per un confronto più semplice dei risultati tra le distribuzioni, in quanto si è in grado di citare i risultati, ad esempio, "…quando si utilizza il modello Citrix x o y…".
- Un metodo per comunicare i criteri al supporto Citrix o a terze parti attendibili. Lo si può fare importando o esportando modelli.

### Modelli Citrix incorporati

Sono disponibili i seguenti modelli di criteri:

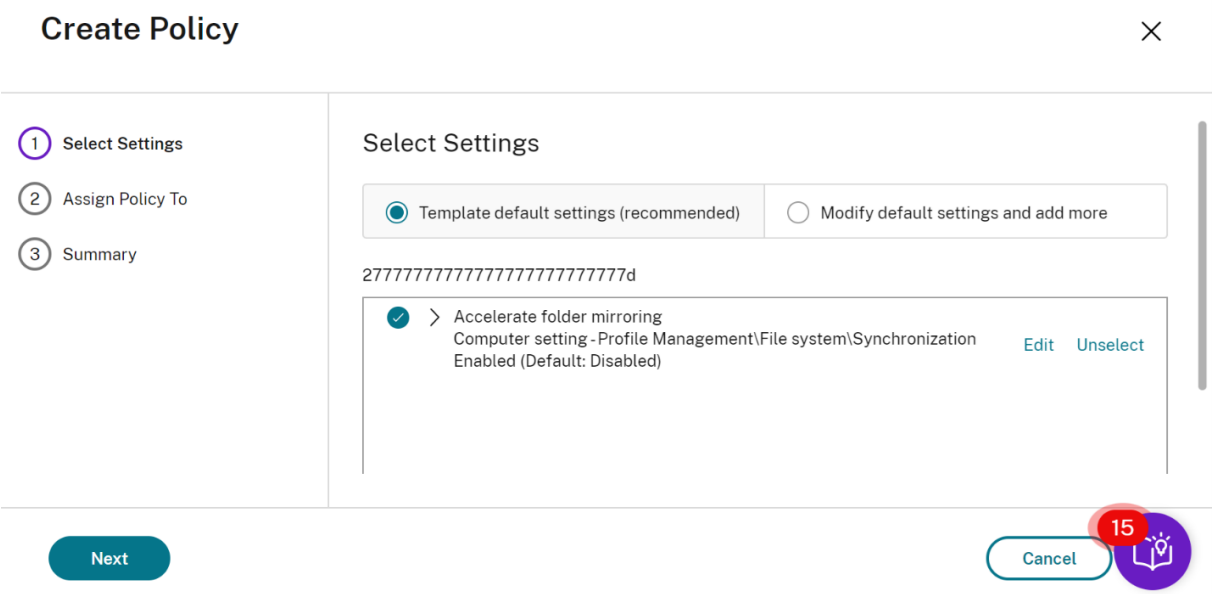
- **Very High Definition User Experience** (Esperienza utente ad altissima definizione). Questo modello applica le impostazioni predefinite che ottimizzano l'esperienza utente. Utilizzare questo modello in scenari in cui più criteri vengono elaborati in ordine di precedenza.
- **High Server Scalability** (Elevata scalabilità server). Applicare questo modello per risparmiare risorse del server. Questo modello consente di bilanciare l'esperienza utente e la scalabilità del server. Offre una buona esperienza utente aumentando al contempo il numero di utenti che è possibile ospitare su un singolo server. Questo modello non utilizza un codec video per la compressione della grafica e impedisce il rendering multimediale sul lato server.
- **High Server Scalability-Legacy OS** (Sistema operativo legacy ad alta scalabilità server). Questo modello di scalabilità server elevata si applica solo ai VDA che eseguono Windows Server 2008 R2 o Windows 7 e versioni precedenti. Questo modello si basa sulla modalità grafica legacy, che è più efficiente per tali sistemi operativi.
- **Optimized for NetScaler SD-WAN** (Ottimizzato per NetScaler SD-WAN). Applicare questo modello per gli utenti che lavorano nelle filiali con NetScaler SD-WAN per ottimizzare la distribuzione di Citrix Virtual Desktops (NetScaler SD-WAN è il nuovo nome di CloudBridge).
- **Optimized for WAN** (Ottimizzato per WAN). Questo modello è destinato ai task worker delle filiali che utilizzano WAN condivise o sedi remote con connessioni a larghezza di banda ridotta. I task worker accedono alle applicazioni con interfacce utente graficamente semplici e pochi contenuti multimediali. Questo modello ottimizza l'efficienza della larghezza di banda a scapito dell'esperienza di riproduzione video e di una parte della scalabilità dei server.
- **Optimized for WAN-Legacy OS** (Ottimizzato per WAN-sistema operativo legacy). Questo modello si applica solo ai VDA che eseguono Windows Server 2008 R2 o Windows 7 e versioni precedenti. Questo modello si basa sulla modalità grafica legacy, che è più efficiente per tali sistemi operativi.
- **Security and Control** (Sicurezza e controllo). Utilizzare questo modello in ambienti con bassa tolleranza al rischio, per ridurre al minimo le funzionalità abilitate per impostazione predefinita in Citrix DaaS. Questo modello include impostazioni che disabilitano l'accesso a quanto segue:
  - Stampa

- Appunti
- Dispositivi periferici
- Mappatura delle unità
- Reindirizzamento delle porte
- Accelerazione flash sui dispositivi degli utenti

L'applicazione di questo modello potrebbe utilizzare più larghezza di banda e ridurre la densità utente per server.

Sebbene sia consigliato utilizzare i modelli Citrix incorporati con le relative impostazioni predefinite, esistono impostazioni che non hanno un valore specifico consigliato. Ad esempio, **Overall session bandwidth limit** (Limite di larghezza di banda generale della sessione), opzione inclusa nei modelli Optimized for WAN (Ottimizzato per WAN). In questo caso, il modello mette in evidenza l'impostazione in modo che l'amministratore capisca che è probabile che questa impostazione si applichi allo scenario.




Si consideri di stare lavorando con una distribuzione (gestione dei criteri e dei VDA) precedente a XenApp e XenDesktop 7.6 FP3. Sono inoltre richiesti High Server Scalability (Elevata scalabilità del server) e modelli Optimized for WAN (Ottimizzati per WAN). In questo caso, utilizzare le versioni del sistema operativo Legacy di questi modelli quando applicabili.

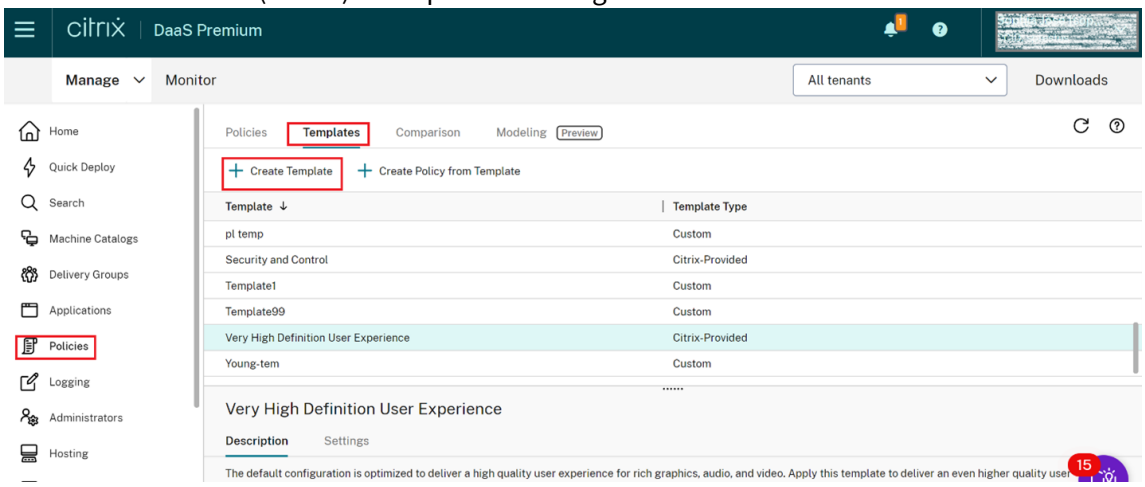
> **Nota:**
>
> Citrix crea e aggiorna i modelli incorporati. Non è possibile modificare o eliminare questi modelli.

### Creare e gestire i modelli utilizzando Web Studio

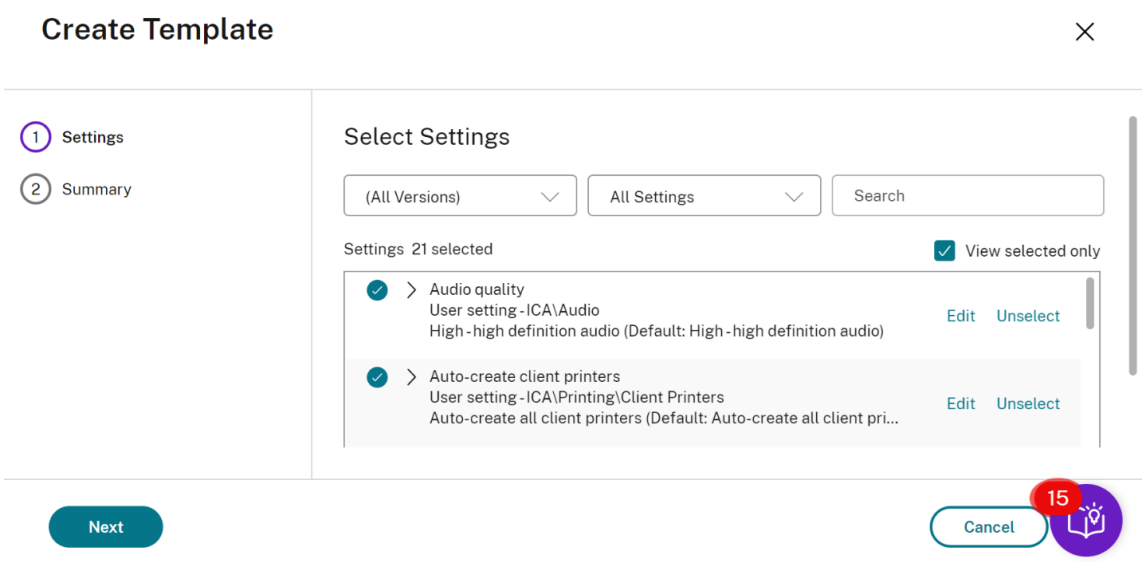
Per creare un modello basato su un modello:

1. Selezionare **Policies** (Criteri) nel riquadro di navigazione di Web Studio.




2. Selezionare la scheda **Templates** (Modelli), quindi selezionare il modello da cui creare il modello.
3. Selezionare la scheda **Create Template** (Crea modello). Viene visualizzata la schermata **Select Settings** (Seleziona impostazioni).



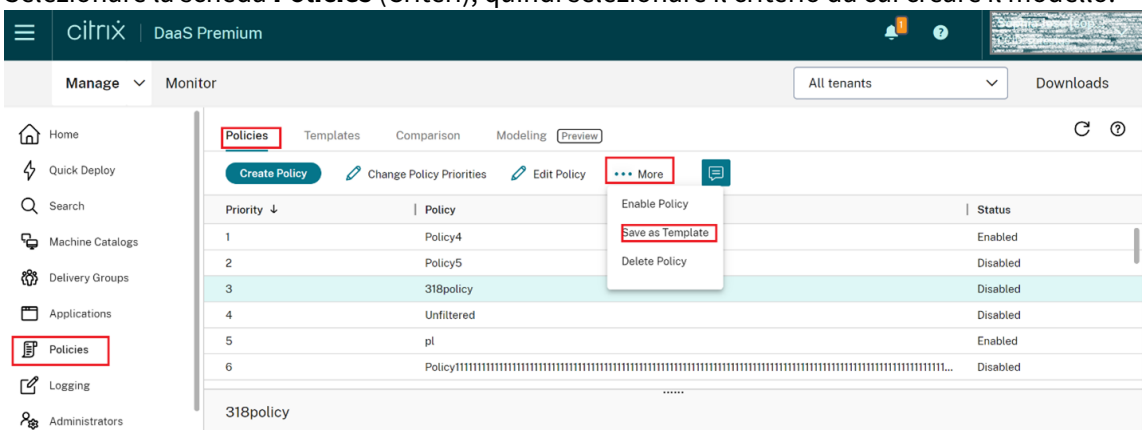

4. Selezionare e configurare le impostazioni dei criteri da includere nel modello.
5. Fare clic su **Next** (Avanti). Viene visualizzata la schermata **Summary** (Riepilogo).
6. Immettere un nome per il modello.
7. Fare clic su **Finish**. Il nuovo modello viene visualizzato nella scheda Templates (Modelli)

**Per creare un modello basato su un criterio**:

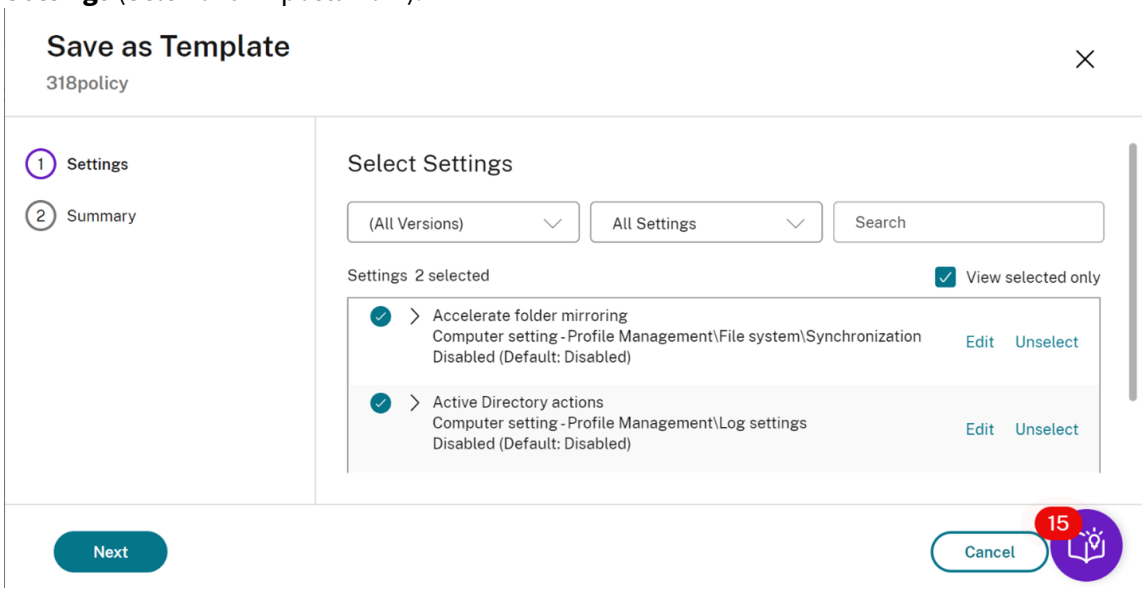
1. Selezionare **Policies** (Criteri) nel riquadro di navigazione di Web Studio.

2. Selezionare la scheda **Policies** (Criteri), quindi selezionare il criterio da cui creare il modello.

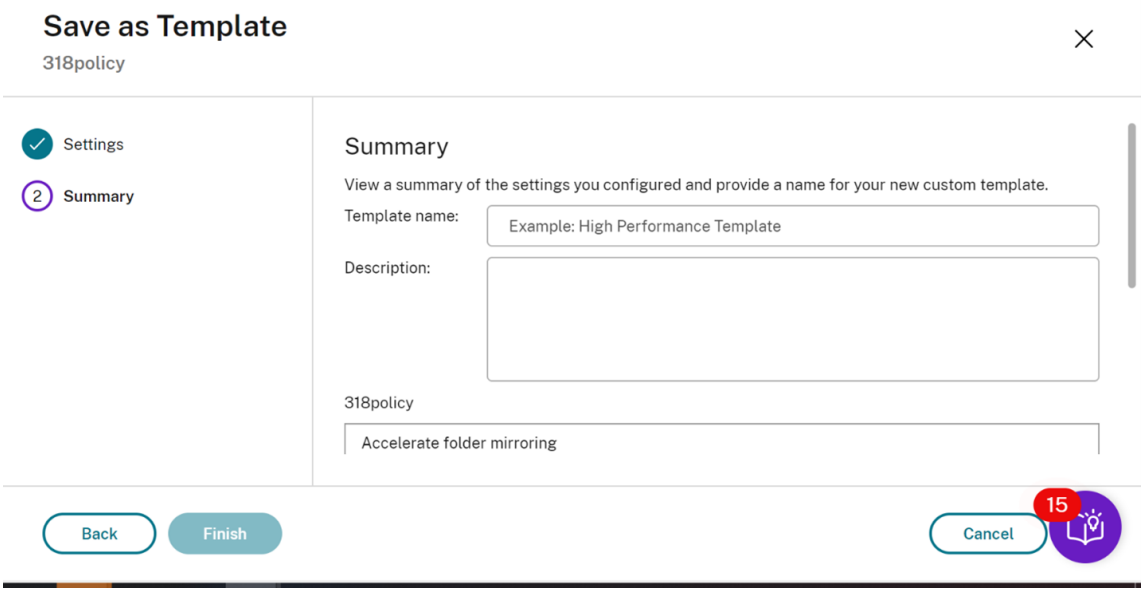



3. Fare clic sulla scheda **More** (Altro).
4. Selezionare **Save as Template** (Salva come modello). Viene visualizzata la schermata **Select Settings** (Seleziona impostazioni).




5. Selezionare e configurare le nuove impostazioni dei criteri da includere nel modello.
6. Fare clic su **Next** (Avanti). Viene visualizzata la schermata **Summary** (Riepilogo).




7. Immettere un nome e una descrizione per il modello, quindi fare clic su **Finish** (Fine).

## Creare criteri

October 30, 2023

Prima di creare un criterio, decidere su quale gruppo di utenti o dispositivi può influire. Potrebbe essere utile creare un criterio basato sulla funzione del processo utente, sul tipo di connessione, sul dispositivo utente o sulla posizione geografica.

Se è già stato creato un criterio applicabile a un gruppo, è consigliabile modificarlo anziché creare un altro criterio. Dopo aver modificato il criterio, configurare le impostazioni appropriate. Evitare di creare un criterio esclusivamente per abilitare un'impostazione specifica o per impedire che il criterio venga applicato a determinati utenti.

Quando si crea un criterio, è possibile basarlo sulle impostazioni di un modello di criterio e personalizzare le impostazioni in base alle esigenze. È anche possibile crearlo senza utilizzare un modello e aggiungere tutte le impostazioni necessarie.

In Citrix Studio, i nuovi criteri creati vengono impostati su Disabled (Disabilitato), a meno che la casella di controllo **Enable policy** (Abilita criterio) non sia esplicitamente selezionata.

Durante la creazione dei criteri e durante la configurazione delle impostazioni, il sistema offre un'opzione per visualizzare il tipo di impostazioni. È possibile visualizzare il seguente tipo di impostazioni:

- All settings: visualizza tutte le impostazioni per tutte le versioni di VDA

- Current settings only: visualizza le impostazioni solo per le versioni VDA correnti
- Legacy settings only: visualizza le impostazioni solo per le versioni VDA deprecate

Per visualizzare le impostazioni mentre le si configura:

1. Accedere a DaaS Premium.
2. Nella barra di navigazione a sinistra, fare clic su **Policies** (Criteri).
3. Nella scheda **Politicies**, fare clic su **Create Policy** (Crea criterio).
4. Nella tabella **Select Settings** (Seleziona impostazioni) fare clic sul menu a discesa accanto a **Settings**.
5. Selezionare una delle seguenti opzioni dal menu a discesa:
    - All settings: visualizza tutte le impostazioni per tutte le versioni di VDA
    - Current settings only: visualizza le impostazioni solo per le versioni VDA correnti
    - Legacy settings only: visualizza le impostazioni solo per le versioni VDA deprecate
6. Nella tabella Settings sono elencate le impostazioni disponibili in base al passaggio precedente.

### Impostazioni dei criteri

Le impostazioni dei criteri possono essere abilitate, disabilitate o non configurate. Per impostazione predefinita, le impostazioni dei criteri non sono configurate, il che significa che non vengono aggiunte a un criterio. Le impostazioni vengono applicate solo quando vengono aggiunte a un criterio.

Quando si configurano le impostazioni per la creazione o la modifica di un criterio, se tutti i gruppi di consegna sono disabilitati, il sistema visualizza il segnale di avviso **None of the elements in this filter is enabled** (Nessuno degli elementi di questo filtro è abilitato). Se è abilitato almeno un gruppo di consegna, il sistema non visualizza il segnale di avviso.

Per visualizzare l'avviso durante la creazione di un criterio:

1. Accedere a DaaS Premium.
2. Nella barra di navigazione a sinistra, fare clic su **Policies** (Criteri).
3. Nella scheda **Politicies**, fare clic su **Create Policy** (Crea criterio).
4. Nella tabella **Select Settings**, selezionare un'impostazione e fare clic su **Next**.
5. Nella tabella **Assign Policy To** (Assegna criterio a), selezionare un filtro dal menu a discesa.
6. Deselezionare la casella di controllo **Enable** e fare clic su **Save**.

> **Nota:**
>
> Non tutti i filtri supportano la deselezione della casella di controllo **Enable**.
> Nella tabella **Filters**, il filtro visualizza l'avviso.

Per visualizzare l'avviso durante la modifica di un criterio:

1. Accedere a DaaS Premium.
2. Nella barra di navigazione a sinistra, fare clic su **Policies** (Criteri).
3. Nella scheda **Policies** (Criteri), selezionare uno dei criteri elencati e fare clic su **Edit Policy** (Modifica criterio).
4. Nella pagina **Edit Policy**, fare clic su **Assign Policy To** (Assegna criterio a) nella barra di navigazione di sinistra.
5. Nella tabella **Filter**, selezionare o fare clic su **Edit** per il filtro richiesto:
   - Se un filtro non dispone del pulsante **Edit**, selezionare il filtro.
   - Se un filtro dispone del pulsante **Edit**, fare clic su di esso.
6. Deselezionare l'opzione **Enable** e fare clic su **Save**.

> **Nota:**
>
> Non tutti i filtri supportano la deselezione della casella di controllo **Enable**.
> Nella tabella **Filters**, il filtro visualizza l'avviso.

Alcune impostazioni dei criteri possono essere in uno dei seguenti stati:

```
1 - Allowed or Prohibited allows or prevents the action controlled by
    the setting. Sometimes users are allowed or prevented from managing
    the setting's action in a session. For example, if the menu
    animation setting is set to Allowed, users can control menu
    animations in their client environment
2 - Enabled or Disabled turns the setting on or off. If you disable a
    setting, it is not enabled in lower-ranked policies.
```

Inoltre, alcune impostazioni controllano l'efficacia delle impostazioni dipendenti. Ad esempio, il reindirizzamento delle unità client controlla se gli utenti possono accedere alle unità sui propri dispositivi. Sia questa impostazione che l'impostazione **Client network drives** (Unità di rete client) devono essere aggiunte al criterio per consentire agli utenti di accedere alle unità di rete. Se l'impostazione **Client drive redirection** (Reindirizzamento unità client) è disabilitata, gli utenti non possono accedere alle unità di rete, anche se l'impostazione **Client network drives** (Unità di rete client) è abilitata.

In generale, le modifiche delle impostazioni dei criteri che influiscono sulle macchine entrano in vigore al riavvio del desktop virtuale o all'accesso di un utente. Le modifiche delle impostazioni dei criteri che influiscono sugli utenti entrano in vigore al successivo accesso degli utenti.

Per alcune impostazioni dei criteri, è possibile immettere o selezionare un valore quando si aggiunge l'impostazione a un criterio. È possibile limitare la configurazione dell'impostazione selezionando Use default value (Usa valore predefinito). Questa selezione disabilita la configurazione dell'impostazione

e consente di utilizzare solo il valore predefinito dell'impostazione quando viene applicato il criterio. Questa selezione è a prescindere dal valore immesso prima di selezionare Use default value (Usa valore predefinito).

Come best practice:

- Assegnare criteri ai gruppi anziché ai singoli utenti. Se si assegnano criteri ai gruppi, le assegnazioni vengono aggiornate automaticamente quando si aggiungono o rimuovono utenti dal gruppo.
- Disabilitare i criteri inutilizzati. I criteri senza impostazioni aggiunte generano un'elaborazione non necessaria.

### Assegnazioni dei criteri

Quando si crea un criterio, viene assegnato a determinati utenti e oggetti macchina. Tale criterio viene applicato alle connessioni in base a criteri o regole specifici. In generale, è possibile aggiungere tutte le assegnazioni desiderate a un criterio, in base a una combinazione di criteri. Se non si specifica alcuna assegnazione, il criterio viene applicato a tutte le connessioni.

Se non si specifica alcuna assegnazione o si specificano assegnazioni ma le si disattiva, il criterio viene applicato a **tutte** le connessioni.

> **Nota:**
>
> Le assegnazioni dei criteri sono note anche come filtri dei criteri. Per ulteriori informazioni, vedere i seguenti argomenti:
>
> - Creare, modificare o eliminare un filtro per un criterio
> - Come vengono applicati i filtri?

Nella tabella seguente sono elencate le assegnazioni disponibili:

| Nome assegnazione | Applica un criterio basato su |
| --- | --- |
| Controllo degli accessi | Condizioni di controllo degli accessi attraverso le quali un client si connette. *Connection type* (Tipo di connessione): indica se applicare il criterio alle connessioni effettuate con o senza NetScaler Gateway. *NetScaler Gateway farm name* (Nome farm NetScaler Gateway): nome del server virtuale NetScaler Gateway. *Access condition* (Condizione di accesso): nome del criterio di analisi degli endpoint o del criterio di sessione da utilizzare. |
| Citrix SD-WAN | Se una sessione utente viene avviata tramite Citrix SD-WAN. **Nota:** è possibile aggiungere una sola assegnazione Citrix SD-WAN a un criterio. |
| Indirizzo IP client | Indirizzo IP del dispositivo utente utilizzato per connettersi alla sessione: esempi IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; esempi IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |
| Nome client | Nome del dispositivo utente. Corrispondenza esatta: NomeABCClient. Utilizzo del carattere jolly: Nome*Client. |
| Gruppo di consegna | Appartenenza al gruppo di consegna. |
| Tipo di gruppo di consegna | Tipo di desktop o applicazione: desktop privato, desktop condiviso, applicazione privata o applicazione condivisa. |
| Unità organizzativa (OU) | Unità organizzativa. |
| Tag | Tag. **Nota:** applicare questo criterio a tutte le macchine con tag. I tag delle applicazioni non sono inclusi. |
| Utente o gruppo | Nome utente o gruppo. |

Quando un utente accede, vengono identificati tutti i criteri corrispondenti alle assegnazioni per la connessione. Tali criteri vengono ordinati in ordine di priorità e vengono confrontate più istanze di tutte le impostazioni. Ogni impostazione viene applicata in base alla classificazione di priorità del criterio. Qualsiasi impostazione dei criteri disabilitata ha la precedenza su un'impostazione di livello inferiore abilitata. Le impostazioni dei criteri non configurate vengono ignorate.

> **Importante:**
>
> Quando si configurano i criteri Active Directory e Citrix utilizzando la Console Gestione Criteri di gruppo, le assegnazioni e le impostazioni potrebbero non essere applicate come previsto. Per ulteriori informazioni, vedere CTX127461.

Per impostazione predefinita viene fornito un criterio denominato "Unfiltered"(Non filtrato).

- Se si utilizza Web Studio per gestire i criteri Citrix, le impostazioni aggiunte al criterio Unfiltered (Non filtrato) vengono applicate a tutti i server, i desktop e le connessioni di un sito.
- I siti e le connessioni devono rientrare nell'ambito degli oggetti Criteri di gruppo (GPO) che includono il criterio. Ad esempio, l'unità organizzativa Vendite include un oggetto Criteri di gruppo denominato Vendite-Stati Uniti che include tutti i membri del team di vendita degli Stati Uniti. L'oggetto Criteri di gruppo Vendite-Stati Uniti è configurato con un criterio Unfiltered (Non filtrato) che include diverse impostazioni dei criteri utente. Quando il responsabile delle vendite degli Stati Uniti accede al sito, le impostazioni del criterio Unfiltered (Non filtrato) vengono applicate automaticamente alla sessione. Questa configurazione è dovuta al fatto che l'utente è un membro dell'oggetto Criteri di gruppo Vendite USA.

La modalità di assegnazione determina se il criterio viene applicato solo alle connessioni che corrispondono a tutti i criteri di assegnazione. Se la modalità è impostata su Allowed (Consenti, impostazione predefinita), il criterio viene applicato solo alle connessioni che corrispondono ai criteri di assegnazione. Se la modalità è impostata su Deny (Nega), il criterio viene applicato se la connessione non corrisponde ai criteri di assegnazione. Gli esempi seguenti illustrano come le modalità di assegnazione influiscono sui criteri Citrix quando sono presenti più assegnazioni.

- **Esempio: assegnazioni di tipo simile con modalità diverse** - Nei criteri con due assegnazioni dello stesso tipo, una impostata su Allow (Consenti) e una impostata su Deny (Nega), l'assegnazione impostata su Deny (Nega) ha la precedenza, a condizione che la connessione soddisfi entrambe le assegnazioni. Ad esempio:

  Il criterio 1 include le seguenti assegnazioni:

  - L'Assegnazione A specifica il gruppo Vendite. La modalità è impostata su Allow (Consenti).
  - L'Assegnazione B specifica l'account del responsabile delle vendite. La modalità è impostata su Deny (Nega).

  Poiché la modalità per l'Assegnazione B è impostata su Deny (Nega), il criterio non viene applicato quando il responsabile delle vendite accede al sito, anche se l'utente è membro del gruppo Vendite.

- **Esempio: assegnazioni di tipo diverso con modalità simili** - Nei criteri con due o più assegnazioni di tipi diversi, impostate su Allow (Consenti), la connessione deve soddisfare almeno un'assegnazione di ogni tipo per applicare il criterio. Ad esempio:

Il criterio 2 include le seguenti assegnazioni:

- L'Assegnazione C è un'assegnazione utente che specifica il gruppo Vendite. La modalità è impostata su Allow (Consenti).
- L'Assegnazione D è un'assegnazione relatiiva all'indirizzo IP client che specifica 10.8.169.* (la rete aziendale). La modalità è impostata su Allow (Consenti).

Quando il responsabile delle vendite accede al sito dall'ufficio, il criterio viene applicato perché la connessione soddisfa entrambe le assegnazioni.

Il criterio 3 include le seguenti assegnazioni:

- L'Assegnazione E è un'assegnazione utente che specifica il gruppo Vendite. La modalità è impostata su Allow (Consenti).
- L'Assegnazione F è un'assegnazione di controllo degli accessi che specifica le condizioni di connessione di NetScaler Gateway. La modalità è impostata su Allow (Consenti).

Quando il responsabile delle vendite accede al sito dall'ufficio, il criterio non viene applicato perché la connessione non soddisfa i requisiti dell'Assegnazione F.

## Set di criteri (anteprima)

November 21, 2023

I set di criteri sono oggetti di Citrix DaaS che aggregano i criteri per consentire un accesso semplificato e basato sui ruoli e una facile gestione. È possibile creare set di criteri per rispecchiare le divisioni logiche del team di amministratori e dell'azienda. Ad esempio, è possibile creare un set di criteri per ogni area geografica, per ogni unità aziendale o per un caso d'uso specifico. Una volta creati, gli ambiti e i gruppi di consegna vengono assegnati ai set di criteri in modo che solo gli amministratori autorizzati possano gestire i criteri che si applicano agli utenti e alle macchine pertinenti.

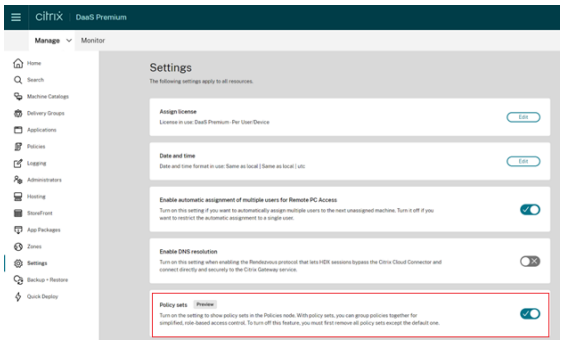
### Vantaggi

- Controllo degli accessi basato sui ruoli per team di amministratori distribuiti
- Fusioni, acquisizioni e consolidamenti semplificati
- Dominio di errore limitato
- Supporto multitenant per i criteri

## Abilitare i set di criteri

Dalla scheda **Manage** di Citrix DaaS, accedere a **Settings** e attivare l'impostazione **Policy sets** (Set di criteri).




> **Nota:**
>
> è necessario abilitare i set di criteri prima di creare un set di criteri.

## Confronto delle funzionalità

| Prima di applicare i set di criteri | Dopo aver applicato i set di criteri |
|---|---|
| I criteri, le impostazioni, i filtri e le priorità dei criteri per l'intero sito sono configurati in un' unica posizione all'interno di Citrix Studio. | I criteri, le impostazioni, i filtri e le priorità dei criteri sono configurati separatamente per ciascun set di criteri. |
| Se si gestisce un criterio, è necessario gestirli tutti. | Gli amministratori completi possono delegare agli amministratori di livello inferiore la capacità di gestire individualmente un determinato set di criteri. |
| In ambienti grandi e distribuiti i criteri diventano complessi e difficili da gestire. | I criteri in ambienti grandi e distribuiti possono essere suddivisi per semplificarne la gestione. |

## Come funzionano i set di criteri?

### Panoramica generale

- I set di criteri vengono assegnati ai gruppi di consegna
- I set di criteri hanno uno o più ambiti
- I gruppi di consegna a cui non è stato assegnato alcun set di criteri ricevono il set di criteri predefinito
- A un gruppo di consegna può essere assegnato un solo set di criteri

- Più gruppi di consegna possono utilizzare lo stesso set di criteri
- Anche se i set di criteri sono assegnati ai gruppi di consegna, i singoli criteri mantengono i propri filtri

### Set di criteri predefinito

- Quando l'impostazione del set di criteri è attivata, tutti i criteri esistenti vengono raggruppati all'interno del set di criteri predefinito
- Ogni gruppo di consegna riceve il set di criteri predefinito a meno che il team di amministrazione non crei un set di criteri e lo assegni a un gruppo di consegna.
- Una volta che a un gruppo di consegna è stato assegnato un set di criteri diverso, non riceverà più i criteri dal set di criteri predefinito

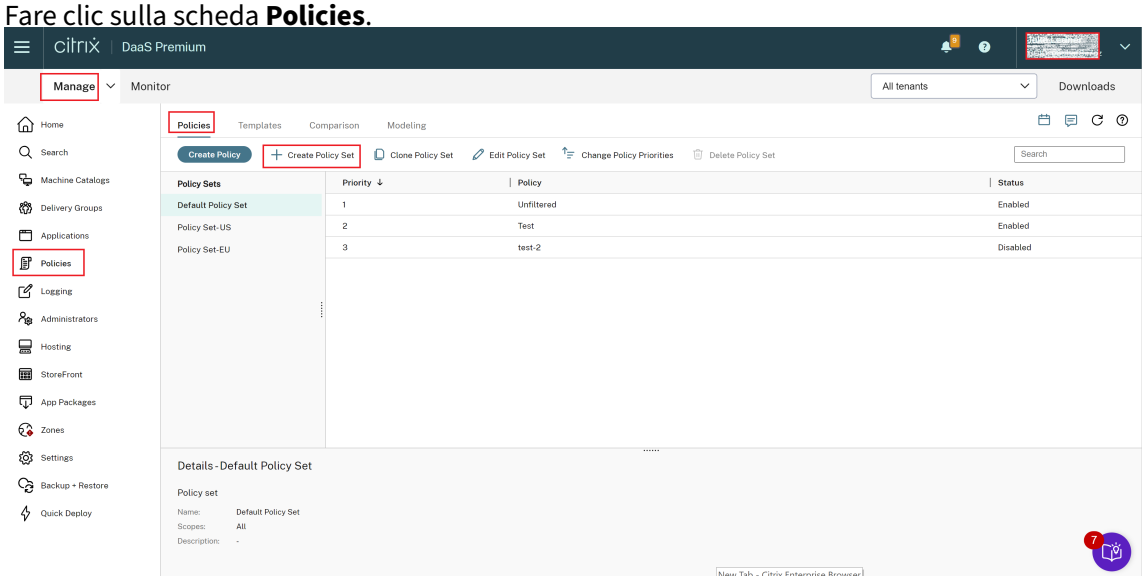
### Creazione di set di criteri

I set di criteri possono essere creati nei due modi seguenti:

- Create policy set: questa azione crea un set di criteri vuoto
- Clone policy set: questa azione crea un set di criteri clonando un set di criteri esistente

### Creare set di criteri

1. Nella pagina di configurazione di Citrix DaaS, fare clic sulla scheda **Manage** (Gestisci).
2. Fare clic sulla scheda **Policies**.




3. Selezionare **Create Policy Set** (Crea set di criteri). Viene visualizzata la scheda **Introduction**.
4. Fare clic su **Next** (Avanti) o sulla scheda **Name and Description** (Nome e descrizione).
5. Immettere il nome e la descrizione del set di criteri.

6. Fare clic su **Next** o sulla scheda **Assignments** (Assegnazioni).
7. Selezionare uno o più gruppi di consegna a cui assegnare il set di criteri.
8. Fare clic su **Next** o sulla scheda **Scopes** (Ambiti).
9. Selezionare gli ambiti del set di criteri.
10. Fare clic su **Create**. Il set di criteri viene creato con l'assegnazione e l'ambito definiti.

#### Clonare set di criteri

1. Nella pagina di configurazione di Citrix DaaS, fare clic sulla scheda **Manage** (Gestisci).
2. Fare clic sulla scheda **Policies**.
3. Selezionare **Clone Policy Set** (Clona set di criteri).
4. Modificare il nome del set di criteri.
5. Modificare o creare le assegnazioni del set di criteri e fare clic su **Next**.
6. Selezionare o deselezionare i criteri da includere nel set di criteri clonato.
7. Modificare l'ambito del criterio.
8. Fare clic su **Create**. Viene creato il set di criteri.

#### Modificare i set di criteri

1. Nella pagina di configurazione di Citrix DaaS, fare clic sulla scheda **Manage** (Gestisci).
2. Fare clic sulla scheda **Policies**.
3. Selezionare **Edit Policy Set** (Modifica set di criteri).
4. Modificare il nome del set di criteri e fare clic su **Next**.
5. Modificare o creare le assegnazioni del set di criteri e fare clic su **Next**.
6. Modificare l'ambito del criterio.
7. Fare clic su **Create**.

#### Assegnazione del set di criteri

I set di criteri vengono assegnati a dei gruppi di consegna. È possibile configurare le assegnazioni quando il set di criteri viene creato o modificato. È possibile anche configurare le assegnazioni quando vengono creati o modificati i gruppi di consegna.

#### Ambiti dei set di criteri

Gli amministratori possono definire l'ambito di un set di criteri in modo che solo gli amministratori autorizzati possano visualizzarlo o modificarlo. È possibile configurare gli ambiti quando il set di criteri viene creato o modificato.

# Assegnare priorità ai criteri, modellarli, confrontarli e risolverne i problemi

June 8, 2023

È possibile utilizzare i criteri per personalizzare l'ambiente in modo da soddisfare le esigenze degli utenti in base a quanto segue:

- Funzioni lavorative
- Posizioni geografiche
- Tipi di connessione

Ad esempio, per migliorare la sicurezza, applicare restrizioni ai gruppi di utenti che interagiscono regolarmente con dati sensibili.

È inoltre possibile creare un criterio che impedisca agli utenti di salvare file sensibili sulle unità client locali. È possibile creare un altro criterio per gli utenti del gruppo di utenti che devono accedere alle proprie unità locali. È quindi possibile classificare i due criteri per controllare quale ha la precedenza. Quando si utilizzano molti criteri, è necessario determinare:

- Come stabilire le priorità dei criteri
- Come creare eccezioni
- Come visualizzare il criterio efficace quando i criteri sono in conflitto

## Assegnare priorità ai criteri

L'assegnazione di priorità ai criteri consente di definire la priorità dei criteri quando contengono impostazioni in conflitto. L'identificazione di tutti i criteri che corrispondono alle assegnazioni per la connessione avviene quando un utente accede al sistema. I criteri identificati e le relative impostazioni associate sono in ordine di priorità. Ogni impostazione viene applicata in base alla classificazione di priorità del criterio.

È possibile assegnare priorità ai criteri dando loro numeri di priorità diversi in **Web Studio**. Per impostazione predefinita, un nuovo criterio ha la priorità più bassa. In caso di conflitti tra le impostazioni dei criteri, un criterio con priorità più alta prevale su un criterio con priorità inferiore. Un criterio con numero di priorità 1 è il criterio con la priorità più alta. Le impostazioni dei criteri vengono unite in base a quanto segue:

- Priorità dei criteri
- Condizioni specificate nei filtri dei criteri

Per assegnare priorità ai criteri, seguire questi passaggi:

1. Selezionare **Policies** (Criteri) nel riquadro a sinistra.
2. Nella scheda **Policies**, selezionare **Change Policy Priorities** (Modifica le priorità dei criteri) nella barra delle azioni. Viene visualizzata la pagina **Change Policy Priorities** (Cambia le priorità dei criteri).
3. Nell'elenco delle priorità, utilizzare i metodi seguenti per modificare la priorità di un criterio:
   - Trascinare il criterio nella posizione desiderata.
   - Per spostarlo verso l'alto o verso il basso di una posizione, fate clic rispettivamente sull'icona freccia su o giù.
   - Per spostarlo nella parte superiore o inferiore dell'elenco, fate clic sull'icona della freccia rispettivamente superiore o inferiore.
   - Per modificare il numero di priorità, fare clic sull'icona **Edit** (Modifica), inserire il numero necessario, quindi fare clic su **Save**.
4. Fare clic su **Salva**.

### Eccezioni

Quando si creano dei criteri e si usano i filtri per assegnarli a gruppi di utenti, dispositivi utente o macchine, alcuni membri del gruppo potrebbero necessitare di eccezioni ad alcune impostazioni dei criteri. È possibile creare eccezioni nei modi seguenti:

- Creare un criterio solo per gli specifici membri del gruppo che necessitano delle eccezioni e quindi assegnando al criterio una classificazione più elevata rispetto al criterio per l'intero gruppo
- Utilizzare la modalità *Deny* (Nega) per un'assegnazione aggiunta al criterio

Un'assegnazione con la modalità impostata su *Deny* (Nega) applica un criterio solo alle connessioni che non corrispondono ai criteri di assegnazione. Ad esempio, un criterio include le seguenti assegnazioni:

- *Assignment A* è l'assegnazione di un indirizzo IP client che specifica l'intervallo `208.77.88.*`. La modalità è impostata su *Allow* (Consenti).
- *Assignment B* è un'assegnazione utente che specifica un determinato account utente. La modalità è impostata su *Deny* (Nega).

Il criterio si applica a tutti gli utenti che accedono al sito con indirizzi IP compresi nell'intervallo specificato in *Assignment A.* Tuttavia, il criterio non si applica all'utente che accede al sito con l'account utente specificato in *Assignment B*.

> **Nota:**
>
> Durante il passaggio **Assign Policy** (Assegna criterio), se si deseleziona la casella di controllo di abilitazione, l'assegnazione viene disattivata per il criterio. Se l'unica assegnazione per il criterio è disabilitata, ciò equivale a non avere alcuna assegnazione e, pertanto, il criterio si applica a tutti gli oggetti del sito.

### Determinare quali criteri si applicano a una connessione

A volte una connessione non risponde come previsto perché si applicano più criteri. Se a una connessione viene applicato un criterio di priorità più alto, è possibile ignorare le impostazioni configurate nel criterio originale. È possibile calcolare il **gruppo di criteri risultante** e determinare la modalità di unione delle impostazioni dei criteri finali per una connessione.

È possibile calcolare il valore di **Resultant Set of Policy** (Gruppo di criteri risultante) nei modi seguenti:

- Utilizzare la **procedura guidata Citrix Group Policy Modeling** (Modellazione Criteri di gruppo Citrix) per simulare uno scenario di connessione e individuare come potrebbero essere applicati i criteri Citrix. È possibile specificare le condizioni per uno scenario di connessione, ad esempio:
  - Utenti
  - Valori delle prove di assegnazione dei criteri Citrix
- Utilizzare **Group Policy Results** (Risultati dei criteri di gruppo) per creare un rapporto che descriva i criteri Citrix in vigore per un determinato utente e Virtual Delivery Agent (VDA).

Le impostazioni dei criteri del sito creati utilizzando **Web Studio** non sono incluse nel **gruppo di criteri risultante** quando si esegue la procedura guidata **Citrix Group Policy Modeling** dalla console di **Group Policy Management**. Per verificare di aver ottenuto il **gruppo di criteri risultanti più completo**, Citrix consiglia di avviare la procedura guidata **Citrix Group Policy Modeling** da **Web Studio**, a meno che non si creino criteri utilizzando solo la console **Group Policy Management**.

### Utilizzare la procedura guidata per la modellazione dei criteri

La modellazione dei criteri consente di simulare i criteri abilitati con filtri per scopi di pianificazione e test. Vengono modellati solo i criteri abilitati con filtri. I criteri disabilitati non vengono mai applicati e i criteri abilitati senza filtri vengono sempre applicati.

Eseguire i seguenti passaggi per aprire la procedura guidata **Policy Modeling**:

1. In Full Configuration, selezionare **Policies** (Criteri).
2. Selezionare la scheda **Modeling** (Modellazione).

3. Selezionare **Policy Modeling** nella barra delle azioni.
4. Leggere la pagina **Introduction** e fare clic su **Next**.
5. Selezionare utenti o computer. È possibile sfogliare per trovare contenitori oppure utenti o computer specifici. Fare clic su **Next** (Avanti).
6. Scegliere le prove da filtrare. Facoltativamente, è possibile ottenere una simulazione più dettagliata inserendo dettagli aggiuntivi, quali **gruppo di consegna**, **tag**, **indirizzo IP del client**e così via. Fare clic su **Next** (Avanti).
7. Rivedere il riepilogo delle selezioni e fai clic su **Run** (Esegui).

Dopo aver fatto clic su **Run**, la procedura guidata genera un report dei risultati della modellazione. Durante la visualizzazione di questo report, è possibile:

- Selezionare se visualizzare **All settings** (Tutte le impostazioni), **Computer settings**(Impostazioni del computer) o **User settings** (Impostazioni utente) nel menu a discesa.
- Utilizzare la barra di ricerca per cercare impostazioni specifiche.
- Fare clic su un'impostazione specifica per visualizzarne i dettagli. Ad esempio, se a un criterio specifico non sono state applicate tutte le impostazioni utente, il riquadro **Dettagli** mostra il motivo per cui le impostazioni non sono state applicate.
- Fare clic su **Export** (Esporta) per esportare i risultati della modellazione in formato JSON, in formato HTML o in entrambi.

Dopo che è stata eseguita la modellazione dei criteri, saranno disponibili più opzioni. È possibile effettuare le seguenti operazioni:

- **View Modeling Report** (Visualizza report di modellazione): questo apre lo stesso report di modellazione di cui sopra in modo da poterlo visualizzare nuovamente o esportarlo.
- **Rerun Policy Modeling** (Rieseguire la modellazione dei criteri): consente di rieseguire la modellazione dei criteri con lo stesso insieme di criteri selezionati in precedenza e generare nuovi risultati di modellazione. Questo è utile se alcuni criteri sono stati modificati e si desidera vedere come le modifiche influiscono sul modello attuale.
- **Delete Modeling Report** (Elimina report di modellazione): questo elimina il report di modellazione corrente.

### Confrontare criteri e modelli

È possibile confrontare le impostazioni di un criterio o di un modello con le impostazioni degli altri criteri o modelli. Ad esempio, potrebbe essere bene verificare i valori delle impostazioni per mantenere la conformità alle procedure consigliate. Oppure potrebbe essere necessario confrontare le impostazioni in un criterio o un modello con le impostazioni predefinite.

1. Selezionare **Policies** (Criteri) nel riquadro di navigazione di **Web Studio**.
2. Fare clic sulla scheda **Comparison** (Confronto) e quindi su **Select** (Seleziona).

3. Scegliere i criteri o i modelli da confrontare. Per includere i valori predefiniti nel confronto, selezionare la casella di controllo **Compare to default settings** (Confronta con le impostazioni predefinite).
4. Dopo che si è fatto clic su **Compare** (Confronta), le impostazioni configurate vengono visualizzate in colonne.
5. Per visualizzare tutte le impostazioni, selezionare **Show All Settings** (Mostra tutte le impostazioni). Per tornare alla visualizzazione predefinita, selezionare **Show Common Settings** (Mostra impostazioni comuni).

### Risolvere i problemi relativi ai criteri

Gli utenti, gli indirizzi IP e altri oggetti assegnati possono avere più criteri che si applicano contemporaneamente. Questo scenario può causare conflitti e un criterio potrebbe non comportarsi come previsto. Quando si esegue la procedura guidata **Citrix Group Policy Modeling**, si potrebbe scoprire che nessun criterio si applica alle connessioni degli utenti. In uno scenario di questo tipo, le impostazioni dei criteri non si applicano agli utenti che si connettono alle loro applicazioni e ai loro desktop in condizioni che corrispondono ai criteri di valutazione dei criteri. Questa situazione si verifica quando:

- Nessun criterio dispone di assegnazioni che corrispondono ai criteri di valutazione dei criteri.
- I criteri che corrispondono all'assegnazione non hanno impostazioni configurate.
- I criteri che corrispondono all'assegnazione sono disabilitati.

Se si desidera applicare le impostazioni dei criteri alle connessioni che soddisfano i criteri specificati, assicurarsi che:

- I criteri che si desidera applicare a tali connessioni siano abilitati.
- I criteri che si desidera applicare dispongano delle impostazioni appropriate configurate.

> **Nota:**
>
> Nel secondo hop di scenari a doppio hop, tenere presente che un VDA con sistema operativo a sessione singola si connette a un VDA con sistema operativo multisessione. In questo caso, i criteri Citrix agiscono sul VDA del sistema operativo a sessione singola come se fosse il dispositivo dell'utente. Ad esempio, considerare che sono impostati criteri per memorizzare nella cache le immagini sul dispositivo utente. In questo esempio le immagini memorizzate nella cache per il secondo hop in uno scenario a doppio hop vengono memorizzate nella cache sulla macchina VDA con sistema operativo a sessione singola.

### Director

I non amministratori possono utilizzare Director per visualizzare i criteri che si applicano a una sessione utente.

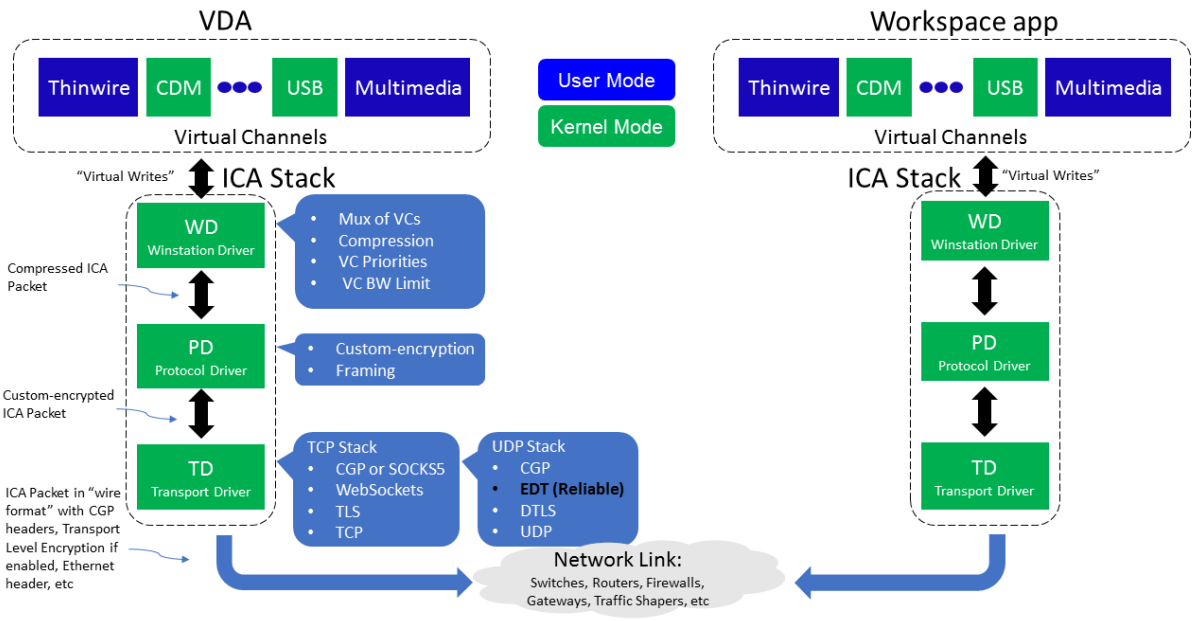
 

# Panoramica di HDX

May 23, 2023

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Citrix HDX rappresenta un ampio set di tecnologie che offrono un'esperienza ad alta definizione agli utenti di applicazioni e desktop centralizzati, su qualsiasi dispositivo e su qualsiasi rete.




HDX è progettato in base a tre principi tecnici:

- Reindirizzamento intelligente
- Compressione adattiva
- Deduplicazione dei dati

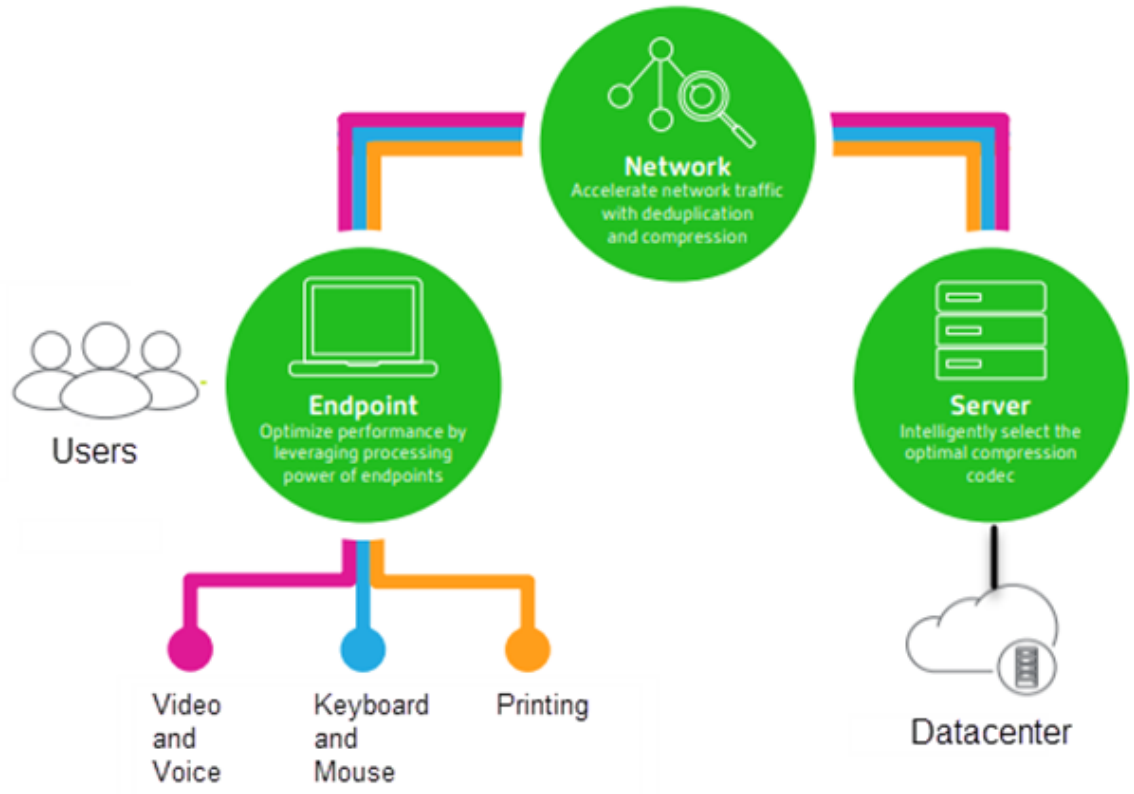
Applicati in diverse combinazioni, questi ottimizzano l'IT e l'esperienza utente, riducono il consumo di larghezza di banda e aumentano la densità degli utenti per server di hosting.

- **Reindirizzamento intelligente**: il reindirizzamento intelligente esamina l'attività sullo schermo, i comandi delle applicazioni, il dispositivo endpoint e le funzionalità di rete e del

server per determinare immediatamente come e dove eseguire il rendering di un'applicazione o un'attività desktop. Il rendering può avvenire sul dispositivo endpoint o sul server di hosting.

- **Compressione adattiva**: la compressione adattiva consente di fornire display multimediali avanzati su connessioni di rete thin. HDX valuta innanzitutto diverse variabili, ad esempio il tipo di input, dispositivo e visualizzazione (testo, video, voce e multimediale). Sceglie il codec di compressione ottimale e la migliore percentuale di utilizzo della CPU e della GPU. Si adatta quindi in modo intelligente in base a ogni singolo utente e base. Questo adattamento intelligente è utente per utente o anche sessione per sessione.




- **Deduplicazione dei dati**: la deduplicazione del traffico di rete riduce i dati aggregati inviati tra client e server. Lo fa sfruttando i modelli ripetuti in dati comunemente accessibili come immagini bitmap, documenti, processi di stampa e dati multimediali in streaming. La memorizzazione nella cache di questi modelli consente di trasmettere solo le modifiche attraverso la rete, eliminando il traffico duplicato. HDX supporta anche il multicasting di flussi multimediali, in cui una singola trasmissione dalla sorgente viene visualizzata da più abbonati in un'unica posizione, piuttosto che utilizzare una connessione individuale per ogni utente.

Per ulteriori informazioni, vedere Aumentare la produttività con un'area di lavoro utente ad alta definizione.

### Nel dispositivo

HDX utilizza la capacità di elaborazione dei dispositivi utente per migliorare e ottimizzare l'esperienza utente. La tecnologia HDX garantisce agli utenti un'esperienza fluida e senza interruzioni con contenuti multimediali nei loro desktop o applicazioni virtuali. Il controllo dell'area di lavoro consente agli utenti di mettere in pausa i desktop e le applicazioni virtuali e di riprendere a lavorare da un dispositivo diverso nel punto in cui si erano interrotti.

### Sulla rete

HDX incorpora funzionalità avanzate di ottimizzazione e accelerazione per offrire le migliori prestazioni su qualsiasi rete, incluse le connessioni WAN a bassa larghezza di banda e ad alta latenza.

Le funzioni HDX si adattano ai cambiamenti dell'ambiente. Le caratteristiche mantengono un equilibrio fra prestazioni e larghezza di banda. Applicano le migliori tecnologie per ogni scenario utente, indipendentemente dal fatto che l'accesso al desktop o l'applicazione venga effettuato localmente sulla rete aziendale o in remoto dall'esterno del firewall aziendale.

### Nel centro dati

HDX utilizza la potenza di elaborazione e la scalabilità dei server per offrire prestazioni grafiche avanzate, indipendentemente dalle funzionalità dei dispositivi client.

Il monitoraggio dei canali HDX fornito da Citrix Director visualizza lo stato dei canali HDX collegati sui dispositivi utente.

### HDX Insight

HDX Insight è l'integrazione di NetScaler Network Inspector e Performance Manager con Director. Acquisisce i dati sul traffico ICA e fornisce una panoramica dei dettagli storici e in tempo reale. Questi dati includono la latenza della sessione ICA lato client e lato server, l'uso della larghezza di banda dei canali ICA e il valore temporale di andata e ritorno ICA di ogni sessione.

È possibile consentire a NetScaler di utilizzare il canale virtuale HDX Insight per spostare tutti i punti dati richiesti in un formato non compresso. Se si disattiva questa funzione, il dispositivo NetScaler decrittografa e decomprime il traffico ICA diffuso su vari canali virtuali. L'utilizzo del singolo canale virtuale riduce la complessità, migliora la scalabilità ed è più conveniente.

**Requisiti minimi:**

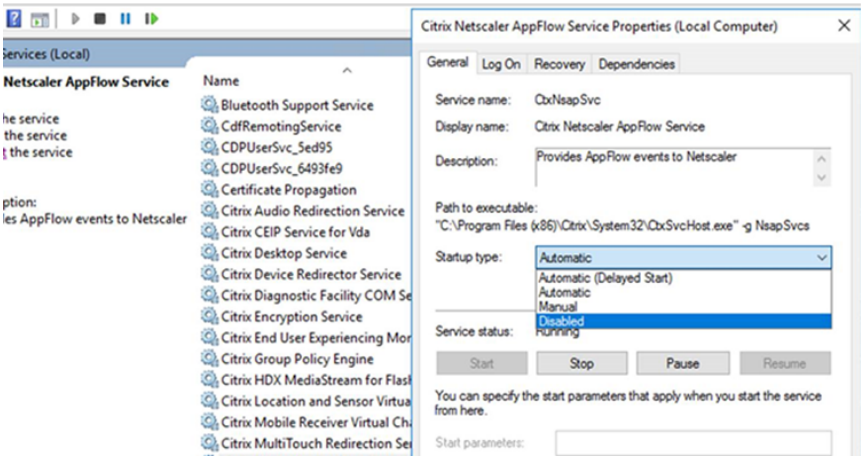
- Citrix Virtual Apps and Desktops 7 v1808

- XenApp e XenDesktop 7.17
- NetScaler versione 12.0 Build 57.x
- App Citrix Workspace per Windows 1808
- Citrix Receiver per Windows 4.10
- App Citrix Workspace per Mac 1808
- Citrix Receiver per Mac 12.8

#### Attivare o disattivare il canale virtuale HDX Insight

Per disattivare questa funzione, impostare le proprietà del servizio Citrix NetScaler Application Flow su Disabilitato. Per attivarla, impostare il servizio su Automatico. In entrambi i casi, si consiglia di riavviare il server dopo aver modificato queste proprietà. Per impostazione predefinita, questo servizio è abilitato (Automatico).




### Sperimentare le funzionalità HDX dal proprio desktop virtuale

- Per vedere come il reindirizzamento dei contenuti del browser, una delle quattro tecnologie di reindirizzamento multimediale HDX, accelera la distribuzione di contenuti multimediali HTML5 e WebRTC:

  1. Scaricare l'estensione del browser Chrome e installarla sul desktop virtuale.
  2. Per scoprire come il reindirizzamento dei contenuti del browser accelera la distribuzione di contenuti multimediali ai desktop virtuali, è possibile visualizzare un video sul desktop da un sito Web contenente video HTML5, come YouTube. Gli utenti non sanno quando è in esecuzione il reindirizzamento dei contenuti del browser. Per verificare se è in uso il reindirizzamento del contenuto del browser, trascinare rapidamente la finestra del browser. Verrà visualizzato un ritardo o un fuori quadro tra il riquadro di visualizzazione e l'interfaccia utente. È inoltre possibile fare clic con il pulsante destro del mouse sulla pagina Web e cercare **Informazioni su HDX Browser Redirection** nel menu.

- Per vedere come HDX fornisce l'audio ad alta definizione:

    1. Configurare il client Citrix per la massima qualità audio; vedere la documentazione dell'app Citrix Workspace per i dettagli.
    2. Riprodurre file musicali utilizzando un lettore audio digitale (ad esempio iTunes) sul desktop.

HDX offre un'esperienza grafica e video superiore per la maggior parte degli utenti per impostazione predefinita e la configurazione non è necessaria. Le impostazioni dei criteri Citrix che offrono la migliore esperienza per la maggior parte dei casi d'uso sono abilitate per impostazione predefinita.

- HDX seleziona automaticamente il metodo di consegna migliore in base al client, alla piattaforma, all'applicazione e alla larghezza di banda della rete, per poi eseguire l'ottimizzazione automatica in base alle condizioni che cambiano.
- HDX ottimizza le prestazioni di grafica e video 2D e 3D.
- HDX consente ai dispositivi utente di trasmettere file multimediali direttamente dal provider di origine su Internet o Intranet, anziché tramite il server host. Se i requisiti per il recupero dei contenuti sul lato client non vengono soddisfatti, la distribuzione dei contenuti multimediali effettua il fallback sul recupero dei contenuti sul lato server e sul reindirizzamento multimediale. In genere, non è necessario modificare i criteri delle funzionalità di reindirizzamento multimediale.
- HDX offre contenuti video avanzati con rendering via server ai desktop virtuali quando non è disponibile il reindirizzamento multimediale: visualizzare un video su un sito Web contenente video ad alta definizione, quale http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Buono a sapersi:

- Per informazioni sul supporto e sui requisiti per le funzionalità HDX, vedere l'articolo Requisiti di sistema. Salvo diversamente indicato, le funzionalità HDX sono disponibili per i computer con il sistema operativo Windows multi-sessione e a sessione singola supportati, oltre ai desktop Accesso remoto PC.
- Questo contenuto descrive come ottimizzare l'esperienza utente, migliorare la scalabilità del server o ridurre i requisiti di larghezza di banda. Per informazioni sull'utilizzo dei criteri e delle impostazioni dei criteri Citrix, vedere la documentazione dei criteri Citrix relativa a questa versione.
- Per istruzioni che includono la modifica del Registro di sistema, procedere con cautela: la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

## Riconnessione automatica del client e affidabilità della sessione

Quando si accede ad applicazioni o desktop ospitati, potrebbe verificarsi un'interruzione della rete. Per godere di una riconnessione più fluida, offriamo la riconnessione automatica del client e l'affidabilità della sessione. In una configurazione predefinita, viene prima avviata l'affidabilità della sessione e quindi segue la riconnessione automatica del client.

**Riconnessione automatica del client:**

La riconnessione automatica del client riavvia il motore client per riconnettersi a una sessione disconnessa. La riconnessione automatica del client chiude (o disconnette) la sessione utente dopo il tempo specificato nella relativa impostazione. Se è in corso la riconnessione automatica del client, il sistema invia all'utente una notifica di interruzione della rete per le applicazioni e i desktop nel modo seguente:

- **Desktop.** La finestra della sessione è disattivata e un conto alla rovescia mostra il tempo che manca alla riconnessione.
- **Applicazioni.** La finestra della sessione si chiude e viene visualizzata una finestra di dialogo contenente un conto alla rovescia che mostra il tempo che manca al tentativo di riconnessione.

Durante la riconnessione automatica del client, le sessioni si riavviano in attesa della connettività di rete. L'utente non può interagire con le sessioni mentre è in corso la riconnessione automatica del client.

Durante la riconnessione, le sessioni disconnesse si riconnettono utilizzando le informazioni di connessione salvate. L'utente può interagire normalmente con le applicazioni e i desktop.

Impostazioni predefinite di riconnessione automatica del client:

- Timeout di riconnessione automatica del client: 120 secondi
- Riconnessione automatica del client: abilitata
- Autenticazione di riconnessione automatica del client: disattivata
- Registrazione della riconnessione automatica del client: disabilitata

Per ulteriori informazioni, vedere Impostazioni dei criteri di riconnessione automatica del client.

**Affidabilità della sessione:**

L'affidabilità della sessione riconnette le sessioni ICA senza problemi durante le interruzioni di rete. L'affidabilità della sessione chiude (o disconnette) la sessione utente dopo il tempo specificato nell'impostazione. Dopo il timeout dell'affidabilità della sessione, avranno effetto le impostazioni di riconnessione automatica del client, tentando di riconnettere l'utente alla sessione disconnessa. Quando l'affidabilità della sessione è in corso, la notifica di interruzione della rete delle applicazioni e dei desktop viene inviata all'utente come segue:

- **Desktop.** La finestra della sessione diventa trasparente e un conto alla rovescia visualizza il tempo che manca alle riconnessioni.

- **Applicazioni.** La finestra diventa trasparente, così come le finestre a comparsa interrotte dalla connessione dall'area di notifica.

Mentre l'affidabilità della sessione è attiva, l'utente non può interagire con le sessioni ICA. Tuttavia, le azioni dell'utente quali le sequenze di tasti vengono memorizzate nel buffer per pochi secondi immediatamente dopo l'interruzione della rete e vengono ritrasmesse quando la rete è disponibile.

Al momento della riconnessione, il client e il server riprendono dallo stesso punto in cui si trovavano nel loro scambio di protocollo. Le finestre di sessione perdono la trasparenza e vengono visualizzate le finestre a comparsa appropriate dell'area di notifica per le applicazioni.

Impostazioni predefinite dell'affidabilità della sessione

- Timeout dell'affidabilità della sessione: 180 secondi
- Livello di opacità dell'interfaccia utente di riconnessione: 80%
- Connessione all'affidabilità della sessione: abilitata
- Numero di porta dell'affidabilità della sessione: 2598

Per ulteriori informazioni, vedere Impostazioni dei criteri di affidabilità delle sessioni.

**NetScaler con riconnessione automatica del client e affidabilità della sessione:**

Se i criteri Multistream e Multiport sono attivati sul server e una o tutte queste condizioni sono vere, la riconnessione automatica del client non funziona:

- L'affidabilità della sessione è disabilitata su NetScaler Gateway.
- Si verifica un failover sull'appliance NetScaler.
- NetScaler SD-WAN viene utilizzato con NetScaler Gateway.

## Velocità effettiva adattiva di HDX

La velocità effettiva adattiva di HDX consente di ottimizzare in modo intelligente la velocità di picco della sessione ICA regolando i buffer di output. Il numero di buffer di output viene inizialmente impostato su un valore elevato. Questo valore elevato consente di trasmettere i dati al client in modo più rapido ed efficiente, soprattutto nelle reti ad alta latenza. Fornire una migliore interattività, trasferimenti di file più rapidi, riproduzione video più fluida, frequenza di aggiornamento e risoluzione più elevate si traduce in un'esperienza utente migliorata.

L'interattività della sessione viene costantemente misurata per determinare se qualsiasi flusso di dati all'interno della sessione ICA influisce negativamente sull'interattività. In tal caso, la velocità effettiva viene ridotta per ridurre l'impatto sulla sessione del flusso di dati di grandi dimensioni e consentire il ripristino dell'interattività.

> **Importante:**
>
> La velocità effettiva adattiva di HDX modifica il modo in cui vengono impostati i buffer di output spostando questo meccanismo dal client alla VDA e non è necessaria alcuna configurazione manuale.

Questa funzione ha i seguenti requisiti:

- VDA versione 1811 o successiva
- App Workspace per Windows 1811 o versione successiva

### Migliorare la qualità dell'immagine inviata ai dispositivi utente

Le seguenti impostazioni dei criteri di visualizzazione visiva controllano la qualità delle immagini inviate dai desktop virtuali ai dispositivi utente.

- Qualità visiva. Controlla la qualità visiva delle immagini visualizzate sul dispositivo utente: media, alta, sempre senza perdite, compila per senza perdite (impostazione predefinita= media). La qualità video effettiva mediante l'impostazione predefinita del supporto dipende dalla larghezza di banda disponibile.
- Frequenza di aggiornamento target. Specifica il numero massimo di fotogrammi al secondo inviati dal desktop virtuale al dispositivo utente (impostazione predefinita= 30). Per i dispositivi con CPU più lente, specificando un valore inferiore, si può migliorare l'esperienza utente. La massima frequenza di fotogrammi supportata al secondo è 60.
- Limite di memoria di visualizzazione. Specifica la dimensione massima del buffer video per la sessione in kilobyte (impostazione predefinita= 65536 KB). Per le connessioni che richiedono una maggiore profondità di colore e una risoluzione più elevata, aumentare il limite. È possibile calcolare la memoria massima richiesta.

### Migliorare le prestazioni delle videoconferenze

Molte delle applicazioni per videoconferenze più diffuse sono ottimizzate per la distribuzione da Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) attraverso il reindirizzamento multimediale (vedere, ad esempio, HDX RealTime Optimization Pack). Per le applicazioni non ottimizzate, la compressione video HDX della webcam migliora l'efficienza della larghezza di banda e la tolleranza alla latenza per le webcam durante le videoconferenze in una sessione. Questa tecnologia trasmette il traffico delle webcam su un canale virtuale multimediale dedicato. Questa tecnologia utilizza meno larghezza di banda rispetto al supporto isocrono HDX Plug-n-Play USB per il reindirizzamento e funziona bene sulle connessioni WAN.

Gli utenti dell'app Citrix Workspace possono ignorare il comportamento predefinito scegliendo l'impostazione Mic & Webcam (Microfono e webcam) di Desktop Viewer **Don't use my microphone or**

**webcam** (Non utilizzare il microfono e la webcam). Per impedire agli utenti di modificare la compressione video HDX della webcam, disabilitare il reindirizzamento dei dispositivi USB utilizzando le impostazioni dei criteri in ICA policy settings (Impostazioni criteri ICA) > USB Devices policy (Criteri dispositivi USB).

La compressione video HDX della webcam richiede che siano abilitate le seguenti impostazioni dei criteri (sono tutte abilitate per impostazione predefinita).

- Client audio redirection (Reindirizzamento audio client)
- Client microphone redirection (Reindirizzamento microfono client)
- Multimedia conferencing (Conferenze multimediali)
- Reindirizzamento di Windows Media

Se una webcam supporta la codifica hardware, la compressione video HDX utilizza la codifica hardware per impostazione predefinita. La codifica hardware potrebbe consumare più larghezza di banda rispetto alla codifica software. Per forzare la compressione del software, aggiungere il seguente valore di chiave DWORD alla chiave del Registro di sistema: `HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1`.

### Priorità relative al traffico di rete

Vengono assegnate priorità al traffico di rete tra più connessioni per una sessione utilizzando router supportati da Quality of Service. Quattro flussi TCP e due flussi UDP (User Datagram Protocol) sono disponibili per trasportare il traffico ICA tra il dispositivo utente e il server:

- Flussi TCP: in tempo reale, interattivi, in background e in blocco
- Flussi UDP: comunicazione remota display Framehawk e voce

Ogni canale virtuale è associato a una priorità specifica e trasportato nella connessione corrispondente. È possibile impostare i canali in modo indipendente, in base al numero della porta TCP utilizzata per la connessione.

Le connessioni in streaming a più canali sono supportate per gli agenti di distribuzione virtuali (VDA) installati su computer Windows 10 e Windows 8. Collaborare con l'amministratore di rete per assicurarsi che le porte CGP (Common Gateway Protocol) configurate nell'impostazione Criterio multi-porta siano assegnate correttamente ai router di rete.

La qualità del servizio è supportata solo quando sono configurate più porte di affidabilità della sessione o le porte CGP.

> **Avviso:**
>
> Utilizzare la sicurezza di trasporto quando si utilizza questa funzione. Citrix consiglia di utilizzare IPsec (Internet Protocol Security) o TLS (Transport Layer Security). Le connessioni TLS sono sup-

> portate solo quando le connessioni attraversano un NetScaler Gateway che supporta ICA multi-flusso. In una rete aziendale interna, le connessioni multi-flusso con TLS non sono supportate.

Per impostare la qualità del servizio per più connessioni in streaming, aggiungere le seguenti impostazioni dei criteri Citrix a un criterio (vedere Impostazioni dei criteri delle connessioni multi-flusso per i dettagli):

- Criterio multi-porta: questa impostazione specifica le porte per il traffico ICA tra più connessioni e stabilisce le priorità della rete.
  - Selezionare una priorità dall'elenco delle priorità per la porta predefinita CGP. Per impostazione predefinita, la porta primaria (2598) ha una priorità alta.
  - Digitare più porte CGP in CGP port1, CGP port2, and CGP port3 in base alle esigenze e identificare le priorità per ciascuna. Ogni porta deve avere una priorità univoca.

  Configurare in modo esplicito i firewall sui VDA per consentire il traffico TCP aggiuntivo.
- Impostazione computer multi-flusso: questa impostazione è disabilitata per impostazione predefinita. Se si utilizza Citrix NetScaler SD-WAN con supporto multi-flusso nell'ambiente, non è necessario configurare questa impostazione. Configurare l'impostazione di questo criterio quando si utilizzano router di terze parti o ripetitori di filiali legacy per ottenere la qualità del servizio desiderata.
- Impostazione utente multi-flusso: questa impostazione è disabilitata per impostazione predefinita.

Perché i criteri contenenti queste impostazioni abbiano effetto, gli utenti devono scollegarsi e quindi accedere alla rete.

### Visualizzare o nascondere la barra della lingua remota

La barra della lingua visualizza la lingua di input preferita in una sessione dell'applicazione. Se questa funzione è abilitata (impostazione predefinita), è possibile mostrare o nascondere la barra della lingua dall'interfaccia utente **Preferenze avanzate > Barra della lingua** nell'app Citrix Workspace per Windows. Utilizzando un'impostazione del Registro di sistema sul lato VDA, è possibile disattivare il controllo client della funzionalità barra della lingua. Se questa funzionalità è disabilitata, l'impostazione dell'interfaccia utente client non ha effetto e l'impostazione corrente per utente determina lo stato della barra della lingua. Per ulteriori informazioni, vedere Migliorare l'esperienza utente.

Per disabilitare il controllo client della funzionalità barra della lingua dal VDA:

1. Nell'editor del Registro di sistema, passare a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`.
2. Creare una chiave valore DWORD, SeamlessFlags, e impostarla su 0x40000.

## Mappatura tastiera Unicode

Le versioni non Windows di Citrix Receiver utilizzano il layout di tastiera locale (Unicode). Se un utente modifica il layout della tastiera locale e il layout della tastiera del server (codice di scansione), questi potrebbero non essere sincronizzati e l'output potrebbe non essere corretto. Ad esempio, Utente1 modifica il layout di tastiera locale da inglese a tedesco. Utente1 cambia quindi la tastiera lato server scegliendo il layout tedesco. Anche se entrambi i layout di tastiera sono tedeschi, potrebbero non essere sincronizzati causando un output di caratteri errati.

### Abilitare o disabilitare il mapping del layout di tastiera Unicode

Per impostazione predefinita, la funzionalità è disabilitata sul lato VDA. Per abilitare la funzionalità, attivarla utilizzando l'editor del Registro di sistema regedit sul VDA. Aggiungere la seguente chiave del Registro di sistema:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: EnableKlMap

Tipo: DWORD

Valore: 1

Per disattivare questa funzione, impostare **EnableKlMap** su 0 o eliminare la chiave **CtxKlMap**.

### Abilitare la modalità compatibile con la mappatura del layout della tastiera Unicode

Per impostazione predefinita, la mappatura del layout di tastiera Unicode effettua automaticamente l'hook di alcune API di Windows per ricaricare la nuova mappa del layout di tastiera Unicode quando si modifica il layout di tastiera sul lato server. Alcune applicazioni non consentono di effettuare l'hook. Per mantenere la compatibilità, è possibile modificare la funzionalità in modalità compatibile per supportare queste applicazioni non collegate con l'hook. Aggiungere la seguente chiave del Registro di sistema:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: DisableWindowHook

Tipo: DWORD

Valore: 1

Per utilizzare la normale mappatura del layout di tastiera Unicode, impostare **DisableWindowHook** su 0.

# Canali virtuali Citrix ICA

October 6, 2022

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

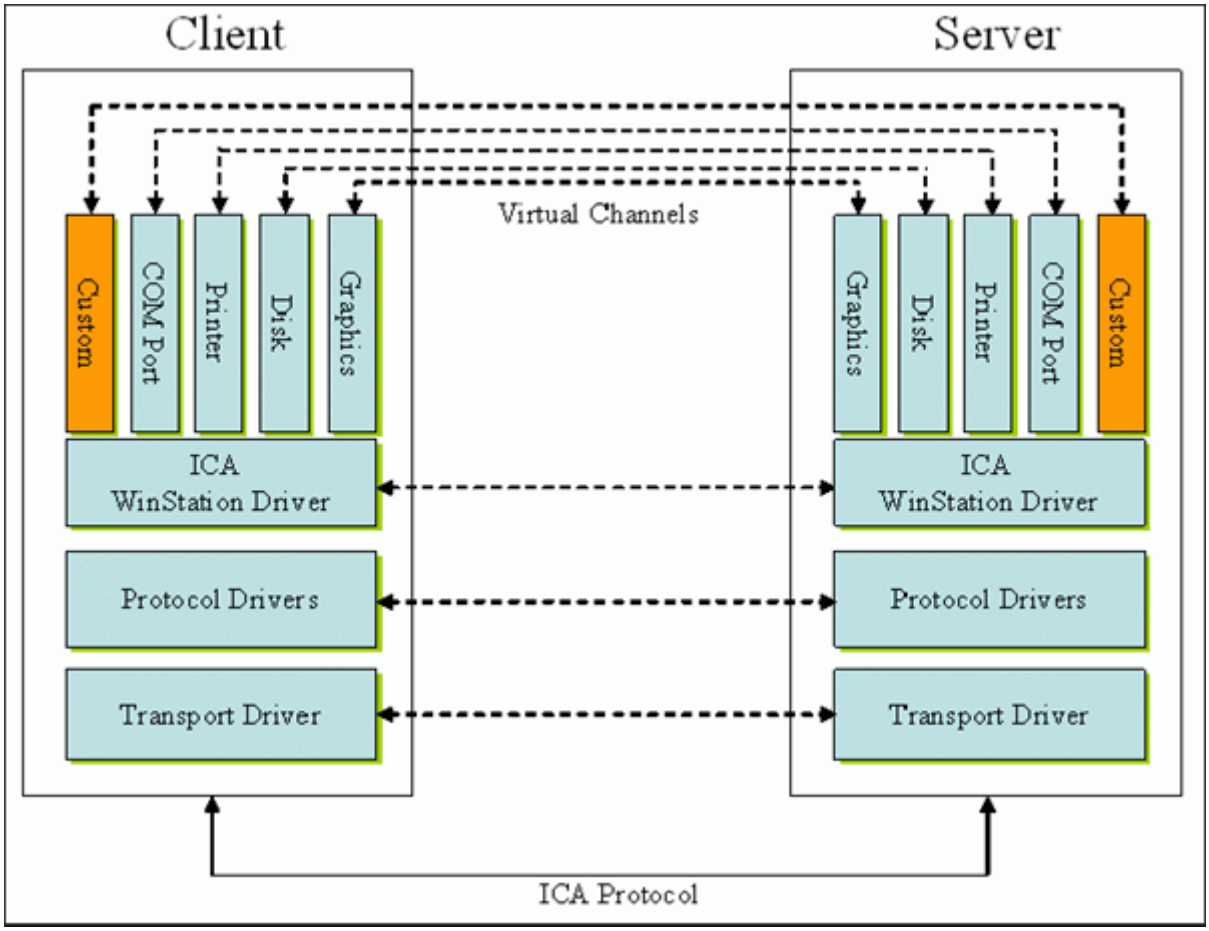
## Cosa sono i canali virtuali ICA?

Gran parte delle funzionalità e della comunicazione tra l'app Citrix Workspace e i server Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) avviene su canali virtuali. I canali virtuali sono una parte necessaria dell'esperienza di elaborazione remota con i server Citrix DaaS. I canali virtuali sono utilizzati per:

- Audio
- Porte COM
- Dischi
- Grafica
- Porte LPT
- Stampanti
- Smart card
- Canali virtuali personalizzati di terze parti
- Video

Talvolta vengono rilasciati nuovi canali virtuali con Citrix DaaS e l'app Citrix Workspace per fornire più funzionalità.




Un canale virtuale è costituito da un driver virtuale lato client che comunica con un'applicazione lato server. Citrix DaaS viene fornito con vari canali virtuali inclusi. Sono progettati per consentire a clienti e fornitori terzi di creare i propri canali virtuali utilizzando uno dei kit di sviluppo software (SDK) in dotazione.

I canali virtuali offrono un modo sicuro per svolgere varie attività. Ad esempio, un'applicazione in esecuzione su un server Citrix Virtual Apps che comunica con un dispositivo lato client o un'applicazione che comunica con l'ambiente lato client.

Sul lato client, i canali virtuali corrispondono a driver virtuali. Ogni driver virtuale fornisce una funzione specifica. Alcuni sono necessari per il normale funzionamento, mentre altri sono facoltativi. I driver virtuali operano a livello di protocollo sul livello di presentazione. Ci possono essere diversi protocolli attivi in qualsiasi momento tramite canali multiplexing forniti dal livello di protocollo Windows Station (WinStation).

Le seguenti funzioni sono contenute nel valore del Registro di sistema VirtualDriver in questo percorso del Registro di sistema:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\
Advanced\Modules\ICA 3.0
```

oppure

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (per 64 bit)

- Thinwire3.0 (obbligatorio)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Appunti
- ClientComm
- ClientAudio
- LicenseHandler (obbligatorio)
- TWI (obbligatorio)
- SmartCard
- ICACTL (obbligatorio)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Nota:**
>
> È possibile disattivare funzionalità client specifiche rimuovendo uno o più di questi valori dalla chiave del Registro di sistema. Ad esempio, se si desidera rimuovere gli Appunti client, rimuovere la parola **Appunti**.

Questo elenco contiene i file dei driver virtuali client e le rispettive funzioni. Citrix Virtual Apps e l'app Citrix Workspace per Windows utilizzano questi file. Sono sotto forma di librerie di collegamento dinamico (modalità utente) e non di driver Windows (modalità kernel) ad eccezione di USB generico come descritto nel canale virtuale USB generico.

- vd3dn.dll: canale virtuale Direct3D utilizzato per il reindirizzamento della composizione desktop
- vdcamN.dll: audio bidirezionale
- vdcdm30n.dll: mappatura unità client
- vdcom30N.dll: mappatura porta COM client
- vdcpm30N.dll: mappatura stampante client
- vdctln.dll: canale dei controlli ICA
- vddvc0n.dll: canale virtuale dinamico
- vdeuemn.dll: monitoraggio dell'esperienza utente finale
- vdgusbn.dll: canale virtuale USB generico
- vdkbhook.dll: pass-through della chiave trasparente

- vdlfpn.dll: canale di visualizzazione Framehawk su trasporto simil-UDP
- vdmmn.dll: supporto multimediale
- vdmrvc.dll: canale virtuale di Receiver mobile
- vdmtchn.dll: supporto multi-touch
- vdscardn.dll: supporto delle smartcard
- vdsens.dll: canale virtuale dei sensori
- vdspl30n.dll: UPD client
- vdsspin.dll: Kerberos
- vdtuin.dll: interfaccia utente trasparente
- vdtw30n.dll: client Thinwire
- vdtwin.dll: Seamless
- vdtwn.dll: Twain

Alcuni canali virtuali sono compilati in altri file. Ad esempio, la mappatura degli Appunti è disponibile in wfica32.exe

#### Compatibilità con 64 bit

L'app Citrix Workspace per Windows è compatibile con 64 bit. Come avviene per la maggior parte dei file binari compilati per 32 bit, questi file client hanno equivalenti compilati a 64 bit:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

#### Canale virtuale USB generico

L'implementazione del canale virtuale USB generico utilizza due driver in modalità kernel insieme al driver del canale virtuale vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

### Come funzionano i canali virtuali ICA

I canali virtuali vengono caricati in più modi. La Shell (WfShell per il server e PicaShell per la workstation) carica alcuni canali virtuali. Alcuni canali virtuali sono ospitati come servizi Windows.

Moduli di canale virtuale caricati dalla Shell, ad esempio:

- EUEM
- Twain
- Appunti
- Contenuti multimediali
- Condivisione delle sessioni Seamless
- Fuso orario

Alcuni sono caricati come modalità kernel, ad esempio:

- CtxDvcs.sys: canale virtuale dinamico
- Icausbb.sys: reindirizzamento USB generico
- Picadm.sys: mappatura dell'unità client
- Picaser.sys: reindirizzamento porta COM
- Picapar.sys: reindirizzamento porta LPT

### Canale virtuale grafico sul lato server

A partire da XenApp 7.0 e XenDesktop7.0, `ctxgfx.exe` ospita il canale virtuale grafico per le sessioni basate su workstation e server terminal. `Ctxgfx` ospita moduli specifici della piattaforma che interagiscono con il driver corrispondente (`Icardd.dll` per RDSH e `vdod.dll` e `vidd.dll` per workstation).

Per le distribuzioni di XenDesktop 3D Pro è installato un driver di grafica OEM per la GPU corrispondente sul VDA. `Ctxgfx` carica moduli adattatori specializzati per interagire con il driver grafico OEM.

### Hosting di canali specializzati nei servizi di Windows

Sui server Citrix DaaS, vari canali sono ospitati come servizi Windows. Tale hosting fornisce semantica da uno a molti per più applicazioni in una sessione e più sessioni sul server. Esempi di tali servizi sono:

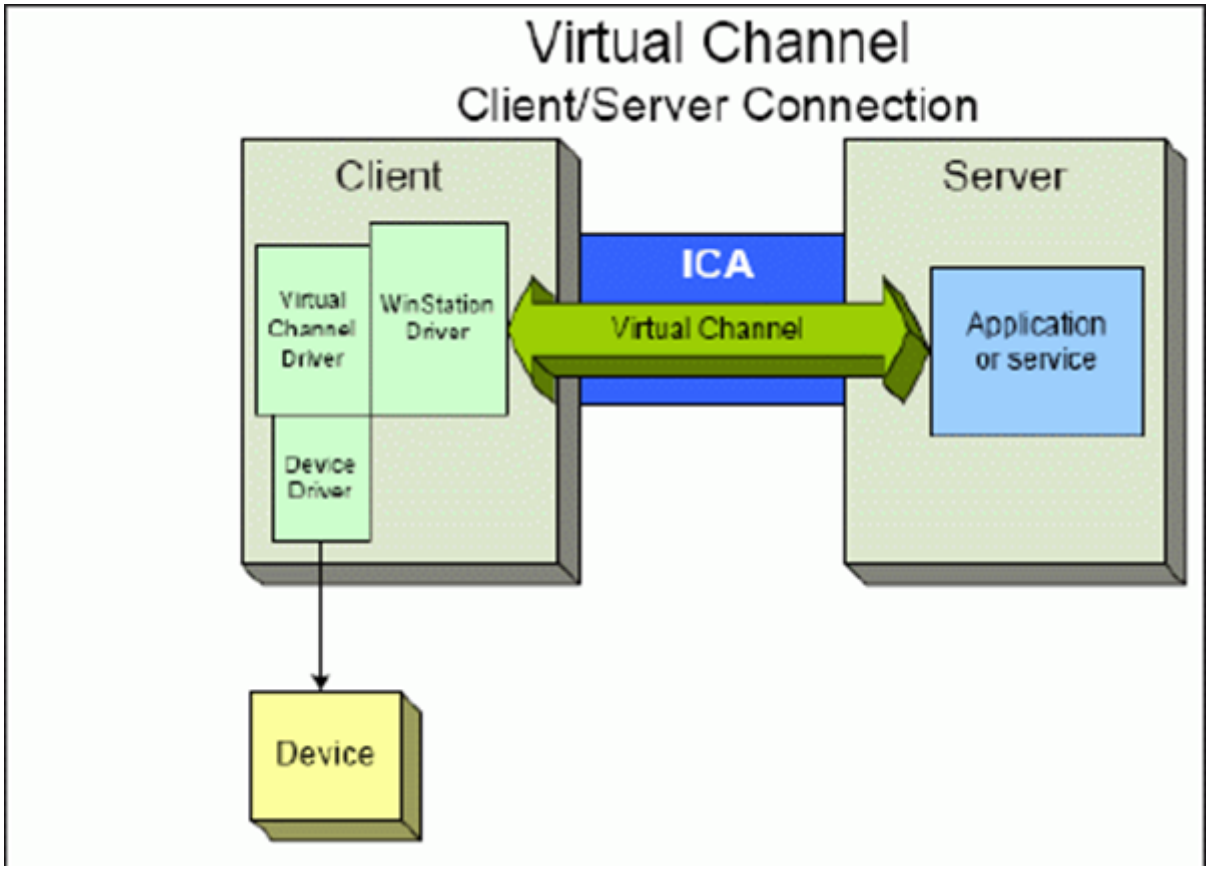
- Servizio di redirector periferiche Citrix
- Servizio di canale virtuale dinamico Citrix
- Servizio di monitoraggio dell'esperienza utente finale Citrix

- Servizio canale virtuale di posizione e sensore Citrix
- Servizio di reindirizzamento Citrix MultiTouch
- Servizio Citrix Print Manager
- Servizio smartcard Citrix
- Servizio di reindirizzamento audio Citrix (solo Citrix Virtual Desktops)

Il canale audio virtuale su Citrix Virtual Apps è ospitato utilizzando il servizio Windows Audio.

Sul lato server, tutti i canali virtuali client vengono instradati tramite il driver WinStation, Wdica.sys. Sul lato client, il driver WinStation corrispondente, incorporato in wfica32.exe, esegue il polling dei canali virtuali del client. Questa immagine illustra la connessione client-server del canale virtuale.




Questa panoramica contiene uno scambio di dati client-server che utilizza un canale virtuale.

1. Il client si connette al server Citrix DaaS. Il client passa informazioni sui canali virtuali che supporta al server.
2. L'applicazione lato server viene avviata, ottiene un handle per il canale virtuale e, facoltativamente, interroga per ottenere ulteriori informazioni sul canale.
3. Il driver virtuale client e l'applicazione lato server passano i dati utilizzando i due metodi seguenti:

- Se l'applicazione server dispone di dati da inviare al client, i dati vengono inviati immediatamente al client. Quando il client riceve i dati, il driver WinStation effettua il de-multiplex dei dati del canale virtuale provenienti dal flusso ICA e li passa immediatamente al driver virtuale client.
- Se il driver virtuale client dispone di dati da inviare al server, i dati vengono inviati alla successiva esecuzione del polling del driver WinStation. Quando il server riceve i dati, questi vengono messi in coda fino a quando l'applicazione del canale virtuale non li legge. Non c'è modo di avvisare l'applicazione del canale virtuale del server che i dati sono stati ricevuti.

4. Una volta completata l'applicazione del canale virtuale del server, chiude il canale virtuale e libera tutte le risorse eventualmente allocate.

### Creazione di un canale virtuale personalizzato utilizzando Virtual Channel SDK

La creazione di un canale virtuale mediante Virtual Channel SDK richiede conoscenze di programmazione di livello intermedio. Utilizzare questo metodo per fornire un percorso di comunicazione principale tra il client e il server. Ad esempio, se si sta implementando l'utilizzo di un dispositivo sul lato client, ad esempio uno scanner, da utilizzare con un processo nella sessione.

> **Nota:**
>
> - L'SDK Virtual Channel richiede l'SDK WFAPI per scrivere il lato server del canale virtuale.
> - Per via della sicurezza avanzata per Citrix DaaS, è necessario specificare quali canali virtuali possono essere aperti in una sessione ICA. Per ulteriori informazioni, vedere Impostazione dei criteri Virtual channel allow list (Elenco di elementi consentiti del canale virtuale).

### Creazione di un proprio canale virtuale utilizzando l'SDK ICA Client Object

Creare un canale virtuale utilizzando l'ICO (ICA Client Object) è più semplice rispetto all'utilizzo di Virtual Channel SDK. Utilizzare l'ICO creando un oggetto con nome nel programma utilizzando il metodo **CreateChannels**.

> **Importante:**
>
> A causa della sicurezza avanzata a partire dalla versione 10.00 di Citrix Receiver per Windows e versioni successive (e le app Citrix Workspace per Windows), è necessario eseguire un ulteriore passo durante la creazione di un canale virtuale ICO.

Per ulteriori informazioni, vedere Guida al programmatore delle specifiche API degli oggetti client

### Funzionalità pass-through dei canali virtuali

La maggior parte dei canali virtuali forniti da Citrix funziona senza modifiche quando si utilizza l'app Citrix Workspace per Windows all'interno di una sessione ICA (nota anche come sessione pass-through). Ci sono aspetti da considerare quando si utilizza il client in hop extra.

Le seguenti funzioni funzionano allo stesso modo in hop singolo o multiplo:

- Mappatura porta COM client
- Mappatura unità client
- Mappatura stampante client
- UPD client
- Monitoraggio dell'esperienza utente finale
- USB generico
- Kerberos
- Supporto multimediale
- Supporto smartcard
- Pass-through della chiave trasparente
- Twain

Poiché la natura intrinseca della latenza e di fattori quali compressione, decompressione e rendering eseguiti a ogni hop, le prestazioni potrebbero essere influenzate da ogni hop aggiuntivo sottoposto al client. Le aree di influenza sono:

- Audio bidirezionale
- Trasferimenti di file
- Reindirizzamento USB generico
- Seamless
- Thinwire

> **Importante:**
>
> Per impostazione predefinita, le unità client mappate da un'istanza del client in esecuzione in una sessione pass-through sono limitate alle unità client del client di connessione.

### Funzionalità pass-through dei canali virtuali tra una sessione di Citrix Virtual Desktop e una sessione di Citrix Virtual App

La maggior parte dei canali virtuali forniti da Citrix funziona senza modifiche quando si utilizza l'app Citrix Workspace per Windows all'interno di una sessione ICA su un server Citrix Virtual Desktops (noto anche come sessione pass-through).

In particolare, sul server Citrix Virtual Desktops, è presente un hook VDA che esegue **picaPassthruHook**. Questo hook fa credere al client di essere in esecuzione su un server CPS e posiziona il client nella sua tradizionale modalità pass-through.

Supportiamo i seguenti canali virtuali tradizionali e le loro funzionalità:

- Client
- Mappatura porta COM client
- Mappatura unità client
- Mappatura stampante client
- USB generico (limitato a causa delle prestazioni)
- Supporto multimediale
- Supporto smartcard
- SSON
- Pass-through della chiave trasparente

## Sicurezza e canali virtuali ICA

La protezione dell'utilizzo è una parte importante della pianificazione, dello sviluppo e dell'implementazione di canali virtuali. Questo documento fa riferimento a specifiche aree di sicurezza in molte sue parti.

## Procedure consigliate

Aprire i canali virtuali quando ci si **connette** e ci si **riconnette**. Chiudere i canali virtuali quando ci si scollega e ci si **disconnette**.

Tenere presenti le seguenti linee guida quando si creano script che utilizzano le funzioni del canale virtuale.

**Denominazione dei canali virtuali:**

È possibile creare un massimo di 32 canali virtuali. Diciassette canali su 32 sono riservati per scopi speciali.

- I nomi dei canali virtuali non devono contenere più di sette caratteri.
- I primi tre caratteri sono riservati al nome del fornitore e i quattro successivi al tipo di canale. Ad esempio, **CTXAUD** rappresenta il canale audio virtuale Citrix.

I canali virtuali sono indicati da un nome ASCII di sette caratteri (o più breve). In alcune versioni precedenti del protocollo ICA, i canali virtuali erano numerati. I numeri vengono ora assegnati dinamicamente in base al nome ASCII, rendendo più facile l'implementazione. Gli utenti che stanno sviluppando codice per canali virtuali solo per uso interno possono utilizzare qualsiasi nome di sette

caratteri che non sia in conflitto con i canali virtuali esistenti. Utilizzare solo numeri e caratteri ASCII maiuscoli e minuscoli. Seguire la convenzione di denominazione esistente quando si aggiungono i propri canali virtuali. Ci sono diversi canali predefiniti. I canali predefiniti iniziano con l'identificatore OEM CTX e sono riservati all'uso da parte di Citrix.

**Supporto a doppio hop:**

| Canale virtuale | Il doppio hop è supportato? |
|---|---|
| Audio | No |
| Browser Content Redirection | No |
| CDM | Sì |
| CEIP | No |
| Appunti | Sì |
| Continuum (MRVC) | No |
| VC di controllo | Sì |
| Reindirizzamento video HTML5 (v1) | Sì |
| Tastiera, mouse | Sì |
| MultiTouch | No |
| NSAPVC | No |
| Stampa | Sì |
| SensVC | No |
| Smartcard | Sì |
| Twain | Sì |
| VC USB | Sì |
| Dispositivi WAYCOM -K2M mediante VC USB | Sì |
| Compressione video della webcam | Sì |
| Reindirizzamento di Windows Media | Sì |

### Vedere anche

- SDK per il canale virtuale ICA
- Citrix Developer Network è la sede di tutte le risorse tecniche e le discussioni che riguardano l'utilizzo di SDK Citrix. In questa rete, è possibile trovare l'accesso a SDK, codice di esempio e

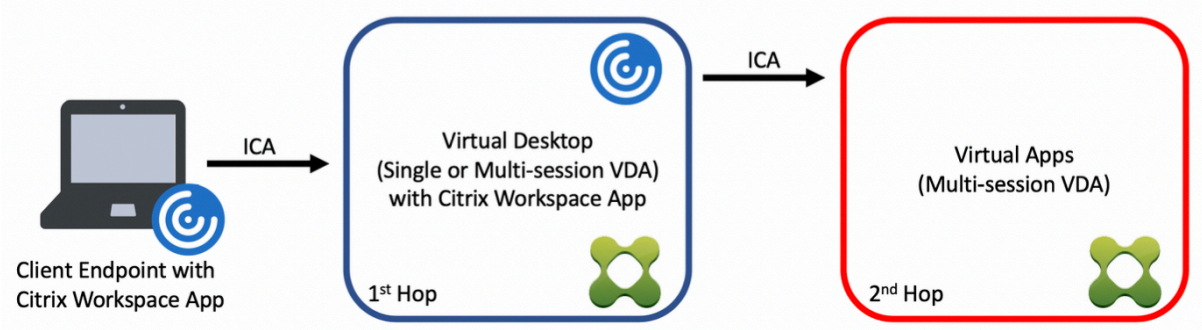
 

script, estensioni e plug-in e documentazione SDK. Sono inclusi anche i forum Citrix Developer Network, dove si svolgono discussioni tecniche su ciascuno degli SDK Citrix.

## Doppio hop in Citrix DaaS

October 6, 2022

Nel contesto di una sessione client Citrix, il termine "doppio hop"si riferisce a una sessione di Citrix Virtual App in esecuzione all'interno di una sessione di Citrix Virtual Desktop. Il diagramma seguente illustra un doppio hop.




In uno scenario a doppio hop, si tratta di quando l'utente si connette a un Citrix Virtual Desktop in esecuzione su un sistema operativo VDA a sessione singola (noto come VDI) o un sistema operativo VDA multisessione (noto come desktop pubblicato), che è considerato il primo hop. Dopo che si connette al desktop virtuale, l'utente può avviare una sessione di Citrix Virtual Apps. Questo è considerato il secondo hop.

È possibile utilizzare un modello di distribuzione a doppio hop per supportare vari casi d'uso. Un esempio comune è il caso in cui gli ambienti Citrix Virtual Desktop e Citrix Virtual Apps sono gestiti da entità diverse. Questo metodo può anche essere efficace nella risoluzione dei problemi di compatibilità delle applicazioni.

### Requisiti di sistema

Tutte le edizioni di Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) supportano il doppio hop.

Il primo hop deve utilizzare una versione supportata del sistema operativo VDA a sessione singola o multisessione e dell'app Citrix Workspace. Il secondo hop deve utilizzare una versione supportata del sistema operativo multisessione VDA. Vedere la pagina Matrice dei prodotti per le versioni supportate.

Per ottenere prestazioni ottimali e compatibilità, Citrix consiglia di utilizzare un client Citrix della stessa versione o più recente rispetto alle versioni VDA in uso.

Negli ambienti in cui il primo hop comporta una soluzione desktop virtuale di terze parti (non Citrix) in combinazione con una sessione di Citrix Virtual Apps, il supporto è limitato all'ambiente Citrix Virtual Apps. In caso di problemi relativi al desktop virtuale di terze parti, tra cui, a titolo esemplificativo e non esaustivo, la compatibilità delle app Citrix Workspace, il reindirizzamento dei dispositivi hardware e le prestazioni delle sessioni, Citrix è in grado di fornire supporto tecnico a livello limitato. Per la risoluzione dei problemi potrebbe essere necessario un Citrix Virtual Desktop al primo hop.

## Considerazioni sulla distribuzione per HDX in doppio hop

In generale, ogni sessione di un doppio hop è univoca e le funzioni client-server sono isolate in un dato hop. Questa sezione include aspetti che richiedono una particolare considerazione da parte degli amministratori di Citrix. Citrix consiglia ai clienti di eseguire test approfonditi delle funzionalità HDX necessarie per garantire che l'esperienza utente e le prestazioni siano adeguate per una determinata configurazione dell'ambiente.

### Grafica

Utilizzare le impostazioni grafiche predefinite (codifica selettiva) per il primo e il secondo hop. Nel caso di HDX 3D Pro, Citrix consiglia vivamente che tutte le applicazioni che richiedono accelerazione grafica vengano eseguite localmente nel primo hop con le risorse GPU appropriate disponibili per il VDA.

### Latenza

La latenza end-to-end può influire sull'esperienza utente complessiva. Considerare la latenza aggiunta tra il primo e il secondo hop. Ciò è particolarmente importante con il reindirizzamento dei dispositivi hardware.

### Contenuti multimediali

Il rendering lato server (in sessione) dei contenuti audio e video funziona meglio nel primo hop. La riproduzione video nel secondo hop richiede la decodifica e la ricodifica al primo hop, aumentando così la larghezza di banda e l'utilizzo delle risorse hardware. I contenuti audio e video devono limitarsi al primo hop quando possibile.

### Reindirizzamento dei dispositivi USB

HDX include modalità di reindirizzamento generiche e ottimizzate per supportare una vasta gamma di tipi di dispositivi USB. Prestare particolare attenzione alla modalità in uso ad ogni hop e utilizzare la seguente tabella come riferimento per ottenere i migliori risultati. Per ulteriori informazioni sulle modalità di reindirizzamento generiche e ottimizzate, vedere Dispositivi USB generici.

| Primo hop (VDI o desktop pubblicato) | Secondo hop (app virtuali) | Note di supporto |
|---|---|---|
| Ottimizzato | Ottimizzato | Consigliato (in base al supporto del dispositivo). Ad esempio, memoria di massa USB, scanner TWAIN, Webcam, Audio. |
| Generico | Generico | Per i dispositivi in cui l'opzione ottimizzata non è disponibile. |
| Generico | Ottimizzato | Sebbene tecnicamente possibile, si consiglia di utilizzare la modalità ottimizzata su entrambi gli hop quando è disponibile il supporto del dispositivo. |
| Ottimizzato | Generico | Non supportata |

> **Nota:**
>
> A causa della verbosità intrinseca dei protocolli USB, le prestazioni possono diminuire fra un hop e l'altro. Funzionalità e risultati variano a seconda dei requisiti specifici del dispositivo e dell'applicazione. I test di convalida sono altamente raccomandati in tutti i casi di reindirizzamento del dispositivo e risultano particolarmente importanti in scenari a doppio hop.

## Eccezioni al supporto

Le sessioni a doppio hop supportano la maggior parte delle funzioni e funzionalità HDX, ad eccezione delle seguenti:

- Browser content redirection (Reindirizzamento del contenuto del browser)
- Accesso alle app locali
- RealTime Optimization Pack for Skype for Business
- Ottimizzazione di Microsoft Teams

## Trasporto HDX

May 9, 2023

Citrix HDX rappresenta un ampio set di tecnologie che offrono un'esperienza ad alta definizione agli utenti di applicazioni e desktop centralizzati, su qualsiasi dispositivo e su qualsiasi rete.

HDX è progettato in base a tre principi tecnici:

- Reindirizzamento intelligente
- Compressione adattiva
- Deduplicazione dei dati

Applicati in diverse combinazioni, questi ottimizzano l'IT e l'esperienza utente, riducono il consumo di larghezza di banda e aumentano la densità degli utenti per server di hosting.

All'interno dell'offerta HDX, è possibile connettersi tramite un protocollo di trasporto esclusivo e proprietario e connettersi con un protocollo rendevous utilizzando Citrix Gateway Service.

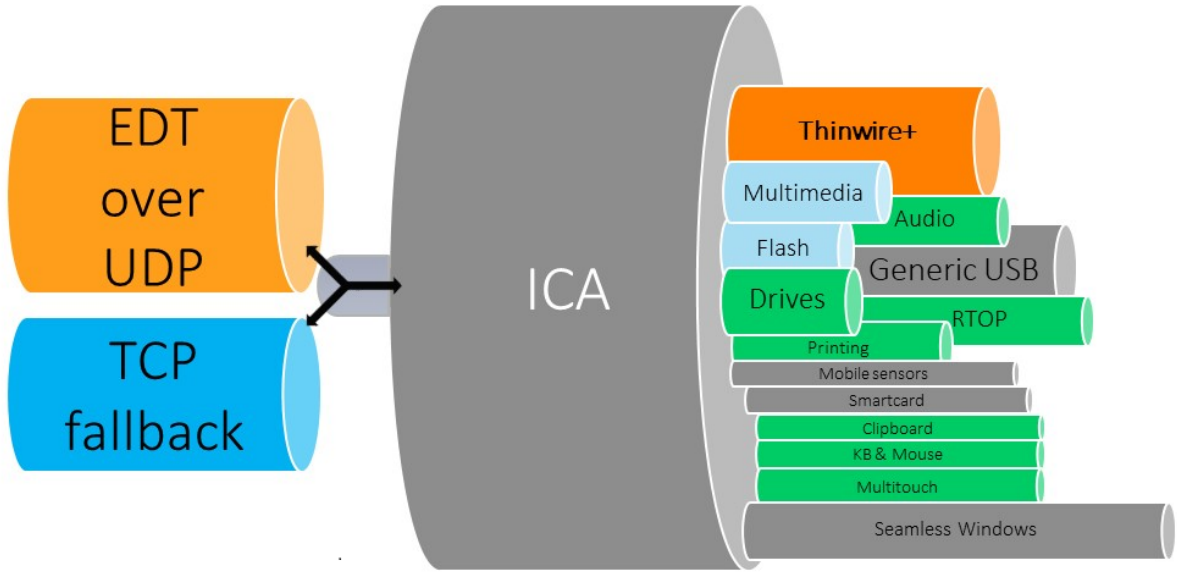
## Trasporto adattivo

August 30, 2023

Adaptive Transport (Trasporto adattivo) è un meccanismo di Citrix Virtual Apps and Desktops che offre la possibilità di utilizzare Enlightened Data Transport (EDT) o EDT Lossy come protocollo di trasporto per le connessioni ICA. Adaptive Transport (Trasporto adattivo) passa a TCP quando EDT non è disponibile.

EDT è un protocollo di trasporto proprietario di Citrix basato su User Datagram Protocol (UDP). Offre un'esperienza utente superiore su connessioni impegnative a lungo raggio, mantenendo al contempo la scalabilità del server. EDT migliora il throughput dei dati per tutti i canali virtuali ICA su reti inaffidabili, offrendo un'esperienza utente migliore e più coerente.

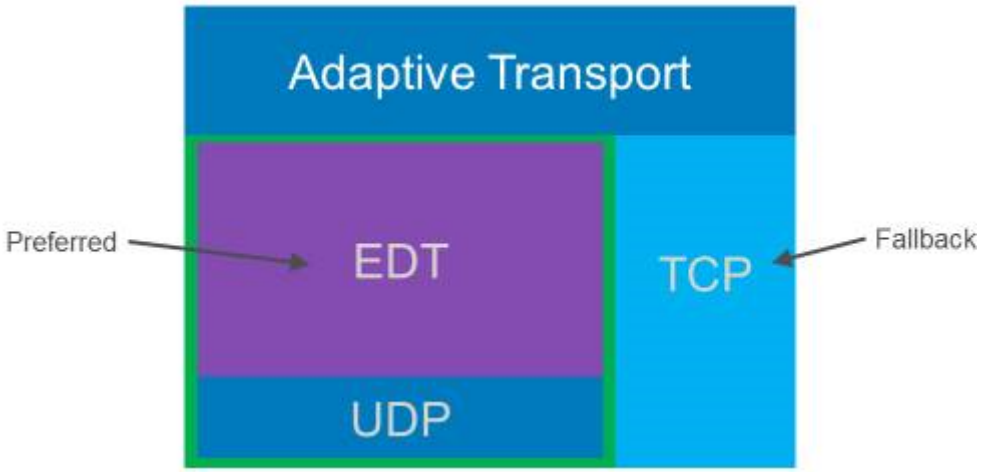



Quando Adaptive Transport (Trasporto adattivo) è impostato su **Preferred** (Preferito), EDT viene utilizzato come protocollo di trasporto principale e TCP viene utilizzato per il fallback. Per impostazione predefinita, Adaptive Transport (Trasporto adattivo) è impostato su **Preferred** (Preferito). È possibile impostare Adaptive Transport (Trasporto adattivo) sulla **modalità Diagnostica** per scopi di test, il che consente solo EDT e disabilita il fallback su TCP.

Con l'app Citrix Workspace per Windows, Mac e iOS, si cerca di stabilire le connessioni EDT e TCP in parallelo durante la connessione iniziale, la riconnessione dell'affidabilità della sessione e la riconnessione automatica del client. In questo modo si riduce il tempo di connessione se il trasporto UDP sottostante non è disponibile e deve essere utilizzato TCP. Se Adaptive Transport (Trasporto adattivo) è impostato su **Preferred** (Preferito) e la connessione viene stabilita tramite TCP, Adaptive Transport (Trasporto adattivo) continua a tentare di passare a EDT ogni cinque minuti.

Con l'app Citrix Workspace per Linux e Android, vengono tentate prima le connessioni EDT. Se la connessione non ha esito positivo, l'app Citrix Workspace tenta di connettersi tramite TCP dopo il timeout della richiesta EDT.




### Requisiti di sistema

Di seguito sono riportati i requisiti per l'utilizzo di Adaptive Transport (Trasporto adattivo) e EDT:

- Piano di controllo
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 1912 o versioni successive
- Virtual Delivery Agent
  - Versione 1912 o successiva (consigliata 2203 o successiva)
  - La versione 2012 è il minimo richiesto per l'utilizzo di EDT con Citrix Gateway Service
- StoreFront (*si applica solo se utilizzato nella distribuzione*)
  - Versione 3.12.x
  - Versione 1912.0.x
- App Citrix Workspace
  - Windows: versione 2105 o successiva
  - Linux: versione 2109 o successiva
  - Mac: versione 2108 o successiva
  - iOS: ultima versione disponibile nell'Apple App Store
  - Android: ultima versione disponibile in Google Play
- Citrix Gateway (ADC)
  - 13.1.17.42 o successivo (consigliato)
  - 13.0.52.24 o versioni successive
  - 12.1.56.22 o versioni successive

- Firewall (dal punto di vista del VDA)
  - UDP 1494 in entrata, se l'affidabilità della sessione è disabilitata
  - UDP 2598 in entrata, se l'affidabilità della sessione è abilitata
  - UDP 443 in entrata, se l'SSL del VDA è abilitato per la crittografia ICA (DTLS)
  - UDP 443 in uscita, se si utilizza il servizio Citrix Gateway. Per ulteriori informazioni, consultare la documentazione del servizio Citrix Gateway.

### Considerazioni

- Abilitare l'affidabilità della sessione per utilizzare EDT MTU Discovery (Rilevamento MTU EDT) e utilizzare EDT con Citrix Gateway e il servizio Citrix Gateway.
- Assicurarsi che l'MTU EDT sia adeguatamente impostata per evitare la frammentazione. In caso contrario, le prestazioni potrebbero peggiorare o le sessioni potrebbero non essere avviate in alcune situazioni. Per ulteriori informazioni, vedere la sezione EDT MTU Discovery.
- Per informazioni dettagliate su requisiti e considerazioni sull'utilizzo di EDT con il servizio Citrix Gateway, vedere HDX Adaptive Transport con supporto EDT per il servizio Citrix Gateway.
- Per informazioni dettagliate sulla configurazione di Citrix Gateway per supportare EDT, vedere Configurare Citrix Gateway per supportare Enlightened Data Transport e HDX Insight.
- Al momento IPv6 non è supportato.

### Configurazione

Adaptive Transport (Trasporto adattivo) è abilitato per impostazione predefinita. È possibile configurare le seguenti opzioni utilizzando l'impostazione **HDX Adaptive Transport** (Trasporto adattivo HDX) nel criterio Citrix.

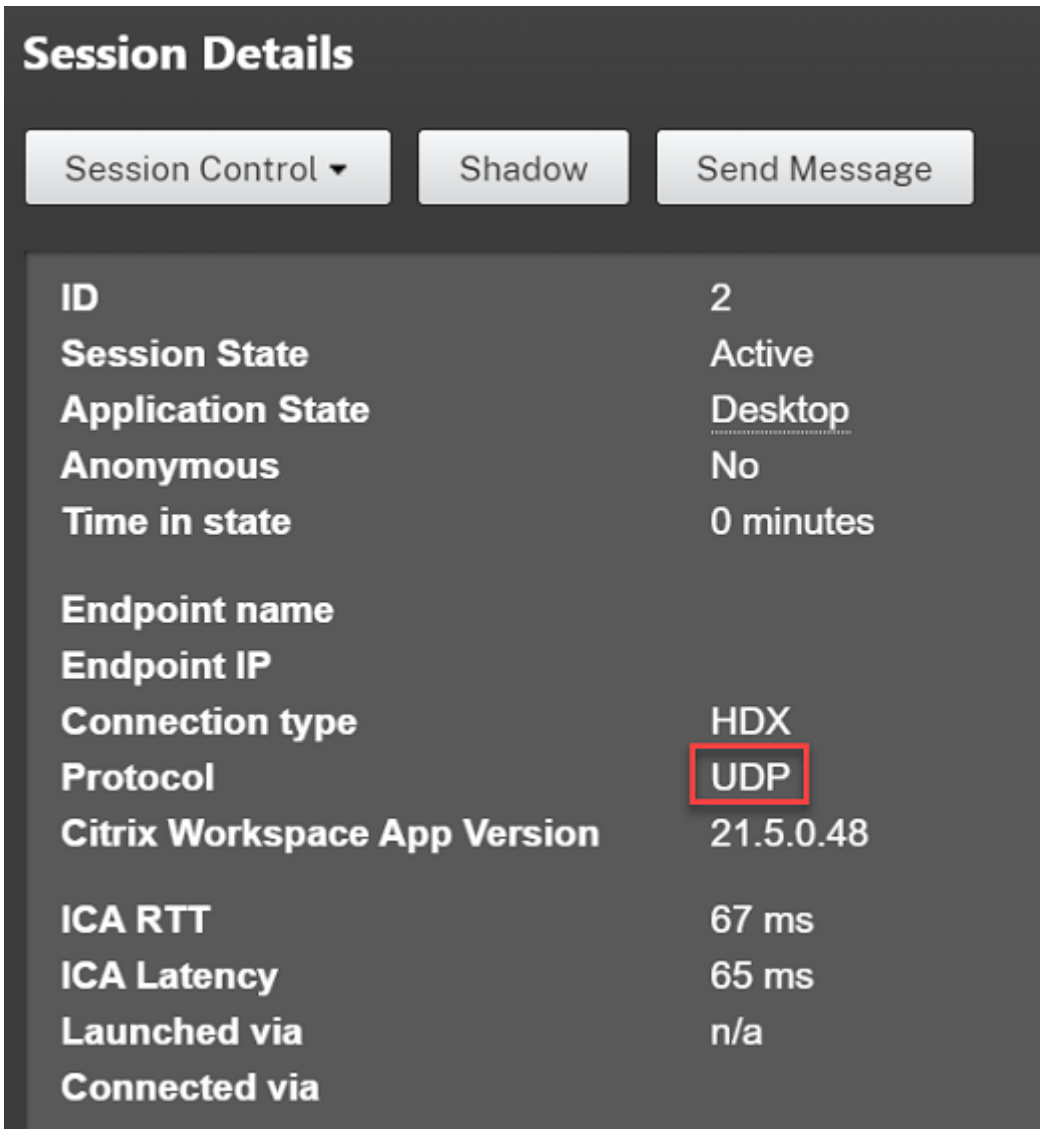
- **Preferred** (Preferito). Questa è l'impostazione predefinita. Adaptive Transport (Trasporto adattivo) è abilitato e utilizza EDT come protocollo di trasporto preferito, con fallback su TCP.
- **Diagnostic mode** (Modalità diagnostica). Adaptive Transport (Trasporto adattivo) è abilitato e forza l'uso di EDT. Il fallback su TCP è disabilitato. Questa impostazione è consigliata solo per il testing e la risoluzione dei problemi.
- **Off**. Adaptive Transport (Trasporto adattivo) è disabilitato e per il trasporto viene utilizzato solo TCP.

Per confermare che EDT viene utilizzato come protocollo di trasporto per la sessione, è possibile utilizzare Director o l'utilità della riga di comando CtxSession.exe sul VDA.

In Director, cercare la sessione e selezionare **Details** (Dettagli). Se **Connection type** (Tipo di connessione) è impostato su **HDX** e **Protocol** (Protocollo) su **UDP**, viene utilizzato EDT come protocollo di trasporto per la sessione. Se **Connection type** (Tipo di connessione) è impostato su **RDP**, ICA non è

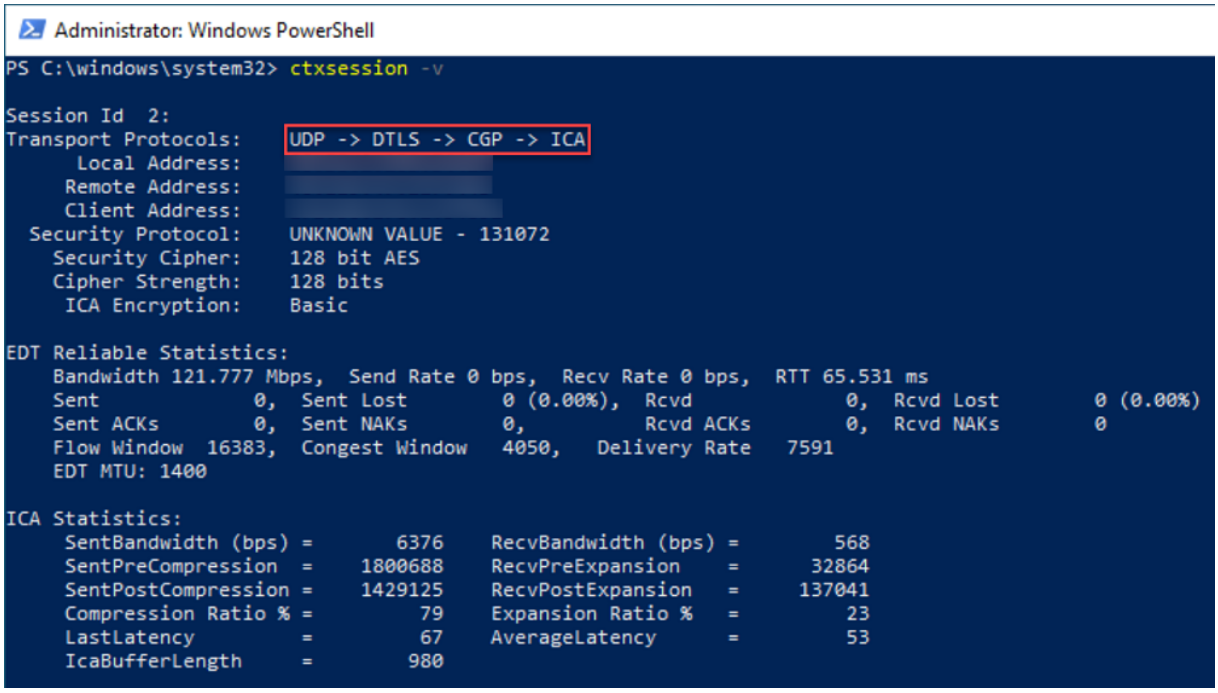
in uso e il campo **Protocol** (Protocollo) visualizza N/A. Per ulteriori informazioni, vedere Monitorare le sessioni.




Per utilizzare l'utilità CtxSession.exe, avviare un prompt dei comandi o PowerShell all'interno della sessione ed eseguire `ctxsession.exe`. Per visualizzare statistiche dettagliate, eseguire `ctxsession.exe -v`. Se EDT è in uso, il protocollo di trasporto mostra uno dei valori seguenti:

- **UDP > ICA** (affidabilità della sessione disabilitata)
- **UDP > CGP > ICA** (affidabilità della sessione abilitata)
- **UDP > DTLS > CGP > ICA** (a ICA è applicata la crittografia DTLS end-to-end)




### EDT MTU Discovery (Rilevamento MTU EDT)

MTU Discovery (Rilevamento MTU) consente a EDT di determinare automaticamente l'unità di trasmissione massima (MTU) quando si stabilisce una sessione. In questo modo si evita la frammentazione dei pacchetti EDT che potrebbe comportare un deterioramento delle prestazioni o l'impossibilità di stabilire una sessione.

> **Importante:**
>
> - L'affidabilità della sessione deve essere abilitata per consentire a MTU Discovery di funzionare.
> - MTU Discovery con Multi-Stream ICA è disponibile con VDA versione 2209 e successive.

#### Per controllare EDT MTU Discovery (Rilevamento MTU EDT) sul VDA

MTU Discovery (Rilevamento MTU) è abilitato per impostazione predefinita. Per disabilitare questa funzionalità, eliminare il valore del Registro di sistema **EDT MTU Discovery** (Rilevamento MTU EDT) e riavviare il VDA. Per ulteriori informazioni, vedere l'impostazione EDT MTU Discovery (Rilevamento MTU EDT) nell'elenco delle funzionalità HDX gestite tramite il Registro di sistema.

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi de-

> rivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

### Loss tolerant mode (Modalità tollerante alle perdite)

La modalità di tolleranza alle perdite utilizza il protocollo di trasporto EDT Lossy per migliorare l'esperienza utente per gli utenti che si connettono attraverso reti con latenza e perdita di pacchetti elevate.

Inizialmente, le sessioni vengono stabilite utilizzando EDT. Se le soglie della latenza e della perdita di pacchetti vengono raggiunte o superate, i canali virtuali applicabili passano da EDT a EDT Lossy, lasciando gli altri canali virtuali su EDT. Se la latenza e la perdita di pacchetti scendono al di sotto delle soglie, i canali virtuali applicabili tornano a EDT.

Le soglie predefinite sono:

- Perdita pacchetto: 5%
- Latenza: 300 ms (RTT)

La modalità di tolleranza alle perdite è abilitata per impostazione predefinita. È possibile disabilitare la funzionalità o regolare le soglie di latenza e di perdita di pacchetti utilizzando le impostazioni Loss tolerant mode (Modalità tollerante alle perdite) e Loss tolerant thresholds (Soglie tolleranti alle perdite).

> **Importante:**
>
> - Affinché la modalità tollerante alle perdite funzioni, è necessario abilitare l'affidabilità della sessione.
> - La modalità di tolleranza alle perdite è disponibile solo con l'app Citrix Workspace per Windows.
> - La modalità tollerante alle perdite non è supportata su Citrix Gateway o Citrix Gateway Service. Questa modalità è disponibile solo con le connessioni dirette.

### Problemi noti

Adaptive Transport (Trasporto adattivo) ed EDT presentano i seguenti problemi:

- La frammentazione dei pacchetti può causare un peggioramento delle prestazioni o addirittura il mancato avvio delle sessioni. È possibile regolare l'MTU EDT per evitare che questo si verifichi. Utilizzare MTU Discovery (Rilevamento MTU) o la soluzione alternativa descritta in CTX231821.

- È possibile che venga visualizzata una schermata grigia o nera quando si avvia una sessione da un client Windows se MTU Discovery (Rilevamento MTU) è abilitato. Per risolvere questo problema, eseguire l'aggiornamento all'app Workspace per Windows 2105 o versioni successive o all'app Workspace per Windows 1912 CU4 o versioni successive.
- Il fallback su TCP potrebbe non riuscire sui client Linux e Android durante la connessione tramite Citrix Gateway o il servizio Citrix Gateway. Questo si verifica quando è presente una negoziazione EDT corretta tra il client e il gateway e la negoziazione EDT non riesce tra il gateway e il VDA. Per risolvere questo problema, eseguire l'aggiornamento all'app Workspace per Linux 2104 o versioni successive e all'app Workspace per Android 21.5 o versioni successive.
- I percorsi di rete asimmetrici possono causare la mancata riuscita di MTU Discovery (Rilevamento MTU) per le connessioni che non passano tramite Citrix Gateway o il servizio Citrix Gateway. Per risolvere questo problema, eseguire l'aggiornamento a VDA versione 2103 o successiva. [CVADHELP-16654]
- Quando si utilizza Citrix Gateway o il servizio Citrix Gateway, i percorsi di rete asimmetrici possono impedire il funzionamento di MTU Discovery (Rilevamento MTU). Ciò è dovuto a un problema di Gateway che causa la mancata propagazione del bit Don't Fragment (DF) (Non frammentare) nell'intestazione dei pacchetti EDT. Una soluzione per questo problema non è ancora disponibile. [CGOP-18438]
- MTU Discovery (Rilevamento MTU) potrebbe non funzionare per gli utenti che si connettono tramite una rete DS-Lite. Alcuni modem non rispettano il bit DF quando l'elaborazione dei pacchetti è abilitata, impedendo a MTU Discovery (Rilevamento MTU) di rilevare la frammentazione. In questa situazione, queste sono le opzioni disponibili:
  - Disabilitare l'elaborazione dei pacchetti sul modem dell'utente.
  - Disabilitare MTU Discovery (Rilevamento MTU) e utilizzare una MTU hardcoded, come descritto in CTX231821.
  - Disabilitare Adaptive Transport (Trasporto adattivo) per obbligare le sessioni a utilizzare TCP. Se solo un sottoinsieme di utenti è interessato, prendere in considerazione la possibilità di disabilitarlo sul lato client in modo che altri utenti possano continuare a utilizzare EDT.

### Risoluzione dei problemi

Per risolvere i problemi relativi ad Adaptive Transport (Trasporto adattivo) ed EDT, suggeriamo quanto segue:

1. Esaminare attentamente e convalidare i requisiti, le considerazionie i problemi noti.
2. Verificare che siano presenti criteri Citrix in Studio o nell'oggetto Criteri di gruppo che sovrascrivono l'impostazione **HDX Adaptive Transport** (Trasporto adattivo HDX) desiderata.

3. Verificare se sul client sono presenti impostazioni che sovrascrivono l'impostazione HDX Adaptive Transport (Trasporto adattivo HDX) desiderata. Può trattarsi di una preferenza dell'oggetto Criteri di gruppo, di un'impostazione configurata utilizzando il modello amministrativo dell'app Workspace opzionale o di una configurazione manuale dell'impostazione **HDXoverUDP** nel Registro di sistema o nel file di configurazione del client.
4. Sui computer VDA multisessione, assicurarsi che i listener UDP siano attivi. Aprire un prompt dei comandi sulla macchina del VDA ed eseguire `netstat -a -p udp`. Per ulteriori informazioni, vedere Come confermare il protocollo HDX Enlightened Data Transport.
5. Avviare una sessione diretta internamente, bypassando Citrix Gateway, e controllare il protocollo in uso. Se la sessione utilizza EDT, il VDA è pronto per utilizzare EDT per le connessioni esterne tramite Citrix Gateway.
6. Se EDT funziona per le connessioni interne dirette e non per le sessioni che passano attraverso Citrix Gateway:
   - Assicurarsi che l'affidabilità della sessione sia abilitata
   - Assicurarsi che su Gateway sia abilitato DTLS
7. Verificare se sono state configurate le regole firewall appropriate sia nei firewall di rete che nei firewall in esecuzione sulle macchine con i VDA.
8. Verificare se le connessioni degli utenti richiedono una MTU non standard. Le connessioni con una MTU effettiva inferiore a 1500 byte causano la frammentazione dei pacchetti EDT, che a sua volta può influire sulle prestazioni o addirittura causare errori di avvio della sessione. Questo problema è comune quando si utilizzano VPN, alcuni punti di accesso Wi-Fi e reti mobili, come 4G e 5G. Per informazioni su come risolvere questo problema, vedere la sezione Rilevamento MTU.

### Interoperabilità con Citrix SD-WAN

L'ottimizzazione WAN Citrix SD-WAN (WANOP) offre la compressione tokenizzata tra le sessioni (deduplicazione dei dati), inclusa la cache video basata su URL, offrendo una notevole riduzione della larghezza di banda. La riduzione si verifica se due o più persone nella sede dell'ufficio guardano lo stesso video recuperato dal client oppure trasferiscono o stampano parti significative dello stesso file o documento. Inoltre, eseguendo i processi per la riduzione dei dati ICA e la compressione dei processi di stampa sull'appliance della filiale, WANOP offre l'offload della CPU del server VDA e consente una maggiore scalabilità del server di Citrix Virtual Apps and Desktops.

Attualmente, SD-WAN WANOP non supporta EDT. Tuttavia, non è necessario disabilitare Adaptive Transport (Trasporto adatttivo) se SD-WAN WANOP è in uso. Quando un utente avvia una sessione che passa attraverso una SD-WAN con WANOP abilitato, imposta automaticamente la sessione in modo

che utilizzi TCP come protocollo di trasporto. Le sessioni non WANOP continuano a utilizzare EDT quando possibile.

## Rendezvous protocol (Protocollo Rendezvous)

June 8, 2023

Quando si utilizza Citrix Gateway Service, il protocollo Rendezvous consente ai VDA di bypassare i Citrix Cloud Connector per connettersi direttamente e in modo sicuro con il piano di controllo Citrix Cloud.

Esistono due tipi di traffico da considerare:

1. Controlla il traffico per la registrazione del VDA e l'intermediazione di sessioni.
2. Traffico di sessione HDX.

Sono disponibili due versioni di Rendezvous:

- Versione 1 (V1): supporta l'esclusione dei Citrix Cloud Connector solo per il traffico di sessione HDX.
- Versione 2 (V2): supporta l'esclusione dei Citrix Cloud Connector sia per il traffico di controllo che per il traffico di sessione HDX.

Per informazioni dettagliate sui requisiti di sistema, le considerazioni e la configurazione relativi a ciascuna delle versioni di Rendezvous, consultare la relativa documentazione.

Documentazione di Rendezvous V1

Documentazione di Rendezvous V2

## Rendezvous V1

May 9, 2023

Quando si utilizza Citrix Gateway Service, il protocollo Rendezvous consente ai VDA di bypassare i Citrix Cloud Connector per connettersi direttamente e in modo sicuro con il piano di controllo Citrix Cloud.

### Requisiti

- Accesso all'ambiente utilizzando il servizio Citrix Workspace e Citrix Gateway.

- Piano di controllo: Citrix DaaS (Citrix Cloud).
- VDA: versione 1912 o successiva.
  - La versione 2012 è il minimo richiesto per EDT Rendezvous.
  - La versione 2012 è il minimo richiesto per il supporto proxy non trasparente (nessun supporto per i file PAC).
  - La versione 2103 è il minimo richiesto per la configurazione del proxy con un file PAC.
- Abilitare il protocollo Rendezvous nella politica Citrix. Per ulteriori informazioni, vedere Rendezvous protocol policy setting.
- I VDA devono avere accesso a `https://*.nssvc.net`, compresi tutti i sottodomini. Se non è possibile aggiungere tutti i sottodomini all'elenco consentiti in questo modo, utilizzare invece `https://*.c.nssvc.net` e `https://*.g.nssvc.net`. Per ulteriori informazioni, vedere la sezione Internet Connectivity Requirements della documentazione di Citrix Cloud (all'interno di Citrix DaaS) e l'articolo del Knowledge Center CTX270584.
- I VDA devono essere in grado di connettersi agli indirizzi menzionati in precedenza su TCP 443 e UDP 443 rispettivamente per TCP Rendezvous ed EDT Rendezvous.
- I Cloud Connector devono ottenere i nomi di dominio completi dei VDA durante l'intermediazione di una sessione. Eseguire questa attività in uno di questi due modi:
  - **Abilitare la risoluzione DNS per il sito.** Accedere a **Full Configuration > Settings** (Configurazione completa > Impostazioni) e attivare l'impostazione **Enable DNS resolution** (Abilita risoluzione DNS). In alternativa, utilizzare Remote PowerShell SDK di Citrix Virtual Apps and Desktops ed eseguire il comando `Set-BrokerSite -DnsResolutionEnabled $true`. Per ulteriori informazioni su Remote PowerShell SDK di Citrix Virtual Apps and Desktops, vedere SDK e API.
  - **Zona di ricerca inversa DNS con record PTR per i VDA.** Se si sceglie questa opzione, consigliamo di configurare i VDA perché tentino sempre di registrare i record PTR. A tale scopo, utilizzare l'editor Criteri di gruppo o l'oggetto Criteri di gruppo, accedere a **Computer Configuration > Administrative Templates > Network > DNS Client** (Configurazione computer > Modelli amministrativi > Rete > Client DNS) e impostare **Register PTR Records** (Registra record PTR) su **Enabled and Register**. Se il suffisso DNS della connessione non corrisponde al suffisso DNS del dominio, è necessario configurare anche l'impostazione **Connection-specific DNS suffix** (Suffisso DNS specifico della connessione) affinché i computer registrino correttamente i record PTR.

> **Nota:**
>
> Se si utilizza l'opzione di risoluzione DNS, i Cloud Connector devono essere in grado di risolvere i nomi di dominio completi (FQDN) delle macchine VDA. Nel caso in cui gli utenti

> interni si connettano direttamente alle macchine VDA, anche i dispositivi client devono essere in grado di risolvere gli FQDN delle macchine VDA.
>
> Se si utilizza una zona di ricerca inversa DNS, gli FQDN inclusi nei record PTR devono corrispondere agli FQDN delle macchine VDA. Se il record PTR contiene un nome di dominio completo diverso, la connessione Rendezvous non riesce. Ad esempio, se il nome di dominio completo della macchina è `vda01.domain.net`, il record PTR deve contenere `vda01.domain.net`. Un nome di dominio completo diverso, ad esempio, `vda01.sub.domain.net` non funziona.

## Configurazione proxy

Il VDA supporta la creazione di connessioni Rendezvous tramite un proxy.

### Considerazioni sui proxy

Quando si utilizzano proxy con Rendezvous, considerare quanto segue:

- Sono supportati proxy trasparenti, proxy HTTP non trasparenti e proxy SOCKS5.
- La decrittografia e l'ispezione dei pacchetti non sono supportate. Configurare un'eccezione in modo che il traffico ICA tra il VDA e il servizio gateway non venga intercettato, decrittografato o ispezionato. Altrimenti la connessione si interrompe.
- I proxy HTTP supportano l'autenticazione basata su computer utilizzando i protocolli di autenticazione Negotiate e Kerberos o NT LAN Manager (NTLM).

  Quando ci si connette al server proxy, lo schema di autenticazione Negotiate seleziona automaticamente il protocollo Kerberos. Se Kerberos non è supportato, Negotiate effettua il fallback su NTLM per l'autenticazione.

  > **Nota:**
  >
  > Per utilizzare Kerberos, è necessario creare il nome dell'entità servizio (SPN) per il server proxy e associarlo all'account Active Directory del proxy. Il VDA genera l'SPN nel formato `HTTP/<proxyURL>` quando si stabilisce una sessione, in cui l'URL proxy viene recuperato dall'impostazione dei criteri **Rendezvous proxy**. Se non si crea un SPN, l'autenticazione effettua il fallback su NTLM. In entrambi i casi, l'identità della macchina VDA viene utilizzata per l'autenticazione.

- L'autenticazione con un proxy SOCKS5 non è attualmente supportata. Se si utilizza un proxy SOCKS5, è necessario configurare un'eccezione in modo che il traffico destinato agli indirizzi del servizio gateway (specificati nei requisiti) possa ignorare l'autenticazione.

- Solo i proxy SOCKS5 supportano il trasporto dei dati tramite EDT. Per un proxy HTTP, utilizzare TCP come protocollo di trasporto per ICA.

#### Proxy trasparente

Se si utilizza un proxy trasparente nella rete, non è richiesta alcuna configurazione aggiuntiva sul VDA.

#### Proxy non trasparente

Se si utilizza un proxy non trasparente nella rete, configurare l'impostazione di Rendezvous proxy configuration (Configurazione del proxy Rendezvous). Quando l'impostazione è abilitata, specificare l'indirizzo proxy HTTP o SOCKS5 oppure immettere il percorso del file PAC in modo che il VDA sappia quale proxy utilizzare. Ad esempio:

- Indirizzo proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`
- File PAC: `http://<URL or IP>/<path>/<filename>.pac`

Se si utilizza il file PAC per configurare il proxy, definire il proxy utilizzando la sintassi richiesta dal servizio HTTP di Windows: `PROXY [<scheme>=]<URL or IP>:<port>`. Ad esempio, `PROXY socks5=<URL or IP>:<port>`.

### Convalida di Rendezvous

Se si soddisfano tutti i requisiti, seguire questi passaggi per effettuare la convalida se Rendezvous è in uso:

1. Avviare PowerShell o un prompt dei comandi all'interno della sessione HDX.
2. Eseguire `ctxsession.exe –v`.
3. I protocolli di trasporto in uso indicano il tipo di connessione:
    - TCP Rendezvous: **TCP > SSL > CGP > ICA**
    - EDT Rendezvous: **UDP > DTLS > CGP > ICA**
    - Proxy tramite Cloud Connector: **TCP > CGP > ICA**

### Altre considerazioni

#### Ordine delle suite di cifratura Windows

Per un ordine delle suite di cifratura personalizzato, assicurarsi di includere le suite di cifratura supportate dal VDA incluse nel seguente elenco:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Se l'ordine della suite di cifratura personalizzato non contiene queste suite di cifratura, la connessione Rendezvous non riesce.

#### Zscaler Private Access

Se si utilizza Zscaler Private Access (ZPA), si consiglia di configurare le impostazioni di bypass per il servizio gateway per evitare una maggiore latenza e l'impatto sulle prestazioni associato. A tale scopo, è necessario definire i segmenti di applicazione per gli indirizzi del servizio gateway specificati nei requisiti e impostarli in modo che vengano sempre ignorati. Per informazioni sulla configurazione dei segmenti di applicazione per ignorare ZPA, vedere la documentazione di Zscaler.

## Rendezvous V2

November 21, 2023

Quando si utilizza Citrix Gateway Service, il protocollo Rendezvous consente ai VDA di bypassare i Citrix Cloud Connector per connettersi direttamente e in modo sicuro con il piano di controllo Citrix Cloud.

Rendezvous V2 è supportato con macchine aggiunte a domini standard, macchine unite ad Azure AD e macchine non aggiunte a domini.

> **Nota:**
>
> Al momento, le distribuzioni senza connettore sono possibili solo con macchine *aggiunte ad Azure AD* e *non aggiunte a un dominio*. Le macchine aggiunte a domini AD standard richiedono ancora i Cloud Connector per la registrazione VDA e l'intermediazione delle sessioni. Tuttavia, non ci sono requisiti DNS per l'utilizzo di Rendezvous V2.
>
> I requisiti di Cloud Connector per altre funzioni non correlate alla comunicazione VDA, come la connessione al dominio AD on-premise, il provisioning MCS agli hypervisor on-premise ecc. rimangono invariati.

### Requisiti

I requisiti per l'utilizzo di Rendezvous V2 sono:

- Accesso all'ambiente utilizzando il servizio Citrix Workspace e Citrix Gateway
- Piano di controllo: Citrix DaaS
- VDA versione 2203
- Abilitare il protocollo Rendezvous nella politica Citrix. Per ulteriori informazioni, vedere Rendezvous protocol policy setting.
- L'affidabilità della sessione deve essere abilitata sui VDA
- Le macchine VDA devono avere accesso a:
  - `https://*.xendesktop.net` in `TCP 443`. Se non si possono consentire tutti i sottodomini in questo modo, è possibile utilizzare `https://<customer_ID>.xendesktop.net`, dove <customer_ID> è il proprio ID cliente Citrix Cloud, come mostrato nel portale degli amministratori di Citrix Cloud.
  - `https://*.*.nssvc.net` in `TCP 443` per la connessione di controllo con Gateway Service.
  - `https://*.*.nssvc.net` in `TCP 443` e `UDP 443` per le sessioni HDX su TCP ed EDT, rispettivamente.

> **Nota:**
>
> Se non si può consentire l'utilizzo di tutti i sottodomini usando `https://*.*.nssvc.net`, è possibile usare invece `https://*.c.nssvc.net` e `https://*.g.nssvc.net`. Per ulteriori informazioni, vedere l'articolo CTX270584 del Knowledge Center.

## Configurazione proxy

Il VDA supporta la connessione tramite proxy sia per il traffico di controllo che per il traffico di sessione HDX quando si utilizza Rendezvous. I requisiti e gli aspetti da considerare per entrambi i tipi di traffico sono diversi, quindi è necessario esaminarli attentamente.

### Considerazioni sul proxy del traffico

- Sono supportati solo i proxy HTTP.
- La decrittografia e l'ispezione dei pacchetti non sono supportate. Configurare un'eccezione in modo che il traffico di controllo tra VDA e il piano di controllo di Citrix Cloud non venga intercettato, decrittografato o ispezionato. In caso contrario, la connessione non riesce.
- L'autenticazione proxy non è supportata.

#### Considerazioni sul proxy del traffico HDX

- I proxy HTTP e SOCKS5 sono supportati.
- L'EDT può essere utilizzato solo con i proxy SOCKS5.
- Per impostazione predefinita, il traffico HDX utilizza il proxy definito per il traffico di controllo. Se è necessario utilizzare un proxy diverso per il traffico HDX, sia esso un proxy HTTP diverso o un proxy SOCKS5, utilizzare l'impostazione dei criteri Rendezvous proxy configuration (configurazione del proxy Rendezvous).
- La decrittografia e l'ispezione dei pacchetti non sono supportate. Configurare un'eccezione in modo che il traffico HDX tra VDA e il piano di controllo di Citrix Cloud non venga intercettato, decrittografato o ispezionato. In caso contrario, la connessione non riesce.
- L'autenticazione basata su computer è supportata solo con i proxy HTTP e solo se la macchina VDA è aggiunta al dominio AD. Può utilizzare l'autenticazione Negotiate/Kerberos o NTLM.

  > **Nota:**
  >
  > Per utilizzare Kerberos, creare il nome dell'entità servizio (SPN) per il server proxy e associarlo all'account Active Directory del proxy. Il VDA genera l'SPN nel formato HTTP/<proxyURL> quando si stabilisce una sessione, in cui l'URL proxy viene recuperato dall'impostazione dei criteri Rendezvous proxy configuration. Se non si crea un SPN, l'autenticazione effettua il fallback su NTLM. In entrambi i casi, l'identità della macchina VDA viene utilizzata per l'autenticazione.

- L'autenticazione con un proxy SOCKS5 non è attualmente supportata. Se si utilizza un proxy SOCKS5, configurare un'eccezione in modo che il traffico destinato agli indirizzi del servizio gateway (specificati nei requisiti) possa ignorare l'autenticazione.
- Solo i proxy SOCKS5 supportano il trasporto dei dati tramite EDT. Per un proxy HTTP, utilizzare TCP come protocollo di trasporto per ICA.

#### Proxy trasparente

Se si utilizza un proxy trasparente nella rete, non è richiesta alcuna configurazione aggiuntiva sul VDA.

#### Proxy non trasparente

Se si utilizza un proxy non trasparente nella rete, specificare il proxy durante l'installazione di VDA in modo che il traffico di controllo possa raggiungere il piano di controllo di Citrix Cloud. Consigliamo di

leggere le considerazioni sul proxy del traffico di controllo prima di procedere all'installazione e alla configurazione.

Nell'installazione guidata VDA, selezionare **Rendezvous Proxy Configuration** nella pagina **Additional Components** (Componenti aggiuntivi). Questa opzione rende disponibile la pagina **Rendezvous Proxy Configuration** in una fase successiva dell'installazione guidata. Una volta qui, inserire l'indirizzo proxy o il percorso del file PAC per specificare quale proxy deve utilizzare il VDA. Ad esempio:

- Indirizzo proxy: `http://<URL or IP>:<port>`
- File PAC: `http://<URL or IP>/<path/<filename>.pac`

Come indicato nelle considerazioni sul proxy del traffico HDX, il traffico HDX utilizza il proxy definito durante l'installazione del VDA per impostazione predefinita. Se è necessario utilizzare un proxy diverso per il traffico HDX, sia esso un proxy HTTP diverso o un proxy SOCKS5, utilizzare l'impostazione dei criteri Rendezvous proxy configuration (configurazione del proxy Rendezvous). Quando l'impostazione è abilitata, specificare l'indirizzo proxy HTTP o SOCKS5. È inoltre possibile immettere il percorso del file PAC in modo da definire il proxy che dovrà essere utilizzato dal VDA. Ad esempio:

- Indirizzo proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`
- File PAC: `http://<URL or IP>/<path/<filename>.pac`

Se si utilizza il file PAC per configurare il proxy, definire il proxy utilizzando la sintassi richiesta dal servizio HTTP di Windows: `PROXY [<scheme>=]<URL or IP>:<port>`. Ad esempio, `PROXY socks5=<URL or IP>:<port>`.

### Come configurare Rendezvous

Di seguito sono riportati i passaggi per configurare Rendezvous nel proprio ambiente:

1. Assicurarsi che tutti i requisiti siano soddisfatti.
2. Se è necessario utilizzare un proxy HTTP non trasparente nel proprio ambiente, configurarlo durante l'installazione del VDA. Fare riferimento alla sezione relativa alla configurazione del proxy per i dettagli.
3. Dopo aver installato il VDA, aggiungere il seguente valore di registro:
   Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   Tipo di valore: DWORD
   Nome del valore: GctRegistration
   Dati del valore: 1
4. Riavviare la macchina del VDA.
5. Creare un criterio Citrix o modificarne uno esistente:
   - Impostare **Rendezvous Protocol** su **Allowed**.

- Se è necessario configurare un proxy HTTP o SOCKS5 per il traffico HDX, configurare l'impostazione **Rendezvous proxy configuration**.
- Assicuratevi che i filtri dei criteri Citrix siano impostati correttamente. Il criterio si applica alle macchine che necessitano di Rendezvous abilitato.

6. Assicurarsi che il criterio Citrix abbia la priorità corretta in modo che non ne sovrascriva un altro.

#### Convalida di Rendezvous

Se si soddisfano tutti i requisiti e si è completata la configurazione, seguire questi passaggi per verificare se Rendezvous è in uso:

1. All'interno del desktop virtuale, aprire un prompt dei comandi o PowerShell.
2. Eseguire `ctxsession.exe -v`.
3. I protocolli di trasporto visualizzati indicano il tipo di connessione:
   - TCP Rendezvous: TCP > SSL > CGP > ICA
   - EDT Rendezvous: UDP > DTLS > CGP > ICA
   - Non Rendezvous: TCP > CGP > ICA
4. La versione di Rendezvous riportata indica la versione in uso.

### Altre considerazioni

#### Ordine delle suite di cifratura Windows

Se l'ordine della suite di cifratura è stato modificato nelle macchine VDA, assicurarsi di includere le suite di cifratura supportate dal VDA:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Se l'ordine della suite di cifratura personalizzato non contiene queste suite di cifratura, la connessione Rendezvous non riesce.

#### Zscaler Private Access

Se si utilizza Zscaler Private Access (ZPA), si consiglia di configurare le impostazioni di bypass per il servizio gateway per evitare una maggiore latenza e l'impatto sulle prestazioni associato. A tale scopo, è necessario definire i segmenti di applicazione per gli indirizzi del servizio gateway specificati nei requisiti e impostarli in modo che vengano sempre ignorati. Per informazioni sulla configurazione dei segmenti di applicazione per ignorare ZPA, vedere la documentazione di Zscaler.

## Problemi noti

### Rendezvous V2 non funziona se Rendezvous V1 era precedentemente in uso

Se è stata abilitata l'impostazione della risoluzione DNS nel sito DaaS per utilizzare Rendezvous V1, le connessioni Rendezvous V2 non andranno a buon fine. Per utilizzare Rendezvous V2, è necessario disabilitare la risoluzione DNS nel sito DaaS utilizzando una delle seguenti opzioni:

- Accedere a **Full Configuration > Settings** (Configurazione completa > Impostazioni) e disattivare l'impostazione **Enable DNS resolution** (Abilita risoluzione DNS)
- Utilizzare l'SDK Remote PowerShell Citrix DaaS ed eseguire il comando `Set-BrokerSite -DnsResolutionEnabled $false`

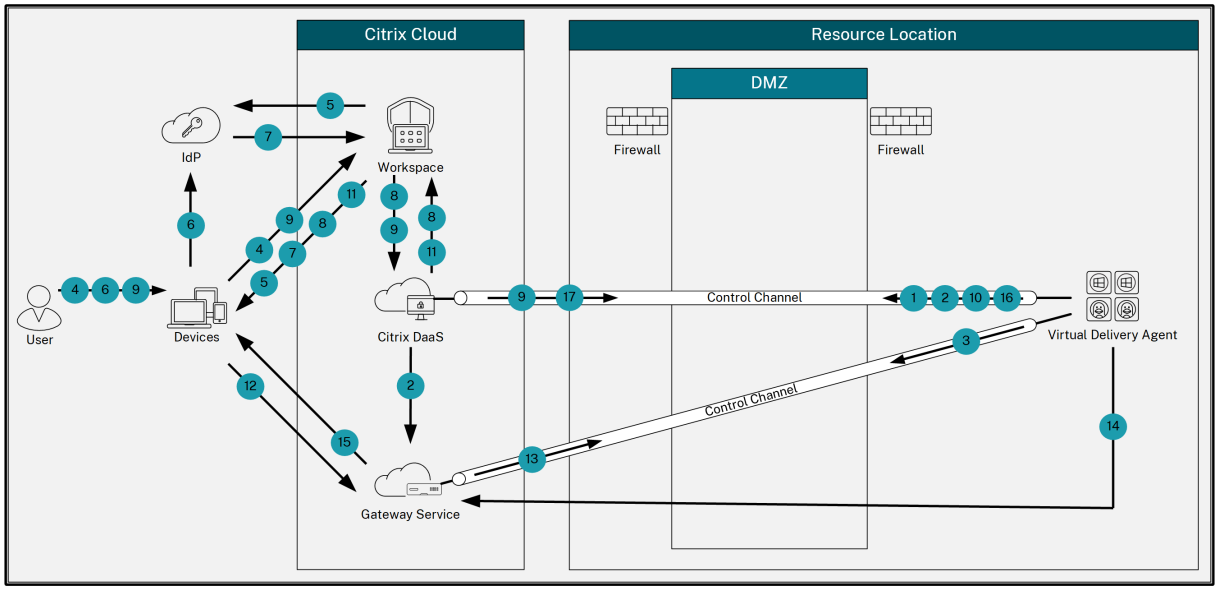
### Il programma di installazione del VDA 2203 non consente di inserire una barra (/) per l'indirizzo del proxy

Come soluzione alternativa, è possibile configurare il proxy nel registro a installazione avvenuta:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
Value type: String
Value name: ProxySettings
Value data: Proxy address or path to pac file. For example:
    Proxy address: http://squidk.test.local:3128
    Pac file: http://file.test.com/config/proxy.pac
```

## Flusso di traffico Rendezvous

Il diagramma seguente illustra la sequenza di passaggi relativi al flusso di traffico Rendezvous.



1. Il VDA stabilisce una connessione WebSocket con Citrix Cloud e si registra.
2. Il VDA si registra con Citrix Gateway Service e ottiene un token dedicato.
3. Il VDA stabilisce una connessione di controllo persistente con il Gateway Service.
4. L'utente accede a Citrix Workspace.
5. Workspace valuta la configurazione dell'autenticazione e reindirizza gli utenti all'IdP appropriato per l'autenticazione.
6. L'utente inserisce le proprie credenziali.
7. Dopo aver convalidato correttamente le credenziali utente, l'utente viene reindirizzato a Workspace.
8. Workspace conta le risorse per l'utente e le visualizza.
9. L'utente seleziona un desktop o un'applicazione da Workspace. Workspace invia la richiesta a Citrix DaaS, che esegue l'intermediazione della connessione e ordina al VDA di prepararsi per la sessione.
10. Il VDA risponde con la funzionalità Rendezvous e la relativa identità.
11. Citrix DaaS genera un ticket di avvio e lo invia al dispositivo utente tramite Workspace.
12. L'endpoint dell'utente si connette a Gateway Service e fornisce il ticket di avvio per autenticare e identificare la risorsa a cui connettersi.
13. Gateway Service invia le informazioni di connessione al VDA.
14. Il VDA stabilisce una connessione diretta per la sessione con il Gateway Service.
15. Il Gateway Service completa la connessione tra l'endpoint e il VDA.
16. Il VDA verifica le licenze per la sessione.
17. Citrix DaaS invia le policy applicabili al VDA.

## HDX Direct (anteprima tecnica)

May 11, 2023

Quando si accede alle risorse fornite da Citrix, HDX Direct consente ai dispositivi client di stabilire una connessione diretta sicura con il VDA se esiste una linea di vista diretta.

> **Importante:**
>
> HDX Direct è attualmente disponibile in anteprima tecnica. Per inviare commenti o segnalare problemi, utilizzare questo modulo.

### Requisiti

Di seguito sono riportati i requisiti per l'uso di HDX Direct:

- Piano di controllo

  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2303 o versioni successive
- Virtual Delivery Agent (VDA)
  - Windows: versione 2303 o successiva
- App Workspace
  - Windows: versione 2303 o successiva
- Livello di accesso
  - Citrix Workspace
  - Citrix Gateway Service
  - NetScaler Gateway
- Firewall
  - Macchina VDA
    - TCP 443 in entrata (ICA su TCP)
    - UDP 443 in entrata (ICA su EDT)
  - Rete

| Protocollo | Porta | Origine | Destinazione |
|---|---|---|---|
| TCP | 443 | Client | VDA |
| UDP | 443 | Client | VDA |

## Configurazione

HDX Direct è disabilitato per impostazione predefinita. È possibile configurare questa funzionalità utilizzando l'impostazione HDX Direct nei criteri Citrix.

- **Allowed** (Consentito): HDX Direct è abilitato e tenta di stabilire una connessione diretta all'host della sessione quando è connessa una sessione.
- **Prohibited** (Vietato): impostazione predefinita. HDX Direct è disabilitato e impedisce al client di tentare di connettersi direttamente all'host della sessione quando è connesso tramite un gateway.

Per confermare che HDX Direct ha stabilito correttamente una connessione diretta, utilizzare l'utilità CtxSession.exe sulla macchina VDA.

Per utilizzare l'utilità CtxSession.exe, avviare un prompt dei comandi o PowerShell all'interno della sessione ed eseguire ctxsession.exe -v. Se è stata correttamente stabilita una connessione HDX Direct, verrà visualizzato quanto segue:

- Protocollo di trasporto
  - UDP > DTLS > CGP > ICA (se si utilizza EDT)
  - TCP > SSL > CGP > ICA (se si utilizza TCP)
- L'indirizzo remoto e l'indirizzo del client sono gli stessi

## Considerazioni

Di seguito sono riportate considerazioni sull'utilizzo di HDX Direct:

- Quando si utilizzano macchine non persistenti per app e desktop virtuali, non abilitare HDX Direct nell'immagine master/modello per evitare di generare certificati per la macchina virtuale (VM) master.

## Come funziona

HDX Direct consente ai client di stabilire una connessione diretta con l'host della sessione quando è disponibile una comunicazione diretta. Quando le connessioni dirette vengono effettuate utilizzando HDX Direct, viene utilizzata la crittografia a livello di rete (TLS/DTLS) per proteggerle, sfruttando certificati autofirmati.

Esistono tre fasi che coprono diverse parti della funzionalità: pre-avvio, avvio e post-avvio.

### Fase di pre-avvio

Questa è la fase iniziale, che riguarda la creazione e la gestione dei certificati. Queste attività sono gestite dai seguenti servizi sulla macchina VDA, entrambi impostati per essere eseguiti automaticamente all'avvio della macchina:

- Servizio Citrix ClxMtp: responsabile della generazione e della rotazione dei certificati CA.
- Citrix Certificate Manager Service: responsabile della generazione e della gestione del certificato CA root autofirmato, delle chiavi dei certificati della macchina e dei certificati della macchina.

Di seguito è riportata una panoramica del processo di gestione dei certificati:

1. I servizi vengono avviati all'avvio della macchina.
2. Il servizio Citrix ClxMtp crea le chiavi se non ne è già stata creata alcuna.

3. Il servizio Citrix Certificate Manager verifica se HDX Direct è abilitato. In caso contrario, il servizio si interrompe da solo.
4. Se HDX Direct è abilitato, Citrix Certificate Manager Service verifica se esiste un certificato CA root autofirmato. In caso contrario, viene creato un certificato root autofirmato.
5. Una volta disponibile un certificato CA root, il servizio Citrix Certificate Manager verifica se esiste un certificato macchina autofirmato. In caso contrario, il servizio genera le chiavi e crea un nuovo certificato utilizzando il nome di dominio completo della macchina.
6. Se esiste un certificato della macchina creato dal servizio Citrix Certificate Manager e il nome dell'oggetto non corrisponde al FQDN della macchina, viene generato un nuovo certificato.

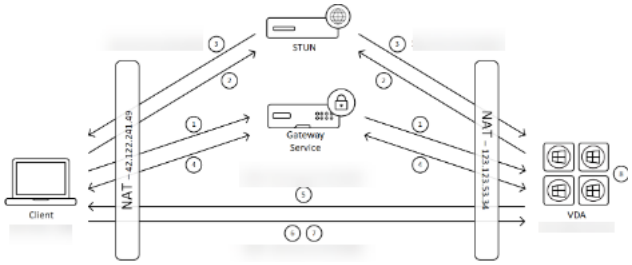
> **Nota:**
>
> Il servizio Citrix Certificate Manager genera certificati RSA che sfruttano chiavi a 2048 bit.

### Fase di avvio

Per riuscire a stabilire una connessione HDX Direct sicura, il client deve considerare attendibili i certificati utilizzati per proteggere la sessione. Per ottenere questo risultato, il VDA invia al Broker le informazioni sul certificato durante l'intermediazione di una sessione. Successivamente, il Broker invia queste informazioni a Workspace per includerle nel file ICA inviato al client per avviare la sessione.

### Fase post-avvio

Una volta che una sessione è stata mediata con successo, la sessione viene avviata. Di seguito è riportata una panoramica del processo di connessione di HDX Direct:




1. Il client stabilisce una connessione con il VDA tramite il servizio Gateway.
2. Dopo una connessione riuscita, il VDA invia al client il nome di dominio completo della macchina VDA e un elenco dei relativi indirizzi IP.
3. Il client analizza gli indirizzi IP per verificare se può raggiungere direttamente il VDA.
4. Se è in grado di raggiungere il VDA direttamente con uno qualsiasi degli indirizzi IP condivisi, il client stabilisce una connessione diretta sicura con il VDA.
5. Una volta stabilita correttamente la connessione diretta, la sessione viene trasferita alla nuova connessione e la connessione al servizio gateway termina.

### Problemi noti

Di seguito sono riportati i problemi noti relativi a HDX Direct:

- La connessione HDX Direct potrebbe non riuscire quando Rendezvous è disabilitato.
- La connessione HDX Direct potrebbe non riuscire quando si avviano sessioni da un sito Citrix Virtual Apps and Desktops 2303 locale.
- L'app Workspace potrebbe bloccarsi se il VDA è in esecuzione su Windows 11.

## Dispositivi

August 30, 2023

HDX offre un'esperienza utente ad alta definizione su qualsiasi dispositivo, in qualsiasi luogo. Gli articoli della sezione Dispositivi descrivono i seguenti dispositivi:

- Mappatura unità client
- Dispositivo USB generico
- Dispositivi mobili e touch screen
- Dispositivi seriali
- Tastiere speciali
- Dispositivi TWAIN
- Webcam
- Dispositivi WIA

### Dispositivo USB ottimizzato e generico

Un dispositivo USB ottimizzato è un dispositivo per il quale l'app Citrix Workspace ha un supporto specifico. Ad esempio, la possibilità di reindirizzare le webcam utilizzando il canale virtuale HDX Multimedia. Un dispositivo generico è un dispositivo USB per il quale non esiste un supporto specifico nell'app Citrix Workspace.

Per impostazione predefinita, il reindirizzamento USB generico non può reindirizzare i dispositivi USB con supporto ottimizzato per i canali virtuali a meno che non vengano inseriti in modalità Generica.

In generale, si ottengono prestazioni migliori per i dispositivi USB in modalità Ottimizzata rispetto alla modalità Generica. Tuttavia, ci sono casi in cui un dispositivo USB non dispone di funzionalità complete in modalità ottimizzata. Potrebbe essere necessario passare alla modalità Generica per ottenere l'accesso completo alle sue funzioni.

Con i dispositivi di archiviazione di massa USB, è possibile utilizzare la mappatura dell'unità client oppure il reindirizzamento USB generico oppure entrambi, controllati dalle politiche Citrix. Le principali differenze sono:

Se sia il reindirizzamento USB generico che i criteri di mappatura delle unità client sono attivati e viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione, questo viene reindirizzato utilizzando il mapping delle unità client.

Quando queste condizioni sono vere, il dispositivo di archiviazione di massa viene reindirizzato utilizzando il reindirizzamento USB generico:

- Sono abilitati sia il reindirizzamento USB generico che i criteri di mappatura delle unità client.
- Un dispositivo è configurato per il reindirizzamento automatico.
- Viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione.

Per ulteriori informazioni, vedere http://support.citrix.com/article/CTX123015.

| Funzionalità | Mappatura unità client | Reindirizzamento USB generico |
|---|---|---|
| Attivato per impostazione predefinita | Sì | No |
| Accesso in sola lettura configurabile | Sì | No |
| Accesso ai dispositivi crittografati | Sì, se la crittografia viene sbloccata prima dell'accesso al dispositivo nella sessione virtuale. | Solo Citrix Virtual Desktops |

## Client Drive Mapping (CDM)

October 30, 2023

Client Drive Mapping rende le unità di archiviazione presenti sull'endpoint client disponibili all'interno di una sessione Citrix HDX per consentire il trasferimento di file e cartelle dal client all'host della sessione e viceversa. Questa funzionalità è abilitata per impostazione predefinita con privilegi di lettura e scrittura. Per impedire agli utenti di aggiungere o modificare file e cartelle nei dispositivi client mappati, attivare l'impostazione dei criteri **Read-only client drive access (Accesso alle unità client di sola lettura)**. Quando si aggiunge questa impostazione a un criterio, assicurarsi che l'impostazione **Client drive redirection** (Reindirizzamento unità client) sia impostata su **Allowed** (Consentita) e sia anche aggiunta al criterio.

Come precauzione di sicurezza, le unità degli endpoint vengono mappate senza l'autorizzazione di esecuzione per impostazione predefinita. Per consentire agli utenti di eseguire gli eseguibili direttamente dalle unità client mappate, modificare il valore del registro **ExecuteFromMappedDrive** nell'host della sessione. Per dettagli, vedere Unità client mappate nella sezione **Funzionalità HDX gestite tramite il Registro di sistema**.

## Requisiti

Di seguito sono riportati i requisiti per l'utilizzo del CDM:

### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 1912 o versioni successive
- Citrix DaaS

### Host della sessione

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Windows Server 2016 o versione successiva
  - Linux: fare riferimento ai requisiti di sistema di Linux VDA
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 o versioni successive
  - Linux: fare riferimento alla documentazione di Linux VDA

### Dispositivo client

- Sistema operativo
  - Windows 10 1809 o versione successiva
  - Linux: fare riferimento all'app Workspace per i requisiti di sistema Linux

## Criteri correlati

Vedere la sezione Riferimento alle impostazioni dei criteri per le impostazioni CDM.

### Scenari a doppio hop

CDM è supportato negli scenari a doppio hop. Per impostazione predefinita, l'unità dell'endpoint client è mappata alla sessione del secondo hop e le unità del primo hop non sono disponibili. Tuttavia, questo può essere impostato in modo che le unità del primo hop vengano mappate nella sessione del secondo hop anziché nelle unità dell'endpoint client.

Per configurare questa funzionalità, modificare il seguente valore di registro:

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
- Nome del valore: NativeDriveMapping
- Tipo di valore: REG_SZ
- Dati del valore:
  - True: mappa le unità della prima sessione di hop nella seconda sessione di hop
  - False: mappa le unità dell'endpoint client nella seconda sessione di hop

> **Nota:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

## Dispositivi USB generici

October 6, 2022

La tecnologia HDX offre **supporto ottimizzato** per i dispositivi USB più diffusi. Questi dispositivi includono:

- Monitor
- Mouse
- Tastiere
- Telefoni VoIP
- Cuffie
- Webcam
- Scanner
- Videocamere
- Stampanti

- Drive
- Lettori di smart card
- Tablet da disegno
- Signature pad

Il supporto ottimizzato offre una migliore esperienza utente con migliori prestazioni ed efficienza della larghezza di banda su una WAN. Il supporto ottimizzato è solitamente l'opzione migliore, soprattutto in ambienti con latenza elevata o sensibili alla sicurezza.

La tecnologia HDX offre il **reindirizzamento USB generico** per dispositivi speciali che non dispongono di alcun supporto ottimizzato o nei casi in cui non è adatto. Per ulteriori informazioni sul reindirizzamento USB generico, vedere Reindirizzamento USB generico.

Per ulteriori informazioni sui dispositivi USB e sull'app Citrix Workspace per Windows, vedere Configurare il reindirizzamento dei dispositivi USB compositi e Configurazione del supporto USB.

## Supporto per dispositivi client mobili e con touch screen

July 12, 2023

Citrix Virtual Apps and Desktops consente agli utenti di accedere alle applicazioni e ai desktop pubblicati da dispositivi client mobili e con touch screen.

### Requisiti

#### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 7.15 o versioni successive
- Citrix DaaS

#### Host della sessione

- Sistema operativo
  - Windows 10 1903 o versione successiva
  - Windows Server 2016 o versione successiva
- VDA
  - Windows: versione 7.15 o successiva

#### Dispositivo client

- Sistema operativo
  - Windows 10 1809 o versione successiva
- App Citrix Workspace per Windows versione 1808 o successiva

### Modalità tablet per dispositivi touch screen che utilizzano Windows Continuum

Continuum è una funzionalità di Windows 10 che si adatta al modo in cui viene utilizzato il dispositivo client. Quando il VDA rileva la presenza di una tastiera o di un mouse su un client abilitato al tocco, mette il client in modalità desktop. Se non è presente una tastiera o un mouse, il VDA mette il client in modalità tablet/mobile. Questo rilevamento si verifica durante la connessione e la riconnessione della sessione e anche durante la sessione quando la tastiera o il mouse sono collegati o scollegati.

Questa funzionalità è abilitata per impostazione predefinita. Per disabilitare questa funzionalità, configurare le impostazioni dei criteri Tablet mode toggle policy settings (Impostazioni dei criteri di abilitazione/disabilitazione della modalità tablet).

Oltre ai requisiti per i dispositivi con touch screen sopra menzionati, per Windows Continuum sono necessari i seguenti requisiti:

#### Citrix Hypervisor

- Citrix Hypervisor 8.2 o versione successiva
- Eseguire il comando CLI di XenServer per consentire il passaggio laptop/tablet:
  **xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1**

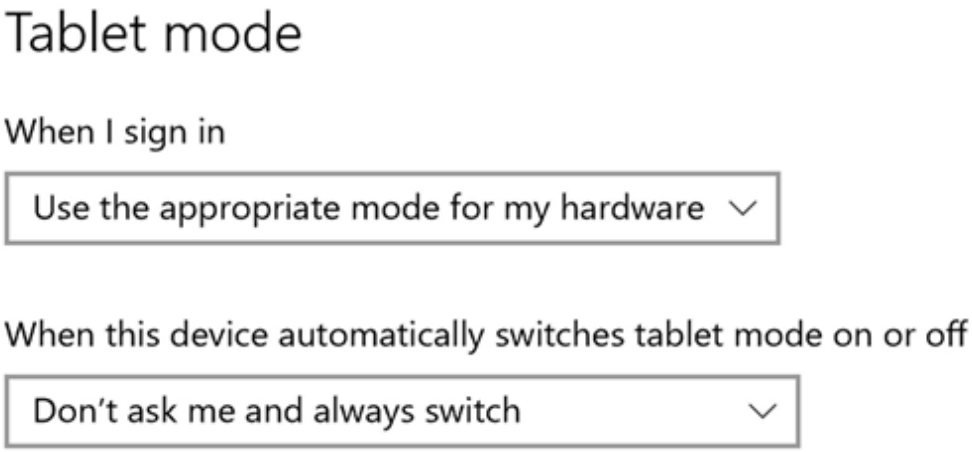
> **Importante:**
>
> L'aggiornamento dell'immagine di base per un catalogo di macchine esistente dopo aver modificato l'impostazione dei metadati non influisce sulle VM precedentemente sottoposte a provisioning. Dopo aver modificato l'immagine di base della VM di XenServer, creare un catalogo, scegliere l'immagine di base ed eseguire il provisioning di una nuova macchina MCS (Machine Creation Services).

#### Host della sessione

- Sistema operativo
  - Windows 10 1903 o versione successiva
  - Windows 11

- VDA
  - Windows: versione 7.16 o successiva
  - **A causa delle attuali limitazioni nelle configurazioni del sistema operativo, dopo aver avviato la prima sessione ICA e riavviato il VDA l'utente dovrà impostare dai menu a discesa le seguenti opzioni:**
    - **Settings > System > Tablet Mode** (Impostazioni > Sistema > Modalità tablet)
      - Use the appropriate mode for my hardware (Utilizza la modalità appropriata per il mio hardware)
      - Don't ask me and always switch (Non mostrare più questo messaggio e cambia sempre modalità)




La **modalità tablet** offre un'interfaccia utente più adatta ai touch screen:

- Pulsanti leggermente più grandi.
- La schermata di avvio e tutte le app avviate vengono aperte a schermo intero.
- La barra delle applicazioni contiene un pulsante Indietro.
- Icone eliminate dalla barra delle applicazioni.

Accesso a Esplora file.

Windows 10 carica il driver GPIO sulla macchina virtuale di destinazione in base a questo BIOS aggiornato. Viene utilizzato per passare dalla modalità tablet alla modalità desktop e viceversa all'interno della macchina virtuale.

L'app Citrix Workspace per HTML5 non supporta le funzionalità di Windows Continuum.

La **modalità desktop** offre l'interfaccia utente tradizionale in cui si interagisce allo stesso modo in cui si usa il PC con una tastiera e un mouse.

### Penne Microsoft Surface Pro e Surface Book

Supportiamo la funzionalità penna standard con le applicazioni basate su Windows Ink. Il supporto include puntamento, cancellazione, pressione della penna, segnali Bluetooth e altre funzionalità a seconda del firmware del sistema operativo e del modello di penna. Ad esempio, la pressione della penna può essere fino a 4096 livelli. Questa funzionalità è abilitata per impostazione predefinita.

Di seguito sono riportati i requisiti per il supporto delle funzionalità della penna:

#### Piano di controllo Citrix

- Citrix Virtual Apps and Desktops 1903 o versioni successive
- Citrix DaaS

#### Host della sessione

- Sistema operativo
  - Windows 10 1809 o versione successiva

  - Windows Server 2016 o versione successiva
- VDA
  - Windows: versione 1903 o successiva

**Dispositivo client**

- Sistema operativo
  - Windows 10 1809 o versione successiva
- App Citrix Workspace per Windows versione minima 1902

Per una dimostrazione di Windows Ink e della funzionalità penna, fare clic sul seguente elemento grafico:


Per disabilitare o abilitare questa funzione, vedere Penne Microsoft Surface Pro e Surface Book nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Problemi noti

Di seguito sono riportati i problemi noti relativi al supporto della penna:

- A causa delle limitazioni del sistema operativo in Windows Server 2k22, gli utenti non saranno in grado di impostare scelte rapide della penna o apportare modifiche alle impostazioni penna/inchiostro del Pannello di controllo durante la connessione alle applicazioni o ai desktop del server 2k22.
- Le scelte rapide della penna non vengono rispettate da un client Windows 11 abilitato alla penna a causa delle limitazioni del sistema operativo.

# Porte seriali

October 6, 2022

La maggior parte dei nuovi PC non dispone di porte seriali (COM) integrate. Le porte sono facili da aggiungere utilizzando convertitori USB. Le applicazioni adatte alle porte seriali spesso comprendono sensori, controller, vecchi lettori di assegni, pad e così via. Alcuni dispositivi con porta COM virtuale USB utilizzano driver specifici del fornitore al posto dei driver forniti da Windows (usbser.sys). Questi driver consentono di forzare la porta COM virtuale del dispositivo USB in modo che non cambi anche se viene collegata a socket USB diversi. Questa operazione può essere eseguita da **Gestione dispositivi > Porte (COM e LPT) > Proprietà** o dall'applicazione che controlla il dispositivo.

Il mapping delle porte COM client consente di utilizzare i dispositivi collegati alle porte COM dell'endpoint dell'utente durante le sessioni virtuali. È possibile utilizzare questi mapping come qualsiasi altro mapping di rete.

Per ogni porta COM, un driver nel sistema operativo assegna un nome di collegamento simbolico, ad esempio COM1 e COM2. Le applicazioni utilizzano quindi il collegamento per accedere alla porta.

> **Importante:**
>
> Poiché un dispositivo può collegarsi all'endpoint utilizzando direttamente USB, non significa che possa essere reindirizzato utilizzando il reindirizzamento USB generico. Alcuni dispositivi USB funzionano come porte COM virtuali, alle quali le applicazioni possono accedere allo stesso modo della porta seriale fisica. Il sistema operativo può astrarre le porte COM e trattarle come condivisioni file. Due protocolli comuni per la COM virtuale sono CDC ACM o MCT. In caso di connessione tramite una porta RS-485, le applicazioni potrebbero non funzionare affatto. Usare un convertitore RS-485-RS232 per utilizzare RS-485 come porta COM.
> **Importante:**
>
> Alcune applicazioni riconoscono il dispositivo (ad esempio un signature pad) in modo coerente solo se è collegato a COM1 o COM2 sulla workstation client.

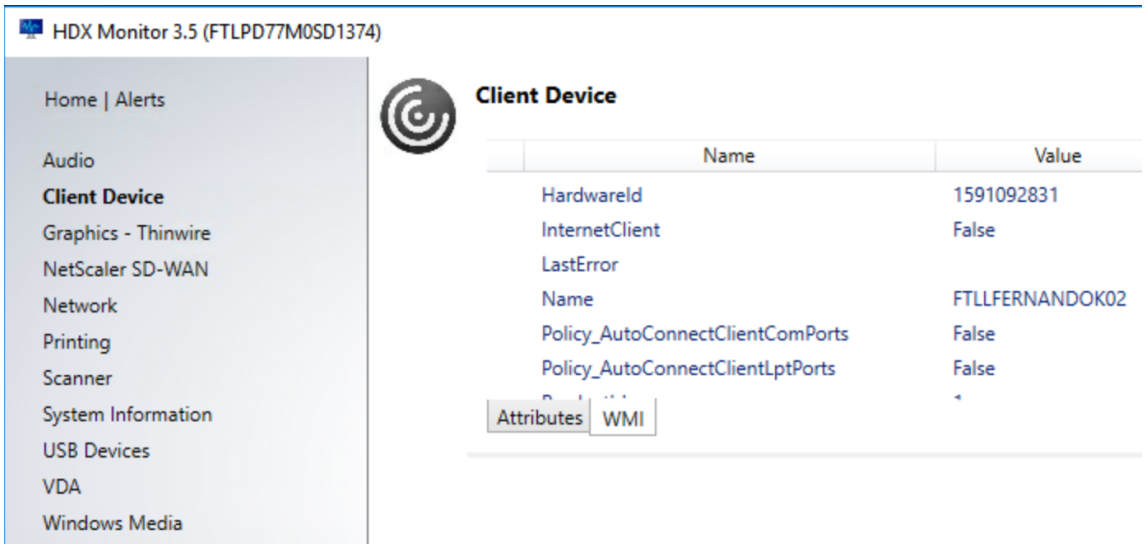
## Mappare una porta COM client a una porta COM server

È possibile mappare le porte COM client a una sessione Citrix in tre modi:

- Gestire i criteri della console. Per ulteriori informazioni sui criteri, vedere Impostazioni dei criteri di reindirizzamento delle porte.
- Prompt dei comandi VDA.
- Strumento di configurazione Desktop remoto (Servizi terminal).

1. Abilitare il **reindirizzamento della porta COM client** e i **criteri di Studio per la connessione automatica delle porte COM client**. Dopo l'applicazione, sono disponibili alcune informazioni in HDX Monitor.




2. Se la **connessione automatica delle porte COM client** non riesce a mappare la porta, è possibile mappare manualmente la porta o utilizzare script di accesso. Accedere al VDA e in una finestra del prompt dei comandi digitare:

   NET USE COMX: \\CLIENT\COMZ:

   oppure

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   **X** è il numero della porta COM sul VDA (le porte da 1 a 9 sono disponibili per il mapping). **Z** è il numero della porta COM client che si desidera mappare.

   Per confermare che l'operazione ha avuto esito positivo, digitare **NET USE** al prompt dei comandi VDA. L'elenco visualizzato contiene unità mappate, porte LPT e porte COM mappate.

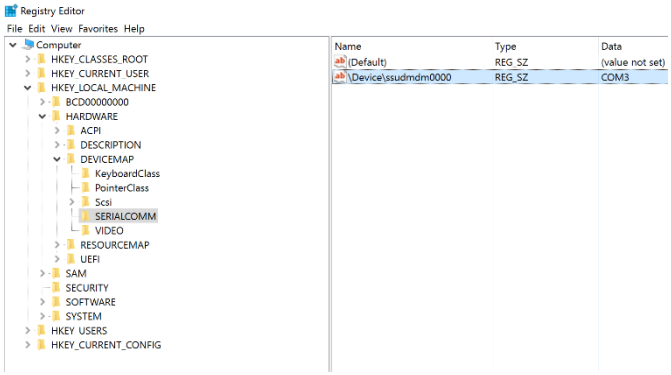

3. Per utilizzare questa porta COM in un desktop virtuale o in un'applicazione, installare l'applicazione del dispositivo utente e puntare al nome della porta COM mappata. Ad esempio, se si esegue il mapping di COM1 sul client a COM3 sul server, installare l'applicazione del dispositivo della porta COM nel VDA e puntare a COM3 durante la sessione. Utilizzare questa porta COM mappata come una porta COM sul dispositivo utente.

> **Importante:**
>
> Il mapping delle porte COM non è compatibile con TAPI. Non è possibile mappare i dispositivi TAPI (Telephony Application Programming Interface) di Windows alle porte COM client. TAPI definisce un modo standard di controllare le funzioni telefoniche per dati, fax e chiamate vocali per le applicazioni. TAPI gestisce la segnalazione, comprese la composizione, la risposta e la fine delle chiamate. Inoltre, gestisce servizi supplementari come l'attesa, il trasferimento e le chiamate in conferenza.

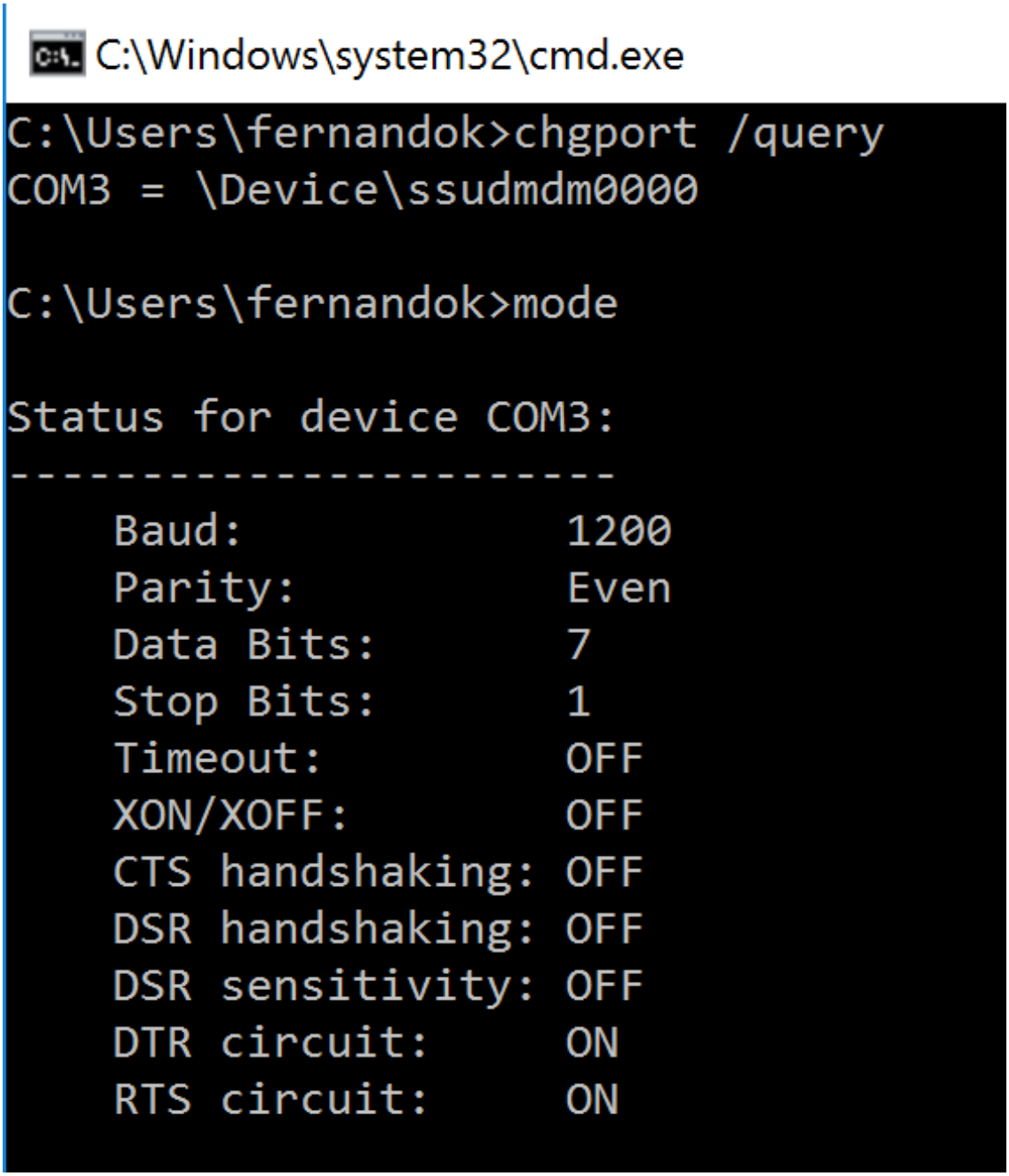
## Risoluzione dei problemi

1. Assicurarsi di poter accedere al dispositivo direttamente dall'endpoint, evitando Citrix. Se la porta non è mappata al VDA, non si è connessi a una sessione Citrix. Seguire le istruzioni per la risoluzione dei problemi fornite con il dispositivo e verificare innanzitutto che funzioni localmente.
   Quando un dispositivo è connesso a una porta COM seriale, viene creata una chiave del Registro di sistema nell'hive mostrato qui:



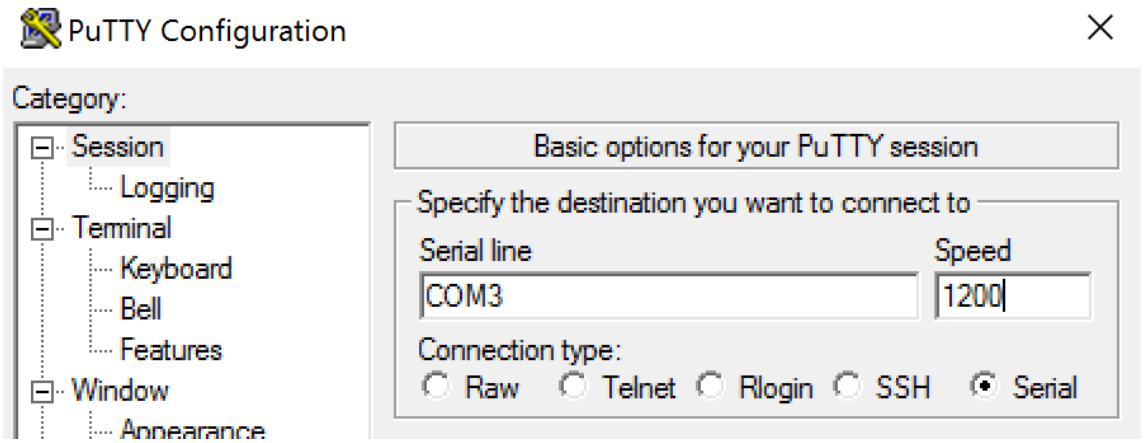

   È inoltre possibile trovare queste informazioni dal prompt dei comandi eseguendo **chgport /query**.




Se le istruzioni per la risoluzione dei problemi relativi al dispositivo non sono disponibili, provare ad aprire una sessione PuTTY. Scegliere **Session (Sessione)** e in **Serial line (Linea seriale)** specificare la porta COM.




È possibile eseguire **MODE** in una finestra di comando locale. L'output potrebbe visualizzare la porta COM in uso e il baud/parità/bit di dati/bit di stop, necessari nella sessione PuTTY. Se la connessione PuTTY ha esito positivo, premere **Invio** per visualizzare il feedback del dispositivo. Qualsiasi carattere digitato potrebbe essere ripetuto sullo schermo o ricevere una risposta. Se questo passaggio non riesce, non è possibile accedere al dispositivo da una sessione virtuale.

2. Mappare la porta COM locale al VDA (utilizzando i criteri o **NET USE COMX: \\CLIENT\COMZ:**) e ripetere le stesse procedure PuTTY del passaggio precedente, ma questa volta dal PuTTY del VDA. Se PuTTY non mostra l'errore **Unable to open connection to COM1. Unable to open serial port (Impossibile aprire la connessione a COM1. Impossibile aprire la porta seriale)**, un altro dispositivo potrebbe utilizzare COM1.

3. Eseguire **chgport /query**. Se il driver seriale Windows incorporato nel VDA assegna automaticamente \Device\Serial0 a una porta COM1 del VDA, effettuare le seguenti operazioni:
   A. Aprire CMD sul VDA e digitare **NET USE.**

   B. Eliminare gli eventuali mapping esistenti (ad esempio, COM1) sul VDA.

   **NET USE COM1 /DELETE**

   C. Mappare il dispositivo al VDA.

   **NET USE COM1: \\CLIENT\COM3:**

   D. Puntare l'applicazione sul VDA su COM3.

   Infine, provare a mappare la porta COM locale (ad esempio, COM3) a una porta COM diversa sul VDA (diversa da COM1, ad esempio COM3). Assicurarsi che l'applicazione punti a questa porta:
   **NET USE COM3: \\CLIENT\COM3**

4. Se ora è visibile la porta mappata, PuTTY funziona ma non vengono trasferiti dati, potrebbe trattarsi di una race condition. L'applicazione potrebbe connettersi e aprire la porta prima che venga mappata, bloccando il mapping. Provare a eseguire una delle seguenti operazioni:

   - Aprire una seconda applicazione pubblicata sullo stesso server. Attendere alcuni secondi

perché la porta venga mappata, quindi aprire l'applicazione reale che tenta di utilizzare la porta.

- Abilitare i criteri di reindirizzamento della porta COM dall'Editor Criteri di gruppo in Active Directory anziché dall'interfaccia Gestisci > Configurazione completa del servizio. Tali criteri sono il **reindirizzamento delle porte COM client** e la **connessione automatica delle porte COM client**. I criteri applicati in questo modo potrebbero essere elaborati prima dei criteri della console di gestione, garantendo che la porta COM sia mappata. I criteri Citrix vengono inviati al VDA e archiviati in:
  `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Utilizzare questo script di accesso per l'utente oppure, invece di pubblicare l'applicazione, pubblicare uno script .bat che elimina innanzitutto qualsiasi mapping sul VDA, rimappa la porta COM virtuale e quindi avvia l'applicazione:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (or whatever value needed)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (or whatever value needed)
START C:\Program Files\<Your Software Path>\
```

5. Come ultima alternativa, è possibile utilizzare lo strumento Process Monitor di Sysinternals. Quando si esegue lo strumento sul VDA, trovare e filtrare oggetti come COM3, picaser.sys, CdmRedirector, ma soprattutto <tua_app>.exe. Eventuali errori potrebbero essere visualizzati come Accesso negato o simile.

## Tastiere speciali

October 6, 2022

### Tastiere Bloomberg

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare

> l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Citrix Virtual Apps and Desktops supporta la tastiera Starboard Bloomberg modello 4 (e il modello precedente 3). Questa tastiera consente ai clienti del settore finanziario di utilizzare le funzionalità speciali della tastiera per accedere ai dati del mercato finanziario e fare trading rapidamente.

Questa tastiera è compatibile con gli switch KVM e può funzionare in due modalità:

- PC (un cavo USB senza KVM)
- Modalità KVM (due cavi USB con uno instradato tramite KVM)

> **Importante:**
>
> Si consiglia di utilizzare la tastiera Bloomberg con una sola sessione. Si sconsiglia di utilizzare la tastiera con più sessioni simultanee (un client per più sessioni).

La tastiera Bloomberg 4 è un dispositivo USB composito composto da quattro dispositivi USB in un' unica shell fisica:

- Tastiera.
- Lettore di impronte digitali.
- Dispositivo audio con tasti per aumentare e diminuire il volume e disattivare l'altoparlante e il microfono. Questo dispositivo include altoparlante integrato, microfono, jack per il microfono e auricolare.
- Hub USB per collegare tutti questi dispositivi al sistema.

**Requisiti:**

- La sessione a cui si connette l'app Citrix Workspace per Windows deve supportare i dispositivi USB.
- App Citrix Workspace (versione minima 1808) per Windows o Citrix Receiver per Windows (versione minima 4.8) per supportare la tastiera Bloomberg modello 3 e 4.
- App Citrix Workspace (versione minima 1808) per Windows o Citrix Receiver per Windows (versione minima 4.12) per utilizzare la modalità KVM (due cavi USB con uno instradato tramite KVM) per il modello 4.

Per informazioni sulla configurazione delle tastiere Bloomberg nell'app Citrix Workspace per Windows, vedere Configurazione delle tastiere Bloomberg.

Per abilitare il supporto per la tastiera Bloomberg, vedere Tastiere Bloomberg nell'elenco delle funzionalità gestite tramite il Registro di sistema.

**Verificare il supporto:**

Per determinare se il supporto della tastiera Bloomberg è abilitato nell'app Citrix Workspace, verificare se Desktop Viewer segnala correttamente i dispositivi della tastiera Bloomberg.

Scenario desktop:

Aprire Desktop Viewer. Se il supporto per la tastiera Bloomberg è abilitato, Desktop Viewer mostra tre dispositivi sotto l'icona USB:

- Scanner di impronte digitali Bloomberg
- Funzionalità della tastiera Bloomberg
- Tastiera Bloomberg LP 2013

Solo per lo scenario con applicazioni integrate:

Aprire il menu **Connection Center** dall'icona dell'area di notifica dell'app Citrix Workspace. Se il supporto per la tastiera Bloomberg è abilitato, i tre dispositivi vengono visualizzati nel menu **Devices** (Dispositivi).

Il segno di spunta accanto a ciascuno di questi dispositivi indica che sono utilizzati in remoto nella sessione.

## Dispositivi TWAIN

October 6, 2022

### Requisiti

- Lo scanner deve essere conforme a TWAIN.
- Installare i driver TWAIN sul dispositivo locale. Non sono necessari sul server.
- Collegare lo scanner localmente (ad esempio, tramite USB).
- Verificare che lo scanner utilizzi il driver TWAIN locale e non il servizio Acquisizione di immagini di Windows.
- Verificare che non vi siano criteri applicati all'account utente utilizzato per il test e che limitino la larghezza di banda all'interno della sessione ICA. Ad esempio, il limite della larghezza di banda di reindirizzamento USB del client.

Per informazioni sulle impostazioni dei criteri, vedere Impostazioni dei criteri dei dispositivi TWAIN.

# Webcam

October 6, 2022

### Streaming con webcam ad alta definizione

Le webcam possono essere utilizzate dalle applicazioni di videoconferenza in esecuzione all'interno della sessione virtuale. L'applicazione sul server seleziona il formato e la risoluzione della webcam in base ai tipi di formato supportati. Quando si avvia una sessione, il client invia le informazioni della webcam al server. Scegliere una webcam dall'applicazione di videoconferenza. Quando sia la webcam che l'applicazione supportano il rendering ad alta definizione, l'applicazione utilizza una risoluzione ad alta definizione. Supportiamo risoluzioni webcam fino a 1920x1080.

Questa funzionalità richiede Citrix Receiver per Windows, versione minima 4.10. Per un elenco delle piattaforme di app Citrix Workspace che supportano il reindirizzamento della webcam HDX, vedere Matrice delle funzionalità dell'app Citrix Workspace.

Per ulteriori informazioni sullo streaming con webcam ad alta definizione, vedere Videoconferenze HDX e compressione video della webcam.

È possibile utilizzare una chiave del Registro di sistema per disabilitare e abilitare la funzionalità e quindi configurare una risoluzione specifica. Per informazioni, vedere Streaming della webcam ad alta definizione e risoluzione della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il Registro di sistema.

# Dispositivi WIA

October 6, 2022

### Requisiti

- Lo scanner deve essere conforme a WIA.
- Installare i driver WIA sul dispositivo locale. Non sono necessari sul server.
- Collegare lo scanner localmente (ad esempio, tramite USB).
- Verificare che lo scanner utilizzi il servizio Acquisizione di immagini di Windows e non il driver TWAIN.

- Verificare che non vi siano criteri applicati all'account utente utilizzato per il test e che limitino la larghezza di banda all'interno della sessione ICA. Ad esempio, il limite della larghezza di banda di reindirizzamento USB del client.

**Windows Image Acquisition application allow list (Elenco di elementi consentiti dell'applicazione Acquisizione di immagini di Windows)**

Un elenco di elementi consentiti permette di controllare quali applicazioni sul VDA possono accedere al reindirizzamento dello scanner di Acquisizione di immagini di Windows. L'Editor del Registro di sistema utilizza l'input dell'impostazione dell'elenco di elementi consentiti su ogni VDA che contiene l'Acquisizione di immagini di Windows. Per impostazione predefinita, nessuna applicazione ha accesso ad Acquisizione di immagini di Windows.

Per regolare l'acquisizione di immagini Windows per le applicazioni sul VDA, vedere l'impostazione Windows Image Acquisition application allow list nell'elenco delle funzionalità gestite tramite il Registro di sistema.

Per informazioni sulle impostazioni dei criteri, vedere Impostazioni dei criteri dei dispositivi WIA.

## Grafica

October 6, 2022

La grafica Citrix HDX include una vasta gamma di tecnologie di accelerazione grafica e codifica che ottimizza la distribuzione di applicazioni grafiche avanzate da Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops). Le tecnologie grafiche offrono la stessa esperienza dell'utilizzo di un desktop fisico quando si lavora in remoto con applicazioni virtuali che fanno uso intensivo della grafica.

È possibile utilizzare software o hardware per il rendering grafico. Il rendering software richiede una libreria di terze parti chiamata rasterizzatore software. Ad esempio, Windows include il rasterizzatore WARP per la grafica basata su DirectX. A volte, è possibile utilizzare un renderer software alternativo. Il rendering hardware (accelerazione hardware) richiede un processore grafico (GPU).

HDX Graphics offre una configurazione di codifica predefinita ottimizzata per i casi d'uso più comuni. Utilizzando i criteri Citrix, gli amministratori IT possono anche configurare varie impostazioni correlate alla grafica per soddisfare i diversi requisiti e fornire l'esperienza utente desiderata.

### Thinwire

Thinwire è la tecnologia di visualizzazione remota predefinita di Citrix utilizzata in Citrix DaaS.

La tecnologia di visualizzazione remota consente la trasmissione della grafica generata su un computer, in genere attraverso una rete, a un altro computer per la visualizzazione. La grafica viene generata come risultato di input dell'utente, ad esempio le sequenze di tasti o le azioni del mouse.

### HDX 3D Pro

Le funzionalità HDX 3D Pro di Citrix DaaS consentono di fornire desktop e applicazioni che offrono prestazioni ottimali utilizzando un'unità di elaborazione grafica (GPU) per l'accelerazione hardware. Queste applicazioni includono applicazioni grafiche professionali 3D basate su OpenGL e DirectX. Il VDA standard supporta solo l'accelerazione GPU di DirectX.

#### Accelerazione GPU per il sistema operativo Windows a sessione singola

Utilizzando HDX 3D Pro, è possibile distribuire applicazioni a uso intensivo della grafica nell'ambito di desktop o applicazioni ospitati su computer con sistema operativo a sessione singola. HDX 3D Pro supporta computer host fisici (tra cui workstation desktop, blade e rack) e le tecnologie di virtualizzazione GPU Passthrough e GPU offerte dagli hypervisor XenServer, vSphere e Hyper-V (solo passthrough).

Utilizzando GPU Passthrough, è possibile creare macchine virtuali con accesso esclusivo a hardware dedicato per l'elaborazione grafica. È possibile installare più GPU nell'hypervisor e assegnare VM a ciascuna di queste GPU in modo individuale.

Utilizzando la virtualizzazione GPU, più macchine virtuali possono accedere direttamente alla potenza di elaborazione grafica di una singola GPU fisica.

#### Accelerazione GPU per il sistema operativo Windows multisessione

HDX 3D Pro consente di eseguire il rendering di applicazioni ricche di grafica in esecuzione in sessioni di sistema operativo multisessione Windows sulla GPU (unità di elaborazione grafica) del server. Spostando il rendering OpenGL, DirectX, Direct3D e WPF (Windows Presentation Foundation) sulla GPU del server, il rendering grafico non rallenta la CPU del server. Inoltre, il server è in grado di elaborare più grafica perché il carico di lavoro è diviso tra CPU e GPU.

### Framehawk

> **Importante:**
>
> A partire da Citrix Virtual Apps and Desktops 7 1903, Framehawk non è più supportato. Utilizzare invece Thinwire con il trasporto adattivo abilitato.

Framehawk è una tecnologia di visualizzazione remota per lavoratori mobili su connessioni wireless a banda larga (Wi-Fi e reti cellulari 4G/LTE). Framehawk supera le sfide dell'interferenza spettrale e della propagazione multipath e offre un'esperienza utente fluida e interattiva agli utenti di app virtuali e desktop.

### Filigrana di sessione basata su testo

Le filigrane di sessione basate su testo aiutano a scoraggiare e abilitare il furto dei dati di tracciabilità. Queste informazioni tracciabili vengono visualizzate sul desktop della sessione come deterrente per

coloro che utilizzano fotografie e acquisizioni dello schermo per rubare i dati. È possibile specificare una filigrana che è testo sovrapposto. La filigrana può essere visualizzata sull'intera schermata della sessione senza modificare il contenuto del documento originale. Le filigrane di sessione basate su testo richiedono il supporto VDA.

### Informazioni correlate

- HDX 3D Pro
- Accelerazione GPU per il sistema operativo Windows a sessione singola
- Accelerazione GPU per il sistema operativo Windows multisessione
- Thinwire
- Filigrana di sessione basata su testo

## HDX 3D Pro

October 6, 2022

Le funzionalità HDX 3D Pro di Citrix Virtual Apps and Desktops consentono di fornire desktop e applicazioni che offrono prestazioni ottimali utilizzando un'unità di elaborazione grafica (GPU) per l'accelerazione hardware. Queste applicazioni includono applicazioni grafiche professionali 3D basate su OpenGL e DirectX. Il VDA standard supporta solo l'accelerazione GPU di DirectX.

Per le impostazioni dei criteri HDX 3D Pro, vedere Ottimizzazione per carichi di lavoro grafici 3D.

Tutte le app Citrix Workspace supportate possono essere utilizzate con grafica 3D. Per ottenere prestazioni ottimali con carichi di lavoro 3D complessi, monitor ad alta risoluzione, configurazioni multi-monitor e applicazioni con frequenza dei fotogrammi elevata, si consiglia di utilizzare le versioni più recenti dell'app Citrix Workspace per Windows e dell'app Citrix Workspace per Linux. Per ulteriori informazioni sulle versioni supportate dell'app Citrix Workspace, vedere Le tappe del ciclo di vita dell'app Citrix Workspace.

Esempi di applicazioni professionali 3D includono:

- Applicazioni di progettazione, produzione e ingegneria assistita da computer (CAD/CAM/CAE)
- Software per il sistema informativo geografico (GIS)
- PACS (Picture Archiving Communication System) per diagnostica per immagini medicale
- Applicazioni che utilizzano le ultime versioni di OpenGL, DirectX, NVIDIA CUDA, OpenCL e WebGL
- Applicazioni non grafiche a uso intensivo di calcolo che utilizzano GPU CUDA (Compute Unified Device Architecture) NVIDIA per l'elaborazione parallela

HDX 3D Pro offre la migliore esperienza utente su qualsiasi larghezza di banda:

- Sulle connessioni WAN: offre un'esperienza utente interattiva sulle connessioni WAN con larghezze di banda fino a 1,5 Mbps.
- Connessioni LAN: offre un'esperienza utente equivalente a quella di un desktop locale sulle connessioni LAN.

  È possibile sostituire workstation complesse e costose con dispositivi utente più semplici spostando l'elaborazione grafica nel data center per una gestione centralizzata.

HDX 3D Pro fornisce accelerazione GPU per le macchine con sistema operativo Windows a sessione singola e macchine con sistema operativo multisessione Windows. Per ulteriori informazioni, vedere Accelerazione GPU per il sistema operativo Windows a sessione singola e Accelerazione GPU per il sistema operativo multisessione Windows.

HDX 3D Pro è compatibile con le tecnologie di virtualizzazione GPU passthrough e GPU offerte dai seguenti hypervisor, oltre al bare metal:

- Citrix Hypervisor
  - Passthrough GPU con NVIDIA GRID, AMD e Intel GVT-d
  - Virtualizzazione GPU con NVIDIA GRID, AMD e Intel GVT-G
  - Vedere la compatibilità hardware in Elenco di compatibilità hardware di Hypervisor.

Utilizzare lo strumento HDX Monitor per convalidare il funzionamento e la configurazione delle tecnologie di visualizzazione HDX e per diagnosticare e risolvere i problemi HDX. Per scaricare lo strumento e saperne di più, vedere https://taas.citrix.com/hdx/download/.

## Accelerazione GPU per il sistema operativo multisessione Windows

October 6, 2022

HDX 3D Pro consente di eseguire il rendering di applicazioni ad utilizzo intensivo di grafica in esecuzione in sessioni di sistema operativo multisessione Windows sulla GPU (unità di elaborazione grafica) del server. Spostando il rendering OpenGL, DirectX, Direct3D e WPF (Windows Presentation Foundation) sulla GPU del server, il rendering grafico non rallenta la CPU del server. Inoltre, il server è in grado di elaborare più grafica perché il carico di lavoro è diviso tra CPU e GPU.

Poiché Windows Server è un sistema operativo multiutente, più utenti possono condividere una GPU accessibile da Citrix Virtual Apps senza la necessità di virtualizzazione GPU (vGPU).

Per le procedure che includono la modifica del Registro di sistema, procedere con cautela: la modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto

dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

### Condivisione GPU

Condivisione GPU consente il rendering hardware GPU delle applicazioni OpenGL e DirectX nelle sessioni desktop remote. Ha le seguenti caratteristiche:

- Può essere utilizzato su macchine bare metal o virtuali per aumentare la scalabilità e le prestazioni delle applicazioni.
- Consente a più sessioni simultanee di condividere le risorse GPU (la maggior parte degli utenti non richiede le prestazioni di rendering di una GPU dedicata).
- Non richiede impostazioni speciali.

Una GPU può essere assegnata alla macchina virtuale Windows Server in modalità pass-through completa o GPU virtuale (vGPU) in base ai requisiti del fornitore di Hypervisor e GPU. Sono supportate anche distribuzioni bare metal su computer Windows Server fisici.

Condivisione GPU non necessita di alcuna scheda grafica specifica.

- Per le macchine virtuali, selezionare una scheda grafica compatibile con Hypervisor in uso. Per un elenco degli hardware compatibili con Citrix Hypervisor, vedere Elenco di compatibilità hardware di Hypervisor.
- Quando è in esecuzione su bare metal, si consiglia di avere una scheda di visualizzazione singola abilitata dal sistema operativo. Se nell'hardware sono installate più GPU, disattivarle tutte tranne una utilizzando Gestione periferiche.

La scalabilità tramite la condivisione GPU dipende da diversi fattori:

- Le applicazioni in esecuzione
- La quantità di RAM video che consumano
- La potenza di elaborazione della scheda grafica

Alcune applicazioni gestiscono l'insufficienza di RAM video meglio di altre. Se l'hardware viene sovraccaricato, potrebbe verificarsi un'instabilità o un arresto anomalo del driver della scheda grafica. Limitare il numero di utenti simultanei per evitare questo tipo di problemi.

Per confermare che l'accelerazione della GPU si stia verificando, utilizzare uno strumento di terze parti, ad esempio GPU-Z. GPU-Z è disponibile all'indirizzo http://www.techpowerup.com/gpuz/.

- Accesso a un codificatore video ad alte prestazioni per GPU NVIDIA e processori grafici Intel Iris Pro. Un'impostazione dei criteri (abilitata per impostazione predefinita) controlla questa funzione e consente l'uso della codifica hardware per la codifica H.264 (se disponibile). Se tale hardware non è disponibile, il VDA effettua un fallback sulla codifica basata su CPU utilizzando il codec video software. Per ulteriori informazioni, vedere Impostazioni dei criteri di grafica.

### Rendering DirectX, Direct3D e WPF

Il rendering DirectX, Direct3D e WPF è disponibile solo sui server con una GPU che supporta una versione DDI (Display Driver Interface) 9ex, 10 o 11.

- In Windows Server 2008 R2, DirectX e Direct3D non richiedono impostazioni speciali per l'utilizzo di una singola GPU.
- In Windows Server 2012 e versioni successive, le sessioni di Servizi Desktop remoto nel server Host sessione Desktop remoto utilizzano il Driver rendering base Microsoft come scheda predefinita. Per utilizzare la GPU nelle sessioni di Servizi Desktop remoto in Windows Server 2012 e versioni successive, attivare l'impostazione **Usa la scheda grafica predefinita per l'hardware per tutte le sessioni di Servizi Desktop remoto** nel Criterio di gruppo **Criteri del computer locale** > **Configurazione computer** > **Modelli amministrativi** > **Componenti di Windows** > **Servizi Desktop remoto** > **Host sessione Desktop remoto**> **Ambiente sessione remota**.
- Per abilitare il rendering delle applicazioni WPF utilizzando la GPU del server, creare le impostazioni nel Registro di sistema del server che esegue sessioni del sistema operativo multisessione Windows. Per informazioni sulle impostazioni del Registro di sistema, vedere Rendering Windows Presentation Foundation (WPF) nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### Accelerazione GPU per applicazioni CUDA o OpenCL

L'accelerazione GPU delle applicazioni CUDA e OpenCL in esecuzione in una sessione utente è disabilitata per impostazione predefinita.

Per utilizzare le funzionalità POC di accelerazione CUDA, abilitare le impostazioni del Registro di sistema. Per informazioni, vedere Accelerazione GPU per applicazioni CUDA o OpenCL nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Accelerazione GPU per il sistema operativo Windows a sessione singola

October 6, 2022

Con HDX 3D Pro, è possibile distribuire applicazioni a uso intensivo della grafica nell'ambito di desktop o applicazioni ospitati su computer con sistema operativo a sessione singola. HDX 3D Pro supporta computer host fisici (tra cui workstation desktop, blade e rack) e le tecnologie di virtualizzazione GPU Passthrough e GPU offerte da Citrix Hypervisor, vSphere, Nutanix e Hyper-V (solo passthrough).

HDX 3D Pro offre le seguenti funzionalità:

- Compressione profonda adattiva basata su H.264 o H.265 per prestazioni WAN e wireless ottimali. HDX 3D Pro utilizza la compressione H.264 a schermo intero basata su CPU come tecnica di compressione predefinita per la codifica. La codifica hardware con H.264 viene utilizzata con schede NVIDIA, Intel e AMD che supportano NVENC. La codifica hardware con H.265 viene utilizzata con schede NVIDIA che supportano NVENC.
- Opzione di compressione senza perdita di dati per casi d'uso specializzati. HDX 3D Pro offre anche un codec senza perdita di dati basato su CPU per supportare applicazioni in cui è richiesta una grafica con pixel perfetti, come per l'imaging medicale. La compressione senza perdita di dati vera e propria è consigliata solo per casi d'uso specializzati in quanto consuma più risorse di rete e di elaborazione.

  Quando si utilizza la compressione senza perdita di dati:

  - L'indicatore senza perdita, un'icona dell'area di notifica, notifica l'utente se lo schermo visualizzato è un frame con perdita di dati o un frame senza perdita di dati. Questa icona aiuta quando l'impostazione del criterio **Qualità visiva** specifica **Compila per senza perdite**. L'indicatore senza perdita diventa verde quando i fotogrammi inviati sono senza perdita di dati.
  - L'interruttore senza perdita di dati consente all'utente di passare alla modalità Sempre senza perdite in qualsiasi momento all'interno della sessione. Per selezionare o deselezionare **Senza perdite in qualsiasi momento all'interno di una sessione**, fare clic con il pulsante destro del mouse sull'icona e fare clic su **Passa al pixel perfetto** oppure utilizzare la scelta rapida da tastiera ALT+MAIUSC+1.

    Per la compressione senza perdita di dati: HDX 3D Pro utilizza il codec lossless per la compressione indipendentemente dal codec selezionato tramite criterio.

    Per la compressione con perdita di dati: HDX 3D Pro utilizza il codec originale, quello predefinito o quello selezionato tramite criterio.

    Le impostazioni dell'interruttore senza perdita di dati non vengono mantenute per le sessioni successive. Per utilizzare un codec senza perdita per ogni connessione, selezionare **Sempre senza perdite** nell'impostazione dei criteri **Qualità visiva**.

- È possibile ignorare la scelta rapida da tastiera predefinita ALT+MAIUSC+1 per selezionare o deselezionare Senza perdite all'interno di una sessione. Configurare una nuova impostazione del Registro di sistema in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.

  - Nome: HKEY_LOCAL_MACHINE_HotKey, Type: String
  - Il formato per configurare una combinazione di collegamenti è C=0|1, A=0|1, S=0|1, W=0|1, K=val. Le chiavi devono essere separate da virgola ",". L'ordine delle chiavi non ha importanza.

  - A, C, S, W e K sono chiavi, dove C = Control, A = ALT, S = SHIFT, W=Win e K = una chiave valida. I valori consentiti per K sono 0-9, a-z e qualsiasi codice chiave virtuale.
  - Ad esempio:
    * Per F10, impostare K=0x79
    * Per Ctrl + F10, impostare C=1, K=0x79
    * Per Alt + A, impostare A=1, K=a o A=1, K=A o K=A, A=1
    * Per Ctrl + Alt + 5, impostare C=1, A=1, K=5 o A=1, K=5, C=1
    * Per Ctrl + Maiusc + F5 impostare A=1, S=1, K=0x74

> **Attenzione:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

- Supporto di più monitor e di monitor ad alta risoluzione. Per i sistemi operativi a sessione singola, HDX 3D Pro supporta dispositivi utente con un massimo di quattro monitor. Gli utenti possono disporre i monitor in qualsiasi configurazione e combinare monitor con diverse risoluzioni e orientamenti. Il numero di monitor è limitato dalle funzionalità della GPU del computer host, dal dispositivo utente e dalla larghezza di banda disponibile. HDX 3D Pro supporta tutte le risoluzioni dei monitor ed è limitato solo dalle funzionalità della GPU sul computer host.
- Risoluzione dinamica. È possibile ridimensionare il desktop virtuale o la finestra dell'applicazione a qualsiasi risoluzione. **Nota**: l'unico metodo supportato per modificare la risoluzione è ridimensionare la finestra della sessione VDA. La modifica della risoluzione dalla sessione VDA (utilizzando **Pannello di controllo > Aspetto** e **personalizzazione > Schermo > Risoluzione dello schermo) non è supportata**.
- Supporto per l'architettura vGPU NVIDIA. HDX 3D Pro supporta schede vGPU NVIDIA. Per informazioni, consultare vGPU NVIDIA per il passthrough della GPU e la condivisione della GPU. La vGPU NVIDIA consente a più VM di avere accesso diretto e simultaneo a una singola GPU fisica, utilizzando gli stessi driver grafici NVIDIA che sono stati distribuiti sui sistemi operativi non virtualizzati.
- Supporto per VMware vSphere e VMware ESX tramite Virtual Direct Graphics Acceleration (vDGA): è possibile utilizzare HDX 3D Pro con vDGA per carichi di lavoro sia RDS che VDI.
- Supporto per VMware vSphere/ESX utilizzando vGPU NVIDIA e AMD MxGPU.
- Supporto per Microsoft HyperV utilizzando DDA (Discrete Device Assignment) in Windows Server 2016.

- Supporto per la grafica dei data center con famiglia di processori Intel Xeon E3. HDX 3D Pro supporta più monitor (fino a 3), cancellazione del contenuto della console, risoluzione personalizzata e frequenza dei fotogrammi elevata con la famiglia di processori Intel supportata. Per ulteriori informazioni, vedere http://www.citrix.com/intel e http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Supporto per AMD RapidFire sulle schede server AMD FirePro serie S. HDX 3D Pro supporta più monitor (fino a 6), cancellazione del contenuto della console, risoluzione personalizzata e frequenza dei fotogrammi elevata. Nota: il supporto HDX 3D Pro per AMD MxGPU (virtualizzazione GPU) funziona solo con VMware vSphere vGPU. Citrix Hypervisor e Hyper-V sono supportati con il passthrough della GPU. Per ulteriori informazioni, vedere Soluzione di virtualizzazione AMD.
- Accesso a un codificatore video ad alte prestazioni per GPU NVIDIA, GPU AMD e processori grafici Intel Iris Pro. Un'impostazione di criterio (attivata per impostazione predefinita) controlla questa funzionalità. La funzione consente l'utilizzo della codifica hardware per la codifica H.264 (ove disponibile). Se tale hardware non è disponibile, il VDA torna alla codifica basata su CPU utilizzando il codec video software. Per ulteriori informazioni, vedere Impostazioni dei criteri di grafica.

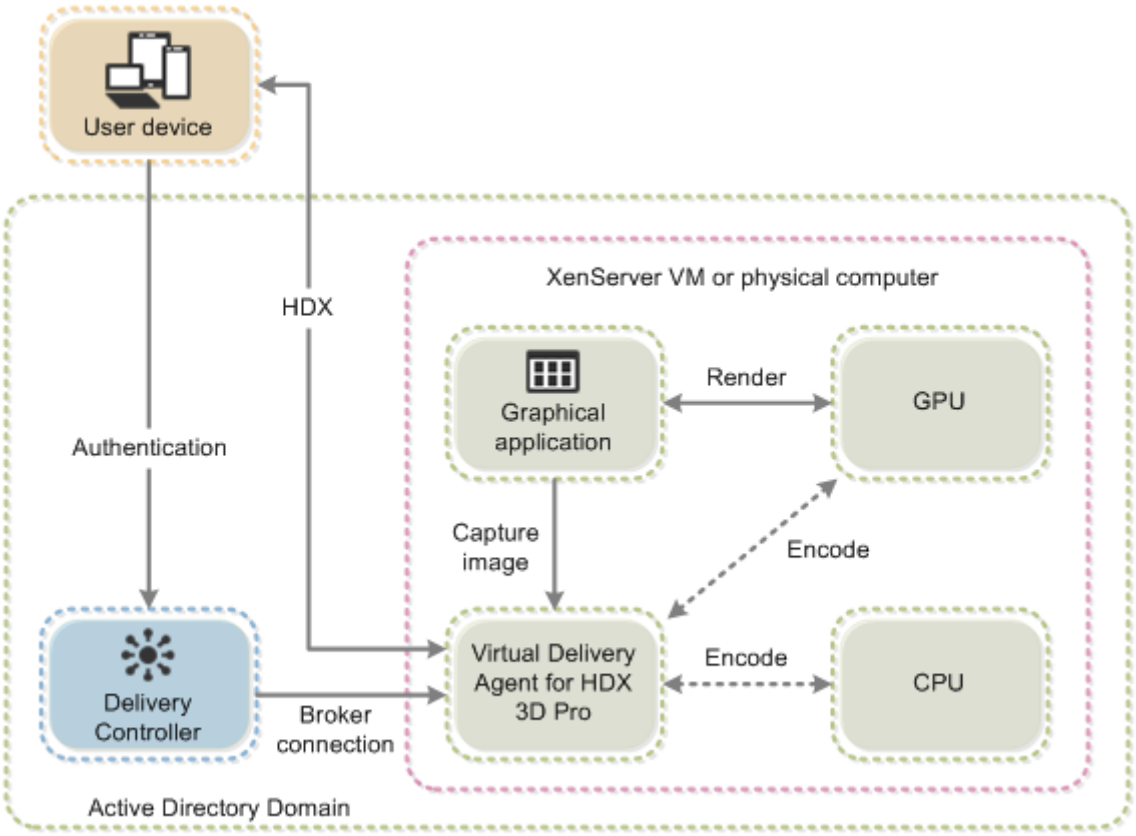
Come illustrato nella figura seguente:

- Quando un utente effettua l'accesso all'app Citrix Workspace e accede all'applicazione virtuale o al desktop, il controller autentica l'utente. Il controller contatta quindi il VDA per HDX 3D Pro per mediare una connessione al computer che ospita l'applicazione grafica.

Il VDA per HDX 3D Pro utilizza l'hardware appropriato sull'host per comprimere le viste del desktop completo o solo dell'applicazione grafica.

- Le viste del desktop o dell'applicazione e le interazioni utente con esse vengono trasmesse tra il computer host e il dispositivo utente. Questa trasmissione avviene tramite una connessione HDX diretta tra l'app Citrix Workspace e il VDA per HDX 3D Pro.




### Ottimizzare l'esperienza utente con HDX 3D Pro

Per utilizzare HDX 3D Pro con più monitor, assicurarsi che il computer host sia configurato con almeno il numero di monitor collegati ai dispositivi utente. I monitor collegati al computer host possono essere fisici o virtuali.

Non collegare un monitor (fisico o virtuale) a un computer host mentre un utente è connesso al desktop virtuale o all'applicazione che fornisce l'applicazione grafica. Così facendo si potrebbe causare instabilità durante la sessione di un utente.

Informare gli utenti che le modifiche della risoluzione del desktop (apportate da loro o da un'applicazione) non sono supportate durante l'esecuzione di una sessione di applicazione grafica. Dopo aver chiuso la sessione dell'applicazione, un utente può modificare la risoluzione della finestra di Desktop Viewer nell'app Citrix Workspace - Preferenze del Desktop Viewer.

Quando più utenti condividono una connessione con larghezza di banda limitata (ad esempio, in una succursale), è consigliabile utilizzare l'impostazione del criterio **Limite larghezza di banda sessione complessiva** per limitare la larghezza di banda disponibile per ciascun utente. L'utilizzo di questa impostazione garantisce che la larghezza di banda disponibile non oscilli notevolmente quando gli utenti accedono e si scollegano. Poiché HDX 3D Pro si regola automaticamente per utilizzare tutta la

larghezza di banda disponibile, grandi variazioni della larghezza di banda disponibile nel corso delle sessioni utente possono influire negativamente sulle prestazioni.

Ad esempio, se 20 utenti condividono una connessione a 60 Mbps, la larghezza di banda disponibile per ciascun utente può variare tra 3 Mbps e 60 Mbps, a seconda del numero di utenti simultanei. Per ottimizzare l'esperienza utente in questo scenario, determinare la larghezza di banda richiesta per utente nei periodi di punta e limitare sempre gli utenti a tale cifra.

Per gli utenti di un mouse 3D, si consiglia di aumentare la priorità del canale virtuale di Reindirizzamento USB generico a 0. Per informazioni sulla modifica della priorità del canale virtuale, vedere l'articolo del Knowledge Center CTX128190.

# Thinwire

May 23, 2023

## Introduzione

Thinwire, parte della tecnologia Citrix HDX, è la tecnologia di visualizzazione predefinita Citrix utilizzata in Citrix Virtual Apps and Desktops.

La tecnologia di visualizzazione remota consente la trasmissione della grafica generata su un computer, in genere attraverso una rete, a un altro computer per la visualizzazione.

Una soluzione di visualizzazione remota che funziona correttamente offre un'esperienza utente altamente interattiva simile a quella di un PC locale. Thinwire realizza questa esperienza utilizzando una serie di tecniche di analisi e compressione delle immagini complesse ed efficienti. Thinwire ottimizza la scalabilità dei server e consuma meno larghezza di banda rispetto ad altre tecnologie di telecomunicazione.

Grazie a questo equilibrio, Thinwire soddisfa la maggior parte dei casi d'uso aziendali generali e viene utilizzato come tecnologia di visualizzazione remota predefinita in Citrix Virtual Apps and Desktops.

## HDX 3D Pro

Nella configurazione predefinita, Thinwire può fornire grafica 3D o altamente interattiva e utilizzare un'unità di elaborazione grafica (GPU), se presente. Tuttavia, si consiglia di attivare la modalità HDX 3D Pro utilizzando i criteri **Optimize for 3D graphics workload** (Ottimizza per i carichi di lavoro con grafica 3D) o **Qualità visiva > Compila per senza perdite** per scenari in cui sono presenti GPU. Questi criteri configurano Thinwire per utilizzare un codec video (H.264 o H.265) per codificare l'

intero schermo utilizzando l'accelerazione hardware se è presente una GPU. Così facendo offre un'esperienza più fluida per la grafica professionale 3D. Per ulteriori informazioni, vedere H.264 Build to lossless (H.264 Compila per senza perdite), HDX 3D Pro e Accelerazione GPU per il sistema operativo Windows a sessione singola.

### Requisiti

Thinwire è ottimizzato per i sistemi operativi moderni, tra cui Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 e Windows 10. Per Windows Server 2008 R2, è consigliata la modalità grafica legacy. Utilizzare i Modelli di criteri Citrix integrati, il sistema operativo legacy ad alta scalabilità server e ottimizzato per il sistema operativo legacy WAN per fornire le combinazioni di impostazioni dei criteri consigliate da Citrix per questi casi d'uso.

> **Nota:**
>
> In questa versione non è supportata la modalità grafica legacy. È inclusa per la compatibilità con le versioni precedenti quando si utilizza XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e le versioni di VDA precedenti.

- L'impostazione dei criteri che guida il comportamento di Thinwire, **Use video codec for compression**, è disponibile nelle versioni di VDA contenute in Citrix Virtual Apps and Desktops 7 1808 o versioni successive e XenApp e XenDesktop 7.6 FP3 e versioni successive. L'opzione **Use video codec when preferred** è l'impostazione predefinita sulle versioni di VDA di Citrix Virtual Apps and Desktops 7 1808 o successive e XenApp e XenDesktop 7.9 e versioni successive.
- Tutte le app Citrix Workspace supportano Thinwire. Alcune app Citrix Workspace potrebbero supportare funzionalità di Thinwire che altre non supportano, ad esempio, grafica a 8 bit o 16 bit per ridurre l'utilizzo della larghezza di banda. Il supporto di tali funzionalità viene negoziato automaticamente dall'app Citrix Workspace.
- Thinwire utilizza più risorse server (CPU, memoria) in scenari multi-monitor e ad alta risoluzione. È possibile ottimizzare la quantità di risorse utilizzate da Thinwire. Tuttavia, l'utilizzo della larghezza di banda potrebbe aumentare di conseguenza.
- In scenari a bassa larghezza di banda o ad alta latenza, è possibile abilitare la grafica a 8 o 16 bit per migliorare l'interattività. La qualità visiva potrebbe essere influenzata, soprattutto con profondità di colore a 8 bit.

### Metodi di codifica

Thinwire può operare in due diverse modalità di codifica a seconda dei criteri e delle funzionalità del client:

- Schermo intero Thinwire H.264 o H.265

- Thinwire con H.264 o H.265 selettivo

La tecnologia remota GDI legacy utilizza il driver remoto XPDM e non un codificatore bitmap Thinwire.

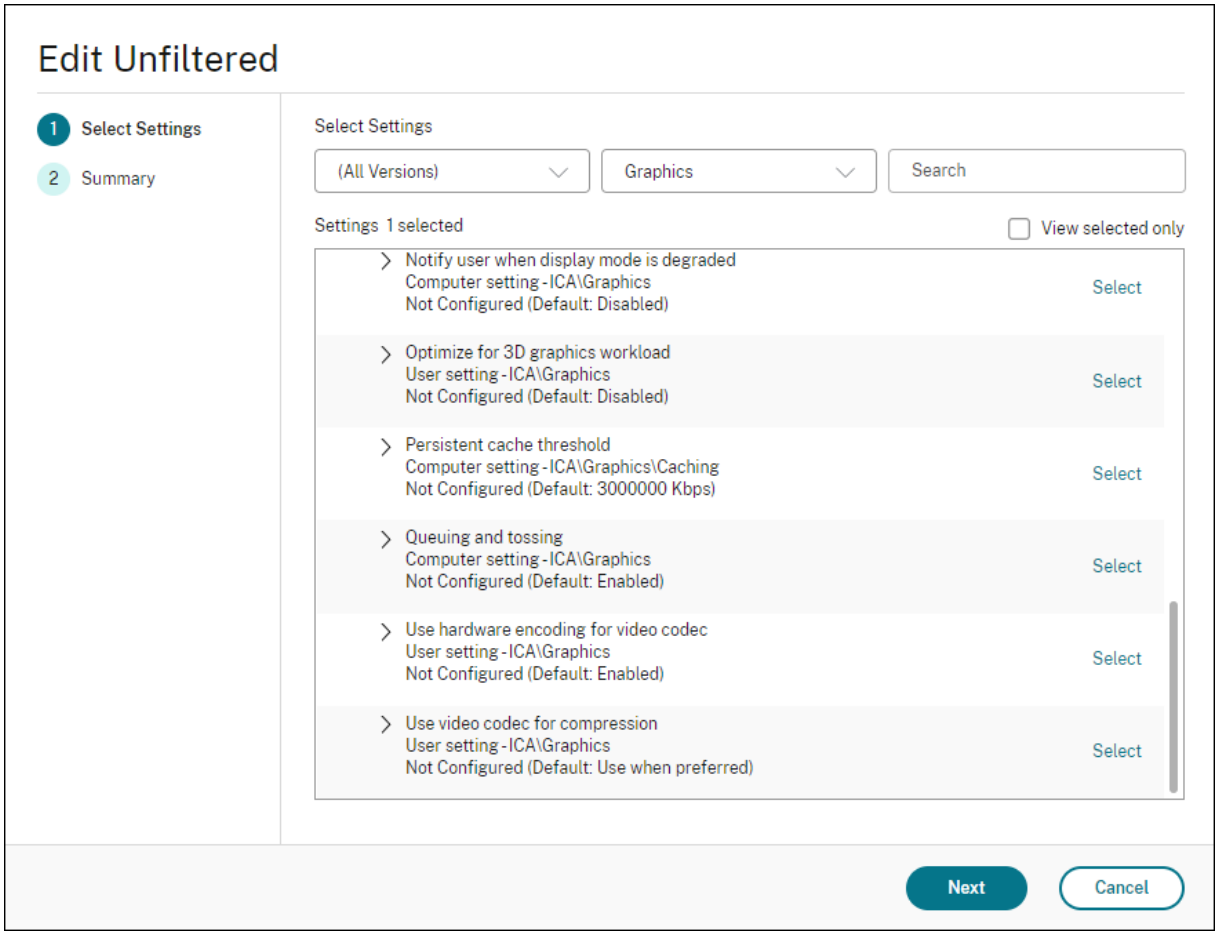
### Configurazione

Thinwire è la tecnologia di visualizzazione remota predefinita.

La seguente impostazione dei criteri di grafica imposta il valore predefinito e fornisce alternative per i diversi casi d'uso:

- Use video codec for compression (Usa codec video per la compressione)
  - **Use video codec when preferred** (Usa video codec quando preferito). Questa è l'impostazione predefinita. Non è richiesta alcuna configurazione aggiuntiva. Mantenere questa impostazione come predefinita garantisce che Thinwire sia selezionato per tutte le connessioni Citrix e sia ottimizzato per scalabilità, larghezza di banda e qualità dell'immagine superiore per i carichi di lavoro desktop tipici. Questo è funzionalmente equivalente a **For actively changing regions** (Per cambiare attivamente le regioni).
- Altre opzioni di questa impostazione di criteri continuano a utilizzare Thinwire con altre tecnologie per diversi casi d'uso. Ad esempio:
  - **For actively changing regions**. La tecnologia di visualizzazione adattiva di Thinwire identifica le immagini in movimento (video, 3D in movimento) e utilizza H.264 o H.265 solo nella parte dello schermo in cui si muove l'immagine.
  - **For the entire screen** (Per l'intero schermo). Fornisce Thinwire con schermo intero H.264 o H.265 per l'ottimizzazione migliorando l'esperienza utente e la larghezza di banda in caso di utilizzo intensivo della grafica 3D. Nel caso di H.264 4:2:0 (il criterio **Visually lossless** (Visivamente senza perdite) è disabilitato), l'immagine finale non è a pixel perfetto (senza perdite) e potrebbe non essere adatta per determinati scenari. In questi casi, prendere in considerazione l'utilizzo alternativo di H.264 Build to lossless (H.264 Compila per senza perdite).




È possibile utilizzare diverse altre impostazioni dei criteri, incluse le seguenti impostazioni dei criteri di visualizzazione visiva per ottimizzare le prestazioni della tecnologia di visualizzazione remota. Thinwire li supporta tutti.

- Profondità di colore preferita per grafiche semplici
- Target frame rate (Frequenza fotogrammi target)
- Qualità visiva

Per ottenere le combinazioni di impostazioni dei criteri per diversi casi di utilizzo aziendale consigliate da Citrix, utilizzare i Modelli di criteri Citrix incorporati. I modelli **High Server Scalability** (Elevata scalabilità del server) e **Very High Definition User Experience** (Esperienza utente ad altissima definizione) utilizzano entrambi Thinwire con la combinazione ottimale di impostazioni dei criteri per le priorità dell'organizzazione e le aspettative degli utenti.

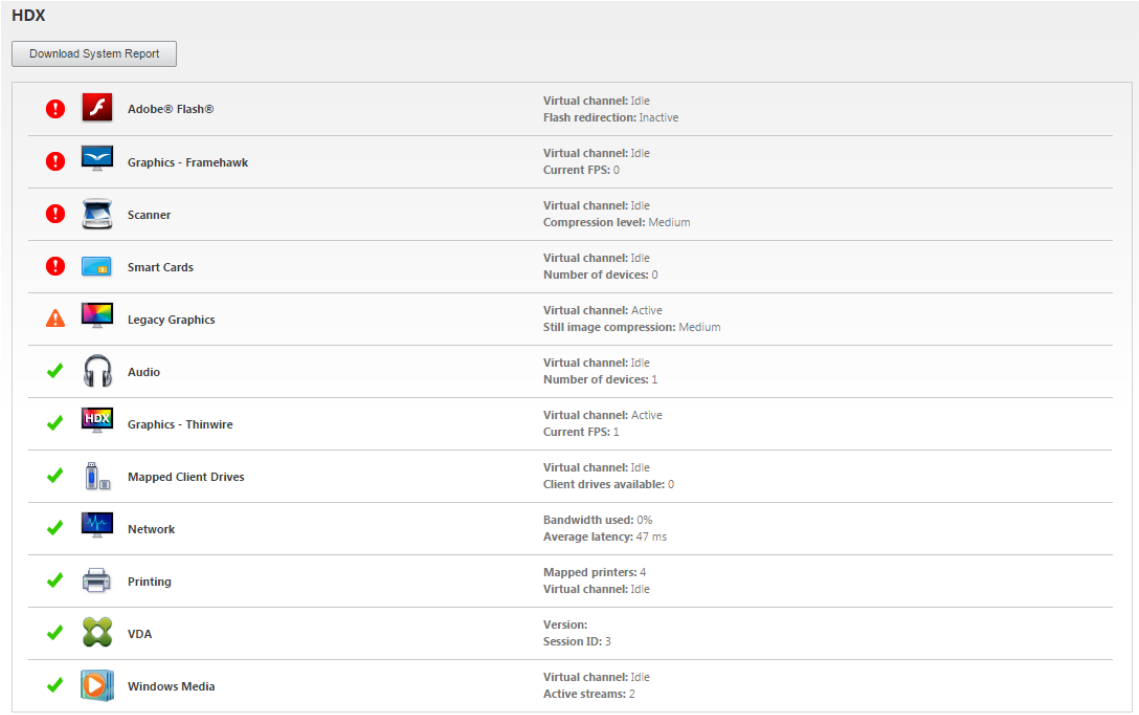
### Monitorare Thinwire

È possibile monitorare l'utilizzo e le prestazioni di Thinwire da Citrix Director. La vista dei dettagli del canale virtuale HDX contiene informazioni utili per la risoluzione dei problemi e il monitoraggio di

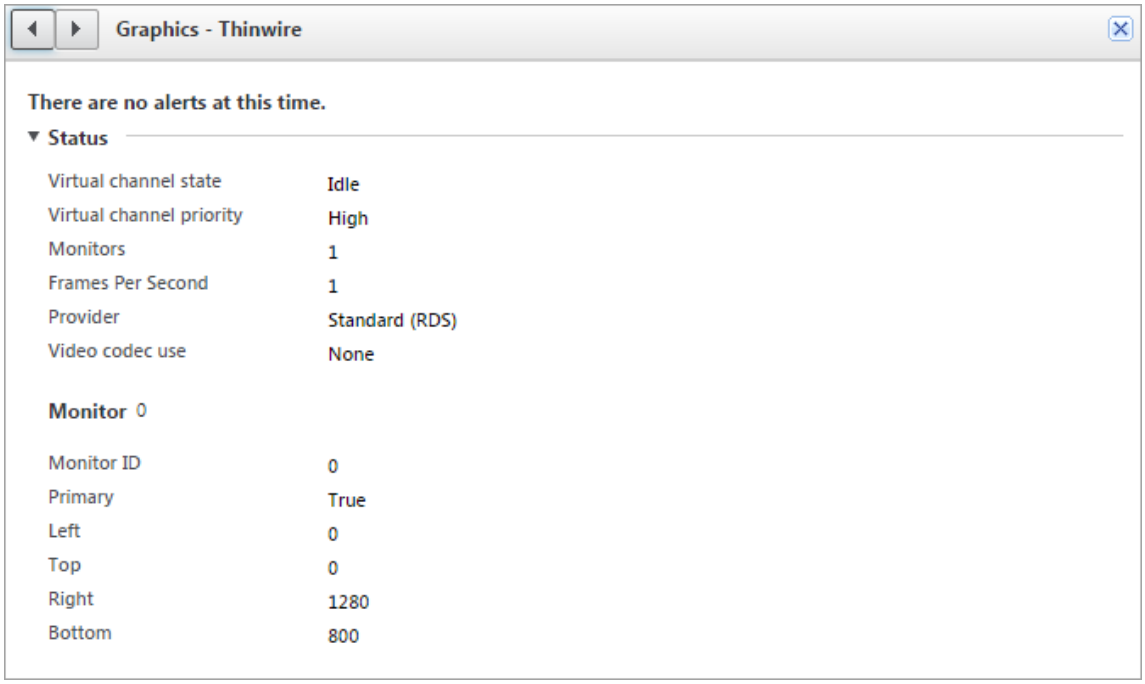
Thinwire in qualsiasi sessione. Per visualizzare le metriche relative a Thinwire:

1. In Director cercare un utente, un computer o un endpoint, aprire una sessione attiva e fare clic su **Dettagli**. In alternativa, è possibile selezionare **Filtri > Sessioni > Tutte le sessioni**, aprire una sessione attiva e fare clic su **Dettagli**.
2. Scorrere verso il basso fino al pannello **HDX**.




3. Selezionare **Graphics - Thinwire**.




### Codec di compressione senza perdite (MDRLE)

In una tipica sessione desktop, la maggior parte delle immagini è grafica semplice o contiene regioni di testo. Thinwire determina la posizione di queste regioni e seleziona queste aree per la codifica senza perdita di dati utilizzando il codec 2DRLE. Sul lato client dell'app Citrix Workspace, questi elementi vengono decodificati utilizzando il decodificatore 2DRLE lato app Citrix Workspace per la visualizzazione delle sessioni.

In XenApp e XenDesktop 7.17, abbiamo aggiunto un codec MDRLE con rapporto di compressione più elevato che consuma meno larghezza di banda nelle sessioni desktop tipiche rispetto al codec 2DRLE. Questo nuovo codec non influisce sulla scalabilità del server.

La larghezza di banda inferiore di solito comporta un miglioramento dell'interattività delle sessioni (specialmente su collegamenti condivisi o vincolati) e una riduzione dei costi. Ad esempio, il consumo di larghezza di banda previsto quando si utilizza il codec MDRLE è di circa il 10-15% in meno rispetto a XenApp e XenDesktop 7.15 LTSR per i carichi di lavoro tipici di Office.

Non è richiesta configurazione per il codec MDRLE. Se l'app Citrix Workspace supporta la decodifica MDRLE, il VDA utilizza la codifica VDA MDRLE e la decodifica MDRLE dell'app Citrix Workspace. Se l'app Citrix Workspace non supporta la decodifica MDRLE, il VDA effettua automaticamente il fallback alla codifica 2DRLE.

**Requisiti di MDRLE:**

- VDA Citrix Virtual Apps and Desktops versione minima 7 1808.
- VDA XenApp e XenDesktop versione minima 7.17.

- App Citrix Workspace per Windows versione minima 1808
- Citrix Receiver per Windows versione minima 4.11

## Modalità progressiva

Citrix Virtual Apps and Desktops 1808 ha introdotto la modalità progressiva che è abilitata per impostazione predefinita. In condizioni di rete vincolate (impostazione predefinita: larghezza di banda <2 Mbps o latenza >200 ms), Thinwire ha aumentato la compressione del testo e delle immagini statiche per migliorare l'interattività durante l'attività dello schermo. Il testo e le immagini fortemente compressi diventano quindi progressivamente più nitidi, in modo casuale, quando l'attività dello schermo si interrompe. Questo tipo di compressione e di aumento della nitidezza migliorano l'interattività generale, riducendo al contempo l'efficienza della cache e aumentando l'utilizzo della larghezza di banda.

A partire da Citrix Virtual Apps and Desktops 1906, la modalità progressiva è disabilitata per impostazione predefinita. Ora adottiamo un approccio diverso. La qualità delle immagini fisse è ora basata sulle condizioni della rete e fluttua tra un valore minimo e massimo predefiniti per ogni impostazione della **qualità visiva**. Poiché non esiste una fase esplicita di nitidezza, Thinwire ottimizza la distribuzione delle immagini e mantiene l'efficienza della cache, offrendo al contempo quasi tutti i vantaggi della modalità progressiva.

### Modifica del comportamento in modalità progressiva

È possibile modificare lo stato della modalità progressiva con la chiave del Registro di sistema. Per informazioni, vedere Modalità progressiva nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## H.264 Build to lossless (H.264 Compila per senza perdite)

**Compila per senza perdite** è una speciale configurazione di Thinwire che ottimizza la distribuzione grafica per l'interattività e la qualità dell'immagine finale. È possibile attivare questa impostazione impostando il criterio **Qualità visiva** su **Compila per senza perdite**.

Compila per senza perdite comprime lo schermo utilizzando H.264 (o H.265) durante l'attività dello schermo e lo rende più nitido fino a pixel perfetti (senza perdite) quando l'attività si interrompe. La qualità dell'immagine H.264 (o H.265) si adatta alle risorse disponibili per mantenere la frequenza dei fotogrammi migliore possibile. La fase di aumento della nitidezza viene eseguita gradualmente, dando una risposta immediata se l'utente inizia l'attività sullo schermo poco dopo l'inizio della fase. Ad esempio, selezionando un modello e ruotandolo.

H.264 **Compila per senza perdite** offre tutti i vantaggi di H.264 o H.265 a schermo intero, inclusa l'accelerazione hardware, ma con l'ulteriore vantaggio di uno schermo finale garantito senza perdita di dati. Questo è fondamentale per i carichi di lavoro di tipo 3D che richiedono un'immagine finale con pixel perfetti. Ad esempio, nella manipolazione della diagnostica per immagini medicale. Inoltre, H.264 **Compila per senza perdite** utilizza meno risorse rispetto allo schermo intero H.264 4:4:4. Di conseguenza, l'uso di **Compila per senza perdite** di solito si traduce in una frequenza di fotogrammi più elevata rispetto a Visivamente senza perdite H.264 4:4:4.

> **Nota:**
>
> Oltre al criterio **Qualità visiva**, impostare il criterio **Use video codec** (Usa codec video) su **Use when preferred** (Usa quando preferito) (impostazione predefinita) o **For actively changing regions** (Per cambiare attivamente le regioni). È possibile ripristinare la condizione senza H.264 Compila per senza perdite impostando il criterio **Use video codec** su **Do not use video codec** (Non utilizzare codec video). In questo modo le immagini in movimento vengono codificate con JPEG anziché H.264 (o H.265).

## Filigrana di sessione basata su testo

October 6, 2022

Le filigrane di sessione basate su testo aiutano a scoraggiare e abilitare il furto dei dati di tracciabilità. Queste informazioni tracciabili vengono visualizzate sul desktop della sessione come deterrente per coloro che utilizzano fotografie e acquisizioni dello schermo per rubare i dati. È possibile specificare una filigrana che sia uno strato di testo, che viene visualizzato sull'intera schermata della sessione senza modificare il contenuto del documento originale. Le filigrane di sessione basate su testo richiedono il supporto VDA.

> **Importante:**
>
> l'applicazione di filigrana di sessione basata su testo non è una funzionalità di sicurezza. La soluzione non impedisce completamente il furto di dati, ma funge da deterrente e fornisce un certo livello di tracciabilità. Sebbene non garantiamo la completa tracciabilità delle informazioni quando si utilizza questa funzione, si consiglia di combinare questa funzionalità con altre soluzioni di sicurezza, come necessario.

La filigrana di sessione è testo e viene applicata alla sessione che viene consegnata all'utente. La filigrana di sessione contiene informazioni per il rilevamento del furto di dati. I dati più importanti sono l'identità dell'utente che ha effettuato l'accesso alla sessione corrente in cui è stata acquisita l'immagine dello schermo. Per tenere traccia della perdita di dati in modo più efficace, includere

altre informazioni come l'indirizzo del protocollo Internet del server o del client e un tempo di connessione.

Per regolare l'esperienza utente, utilizzare le Impostazioni dei criteri per la Filigrana di sessione per configurare il posizionamento e l'aspetto della filigrana sullo schermo.

**Requisiti:**

Virtual Delivery Agent:

Sistema operativo multisessione 7.17
Sistema operativo a sessione singola 7.17

**Limitazioni:**

- Le filigrane di sessione non sono supportate nelle sessioni in cui vengono utilizzate funzionalità quali Accesso alle app locali, reindirizzamento dei supporti Windows, MediaStream, reindirizzamento dei contenuti del browser e reindirizzamento video HTML5. Per utilizzare la filigrana di sessione, assicurarsi che queste funzionalità siano disabilitate.
- La filigrana di sessione non è supportata e non viene visualizzata se la sessione è in esecuzione in modalità hardware accelerata a schermo intero (codifica H.264 o H.265 a schermo intero).
- Se si impostano questi criteri HDX, le impostazioni della filigrana non hanno effetto e non viene visualizzata una filigrana nella visualizzazione della sessione.

**Use hardware encoding for video codec** (Usa codifica hardware per il codec video) su **Enabled**
**Use video codec for compression** (Usa codec video per la compressione) su **For the entire screen** (Per l'intero schermo)

- Se si impostano questi criteri HDX, il comportamento non è determinato e la filigrana potrebbe non essere visualizzata.

  **Use hardware encoding for video codec** su **Enabled**
  **Use video codec for compression** su **Use video codec when preferred** (Usa video codec quando preferito)

  Per garantire la visualizzazione della filigrana, impostare **Use hardware encoding for video codec** su **Disabled** oppure impostare **Use video codec for compression** su **For actively changing regions** (Per cambiare attivamente le regioni) o **Do not use video codec** (Non utilizzare codec video).
- La filigrana di sessione supporta solo la modalità grafica Thinwire.
- Se si utilizza la funzione Registrazione sessione, la sessione registrata non include la filigrana.
- Se si utilizza l'assistenza remota di Windows, la filigrana non viene visualizzata.

- Se un utente preme il tasto **Stamp** per catturare lo schermo, la schermata catturata sul lato VDA non include le filigrane. Si consiglia di adottare misure per evitare che l'immagine acquisita venga copiata.

## Contenuti multimediali

October 5, 2022

Lo stack tecnologico HDX supporta la distribuzione di applicazioni multimediali attraverso due approcci complementari:

- Distribuzioni multimediali di rendering lato server
- Reindirizzamento multimediale di rendering lato client

Questa strategia garantisce la possibilità di offrire una gamma completa di formati multimediali, con un'ottima esperienza utente, ottimizzando al contempo la scalabilità dei server per ridurre il costo per utente.

Con la distribuzione multimediale con rendering server, i contenuti audio e video vengono decodificati e renderizzati sul server Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) dall'applicazione. Il contenuto viene quindi compresso e distribuito mediante il protocollo ICA all'app Citrix Workspace sul dispositivo dell'utente. Questo metodo fornisce il più alto tasso di compatibilità con varie applicazioni e formati multimediali. Poiché l'elaborazione video richiede un uso intensivo dell'elaborazione, la distribuzione multimediale con rendering del server beneficia notevolmente dell'accelerazione hardware integrata. Ad esempio, il supporto di DirectX Video Acceleration (DXVA) alleggerisce la CPU eseguendo la decodifica H.264 in hardware separato. Le tecnologie Intel Quick Sync, AMD RapidFire e NVIDIA NVENC forniscono codifica H.264 con accelerazione hardware.

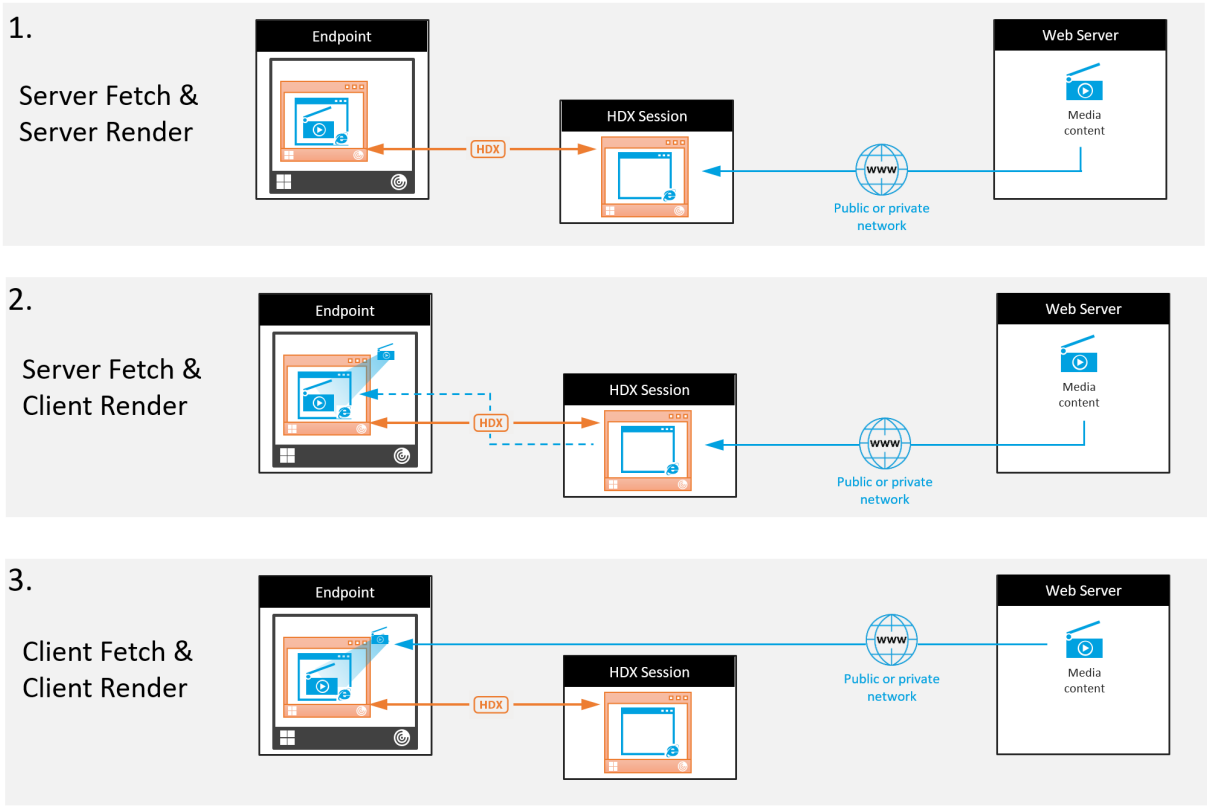
Poiché la maggior parte dei server non offre alcuna accelerazione hardware per la compressione video, la scalabilità del server viene influenzata negativamente se tutta l'elaborazione video viene eseguita sulla CPU del server. È possibile mantenere un'elevata scalabilità del server, reindirizzando molti formati multimediali al dispositivo utente per il rendering locale.

- Il reindirizzamento di Windows Media consente di alleggerire il server per un'ampia varietà di formati multimediali generalmente associati a Windows Media Player.
- Il video HTML5 è diventato di uso generale e Citrix ha introdotto una tecnologia di reindirizzamento per questo tipo di contenuti. Si consiglia il reindirizzamento dei contenuti del browser per siti Web che utilizzano HTML5, HLS, DASH o WebRTC.
- È possibile applicare le tecnologie generali di reindirizzamento dei contatti da host a client e l'accesso delle app locali ai contenuti multimediali.

Mettendo insieme queste tecnologie, se non si configura il reindirizzamento, HDX esegue il rendering lato server.
Se si configura il reindirizzamento, HDX utilizza Server Fetch e Client Render o Client Fetch e Client Render. Se tali metodi non riescono, HDX torna al rendering lato server in base alle esigenze ed è soggetto ai criteri di prevenzione del fallback.

### Esempi di scenari




**Scenario 1. (Server Fetch e Server Rendering):**

1. Il server recupera il file multimediale dalla sua origine, lo decodifica e quindi presenta il contenuto a una periferica audio o a un dispositivo di visualizzazione.
2. Il server estrae l'immagine o l'audio presentati rispettivamente dal dispositivo di visualizzazione o dalla periferica audio.
3. Il server lo comprime facoltativamente e quindi lo trasmette al client.

Questo approccio comporta un costo elevato in termini di CPU, un costo elevato di larghezza di banda (se l'immagine/audio estratto non è compresso in modo efficiente) e ha una bassa scalabilità del server.

I canali virtuali Thinwire e Audio gestiscono questo approccio. Il vantaggio di questo approccio è che riduce i requisiti hardware e software per i client. Utilizzando questo approccio la decodifica avviene

sul server e funziona per una più ampia varietà di dispositivi e formati.

**Scenario 2. (Server Fetch e Client Render):**

Questo approccio si basa sulla possibilità di intercettare il contenuto multimediale prima che venga decodificato e presentato al dispositivo audio o di visualizzazione. Il contenuto audio/video compresso viene invece inviato al client dove viene quindi decodificato e presentato localmente. Il vantaggio di questo approccio è che vengono scaricati sui dispositivi client, risparmiando cicli della CPU sul server.

Tuttavia, introduce anche alcuni requisiti hardware e software aggiuntivi per il client. Il client deve essere in grado di decodificare ciascun formato che potrebbe ricevere.

**Scenario 3. (Client Fetching e Client Rendering):**

Questo approccio si basa sulla possibilità di intercettare l'URL del contenuto multimediale prima che venga recuperato dall'origine. L'URL viene inviato al client in cui il contenuto multimediale viene recuperato, decodificato e presentato localmente. Questo approccio è concettualmente semplice. Il suo vantaggio è che risparmia sia cicli della CPU sul server che larghezza di banda, perché il server invia solo comandi di controllo. Tuttavia, il contenuto multimediale non è sempre accessibile ai client.

**Framework e piattaforma:**

I sistemi operativi a sessione singola (Windows, Mac OS X e Linux) forniscono framework multimediali che consentono lo sviluppo più rapido di applicazioni multimediali. Questa tabella elenca alcuni dei framework multimediali più popolari. Ogni framework divide l'elaborazione multimediale in più fasi e utilizza un'architettura basata su pipeline.

| Framework | Piattaforma |
| --- | --- |
| DirectShow | Windows (98 e versioni successive) |
| Media Foundation | Windows (Vista e versioni successive) |
| Gstreamer | Linux |
| Quicktime | Mac OS X |

## Supporto a doppio hop con tecnologie di reindirizzamento dei supporti

| | |
| --- | --- |
| Reindirizzamento audio | No |

| | | |
|---|---|---|
| | Browser content redirection (Reindirizzamento del contenuto del browser) | No |
| | Reindirizzamento webcam HDX | Sì |
| | Reindirizzamento video HTML5 | Sì |
| | Reindirizzamento di Windows Media | Sì |

## Funzionalità audio

November 21, 2023

È possibile configurare e aggiungere le seguenti impostazioni dei criteri Citrix a un criterio che ottimizza le funzionalità audio HDX. Per i dettagli sull'utilizzo, nonché le relazioni e le dipendenze con altre impostazioni dei criteri, vedere Impostazioni dei criteri audio, Impostazioni dei criteri di larghezza di banda e Impostazioni dei criteri per le connessioni multi-flusso.

> **Importante:**
>
> Si consiglia di fornire l'audio utilizzando UDP (User Datagram Protocol) anziché TCP. Solo Windows Virtual Delivery Agent (VDA) supporta l'audio su UDP.
>
> La crittografia audio UDP tramite DTLS è disponibile solo tra Citrix Gateway e l'app Citrix Workspace. Pertanto, a volte potrebbe essere preferibile utilizzare il trasporto TCP. TCP supporta la crittografia TLS end-to-end dal VDA all'app Citrix Workspace.

### Audio quality (Qualità audio)

In generale, una qualità audio più elevata consuma più larghezza di banda e prevede un maggiore utilizzo della CPU del server, inviando più dati audio ai dispositivi utente. La compressione audio consente di bilanciare la qualità del suono rispetto alle prestazioni generali della sessione. Utilizzare le impostazioni dei criteri Citrix per configurare i livelli di compressione da applicare ai file audio.

Per impostazione predefinita, l'opzione **Audio quality policy (Criteri di qualità audio)** è impostata su High - high definition audio (Elevata - Audio ad alta definizione) quando si utilizza il trasporto TCP. Il criterio è impostato su Medium - optimized-for-speech (Medio - ottimizzato per il riconoscimento vocale) quando viene utilizzato il trasporto UDP (opzione consigliata). L'impostazione **High Definition**

**audio (Audio ad alta definizione)** fornisce audio stereo ad alta fedeltà, ma consuma più larghezza di banda rispetto ad altre impostazioni di qualità. Non utilizzare questa qualità audio per applicazioni di chat vocale o chat video non ottimizzate (come i softphone). Il motivo è che potrebbe introdurre nel percorso audio una latenza che non è adatta per le comunicazioni in tempo reale. Si consiglia di impostare il criterio su Optimized for speech (Ottimizzato per il parlato) per l'audio in tempo reale, indipendentemente dal protocollo di trasporto selezionato.

Quando la larghezza di banda è limitata, ad esempio nelle connessioni via satellite o dial-up, la riduzione della qualità audio a **Low (Bassa)** consuma la minore larghezza di banda possibile. In questo caso, creare criteri separati per gli utenti con connessioni a larghezza di banda ridotta in modo che non vi siano ripercussioni negative per gli utenti con connessioni a larghezza di banda elevata.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

Linee guida sulla larghezza di banda per la riproduzione e la registrazione audio:

- Alta qualità (impostazione predefinita)
  - Velocità in bit: ~100 kbps (min 75, max 175 kbps) per la riproduzione/~70 kbps per l'acquisizione del microfono
  - Numero di canali: 2 (stereo) per la riproduzione, 1 (mono) per l'acquisizione del microfono
  - Frequenza: 44100 Hz
  - Profondità di bit: 16 bit
- Qualità media (consigliata per VoIP)
  - Velocità in bit: ~16 kbps (min 20, max 40 kbps) per la riproduzione, ~16 kbps per l'acquisizione del microfono
  - Numero di canali: 1 (mono) sia per la riproduzione che per l'acquisizione
  - Frequenza: 16.000 Hz (banda larga)
  - Profondità di bit: 16 bit
- Bassa qualità
  - Velocità in bit: ~11 kbps (min 10; max 25 kbps) per la riproduzione, ~11 kbps per l'acquisizione del microfono
  - Numero di canali: 1 (mono) sia per la riproduzione che per l'acquisizione
  - Frequenza: 8000 Hz (banda stretta)
  - Profondità di bit: 16 bit

### Client audio redirection (Reindirizzamento audio client)

Per consentire agli utenti di ricevere audio da un'applicazione su un server tramite altoparlanti o altri dispositivi audio sul dispositivo utente, lasciare l'impostazione **Client audio redirection (Reindiriz-**

**zamento audio client)** su **Allowed (Consentito)**. Questa è l'impostazione predefinita.

La mappatura audio client comporta un carico extra sui server e sulla rete. Tuttavia, il divieto di reindirizzamento audio client disabilita tutte le funzionalità audio HDX.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio. Ricordarsi di abilitare le impostazioni audio client sul dispositivo utente.

### Client microphone redirection (Reindirizzamento microfono client)

Per consentire agli utenti di registrare audio utilizzando dispositivi di input come i microfoni sul dispositivo utente, lasciare l'impostazione **Client microphone redirection (Reindirizzamento microfono client)** sul valore predefinito Allowed (Consentito).

Per motivi di sicurezza, i dispositivi utente avvisano gli utenti quando i server di cui non si fidano tentano di accedere ai microfoni. Gli utenti possono scegliere di accettare o rifiutare l'accesso prima di utilizzare il microfono. Gli utenti possono disabilitare questo avviso sull'app Citrix Workspace.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

### Audio Plug N Play

L'impostazione dei criteri Audio Plug N Play consente o impedisce l'utilizzo di più dispositivi audio per registrare e riprodurre suoni. Questa impostazione è **abilitata** per impostazione predefinita. Audio Plug N Play consente di riconoscere i dispositivi audio. I dispositivi vengono riconosciuti anche se non sono collegati solo dopo l'avvio della sessione utente.

Questa impostazione si applica solo alle macchine con sistema operativo Windows multisessione.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri audio.

### Limite di larghezza di banda di reindirizzamento audio e percentuale limite di larghezza di banda di reindirizzamento audio

L'impostazione del criterio relativo al limite della larghezza di banda di reindirizzamento audio specifica la larghezza di banda massima (in kilobit al secondo) per la riproduzione e la registrazione di audio in una sessione.

L'impostazione Audio redirection bandwidth limit percent (Percentuale limite della larghezza di banda di reindirizzamento audio) specifica la larghezza di banda massima per il reindirizzamento audio come percentuale della larghezza di banda totale disponibile.

Per impostazione predefinita, per entrambe le impostazioni viene specificato zero (nessun massimo). Se entrambe le impostazioni sono configurate, viene utilizzata quella con il limite di larghezza di banda più basso.

Per i dettagli sulle impostazioni, vedere Impostazioni dei criteri di larghezza di banda. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

### Trasporto in tempo reale dell'audio su UDP e intervallo delle porte UDP audio

Per impostazione predefinita, è consentito il trasporto in tempo reale dell'audio su UDP (User Datagram Protocol), se selezionato al momento dell'installazione. Si apre una porta UDP sul server per le connessioni che utilizzano il trasporto in tempo reale dell'audio su UDP. In caso di congestione della rete o perdita di pacchetti, si consiglia di configurare UDP/RTP per l'audio per garantire la migliore esperienza utente possibile. Per l'audio in tempo reale come applicazioni softphone, l'audio UDP è preferibile a EDT. UDP consente la perdita di pacchetti senza ritrasmissione, garantendo che non venga aggiunta alcuna latenza nelle connessioni con perdita di pacchetti elevata.

> **Importante:**
>
> Quando Citrix Gateway non è nel percorso, i dati audio trasmessi con UDP non vengono crittografati. Se Citrix Gateway è configurato per accedere alle risorse di Citrix Virtual Apps and Desktops, il traffico audio tra il dispositivo endpoint e Citrix Gateway è protetto utilizzando il protocollo DTLS.

L'intervallo di porte UDP audio specifica l'intervallo di numeri di porta utilizzato dal VDA di Windows per scambiare i dati dei pacchetti audio con il dispositivo utente.

Per impostazione predefinita, l'intervallo è compreso tra 16500 e 16509.

Per informazioni sulle impostazioni relative ad Audio over UDP real-time transport (Audio con trasporto UDP in tempo reale), vedere Impostazioni dei criteri audio. Per informazioni dettagliate sull'intervallo di porte UDP audio, vedere Impostazioni dei criteri di connessione multi-stream. Ricordarsi di abilitare le impostazioni audio del client sul dispositivo utente.

L'audio su UDP richiede il VDA di Windows. Per i criteri supportati su Linux VDA, vedere Elenco di supporto dei criteri.

### Criteri di impostazione audio per i dispositivi utente

1. Caricare i modelli di criteri di gruppo seguendo Configurazione del modello amministrativo Oggetto Criteri di gruppo.
2. Nell'Editor Criteri di gruppo espandere **Modelli amministrativi > Citrix Components (Componenti Citrix) > Citrix Workspace > Citrix Components (Esperienza utente)**.

3. Per **Client audio settings (Impostazioni audio client)**, selezionare **Not Configured** (Non configurate), **Enabled (Abilitate)**o **Disabled (Disabilitate)**.

   - **Not Configured (Non configurate)**. Per impostazione predefinita, il reindirizzamento audio è abilitato utilizzando l'audio di alta qualità o le impostazioni audio personalizzate precedentemente configurate.
   - **Enabled** (Abilitato). Abilita il reindirizzamento audio utilizzando le opzioni selezionate.
   - **Disabled.** Disabilita il reindirizzamento audio.

4. Se si seleziona **Enabled (Abilitate)**, scegliere una qualità audio. Per l'audio UDP, utilizzare **Medium (Medio)** (impostazione predefinita).
5. Solo per l'audio UDP, selezionare **Enable Real-Time Transport (Abilita trasporto in tempo reale)**, quindi impostare l'intervallo di porte in ingresso da aprire nel firewall locale di Windows.
6. Per utilizzare l'audio UDP con Citrix Gateway, selezionare **Allow Real-Time Transport Through gateway (Consenti trasporto in tempo reale tramite gateway)**. Configurare Citrix Gateway con DTLS. Per ulteriori informazioni, vedere questo articolo.

In qualità di amministratore, se non si dispone del controllo sui dispositivi endpoint per apportare queste modifiche, utilizzare gli attributi default.ica di StoreFront per abilitare l'audio UDP. Ad esempio, per i dispositivi BYOD o i computer di casa.

1. Sul computer StoreFront, aprire C:\inetpub\wwwroot\Citrix\<Store Name>\App_Data\default.ica con un editor come Blocco note.
2. Inserire le voci seguenti nella sezione [Application] (Applicazione).

   ; This text enables Real-Time Transport

   EnableRtpAudio=true

   ; This text allows Real-Time Transport Through gateway

   EnableUDPThroughGateway=true

   ; This text sets audio quality to Medium

   AudioBandwidthLimit=1

   ; UDP Port range

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

Se si abilita l'audio UDP (User Datagram Protocol) modificando default.ica, l'audio UDP è abilitato per tutti gli utenti che utilizzano tale archivio.

### Evitare l'eco durante le conferenze multimediali

Gli utenti delle conferenze audio o video potrebbero sentire un'eco. Gli echi di solito si verificano quando altoparlanti e microfoni sono troppo vicini l'uno all'altro. Per questo motivo, si consiglia l'uso di cuffie per le conferenze audio e video.

HDX fornisce un'opzione di cancellazione dell'eco (attivata per impostazione predefinita) che riduce al minimo qualsiasi eco. L'efficacia della cancellazione dell'eco è sensibile alla distanza tra gli altoparlanti e il microfono. Assicurarsi che i dispositivi non siano troppo vicini o troppo lontani l'uno dall'altro.

È possibile modificare un'impostazione del Registro di sistema per disabilitare l'annullamento dell'eco. Per informazioni, vedere Evitare l'eco durante le conferenze multimediali nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Softphone

Un softphone è un software che funge da interfaccia telefonica. È possibile utilizzare un softphone per effettuare chiamate via Internet da un computer o un altro dispositivo smart. Utilizzando un softphone, è possibile comporre numeri di telefono ed eseguire altre funzioni correlate al telefono utilizzando uno schermo.

Citrix Virtual Apps and Desktops supporta diverse alternative per la distribuzione di softphone.

- **Modalità di controllo**. Il softphone ospitato controlla un telefono fisico. In questa modalità, nessun traffico audio passa attraverso il server di Citrix Virtual Apps and Desktops.
- **Supporto per softphone ottimizzato HDX RealTime (consigliato)**. Il motore multimediale viene eseguito sul dispositivo utente e il traffico VoIP scorre peer-to-peer. Per esempi, vedere:
  - Ottimizzazione di HDX per Microsoft Teams
  - HDX RealTime Optimization Pack, che ottimizza la distribuzione di Microsoft Skype for Business
  - Cisco Jabber Softphone per VDI (precedentemente noto come VXME)
  - Cisco Webex Meetings per VDI
  - Avaya VDI Equinox (già noto come VDI Communicator)
  - Plugin Zoom VDI
  - Genesys PureEngage Cloud
  - Dispositivo di dettatura Nuance Dragon PowerMic
- **Accesso alle app locali**. Una funzionalità di Citrix Virtual Apps and Desktops e di Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops) che consente a un'applicazione come un softphone di venire eseguita localmente sul dispositivo utente Windows, pur apparendo perfettamente integrata con il relativo desktop virtuale/pubblicato. Questa funzionalità consente

l'offload di tutte le elaborazioni audio sul dispositivo dell'utente. Per ulteriori informazioni, vedere Accesso alle app locali e reindirizzamento URL.

- **Supporto per softphone generico HDX RealTime.** Voice over Internet Protocol-over-ICA.

***Supporto per softphone generico***

Supporto per softphone generico, consente di ospitare un softphone non modificato su XenApp o XenDesktop nel centro dati. Il traffico audio passa attraverso il protocollo Citrix ICA (preferibilmente utilizzando UDP/RTP) e raggiunge il dispositivo utente che esegue l'app Citrix Workspace.

Il supporto generico di softphone è una funzionalità di HDX RealTime. Questo approccio alla distribuzione di softphone è particolarmente utile quando:

- Non è disponibile una soluzione ottimizzata per la distribuzione del softphone e l'utente non utilizza un dispositivo Windows in cui è possibile utilizzare l'accesso alle app locali.
- Il motore multimediale necessario per la distribuzione ottimizzata del softphone non è installato sul dispositivo utente o non è disponibile per la versione del sistema operativo in esecuzione sul dispositivo utente. In questo scenario, Generic HDX RealTime fornisce una valida soluzione di fallback.

Vi sono due considerazioni da fare sulla distribuzione di softphone utilizzando Citrix Virtual Apps and Desktops:

- Come l'applicazione softphone viene distribuita al desktop virtuale/pubblicato.
- Come viene inviato l'audio da e verso le cuffie, il microfono e gli altoparlanti dell'utente o il telefono USB.

Citrix Virtual Apps and Desktops include numerose tecnologie per supportare la distribuzione generica di softphone:

- Codec ottimizzato per il parlato per la codifica rapida dell'audio in tempo reale e l'efficienza della larghezza di banda.
- Stack audio a bassa latenza.
- Buffer del jitter lato server per migliorare l'audio quando la latenza di rete è variabile.
- Tagging dei pacchetti (DSCP e WMM) per la qualità del servizio.
  - Tagging DSCP per pacchetti RTP (Livello 3)
  - Tagging WMM per Wi-Fi

Anche le versioni dell'app Citrix Workspace per Windows, Linux, Chrome e Mac possono utilizzare VoIP. L'app Citrix Workspace per Windows offre le seguenti funzionalità:

- Buffer del jitter lato client: assicura un audio fluido anche quando la latenza di rete è variabile.
- Cancellazione dell'eco: consente una maggiore variazione della distanza tra il microfono e gli altoparlanti per i lavoratori che non utilizzano cuffie.

- Audio plug-n-play: non è necessario che i dispositivi audio siano collegati prima di iniziare una sessione. Possono essere collegati in qualsiasi momento.
- Routing dei dispositivi audio: gli utenti possono indirizzare la suoneria agli altoparlanti, ma il percorso vocale verso le cuffie.
- ICA multi-stream: consente un routing flessibile basato sulla qualità del servizio sulla rete.
- ICA supporta quattro flussi TCP e due flussi UDP. Uno dei flussi UDP supporta l'audio in tempo reale su RTP.

Per un riepilogo delle funzionalità dell'app Citrix Workspace, vedere Matrice delle funzionalità di Citrix Receiver.

***Consigli per la configurazione del sistema***

*Hardware e software client*:
per una qualità audio ottimale, si consiglia l'ultima versione dell'app Citrix Workspace e una cuffia di buona qualità con cancellazione dell'eco acustico (AEC). Le versioni dell'app Citrix Workspace per Windows, Linux e Mac supportano VoIP. Inoltre, Dell Wyse offre il supporto VoIP per ThinOS (WTOS).

*Considerazioni sulla CPU*:
monitorare l'utilizzo della CPU sul VDA per determinare se è necessario assegnare due CPU virtuali a ciascuna macchina virtuale. Voce e video in tempo reale richiedono un uso intensivo di dati. La configurazione di due CPU virtuali riduce la latenza di commutazione dei thread. Pertanto, si consiglia di configurare due vCPU in un ambiente VDI Citrix Virtual Desktops.

Avere due CPU virtuali non significa necessariamente raddoppiare il numero di CPU fisiche, perché le CPU fisiche possono essere condivise tra le sessioni.

Anche Citrix Gateway Protocol (CGP), utilizzato per la funzionalità di affidabilità delle sessioni, aumenta il consumo della CPU. Nelle connessioni di rete di alta qualità, è possibile disabilitare questa funzionalità per ridurre il consumo di CPU sul VDA. Nessuno dei passaggi precedenti potrebbe essere necessario su un server potente.

*Audio UDP*:
l'audio su UDP fornisce un'eccellente tolleranza alla congestione della rete e alla perdita di pacchetti. Si consiglia di utilizzarlo al posto di TCP quando è disponibile.

*Configurazione LAN/WAN*:
una corretta configurazione della rete è fondamentale per una buona qualità dell'audio in tempo reale. In genere, è necessario configurare reti LAN virtuali (VLAN) perché i pacchetti broadcast eccessivi possono introdurre instabilità. I dispositivi abilitati per IPv6 potrebbero generare molti pacchetti broadcast. Se il supporto IPv6 non è necessario, è possibile disabilitare IPv6 su tali dispositivi. Eseguire questa configurazione per supportare la qualità del servizio.

*Impostazioni per l'uso delle connessioni WAN*:
è possibile utilizzare la chat vocale sulle connessioni LAN e WAN. In una connessione WAN, la qualità audio dipende dalla latenza, dalla perdita di pacchetti e dall'instabilità sulla connessione. Se si

distribuiscono softphone agli utenti con una connessione WAN, si consiglia di utilizzare NetScaler SD-WAN tra il centro dati e l'ufficio remoto. In tal modo si mantiene un'alta qualità del servizio. NetScaler SD-WAN supporta ICA multi-flusso, tra cui UDP. Inoltre, per un singolo flusso TCP è possibile distinguere le priorità dei vari canali virtuali ICA per garantire che i dati audio in tempo reale ad alta priorità ricevano un trattamento preferenziale.

Utilizzare Director o HDX Monitor per convalidare la configurazione HDX.

*Connessioni utente remote*:
Citrix Gateway supporta DTLS per fornire traffico UDP/RTP in modo nativo (senza incapsulamento in TCP).
Aprire i firewall in modo bidirezionale per il traffico UDP sulla porta 443.

*Selezione del codec e consumo di larghezza di banda*:
tra il dispositivo utente e il VDA nel centro dati, si consiglia di utilizzare l'impostazione del codec **Optimized-for-Speech (Ottimizzato per il parlato)**, nota anche come audio di qualità media. Tra la piattaforma VDA e l'IP-PBX, il softphone utilizza qualsiasi codec configurato o negoziato. Ad esempio:

- G711 offre una buona qualità della voce, ma ha un requisito di larghezza di banda che va da 80 kilobit al secondo fino a 100 kilobit al secondo per chiamata (a seconda dei sovraccarichi di Network Layer2).
- G729 offre una buona qualità della voce e ha un requisito di larghezza di banda ridotta che va da 30 kilobit al secondo fino a 40 kilobit al secondo per chiamata (a seconda dei sovraccarichi Network Layer 2).

#### *Distribuire applicazioni softphone al desktop virtuale*

Esistono due metodi con cui è possibile distribuire un softphone al desktop virtuale XenDesktop:

- L'applicazione può essere installata nell'immagine desktop virtuale.
- L'applicazione può essere trasmessa in streaming sul desktop virtuale utilizzando Microsoft App-V. Questo approccio presenta vantaggi di gestibilità perché l'immagine del desktop virtuale viene mantenuta pulita. Dopo essere stata trasmessa al desktop virtuale, l'applicazione viene eseguita in tale ambiente come se fosse installata nel modo consueto. Non tutte le applicazioni sono compatibili con App-V.

#### *Distribuire audio da e verso il dispositivo utente*

HDX RealTime generico supporta due metodi di trasmissione audio da e verso il dispositivo utente:

- **Canale virtuale audio Citrix**. Generalmente consigliamo il canale virtuale audio Citrix perché è progettato specificamente per il trasporto audio.
- **Reindirizzamento USB generico**. Supporta dispositivi audio con pulsanti o display (o entrambi), HID (Human Interface Device), se il dispositivo utente è su una connessione LAN o è disponibile una connessione simile a LAN verso il server di Citrix Virtual Apps and Desktops.

#### *Canale virtuale audio Citrix*

Il canale virtuale audio Citrix bidirezionale (CTXCAM) consente di trasmettere l'audio in modo efficiente sulla rete. HDX RealTime generico acquisisce l'audio dalla cuffia o dal microfono dell'utente e lo comprime. Quindi, lo invia tramite ICA all'applicazione softphone sul desktop virtuale. Allo stesso modo, l'uscita audio del softphone viene compressa e inviata nella direzione opposta alla cuffia o agli altoparlanti dell'utente. Questa compressione è indipendente dalla compressione utilizzata dal softphone stesso (come G.729 o G.711). Viene eseguita utilizzando il codec Optimized-for-Speech (Ottimizzato per il parlato, qualità media). Le sue caratteristiche sono ideali per VoIP. Offre un tempo di codifica rapido e consuma solo circa 56 kilobit al secondo di larghezza di banda della rete (28 Kbps in ogni direzione) nei momenti di picco. Questo codec deve essere selezionato esplicitamente nella console Manage del servizio perché non è il codec audio predefinito. Il codec predefinito è HD Audio (Audio HD, alta qualità). Questo codec è eccellente per colonne sonore stereo ad alta fedeltà, ma è più lento da codificare rispetto al codec ottimizzato per il parlato.

#### *Reindirizzamento USB generico*

La tecnologia di reindirizzamento USB generico Citrix (canale virtuale CTXGUSB) fornisce un mezzo generico per la gestione remota di dispositivi USB, inclusi dispositivi compositi (audio più HID) e dispositivi USB isocroni. Questo approccio è limitato agli utenti connessi tramite LAN. Questo perché il protocollo USB tende a essere sensibile alla latenza di rete e richiede una notevole larghezza di banda di rete. Il reindirizzamento USB isocrono funziona bene quando si utilizzano alcuni softphone. Questo reindirizzamento offre un'eccellente qualità della voce e bassa latenza. Tuttavia, il canale virtuale Citrix Audio è preferibile perché è ottimizzato per il traffico audio. L'eccezione principale è il caso in cui si utilizza un dispositivo audio con pulsanti. Ad esempio, un telefono USB collegato al dispositivo utente che è collegato al centro dati tramite LAN. In questo caso, il reindirizzamento USB generico supporta i pulsanti del telefono o della cuffia che controllano le funzionalità inviando un segnale al softphone. Non si verifica alcun problema con i pulsanti che funzionano localmente sul dispositivo.

### Limitazione

Dopo aver installato un dispositivo audio sul client, abilitare il reindirizzamento audio e avviare una sessione RDS, i file audio potrebbero non riprodurre l'audio. Come soluzione alternativa, aggiungere la chiave del Registro di sistema sul computer RDS e quindi riavviare la macchina. Per informazioni, vedere Audio limitation (Limitazione audio) nell'elenco delle funzionalità gestite tramite il Registro di sistema.

# Browser content redirection (Reindirizzamento del contenuto del browser)

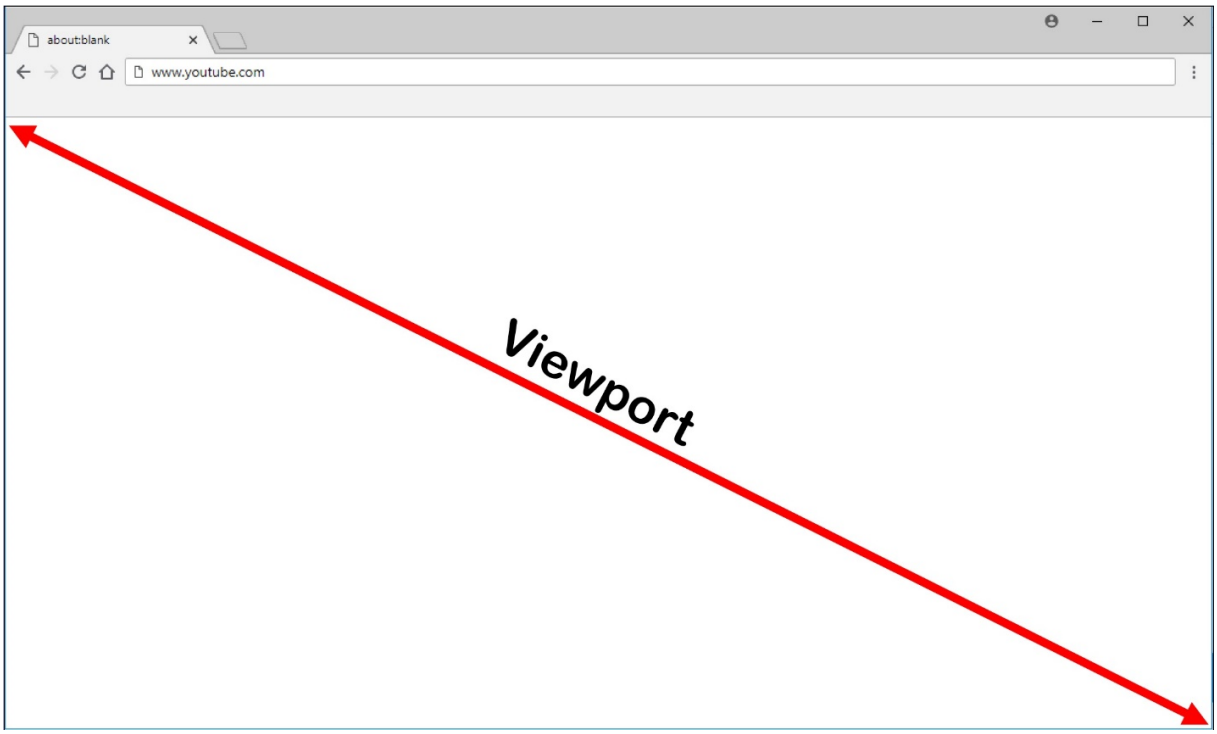
October 6, 2022

Il reindirizzamento del contenuto del browser impedisce il rendering delle pagine Web nell'elenco di elementi consentiti sul lato VDA. Questa funzionalità utilizza l'app Citrix Workspace per creare un'istanza di un motore di rendering corrispondente sul lato client, che recupera i contenuti HTTP e HTTPS dall'URL.

> **Nota:**
>
> È possibile specificare che le pagine Web vengano reindirizzate al lato VDA (e non sul lato client) utilizzando un elenco di blocco.

Questo motore di layout Web di sovrapposizione viene eseguito sul dispositivo endpoint anziché sul VDA e utilizza la CPU, la GPU, la RAM e la rete dell'endpoint.

Viene reindirizzato solo il riquadro di visualizzazione del browser. Il riquadro di visualizzazione è l'area rettangolare del browser in cui viene visualizzato il contenuto. Il riquadro di visualizzazione non include elementi quali barra degli indirizzi, barra dei Preferiti e barra di stato. Tali elementi sono nell'interfaccia utente e sono ancora in esecuzione sul browser nel VDA.




1. Configurare nell'interfaccia Manage > Full Configuration (Gestisci > Configurazione completa) un criterio che specifichi l'elenco di controllo dell'accesso contenente gli URL per il reindirizza-

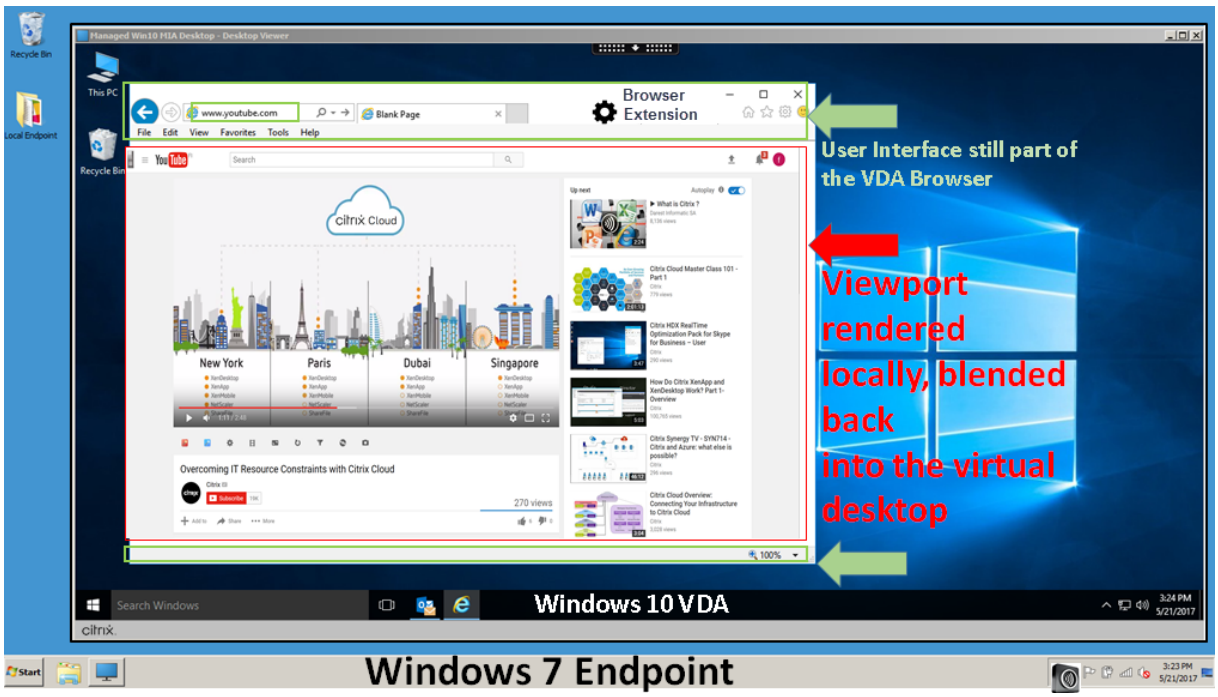
mento dagli elenchi consentiti o bloccati. Perché il browser sul VDA rilevi che l'URL che l'utente sta per aprire corrisponde all'elenco di elementi consentiti o non corrisponde a un elenco di blocco, un'estensione del browser esegue il confronto. L'estensione del browser (BHO) per Internet Explorer 11 è inclusa nel supporto di installazione e viene installata automaticamente. Per Chrome, l'estensione del browser è disponibile nel Chrome Web Store ed è possibile distribuirla utilizzando i Criteri di gruppo e i file ADMX. Le estensioni di Chrome vengono installate per ciascun utente. Non è necessario aggiornare un'immagine golden per aggiungere o rimuovere un'estensione.

2. Se viene trovata una corrispondenza nell'elenco degli elementi consentiti (ad esempio `https://www.mycompany.com/`) e non esiste alcuna corrispondenza con un URL nell'elenco di blocco (ad esempio `https://www.mycompany.com/engineering`), un canale virtuale (CTXCSB) indica all'app Citrix Workspace che è necessario un reindirizzamento e inoltra l'URL. L'app Citrix Workspace crea un'istanza di un motore di rendering locale e visualizza il sito Web.
3. L'app Citrix Workspace riporta quindi senza problemi il sito Web nell'area del contenuto del browser del desktop virtuale.

Il colore del logo specifica lo stato dell'estensione Chrome. Si tratta di uno di questi tre colori:

- Verde: attivo e connesso.
- Grigio: non attivo/inattivo nella scheda corrente.
- Rosso: non funzionante.

È possibile eseguire il debug dei log utilizzando **Opzioni** nel menu delle estensioni.




Di seguito sono riportati gli scenari dei modi in cui l'app Citrix Workspace recupera il contenuto:

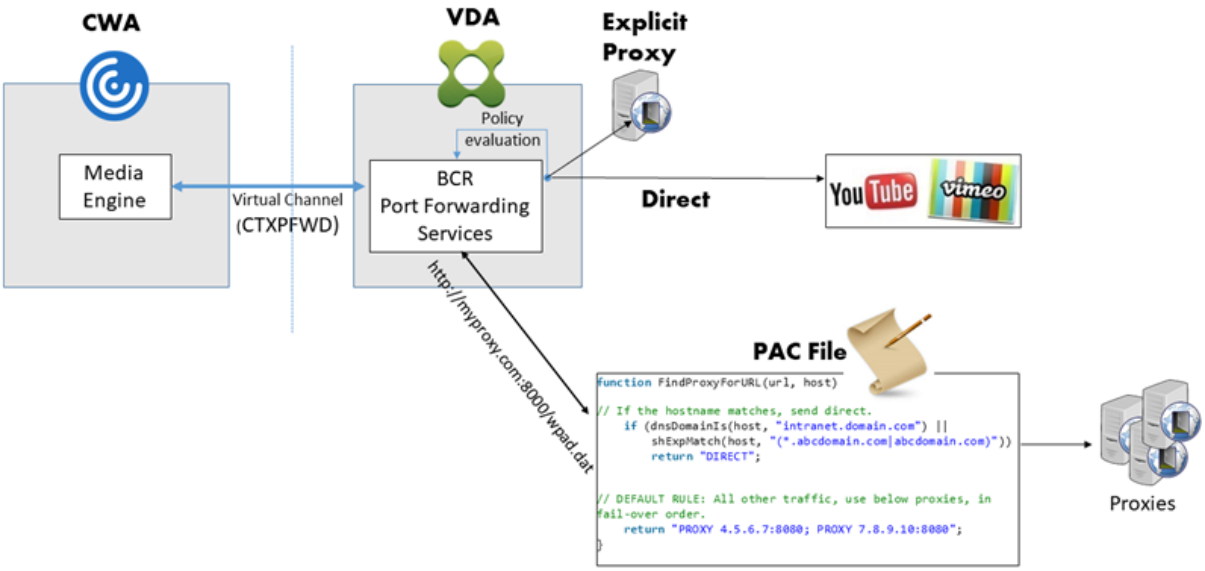
 

- **Recupero dal server e rendering sul server**: non vi è alcun reindirizzamento perché il sito non è stato aggiunto all'elenco degli elementi consentiti o il reindirizzamento non è riuscito. Si ritorna al rendering della pagina Web sul VDA e si utilizza Thinwire per la gestione remota della grafica. Utilizzare i criteri per controllare il comportamento di fallback. Elevato consumo di CPU, RAM e larghezza di banda sul VDA.
- **Recupero dal server e rendering sul client**: l'app Citrix Workspace contatta e recupera i contenuti dal server Web tramite il VDA utilizzando un canale virtuale (CTXPFWD). Questa opzione è utile quando il client non dispone di accesso a Internet (ad esempio, thin client). Basso consumo di CPU e RAM sul VDA, ma la larghezza di banda viene consumata sul canale virtuale ICA.

  Esistono tre modalità di funzionamento per questo scenario. Il termine proxy si riferisce a un dispositivo proxy a cui il VDA accede per ottenere l'accesso a Internet.

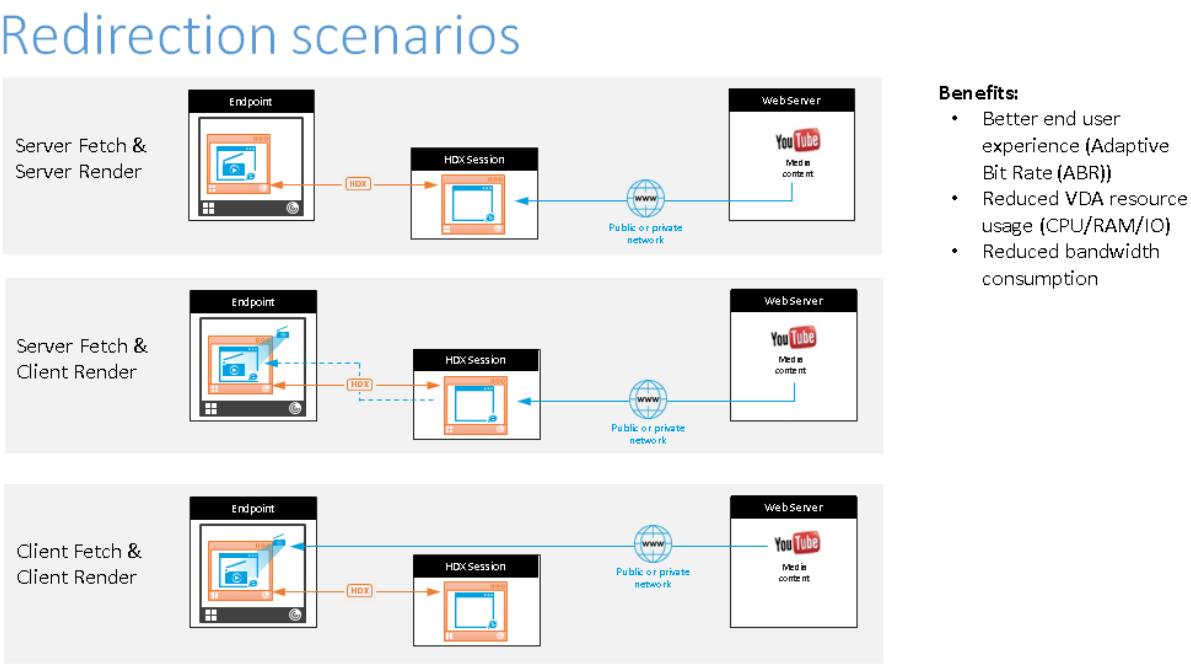
  Quale opzione dei criteri scegliere:

  - Explicit Proxy (Proxy esplicito): se si dispone di un singolo proxy esplicito nel centro dati.
  - Direct (Diretto) o Transparent (Trasparente) : se non si dispone di proxy o se si utilizzano proxy trasparenti.
  - PAC files (File PAC): se si fa affidamento su file PAC in modo che i browser nel VDA possano scegliere automaticamente il server proxy appropriato per il recupero di un URL specificato.




- **Recupero dal client e rendering sul client**: poiché l'app Citrix Workspace contatta direttamente il server Web, richiede l'accesso a Internet. Questo scenario consente l'offload di tutto l'utilizzo di rete, CPU e RAM dal sito XenApp e XenDesktop.




**Meccanismo di fallback:**

In alcuni casi, il reindirizzamento del client non riesce. Ad esempio, se il computer client non dispone di accesso diretto a Internet, al VDA potrebbe essere restituita una risposta di errore. In questi casi, il browser sul VDA può quindi ricaricare la pagina sul server ed eseguirne il rendering.

È possibile impedire il rendering sul server di elementi video utilizzando i criteri di **prevenzione del fallback di Windows Media** esistenti. Impostare questo criterio su **Play all content only on client (Riproduci tutto il contenuto solo sul client)** o **Play only client-accessible content on client (Riproduci solo il contenuto accessibile dal client sul client)**. Queste impostazioni impediscono la riproduzione di elementi video sul server in caso di errori nel reindirizzamento del client. Questo criterio ha effetto solo quando si attiva il reindirizzamento del contenuto del browser e il criterio **Elenco di controllo di accesso** contiene l'URL di cui viene eseguito il fallback. L'URL non può essere incluso nel criterio dell'elenco di blocco.

**Requisiti di sistema:**

Endpoint Windows:

- Windows 10 o 11
- App Citrix Workspace 1809 per Windows o versioni successive

> **Nota:**
>
> Il reindirizzamento del contenuto del browser è supportato solo nella versione corrente dell'app Citrix Workspace per Windows, ma non nelle versioni LTSR dell'app Citrix Workspace, 1912 e 2203.1.

Endpoint Linux:

- App Citrix Workspace 1808 per Linux o versioni successive
- Citrix Receiver per Linux 13.9 o versioni successive
- I terminali thin client devono includere WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 e XenApp e XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

- Sistema operativo VDA: Windows 10 (versione minima 1607), Windows Server 2012 R2, Windows Server 2016
- Browser sul VDA:
  - Google Chrome v66 o versioni successive (Chrome richiede l'app Citrix Workspace 1809 per Windows sull'endpoint utente, Citrix Virtual Apps and Desktops 7 1808 VDA e l'estensione di reindirizzamento del contenuto del browser)
  - Internet Explorer 11 con le seguenti opzioni configurate:
    * Disabilitare **Modalità protetta avanzata** in: **Opzioni Internet** > **Avanzate > Sicurezza**
    * Selezionare **Abilita estensioni del browser di terze parti** in: **Opzioni Internet > Avanzate > Esplorazione**

## Risoluzione dei problemi

Per informazioni sulla risoluzione dei problemi, vedere l'articolo del Knowledge Center https://support.citrix.com/article/CTX230052

## Estensione Chrome per il reindirizzamento del contenuto del browser

Per utilizzare il reindirizzamento del contenuto del browser con Chrome, aggiungere l'estensione di reindirizzamento del contenuto del browser dal Chrome Web Store. Fare clic su **Add to Chrome** (Aggiungi a Chrome) nell'ambiente Citrix Virtual Apps and Desktops.

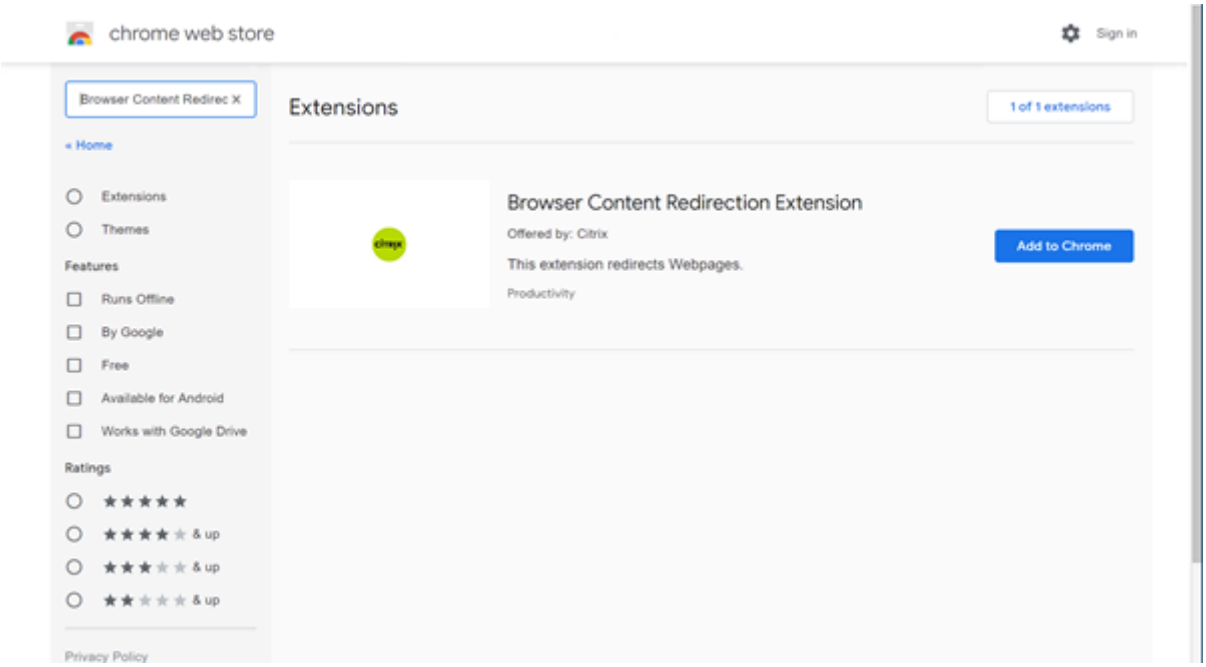
L'estensione **non** è richiesta sul computer client dell'utente, ma solo sul VDA.

### Requisiti di sistema

- Chrome v66 o versione successiva
- Estensione per il reindirizzamento del contenuto del browser
- Citrix Virtual Apps and Desktops 7 1808 o versioni successive
- App Citrix Workspace 1809 per Windows o versioni successive

> **Nota:**
>
> Il reindirizzamento del contenuto del browser è supportato solo nella versione corrente dell'app Citrix Workspace per Windows, ma non nelle versioni LTSR dell'app Citrix Workspace, 1912 e 2203.1.

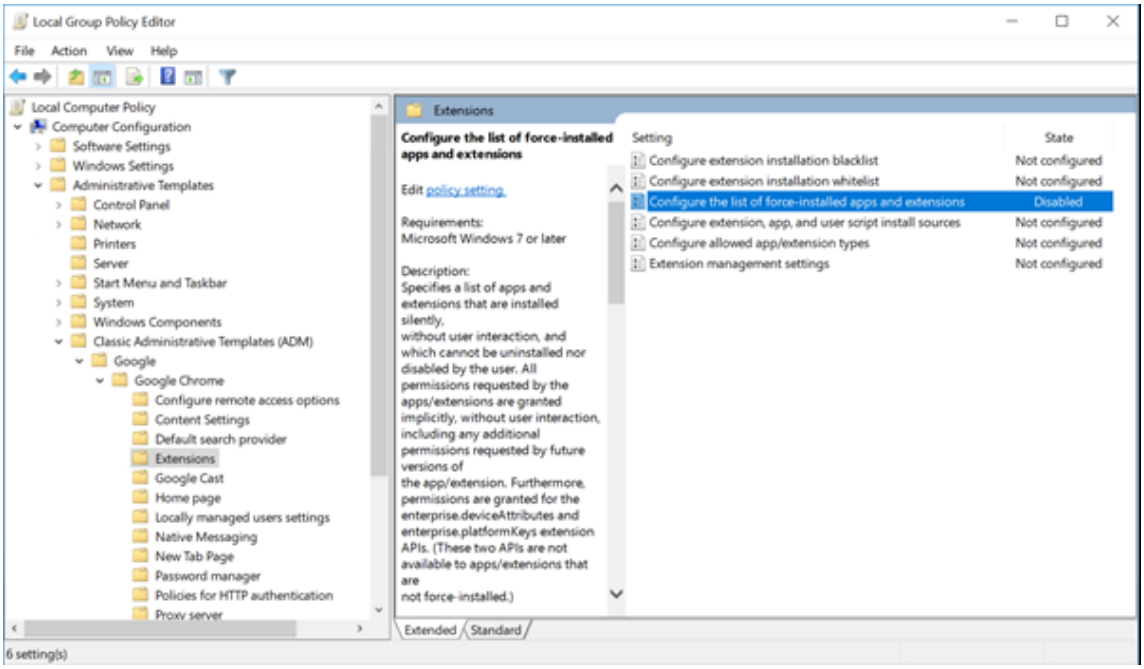



Questo metodo funziona per i singoli utenti. Per distribuire l'estensione a un grande gruppo di utenti dell'organizzazione, distribuire l'estensione utilizzando Criteri di gruppo.

### Distribuire l'estensione utilizzando Criteri di gruppo

1. Importare i file ADMX di Google Chrome nell'ambiente. Per informazioni sul download dei modelli di criteri e sull'installazione e la configurazione dei modelli nell'Editor Criteri di gruppo, vedere Impostare i criteri del browser Chrome sui PC gestiti.
2. Aprire la console Gestione Criteri di gruppo e andare a **Configurazione utente\Modelli amministrativi classici (ADM)\Google\Google Chrome\Estensioni**. Abilitare l'impostazione **Configure the list of force-installed apps and extensions (Configura l'elenco delle app e delle estensioni installate forzatamente)**.

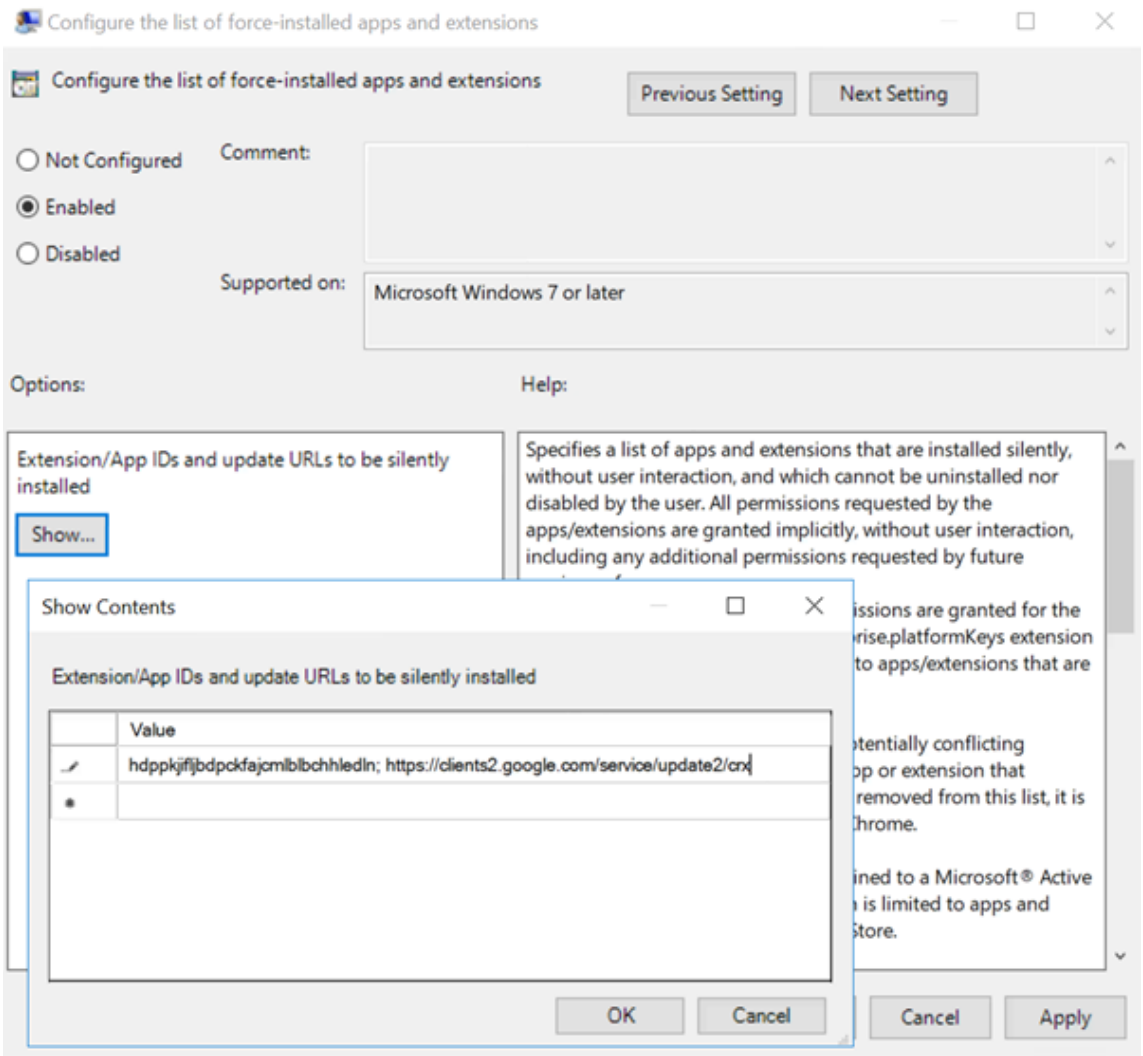
 




3. Fare clic su **Show (Mostra)** e digitare la seguente stringa, che corrisponde all'ID estensione. Aggiornare l'URL per l'estensione di reindirizzamento del contenuto del browser.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```




4. Applicare l'impostazione e dopo un aggiornamento di **gpupdate**, l'utente riceve automaticamente l'estensione. Se si avvia il browser Chrome nella sessione dell'utente, l'estensione è già applicata e l'utente non può rimuoverla.

   Eventuali aggiornamenti dell'estensione vengono installati automaticamente sui computer degli utenti tramite l'URL di aggiornamento specificato nell'impostazione.

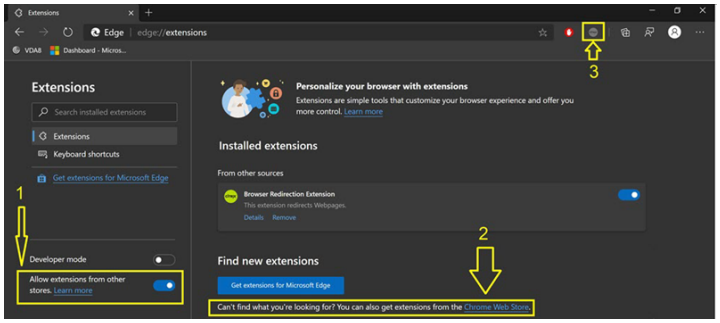
   Se l'impostazione **Configure the list of force-installed apps and extensions (Configura l'elenco delle app e delle estensioni installate forzatamente)** è impostata su **Disabled (Disabilitata)**, l'estensione viene rimossa automaticamente da Chrome per tutti gli utenti.

### Estensione Edge Chromium per il reindirizzamento del contenuto del browser

Per installare l'estensione di reindirizzamento del contenuto del browser in Edge, assicurarsi di avere installato la versione **83.0.478.37** o successiva del browser Edge.

1. Fare clic sull'opzione **Estensioni** nel menu e attivare **Allow extensions from other stores (Consenti estensioni da altri store)**.
2. Fare clic sul collegamento **Chrome Web Store** e l'estensione verrà visualizzata nella barra in alto a destra.
   Per ulteriori informazioni sulle estensioni di Microsoft Edge, vedere Estensioni.




## Reindirizzamento del contenuto del browser e DPI

Quando si utilizza il reindirizzamento del contenuto del browser con DPI (ridimensionamento) impostato su un valore superiore al 100% sul computer dell'utente, la schermata del contenuto del browser reindirizzato viene visualizzata in modo errato. Per evitare questo problema, non impostare il DPI quando si utilizza il reindirizzamento del contenuto del browser. Un altro modo per evitare il problema è disabilitare l'accelerazione GPU per il reindirizzamento del contenuto del browser per Chrome creando la chiave del Registro di sistema sulla macchina dell'utente. Per informazioni, vedere Reindirizzamento del contenuto del browser e DPI nell'elenco delle funzionalità gestite tramite il registro.

## Intestazione della richiesta utente-agente

L'intestazione utente-agente aiuta a identificare le richieste HTTP inviate dal reindirizzamento del contenuto del browser. Questa impostazione può essere utile quando si configurano regole proxy e firewall. Ad esempio, se il server blocca le richieste inviate dal reindirizzamento del contenuto del browser, è possibile creare una regola che contiene l'intestazione utente-agente per ignorare determinati requisiti.

Solo i dispositivi Windows supportano l'intestazione della richiesta utente-agente.

Per impostazione predefinita, la stringa di intestazione della richiesta utente-agente è disabilitata. Per abilitare l'intestazione utente-agente per il contenuto con rendering sul client, utilizzare l'editor del Registro di sistema. Per informazioni, vedere Intestazione della richiesta utente-agente nell'elenco delle funzionalità gestite tramite il Registro di sistema.

# Videoconferenze HDX e compressione video della webcam

October 6, 2022

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Le webcam possono essere utilizzate dalle applicazioni in esecuzione all'interno della sessione virtuale utilizzando la compressione video della webcam HDX o il reindirizzamento USB generico HDX plug-n-play. Utilizzare l'**app Citrix Workspace > Preferences (Preferenze) > Devices (Dispositivi)** per passare da una modalità all'altra. Citrix consiglia di utilizzare sempre la compressione video della webcam HDX, se possibile. Il reindirizzamento USB generico HDX è consigliato solo in caso di problemi di compatibilità delle applicazioni con la compressione video HDX o quando si richiedono funzionalità native avanzate della webcam. Per migliorare le prestazioni, Citrix consiglia che sul Virtual Delivery Agent siano disponibili almeno due CPU virtuali.

Per impedire agli utenti di modificare la compressione video HDX della webcam, disabilitare il reindirizzamento dei dispositivi USB utilizzando le impostazioni dei criteri in **ICA policy settings (Impostazioni criteri ICA) > USB Devices policy (Criteri dispositivi USB)**. Gli utenti dell'app Citrix Workspace possono ignorare il comportamento predefinito scegliendo l'impostazione **Non usare il microfono e la web** in Microfono e webcam in Desktop Viewer.

## Compressione video della webcam HDX

La compressione video della webcam HDX è anche chiamata modalità webcam **ottimizzata**. Questo tipo di compressione del video della webcam invia il video H.264 direttamente all'applicazione di videoconferenza in esecuzione nella sessione virtuale. Per ottimizzare le risorse VDA, la compressione della webcam HDX non codifica, transcodifica e decodifica i video della webcam. Questa funzionalità è abilitata per impostazione predefinita.

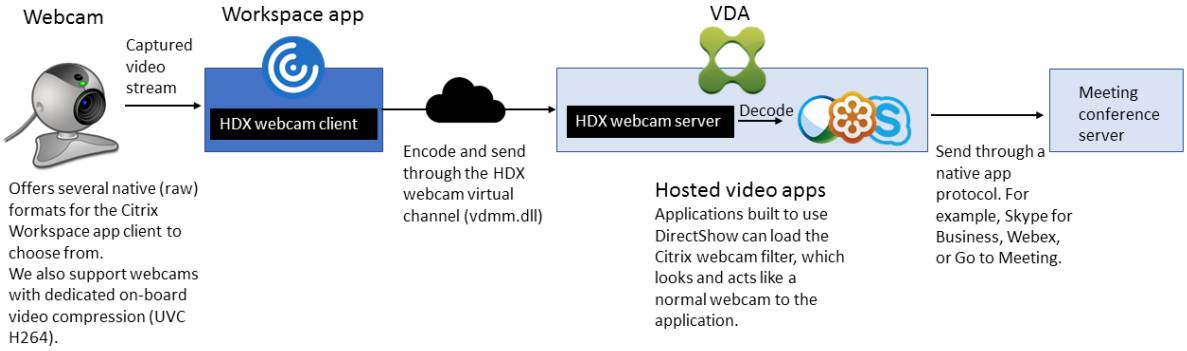
Per disabilitare lo streaming video diretto dal server all'app per videoconferenze, impostare la chiave del Registro di sistema su 0 nel VDA. Per informazioni, vedere Compressione video webcam nell'elenco delle funzionalità gestite tramite il registro.

Se si disabilita la funzionalità predefinita per lo streaming delle risorse video, la compressione video della webcam HDX utilizza la tecnologia del framework multimediale che fa parte del sistema operativo client per intercettare il video dai dispositivi di acquisizione, transcodificarlo e comprimerlo. I

produttori di dispositivi di acquisizione forniscono i driver che si collegano all'architettura di streaming del kernel del sistema operativo.

Il client gestisce la comunicazione con la webcam. Il client invia quindi il video solo al server che può visualizzarlo correttamente. Il server non interagisce direttamente con la webcam, ma la sua integrazione offre la stessa esperienza sul desktop. L'app Workspace comprime il video per risparmiare larghezza di banda e fornire una migliore resilienza negli scenari WAN.




La compressione video HDX della webcam richiede che siano abilitate le seguenti impostazioni dei criteri (sono tutte abilitate per impostazione predefinita).

- Multimedia conferencing (Conferenze multimediali)
- Reindirizzamento di Windows Media

Se una webcam supporta la codifica hardware, la compressione video HDX utilizza la codifica hardware per impostazione predefinita. La codifica hardware potrebbe consumare più larghezza di banda rispetto alla codifica software. Per forzare la compressione del software, modificare la chiave del Registro di sistema sul client. Per informazioni, vedere Compressione del software della webcam nell'elenco delle funzionalità gestite tramite il registro.

### Requisiti di compressione video della webcam HDX

La compressione video della webcam HDX supporta le seguenti versioni dell'app Citrix Workspace:

| Piattaforma | Processore |
| --- | --- |
| App Citrix Workspace per Windows | L'app Citrix Workspace per Windows supporta la compressione video della webcam per applicazioni a 32 e 64 bit su XenApp e XenDesktop 7.17 e versioni successive. Nelle versioni precedenti, l'app Citrix Workspace per Windows supporta solo app a 32 bit. |

| Piattaforma | Processore |
| --- | --- |
| App Citrix Workspace per Mac | L'app Citrix Workspace per Mac 2006 o versioni successive supporta la compressione video della webcam per app a 64 bit su XenApp e XenDesktop 7.17 e versioni successive. Nelle versioni precedenti, l'app Citrix Workspace per Mac supporta solo app a 32 bit. |
| App Citrix Workspace per Linux | L'app Citrix Workspace per Linux supporta solo app a 32 bit sul desktop virtuale. |
| App Citrix Workspace per Chrome | Poiché alcuni Chromebook ARM non supportano la codifica H.264, solo le app a 32 bit possono utilizzare la compressione video ottimizzata della webcam HDX. |

Le applicazioni video basate su Media Foundation supportano la compressione video della webcam HDX su Windows 8.x o versioni successive e Windows Server 2012 R2 e versioni successive. Per ulteriori informazioni, vedere l'articolo CTX132764 del Knowledge Center.

Altri requisiti del dispositivo utente:

- Hardware appropriato per riprodurre il suono.
- Webcam compatibile con DirectShow (utilizzare le impostazioni predefinite della webcam). Le webcam con funzionalità di codifica hardware riducono l'utilizzo della CPU lato client.
- Per la compressione video della webcam HDX, installare i driver della webcam sul client, ottenuti dal produttore della videocamera, se possibile. L'installazione dei driver del dispositivo non è necessaria sul server.

Webcam diverse offrono frequenze dei fotogrammi diverse e hanno livelli diversi di luminosità e contrasto. La regolazione del contrasto della webcam può ridurre significativamente il traffico a monte. Citrix utilizza le seguenti webcam per la convalida iniziale delle funzionalità:

- Modelli Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- Webcam HP Deluxe

Per regolare la frequenza dei fotogrammi video preferita, modificare la chiave del Registro di sistema sul client. Per informazioni, vedere Frequenza dei fotogrammi di compressione video della webcam nell'elenco delle funzionalità gestite tramite il Registro di sistema.

### Streaming della webcam ad alta definizione

L'applicazione di videoconferenza sul server seleziona il formato e la risoluzione della webcam in base ai tipi di formato supportati. Quando si avvia una sessione, il client invia le informazioni della webcam al server. Scegliere una webcam dall'applicazione. Quando la webcam e l'applicazione di videoconferenza supportano il rendering ad alta definizione, l'applicazione utilizza una risoluzione ad alta definizione. Supportiamo risoluzioni webcam fino a 1920x1080.

Questa funzionalità richiede l'app Citrix Workspace per Windows, versione minima 1808 o Citrix Receiver per Windows, versione minima 4.10.

È possibile utilizzare una chiave del Registro di sistema per disabilitare e abilitare la funzionalità. Per informazioni, vedere Streaming della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il registro.

Se la negoziazione del tipo di contenuti multimediali non riesce, HDX torna alla risoluzione predefinita di 352x288 CIF. È possibile utilizzare le chiavi del Registro di sistema nel client per configurare la risoluzione predefinita. Assicurarsi che la videocamera supporti la risoluzione specificata. Per informazioni, vedere Risoluzione della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il registro.

La compressione video della webcam HDX utilizza una larghezza di banda significativamente inferiore rispetto al reindirizzamento USB generico plug-n-play e funziona bene sulle connessioni WAN. Per regolare la larghezza di banda, impostare la chiave del Registro di sistema sul client. Per informazioni, vedere Larghezza di banda della webcam ad alta definizione nell'elenco delle funzionalità gestite tramite il registro.

Immettere un valore in bit al secondo. Se non si specifica la larghezza di banda, le applicazioni di videoconferenza utilizzano 350.000 bps per impostazione predefinita.

### Reindirizzamento USB generico HDX plug-n-play

Il reindirizzamento USB generico HDX plug-n-play (isocrono) è anche chiamato modalità webcam **generica**. Il vantaggio del reindirizzamento USB generico HDX plug-n-play è che non è necessario installare driver sul thin client/endpoint. Lo stack USB è virtualizzato in modo tale che tutto ciò che si collega al client locale venga inviato alla macchina virtuale remota. Il desktop remoto agisce come se fosse collegato in modo nativo. Il desktop Windows gestisce tutte le interazioni con l'hardware ed esamina la logica plug-n-play per trovare i driver corretti. La maggior parte delle webcam funziona se i driver sono presenti sul server e possono funzionare su ICA. La modalità webcam generica utilizza una larghezza di banda significativamente maggiore (molti megabit al secondo) perché vengono inviati video non compressi sulla rete con il protocollo USB.

# Reindirizzamento multimediale HTML5

May 23, 2023

Il reindirizzamento multimediale HTML5 estende le funzionalità di reindirizzamento multimediale di HDX MediaStream per includere audio e video HTML5. A causa della crescita della distribuzione online di contenuti multimediali, in particolare ai dispositivi mobili, l'industria dei browser ha sviluppato modi più efficienti per presentare audio e video.

Flash è stato lo standard, ma richiede un plug-in, non funziona su tutti i dispositivi e richiede un maggiore utilizzo della batteria nei dispositivi mobili. Aziende come YouTube, NetFlix.com e le versioni più recenti dei browser di Mozilla, Google e Microsoft stanno passando a HTML5, che sta diventando il nuovo standard.

I contenuti multimediali basati su HTML5 presentano molti vantaggi rispetto ai plug-in proprietari, tra cui:

- Standard indipendenti dall'azienda (W3C)
- Flusso di lavoro DRM (Digital Rights Management) semplificato
- Prestazioni migliori senza problemi di sicurezza generati dai plug-in

## Download progressivi HTTP

Il download progressivo HTTP è un metodo di pseudo-streaming basato su HTTP che supporta HTML5. In un download progressivo, il browser riproduce un singolo file (codificato con un'unica qualità) mentre viene scaricato da un server Web HTTP. Il video viene memorizzato sull'unità mentre viene ricevuto e viene riprodotto dall'unità. Se si guarda nuovamente il video, il browser può caricarlo dalla cache.

Per un esempio di download progressivo, vedere la pagina di test di reindirizzamento video HTML5. Per ispezionare gli elementi video nella pagina Web e trovare le fonti (formato contenitore mp4) nei tag video HTML5, utilizzare gli strumenti di sviluppo nel browser:

## Confronto tra HTML5 e Flash

| Funzionalità | HTML5 | Flash |
|---|---|---|
| Richiede un lettore proprietario | No | Sì |
| Funziona su dispositivi mobili | Sì | Alcuni |
| Velocità di esecuzione su piattaforme diverse | Elevata | Bassa |

| Funzionalità | HTML5 | Flash |
|---|---|---|
| Supportato da iOS | Sì | No |
| Utilizzo delle risorse | Minore | Maggiore |
| Caricamento più rapido | Sì | No |

### Requisiti

Supportiamo solo il reindirizzamento per download progressivi in formato mp4. Non supportiamo le tecnologie di streaming della velocità in bit WebM e Adaptive come DASH/HLS.

Supportiamo quanto segue e utilizziamo i criteri per il controllo. Per ulteriori informazioni, vedere Impostazioni dei criteri multimediali.

- Rendering lato server
- Rendering sul client con recupero dal server
- Recupero e rendering lato client

Versioni minime dell'app Citrix Workspace e di Citrix Receiver:

- App Citrix Workspace 1808 per Windows
- Citrix Receiver per Windows 4.5
- App Citrix Workspace 1808 per Linux
- Citrix Receiver per Linux 13.5

| Versione minima del browser del VDA | Versione del sistema operativo/build/SP Windows |
|---|---|
| Internet Explorer 11.0 | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Firefox 47 Aggiungere manualmente i certificati all'archivio dei certificati di Firefox o configurare Firefox per cercare i certificati da un archivio di certificati attendibili di Windows. Per ulteriori informazioni, vedere `https://wiki.mozilla.org/CA:AddRootToFirefox` | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Chrome 51 | Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |

### Componenti della soluzione di reindirizzamento video HTML5

- **HdxVideo.js**: hook JavaScript che intercetta i comandi video sul sito Web. HdxVideo.js comunica con WebSocketService utilizzando Secure WebSockets (SSL/TLS).
- **Certificati SSL WebSocket**
  - Per la CA (root): **Citrix XenApp/XenDesktop HDX In-Product CA**(C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    Posizione: Certificati (Computer locale) > Autorità di certificazione radice attendibili > Certificati.
  - Per l'entità finale (foglia): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp\XenDesktop HDX Service)
    Posizione: Certificati (Computer locale) > Personale > Certificati.
- **WebSocketService.exe**: viene eseguito sul sistema locale ed esegue la terminazione SSL e il mapping della sessione utente. TLS Secure WebSocket in ascolto sulla porta 127.0.0.1 9001.
- **WebSocketAgent.exe**: viene eseguito nella sessione utente ed esegue il rendering del video come indicato dai comandi WebSocketService.

### Come è possibile abilitare il reindirizzamento video HTML5?

In questa versione, questa funzionalità è disponibile solo per le pagine Web controllate. Richiede l'aggiunta del JavaScript HdxVideo.js (incluso nel supporto di installazione di Citrix Virtual Apps and Desktops) alle pagine Web in cui è disponibile il contenuto multimediale HTML5. Ad esempio, i video su un sito di formazione interno.

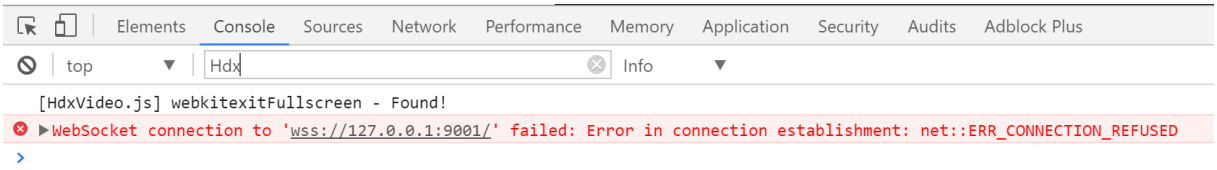
Siti Web come youtube.com, basati su tecnologie di bitrate adattivo (ad esempio, HTTP Live Streaming [HLS] e Dynamic Adaptive Streaming over HTTP [DASH]), non sono supportati.

Per ulteriori informazioni, vedere *Impostazioni dei criteri multimediali*.

### Consigli per la risoluzione dei problemi

Possono verificarsi degli errori quando la pagina Web tenta di eseguire HdxVideo.js. Se il JavaScript non viene caricato, il meccanismo di reindirizzamento HTML5 non va a buon fine. Assicurarsi che non vi siano errori relativi a HdxVideo.js ispezionando la console nelle finestre degli strumenti di sviluppo del browser. Ad esempio:




## Ottimizzazione di Microsoft Teams

November 21, 2023

Citrix offre ottimizzazione per Microsoft Teams basato su desktop utilizzando Citrix Virtual Apps and Desktops e l'app Citrix Workspace. Per impostazione predefinita, tutti i componenti necessari vengono raggruppati nell'app Citrix Workspace e nel Virtual Delivery Agent (VDA).

L'ottimizzazione di Citrix per Microsoft Teams include servizi HDX lato VDA e un'API per interfacciarsi con l'app ospitata Microsoft Teams per ricevere comandi. Questi componenti aprono un canale virtuale di controllo (CTXMTOP) verso il motore multimediale sul lato dell'app Citrix Workspace. L'endpoint decodifica i contenuti multimediali e ne esegue il provisioning localmente, spostando nuovamente la finestra dell'app Citrix Workspace nell'app Microsoft Teams ospitata.

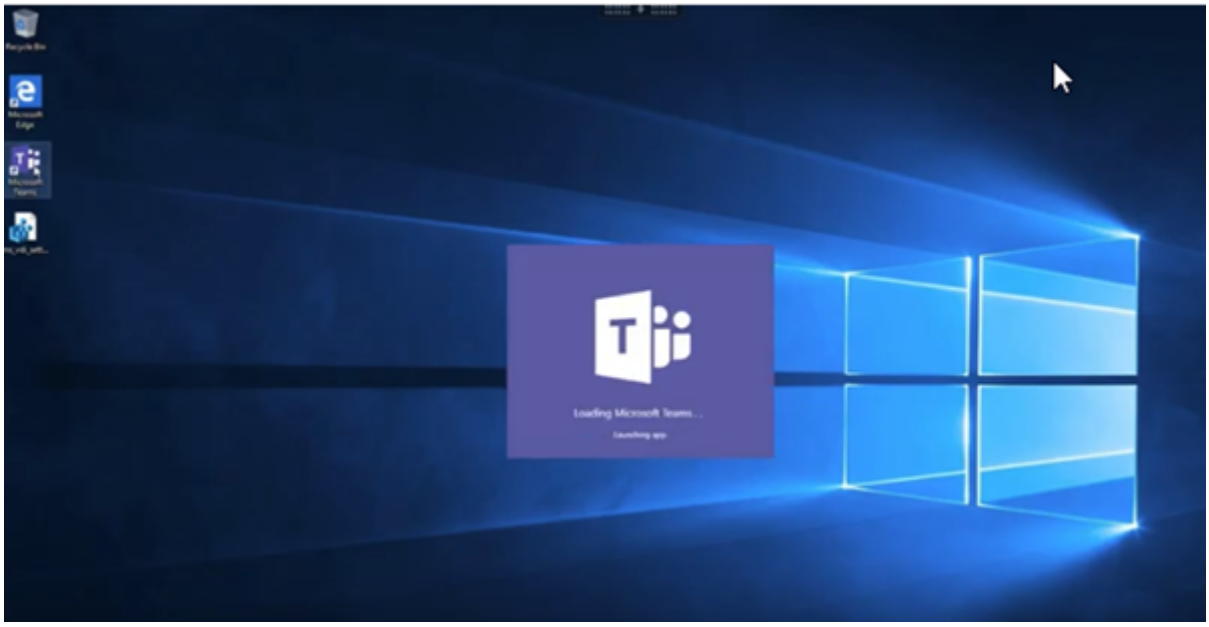
L'autenticazione e la segnalazione si verificano in modo nativo nell'app ospitata Microsoft Teams, proprio come gli altri servizi Microsoft Teams (ad esempio chat o collaborazione). Il reindirizzamento audio/video non influisce.

`CTXMTOP` è un comando e un canale virtuale di controllo. Ciò significa che i contenuti multimediali non vengono scambiati tra l'app Citrix Workspace e il VDA.

È disponibile solo il recupero dal client e il rendering sul client.

Questa demo video dà un'idea di come Microsoft Teams funziona in un ambiente virtuale Citrix.



### Installazione di Microsoft Teams

Citrix e Microsoft consigliano di utilizzare l'ultima versione disponibile di Microsoft Teams e di mantenerla aggiornata.
Le versioni dell'app desktop Microsoft Teams con date di rilascio più vecchie di 90 giorni rispetto alla data di rilascio della versione corrente non sono supportate.
Le versioni dell'app desktop Microsoft Teams non supportate presentano agli utenti una pagina di blocco e richiedono di aggiornare l'app.

Per informazioni sulle ultime versioni disponibili, vedere Cronologia degli aggiornamenti per la versione dell'app Microsoft Teams (desktop e Mac).

Si consiglia di seguire le linee guida per l'installazione di Microsoft Teams a livello di macchina. e di evitare di utilizzare il programma di installazione .exe che installa Microsoft Teams in `AppData`. Installare invece in `C:\Program Files (x86)\Microsoft\Teams` utilizzando il flag `ALLUSER=1` dalla riga di comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

In questo esempio viene utilizzato anche il parametro `ALLUSERS=1`. Quando si imposta questo parametro, il programma di installazione di Microsoft Teams a livello di macchina viene visualizzato in **Programmi e funzionalità** nel **Pannello di controllo**. Inoltre, in **App e funzionalità** nelle Impostazioni di Windows per tutti gli utenti del computer. Tutti gli utenti possono quindi disinstallare Microsoft Teams se dispongono di credenziali di amministratore.

È importante capire la differenza tra `ALLUSERS=1` e `ALLUSER=1`. È possibile utilizzare il parametro

ALLUSERS=1 in ambienti non VDI e VDI. Utilizzare il parametro ALLUSER=1 solo negli ambienti VDI per specificare un'installazione per ogni macchina.

In modalità ALLUSER=1 l'applicazione Microsoft Teams non si aggiorna automaticamente ogni volta che è disponibile una nuova versione. Questa modalità è consigliata per ambienti non persistenti, come app o desktop condivisi ospitati di Windows Server o cataloghi random/in pool di Windows 10. Per ulteriori informazioni, vedere Installare Microsoft Teams utilizzando MSI (sezione Installazione VDI).

Supponiamo che si disponga di ambienti VDI persistenti Windows 10 dedicati. Si desidera che l'applicazione Microsoft Teams si aggiorni automaticamente e si preferisce che Microsoft Teams si installi per ciascun utente in Appdata/Local. In questo caso, utilizzare il programma di installazione di .exe o il file MSI senza ALLUSER=1.

> **Nota:**
>
> Si consiglia di installare il VDA prima di installare Microsoft Teams nell'immagine golden. Questo ordine di installazione è necessario perché il flag ALLUSER=1 abbia effetto. Se è stato installato Microsoft Teams sulla macchina virtuale prima di installare il VDA, disinstallare e reinstallare Microsoft Teams.

### Per l'accesso remoto al PC

Si consiglia di installare Microsoft Teams versione 1.4.00.22472 o successiva, dopo aver installato il VDA. In caso contrario, è necessario disconnettersi e accedere nuovamente in modo che Microsoft Teams rilevi il VDA come previsto. La versione 1.4.00.22472 e le successive includono la logica aumentata eseguita al momento dell'avvio di Microsoft Teams e il tempo di accesso per il rilevamento del VDA. Queste versioni includono anche l'identificazione del tipo di sessione attiva (HDX, RDP o connessione locale alla macchina client). Se si è connessi localmente, le versioni precedenti di Microsoft Teams potrebbero non riuscire a rilevare e disabilitare determinate funzionalità o elementi dell'interfaccia utente. Ad esempio, stanze per sottogruppi di lavoro, finestre a comparsa per riunioni e chat o reazioni alle riunioni.

> **Importante:**
>
> Quando si esegue il roaming da una sessione locale a una sessione HDX e Microsoft Teams viene mantenuto aperto e in esecuzione in background, è necessario uscire e riavviare Microsoft Teams per ottimizzare correttamente con HDX.
> Al contrario, se si utilizza Microsoft Teams in remoto tramite una sessione HDX ottimizzata, disconnettere la sessione HDX e riconnettersi alla stessa sessione di Windows localmente sul dispositivo. Quando si lavora dall'ufficio, è necessario riavviare Microsoft Teams in modo che possa rilevare correttamente lo stato del PC remoto (HDX o locale), poiché Microsoft Teams può valutare la modalità VDI solo al momento dell'avvio dell'app e non mentre è già in esecuzione in back-

> ground. Senza un riavvio, Microsoft Teams potrebbe non riuscire a caricare funzionalità come finestre disancorate, stanze di lavoro o reazioni alle riunioni.

### Per App Layering

Se si utilizza Citrix App Layering per gestire le installazioni di VDA e Microsoft Teams in livelli diversi, è necessario creare una nuova chiave del Registro di sistema sui VDA Windows prima di installare Microsoft Teams con il flag `ALLUSER=1` dalla riga di comando. Per ulteriori informazioni, vedere la sezione *Ottimizzazione per Microsoft Teams con Citrix App Layering* in Multimedia.

### Consigli per la gestione dei profili

Si consiglia di utilizzare il programma di installazione a livello di macchina per ambienti Windows Server e Windows 10 VDI in pool.

Quando il flag **ALLUSER=1** viene trasferito all'MSI dalla riga di comando (il programma di installazione a livello di macchina), l'app Microsoft Teams viene installata in `C:\Program Files (x86)` (~300 MB). L'app utilizza `AppData\Local\Microsoft\TeamsMeetingAddin` per i log e `AppData\Roaming\Microsoft\Teams` (~ 600-700 MB) per configurazioni specifiche dell'utente, memorizzazione nella cache degli elementi nell'interfaccia utente e così via.

> **Importante:**
>
> Se non si trasferisce il flag **ALLUSER=1**, il file MSI inserisce il programma di installazione Teams.exe e `setup.json` in `C:\Program Files (x86)\Teams Installer`. Una chiave del Registro di sistema (TeamsMachineInstaller) viene aggiunta in: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> Un successivo accesso utente attiva invece l'installazione finale in **AppData**.

#### Programma di installazione a livello di macchina

Di seguito è riportato un esempio di cartelle, collegamenti sul desktop e chiavi del Registro di sistema creati installando il programma di installazione di Microsoft Teams a livello di macchina in una macchina virtuale Windows Server 2016 a 64 bit:

*Cartella:*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Collegamento sul desktop:*

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

*Chiavi del Registro di sistema:*

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nome: `Teams`
- Tipo: `REG_SZ`
- Valore: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Nota:**
>
> La posizione del Registro di sistema varia in base ai sistemi operativi sottostanti e al numero di bit.

#### Consigli

- Si consiglia di disabilitare l'avvio automatico eliminando le chiavi del Registro di sistema di Microsoft Teams. Ciò impedisce che molti accessi che si verificano contemporaneamente (ad esempio, all'inizio della giornata lavorativa) sovraccarichino la CPU della VM.
- Se il desktop virtuale non dispone di una GPU/vGPU, si consiglia di impostare l'opzione **Disable GPU hardware acceleration** (Disabilita l'accelerazione hardware della GPU) nelle **impostazioni** di Microsoft Teams per migliorare le prestazioni. Questa impostazione (`"disableGpu":true`) è memorizzata in `%Appdata%\Microsoft\Teams` in `desktop-config.json`. È possibile utilizzare uno script di accesso per modificare tale file e impostare il valore su **true**.
- Se si utilizza Citrix Workspace Environment Management (WEM), abilitare **CPU Spikes Protection** (Protezione dai picchi di utilizzo della CPU) per gestire il consumo del processore per Microsoft Teams.

#### Programma di installazione per ciascun utente

Quando si utilizza il programma di installazione di `.exe`, il processo di installazione è diverso. Tutti i file sono inseriti in AppData.

*Cartella:*

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Collegamento sul desktop:*

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

*Chiavi del Registro di sistema:*

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

**Procedure consigliate**

I consigli sulle procedure consigliate si basano sugli scenari di utilizzo.
L'utilizzo di Microsoft Teams con una configurazione non persistente richiede un gestore di memorizzazione nella cache dei profili per una sincronizzazione efficiente dei dati di runtime di Microsoft Teams. Con un gestore di memorizzazione nella cache dei profili, le informazioni appropriate specifiche dell'utente vengano memorizzate nella cache durante la sessione utente. Ad esempio, le informazioni specifiche dell'utente includono dati utente, profilo e impostazioni. Sincronizzare i dati in queste due cartelle:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

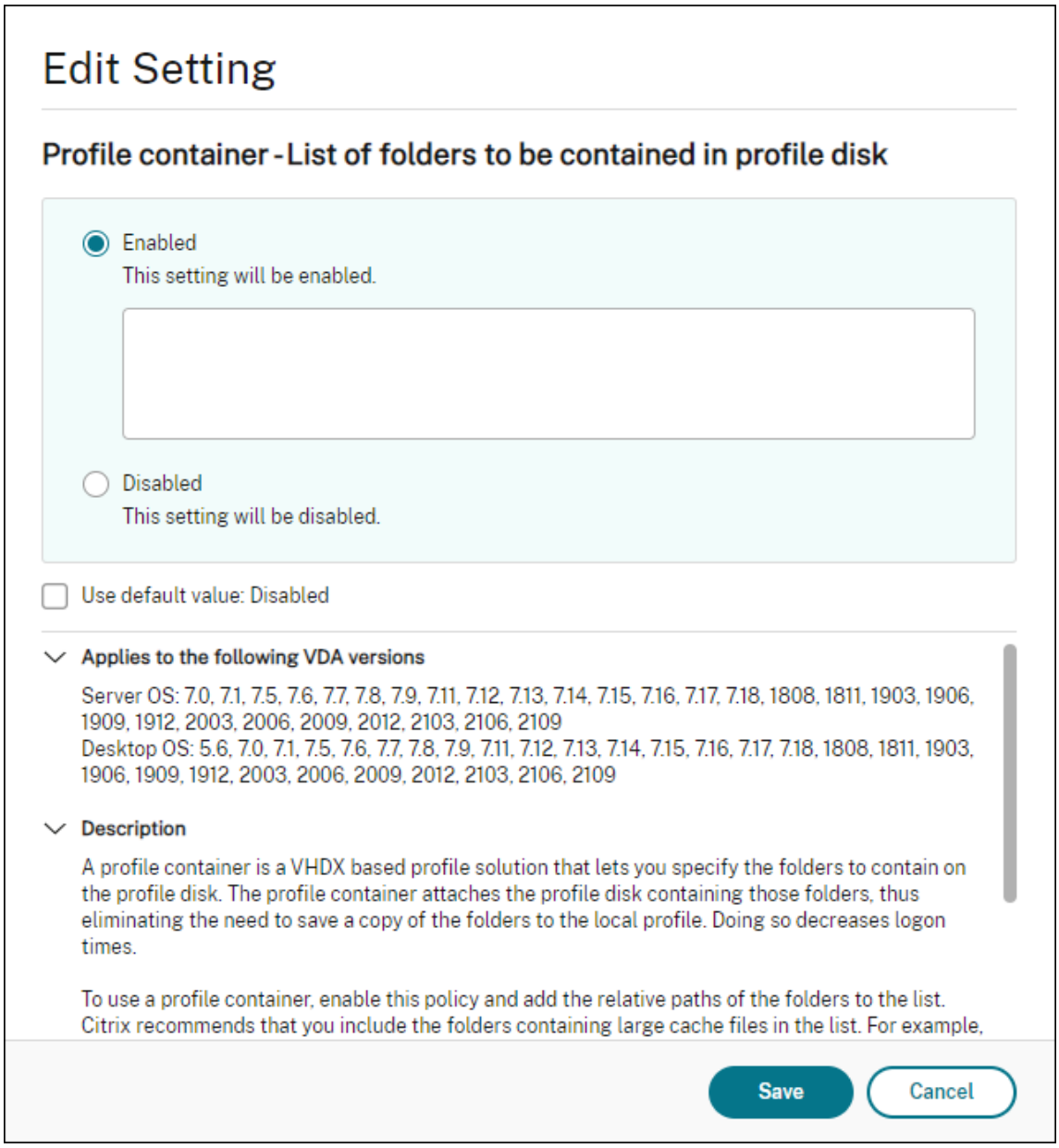
**Elenco di esclusione dei contenuti di Microsoft Teams memorizzati nella cache per la configurazione non persistente** Escludere i file e le directory dalla cartella di memorizzazione nella cache di Microsoft Teams come descritto nella documentazione Microsoft. Questa azione consente di ridurre le dimensioni della memorizzazione nella cache dell'utente per ottimizzare ulteriormente la configurazione non persistente.

**Caso d'uso: scenario con sessione singola** In questo scenario, l'utente finale utilizza Microsoft Teams in una posizione alla volta. Non è necessario eseguire Microsoft Teams in due sessioni Windows contemporaneamente. In una distribuzione di desktop virtuale comune, ogni utente viene assegnato a un desktop e Microsoft Teams viene distribuito all'interno del desktop virtuale come un'unica applicazione.
Si consiglia di abilitare il contenitore Citrix Profile e di reindirizzare nel contenitore le directory per utente elencate in Per-user installer.

1. Distribuire il programma di installazione a livello di macchina di Microsoft Teams (**ALLUSER=1**) nell'immagine golden.
2. Abilitare Citrix Profile Management e configurare l'archivio dei profili utente con le autorizzazioni appropriate.

3. Abilitare la seguente impostazione dei criteri di Profile Management (Gestione profili): **File system > Synchronization (Sincronizzazione) > Profile container –List of folders to be contained in profile disk (Contenitore profilo - Elenco delle cartelle che devono essere contenute nel disco del profilo)**.




Elencare tutte le directory per ciascun utente in questa configurazione. È anche possibile configurare queste impostazioni utilizzando il servizio Citrix WEM (Workspace Environment Management).

4. Applicare le impostazioni al gruppo di consegna corretto.
5. Accedere per convalidare la distribuzione.

## Requisiti di sistema

### Versione minima consigliata - Delivery Controller (DDC) 1906.2

Se si utilizza una versione precedente, vedere Abilitare l'ottimizzazione di Microsoft Teams:

Sistemi operativi supportati:

- Windows Server 2022, 2019, 2016, 2012R2 edizioni Standard e per centri dati e con l'opzione Server Core

### Versione minima - Virtual Delivery Agent (VDA) 1906.2

Sistemi operativi supportati:

- Windows 11.
- Windows 10 a 64 bit, versioni 1607 e successive. Le app ospitate da VM sono supportate nell' app Citrix Workspace per Windows 2109.1 e versioni successive.
- Windows Server 2022, 2019, 2016 e 2012 R2 (edizioni standard e per data center).

Requisiti:

- BCR_x64.msi: file MSI che include il codice di ottimizzazione di Microsoft Teams e viene avviato automaticamente dalla GUI. Se si utilizza l'interfaccia della riga di comando per l'installazione del VDA, non escluderlo.

### Versione consigliata: versione corrente più recente dell'app Citrix Workspace per Windows e versione minima: app Citrix Workspace 1907 per Windows

- Windows 11.
- Windows 10 (edizioni a 32 bit e 64 bit, incluse le edizioni Embedded) (il supporto di Windows 7 è stato interrotto alla versione 2006) (il supporto di Windows 8.1 è stato interrotto alla versione 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Architetture di processore (CPU) supportate: x86 e x64 (ARM non è supportato).
- Requisiti endpoint: CPU dual core di circa 2,2-2,4 GHz in grado di supportare una risoluzione HD a 720p durante una chiamata in videoconferenza peer-to-peer.
- CPU dual o quad-core con velocità base più basse (~1,5 GHz) dotate di Intel Turbo Boost o AMD Turbo Core con possibile aumento fino ad almeno 2,4 GHz.
- Thin client HP verificati: t630/t640, t730/t740, mt44/mt45.
- Thin client Dell verificati: 5070, 5470 Mobile TC e AIO.
- Thin Client 10ZiG verificati: 4510 e 5810q.

- Per un elenco completo degli endpoint verificati, vedere Thin client.
- L'app Citrix Workspace richiede almeno 600 MB di spazio libero su disco e 1 GB di RAM.
- Il requisito minimo di Microsoft .NET Framework è la versione 4.8. L'app Citrix Workspace scarica e installa automaticamente .NET Framework se non è presente sul sistema.

Gli amministratori possono abilitare/disabilitare Microsoft Teams a partire dalla modalità ottimizzata modificando il criterio di ottimizzazione di Teams. Gli utenti che iniziano in modalità ottimizzata nell'app Citrix Workspace non possono di disabilitare Microsoft Teams.

#### Versione minima: app Citrix Workspace 2006 per Linux

Software:

- `GStreamer` 1.0 o versione successiva o Cairo 2
- libc++-9.0 o versioni successive
- `libgdk` 3.22 o versione successiva
- OpenSSL 1.1.1d
- Distribuzione Linux x64

Hardware:

- CPU dual-core da almeno 1,8 GHz in grado di supportare una risoluzione HD a 720p durante una chiamata in videoconferenza peer-to-peer
- CPU dual o quad-core con una velocità base di 1,8 GHz e un'alta velocità Intel Turbo Boost di almeno 2,9 GHz

Per un elenco completo degli endpoint verificati, vedere Thin client.

Per ulteriori informazioni, vedere Prerequisiti per installare l'app Citrix Workspace.

È possibile disabilitare l'ottimizzazione di Microsoft Teams aggiornando il valore del campo **VDWEBRTC** su Off nel file `/opt/Citrix/ICAClient/config/module.ini`. Il valore predefinito è VDWEBRTC=On. Una volta completato l'aggiornamento, riavviare la sessione. (è richiesta l'autorizzazione root).

#### Versione minima: app Citrix Workspace 2012 per Mac

Sistemi operativi supportati:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 e versione successiva.
- macOS Monterey.

Funzionalità supportate:

- Audio
- Video
- Ottimizzazione della condivisione dello schermo (in entrata e in uscita)

> **Nota:**
>
> L'app Citrix Viewer richiede l'accesso alle preferenze di sicurezza e privacy di macOS perché la condivisione dello schermo possa funzionare. Gli utenti configurano questa preferenza accedendo al **menu Apple > Preferenze di sistema > Sicurezza e privacy > scheda Privacy > Registrazione dello schermo** e selezionando **Citrix Viewer**.

L'ottimizzazione di Microsoft Teams funziona per impostazione predefinita con l'app Citrix Workspace 2012 o versioni successive e macOS 10.15.

Se si desidera disabilitare l'ottimizzazione di Microsoft Teams, eseguire questo comando nel terminale e riavviare l'app Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

**Versione minima: l'ultima versione dell'app Citrix Workspace per Chrome OS in esecuzione sull'ultima versione di Chrome OS**

Hardware:

- Processori che funzionano alla pari o meglio di Intel i3, quad core da 2,4 GHz.

Funzionalità supportate:

- Audio
- Video
- Ottimizzazione della condivisione dello schermo (in entrata e in uscita): disabilitata per impostazione predefinita. Consultare queste impostazioni per istruzioni su come abilitarla.

## Scalabilità di un singolo server

Questa sezione fornisce consigli e indicazioni su come stimare il numero di utenti o macchine virtuali (VM) che possono essere supportati su un singolo host fisico. Questo è comunemente indicato come Scalabilità per server singolo di Citrix Virtual Apps and Desktops (SSS). Nel contesto di Citrix Virtual Apps (CVA) o della virtualizzazione delle sessioni, è anche comunemente noto come densità degli utenti. L'idea è scoprire quanti utenti o quante macchine virtuali possono essere eseguiti su un singolo componente hardware che esegue un hypervisor principale.

> **Nota:**
>
> Questa sezione include una guida per stimare l'SSS. Tenere presente che la guida è di alto livello e potrebbe non essere necessariamente specifica per la propria situazione o il proprio ambiente specifico. L'unico modo per comprendere veramente l'SSS di Citrix Virtual Apps and Desktops è utilizzare uno strumento di test di scalabilità o carico come Login VSI. Citrix consiglia di utilizzare questa guida e queste semplici regole per stimare rapidamente solo l'SSS. Tuttavia, Citrix consiglia di utilizzare Login VSI o lo strumento di test di carico preferito per convalidare i risultati, soprattutto prima di acquistare hardware o prendere decisioni finanziarie.

#### Hardware (sistema in prova)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (max Turbo 3,70 GHz), 12 core per socket, doppio socket con Hyperthreading abilitato
- 382 GB di RAM
- Archiviazione RAID 0 SSD locale (11 dischi) 6 TB

#### Software

Una singola macchina virtuale (40 processori logici) con Windows 2019 (TSVDA) che esegue Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

#### Terminologia

- Carico di lavoro del lavoratore della conoscenza: include Acrobat Reader, Freemind/Java, Photo Viewer, Edge e app MS Office come Excel, Outlook, PowerPoint e Word.
- Baseline: test di scalabilità server eseguiti con il carico di lavoratore della conoscenza (senza Microsoft Teams)
- Carico di lavoro di Microsoft Teams: carico di lavoro tipico dei lavoratori della conoscenza + Microsoft Teams

#### Come Microsoft Teams viene sottoposto a test di stress

- Microsoft Teams è ottimizzato con HDX. Pertanto, tutta l'elaborazione multimediale viene scaricata sull'endpoint o sul client e non fa parte della misurazione.
- Tutti i processi di Microsoft Teams si sono arrestati o interrotti prima dell'inizio
- Aprire Microsoft Teams (avvio a freddo).

- Misurare il tempo impiegato da Microsoft Teams per caricare e catturare l'attenzione della finestra principale di Microsoft Teams.
- Passare alla finestra di chat usando i tasti di scelta rapida.
- Passare alla finestra del calendario usando i tasti di scelta rapida.
- Inviare il messaggio di chat a un utente specifico utilizzando le scorciatoie da tastiera.
- Passare alla finestra di Microsoft Teams utilizzando le scorciatoie da tastiera

**Risultati**

- Impatto sulla scalabilità del 40% con Microsoft Teams Workload (81 utenti) rispetto a Baseline (137 utenti).
- L'aumento della capacità del server di circa il 40% (in CPU) ripristina il numero di utenti come con il carico di lavoro Baseline.
- 20% di memoria extra richiesta con Microsoft Teams Workload, rispetto a Baseline.
- Aumento delle dimensioni di archiviazione per utente di 512-1024 MB.
- circa il 50% di incremento in scrittura IOPS, circa il 100% di incremento nelle letture IOPS. Microsoft Teams può avere un impatto significativo in ambienti con archiviazione più lenta.

## Supporto delle funzionalità e versioni supportate

| Funzionalità | Microsoft Teams (versione minima) | VDA (versione minima) | App Citrix Workspace per Windows CR (versione minima) | App Citrix Workspace per Mac (versione minima) | App Citrix Workspace per Linux (versione minima) | App Citrix Workspace per Chrome OS |
|---|---|---|---|---|---|---|
| Audio/Video (P2P e conferenza) | versione attuale meno 90 giorni | 1906 | 1907 | 2009 | 2004 | 2105.5 |
| Condivisione dello schermo | Versione attuale meno 90 giorni | 1906 | 1907 | 2012 | 2006 | 2105.5 |

| Funzionalità | Microsoft Teams (versione minima) | VDA (versione minima) | App Citrix Workspace per Windows CR (versione minima) | App Citrix Workspace per Mac (versione minima) | App Citrix Workspace per Linux (versione minima) | App Citrix Workspace per Chrome OS |
|---|---|---|---|---|---|---|
| i. Indicatore schermo Bordo rosso | Versione attuale meno 90 giorni | 1906 | 2002 | 2012 | 2006 | No |
| ii. Limita l' acqui-sizione in Desktop Viewer | Versione attuale meno 90 giorni | 1906 | 2009.5 | 2012 | 2006 | No |
| iii. Multi-monitor | Versione attuale meno 90 giorni | 1912 CU6+ | 2106 (1) | 2106 | 2106 | No |
| DTMF | Versione attuale meno 90 giorni | N/A | 2102 | 2101 | 2101 | 2111.1 |
| Supporto dei server proxy | Versione attuale meno 90 giorni | N/A | 2012 (2) | 2104 (3) | 2101 (3) | 2305 |
| Condivisione di app | Versione attuale meno 90 giorni | 2109 | 2109.1 | 2203.1 | 2209 | No |
| Sottotitoli live | Versione attuale meno 90 giorni | N/A (4) | 2109.1 | 2109 | 2109 | 2303 |

| Funzionalità | Microsoft Teams (versione minima) | VDA (versione minima) | App Citrix Workspace per Windows CR (versione minima) | App Citrix Workspace per Mac (versione minima) | App Citrix Workspace per Linux (versione minima) | App Citrix Workspace per Chrome OS |
|---|---|---|---|---|---|---|
| e911 dinamico | Versione attuale meno 90 giorni | N/A | 2112.1 | 2112 | 2112 | 2112 |
| Concedere il controllo | Versione attuale meno 90 giorni | N/A | 2112.1 | 2203.1 | No | No |
| Richiedi il controllo | Versione attuale meno 90 giorni | N/A | 2112.1 | 2203.1 | 2203 | 2303 |
| Multifinestra | 1.5.00.11865 | 2112, 1912 CU6 (5) | 2112.1 | 2203.1 | 2203 | 2303 |
| Trascrizioni delle riunioni | Versione attuale meno 90 giorni | 2112.1, 1912 CU6+ | 2112 | 2203.1 | 2203 | 2303 |
| Sfocatura dello sfondo | Versione attuale meno 90 giorni | 2112, 1912 CU6+ | 2207 | 2301 | 2212 | 2303 |

1. Visualizzatore CD solo in modalità a schermo intero. MAIUSC+F2 non supportato.
2. Negotiate/Kerberos, NTLM, Basic e Digest. Sono supportati anche i file Pac.
3. Solo anonimo.
4. Se VDA è 2112 o superiore, Live Captions funzionerà solo se la versione dell'app Citrix Workspace è 2203.1 per MAC e 2203 Linux o 2112 per Windows. Questo perché Live Captions si comporta in modo diverso se Microsoft Teams è in modalità interfaccia utente a finestra singola o multifinestra.
5. La modalità multifinestra è stata introdotta nel VDA versione 2112, ma è stata trasferita alla versione VDA 1912 LTSR CU6.

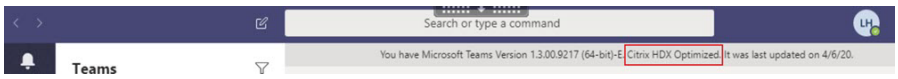
> **Nota:**
>
> Tutte le funzionalità elencate nell'**app Citrix Workspace per Windows 1912 CU6 (o versione successiva)** sono applicabili all'app Citrix Workspace per Windows 2203.1 LTSR CU1.

### Abilitare l'ottimizzazione di Microsoft Teams

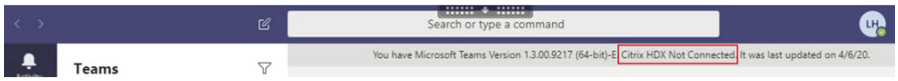
Per abilitare l'ottimizzazione per Microsoft Teams, utilizzare i criteri di gestione della console descritti nel criterio di reindirizzamento di Microsoft Teams. Questo criterio è **ON** (attivato) per impostazione predefinita. Oltre all'abilitazione di questo criterio, HDX verifica che la versione dell'app Citrix Workspace corrisponda almeno alla versione minima richiesta. Se il criterio è stato abilitato e la versione dell'app Citrix Workspace è supportata, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRe** viene impostato automaticamente su **1** sul VDA. Microsoft Teams legge la chiave per caricarsi in modalità VDI.

> **Nota:**
>
> Se si utilizzano VDA versione 1906.2 o successiva con versioni precedenti del controller (ad esempio, versione 7.15) che non dispongono del criterio disponibile in Manage console (Gestione console) (Studio), il VDA può comunque essere ottimizzato. L'ottimizzazione HDX per Microsoft Teams è abilitata per impostazione predefinita nel VDA.

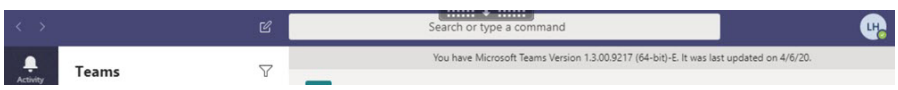
Se si fa clic su **About (Informazioni) > Version (Versione)**, viene visualizzata la legenda **Citrix HDX Optimized (Ottimizzato per Citrix HDX)**:




Se viene visualizzato il messaggio **Citrix HDX Not Connected** (Citrix HDX non connesso), l'API Citrix viene caricata in Microsoft Teams. Il caricamento dell'API è il primo passo verso il reindirizzamento. Ma c'è un errore nelle parti successive dello stack. L'errore è molto probabilmente nei servizi VDA o nell'app Citrix Workspace.




Se non viene visualizzata alcuna legenda, Microsoft Teams non è riuscito a caricare l'API Citrix. Uscire da Microsoft Teams facendo clic con il pulsante destro del mouse sull'icona dell'area di notifica e riavviare l'applicazione. Assicurarsi che il criterio Manage console (Gestisci console) non sia impostato su **Prohibited** (Non consentito) e che la versione dell'app Citrix Workspace sia supportata.



> **Importante: riconnessioni di sessione**
>
> - Potrebbe essere necessario riavviare Microsoft Teams per ottenere una sessione ottimizzata per HDX quando la connettività cambia. Ad esempio, se si sta eseguendo il roaming da un endpoint non supportato (app Workspace per iOS, Android o versioni precedenti di Windows/Linux/Mac) a uno supportato (app Workspace per Windows/Linux/Mac/ChromeOS/HTML5) o nella direzione opposta.
> - Un rilancio di Microsoft Teams è necessario anche se è stata installata l'app utilizzando il programma di installazione .exe di Microsoft Teams nel VDA. Il programma di installazione .exe è consigliato per le distribuzioni VDI persistenti. In questi casi, Microsoft Teams può aggiornarsi automaticamente mentre la sessione HDX è in stato disconnesso. Pertanto, gli utenti che si riconnettono a una sessione HDX trovano che l'esecuzione di Microsoft Teams non è ottimizzata.
> - Quando si passa da una sessione locale a una sessione HDX, si deve riavviare Microsoft Teams per l'ottimizzazione con HDX. Questa azione è necessaria in uno scenario di accesso remoto al PC.

## Requisiti di rete

Microsoft Teams si affida ai server del processore di contenuti multimediali di Microsoft 365 per riunioni o chiamate con più partecipanti. Inoltre, Microsoft Teams si basa sui relè di trasporto di Microsoft 365 per questi scenari:

- Due peer in una chiamata point-to-point non hanno connettività diretta
- Un partecipante non dispone di connettività diretta al processore multimediale.

Di conseguenza, l'integrità della rete tra il peer e il cloud di Microsoft 365 determina le prestazioni della chiamata. Per linee guida dettagliate sulla pianificazione della rete, vedere Principi di connettività di rete di Microsoft 365.

Si consiglia di valutare l'ambiente per identificare eventuali rischi e requisiti che possono influenzare la distribuzione globale di voce e video nel cloud.
Utilizzare lo strumento di valutazione della rete Skype for Business per verificare se la rete è pronta per Microsoft Teams. Per informazioni sull'assistenza, vedere Supporto.

### Riepilogo delle principali raccomandazioni di rete per il traffico RTP (Real Time Protocol)

- Connettersi alla rete di Microsoft 365 il più direttamente possibile dalla filiale.
- Pianificare e fornire una larghezza di banda sufficiente presso la filiale.
- Verificare la connettività e la qualità della rete di ogni filiale.

- Assicurarsi che sia adottato il traffico RTP/UDP (gestito da HdxRtcEngine.exe nell'app Citrix Workspace) se è necessario utilizzare uno dei seguenti elementi presso la filiale.
  - Ignorare i server proxy
  - Intercettazione SSL di rete
  - Dispositivi di ispezione profonda dei pacchetti
  - Hairpin VPN (utilizzare lo split tunneling se possibile)

> **Importante: configurazione VPN Split tunnel**
>
> Il traffico di HdxRtcEngine.exe deve essere deviato dal tunnel VPN e autorizzato a utilizzare la connessione Internet locale dell'utente per connettersi direttamente al servizio. Il modo in cui ciò viene realizzato varia a seconda del prodotto VPN e della piattaforma della macchina utilizzata, ma la maggior parte delle soluzioni VPN consente una semplice configurazione dei criteri per applicare questa logica. Per ulteriori informazioni sulla guida allo split tunnelling specifico per la piattaforma VPN, vedere questo articolo Microsoft.

Il motore multimediale WebRTC nell'app Workspace (HdxRtcEngine.exe) utilizza il protocollo SRTP (Secure Real-Time Transport Protocol) per i flussi multimediali di cui viene eseguito l'offloading nel client. SRTP assicura riservatezza e autenticazione all'RTP. Per questa funzione, vengono utilizzate le chiavi simmetriche (negoziate con DTLS) per crittografare i media e controllare i messaggi utilizzando il cifrario di crittografia AES.

Le seguenti metriche sono consigliate per un'esperienza utente positiva:

| Metrica | Endpoint a Microsoft 365 |
|---|---|
| Latenza (a senso unico) | < 50 msec |
| Latenza (RTT) | < 100 msec |
| Perdita di pacchetti | <1% durante ogni intervallo di 15 secondi |
| Jitter inter-arrivo dei pacchetti | <30 ms durante ogni intervallo di 15 secondi |

Per ulteriori informazioni, vedere Preparare la rete dell'organizzazione per Microsoft Teams.

Per quanto riguarda i requisiti di larghezza di banda, l'ottimizzazione per Microsoft Teams può utilizzare un'ampia gamma di codec per audio (OPUS/G.722/PCM G711) e video (H264).

I peer negoziano questi codec durante il processo di creazione delle chiamate utilizzando l'offerta/risposta SDP (Session Description Protocol).
Le raccomandazioni minime di Citrix per utente sono:

| Tipo | Larghezza di banda | Codec |
|---|---|---|
| Audio (tutte le direzioni) | ~ 90 kbps | G.722 |
| Audio (tutte le direzioni) | ~ 60 kbps | Opus* |
| Video (tutte le direzioni) | ~ 700 kbps | H264 360p @ 30 fps 16:9 |
| Condivisione dello schermo | ~ 300 kbps | H264 1080p @ 15 fps |

Opus e H264 sono i codec preferiti per le chiamate peer-to-peer e in conferenza.

> **Importante:**
>
> Per quanto riguarda le prestazioni, la codifica è più costosa della decodifica per l'uso della CPU sul computer client. È possibile codificare la massima risoluzione di codifica nell'app Citrix Workspace per Linux e Windows. Vedere Stima delle prestazioni dell'encoder e Ottimizzazione per Microsoft Teams.

### Server proxy

A seconda della posizione del proxy, considerare quanto segue:

- Configurazione proxy sul VDA:

  Se si configura un server proxy esplicito nel VDA e si instradano le connessioni all'host locale tramite un proxy, il reindirizzamento non riesce. Per configurare correttamente il proxy, è necessario selezionare l'impostazione **Bypass proxy servers for local address** (Ignora i server proxy per l'indirizzo locale) in **Opzioni Internet > Connessioni > Impostazioni LAN > Server proxy** e ignorare `127.0.0.1:9002`.

  Se si utilizza un file PAC, lo script di configurazione del proxy VDA del file PAC deve restituire **DIRECT** per `wss://127.0.0.1:9002`. In caso contrario, l'ottimizzazione non riesce. Per assicurarsi che lo script restituisca **DIRECT**, utilizzare `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configurazione proxy sull'app Citrix Workspace:

  Se la filiale è configurata per accedere a Internet tramite un proxy, queste versioni supportano i server proxy:

  - App Citrix Workspace per Windows versione 2012 (Negotiate/Kerberos, NTLM, Basic e Digest; sono supportati anche i file Pac)
  - App Citrix Workspace per Windows versione 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Sono supportati anche i file Pac)

- App Citrix Workspace per Linux versione 2101 (autenticazione anonima)
- App Citrix Workspace per Mac versione 2104 (autenticazione anonima)

I dispositivi client con versioni precedenti dell'app Citrix Workspace non possono leggere le configurazioni proxy. Questi dispositivi inviano il traffico direttamente ai server TURN di Microsoft 365.

> **Importante:**
>
> - Verificare che il dispositivo client possa connettersi al server DNS per effettuare le risoluzioni DNS. Un dispositivo client deve essere in grado di risolvere i seguenti FQDN del server Microsoft Teams Relay:
>
>   - `worldaz.relay.teams.microsoft.com`
>   - `inaz.relay.teams.microsoft.com`
>   - `uaeaz.relay.teams.microsoft.com`
>   - `euaz.relay.teams.microsoft.com`
>   - `usaz.relay.teams.microsoft.com`
>   - `turn.dod.teams.microsoft.us`
>   - `turn.gov.teams.microsoft.us`
>
> Se le richieste DNS non hanno esito positivo, le chiamate P2P con utenti esterni e la creazione di supporti per le teleconferenze non riescono.
>
> - La posizione del server della conferenza viene selezionata in base alla posizione del desktop virtuale (non al client) del primo partecipante.

### Percorsi per l'avvio di chiamate e il flusso di contenuti multimediali

Quando possibile, il motore multimediale HDX WebRTC nell'app Citrix Workspace (HdxRtcEngine.exe) tenta di stabilire una connessione SRTP (Secure Real-Time Transport Protocol) di rete diretta tramite UDP (User Datagram Protocol) in una chiamata peer-to-peer. Se le porte UDP alte sono bloccate, il motore multimediale torna a TCP/TLS 443.

Il motore multimediale HDX supporta ICE, STUN (Session Traversal Utilities for NAT) e TURN (Traversal Using Relays around NAT) per individuare candidati e stabilire connessioni. Questo supporto significa che l'endpoint deve essere in grado di eseguire risoluzioni DNS.

Si consideri uno scenario in cui non esiste un percorso diretto tra i due peer o tra un peer e un server di conferenza e si sta partecipando a una chiamata o a una riunione con più parti. HdxRtcEngine.exe utilizza un relé server di trasporto Microsoft Teams in Microsoft 365 per raggiungere l'altro peer o il processore multimediale, dove sono ospitate le riunioni. Il computer client deve avere accesso a tre intervalli di indirizzi IP di subnet di Microsoft 365 e quattro porte UDP (o TCP/TLS 443 come fallback se UDP è bloccato). Per ulteriori informazioni, vedere il diagramma Architettura in Configurazione delle chiamate e URL di Office 365 e intervalli di indirizzi IP ID 11.

| ID | Categoria | Indirizzi | Porte di destinazione |
|---|---|---|---|
| 11 | Ottimizzazione richiesta | 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14 | **UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (fallback) |

Questi intervalli includono sia i relè di trasporto che i processori multimediali, con un sistema di bilanciamento del carico di Azure come front-end.
I relè di trasporto di Microsoft Teams forniscono funzionalità STUN e TURN, ma non sono endpoint ICE. Inoltre, i relè di trasporto di Microsoft Teams non interrompono gli elementi multimediali o TLS e non eseguono alcuna transcodificazione. Possono collegare TCP (se HdxRtcEngine.exe utilizza TCP) a UDP quando inoltrano il traffico ad altri peer o processori multimediali.

Il motore multimediale WebRTC dell'app Workspace contatta il relè di trasporto di Microsoft Teams più vicino nel cloud di Microsoft 365. Il motore multimediale utilizza IP anycast e le porte UDP 3478-3481 (porte UDP diverse per carico di lavoro, anche se può verificarsi il multiplexing) o 443 TCP/TLS per i fallback. La qualità delle chiamate dipende dal protocollo di rete sottostante. Poiché UDP è sempre consigliato su TCP, si consiglia di progettare le reti in modo da supportare il traffico UDP nella filiale.

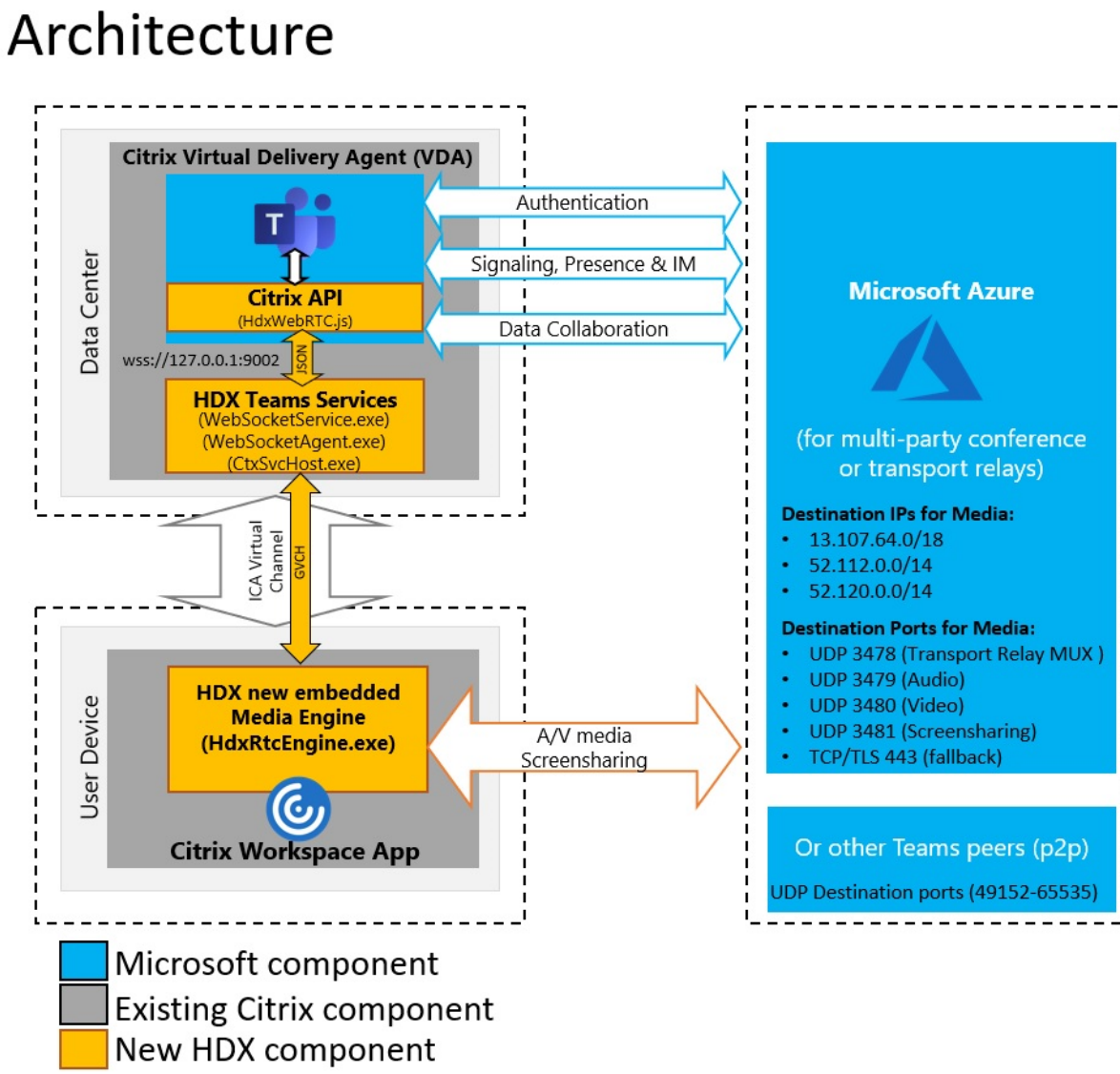
Se Microsoft Teams è stato caricato in modalità ottimizzata e HdxRtcEngine.exe è in esecuzione sull'endpoint, gli errori ICE potrebbero causare un errore di configurazione delle chiamate o audio/video monodirezionale. Quando una chiamata non può essere completata o i flussi multimediali non sono full duplex, controllare prima la **traccia Wireshark** sull'endpoint. Per ulteriori informazioni sul processo di raccolta dei candidati ICE, vedere "Raccolta dei log"nella sezione Supporto.

> **Nota:**
>
> Se gli endpoint non hanno accesso a Internet, potrebbe comunque essere possibile per gli utenti effettuare una chiamata peer-to-peer se si trovano entrambi sulla stessa LAN. Non è possibile tenere riunioni. In questo caso, c'è un timeout di 30 secondi prima dell'inizio della configurazione della chiamata.

#### Configurazione delle chiamate

Utilizzare questo diagramma di architettura come riferimento visivo per la sequenza del flusso di chiamata. I passaggi corrispondenti sono indicati nel diagramma.




**Architettura**

1. Avviare Microsoft Teams.
2. Microsoft Teams si autentica in O365. I criteri tenant vengono spostati al client Microsoft Teams e le informazioni pertinenti relative a TURN e al canale di segnalazione vengono inoltrate all'app.
3. Microsoft Teams rileva che è in esecuzione in un VDA ed effettua chiamate API all'API JavaScript Citrix.
4. Il JavaScript Citrix in Microsoft Teams apre una connessione WebSocket sicura a WebSocketService.exe in esecuzione sul VDA, che genera WebSocketAgent.exe all'interno della sessione utente.
5. WebSocketAgent.exe crea un'istanza di un canale virtuale generico chiamando il servizio di reindirizzamento di Microsoft Teams Citrix HDX (CtxSvcHost.exe).

6. wfica32.exe (motore HDX) dell'app Citrix Workspace genera un nuovo processo chiamato HdxRtcEngine.exe, che è il nuovo motore WebRTC utilizzato per l'ottimizzazione di Microsoft Teams.
7. Il motore multimediale Citrix e Teams.exe hanno un percorso di canale virtuale a 2 vie e possono iniziare a elaborare le richieste multimediali.

   ——Chiamate dell'utente——

8. Il **peer A** fa clic sul pulsante di **chiamata**. Teams.exe comunica con i servizi Microsoft Teams in Microsoft 365 stabilendo un percorso di segnalazione end-to-end con il **peer B**. Microsoft Teams chiede a HdxRtcEngine una serie di parametri di chiamata supportati (codec, risoluzioni e così via, questo è noto come offerta SDP [Session Description Protocol]). Questi parametri di chiamata vengono quindi inoltrati utilizzando il percorso di segnalazione ai servizi Microsoft Teams in Microsoft 365 e da lì all'altro peer.
9. L'offerta/risposta SDP (negoziazione a passaggio singolo) avviene attraverso il canale di segnalazione e vengono completati i controlli di connettività ICE (attraversamenti NAT e firewall utilizzando le richieste di associazione STUN). Quindi, i contenuti multimediali SRTP (Secure Real-time Transport Protocol) vanno direttamente da HdxRtcEngine all'altro peer e viceversa (o i Conference Server Microsoft 365 se si tratta di una riunione).

### Microsoft Phone System

Phone System è la tecnologia Microsoft che consente il controllo delle chiamate e PBX nel cloud di Microsoft 365 con Microsoft Teams. L'ottimizzazione per Microsoft Teams supporta Phone System, utilizzando i piani di chiamata di Microsoft 365 o il routing diretto. Con il routing diretto è possibile connettere il session border controller supportato da Microsoft Phone System direttamente senza alcun software locale aggiuntivo.
Sono supportati code di chiamata, trasferimento, inoltro, messa in pausa, disattivazione dell'audio e ripresa di una chiamata.

#### DTMF

La funzione DTMF (Dual Tone Multi Frequency) è supportata con queste versioni dell'app Citrix Workspace (e versione successiva):

- App Citrix Workspace per Windows versione 2102
- App Citrix Workspace per Windows LTSR 1912 CU5 (solo sistema operativo Windows 10)
- App Citrix Workspace per Linux versione 2101
- App Citrix Workspace per Mac versione 2101
- App Citrix Workspace per Chrome OS versione 2111.1

### Supporto di e911 dinamico

A partire dalla versione 2112, l'app Citrix Workspace supporta le chiamate di emergenza dinamiche. Se utilizzato in Microsoft Calling Plans, Operator Connect e Direct Routing, consente di eseguire le seguenti operazioni:

- Configurare e indirizzare le chiamate di emergenza.
- Informare il personale di sicurezza.

La notifica viene fornita in base alla posizione corrente dell'app Citrix Workspace in esecuzione sull'endpoint, anziché sul client Microsoft Teams in esecuzione sul VDA.

La legge di Ray Baum richiede che la posizione inviabile di chi chiama il 911 sia trasmessa al Public Safety Answering Point (PSAP) appropriato. L'ottimizzazione di Microsoft Teams con HDX è conforme alla legge di Ray Baum se utilizzata con le seguenti versioni dell'app Citrix Workspace:

- App Citrix Workspace per Windows versione 2112.1 e successiva
- App Citrix Workspace per Linux versione 2112 e successiva
- App Citrix Workspace per Mac versione 2112 e successiva
- App Citrix Workspace per Chrome OS versione 2112 e successiva

Per abilitare le chiamate di emergenza dinamiche, l'amministratore deve utilizzare l'interfaccia di amministrazione di Microsoft Teams e configurare quanto segue per creare una mappa della posizione di rete o di emergenza:

- Impostazioni di rete
- Servizio informazioni sulla posizione (LIS)

Per ulteriori informazioni sulle chiamate di emergenza dinamiche, vedere la documentazione di Microsoft.

Le informazioni sulla posizione inviabili che l'app Citrix Workspace inoltra a Microsoft Teams sono:

- ID chassis/ID porta utilizzando il Link Layer Discovery Protocol (LLDP) per le connessioni Ethernet/Switch. Ethernet/Switch (LLDP) è supportato su:
  - Versioni Windows 8.1 e 10
  - macOS, che richiede il software di abilitazione LLDP. Per scaricare il software di abilitazione LLDP, passare a `www.microsoft.com` e cercare il software di abilitazione LLDP.
  - Linux, che richiede che la libreria LLDP sia inclusa nella distribuzione del sistema operativo (OS) del Thin Client.
- WLAN BBSID e {IPv4-IPv6; Subnet; MAC Address} dell'endpoint in cui è installata l'app Citrix Workspace.

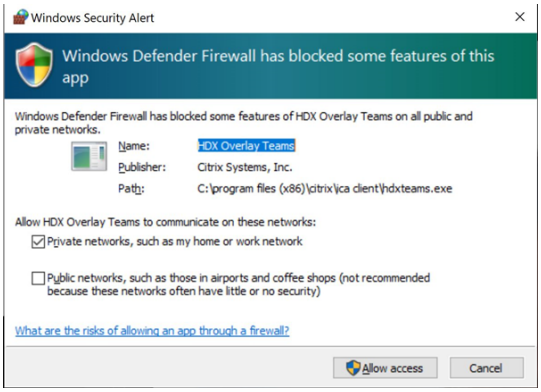
  - Le posizioni basate su subnet e WiFi sono supportate nell'app Workspace per Windows, Linux e Mac.

- Latitudine e longitudine, se l'autorizzazione dell'utente è concessa a livello del sistema operativo in cui è installata l'app Citrix Workspace.

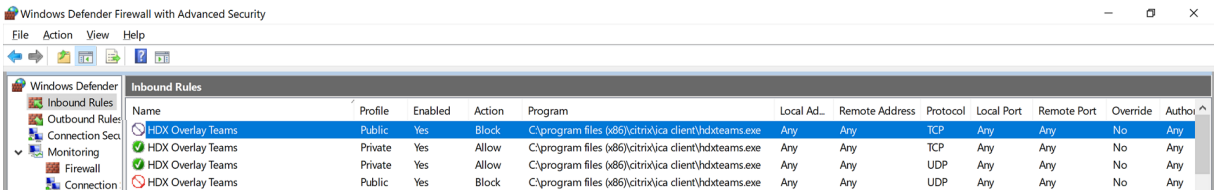
  - Funzionalità supportata su tutte le piattaforme app Workspace. Tuttavia, in Citrix Workspace for Linux, è necessario includere la libreria `libgps` nella distribuzione del sistema operativo del Thin Client (sudo apt-get install libgps23 gpsd lldpd).

### Considerazioni sul firewall

Quando gli utenti avviano una chiamata ottimizzata utilizzando il client Microsoft Teams per la prima volta, potrebbero notare un avviso nelle impostazioni del **firewall di Windows**. L'avviso richiede agli utenti di consentire la comunicazione per HdxTeams.exe o HdxRtcEngine.exe (HDX Overlay Microsoft Teams).




Le quattro voci seguenti vengono aggiunte in **Regole in entrata** nella console **Windows Defender Firewall > Sicurezza avanzata**. Se si desidera, è possibile applicare regole più restrittive.



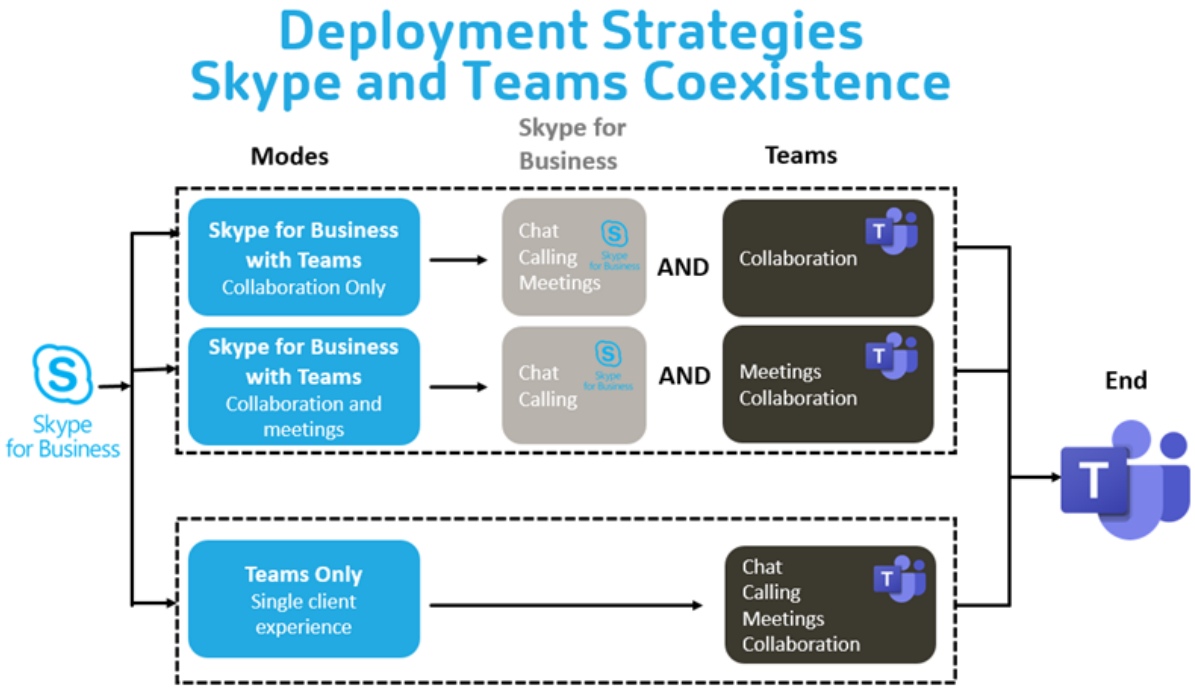

### Coesistenza di Microsoft Teams e Skype for Business

È possibile distribuire Microsoft Teams e Skype for Business fianco a fianco, come due soluzioni separate con funzionalità sovrapposte.
Per ulteriori informazioni, vedere Comprendere la coesistenza e l'interoperabilità di Microsoft Teams e Skype for Business.

Citrix RealTime Optimization Pack e l'ottimizzazione HDX per i motori multimediali di Microsoft Teams rispettano quindi la configurazione impostata nell'ambiente. Gli esempi includono le modalità isola e Skype for Business con la collaborazione in Microsoft Teams. Inoltre, Skype for Business con la collaborazione e le riunioni di Microsoft Teams.

L'accesso alle periferiche può essere concesso solo a una singola applicazione alla volta. Ad esempio, l'accesso alla webcam da parte di RealTime Media Engine durante una chiamata blocca il dispositivo di imaging durante una chiamata. Quando il dispositivo viene rilasciato, diventa disponibile per Microsoft Teams.




### Citrix SD-WAN: connettività di rete ottimizzata per Microsoft Teams

La qualità audio e video ottimale richiede una connessione di rete al cloud di Microsoft 365 con bassa latenza, basso jitter e bassa perdita di pacchetti. Il backhauling del traffico RTP audio-video di Microsoft Teams dagli utenti dell'app Citrix Workspace nelle sedi delle filiali a un centro dati prima del passaggio a Internet può aggiungere latenza eccessiva. Potrebbe anche causare congestione sui collegamenti WAN. Citrix SD-WAN ottimizza la connettività per Microsoft Teams seguendo i principi di connettività di rete di Microsoft 365. Citrix SD-WAN utilizza l'indirizzo IP e il servizio web di Microsoft 365 basati su Microsoft REST e il DNS di prossimità. Tutto questo serve a identificare, classificare e indirizzare il traffico di Microsoft Teams.

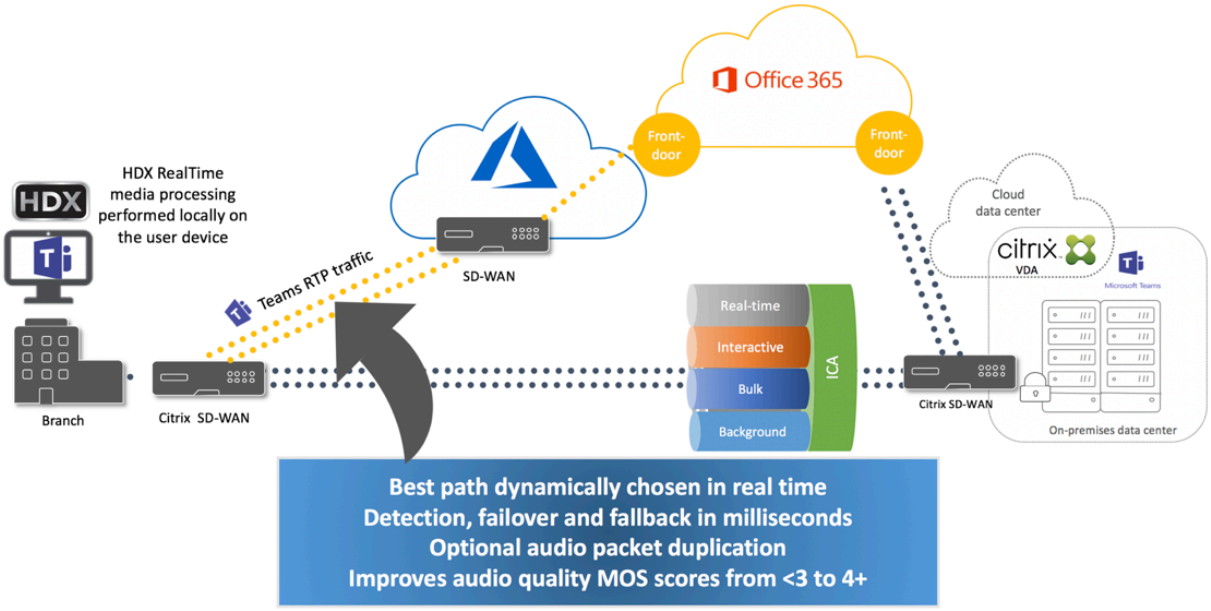
Le connessioni a Internet aziendali a banda larga in molte zone soffrono di perdite intermittenti di pacchetti, periodi di jitter eccessivo e interruzioni.

Citrix SD-WAN offre due soluzioni per preservare la qualità audio-video di Microsoft Teams quando lo stato della rete è variabile o degradato.

- Se si utilizza Microsoft Azure, un'appliance virtuale Citrix SD-WAN (VPX) distribuita nella rete virtuale di Azure fornisce ottimizzazioni di connettività avanzate. Queste ottimizzazioni includono il failover dei collegamenti senza soluzione di continuità e il racing dei pacchetti audio.
- I clienti Citrix SD-WAN possono connettersi a Microsoft 365 tramite il servizio Citrix Cloud Direct. Questo servizio offre una consegna affidabile e sicura per tutto il traffico collegato a Internet.

Se la qualità della connessione internet della filiale non è un problema, potrebbe essere sufficiente per ridurre al minimo la latenza. Indirizzare il traffico di Microsoft Teams direttamente dall'appliance della filiale Citrix SD-WAN alla porta principale di Microsoft 365 più vicina per ridurre al minimo la latenza. Per ulteriori informazioni, vedere Ottimizzazione di Citrix SD-WAN Office 365.




## Riunioni e chat con più finestre

È possibile utilizzare più finestre di riunione o chat per Microsoft Teams in Windows. Per informazioni dettagliate sulla funzionalità pop-out, vedere You can use multiple meetings or chat windows for Microsoft Teams in Windows sul sito di Microsoft 365.

> **Nota:**
>
> Questa funzione è supportata con l'app Citrix Workspace per Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Richiede VDA 2112 o versioni successive ed è stato trasferito su 1912 CU6+ LTSR e VDA 2112.

### Sfocatura dello sfondo ed effetti di sfondo

L'app Citrix Workspace per Windows, Mac, Linux e ChromeOS/HTML5 supporta la sfocatura dello sfondo e gli effetti per gli effetti di sfondo presenti nell'ottimizzazione di Microsoft Teams con HDX.

È possibile sfocare lo sfondo o sostituirlo con un'immagine predefinita ed evitare distrazioni impreviste aiutando la conversazione a rimanere concentrata sulla silhouette (corpo e viso). È possibile utilizzare questa funzionalità con chiamate P2P o in conferenza.

> **Nota:**
>
> Questa funzionalità è integrata con i pulsanti dell'interfaccia utente di Microsoft Teams. Il supporto MultiWindow è un prerequisito che richiede un aggiornamento del VDA alla versione 2112 o a una versione successiva. Per ulteriori informazioni, vedere Riunioni e chat con più finestre.

I controlli dell'interfaccia utente di Microsoft Teams sulla sfocatura e gli effetti dello sfondo richiedono le seguenti versioni minime:

- App Citrix Workspace per Windows 2207
- App Citrix Workspace per Mac 2301
- App Citrix Workspace per Linux versione 2212
- App Citrix Workspace per ChromeOS 2303

**Limitazioni:**

- Il client deve essere connesso a Internet mentre si sostituisce l'immagine di sfondo con un'immagine predefinita di Microsoft Teams.
- La sostituzione dell'immagine di sfondo definita dall'amministratore e dall'utente non è supportata nell'interfaccia utente di Microsoft Teams. Le immagini di sfondo personalizzate possono essere configurate utilizzando le impostazioni del client, se anche l'immagine è memorizzata sul client.

#### Impostare un'immagine di sfondo personalizzata

Le seguenti chiavi di registro sono necessarie solo se non si prevede di utilizzare l'interfaccia utente di Microsoft Teams per controllare la funzionalità o se un amministratore desidera ignorare i comportamenti predefiniti. Ad esempio, è possibile disabilitare la sfocatura dello sfondo quando l'endpoint non è abbastanza potente.

**In Windows** Per impostare un'immagine di sfondo personalizzata, gli amministratori o gli utenti finali devono configurare la seguente chiave del Registro di sistema sul client o sull'endpoint:

Posizione:`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valore: 0 (disabilitato), 1 (abilitato), 2 (sostituzione immagine di sfondo)

Il valore impostato su 1 sfoca lo sfondo. Questo valore può essere impostato dall'utente finale o dall'amministratore.

Il valore impostato su 2 richiede anche la presenza della chiave **VideoBackgroundImage**. Solo l'amministratore può impostare questo valore. La chiave seguente è necessaria solo se si desidera sostituire l'immagine di sfondo e non per la sfocatura:

- Nome: VideoBackgroundImage
- Tipo: REG_SZ
- Valore: my_image_name.jpeg

L'immagine di sfondo video deve essere presente nella directory `C:\Program Files (x86)\Citrix\ICA Client`.

Questa configurazione del Registro di sistema può essere utilizzata anche per abilitare la sfocatura dello sfondo o la sostituzione dell'immagine nell'app Citrix Workspace 2206 senza il selettore dell'interfaccia utente di Microsoft Teams. In altre parole, se l'ambiente o il VDA non supporta più finestre, è comunque possibile applicare la soluzione alternativa del registro HKCU con l'app Citrix Workspace 2206 o superiore per ottenere un risultato simile, sebbene l'utente non possa controllare la funzionalità durante la sessione HDX o della chiamata di Microsoft Teams.

Le modifiche delle chiavi di registro hanno effetto solo quando la sessione HDX si connette.

**Su Mac** Posizione dell'immagine scaricata dall'utente: */Users/username/Downloads/any_image.png*

Eseguire i seguenti comandi per impostare l'immagine personalizzata come immagine predefinita:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2

defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

**Su Linux** Posizione dell'immagine scaricata dall'utente: */home/username/Downloads/any_image.jpg*

Creare il file */var/.config/citrix/hdx_rtc_engine/config.json* e aggiungere le seguenti chiavi di configurazione in formato JSON. Ad esempio,

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
```

```
7
8   }
9
10 <!--NeedCopy-->
```

**Su HTML5** Per HTML5, è supportata solo la sfocatura dello sfondo. La sostituzione con immagini personalizzate non è supportata.

Per sfocare lo sfondo, effettuare le seguenti operazioni:

1. Accedere al file **configuration.js** nella cartella **HTML5Client**.
2. Aggiungere l'attributo **backgroundEffects** e impostare l'attributo su **true**. Ad esempio,

```
1  'features' : {
2
3      'msTeamsOptimization' :
4      {
5
6          'backgroundEffects' : true
7       }
8
9   }
10
11 <!--NeedCopy-->
```

3. Salvare le modifiche.

#### Considerazioni sul consumo di CPU client

Sebbene la funzionalità di sfocatura non sfrutti eccessivamente la CPU, ci si può aspettare un aumento dei consumi. Ad esempio, su un thin client con chip Intel® Pentium® Silver 4 Core da 1,5 GHz con TurboBoost fino a 2,8 GHz, la sfocatura dello sfondo aggiunge circa il 2% all'utilizzo della CPU. L'utilizzo medio della CPU è inferiore al 20%.

### Visualizzazione Raccolta e altoparlanti attivi in Microsoft Teams

Microsoft Teams supporta i layout **Gallery** (Galleria), **Large gallery** (Galleria ampia) e la **modalità Together** (Insieme).

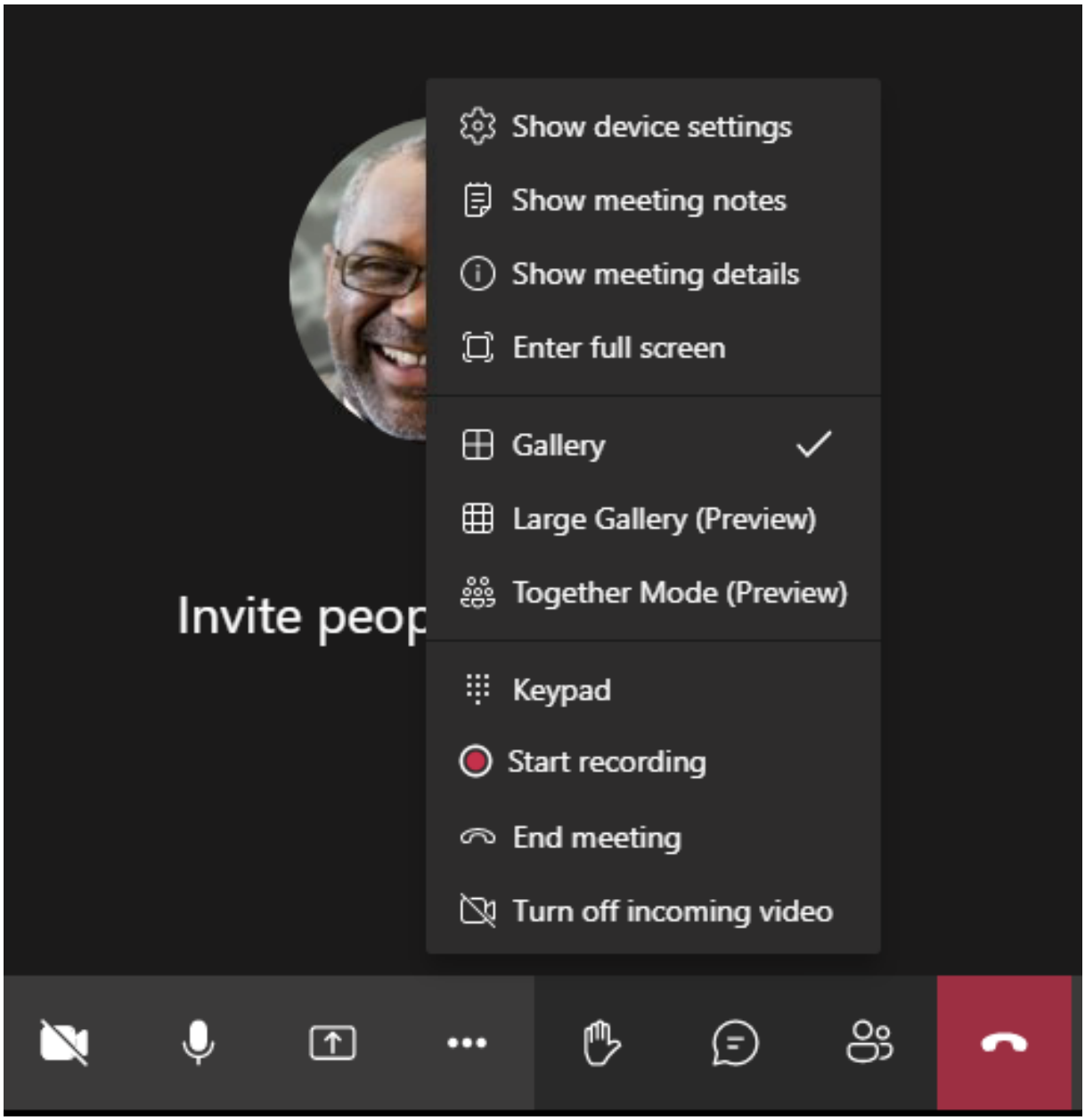
Microsoft Teams visualizza una griglia 2x2 con flussi video di quattro partecipanti (nota come **Gallery** [Galleria]). In questo caso, Microsoft Teams invia quattro flussi video al dispositivo client per la decodifica. Quando più di quattro partecipanti condividono video, sullo schermo appaiono solo gli ultimi quattro partecipanti che hanno parlato di più.

Microsoft Teams fornisce inoltre un'ampia vista galleria con una griglia fino a 7x7. Di conseguenza, il Conference Server di Microsoft Teams combina un singolo feed video e lo invia al dispositivo client per la decodifica, con conseguente riduzione del consumo della CPU. Questo feed singolo in stile matrice potrebbe includere anche il video con anteprima automatica degli utenti.

Infine, Microsoft Teams supporta la **modalità Together** (Insieme), che fa parte della nuova esperienza di riunione. Utilizzando la tecnologia di segmentazione IA per posizionare digitalmente i partecipanti in un background condiviso, Microsoft Teams mette tutti i partecipanti nello stesso auditorium.

L'utente può controllare queste modalità durante una chiamata in conferenza selezionando i layout **Gallery** (Galleria), **Large gallery** (Galleria ampia) o la **modalità Together** (Insieme) nel menu con i tre puntini.



Supporto per le limitazioni delle proporzioni video (CWA per Windows 2102, CWA per Linux 2106, CWA per MAC 2106 o versione superiore):

- L'opzione **Fill to frame** (Riempi inquadratura) è disponibile nelle viste Gallery (Galleria)/Large Gallery (Galleria ampia). Questa opzione ritaglia le dimensioni del video per adattarlo alla sottofinestra. **Fit to frame** (Adatta all'inquadratura), invece, visualizza barre nere (formato 16:9) sui lati del video in modo che non ci siano ritagli.

La tabella seguente fornisce un confronto tra i layout Gallery (Galleria) e Large gallery (Galleria ampia):

| | Vista Gallery (Galleria) 2x2 (impostazione predefinita) | Vista Large Gallery (Galleria ampia) |
|---|---|---|
| Layout/Griglia | Visualizza una griglia 2x2 con flussi video di quattro partecipanti. Sullo schermo vengono visualizzati solo gli ultimi quattro altoparlanti più attivi e gli altri partecipanti non appaiono sulla griglia. | Visualizza una griglia 7x7 con flussi video di 49 partecipanti. |
| Tecnica di mixing | Un router multimediale inoltra i singoli flussi di ciascun partecipante a ogni utente. | Un server centrale per conferenze mixa e transcodifica tutto l'audio o il video per creare un layout composito su misura per ogni partecipante. Questa azione introduce una certa latenza aggiuntiva. |
| Altoparlante attivo | Il nuovo altoparlante attivo sostituisce l'altoparlante meno attivo nella griglia. | Visualizza tutti i partecipanti indipendentemente dal fatto che siano attivi o inattivi. |
| Codifica in corrispondenza dell'endpoint | Sull'endpoint potrebbero essere codificati uno o più flussi video se Simulcast è abilitato. Per ulteriori informazioni sul supporto di Simulcast, vedere Simulcast. | Sull'endpoint potrebbero essere codificati uno o più flussi video se Simulcast è abilitato. Per ulteriori informazioni sul supporto di Simulcast, vedere Simulcast. |

| | Vista Gallery (Galleria) 2x2 (impostazione predefinita) | Vista Large Gallery (Galleria ampia) |
|---|---|---|
| Decodifica in corrispondenza dell'endpoint | Ogni partecipante riceve fino a quattro flussi multimediali individuali. Ciò aumenta il consumo di CPU nell'endpoint di HdxRtcEngine.exe (per decodifica/rendering). | Ogni partecipante riceve un solo flusso per audio e video. Questa impostazione riduce il consumo di CPU nell'endpoint. |
| Risoluzione massima | 720p. Quando quattro partecipanti condividono video, la risoluzione massima è di 360p per feed video. Se meno di quattro partecipanti condividono video, la risoluzione per feed video potrebbe essere più alta. | 720p per il layout composito o il mixaggio. Non è necessario un flusso video di alta qualità per partecipante in un layout composito. A causa di questa condizione, ogni mittente riduce la risoluzione o la velocità in bit di caricamento. |
| Problema di "utente lento" | Il mittente modifica la qualità di ciascuna modalità (audio/video/condivisione dello schermo) sulla qualità di rete più bassa comune tra i partecipanti. Questo flusso multimediale viene quindi inoltrato a tutti gli altri partecipanti. Di conseguenza, un partecipante con cattive condizioni di rete influisce sulla qualità di tutti gli altri partecipanti alla chiamata. | Meno suscettibile allo scenario di qualità della rete più bassa comune. Il server per conferenze offre qualità diverse in base alle condizioni di rete dei singoli partecipanti. |
| Anteprima automatica | L'utente viene visualizzato in una piccola miniatura in tempo reale. | L'utente viene visualizzato in una miniatura e mescolato con il resto dei feed video. Di conseguenza, l'utente potrebbe vedersi incluso nel layout del video principale con un ritardo aggiuntivo. |

### Condivisione dello schermo in Microsoft Teams

Microsoft Teams si basa sulla condivisione dello schermo basata su video (VBSS), codificando essenzialmente il desktop condiviso con codec video come H264 e creando un flusso ad alta definizione. Con l'ottimizzazione HDX, la condivisione dello schermo in entrata viene considerata come un flusso video.

A partire dall'app Citrix Workspace 2109 o versione successiva per Windows, Linux, Mac e dall'app Citrix Workspace 2303 per ChromeOS, gli utenti possono condividere gli schermi e la videocamera contemporaneamente.

Con le versioni precedenti, se ci si trova nel mezzo di una videochiamata e l'altro peer inizia a condividere il desktop, il feed video della videocamera originale viene sospeso. Viene invece visualizzato il feed video per la condivisione dello schermo. Il peer deve quindi riprendere manualmente la condivisione della videocamera.

> **Nota per PowerPoint Live**
>
> Questa limitazione non esiste se si condividono contenuti da PowerPoint Live. In tal caso, gli altri colleghi possono ancora vedere la webcam e i contenuti e navigare avanti e indietro per esaminare altre diapositive. In questo scenario, le diapositive vengono renderizzate sul VDA. Per accedere a una presentazione PowerPoint Live, fare clic sul pulsante del pannello di condivisione e selezionare una delle diapositive di PowerPoint suggerite, oppure fare clic su "Sfoglia"e trovare un file PowerPoint sul proprio computer o in OneDrive.

Anche la condivisione dello schermo in uscita è ottimizzata e assegnata all'app Citrix Workspace. In questo caso, il motore multimediale acquisisce e trasmette solo la finestra Citrix Desktop Viewer (CDViewer.exe), con un bordo rosso disegnato all'intorno. Qualsiasi applicazione locale che si sovrappone a Desktop Viewer non viene acquisita.

> **Nota**
>
> Impostare autorizzazioni specifiche nell'app Citrix Workspace per Mac per abilitare la condivisione dello schermo. Per ulteriori informazioni, vedere Requisiti di sistema.

#### Multimonitor

Se Desktop Viewer (CDViewer.exe) è in modalità a schermo intero e si estende a configurazioni multimonitor, l'app Citrix Workspace 2106 o versione successiva (Windows/Linux/Mac) consente al selettore dello schermo di selezionare il monitor da condividere.

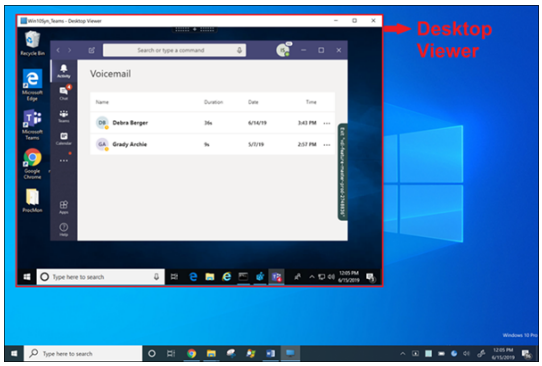
**Limitazione nota:**

- Se Desktop Viewer è disabilitato o se viene utilizzato Desktop Lock, la selezione multimonitor non è disponibile nel selettore dello schermo di Microsoft Teams. Desktop Viewer potrebbe

essere disabilitato modificando il modello di file `.ICA` o `StoreFront web.config`. Il tasto di scelta rapida MAIUSC+F2 non è compatibile con la condivisione dello schermo multimonitor.

- Nelle versioni dell'app Workspace precedenti alla 2106, viene condiviso solo il monitor principale. Trascinare l'applicazione nel desktop virtuale sul monitor principale in modo che l'altro peer nella chiamata la veda.
- La condivisione dello schermo multimonitor potrebbe non funzionare se si configura l'app Citrix Workspace con la funzionalità di layout del monitor virtuale (partizione logica di un singolo monitor fisico). In questo caso, tutti i monitor virtuali vengono condivisi come immagine composita.
- Le versioni precedenti dell'app Citrix Workspace per Windows (dalla 1907 alla 2008) condividono anche un'applicazione locale che viene eseguita nel computer client. Questa condivisione è possibile solo se l'app locale è stata sovrapposta a Desktop Viewer. Questo comportamento è stato rimosso nella versione 2009.6 o superiore e nella versione 1912 CU5 o superiore.
- Durante la condivisione dello schermo, se si passa dalla modalità finestra alla modalità a schermo intero, la condivisione dello schermo si interrompe. È necessario interrompere e condividere di nuovo affinché la condivisione dello schermo funzioni.




**Condivisione dello schermo da un'applicazione senza soluzione di continuità:**

Se si pubblica Microsoft Teams come applicazione autonoma senza soluzione di continuità, la condivisione dello schermo acquisisce il desktop locale dell'endpoint fisico. La versione minima dell'app Citrix Workspace deve essere 1909.

### Condivisione di app

A partire dall'app Citrix Workspace per Windows 2112.1 e dal VDA 2112, Microsoft Teams supporta la condivisione delle app.

A partire dall'app Citrix Workspace per Windows 2109, Mac 2203, Linux 2209 e VDA 2109, Microsoft Teams supporta la condivisione sullo schermo di app specifiche in esecuzione nella sessione virtuale. Per condividere un'app specifica:

1. Accedere all'app Microsoft Teams nella sessione remota.

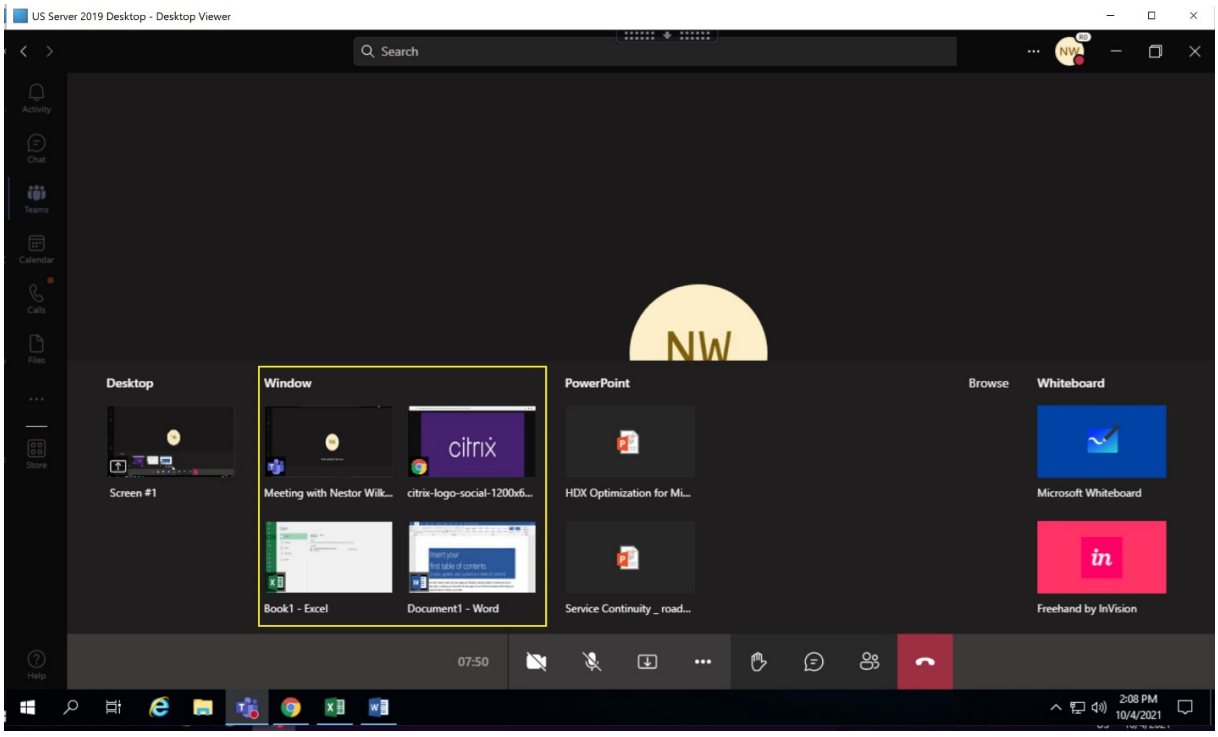
 

2. Fare clic su **Condividi contenuto** nell'interfaccia utente di Microsoft Teams.
3. Selezionare un'app da condividere durante la riunione. Viene visualizzato un bordo rosso intorno all'app selezionata e i partecipanti alla chiamata possono vedere l'app condivisa.

Per condividere un'altra app, fare nuovamente clic su **Condividi contenuto** e selezionare una nuova app.

Se si desidera disabilitare la condivisione delle app, creare la seguente chiave di registro sul VDA all'indirizzo `HKLM\SOFTWARE\Citrix\Graphics`:
Nome: `UseWsProvider`
Tipo: `DWORD`
Valore: 0

> **Nota:**
>
> - Quando l'aggiornamento verrà implementato da Microsoft, sarà possibile leggere l'articolo CTX253754 per il relativo annuncio e l'aggiornamento della documentazione.
> - Se si riduce a icona un'app, Microsoft Teams visualizza l'ultima immagine dell'app condivisa. È possibile ingrandire la finestra per riprendere la condivisione dello schermo.
> - La condivisione dello schermo fa affidamento sull'acquisizione della finestra lato VDA. Il contenuto viene quindi inoltrato alla velocità massima all'app Citrix Workspace. La velocità massima è di 30 frame al secondo. L'app Citrix Workspace inoltra il contenuto ai colleghi o al server della conferenza.




**Limitazioni note della condivisione dello schermo di app specifiche:**

- Il puntatore del mouse non è visibile quando si condivide un'app sullo schermo.
- Se si riduce a icona un'app quando la si condivide, nel selettore dello schermo viene visualizzata solo l'icona dell'app. La miniatura dell'app non viene visualizzata in anteprima nel selettore dello schermo. Non è possibile condividere il contenuto e non viene visualizzato il bordo rosso finché non si ingrandisce l'app.
- In LAA apps è visualizzato un elenco delle app che possono essere condivise con le app desktop nel Microsoft Teams ottimizzato nel VDA. Tuttavia, quando si seleziona l'app dall'elenco, il risultato potrebbe non essere quello previsto.

**Compatibilità con la protezione delle app**
La condivisione sullo schermo di un'app specifica è compatibile con la funzione di protezione delle app in Microsoft Teams ottimizzato per HDX. È possibile condividere lo schermo di un'app specifica, se l'app o il desktop è stato avviato da un gruppo di consegna per il quale è abilitata la protezione delle app.

Quando si fa clic su **Condividi contenuto** nell'interfaccia utente di Microsoft Teams, il selettore dello schermo rimuove l'opzione **Desktop**. È possibile selezionare l'opzione **Finestra** solo per condividere qualsiasi app aperta.

> **Nota:**
>
> Quando si avviano app o desktop da un gruppo di consegna con protezione app abilitata, non è possibile vedere il video in arrivo o la condivisione dello schermo.

**Dare e richiedere il controllo in Microsoft Teams** Questa funzione è supportata nelle seguenti versioni dell'app Citrix Workspace (non vi è alcuna dipendenza dalla versione del VDA o dal sistema operativo, a sessione singola o multisessione):

- App Citrix Workspace per Windows versione 2112.1 e successiva
- App Citrix Workspace per Mac versione 2203.1 e successiva
- App Citrix Workspace per Linux versione 2203 e successiva
- App Citrix Workspace per ChromeOS versione 2303 e successiva

È possibile richiedere il controllo durante una chiamata di Microsoft Teams quando un partecipante condivide lo schermo. Una volta ottenuto il controllo, è possibile effettuare selezioni, modifiche o altre attività con tastiera e mouse sullo schermo condiviso.

Per assumere il controllo quando uno schermo viene condiviso, fare clic sul pulsante **Richiedi controllo** nell'interfaccia utente di Microsoft Teams. Il partecipante alla riunione che condivide lo schermo può accettare o rifiutare la richiesta.

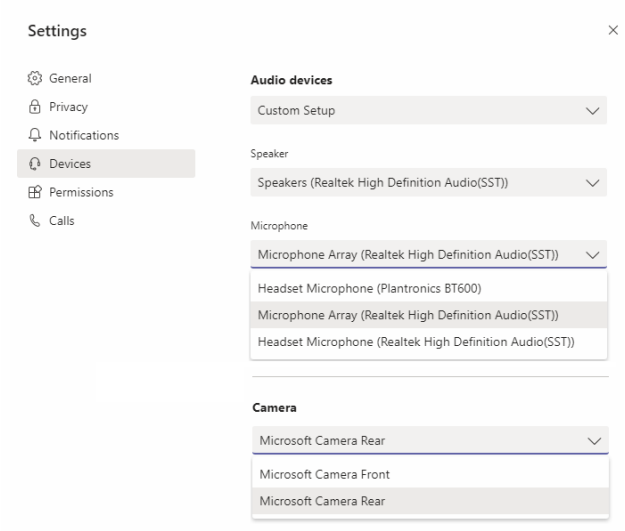
Mentre si dispone del controllo, è possibile effettuare selezioni, modifiche e altre alterazioni nello schermo condiviso. Per queste azioni, è possibile usare sia la tastiera che il mouse. Al termine fare clic su **Richiedi controllo**.

> **Limitazioni:**
>
> - I comandi Concedi controllo e Richiedi controllo non sono disponibili se l'utente sta condividendo una singola app (nota anche come condivisione app). È necessario condividere il desktop o il monitor completo.
> - La funzione per fissare la barra di controllo in una posizione specifica non è disponibile.

### Periferiche in Microsoft Teams

Quando l'ottimizzazione per Microsoft Teams è attiva, l'app Citrix Workspace accede alle periferiche (cuffie, microfono, videocamere, altoparlanti e così via). Quindi le periferiche vengono elencate correttamente nell'interfaccia utente di Microsoft Teams (**Impostazioni > Dispositivi**).




Microsoft Teams non accede direttamente ai dispositivi. Si basa invece sul motore multimediale WebRTC dell'app Workspace per l'acquisizione e l'elaborazione dei contenuti multimediali. Microsoft Teams elenca i dispositivi che l'utente può selezionare.

Le periferiche inserite mentre Microsoft Teams è attivo non sono selezionate per impostazione predefinita. È necessario selezionare manualmente le periferiche dalla schermata **Impostazioni** > **Dispositivi** dell'interfaccia utente di Microsoft Teams. Dopo che le periferiche sono state selezionate, Microsoft Teams ne memorizza le informazioni nella cache. Di conseguenza, le periferiche vengono selezionate automaticamente quando ci si riconnette a una sessione dallo stesso endpoint.

**Raccomandazioni:**

- Cuffie certificate Microsoft Teams con cancellazione dell'eco integrata. Nelle configurazioni con periferiche aggiuntive, in cui microfono e altoparlanti si trovano su dispositivi separati, potrebbe essere presente un'eco. Un esempio è una webcam con un microfono incorporato

e un monitor con altoparlanti. Quando si utilizzano altoparlanti esterni, posizionarli il più lontano possibile dal microfono. Inoltre, posizionarli lontano da qualsiasi superficie che potrebbe rifrangere il suono nel microfono.

- Fotocamere certificate Microsoft Teams, sebbene le periferiche certificate Skype for Business siano compatibili con Microsoft Teams.
- Il motore multimediale dell'app Citrix Workspace non può sfruttare l'offload della CPU con webcam che eseguono la codifica H.264 on-board UVC 1.1 e 1.5.

> **Nota:**
>
> L'app Workspace 2009.6 per Windows è ora in grado di acquisire periferiche con formati audio a 24 bit o con frequenze superiori a 96 kHz.
>
> HdxTeams.exe (nell'app Citrix Workspace per Windows 2009 o versioni precedenti) supporta solo questi formati specifici dei dispositivi audio (canali, profondità di bit e frequenza di campionamento):
>
> - Dispositivi di riproduzione: fino a 2 canali, 16 bit, frequenze fino a 96.000 Hz
> - Dispositivi di registrazione: fino a 4 canali, 16 bit, frequenze fino a 96.000 Hz
>
> Anche se un solo altoparlante o microfono non corrisponde alle impostazioni previste, l'enumerazione dei dispositivi in Microsoft Teams non va a buon fine e viene visualizzato **Nessuno** in **Impostazioni > Dispositivi**.
> I log
> **Webrpc** in **HdxTeams.exe** mostrano questo tipo di informazioni:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```
>
> Come soluzione alternativa, disabilitare il dispositivo specifico oppure:
>
> 1. Aprire **Audio nel Pannello di controllo** (mmsys.cpl).
> 2. Selezionare il dispositivo di riproduzione o registrazione.
> 3. Andare a **Proprietà > Avanzate** e modificare le impostazioni su una modalità supportata.

#### Modalità di fallback

Se Microsoft Teams non riesce a caricarsi in modalità VDI ottimizzata ("Citrix HDX Not Connected"[Citrix HDX non connesso] in Teams/Informazioni/Versione), il VDA torna a utilizzare le tecnologie HDX legacy. Le tecnologie HDX legacy potrebbero essere il reindirizzamento della webcam e il reindirizzamento del microfono e dell'audio del client. Se si utilizza una versione dell'app Workspace/un sistema

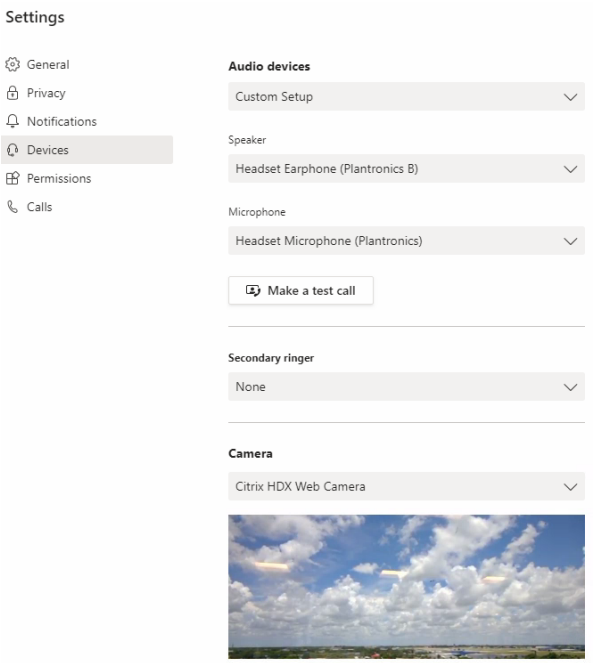
 

operativo della piattaforma che non supporta l'ottimizzazione di Microsoft Teams, le chiavi del Registro di sistema di fallback non si applicano.
In modalità di fallback, le periferiche sono mappate al VDA. Le periferiche vengono visualizzate nell'app Microsoft Teams come se fossero collegate localmente al desktop virtuale.

Ora è possibile controllare granularmente il meccanismo di fallback impostando le chiavi del Registro di sistema nel VDA. Per informazioni, vedere Modalità di fallback di Microsoft Teams nell'elenco delle funzionalità gestite tramite il Registro di sistema.

Questa funzionalità richiede Microsoft Teams versione 1.3.0.13565 o successiva.

Per determinare se si è in modalità ottimizzata o non ottimizzata quando si esamina la scheda **Impostazioni > Dispositivi** nell'app Microsoft Teams, la differenza più significativa è il nome della videocamera. Se Microsoft Teams è stato caricato in modalità non ottimizzata, vengono avviate le tecnologie HDX legacy. Il nome della webcam presenta il suffisso **Citrix HDX**, come mostrato nell'immagine seguente. I nomi dell'altoparlante e del microfono potrebbero essere leggermente diversi (o troncati) rispetto alla modalità ottimizzata.




Quando vengono utilizzate tecnologie HDX legacy, Microsoft Teams non esegue l'offload dell'elaborazione di audio, video e condivisione dello schermo nel motore multimediale WebRTC dell'app Citrix Workspace dell'endpoint. Le tecnologie HDX utilizzano invece il rendering lato server. È previsto un elevato consumo di CPU sul VDA quando viene attivato il video. Le prestazioni audio in tempo reale potrebbero non essere ottimali.

## Limitazioni note

### Limitazioni Citrix

Limitazioni sull'app Citrix Workspace:

- Pulsanti HID: risposta e fine chiamata non sono supportati. I tasti per abbassare e alzare il volume sono supportati.
- Le impostazioni QoS nell'interfaccia di amministrazione per Microsoft Teams non sono valide per gli utenti VDI.
- La funzionalità aggiuntiva per la protezione delle app per l'app Citrix Workspace impedisce la condivisione dello schermo in uscita e blocca la condivisione di schermo e video in entrata.
- Gli utenti non possono acquisire schermate dei contenuti di Microsoft Teams quando utilizzano uno strumento di cattura su VDA. Tuttavia, se viene utilizzato uno strumento di cattura sul lato client, il contenuto può essere acquisito.

Limitazione sul VDA:

- Quando si configura l'impostazione High DPI (DPI elevato) dell'app Citrix Workspace su **Yes** (Sì), la finestra video reindirizzata non è nella posizione corretta. Questa limitazione si verifica quando il fattore di ridimensionamento DPI del monitor è impostato su un valore superiore al 100%

Limitazioni sull'app Citrix Workspace e sul VDA:

- È possibile controllare il volume di una chiamata ottimizzata solo utilizzando la barra del volume sul computer client, non sul VDA.

### Simulcast

Il supporto di Simulcast è abilitato per videoconferenze Microsoft Teams ottimizzate su Windows e Mac. Per Linux, rivolgersi al proprio fornitore di thin client.
Con Simulcast, la qualità e l'esperienza delle videoconferenze su diversi endpoint vengono migliorate adattandosi alla risoluzione corretta per la migliore esperienza di chiamata per tutti i chiamanti.

Con questa esperienza migliorata, ogni utente potrebbe fornire più flussi video con risoluzioni diverse (ad esempio 720p, 360p e così via) a seconda di diversi fattori, tra cui la capacità dell'endpoint, le condizioni della rete e così via. L'endpoint ricevente richiede quindi la massima risoluzione di qualità che può gestire, offrendo così a tutti gli utenti un'esperienza video ottimale.

> **Nota:**
>
> Questa funzionalità è disponibile solo dopo l'implementazione di un aggiornamento di Microsoft Teams. Per informazioni sulla data di pubblicazione, passare a https://www.microsoft.com/ e

> cercare la roadmap di Microsoft 365. Quando l'aggiornamento verrà implementato da Microsoft, sarà possibile leggere l'articolo CTX253754 per il relativo annuncio e l'aggiornamento della documentazione.

#### Limitazioni Microsoft

- La vista galleria 3x3 non è supportata. Dipendenza di Microsoft Teams: contattare Microsoft per sapere quando sarà disponibile la griglia 3x3.
- L'interoperabilità con Skype for Business è limitata alle chiamate audio, nessuna modalità video.
- La risoluzione massima del flusso video in entrata e in uscita è 720p. Dipendenza di Microsoft Teams: contattare Microsoft per sapere quando sarà disponibile 1080p.
- Il tono di suoneria delle chiamate PSTN non è supportato.
- Il bypass dei contenuti multimediali per il routing diretto non è supportato.
- I ruoli di produttore e presentatore di eventi broadcast e live non sono supportati. Il ruolo di partecipante è supportato ma non ottimizzato (viene invece eseguito il rendering sul VDA).
- La funzione zoom avanti e zoom indietro in Microsoft Teams non è supportata.
- Il routing basato sulla posizione e il bypass dei supporti non sono supportati.
- L'unione delle chiamate non è supportata (opzione non visualizzata nell'interfaccia utente).

#### Limitazioni Citrix e Microsoft

- Quando si esegue la condivisione dello schermo, l'opzione **Includi audio di sistema** non è disponibile.
- Simulcast non è supportato su ChromeOS.

### Imminente la fine del ciclo di vita di Microsoft Teams a finestra singola

Il 31 gennaio 2024, Microsoft ritirerà il supporto di Microsoft Teams per l'interfaccia utente a finestra singola quando si utilizza l'ottimizzazione VDI Microsoft Teams e supporterà solo l'esperienza multifinestra. Microsoft ha comunicato tale deprecazione l'8 settembre 2023 nell'M365s Admin Center (ID post: MC674419).
I dettagli pubblici sulla funzionalità multifinestra sono disponibili nell'articolo della Tech Community New Meeting and Calling Experience in Microsoft Teams (Nuova esperienza di riunioni e chiamate in Microsoft Teams).

È necessario aggiornare l'app VDA e Citrix Workspace alle versioni supportate per continuare a utilizzare Microsoft Teams in modalità ottimizzata per la condivisione di video e schermo. Se non si effettua

l'aggiornamento dell'infrastruttura e degli endpoint per supportare il multi-finestra, è possibile effettuare solo chiamate audio. Non sarà possibile utilizzare la funzionalità ottimizzata di condivisione di video e schermo.

La tabella seguente illustra le versioni minime, LTSR e consigliate dei VDA e dell'app Citrix Workspace necessarie per continuare a utilizzare le chiamate ottimizzate in Microsoft Teams su Citrix VDI:

| Componente | Versione minima | Versione supportata dalla LTSR | Versione consigliata |
|---|---|---|---|
| Microsoft Teams | 1.5.00.11865 | Non applicabile | Più recente |
| VDA | 1912 CU6 LTSR, 2203 LTSR, 2112 CR | 1912 CU7+, 2203 CU2+ | 2308 CR+ |
| App Citrix Workspace per Windows | 2205 CR | 2203 CU2+ | 2309 CR+ |
| App Citrix Workspace per Mac | 2209 CR | Non applicabile | 2308 CR+ |
| App Citrix Workspace per Linux | 2209 CR | Non applicabile | 2308 CR+ |
| App Citrix Workspace per ChromeOS o HTML5 | 2303 CR | Non applicabile | 2309 CR+ |

## Annuncio di obsolescenza del formato SDP (Piano B) di WebRTC

Citrix prevede di eliminare l'attuale supporto del formato SDP (Piano B) di WebRTC nelle versioni future. È necessario utilizzare Unified Plan in WebRTC per supportare le funzionalità ottimizzate di Microsoft Teams.

### Prodotti interessati

In una delle versioni future dell'applicazione Citrix Workspace, le chiamate tra endpoint con la prossima versione dell'app Citrix Workspace e gli endpoint con l'app Citrix Workspace 2108 o versioni precedenti non saranno supportate. Questa incompatibilità di chiamata include i client dell'app Citrix Workspace (CWA) 1912 LTSR. Sono interessati i seguenti client CWA:

- App Citrix Workspace per Windows
- App Citrix Workspace per Linux
- App Citrix Workspace per Mac
- App Citrix Workspace per Chrome

**Sostituto per Plan B**

Se si utilizza una versione dell'app Citrix Workspace precedente alla 2109, è necessario eseguire l'aggiornamento a una versione supportata (preferibilmente l'ultima versione CR). In caso contrario, le chiamate con una versione futura o con endpoint più recenti non riusciranno a connettersi. Potrebbe inoltre non essere possibile completare le chiamate tra le versioni future e i partner di comunicazione federati se il partner federato non ha aggiornato il proprio Citrix Workspace.

La versione 2108 dell'app Citrix Workspace ha completato la data di supporto in marzo 2023 e deve essere aggiornata a una versione più recente. Per ulteriori informazioni, vedere App Workspace che illustra i dettagli sul supporto della versione dell'app Citrix Workspace.

Per ulteriori informazioni sulla deprecazione del Piano B, consulta la documentazione di WebRTC.

### Informazioni aggiuntive

- Monitorare, risolvere i problemi e supportare Microsoft Teams
- Distribuire l'app desktop Microsoft Teams nella macchina virtuale
- Installare Microsoft Teams utilizzando MSI (sezione Installazione VDI)
- Thin client
- Strumento di valutazione della rete di Skype for Business
- Comprendere la coesistenza e l'interoperabilità di Microsoft Teams e Skype for Business

## Reindirizzamento di Windows Media

October 6, 2022

Il reindirizzamento di Windows Media controlla e ottimizza il modo in cui i server forniscono audio e video in streaming agli utenti. Riproducendo i file multimediali di runtime sul dispositivo client anziché sul server, il reindirizzamento di Windows Media riduce i requisiti di larghezza di banda per la riproduzione di file multimediali. Il reindirizzamento di Windows Media migliora le prestazioni di Windows Media Player e dei lettori compatibili in esecuzione su desktop Windows virtuali.

Se i requisiti per il recupero dei contenuti sul lato client di Windows Media non vengono soddisfatti, la distribuzione dei contenuti multimediali utilizza automaticamente il recupero lato server. Questo metodo è trasparente per gli utenti. È possibile utilizzare Citrix Scout per eseguire una traccia Citrix Diagnosis Facility (CDF) da HostMMTransport.dll per determinare il metodo utilizzato. Per ulteriori informazioni, vedere Citrix Scout.

Il reindirizzamento di Windows Media intercetta la pipeline dei contenuti multimediali nel server host, acquisisce i dati multimediali nel formato compresso nativo e reindirizza i contenuti al dispositivo

client. Il dispositivo client ricrea quindi la pipeline dei contenuti multimediali per decomprimere i dati multimediali ricevuti dal server host ed eseguirne il rendering. Il reindirizzamento di Windows Media funziona bene sui dispositivi client con sistema operativo Windows. Questi dispositivi dispongono del framework multimediale necessario per ricostruire la pipeline dei contenuti multimediali così come era presente sul server host. I client Linux utilizzano framework multimediali open source simili per ricostruire la pipeline dei contenuti multimediali.

L'impostazione del criterio **Windows Media Redirection (Reindirizzamento di Windows Media)** controlla questa funzionalità e il valore predefinito è **Allowed (Consentito)**. In genere, questa impostazione aumenta la qualità audio e video di cui il server esegue il rendering a un livello paragonabile ai contenuti riprodotti localmente su un dispositivo client. In rari casi, la riproduzione di file multimediali utilizzando il reindirizzamento di Windows Media risulta peggiore rispetto ai contenuti multimediali sottoposti a rendering utilizzando la compressione ICA di base e l'audio normale. È possibile disabilitare questa funzionalità aggiungendo l'impostazione **Windows Media Redirection (Reindirizzamento di Windows Media)** a un criterio e impostandone il valore su **Prohibited (Vietato)**.

Per ulteriori informazioni sulle impostazioni dei criteri, vedere Impostazioni dei criteri multimediali.

**Limitazione:**

Quando si utilizza Windows Media Player e RAVE (Remote Audio & Video Extensions) abilitati all'interno di una sessione, potrebbe essere visualizzata una schermata nera. Questa schermata nera potrebbe essere visualizzata facendo clic con il pulsante destro del mouse sul contenuto video e selezionando **Mostra sempre In esecuzione in primo piano**.

## Reindirizzamento generale del contenuto

October 6, 2022

Il reindirizzamento dei contenuti consente di controllare se gli utenti accedono alle informazioni utilizzando applicazioni pubblicate sui server o utilizzando applicazioni in esecuzione localmente sui dispositivi utente.

### Reindirizzamento delle cartelle client

Il reindirizzamento delle cartelle client modifica il modo in cui i file lato client sono accessibili nella sessione lato host.

- Quando si abilita solo il mapping delle unità client sul server, i volumi completi lato client vengono automaticamente mappati alle sessioni come collegamenti UNC (Universal Naming Convention).

- Quando si abilita il reindirizzamento delle cartelle client sul server e l'utente lo configura sul dispositivo desktop Windows, la parte del volume locale specificata dall'utente viene reindirizzata.

### Reindirizzamento da host a client

Prendere in considerazione l'utilizzo del reindirizzamento da host a client per specifici casi di utilizzo non comuni. Normalmente, altre forme di reindirizzamento dei contenuti potrebbero essere migliori. Supportiamo questo tipo di reindirizzamento solo sui VDA del sistema operativo multisessione e non sui VDA del sistema operativo a sessione singola.

### Accesso alle app locali e reindirizzamento URL

L'accesso alle app locali integra perfettamente le applicazioni Windows installate localmente in un ambiente desktop ospitato. Lo fa senza passare da un computer all'altro.

La tecnologia HDX fornisce un **reindirizzamento USB generico** per dispositivi speciali che non dispongono di alcun supporto ottimizzato o dove questo non è adatto.

## Reindirizzamento delle cartelle client

October 6, 2022

Il reindirizzamento delle cartelle client modifica il modo in cui i file lato client sono accessibili nella sessione lato host. Se si abilita solo il mapping delle unità client sul server, i volumi completi lato client vengono automaticamente mappati come collegamenti UNC (Universal Naming Convention) alle sessioni. Quando si abilita il reindirizzamento delle cartelle client sul server e l'utente lo configura sul dispositivo utente, la parte del volume locale specificata dall'utente viene reindirizzata.

Solo le cartelle specificate dall'utente vengono visualizzate come collegamenti UNC all'interno delle sessioni. Ossia invece del file system completo sul dispositivo utente. Se si disattivano i collegamenti UNC tramite il Registro di sistema, le cartelle client vengono visualizzate come unità mappate all'interno della sessione.

Il reindirizzamento delle cartelle client è supportato solo sui computer con sistema operativo Windows a sessione singola.

Il reindirizzamento delle cartelle client per un'unità USB esterna non viene salvato durante lo scollegamento e il collegamento del dispositivo.

Abilitare la direzione della cartella client sul server. Quindi, sul dispositivo client, specificare quali cartelle reindirizzare. L'applicazione utilizzata per specificare le opzioni delle cartelle client è inclusa nell'app Citrix Workspace fornita con questa versione.

**Requisiti:**

Per i server:

- Windows Server 2019 edizioni Standard e Datacenter
- Windows Server 2016, edizioni standard e Datacenter
- Windows Server 2012 R2, edizioni standard e Datacenter

Per i client:

- Windows 10, edizioni a 32 bit e a 64 bit (versione minima 1607)
- Windows 8.1, edizioni a 32 bit e 64 bit (inclusa l'edizione Embedded)
- Windows 7, edizioni a 32 bit e 64 bit (inclusa l'edizione Embedded)

Per abilitare il reindirizzamento delle cartelle client sul server, vedere Reindirizzamento delle cartelle clientnell'elenco delle funzionalità gestite tramite il Registro di sistema.

Sul dispositivo utente, specificare quali cartelle reindirizzare:

1. Assicurarsi che sia installata la versione più recente dell'app Citrix Workspace.
2. Dalla directory di installazione dell'app Citrix Workspace, avviare CtxCFRUI.exe.
3. Scegliere il pulsante di opzione **Custom (Personalizza)** e aggiungere, modificare o rimuovere cartelle.
4. Disconnettere e riconnettere le sessioni in modo che l'impostazione venga applicata.

## Reindirizzamento da host a client

October 6, 2022

Il reindirizzamento da host a client consente l'apertura degli URL, incorporati come collegamenti ipertestuali nelle applicazioni in esecuzione su una sessione Citrix, utilizzando l'applicazione corrispondente sul dispositivo endpoint dell'utente. Alcuni casi d'uso comuni per il reindirizzamento da host a client includono:

- Reindirizzamento di siti Web nei casi in cui il server Citrix non dispone di accesso a Internet o di rete all'origine.
- Non si desidera utilizzare il reindirizzamento dei siti Web quando si esegue un browser Web all'interno della sessione Citrix per motivi di sicurezza, prestazioni, compatibilità o scalabilità.
- Reindirizzamento di tipi di URL specifici nei casi in cui le applicazioni richieste per aprire l'URL non sono installate sul server Citrix.

Il reindirizzamento da host a client non è destinato agli URL a cui si accede su una pagina Web o che si digitano nella barra degli indirizzi del browser Web in esecuzione nella sessione Citrix. Per il reindirizzamento degli URL nei browser Web, vedere Reindirizzamento URL bidirezionale o Reindirizzamento del contenuto del browser.

### Requisiti di sistema

- VDA con sistema operativo multisessione
- Client supportati:
  - App Citrix Workspace per Windows
  - App Citrix Workspace per Mac
  - App Citrix Workspace per Linux
  - App Citrix Workspace per HTML5
  - App Citrix Workspace per Chrome

Il dispositivo client deve avere un'applicazione installata e configurata per gestire il reindirizzamento dei tipi di URL.

### Configurazione

Utilizzare il criterio Citrix Host to client redirection (reindirizzamento da host a client) per abilitare questa funzionalità. Il **reindirizzamento da host a client** è disabilitato per impostazione predefinita. Dopo aver abilitato il criterio di reindirizzamento da host a client, l'applicazione Citrix Launcher si registra con il server Windows per assicurarsi che possa intercettare gli URL e inviarli al dispositivo client.

Successivamente è necessario configurare i criteri di gruppo di Windows per utilizzare Citrix Launcher come applicazione predefinita per i tipi di URL richiesti. Sul VDA del server Citrix, creare il file ServerFTAdefaultPolicy.xml e inserire il seguente codice XML.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>
<!--NeedCopy-->
```

Dalla Console Gestione Criteri di gruppo, andare a **Configurazione computer > Modelli amministrativi > Componenti di Windows > Esplora file > Imposta file di configurazione delle associazioni predefinite** e salvare il file ServerFTAdefaultPolicy.xml.

> **Nota:**
>
> Se un server Citrix non dispone delle impostazioni Criteri di gruppo, Windows richiede agli utenti

> di selezionare un'applicazione per l'apertura degli URL.

Per impostazione predefinita, supportiamo il reindirizzamento dei seguenti tipi di URL:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Per includere altri tipi di URL standard o personalizzati nell'elenco per il reindirizzamento, creare una nuova riga **Association Identifier** (Identificatore di associazione) nel file ServerFTAdefaultPolicy.xml citato in precedenza. Ad esempio:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>

<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

L'aggiunta di tipi di URL all'elenco richiede anche la configurazione del client. Creare la chiave del Registro di sistema e i valori seguenti sul client Windows.

> **Nota:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nome del valore: ExtraURLProtocols
- Tipo di valore: REG_SZ
- Dati valore: specificare i tipi di URL richiesti separati da punto e virgola. Includere tutto prima della parte dell'URL relativa all'autorità. Ad esempio:
  `ftp://;mailto:;customtype1://;custometype2://`

È possibile aggiungere tipi di URL solo per i client Windows. I client che non hanno le impostazioni del Registro di sistema sopra indicate rifiutano il reindirizzamento alla sessione Citrix. Il client deve avere un'applicazione installata e configurata per gestire i tipi di URL specificati.

Per rimuovere i tipi di URL dall'elenco di reindirizzamento predefinito, creare la chiave del Registro di sistema e i valori seguenti sul server VDA.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome valore: DisableServerFTA
- Tipo di valore: DWORD
- Dati del valore: 1
- Nome valore: NoRedirectClasses
- Tipo di valore: REG_MULTI_SZ
- Dati del valore: specificare qualsiasi combinazione di valori: `http`,`https`, `rtsp`, `rtspu`, `pnm` o `mms`. Digitare più valori su righe separate. Ad esempio:

```
http
https
rtsp
```

Per abilitare il reindirizzamento da host a client per un insieme specifico di siti Web, creare una chiave del Registro di sistema e i valori sul server VDA.

- Chiave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome del valore: ValidSites
- Tipo di valore: REG_MULTI_SZ
- Dati del valore: specificare qualsiasi combinazione di nomi di dominio completi (FQDN). Digitare più FQDN su righe separate. Includere solo il nome di dominio completo, senza protocolli (`http://` o `https://`). Un nome di dominio completo può includere un asterisco (`*`) come carattere jolly solo nella posizione più a sinistra. Questo carattere jolly corrisponde a un singolo livello di dominio, che è coerente con le regole in RFC 6125. Ad esempio:

```
www.exmaple.com
*.example.com
```

> **Nota:**
>
> Non è possibile utilizzare il tasto **ValidSites** in combinazione con le chiavi **DisableServerFTA** e **NoRedirectClasses**.

### Configurazione predefinita del browser del server VDA

L'abilitazione del reindirizzamento da host al client come indicato in questa sezione sostituisce qualsiasi precedente configurazione predefinita del browser sul server VDA. Se un URL Web non viene reindirizzato, Citrix Launcher trasferisce l'URL al browser configurato nella chiave del Registro di sistema`command_backup`. La chiave punta a Internet Explorer per impostazione predefinita, ma è possibile modificarla per includere il percorso a un browser diverso. Per ulteriori informazioni, vedere Configurazione predefinita del browser del server VDA nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Reindirizzamento del contenuto bidirezionale

October 6, 2022

Il reindirizzamento bidirezionale dei contenuti consente di trasmettere gli URL HTTP o HTTPS presenti nei browser Web o incorporati nelle applicazioni fra la sessione Citrix VDA e l'endpoint client in entrambe le direzioni. Un URL inserito in un browser in esecuzione nella sessione Citrix può essere aperto utilizzando il browser predefinito del client. Al contrario, un URL inserito in un browser in esecuzione sul client può essere aperto in una sessione Citrix, con un'applicazione pubblicata o un desktop. Alcuni casi d'uso comuni per il reindirizzamento bidirezionale dei contenuti includono:

- Reindirizzamento degli URL Web nei casi in cui il browser di partenza non abbia accesso alla rete alla fonte.
- Reindirizzamento degli URL Web per motivi di compatibilità e sicurezza del browser.
- Il reindirizzamento degli URL Web incorporati nelle applicazioni quando si esegue un browser Web nella sessione Citrix o sul client non è richiesto.

### Requisiti di sistema

- VDA con sistema operativo a sessione singola o multisessione
- App Citrix Workspace per Windows

Browser:

- Internet Explorer 11
- Google Chrome con estensione per il reindirizzamento del browser Citrix (disponibile sul Google Chrome Web Store)
- Microsoft Edge (Chromium) con Citrix Browser Redirection Extension (disponibile sul Google Chrome Web Store)

### Configurazione

Il reindirizzamento bidirezionale dei contenuti deve essere abilitato utilizzando la politica Citrix sia sul VDA che sul client affinché il reindirizzamento funzioni. Il reindirizzamento bidirezionale dei contenuti è disabilitato per impostazione predefinita.

Per la configurazione del VDA, vedere Reindirizzamento bidirezionale del contenuto nelle impostazioni dei criteri ICA.

Per la configurazione del client, vedere Reindirizzamento bidirezionale del contenuto nella documentazione dell'app Citrix Workspace per Windows.

Le estensioni del browser devono essere registrate utilizzando i comandi descritti. Eseguire i comandi secondo necessità sul VDA e sul client in base al browser in uso.

Per registrare le estensioni del browser su VDA, aprire un prompt dei comandi. Quindi, eseguire `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` con l'opzione del browser richiesta come negli esempi illustrati:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

Per registrare l'estensione su tutti i browser disponibili eseguire:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

Per annullare la registrazione di un'estensione del browser utilizzare l'opzione `/unreg<browser>` come nell'esempio:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Per registrare le estensioni del browser sul client, aprire un prompt dei comandi ed eseguire `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` con le stesse opzioni degli esempi.

> **Nota:**
>
> Il comando register fa sì che i browser Chrome ed Edge chiedano agli utenti di abilitare l'estensione di reindirizzamento del browser Citrix durante il primo avvio. L'estensione del browser può essere installata anche manualmente dal Google Chrome Web Store.

### Reindirizzamento con caratteri jolly da Citrix VDA al client

Il reindirizzamento bidirezionale dei contenuti supporta l'uso di caratteri jolly quando si definiscono gli URL da reindirizzare. Per configurare il reindirizzamento bidirezionale dei contenuti, vedere le istruzioni di configurazione.

In Citrix Studio, impostare l'URL con caratteri jolly in **Allowed URLs to be redirected to Client** (URL consentiti da reindirizzare al client). L'asterisco (*) è il carattere jolly.

> **NOTA:**
>
> - Non impostare **Allowed URLs to be redirected to VDA** (URL con reindirizzamento a VDA consentito) nei criteri del client. Assicurarsi che i siti impostino **Allowed URLs to be redirected to VDA** (URL con reindirizzamento a VDA consentito) per evitare cicli di reindirizzamento infiniti.
> - I domini di primo livello non sono supportati. Ad esempio, `https://www.citrix.*` oppure `http://www.citrix.co*` non viene reindirizzato.

### Reindirizzamento del protocollo personalizzato dal VDA al client

Il reindirizzamento bidirezionale dei contenuti supporta il reindirizzamento di protocolli personalizzati da Citrix VDA al client. Sono supportati protocolli diversi da HTTP o HTTPS. Per configurare il reindirizzamento bidirezionale dei contenuti, vedere le istruzioni di configurazione.

In Citrix Studio, impostare il protocollo personalizzato in **Allowed URLs to be redirected to Client** (URL con reindirizzamento al client consentito).

> **NOTA:**
>
> - Il client deve avere un'applicazione registrata per gestire il protocollo. In caso contrario, l'URL reindirizza al client e l'avvio non riesce.
> - Gli URL di protocollo personalizzati immessi o avviati nei browser Chrome ed Edge non sono supportati e non sono reindirizzati.
> - I seguenti protocolli non sono supportati: `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

### Altre considerazioni

- I requisiti e le configurazioni del browser sono applicabili solo al browser che avvia il reindirizzamento. Il browser di destinazione, in cui l'URL si apre dopo che il reindirizzamento è riuscito, non è considerato per il supporto. Quando si reindirizzano gli URL dal VDA a un client, una configurazione del browser supportata è richiesta solo sul VDA. Invece, quando si reindirizzano gli URL dal client a un VDA, una configurazione del browser supportata è richiesta solo sul client. Gli URL reindirizzati vengono trasferiti al browser predefinito configurato sulla macchina di destinazione, il client o il VDA, a seconda della direzione. L'utilizzo dello stesso tipo di browser sul VDA e il client NON è richiesto.
- Verificare che le regole di reindirizzamento non determinino una configurazione ciclica. Ad esempio, una politica VDA è impostata per reindirizzare `https://www.citrix.com` e il criterio del client è impostato per reindirizzare lo stesso URL, con conseguente loop infinito.

- Sono supportati solo gli URL con protocollo HTTP/HTTPS. Gli abbreviatori di URL non sono supportati.
- Il reindirizzamento da client a VDA richiede che il client Windows sia installato con diritti di amministratore.
- Se il browser di destinazione è già aperto, l'URL reindirizzato si apre in una nuova scheda. Altrimenti l'URL si apre in una nuova finestra del browser.
- Il reindirizzamento bidirezionale dei contenuti non funziona quando Local App Access (LAA) è abilitato.

## Accesso alle app locali e reindirizzamento URL

October 6, 2022

### Introduzione

L'accesso alle app locali integra perfettamente le applicazioni Windows installate localmente in un ambiente desktop ospitato senza passare da un desktop all'altro. Con l'accesso alle app locali, è possibile:

- Accedere alle applicazioni installate localmente su un laptop, PC o altro dispositivo fisico direttamente dal desktop virtuale.
- Fornire una soluzione flessibile per la distribuzione delle applicazioni. Se gli utenti dispongono di applicazioni locali che non è possibile virtualizzare o che l'IT non gestisce, tali applicazioni si comportano comunque come se fossero installate su un desktop virtuale.
- Eliminare la latenza a doppio hop quando le applicazioni sono ospitate separatamente dal desktop virtuale. È possibile farlo inserendo un collegamento all'applicazione pubblicata sul dispositivo Windows dell'utente.
- Utilizzare applicazioni quali:
  - Software per videoconferenze come GoToMeeting.
  - Applicazioni speciali o di nicchia che non sono ancora virtualizzate.
  - Applicazioni e periferiche che altrimenti trasferirebbero grandi quantità di dati da un dispositivo utente a un server e da un server al dispositivo utente. Ad esempio, masterizzatori DVD e sintonizzatori TV.

In Citrix Virtual Apps and Desktops, le sessioni desktop ospitate utilizzano il reindirizzamento URL per avviare le applicazioni della funzionalità di accesso alle app locali. Il reindirizzamento URL rende l'applicazione disponibile in più di un indirizzo URL. Avvia un browser locale (basato sull'elenco di blocco URL del browser) selezionando i collegamenti incorporati all'interno di un browser in una sessione

desktop. Se si passa a un URL non presente nell'elenco di blocco, l'URL viene riaperto nella sessione desktop.

Il reindirizzamento URL funziona solo per le sessioni desktop, non per le sessioni di applicazioni. L'unica funzionalità di reindirizzamento che è possibile utilizzare per le sessioni di applicazione è il reindirizzamento del contenuto da host a client, ovvero un tipo di reindirizzamento FTA (File Type Association) del server. Questa FTA reindirizza determinati protocolli al client, ad esempio HTTP, HTTPS, RTSP o MMS. Ad esempio, se si aprono solo collegamenti incorporati con HTTP, i collegamenti vengono aperti direttamente con l'applicazione client. Gli elenchi di blocco o le liste consentite di URL non sono supportati.

Quando l'accesso alle app locali è abilitato, gli URL che per gli utenti vengono visualizzati come collegamenti da applicazioni eseguite localmente, da applicazioni ospitate dagli utenti o come collegamenti sul desktop vengono reindirizzati in uno dei modi seguenti:

- Dal computer dell'utente al desktop ospitato
- Dal server Citrix Virtual Apps and Desktops al computer dell'utente
- Ne viene eseguito il rendering nell'ambiente in cui vengono avviati (non reindirizzati)

Per specificare il percorso di reindirizzamento del contenuto di siti Web specifici, configurare l'elenco di blocco e la lista consentita di URL nel Virtual Delivery Agent. Tali elenchi contengono chiavi del Registro di sistema a più stringhe che specificano le impostazioni dei criteri di reindirizzamento URL. Per ulteriori informazioni, vedere Impostazioni dei criteri di accesso alle app locali.

Può essere eseguito il rendering degli URL sul VDA, con le seguenti eccezioni:

- Informazioni locali/geografiche: siti Web che richiedono informazioni sulle impostazioni internazionali, come msn.com o news.google.com (apre una pagina specifica per il paese in base all'area geografica). Ad esempio, se viene eseguito il provisioning del VDA da un centro dati nel Regno Unito e il client si connette dall'India, l'utente si aspetta di vedere in.msn.com. Invece, l'utente vede uk.msn.com.
- Contenuti multimediali: i siti Web con contenuti multimediali, quando ne viene eseguito il rendering sul dispositivo client, offrono agli utenti finali un'esperienza nativa e consentono inoltre di risparmiare larghezza di banda anche in reti ad alta latenza. Questa funzionalità reindirizza i siti con altri tipi di supporti, ad esempio Silverlight. Questo processo avviene in un ambiente sicuro. Ossia gli URL approvati dall'amministratore vengono eseguiti sul client, mentre gli altri URL vengono reindirizzati al VDA.

Oltre al reindirizzamento URL, è possibile utilizzare il reindirizzamento FTA. FTA avvia le applicazioni locali quando viene rilevato un file nella sessione. Se l'app locale viene avviata, deve avere accesso al file per aprirlo. Di conseguenza, è possibile aprire solo i file che risiedono in condivisioni di rete o su unità client (utilizzando il mapping delle unità client) tramite applicazioni locali. Ad esempio, quando si apre un file PDF, se un lettore PDF è un'app locale, il file si apre utilizzando quel lettore PDF. Poiché

l'app locale può accedere direttamente al file, non vi è alcun trasferimento di rete del file tramite ICA per aprirlo.

### Requisiti, considerazioni e limitazioni

Supportiamo l'accesso alle app locali sui sistemi operativi validi per i VDA per i sistemi operativi Windows multisessione e per i VDA per i sistemi operativi Windows a sessione singola. L'accesso alle app locali richiede l'app Citrix Workspace per Windows (versione minima 4.1). Sono supportati i seguenti browser:

- Edge, ultima versione
- Firefox, ultima versione e rilascio del supporto esteso
- Chrome, ultima versione

Tenere presenti le considerazioni e le limitazioni seguenti quando si utilizza l'accesso alle app locali e il reindirizzamento URL.

- L'accesso alle app locali è progettato per desktop virtuali a schermo intero che occupano l'intero monitor:
  - L'esperienza utente può risultare confusa se si utilizza l'accesso alle app locali con un desktop virtuale che viene eseguito in modalità finestra o non copre tutti i monitor.
  - Più monitor: quando un monitor viene ingrandito, diventa il desktop predefinito per tutte le applicazioni avviate in quella sessione. Questa impostazione predefinita si verifica anche se le applicazioni successive si avviano in genere su un altro monitor.
  - La funzionalità supporta un VDA. Non vi è alcuna integrazione con più VDA simultanei.
- Alcune applicazioni possono comportarsi in modo imprevisto, con conseguenze per gli utenti:
  - Le lettere di unità potrebbero confondere gli utenti, ad esempio la C: del computer locale anziché l'unità C: del desktop virtuale.
  - Le stampanti disponibili nel desktop virtuale non sono disponibili per le applicazioni locali.
  - Le applicazioni che richiedono autorizzazioni elevate non possono essere avviate come applicazioni ospitate dal client.
  - Non esiste una gestione speciale per le applicazioni a istanza singola (ad esempio Windows Media Player).
  - Le applicazioni locali vengono visualizzate con il tema Windows del computer locale.
  - Le applicazioni a schermo intero non sono supportate. Queste applicazioni includono applicazioni che si aprono a schermo intero, come presentazioni di PowerPoint o visualizzatori di foto che occupano l'intero desktop.

  - L'accesso alle app locali copia le proprietà dell'applicazione locale (ad esempio i collegamenti sul desktop del client e il menu Start) sul VDA. Tuttavia, non copia altre proprietà, come i tasti di scelta rapida e gli attributi di sola lettura.
  - Le applicazioni che personalizzano la modalità di gestione dell'ordine delle finestre sovrapposte possono avere risultati imprevedibili. Ad esempio, alcune finestre potrebbero essere nascoste.
  - I collegamenti non sono supportati, tra cui Risorse del computer, Cestino, Pannello di controllo, collegamenti alle unità di rete e collegamenti alle cartelle.
  - I tipi di file e i file seguenti non sono supportati: tipi di file personalizzati, file senza programmi associati, file zip e file nascosti.
  - Il raggruppamento della barra delle applicazioni non è supportato per le applicazioni ospitate su client a 32 e 64 bit o le applicazioni VDA miste. Ossia, il raggruppamento di applicazioni locali a 32 bit con applicazioni VDA a 64 bit.
  - Le applicazioni non possono essere avviate utilizzando COM. Ad esempio, se si fa clic su un documento di Office incorporato da un'applicazione Office, l'avvio del processo non può essere rilevato e l'integrazione dell'applicazione locale ha esito negativo.

- Gli scenari a doppio hop, in cui un utente avvia un desktop virtuale da un'altra sessione di desktop virtuale, non sono supportati.
- Il reindirizzamento URL supporta solo URL espliciti (ovvero URL visualizzati nella barra degli indirizzi del browser o trovati utilizzando la navigazione nel browser, a seconda del browser).
- Il reindirizzamento URL funziona solo con le sessioni desktop, non con le sessioni delle applicazioni.
- La cartella desktop locale in una sessione VDA non consente agli utenti di creare file.
- Più istanze di un'applicazione in esecuzione localmente si comportano in base alle impostazioni della barra delle applicazioni impostate per il desktop virtuale. Tuttavia, i collegamenti alle applicazioni eseguite localmente non vengono raggruppati con istanze in esecuzione di tali applicazioni. Inoltre, non sono raggruppati con istanze in esecuzione di applicazioni ospitate o collegamenti alle applicazioni ospitate aggiunti. Gli utenti possono chiudere solo le finestre delle applicazioni in esecuzione localmente dalla barra delle applicazioni. Sebbene gli utenti possano aggiungere le finestre delle applicazioni locali alla barra delle applicazioni del desktop e al menu Start, le applicazioni potrebbero non essere avviate in modo coerente quando si utilizzano questi collegamenti.
- Se l'impostazione del criterio **Allow Local App Access (Consenti accesso alle app locali)** è **Abilitata**, il reindirizzamento del contenuto del browser non è supportato.

### Interazione con Windows

L'interazione dell'accesso alle app locali con Windows include i seguenti comportamenti.

- Comportamento dei collegamenti di Windows 8 e Windows Server 2012

  - Le applicazioni di Windows Store installate nel client non vengono enumerate come parte dei collegamenti dell'accesso alle app locali.
  - I file di immagine e video vengono aperti per impostazione predefinita utilizzando le applicazioni di Windows Store. Tuttavia, l'accesso alle app locali enumera le applicazioni di Windows Store e apre i collegamenti con le applicazioni desktop.

- Programmi locali
  - Per Windows 7, la cartella è disponibile nel menu Start.
  - Per Windows 8, Programmi locali è disponibile solo quando l'utente sceglie **Tutte le app** come categoria dalla schermata Start. Non tutte le sottocartelle vengono visualizzate in Programmi locali.

- Funzionalità grafiche di Windows 8 per le applicazioni
  - Le applicazioni desktop sono limitate all'area desktop e sono coperte dalla schermata Start e dalle applicazioni in stile Windows 8.
  - Le applicazioni dell'accesso alle app locali non si comportano come le applicazioni desktop in modalità multi-monitor. In modalità multi-monitor, la schermata Start e il desktop vengono visualizzati su monitor diversi.

- Reindirizzamento URL dell'accesso alle app locali e di Windows 8
  - Poiché Internet Explorer di Windows 8 non dispone di componenti aggiuntivi abilitati, utilizzare Internet Explorer desktop per abilitare il reindirizzamento degli URL.
  - In Windows Server 2012, Internet Explorer disabilita i componenti aggiuntivi per impostazione predefinita. Per implementare il reindirizzamento URL, disabilitare la configurazione avanzata di Internet Explorer. Quindi reimpostare le opzioni di Internet Explorer ed eseguire il riavvio per assicurarsi che i componenti aggiuntivi siano abilitati per gli utenti standard.

### Configurare l'accesso alle app locali e il reindirizzamento URL

Per utilizzare l'accesso alle app locali e il reindirizzamento URL con l'app Citrix Workspace:

- Installare l'app Citrix Workspace sul computer client locale. È possibile abilitare entrambe le funzionalità durante l'installazione dell'app Citrix Workspace oppure abilitare il modello di accesso alle app locali utilizzando l'Editor Criteri di gruppo.
- Configurare l'impostazione del criterio **Allow local app access (Consenti accesso alle app locali)** su **Enabled (Abilitato)**. È inoltre possibile configurare le impostazioni dei criteri degli elenchi di blocco e delle liste consentite di URL per il reindirizzamento degli URL. Per ulteriori informazioni, vedere Impostazioni dei criteri di accesso alle app locali.

### Abilitare l'accesso alle app locali e il reindirizzamento URL

Per abilitare l'accesso alle app locali per tutte le applicazioni locali, attenersi alla seguente procedura:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Policies** (Criteri) nel riquadro di sinistra.
2. Selezionare **Create Policy** (Crea criterio) nella barra delle azioni.
3. Nella finestra Create Policy (Crea criterio) digitare "Allow Local App Access"(Consenti accesso alle app locali) nella casella di ricerca, quindi fare clic su **Select (Seleziona)**.
4. Nella finestra Edit Setting (Modifica impostazione), selezionare **Allowed (Consentita)**. Per impostazione predefinita, il criterio **Allow local app access (Consenti accesso alle app locali)** è vietato. Una volta consentita questa impostazione, il VDA consente all'utente finale di decidere se le applicazioni pubblicate e i collegamenti dell'accesso alle app locali sono ablitati nella sessione. Se questa impostazione è vietata, sia le applicazioni pubblicate che i collegamenti dell'accesso alle app locali non funzionano per il VDA. Questa impostazione del criterio si applica all'intero computer e al criterio di reindirizzamento URL.
5. Nella finestra Crea criterio digitare "URL redirection allow list"(Elenco consentito per il reindirizzamento URL) nella casella di ricerca, quindi fare clic su **Select (Seleziona)**. L'elenco consentito per il reindirizzamento URL specifica gli URL da aprire nel browser predefinito della sessione remota.
6. Nella finestra Edit Setting (Modifica impostazione) fare clic su **Add (Aggiungi)** per aggiungere gli URL, quindi fare clic su **OK**.
7. Nella finestra Create Policy (Crea criterio), digitare "URL redirection block list"(Elenco di blocco per il reindirizzamento URL) nella casella di ricerca, quindi fare clic su **Select (Seleziona)**. L'elenco di blocco per il reindirizzamento URL specifica gli URL reindirizzati al browser predefinito in esecuzione sull'endpoint.
8. Nella finestra Edit Setting (Modifica impostazione) fare clic su **Add (Aggiungi)** per aggiungere gli URL, quindi fare clic su **OK**.
9. Nella pagina Settings (Impostazioni) fare clic su **Next (Avanti)**.
10. Nella pagina Users and Machines (Utenti e computer) assegnare il criterio ai gruppi di consegna applicabili, quindi fare clic su **Next (Avanti)**.
11. Nella pagina Summary (Riepilogo) esaminare le impostazioni e fare clic su **Finish (Fine)**.

Per abilitare il reindirizzamento URL per tutte le applicazioni locali durante l'installazione dell'app Citrix Workspace, attenersi alla seguente procedura:

1. Abilitare il reindirizzamento URL quando si installa l'app Citrix Workspace per tutti gli utenti su un computer. In questo modo vengono registrati anche i componenti aggiuntivi del browser necessari per il reindirizzamento URL.
2. Dal prompt dei comandi eseguire il comando appropriato per installare l'app Citrix Workspace

utilizzando una delle seguenti opzioni:

- Per CitrixReceiver.exe, utilizzare /`ALLOW_CLIENTHOSTEDAPPSURL`=1.
- Per CitrixReceiverWeb.exe, utilizzare /`ALLOW_CLIENTHOSTEDAPPSURL`=1.

#### Attivare il modello dell'accesso alle app locali utilizzando l'Editor Criteri di gruppo

> **Nota:**
>
> - Prima di abilitare il modello dell'accesso alle app locali utilizzando l'Editor Criteri di gruppo, aggiungere i `receiver.admx`/`adml`file del modello all'oggetto Criteri di gruppo locale. Per ulteriori informazioni, vedere Introduzione e cercare il *modello amministrativo dell'oggetto Criteri di gruppo*.
> - I file del modello dell'app Citrix Workspace per Windows sono disponibili nell'oggetto Criteri di gruppo locale nella cartella **Modelli amministrativi > Citrix Components (Componenti Citrix) > Citrix Workspace** solo quando si aggiunge `CitrixBase.admx`/`CitrixBse.adml` alla cartella %systemroot%\policyDefinitions.

Per abilitare il modello dell'accesso alle app locali utilizzando l'editor Criteri di gruppo, attenersi alla seguente procedura:

1. Eseguire **gpedit.msc**.
2. Andare a **Configurazione computer > Modelli amministrativi > Modelli amministrativi classici (ADM) > Citrix Components (Componenti Citrix) > Citrix Workspace > User Experience (Esperienza utente)**.
3. Fare clic su **Local App Access settings (Impostazioni di accesso alle app locali)**.
4. Selezionare **Enabled (Abilitate)**, quindi **Allow URL Redirection (Consenti reindirizzamento URL)**. Per il reindirizzamento URL, registrare i componenti aggiuntivi del browser utilizzando la riga di comando descritta nella sezione *Registrare i componenti aggiuntivi del browser* più oltre in questo articolo.

#### Fornire l'accesso solo alle applicazioni pubblicate

È possibile fornire l'accesso alle applicazioni pubblicate utilizzando l'Editor del Registro di sistema o l'SDK PowerShell.

Nell'Editor del Registro di sistema, vedere Accesso alle app locali per le applicazioni pubblicate nell'elenco delle funzionalità gestite tramite il Registro di sistema.

Per utilizzare l'SDK PowerShell:

1. Aprire PowerShell sul computer su cui è in esecuzione il Delivery Controller.

2. Immettere il seguente comando: `set-configsitemetadata -name "studio_clientHostedApp "-value "true"`.

Per avere accesso a **Add Local App Access Application (Aggiungi applicazione di accesso alle app locali)** in una distribuzione di Citrix DaaS, utilizzare Remote PowerShell SDK di Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere Remote PowerShell SDK per Citrix Virtual Apps and Desktops.

1. Scaricare il programma di installazione:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Eseguire questi comandi:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. Immettere il seguente comando: `set-configsitemetadata -name "studio_clientHostedApp " -value "true"`.

Dopo aver completato i passaggi precedenti applicabili, attenersi alla seguente procedura per continuare.

1. Andare a **Manage > Full Configuration**, quindi selezionare **Applications** nel riquadro di sinistra.
2. Nel riquadro centrale superiore, fare clic con il pulsante destro del mouse sull'area vuota e selezionare **Add Local App Access Application (Aggiungi applicazione di accesso alle app locali)** dal menu. È inoltre possibile fare clic su **Add Local App Access Application (Aggiungi applicazione di accesso alle app locali)** nel riquadro Actions (Azioni). Per visualizzare l'opzione Add Local App Access Application (Aggiungi applicazione di accesso alle app locali) nel riquadro Actions (Azioni), fare clic su **Refresh (Aggiorna)**.
3. Pubblicare l'applicazione di accesso alle app locali.

   - Viene avviata la procedura guidata dell'accesso alle applicazioni locali con una pagina introduttiva, che è possibile rimuovere dai futuri avvii della procedura guidata.
   - La procedura guidata guida l'utente attraverso le pagine Groups (Gruppi), Location (Posizione), Identification (Identificazione), Delivery (Consegna) e Summary (Riepilogo) descritte di seguito. Al termine di ogni pagina, fare clic su **Next (Avanti)** fino a raggiungere la pagina Summary (Riepilogo).
   - Nella pagina Groups (Gruppi) selezionare uno o più gruppi di consegna in cui verranno aggiunte le nuove applicazioni, quindi fare clic su **Next (Avanti)**.
   - Nella pagina Location (Posizione) digitare il percorso eseguibile completo dell'applicazione sul computer locale dell'utente e digitare il percorso della cartella in cui si trova

l'applicazione. Citrix consiglia di utilizzare il percorso della variabile di ambiente di sistema, ad esempio %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.

- Nella pagina Identification (Identificazione) accettare i valori predefiniti o digitare le informazioni desiderate, quindi fare clic su **Next (Avanti)**.
- Nella pagina Delivery (Consegna) configurare il modo in cui l'applicazione viene consegnata agli utenti, quindi fare clic su **Next (Avanti)**. È possibile specificare l'icona per l'applicazione selezionata. È inoltre possibile specificare se il collegamento all'applicazione locale sul desktop virtuale dovrà essere visibile nel menu Start, sul desktop o in entrambi.
- Nella pagina Summary (Riepilogo) esaminare le impostazioni, quindi fare clic su **Finish (Fine)** per uscire dalla procedura guidata dell'accesso alle applicazioni locali.

### Registrare i componenti aggiuntivi del browser

> **Nota:**
>
> I componenti aggiuntivi del browser necessari per il reindirizzamento degli URL vengono registrati automaticamente quando si installa l'app Citrix Workspace dalla riga di comando utilizzando l'opzione `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

È possibile utilizzare i seguenti comandi per registrare uno o tutti i componenti aggiuntivi e annullarne la registrazione:

- Per registrare componenti aggiuntivi su un dispositivo client: <*client-installation-folder*>\redirector.exe /reg<*browser*>
- Per annullare la registrazione dei componenti aggiuntivi su un dispositivo client: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- Per registrare componenti aggiuntivi in un VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- Per annullare la registrazione di componenti aggiuntivi in un VDA: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

In cui <*browser*> è Internet Explorer, Firefox, Chrome o Tutti.

Ad esempio, il comando seguente registra i componenti aggiuntivi di Internet Explorer su un dispositivo con l'app Citrix Workspace in esecuzione.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

Il comando seguente registra tutti i componenti aggiuntivi in un VDA con sistema operativo Windows multisessione.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

**Intercettazione URL tra browser**

- Per impostazione predefinita, Internet Explorer reindirizza l'URL specificato. Se l'URL non è incluso nell'elenco di blocco ma il browser o il sito Web lo reindirizza a un altro URL, l'URL finale non viene reindirizzato. Non viene reindirizzato anche se è incluso nell'elenco di blocco.

Perché il reindirizzamento URL funzioni correttamente, abilitare il componente aggiuntivo quando viene richiesto dal browser. Se i componenti aggiuntivi che utilizzano le opzioni Internet o i componenti aggiuntivi nel prompt sono disabilitati, il reindirizzamento URL non funziona correttamente.

- I componenti aggiuntivi di Firefox reindirizzano sempre gli URL.

Quando viene installato un componente aggiuntivo, Firefox chiede di consentire o impedire l'installazione del componente aggiuntivo in una nuova scheda. Consentire il componente aggiuntivo per garantire il corretto funzionamento della funzionalità.

- Il componente aggiuntivo di Chrome reindirizza sempre l'URL finale a cui si accede e non gli URL inseriti.

Le estensioni sono state installate esternamente. Quando si disabilita l'estensione, la funzionalità di reindirizzamento URL non funziona in Chrome. Se il reindirizzamento URL è richiesto in modalità di navigazione in incognito, consentire l'esecuzione dell'estensione in tale modalità nelle impostazioni del browser.

**Configurare il comportamento dell'applicazione locale allo scollegamento e alla disconnessione**

> **Nota:**
>
> Se non si esegue questa procedura per configurare le impostazioni, per impostazione predefinita le applicazioni locali continuano a essere eseguite quando un utente si scollega o si disconnette dal desktop virtuale. Dopo la riconnessione, le applicazioni locali vengono reintegrate se sono disponibili sul desktop virtuale.

Per configurare il comportamento dell'applicazione locale in caso di scollegamento e disconnessione, vedere Comportamento dell'applicazione locale allo scollegamento e alla disconnessione nell'elenco delle funzionalità gestite tramite il Registro di sistema.

## Considerazioni generiche sul reindirizzamento USB e sulle unità client

August 17, 2023

La tecnologia HDX offre **supporto ottimizzato** per i dispositivi USB più diffusi. Il supporto ottimizzato offre una migliore esperienza utente con migliori prestazioni ed efficienza della larghezza di banda su una WAN. Il supporto ottimizzato è solitamente l'opzione migliore, soprattutto in ambienti con latenza elevata o sensibili alla sicurezza.

La tecnologia HDX fornisce un **reindirizzamento USB generico** per dispositivi speciali che non dispongono di alcun supporto ottimizzato o dove questo non è adatto, ad esempio:

- Il dispositivo USB dispone di funzioni più avanzate che non fanno parte del supporto ottimizzato, come un mouse o una webcam con più pulsanti.
- Gli utenti hanno bisogno di funzioni che non fanno parte del supporto ottimizzato.
- Il dispositivo USB è un dispositivo specializzato, come apparecchiature di test e misurazione o un controller industriale.
- Un'applicazione richiede l'accesso diretto al dispositivo come dispositivo USB.
- La periferica USB ha solo un driver Windows disponibile. Ad esempio, un lettore di smart card potrebbe non avere un driver disponibile per l'app Citrix Workspace per Android.
- La versione dell'app Citrix Workspace non fornisce alcun supporto ottimizzato per questo tipo di dispositivo USB.

Con il reindirizzamento USB generico:

- Gli utenti non devono installare driver del dispositivo sul dispositivo utente.
- I driver del client USB sono installati sul computer VDA.

> **Importante:**
>
> - Il reindirizzamento USB generico può essere usato insieme al supporto ottimizzato. Se si abilita il reindirizzamento USB generico, configurare le impostazioni dei criteri dei dispositivi USB Citrix sia per il reindirizzamento USB generico che per il supporto ottimizzato.
> - L'impostazione dei criteri Citrix nelle regole di ottimizzazione dei dispositivi USB client è un'impostazione specifica per il reindirizzamento USB generico, per un particolare dispositivo USB. Non si applica al supporto ottimizzato come descritto qui.
> - Quando si esegue l'intermediazione di una sessione utilizzando il software Citrix su una macchina virtuale di Azure, Citrix fornisce il miglior supporto per il reindirizzamento USB alla macchina virtuale di Azure. Supportiamo la risoluzione di un problema del software Citrix, ma non supportiamo la macchina virtuale di Azure sottostante.
> - I dispositivi CD/DVD con capacità di masterizzazione di dischi possono essere reindirizzati, ma le capacità di masterizzazione di questi dispositivi non possono essere utilizzate. Ciò è dovuto ai limiti del buffer di una sessione.

### Considerazioni sulle prestazioni per i dispositivi USB

La latenza e la larghezza di banda della rete possono influire sull'esperienza utente e sul funzionamento dei dispositivi USB quando si utilizza il reindirizzamento USB generico per alcuni tipi di dispositivi USB. Ad esempio, i dispositivi sensibili all'orario potrebbero non funzionare correttamente su collegamenti a bassa larghezza di banda e a latenza elevata. Utilizzare invece il supporto ottimizzato, dove possibile.

Alcuni dispositivi USB richiedono un'elevata larghezza di banda per poter essere utilizzati, ad esempio un mouse 3D (utilizzato con app 3D che in genere richiedono un'elevata larghezza di banda). Se la larghezza di banda non può essere aumentata, potrebbe esssere possibile mitigare il problema ottimizzando l'utilizzo della larghezza di banda di altri componenti tramite le impostazioni dei criteri di larghezza di banda. Per ulteriori informazioni, vedere Impostazioni dei criteri di larghezza di banda per il reindirizzamento del dispositivo USB client e Impostazioni dei criteri delle connessioni multiflusso.

### Considerazioni sulla sicurezza per i dispositivi USB

Alcuni dispositivi USB sono sensibili alla sicurezza per natura, ad esempio i lettori di smart card, i lettori di impronte digitali e i signature pad. Altri dispositivi USB, come i dispositivi di archiviazione USB, possono essere utilizzati per trasmettere dati potenzialmente sensibili.

I dispositivi USB vengono spesso utilizzati per distribuire malware. La configurazione dell'app Citrix Workspace e di Citrix Virtual Apps and Desktops può ridurre, ma non eliminare, i rischi derivanti da questi dispositivi USB. Questa situazione è valida sia che venga utilizzato il reindirizzamento USB generico sia che venga utilizzato il supporto ottimizzato.

> **Importante:**
>
> Per i dispositivi e i dati sensibili alla sicurezza, proteggere sempre la connessione HDX utilizzando TLS o IPsec.
>
> Abilitare il supporto solo per i dispositivi USB necessari. Configurare sia il reindirizzamento USB generico che il supporto ottimizzato per soddisfare questa esigenza.
>
> Fornire indicazioni agli utenti per l'uso sicuro dei dispositivi USB:
>
> - Utilizzare solo dispositivi USB che sono stati ottenuti da una fonte affidabile.
> - Non lasciare i dispositivi USB incustoditi in ambienti aperti, ad esempio un'unità flash in un Internet café.
> - Spiegare i rischi derivanti dall'utilizzo di un dispositivo USB su più di un computer.

### Compatibilità con il reindirizzamento USB generico

Il reindirizzamento USB generico è supportato per i dispositivi USB 2.0 e precedenti. Il reindirizzamento USB generico è supportato anche per i dispositivi USB 3.0 collegati a una porta USB 2.0 o USB 3.0. Il reindirizzamento USB generico non supporta le funzionalità USB introdotte in USB 3.0, ad esempio la super velocità.

Queste app Citrix Workspace supportano il reindirizzamento USB generico:

- App Citrix Workspace per Windows, vedere Configurazione della distribuzione delle applicazioni.
- App Citrix Workspace per Mac, vedere App Citrix Workspace per Mac.
- App Citrix Workspace per Linux, vedere Ottimizzare.
- App Citrix Workspace per Chrome OS, vedere App Citrix Workspace per Chrome.

Per le versioni dell'app Citrix Workspace, vedere la matrice delle funzionalità dell'app Citrix Workspace.

Se si utilizzano versioni precedenti dell'app Citrix Workspace, consultare la documentazione dell'app Citrix Workspace per verificare che il reindirizzamento USB generico sia supportato. Per eventuali restrizioni sui tipi di dispositivi USB supportati, consultare la documentazione dell'app Citrix Workspace.

Il reindirizzamento USB generico è supportato per le sessioni desktop da VDA per sistema operativo a sessione singola versione 7.6 fino alla versione corrente.

Il reindirizzamento USB generico è supportato per le sessioni desktop da VDA per sistema operativo multisessione dalla versione 7.6 fino alla versione corrente, con le seguenti restrizioni:

- Il VDA deve eseguire Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 o Windows Server 2022.
- I driver dei dispositivi USB devono essere completamente compatibili con l'host di sessione Desktop remoto (RDSH) per il sistema operativo del VDA (Windows 2012 R2), incluso il supporto completo della virtualizzazione.

Alcuni tipi di dispositivi USB non sono supportati per il reindirizzamento USB generico perché non sarebbe utile reindirizzarli:

- Modem USB.
- Schede di rete USB.
- Hub USB. I dispositivi USB collegati agli hub USB vengono gestiti singolarmente.
- Porte COM virtuali USB. Utilizzare il reindirizzamento della porta COM anziché il reindirizzamento USB generico.

Per informazioni sui dispositivi USB testati con il reindirizzamento USB generico, vedere Citrix Ready Marketplace. Alcuni dispositivi USB non funzionano correttamente con il reindirizzamento USB generico.

### Configurare il reindirizzamento USB generico

È possibile controllare e configurare separatamente quali tipi di dispositivi USB utilizzano il reindirizzamento USB generico:

- Sul VDA, utilizzando le impostazioni dei criteri Citrix. Per ulteriori informazioni, vedere Reindirizzamento delle unità client e dei dispositivi utente e Impostazioni dei criteri dei dispositivi USB nella sezione Riferimenti per le impostazioni dei criteri.
- Nell'app Citrix Workspace, utilizzando meccanismi dipendenti dall'app Citrix Workspace. Ad esempio, un modello amministrativo controlla le impostazioni del Registro di sistema che configurano l'app Citrix Workspace per Windows. Per impostazione predefinita, il reindirizzamento USB è consentito per determinate classi di dispositivi USB e negato per altri. Per ulteriori informazioni, vedere Configurare nella documentazione dell'app Citrix Workspace per Windows.

Questa configurazione separata offre flessibilità. Ad esempio:

- Se due diverse organizzazioni o reparti sono responsabili dell'app Citrix Workspace e del VDA, esse possono applicare il controllo separatamente. Questa configurazione si applica quando un utente di un'organizzazione accede a un'applicazione in un'altra organizzazione.
- Le impostazioni dei criteri Citrix possono controllare i dispositivi USB consentiti solo per determinati utenti o per gli utenti che si connettono solo tramite una LAN (anziché tramite Citrix Gateway).

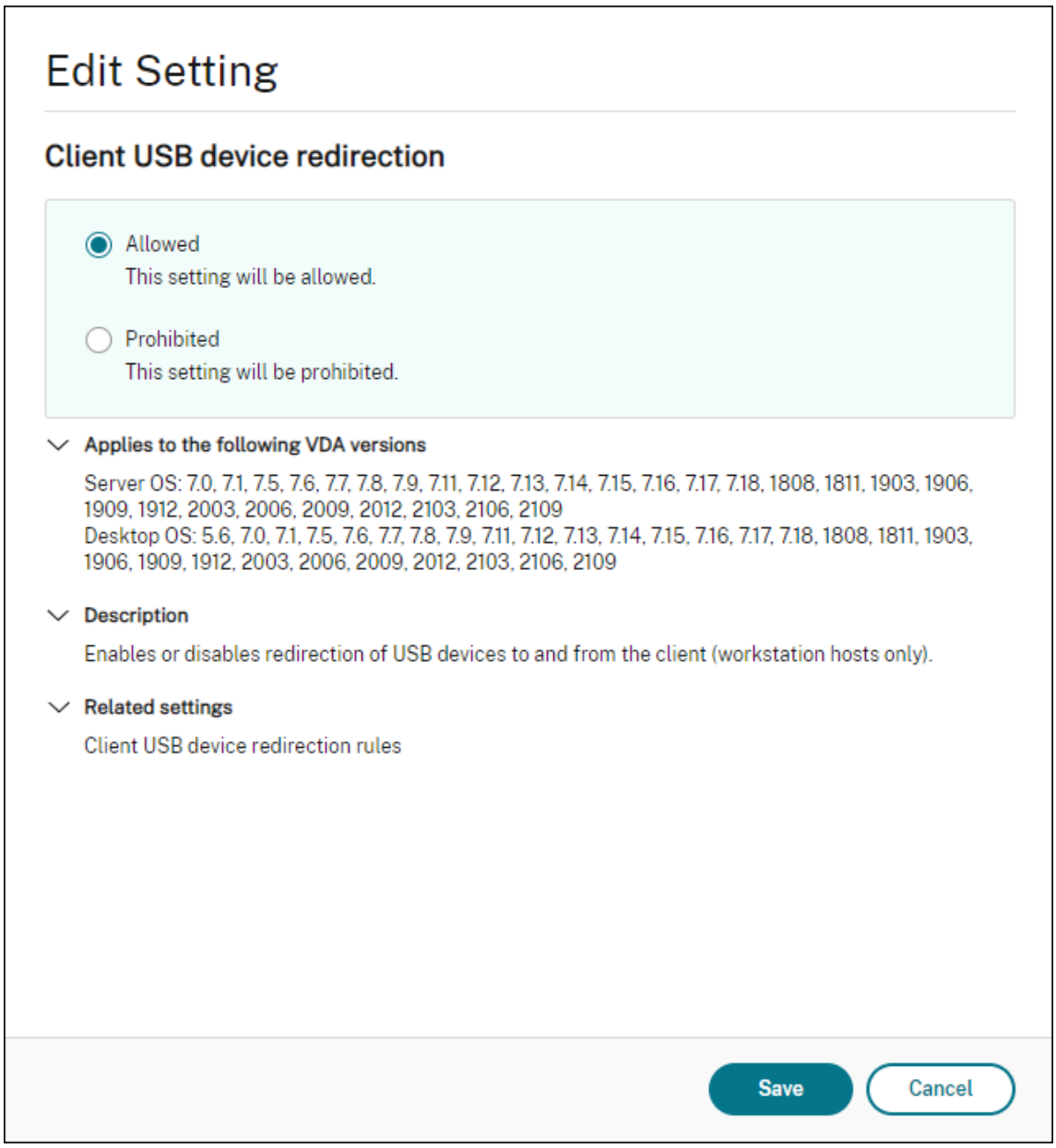
### Abilitare il reindirizzamento USB generico

Per abilitare il reindirizzamento USB generico e non richiedere il reindirizzamento manuale da parte dell'utente, configurare sia le impostazioni dei criteri Citrix che le preferenze di connessione dell'app Citrix Workspace.

Nelle impostazioni dei criteri Citrix:

1. Aggiungere il reindirizzamento del dispositivo USB client a un criterio e impostarne il valore su **Consentito**.

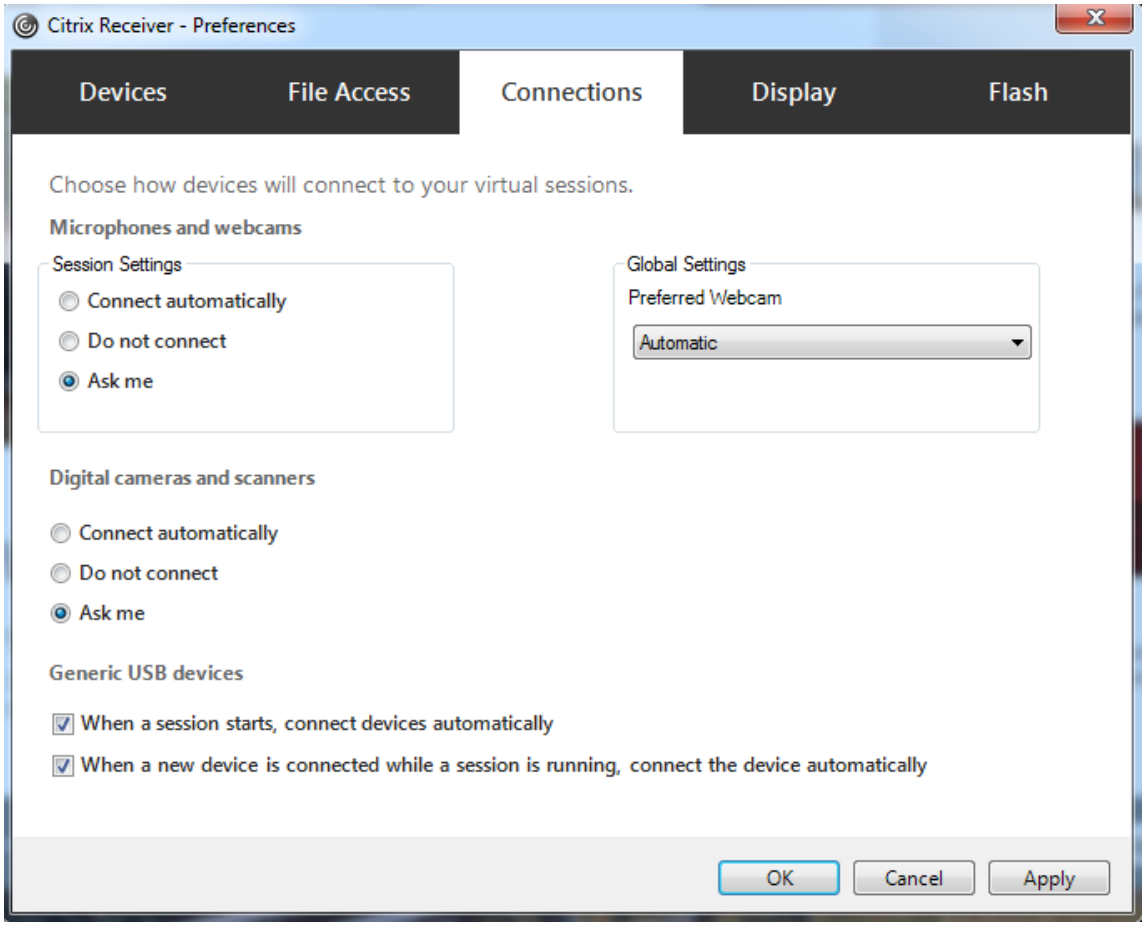



2. (Facoltativo) Per aggiornare l'elenco dei dispositivi USB disponibili per il reindirizzamento, aggiungere l'impostazione Client USB device redirection rules (Reole di reindirizzamenot dispositivo USB client) a un criterio e specificare le regole dei criteri USB.

   Nell'app Citrix Workspace:

3. Specificare che i dispositivi siano collegati automaticamente senza reindirizzamento manuale. È possibile eseguire questa operazione utilizzando un modello amministrativo o nell'app Citrix Workspace per Windows > Preferenze > Connessioni.




Se nel passaggio precedente sono state specificate le regole dei criteri USB per il VDA, specificare le stesse regole dei criteri per l'app Citrix Workspace.

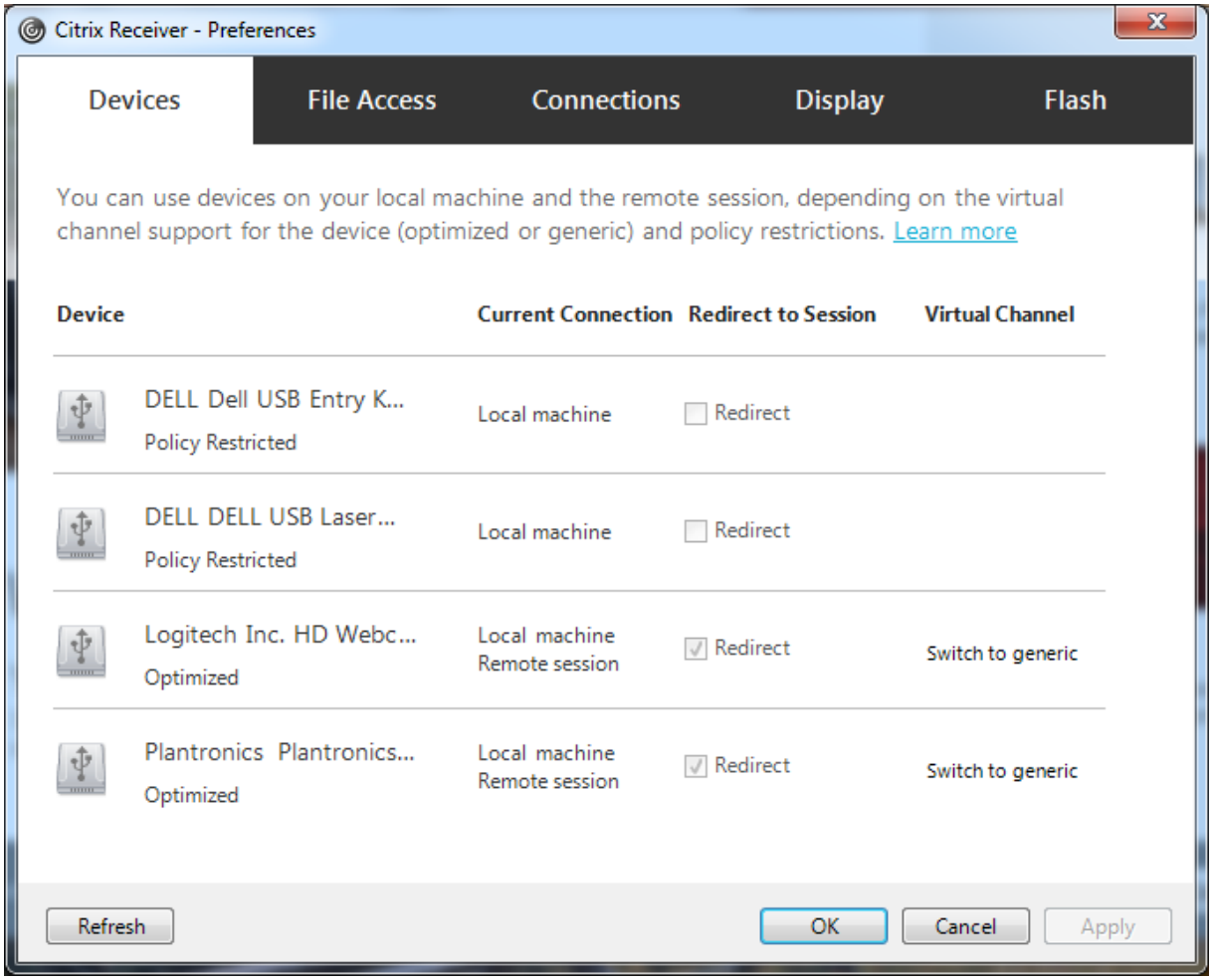
Per i thin client, consultare il produttore per informazioni dettagliate sul supporto USB e per eventuali configurazioni richieste.

### Configurazione dei tipi di dispositivi USB disponibili per il reindirizzamento USB generico

I dispositivi USB vengono reindirizzati automaticamente quando il supporto USB è abilitato e le impostazioni delle preferenze utente USB sono impostate per collegare automaticamente i dispositivi USB. Anche i dispositivi USB vengono reindirizzati automaticamente quando la barra di connessione non è presente.

Gli utenti possono reindirizzare esplicitamente i dispositivi che non vengono reindirizzati automaticamente selezionando i dispositivi dall'elenco dei dispositivi USB. Per ulteriori informazioni, l'articolo della guida per l'utente dell'app Citrix Workspace per Windows, Visualizzare i dispositivi in Desktop Viewer.




Per utilizzare il reindirizzamento USB generico anziché il supporto ottimizzato, è possibile:

- Nell'app Citrix Workspace, selezionare manualmente il dispositivo USB per utilizzare il reindirizzamento USB generico e scegliere **Switch to generic (Passa a generico)** dalla scheda Devices (Dispositivi) della finestra di dialogo Preferences (Preferenze).
- Selezionare automaticamente il dispositivo USB per utilizzare il reindirizzamento USB generico, configurando il reindirizzamento automatico per il tipo di dispositivo USB (ad esempio, AutoRedirectStorage=1) e impostare le impostazioni delle preferenze utente USB per collegare automaticamente i dispositivi USB. Per ulteriori informazioni, vedere Configurare il reindirizzamento automatico dei dispositivi USB.

> **Nota:**
>
> Configurare il reindirizzamento USB generico per l'utilizzo con una webcam solo se la webcam risulta incompatibile con il reindirizzamento multimediale HDX.

Per evitare che i dispositivi USB vengano elencati o reindirizzati, è possibile specificare le regole dei dispositivi per l'app Citrix Workspace e il VDA.

Per il reindirizzamento USB generico, è necessario conoscere almeno la classe e la sottoclasse del dispositivo USB. Non tutti i dispositivi USB utilizzano la relativa classe e sottoclasse ovvie di dispositivi USB. Ad esempio:

- Le penne utilizzano la classe del mouse.
- I lettori di smart card possono utilizzare la classe di dispositivo HID o definita dal fornitore.

Per un controllo più preciso, è necessario conoscere l'ID fornitore, l'ID prodotto e l'ID versione. È possibile ottenere queste informazioni dal fornitore del dispositivo.

> **Importante:**
>
> I dispositivi USB dannosi potrebbero presentare caratteristiche dei dispositivi USB che non corrispondono all'utilizzo previsto. Le regole del dispositivo non hanno lo scopo di impedire questo comportamento.

È possibile controllare i dispositivi USB disponibili per il reindirizzamento USB generico specificando le regole di reindirizzamento dei dispositivi USB sia per il VDA che per l'app Citrix Workspace, per ignorare le regole dei criteri USB predefinite.

Per il VDA:

- Modificare le regole di override dell'amministratore per i computer con sistema operativo multisessione tramite le regole dei criteri di gruppo. La Console Gestione Criteri di gruppo è inclusa nel supporto di installazione:
  - Per x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Per x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Per l'app Citrix Workspace per Windows:

- Modificare il Registro di sistema del dispositivo utente. Nel supporto di installazione è incluso un modello amministrativo (file ADM) che consente di modificare il dispositivo utente tramite Criteri di gruppo di Active Directory:
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Le regole predefinite del prodotto sono archiviate in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Non modificare queste regole predefinite del prodotto. Utilizzarle invece come guida per la creazione

di regole di override dell'amministratore, come illustrato più avanti in questo articolo. Le regole di override dell'Oggetto Criteri di gruppo vengono valutate prima delle regole predefinite del prodotto.

Le regole di override dell'amministratore sono memorizzate in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericU
Le regole dei criteri Criteri di gruppo hanno il formato **{Allow:|Deny:}** seguito da un insieme di espressioni *tag=value* separate da uno spazio bianco.

Sono supportati i seguenti tag:

| Tag | Descrizione |
|---|---|
| VID | ID fornitore del descrittore del dispositivo |
| PID | ID prodotto del descrittore del dispositivo |
| REL | ID versione del descrittore del dispositivo |
| Class | Classe del descrittore del dispositivo o di un descrittore di interfaccia; vedere il sito Web USB alla pagina http://www.usb.org/ per i codici di classe USB disponibili |
| SubClass | Sottoclasse del descrittore del dispositivo o di un descrittore di interfaccia |
| Prot | Protocollo del descrittore del dispositivo o di un descrittore di interfaccia |

Durante la creazione di regole dei criteri, tenere presente quanto segue:

- Le regole non fanno distinzione tra maiuscole e minuscole.
- Le regole possono avere un commento facoltativo alla fine, introdotto da #. Non è necessario un delimitatore e il commento viene ignorato per scopi di corrispondenza.
- Le righe di commento vuote e pure vengono ignorate.
- Lo spazio bianco viene utilizzato come separatore, ma non può essere visualizzato al centro di un numero o di un identificatore. Ad esempio, Deny: Class = 08 SubClass=05 è una regola valida, ma non Deny: Class=0 Sub Class=05.
- I tag devono utilizzare l'operatore corrispondente =. Ad esempio, VID=1230.
- Ogni regola deve iniziare su una nuova riga o far parte di un elenco separato da punto e virgola.

> **Nota:**
>
> Se si utilizza il file del modello ADM, è necessario creare regole su un'unica riga, come elenco separato da punto e virgola.

Esempi:

- Nell'esempio seguente viene illustrata una regola dei criteri USB definita dall'amministratore per gli identificatori di fornitore e prodotto:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- Nell'esempio seguente viene illustrata una regola dei criteri USB definita dall'amministratore per una classe, una sottoclasse e un protocollo definiti:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

### Utilizzare e rimuovere dispositivi USB

Gli utenti possono collegare un dispositivo USB prima o dopo l'avvio di una sessione virtuale.

Quando si utilizza l'app Citrix Workspace per Windows, si applicano le seguenti condizioni:

- I dispositivi collegati dopo l'inizio di una sessione vengono visualizzati immediatamente nel menu USB di Desktop Viewer.
- Se un dispositivo USB non viene reindirizzato correttamente, è possibile provare a risolvere il problema aspettando di connettere il dispositivo fino all'avvio della sessione virtuale.
- Per evitare la perdita di dati, utilizzare l'icona "Rimozione sicura dell'hardware"di Windows prima di rimuovere il dispositivo USB.

### Controlli di sicurezza per dispositivi di archiviazione di massa USB

Il supporto ottimizzato è fornito per i dispositivi di archiviazione di massa USB. Questo supporto fa parte della mappatura delle unità client di Citrix Virtual Apps and Desktops. Le unità sul dispositivo utente vengono mappate automaticamente alle lettere di unità sul desktop virtuale quando gli utenti accedono. Le unità vengono visualizzate come cartelle condivise con lettere di unità mappate. Per configurare il mapping delle unità client, utilizzare l'impostazione **Client removable drives (Unità client rimovibili)**. Questa impostazione si trova nella sezione Impostazioni dei criteri di reindirizzamento file delle impostazioni dei criteri ICA.

Con i dispositivi di archiviazione di massa USB, è possibile utilizzare la mappatura delle unità client oppure il reindirizzamento USB generico oppure entrambi. È possibile controllarli utilizzando i criteri Citrix. Le principali differenze sono:

| Funzionalità | Mappatura unità client | Reindirizzamento USB generico |
|---|---|---|
| Attivato per impostazione predefinita | Sì | No |
| Accesso in sola lettura configurabile | Sì | No |
| Accesso ai dispositivi crittografati | Sì, se la crittografia viene sbloccata prima dell'accesso al dispositivo | Sì |
| Dispositivi BitLocker To Go | No | No |
| Eliminazione sicura del dispositivo durante una sessione | No | Sì, a condizione che gli utenti seguano le raccomandazioni del sistema operativo per la rimozione sicura |

Se sia il reindirizzamento USB generico che i criteri di mappatura delle unità client sono abilitati e viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione, questo viene reindirizzato utilizzando la mappatura delle unità client. Se sia il reindirizzamento USB generico che i criteri di mappatura delle unità client sono abilitati e un dispositivo è configurato per il reindirizzamento automatico e viene inserito un dispositivo di archiviazione di massa prima o dopo l'avvio di una sessione, viene reindirizzato utilizzando il reindirizzamento USB generico. Per ulteriori informazioni, vedere l'articolo CTX123015 del Knowledge Center.

> **Nota:**
>
> Il reindirizzamento USB è supportato su connessioni a larghezza di banda inferiore, ad esempio 50 Kbps. Tuttavia, la copia di file di grandi dimensioni non funziona.

## Gestione

November 16, 2022

Citrix gestisce le distribuzioni dei servizi Citrix Virtual Apps and Desktops installando e mantenendo i componenti e le funzionalità principali in Citrix Cloud.

L'amministratore si occupa delle macchine (VDA) nelle posizioni delle risorse che distribuiscono app e desktop. L'amministratore gestisce le connessioni a tali posizioni di risorse, nonché le app, i desktop e gli utenti.

- **Autoscale:** soluzione coerente e ad alte prestazioni per la gestione proattiva delle macchine.
- **Applicazioni:** gestione delle applicazioni incluse nei gruppi di consegna.
- **IP virtuale e loopback virtuale:** la funzionalità di indirizzo IP virtuale di Microsoft fornisce a un'applicazione pubblicata un indirizzo IP univoco assegnato dinamicamente per ciascuna sessione. Con la funzione di loopback virtuale Citrix è possibile configurare applicazioni che dipendono dalle comunicazioni con localhost (127.0.0.1 per impostazione predefinita) per l'uso di un indirizzo di loopback virtuale univoco compreso nell'intervallo localhost (127.*).
- **Registrazione VDA:** prima che un VDA possa facilitare la distribuzione di app e desktop, deve registrarsi (stabilire una comunicazione) con un Cloud Connector. È possibile specificare gli indirizzi di Cloud Connector utilizzando diversi metodi, descritti in questo articolo. Quando si aggiungono i Cloud Connector, i VDA devono disporre di informazioni aggiornate.
- **Sessioni:** mantenere l'attività della sessione è fondamentale per fornire la migliore esperienza utente. Diverse funzionalità possono ottimizzare l'affidabilità delle sessioni, ridurre gli inconvenienti, i tempi di inattività e la perdita di produttività.
- **Utilizzo della ricerca:** per visualizzare informazioni su macchine, sessioni, cataloghi di macchine, applicazioni o gruppi di consegna nell'interfaccia di gestione della configurazione completa, utilizzare la funzione di ricerca flessibile.
- **Supporto di IPv4/IPv6:** Citrix Virtual Apps and Desktops supporta le distribuzioni IPv4 pure, IPv6 pure e dual-stack che utilizzano reti IPv4 e IPv6 sovrapposte. In questo articolo vengono descritte e illustrate queste distribuzioni. Vengono inoltre descritte le impostazioni dei criteri Citrix che controllano l'utilizzo di IPv4 o IPv6.
- **Gestione dei profili:** Citrix Profile Management può essere installato quando si installa un VDA. Se si utilizza questa soluzione per profili utente, consultare la relativa documentazione.
- **Citrix Insight Services:** Citrix Insight Services (CIS) è una piattaforma Citrix per la strumentazione, la telemetria e la generazione di informazioni aziendali. Vengono raccolte analisi e diagnostica quando si installa un VDA.
- **Local Host Cache:** Local Host Cache consente di continuare le operazioni di intermediazione delle connessioni quando un Cloud Connector che si trova nella posizione di una risorsa non può comunicare con Citrix Cloud. Vengono inoltre fornite considerazioni su scala, dimensioni e altri aspetti della configurazione .
- **Amministrazione delegata:** con l'amministrazione delegata, è possibile configurare le autorizzazioni di accesso necessarie a tutti gli amministratori, in base al loro ruolo nell'organizzazione.
- **Registrazione della configurazione:** la registrazione della configurazione tiene traccia delle modifiche apportate alla configurazione e delle attività amministrative.
- **Log degli eventi:** i servizi disponibili in Citrix Virtual Apps and Desktops registrano gli eventi

che si verificano. I log eventi possono essere utilizzati per monitorare e risolvere i problemi operativi.

- **Licenze:** è possibile visualizzare le informazioni sull'utilizzo delle licenze Citrix per questo servizio dalla console Citrix Cloud.
- **Macchine per il bilanciamento del carico:** è possibile controllare come bilanciare il carico delle macchine.

## Accesso adattivo

October 5, 2022

Nelle situazioni in continua evoluzione di oggi, la sicurezza delle applicazioni è fondamentale per qualsiasi azienda. Prendere decisioni di sicurezza sensibili al contesto e quindi abilitare l'accesso alle applicazioni riduce i rischi associati, oltre a fornire l'accesso agli utenti.

La funzionalità di accesso adattivo offre un approccio completo di accesso zero-trust che fornisce un accesso sicuro alle applicazioni. L'accesso adattivo consente agli amministratori di fornire un accesso di livello granulare alle app a cui gli utenti possono accedere in base al contesto. Il termine "contesto" si riferisce a:

- Utenti e gruppi (utenti e gruppi di utenti)
- Dispositivi (desktop o dispositivi mobili)
- Posizione (geolocalizzazione o posizione di rete)
- Postura del dispositivo (controllo della postura del dispositivo)
- Rischio (punteggio di rischio dell'utente)

## Postura del dispositivo

November 21, 2023

Il servizio Citrix Device Posture è una soluzione basata su cloud che aiuta gli amministratori a far rispettare determinati requisiti che i dispositivi finali devono soddisfare per ottenere l'accesso alle risorse Citrix DaaS (Citrix Virtual Apps and
Desktops) o Citrix Secure Private Access (app SaaS e Web o app TCP e UDP). Stabilire l'affidabilità del dispositivo controllandone la postura è fondamentale per implementare l'accesso Zero Trust. Il servizio Device Posture applica i principi Zero Trust nella rete controllando la conformità dei dispositivi terminali (gestito/BYOD e livello di sicurezza) prima di consentire a un utente finale di accedere.

Per ulteriori informazioni, vedere Postura del dispositivo.

## Servizio di autenticazione adattiva

October 5, 2022

I clienti di Citrix Cloud possono utilizzare Citrix Workspace per fornire l'autenticazione adattiva a Citrix DaaS. L'autenticazione adattiva è un servizio Citrix Cloud che consente l'autenticazione avanzata per i clienti e gli utenti che accedono a Citrix Workspace. Il servizio di autenticazione adattiva è un ADC gestito da Citrix e ospitato da Citrix Cloud che fornisce tutte le funzionalità di autenticazione avanzate come le seguenti:

- Autenticazione a più fattori utilizzando diversi metodi di autenticazione come AD, RADIUS, certificato, più IdP di terze parti che utilizzano SAML 2.0, OAuth, OIDC, Google Captcha.
- Verifica l'identità dell'utente e dei livelli di autorizzazione in base a fattori quali posizione, stato del dispositivo e gruppo di utenti.
- Abilita l'accesso contestuale o intelligente a DaaS (virtualizzato) e SPA (risorse non virtualizzate come app Web e SaaS).
- Personalizzazione della pagina di accesso

Per i dettagli completi sull'autenticazione adattiva, consultare Servizio di autenticazione adattiva.

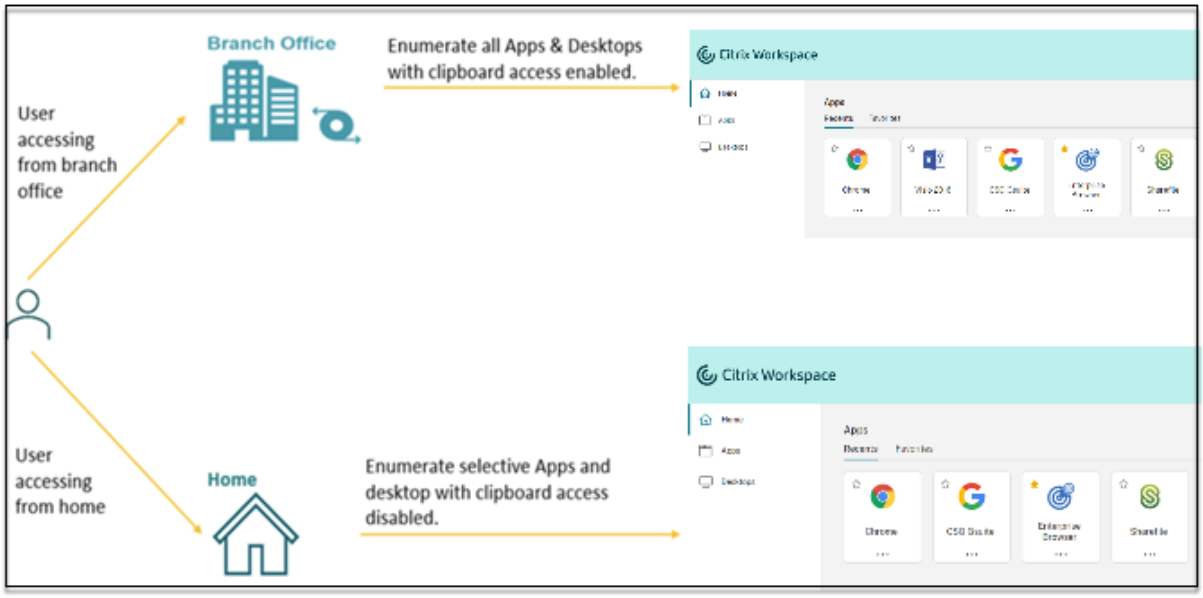
## Accesso adattivo basato sulla posizione di rete dell'utente

November 21, 2023

La funzione Adaptive Access (Accesso adattivo) di Citrix Workspace utilizza un'infrastruttura di criteri avanzata per consentire l'accesso a Citrix DaaS in base alla posizione di rete dell'utente. La posizione viene definita utilizzando l'intervallo di indirizzi IP o gli indirizzi di sottorete.

Gli amministratori possono definire criteri per enumerare o non enumerare i desktop e le app virtuali in base alla posizione di rete dell'utente. Gli amministratori possono anche controllare le azioni degli utenti abilitando o disabilitando l'accesso agli appunti, alle stampanti, alla mappatura delle unità client e così via, in base alla posizione di rete dell'utente. Ad esempio, gli amministratori possono impostare criteri per cui gli utenti che accedono alle risorse da casa abbiano un accesso limitato alle applicazioni e gli utenti che accedono alle risorse dalle filiali abbiano l'accesso completo.




Un amministratore può implementare i seguenti criteri per l'accesso alle applicazioni:

- Enumerare alcune applicazioni sensibili accessibili solo dalla sede aziendale o dalle filiali.
- Non enumerare le applicazioni riservate se i dipendenti accedono all'area di lavoro da una rete esterna.
- Disabilitare l'accesso alla stampante dalle filiali.
- Disabilitare l'accesso agli appunti e alla stampante quando gli utenti sono al di fuori della rete aziendale.

## Diritti

La funzionalità Adaptive Access è disponibile per i clienti con le seguenti licenze.

- Distribuzione Citrix DaaS con accesso tramite la piattaforma Citrix Workspace
- DaaS Premium/Premium Plus
- Accesso privato sicuro avanzato

## Prerequisiti

- Assicurarsi che la funzione **Adaptive Access** (Accesso adattivo) sia abilitata (**Citrix Workspace > Access > Adaptive Access**). Per informazioni dettagliate, vedere Abilitare la funzionalità Adaptive Access.

  Quando l'accesso adattivo è abilitato, i criteri di accesso di DaaS vengono aggiornati in modo che utilizzi l'opzione **Connections through Citrix Gateway** (Connessioni tramite Citrix Gateway).

> **Nota:**
>
> NetScaler Gateway è necessario per aggiungere le tag Smart Access ai criteri di accesso DaaS. Tuttavia, poiché DaaS utilizza i tag dei servizi Device Posture, Adaptive Access e Adaptive Authentication, non è necessario avere un NetScaler Gateway configurato nella configurazione.

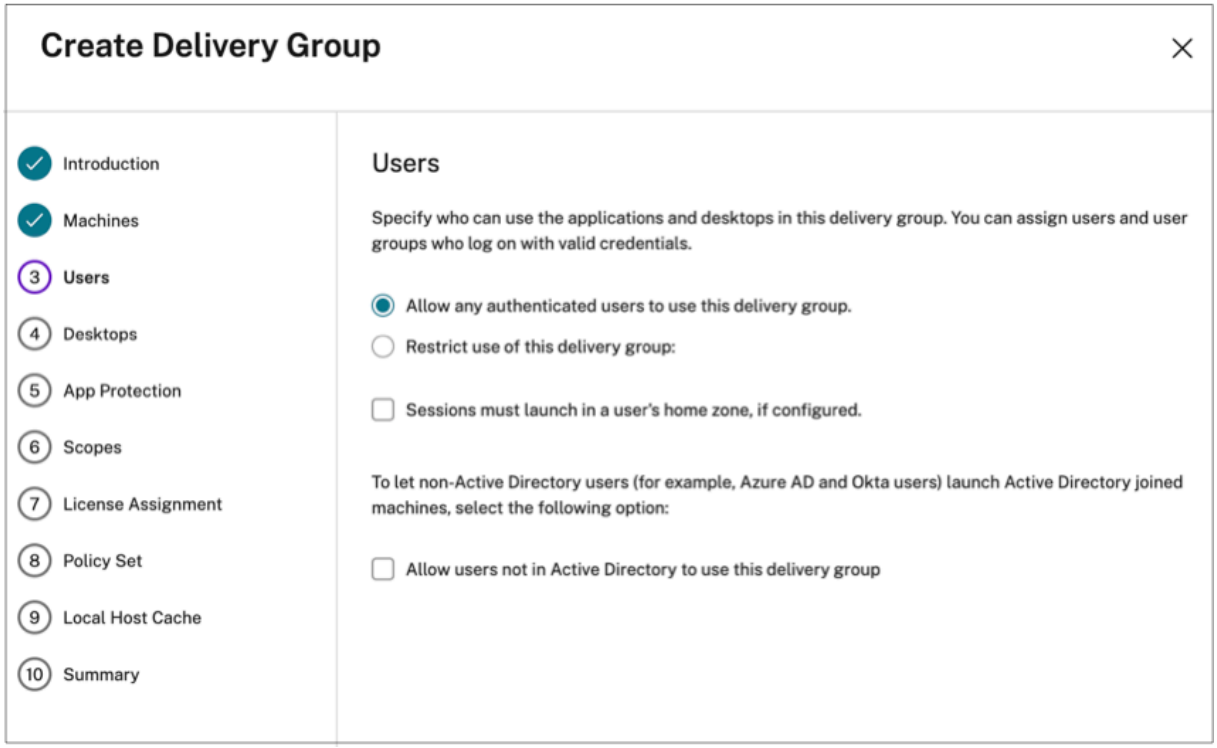
- Comprendere i tag di posizione. Per informazioni dettagliate, vedere Tag di posizione della rete.

### Punti da notare

I seguenti punti sono applicabili solo se si desidera limitare l'enumerazione delle applicazioni in base alla posizione. Se si prevede di utilizzare l'accesso adattivo per limitare controlli utente come la disattivazione dell'accesso agli appunti, il reindirizzamento della stampante, la mappatura delle unità client in base alla posizione della rete, è possibile ignorare queste linee guida.

- Durante la creazione di un gruppo di consegna, se si seleziona l'opzione **Leave user management to Citrix Cloud** (Lasciare la gestione degli utenti a Citrix Cloud), non è possibile applicare i criteri Smart Access (ad esempio, l'accesso adattivo a Citrix DaaS in base alla posizione di rete). Questo perché i gruppi di consegna diventano librerie e quindi non vengono più gestiti da Web Studio.
- Se si prevede di enumerare in modo selettivo Citrix DaaS in base al percorso di rete, la gestione degli utenti deve essere eseguita per quei gruppi di consegna utilizzando i criteri di Citrix Studio anziché Workspace. Quando si crea un gruppo di consegna, in **User setting** (Impostazione utente), scegliere **Restrict use of this Delivery Group** (Limita l'uso di questo gruppo di consegna) o **Allow any authenticated users to use this Delivery Group** (Consenti a qualsiasi utente autenticato di utilizzare questo gruppo di consegna). In questo modo si configura l'accesso adattivo alla scheda **Access Policy** (Criteri di accesso) in **Delivery Group** (Gruppo di consegna).

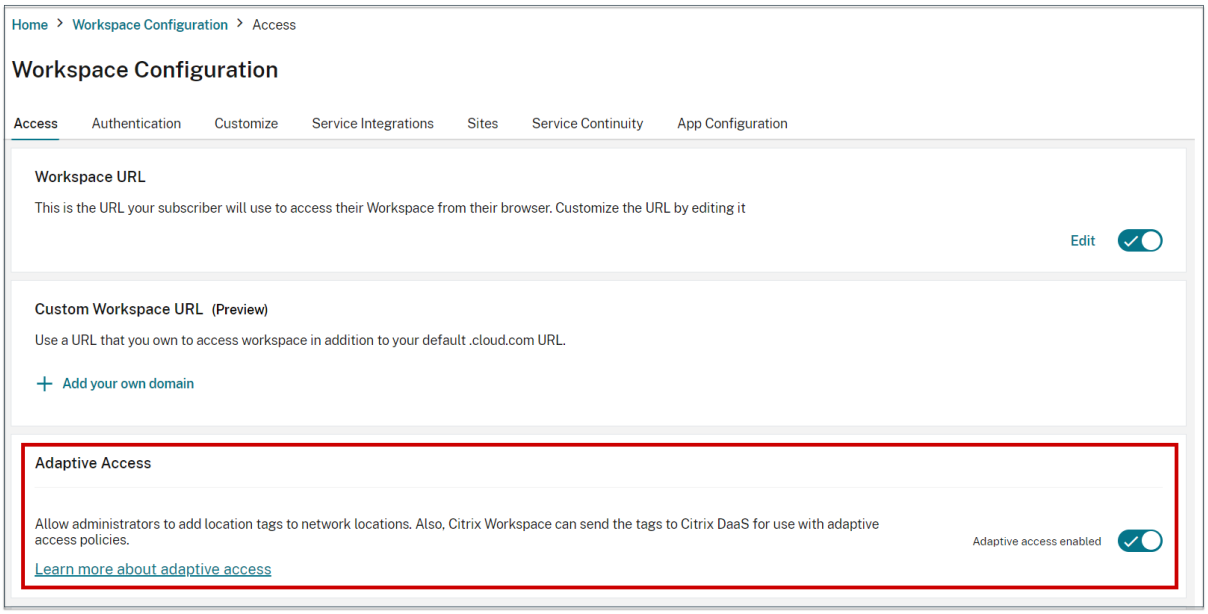


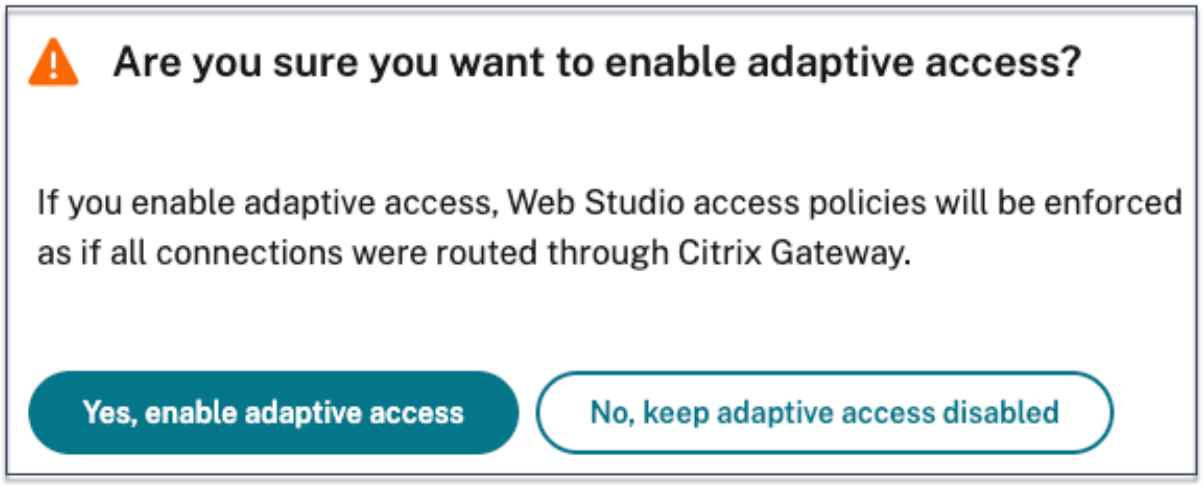

- Diventa Direct Workload Connection (Connessione diretta al carico di lavoro) quando l'accesso adattivo è abilitato.
  - Il campo **Location tags** (Tag di posizione) è visibile in **Citrix Cloud > Network Locations > Add a Network Location > Location tags** (Citrix Cloud > Posizioni di rete > Aggiungi una posizione di rete > Tag di posizione).
  - I criteri esistenti di Direct Workload Connection funzionano come previsto.
  - È necessario creare nuovi criteri nel servizio Network Locations (senza definire i tag) e anche nel gruppo di consegna. Inoltre, il tipo di connettività di rete deve essere **Internal**.
  - Per i nuovi criteri relativi a Direct Workload Connection con tag, i tag devono essere definiti nel servizio Network Locations e gli stessi tag devono essere definiti anche nel gruppo di consegna o nei criteri di accesso in DaaS Studio. Inoltre, il tipo di connettività di rete deve essere **Internal**. I tag di posizione non sono pertinenti per Direct Workload Connection.
- Quanto segue è consigliato per mettere alla prova la distribuzione Citrix DaaS.
  - Identificare un gruppo di consegna di prova o creare un gruppo di consegna per implementare questa funzionalità.
  - Creare un criterio o identificare un criterio che può essere utilizzato con un gruppo di consegna di prova.

### Abilitare la funzione Adaptive Access

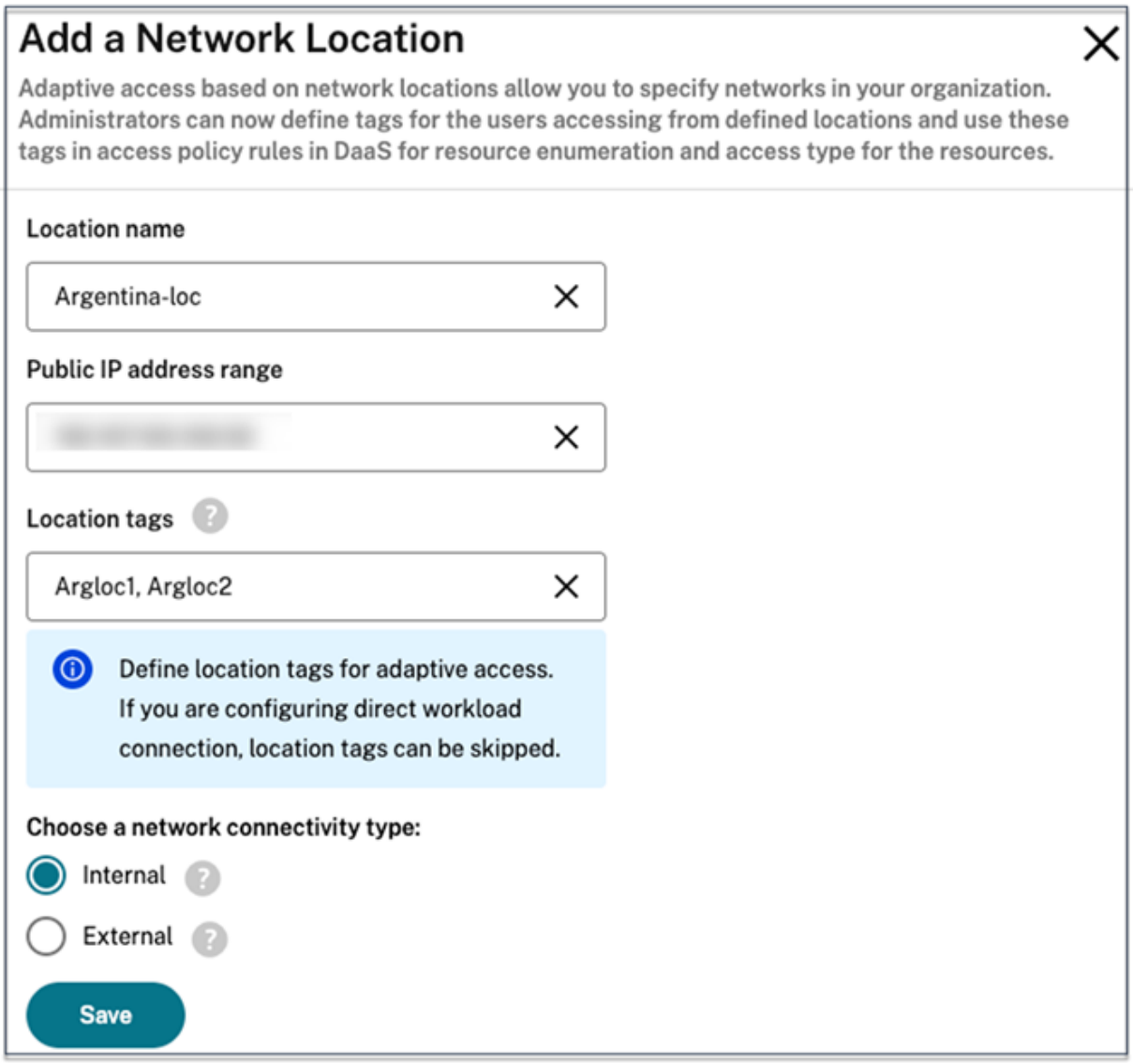
1. Accedere a Citrix Cloud.
2. Selezionare **Workspace Configuration** dal menu a forma di hamburger.
3. L'opzione **Adaptive Access** è disattivata per impostazione predefinita. Attivare l'opzione **Adaptive Access**.
4. Fare clic su **Yes, enable adaptive access** (Sì, abilita l'accesso adattivo) nel messaggio di conferma.



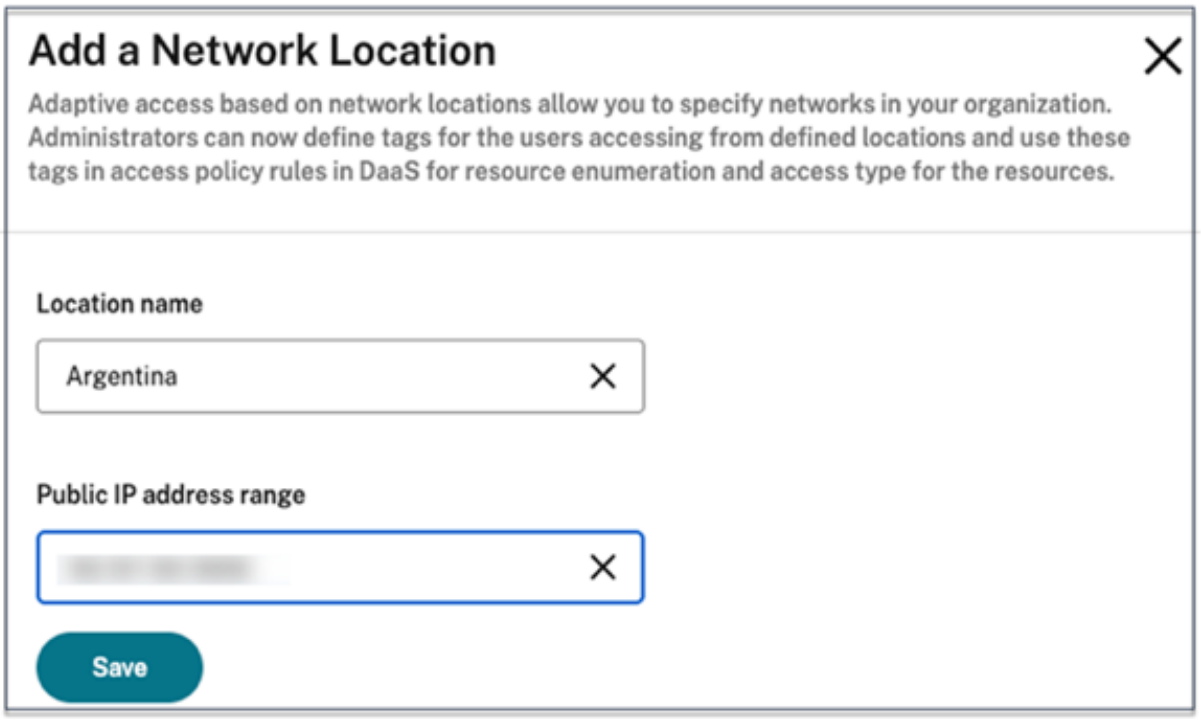

Quando l'accesso adattivo è abilitato, è possibile definire i tag di posizione per l'accesso adattivo (**Citrix Cloud > Network Locations > Add a Network Location > Location tags** [Citrix Cloud > Posizioni di rete > Aggiungi una posizione di rete > Tag di posizione]).



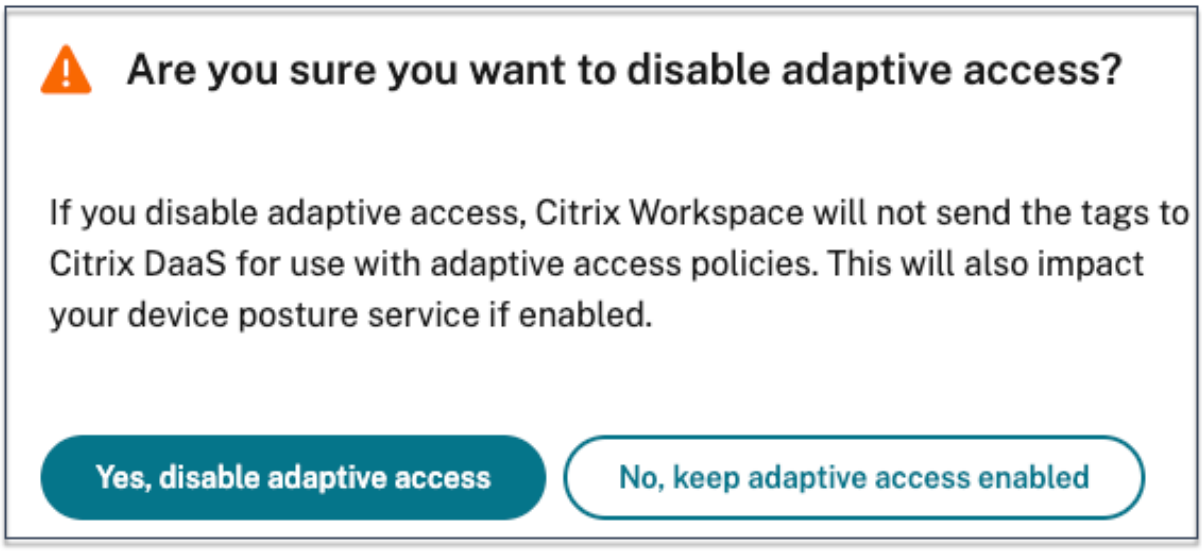

Quando Adaptive Access è disabilitato, non è possibile aggiungere una posizione di rete. I tag di posizione non sono applicabili in questo caso.




**Importante:**

Quando si tenta di disattivare la funzionalità Adaptive Access, viene visualizzato il seguente messaggio. Notare che Workspace non invia i tag al DaaS per l'accesso adattivo quando la funzionalità è disabilitata.



## Configurare l'accesso adattivo

Per configurare l'accesso adattivo in base alle posizioni di rete, sono necessari i seguenti passaggi di alto livello.

1. Definire i criteri di posizione della rete
2. Definire i tag in DaaS Studio

Come esempi di configurazione, vengono selezionati due tipi di utenti (utenti di **BrancOffice** [Filiale] e utenti **WorkFromHome** [LavoratoriDaCasa]) per ottenere il seguente caso d'uso.

- Gli utenti di BranchOffice devono poter accedere alle applicazioni con tutti gli accessi.
- Gli utenti WorkFromHome non devono avere accesso agli appunti.

In questo esempio di configurazione, **Home** e **Office** vengono utilizzati come tag negli esempi.

### Configurazione dei criteri di posizione della rete

1. Accedere a Citrix Cloud.
2. Selezionare **Network Locations** (Posizioni di rete) dal menu a forma di hamburger.
   Assicurarsi che Adaptive Access sia abilitato. Altrimenti viene visualizzata l'interfaccia utente di Direct Workload Connection.
3. Fare clic su **Add network location** (Aggiungi posizione di rete).

   - **Location name** (Nome posizione): immettere un nome appropriato per il criterio.

     Esempio: BranchOffice o WorkFromHome

   - **Public IP address range** (Intervallo di indirizzi IP pubblici): definire qui l'intervallo di indirizzi IP pubblici della rete.

     Esempio: 172.9.2.1-172.9.2.30

   - **Location Tags** (Tag di posizione): definire qui i tag della propria posizione. Questo può essere un nome che si riferisce alla propria posizione. Questi tag vengono utilizzati per configurare i criteri di accesso adattivi in Citrix Studio. Per i dettagli, vedere **Definire i tag in Citrix Studio**.

     Esempio: *Office* o *Home*

   - **Connectivity type** (Tipo di connettività): definisce il tipo di avvio dell'applicazione.

   **Internal**: ignorare il gateway per l'avvio dell'applicazione.
   **External**: utilizzare il servizio Citrix Gateway o il gateway tradizionale per l'avvio dell'applicazione.

4. Fare clic su **Salva**.

Ora è possibile utilizzare questi tag su DaaS Studio per abilitare l'accesso adattivo.

#### Definire i tag in Citrix Studio

In questo esempio, nei gruppi di consegna vengono definiti tag per limitare l'enumerazione delle applicazioni per gli utenti. Vengono creati due gruppi di consegna.

- Gruppo di consegna Adaptive Access per gli utenti dalla sede **BranchOffice**. Questi utenti devono visualizzare tutte le applicazioni disponibili in questo gruppo di consegna.
- Grupo di consegna WFH: per gli utenti dalla posizione **WorkFromHome**. Questi utenti devono visualizzare le applicazioni disponibili in questo gruppo di consegna.

1. Accedere a Citrix Cloud.
2. Nel riquadro **Citrix DaaS**, fare clic su **Manage** (Gestisci).
3. Creare un gruppo di consegna. Per ulteriori informazioni, vedere Creare gruppi di consegna.
4. Selezionare il gruppo di consegna creato e fare clic su **Edit Delivery Group** (Modifica gruppo di consegna).
5. Fare clic su **Access Policy** (Criteri d'accesso).
6. Fare clic su **Add** (Aggiungi) e selezionare quanto segue:

   - Farm: **Workspace**
   - Filtro: **LOCATION_TAG_OFFICE**

   Allo stesso modo, è possibile creare un tag per il gruppo di consegna WFH.
7. Fare clic su **Add** (Aggiungi) e selezionare quanto segue:

   - Farm: Workspace
   - Filtro: **LOCATION_TAG_HOME**

Ora è possibile usare questi tag per limitare l'accesso alle applicazioni.

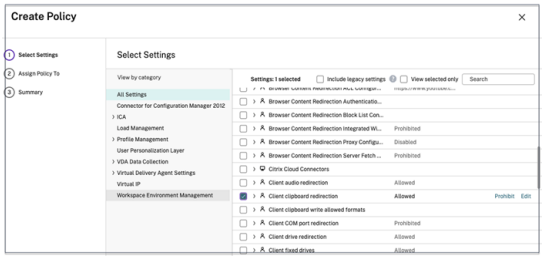
#### Limitare l'accesso alle applicazioni

In questo esempio, il reindirizzamento degli appunti del client è disabilitato per gli utenti della posizione WorkFromHome.

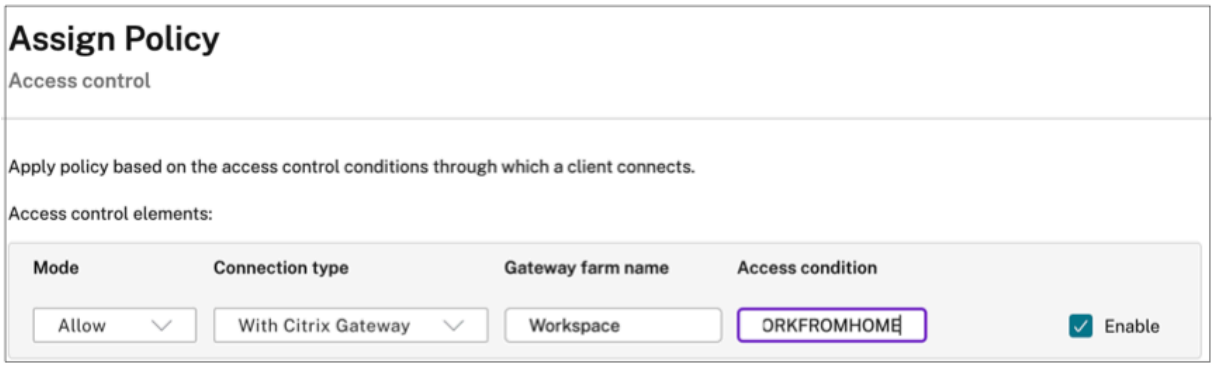
1. Accedere a Citrix DaaS.
2. Pssare a **Policies** (Criteri) e fare clic su **Create Policy** (Crea criterio).

3. Selezionare **Client clipboard redirection** (Reindirizzamento degli appunti del client), quindi fare clic su **Prohibit** (Proibisci).
4. Fare clic su **Next** (Avanti).




1. In Assign policy to page (Assegna criterio alla pagina), selezionare **Access control** (Controllo dell'accesso).
2. Definire i seguenti valori per il criterio:
   - Modalità: **Allow** (Consenti)
   - Tipo di connessione: **With Citrix Gateway**
   - Nome della farm gateway: **Workspace**
   - Condizione di accesso: **LOCATION_TAG_HOME** (tutto in maiuscolo)




1. Fare clic su **Next** (Avanti).
2. Inserire un nome e una descrizione del criterio.
3. Fare clic su **Finish**.

Gli utenti che accedono dalla posizione **WorkFromHome** non possono accedere agli Appunti delle risorse avviate.

### Tag della posizione di rete

Il servizio Network Locations fornisce i seguenti tag.

- **Default tags:** questi tag sono definiti nel servizio Network Locations. Sono disponibili i seguenti tag predefiniti.

  - **Location_internal:** tag inviato per impostazione predefinita quando il tipo di connettività di rete è impostato su **INTERNAL**.
  - **Location_external:** tag inviato per impostazione predefinita quando il tipo di connettività di rete è impostato su **EXTERNAL**.
  - **Location_undefined:** tag inviato per un indirizzo IP non definito nel criterio ma proveniente dal servizio Network Locations. L'avvio per questi utenti è quello che è stato definito nel gruppo di risorse.

- **Custom tags:** gli amministratori possono definire nomi di tag personalizzati nei criteri. Esempio: ufficio, casa, filiale

**Esempi:**

Tag predefiniti: LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

Tag personalizzati: LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

> **Nota:**
>
> quando si definiscono i tag per il servizio Network Location, verificare le seguenti condizioni:
>
> - I tag predefiniti iniziano sempre con il prefisso "LOCATION_<tag name>. Ad esempio LOCATION_INTERNAL.
> - I tag personalizzati iniziano sempre con il prefisso "LOCATION_TAG<tag name>. Ad esempio LOCATION_TAG_OFFICE.

### Problemi noti

Se si disattiva la funzionalità Adaptive Access dopo che è stata abilitata e sono state impostate le regole (tag e tipo di connettività), non vengono rimosse le posizioni dalla pagina Network Locations (Posizioni di rete) sebbene i tag di posizione e le colonne del tipo di connettività siano nascosti. Ma queste posizioni sono disabilitate nel back-end. Si tratta di un problema estetico.

## Pacchetti di app

July 6, 2023

Microsoft offre tre tecnologie di packaging per fornire applicazioni agli utenti: App-V, MSIX e MSIX App Attach. Questo articolo illustra come distribuire e distribuire questi pacchetti di applicazioni nel proprio ambiente Citrix DaaS:

- Distribuire e rendere disponibili applicazioni App-V
- Implementare e distribuire applicazioni MSIX e MSIX App Attach

## Distribuire e rendere disponibili applicazioni App-V

Questa sezione contiene le seguenti informazioni:

- Overview. Descrive i metodi di gestione utilizzati da Citrix DaaS per fornire e gestire i pacchetti App-V.
- Procedures. Offre procedure per la distribuzione e la distribuzione di questi pacchetti.

### Panoramica

Questa sezione descrive i metodi di gestione utilizzati da Citrix DaaS per fornire e gestire i pacchetti App-V. Per ulteriori informazioni sui componenti e sui concetti con cui si interagisce durante la distribuzione di applicazioni in pacchetto App-V, vedere la documentazione Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Citrix DaaS fornisce e gestisce pacchetti App-V utilizzando i seguenti metodi:

- **Dual Admin** (Amministrazione doppia). I pacchetti di applicazioni sono configurati e gestiti sui server App-V. I server Citrix DaaS e App-V lavorano insieme per fornire e gestire pacchetti.

  Questo metodo richiede che Citrix DaaS aggiorni periodicamente la vista snapshot dello stato del server App-V. Ciò comporta costi in termini di hardware, infrastruttura e amministrazione. I server Citrix DaaS e App-V devono rimanere sincronizzati, in particolare per quanto riguarda le autorizzazioni degli utenti.

  Dual Admin funziona meglio nelle distribuzioni in cui App-V e Citrix Cloud sono strettamente associati:

  - **Server di gestione App-V**. Pubblica e gestisce il ciclo di vita dei pacchetti App-V e dei file di configurazione dinamici.
  - **Componente Citrix Personalization** installato su macchine VDA. Gestire la registrazione del server di pubblicazione App-V appropriato richiesto per gli avvii delle applicazioni.

  Questo metodo garantisce che il server di pubblicazione App-V sia sincronizzato per l'utente al momento appropriato. Il server di pubblicazione conserva altri aspetti del ciclo di vita del pacchetto, come l'aggiornamento all'accesso e i gruppi di connessione.

- **Single Admin** (Amministrazione singola). I pacchetti di applicazioni sono archiviati nelle condivisioni di rete. Citrix DaaS fornisce e gestisce i pacchetti in modo indipendente.

  Questo metodo riduce il sovraccarico perché i server App-V e l'infrastruttura di database non sono necessari nella distribuzione.

  In questo metodo, i pacchetti App-V vengono archiviati su una condivisione di rete e i relativi metadati vengono caricati da quella posizione su Citrix Cloud. Quindi il componente Citrix Personalization installato su macchine VDA gestisce e fornisce le applicazioni come segue:

- Elaborare i file di configurazione della distribuzione e i file di configurazione utente all'avvio di un'applicazione.
- Gestire tutti gli aspetti dei cicli di vita dei pacchetti sulla macchina host.

È possibile utilizzare entrambi i metodi di gestione contemporaneamente. In altre parole, quando si aggiungono applicazioni ai gruppi di consegna, le applicazioni possono provenire da pacchetti App-V situati su server App-V o su condivisioni di rete.

> **Nota:**
>
> Se si utilizzano entrambi i metodi di gestione contemporaneamente e il pacchetto App-V dispone di un file di configurazione dinamico in entrambe le posizioni, viene utilizzato il file che si trova nel server App-V (Dual Admin).

#### Procedure

Per supportare la distribuzione di applicazioni App-V, è necessario installare il componente Citrix Personalization su macchine VDA. Vedere Installare il componente Citrix Personalization su macchine VDA per i dettagli.

Per distribuire applicazioni in pacchetto App-V ai propri utenti, effettuare le seguenti operazioni:

1. Archiviare i pacchetti di applicazioni su condivisioni di rete.
2. Caricare i pacchetti di applicazioni in Citrix Cloud.
3. Aggiungere le applicazioni ai gruppi di consegna.
4. Per abilitare la consegna automatica di pacchetti App-V interdipendenti, creare gruppi di isolamento.

Per fare in modo che Citrix DaaS riconosca e applichi i file di configurazione dinamica di App-V nel metodo Single Admin, vedere questo blog di Citrix.

### Implementare e distribuire applicazioni MSIX e MSIX App Attach

Questa sezione contiene le seguenti informazioni:

- Panoramica. Descrive come Citrix DaaS fornisce e gestisce i pacchetti MSIX e MSIX App Attach.
- Procedure. Offre procedure per la distribuzione e la distribuzione di questi pacchetti.

#### Panoramica

Citrix DaaS offre applicazioni MSIX e MSIX App Attach agli utenti tramite il componente Citrix Personalization installato su macchine VDA. Questo componente gestisce tutti gli aspetti dei cicli di vita dei pacchetti sulla macchina host.

Per ulteriori informazioni su MSIX e MSIX App Attach, vedere la documentazione Microsoft: rispettivamente https://docs.microsoft.com/en-us/windows/msix/ e https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach.

#### Procedure

Per supportare la distribuzione di pacchetti MSIX e MSIX App Attach, è necessario installare il componente Citrix Personalization su macchine VDA. Vedere Installare il componente Citrix Personalization su macchine VDA per i dettagli.

Per distribuire applicazioni in pacchetto MSIX e MSIX App Attach ai propri utenti, effettuare le seguenti operazioni:

1. Archiviare i pacchetti di applicazioni su condivisioni di rete.
2. Caricare i pacchetti di applicazioni in Citrix Cloud.
3. Aggiungere le applicazioni ai gruppi di consegna.

### Installare il componente Citrix Personalization su macchine VDA

Il componente Citrix Personalization gestisce il processo di pubblicazione dei pacchetti di applicazioni nei formati App-V, MSIX e MSIX App Attach. Questo componente non viene installato per impostazione predefinita quando si installa un VDA. È possibile installare il componente durante o dopo l'installazione del VDA.

Per installarlo durante l'installazione del VDA, utilizzare uno dei seguenti metodi:

- Nella procedura guidata di installazione, andare alla pagina **Additional Components** (Componenti aggiuntivi), quindi selezionare la casella di controllo **Citrix Personalization for App-V - VDA** (Personalizzazione Citrix per App-V - VDA).
- Nell'interfaccia della riga di comando, utilizzare l'opzione **/includeadditional "Citrix Personalization for App-V –VDA"**.

Per installare il componente dopo l'installazione del VDA, effettuare le seguenti operazioni:

1. Sulla macchina VDA, accedere a **Pannello di controllo > Programmi > Programmi e funzionalità**, fare clic con il pulsante destro del mouse su **Citrix Virtual Delivery Agent**, quindi selezionare **Modifica**.
2. Nella procedura guidata visualizzata, passare alla pagina **Additional Components** (Componenti aggiuntivi) e quindi abilitare la casella di controllo **Citrix Personalization for App-V - VDA** (Personalizzazione Citrix per App-V - VDA).

> **Nota:**
>
> Il client desktop Microsoft App-V è il componente che esegue applicazioni virtuali dai pacchetti App-V sui dispositivi degli utenti. Windows 10 (1607 o versioni successive), Windows Server 2016 e Windows Server 2019 includono già questo software client App-V. È necessario abilitarlo solo su macchine VDA. Per ulteriori informazioni, consultare questo articolo della documentazione Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

### Archiviare pacchetti di applicazioni su condivisioni di rete

Dopo aver configurato l'infrastruttura, generare i pacchetti di applicazioni e archiviarli in un percorso di rete, ad esempio una condivisione di rete UNC o SMB oppure in una condivisione file di Azure.

I passaggi dettagliati sono i seguenti:

1. Generare pacchetti di applicazioni. Per ulteriori informazioni, vedere la documentazione Microsoft.
2. Archiviare i pacchetti di applicazioni in un percorso di rete:
    - Per **App-V Single Admin**: archiviare i pacchetti e i corrispondenti file di configurazione dinamica (App-V) in una condivisione di rete UNC o SMB o in una condivisione file di Azure.
    - Per **App-V Dual Admin**: pubblicare i pacchetti sul server di gestione App-V da un percorso UNC (la pubblicazione da URL HTTP non è supportata).
    - Per **MSIX e MSIX App Attach**: archiviare i pacchetti su una condivisione di rete UNC o SMB oppure su una condivisione di file di Azure.
3. Verificare che il VDA disponga dell'autorizzazione di lettura sul percorso di archiviazione del pacchetto:
    - Se si archiviano pacchetti in una condivisione di rete UNC o SMB nel dominio AD, concedere alla macchina VDA l'autorizzazione di lettura per il percorso di archiviazione. A tale scopo, è possibile concedere esplicitamente all'account AD della macchina l'autorizzazione di lettura per la condivisione o includere l'account in un gruppo AD che dispone di tale autorizzazione.
    - Se si archiviano pacchetti in una condivisione file di Azure, concedere innanzitutto l'autorizzazione di lettura a un account utente per il percorso di archiviazione in Azure. Quindi, configurare `ctxAppVService` in esecuzione sulla macchina VDA in modo che utilizzi quell'account utente per accedere al percorso di archiviazione del pacchetto. Consultare la sezione seguente per i passaggi dettagliati.

#### Modificare l'account di accesso dell'utente

Il VDA chiama `ctxAppVService` per accedere ai percorsi di archiviazione dei pacchetti. Per impostazione predefinita, `ctxAppVService` accede ai percorsi di archiviazione dei pacchetti utilizzando l'**account di sistema locale** della macchina. Questo tipo di autenticazione macchina funziona nei domini AD. Tuttavia, non funziona negli scenari di integrazione di AD e Azure AD, che richiedono l'autenticazione basata sull'account utente.

Se si archiviano pacchetti in una condivisione file di Azure, modificare l'account di accesso per `ctxAppVService` in un account utente che dispone dell'autorizzazione di lettura per il percorso di archiviazione del pacchetto. I passaggi dettagliati sono i seguenti:

1. Avviare **Services** (Servizi), fare clic con il pulsante destro del mouse su **ctxAppVService** e quindi selezionare **Properties** (Proprietà).
2. Nella scheda **Log on** (Accesso), selezionare **This account** (Questo account), immettere un account utente che dispone dell'autorizzazione di lettura per il percorso di archiviazione del pacchetto e quindi immettere due volte la password dell'utente.
3. Fare clic su **OK**.

### Caricare pacchetti di applicazioni in Citrix Cloud

Dopo aver archiviato i pacchetti di applicazioni in una posizione di rete secondo necessità, caricarli su Citrix Cloud per la consegna. Se necessario, utilizzare uno dei seguenti metodi:

- Caricamento in blocco
- Caricamento uno ad uno

#### Preparativi

Citrix DaaS utilizza una macchina VDA per configurare la connessione al percorso di rete per il rilevamento dei pacchetti. Pertanto, creare preventivamente un gruppo di consegna e accertarsi che almeno un VDA nel gruppo soddisfi i seguenti requisiti:

- Versione VDA:
  - Per scoprire i pacchetti App-V: 2203 o versioni successive
  - Per scoprire i pacchetti MSIX e MSIX App Attach: 2209 o versioni successive
- Personalizzazione Citrix per i componenti App-V: installata
- Autorizzazione sulla posizione del pacchetto: Lettura (vedere Passaggio 2: archiviare i pacchetti di applicazioni su condivisioni di rete per i dettagli).
- Alimentazione: attivata
- Stato: registrato

### Ruoli richiesti

Per impostazione predefinita, se si dispone del ruolo Cloud Administrator (Amministratore cloud) o Full Administrator (Amministratore completo), è possibile caricare pacchetti di applicazioni su Citrix Cloud. È inoltre possibile creare ruoli personalizzati per eseguire le azioni di caricamento. Nella tabella seguente sono elencate le autorizzazioni richieste dalle azioni dei pacchetti di app.

| Azione | Autorizzazione richiesta |
|---|---|
| Add package (upload one by one) (Aggiungi pacchetto [carica uno ad uno]) | Create Application Discovery Sessions (Crea sessioni di individuazione delle applicazioni) |
| Add source (upload in bulk) (Aggiungi origine [caricamento in blocco]) | Create Application Discovery Profiles (Crea profili di individuazione delle applicazioni) |
| Check for package updates (Verifica la disponibilità di aggiornamenti dei pacchetti) | Create Application Discovery Sessions (Crea sessioni di individuazione delle applicazioni) |
| Remove source (Rimuovi origine) | Remove Application Discovery Profiles (Rimuovi profili di individuazione delle applicazioni) |

### Caricare pacchetti di applicazioni in blocco

Caricare i pacchetti in un percorso di rete su Citrix Cloud. Assicurarsi di avere a portata di mano i seguenti elementi prima del caricamento:

- Un gruppo di consegna che soddisfa i requisiti di Preparation (Preparazione)
- Il percorso della posizione di rete

Per caricare i pacchetti in blocco, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **App Packages** (Pacchetti di app) nel riquadro di sinistra.
2. Nella scheda **Sources** (Origini), fare clic sul pulsante **Add Source** (Aggiungi origine). Viene visualizzata la pagina **Add Source** (Aggiungi origine).
3. Nel campo **Name** (Nome), immettere un nome descrittivo per l'origine del pacchetto.
4. Nel campo **Delivery group** (Gruppo di consegna), fare clic su **Select a delivery group** (Seleziona un gruppo di consegna). Quindi, selezionare un gruppo di consegna che soddisfi i requisiti indicati in Preparation (Preparazione) e fare clic su **OK**.
5. Nel campo **Location type** (Tipo di posizione), selezionare il **server Microsoft App-V** o la **condivisione di rete** in base alla posizione in cui vengono archiviati i pacchetti, quindi completare le impostazioni corrispondenti:

- Se si seleziona il **server Microsoft App-V**, immettere le seguenti informazioni:
  - URL del server di gestione. Esempio: `http://appv-server.example.com`
  - Credenziali di accesso dell'amministratore del server di gestione.
  - URL e numero di porta del server di pubblicazione. Esempio: `http://appv-server.example.com:3330`
- Se è stato selezionata l'opzione **Network share** (Condivisione di rete), specificare le seguenti informazioni:
  - Immettere il percorso UNC della condivisione di rete. Esempio: `\\Package-Server\apps\`
  - Selezionare i tipi di pacchetti che si desidera caricare. Le opzioni includono App-V, MSIX e MSIX App Attach.
  - Specificare se cercare i pacchetti nelle sottocartelle.

6. Fare clic su **Add Source** (Aggiungi origine).

   La pagina Add Source (Aggiungi origine) si chiude e la nuova origine aggiunta viene visualizzata nell'elenco delle origini. Citrix DaaS carica i pacchetti su Citrix Cloud utilizzando un VDA nel gruppo di consegna. Al termine del caricamento, il campo Status (Stato) mostra *Import successful* (Importazione riuscita). I pacchetti corrispondenti vengono visualizzati nella scheda **Packages** (Pacchetti).

   > **Nota:**
   >
   > Per verificare la presenza di aggiornamenti dei pacchetti in una posizione di origine e importarli in Citrix Cloud, selezionare la posizione nell'elenco delle origini e fare clic su **Check for Package Updates** (Verifica aggiornamenti del pacchetto).

#### Caricare i pacchetti di applicazioni uno ad uno

Caricare un pacchetto di applicazioni da una condivisione di rete su Citrix Cloud. Prima del caricamento, assicurarsi di avere a portata di mano i seguenti elementi:

- Un gruppo di consegna che soddisfa i requisiti indicati in Preparation (Preparazione)
- Il percorso della posizione di rete

Per caricare un pacchetto su Citrix Cloud, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **App Packages** (Pacchetti di app) nel riquadro di sinistra.
2. Nella scheda **Packages** (Pacchetti), fare clic sul pulsante **Add Package** (Aggiungi pacchetto). Viene visualizzata la pagina **Add Package** (Aggiungi pacchetto).

3. Nel campo **Delivery group** (Gruppo di consegna), fare clic su **Select a delivery group** (Seleziona un gruppo di consegna). Quindi, selezionare un gruppo di consegna che soddisfi i requisiti indicati in Preparation (Preparazione) e fare clic su **OK**.
4. Nel campo **Package full path** (Percorso completo del pacchetto), immettere un percorso secondo necessità:
   - Per caricare più pacchetti contemporaneamente, inserirne i percorsi completi, separati da punto e virgola (;). Esempio: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Per caricare tutti i pacchetti presenti in una condivisione di rete, immettere il percorso di archiviazione. Esempio: \package-Server\apps\
5. Fare clic su **Add Package** (Aggiungi pacchetto).

   Il pacchetto dell'applicazione viene visualizzato nella scheda **Packages** (Pacchetti).

### Aggiungere le applicazioni ai gruppi di consegna

Dopo il caricamento completo di un pacchetto di applicazioni, aggiungere le relative applicazioni a uno o più gruppi di consegna in base alle esigenze. Di conseguenza, gli utenti associati a tali gruppi di consegna possono accedere alle applicazioni.

> **Nota:**
>
> Le applicazioni in pacchetto possono essere assegnate solo a gruppi di consegna di tipo *Applicazioni* o *Desktop e Applicazioni*.

Per aggiungere una o più applicazioni in un pacchetto a diversi gruppi di consegna, effettuare le seguenti operazioni:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **App Packages** (Pacchetti di app) nel riquadro di sinistra.
2. Nella scheda **Packages** (Pacchetti), selezionare un pacchetto secondo necessità.
3. Nella barra delle azioni, fare clic su **Add Delivery Groups** (Aggiungi gruppi di consegna). Viene visualizzata la pagina Add Delivery Groups (Aggiungi gruppi di consegna).
4. Selezionare una o più applicazioni nel pacchetto in base alle esigenze, quindi fare clic su **Next** (Avanti). Vengono visualizzati i gruppi di consegna del tipo *Applicazioni* o *Desktop e Applicazioni*.
5. Nell'elenco dei gruppi di consegna, selezionare i gruppi a cui si desidera assegnare le applicazioni e quindi fare clic su **Next** (Avanti).
   **Nota:** se è stato selezionato un pacchetto MSIX o MSIX App Attach, nell'elenco vengono visualizzati solo i gruppi di consegna il cui livello funzionale è 2106 o successivo.

6. Fare clic su **Finish**.

È inoltre possibile aggiungere applicazioni pacchettizzate a un gruppo di consegna quando:

- Si crea un gruppo di consegna. Per ulteriori informazioni, vedere Creare gruppi di consegna.
- Si modificano dei gruppi di consegna o dei gruppi di applicazioni esistenti. Per ulteriori informazioni, consultare Aggiungere applicazioni.

### (Facoltativo) Creare gruppi di isolamento per i pacchetti App-V

È possibile creare gruppi di isolamento per abilitare la consegna automatica di pacchetti App-V interdipendenti.

> **Nota:**
>
> I gruppi di isolamento sono supportati per il metodo App-V Single Admin. Se si utilizza il metodo App-V Dual Admin, è possibile raggiungere lo stesso obiettivo creando *gruppi di connessione* nell'infrastruttura Microsoft App-V. Per ulteriori informazioni, consultare questo articolo della documentazione Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

#### Informazioni sui gruppi di isolamento

Un gruppo di isolamento è una raccolta di pacchetti di applicazioni interdipendenti che devono essere eseguiti nella stessa sandbox di Windows per creare un ambiente virtuale. I gruppi di isolamento Citrix App-V sono simili ma non identici ai gruppi di connessione App-V. Un gruppo di isolamento include due tipi di pacchetti:

- Pacchetti di applicazioni **espliciti**. Applicazioni con requisiti di licenza specifici. È possibile limitare tali applicazioni a un intervallo specifico di utenti aggiungendole ai gruppi di consegna.
- Pacchetti di applicazioni **automatici**. Applicazioni sempre disponibili per tutti gli utenti indipendentemente dal fatto che vengano aggiunte ai gruppi di consegna.

Ad esempio, l'applicazione app-a richiede l'esecuzione di JRE 1.7. È possibile creare un gruppo di isolamento contenente app-a (contrassegnato come *Explicit* [Esplicito]) e JRE 1.7 (contrassegnato come *Automatic* [Automatico]). Successivamente, aggiungere il pacchetto App-V per app-a a uno o più gruppi di consegna. Quando un utente avvia app-a, JRE 1.7 viene distribuito automaticamente con esso.

Quando un utente avvia un'applicazione App-V contrassegnata come *Explicit* (Esplicita) in un gruppo di isolamento, Citrix DaaS verifica l'autorizzazione di accesso dell'utente all'applicazione nei gruppi di consegna. Se l'utente dispone dell'autorizzazione per accedere all'applicazione, tutti i pacchetti di applicazioni *automatici* nello stesso gruppo di isolamento vengono resi disponibili all'utente.

Non è necessario aggiungere i pacchetti *automatici* a nessun gruppo di consegna. Se è presente un altro pacchetto di applicazioni *esplicito* nel gruppo di isolamento, tale pacchetto viene reso disponibile all'utente solo se si trova nello stesso gruppo di consegna.

Per ulteriori informazioni sui gruppi isolati, vedere questo blog di Citrix.

**Creare un gruppo di isolamento App-V** Creare un gruppo di isolamento e aggiungervi pacchetti di applicazioni interdipendenti. I passaggi dettagliati sono i seguenti:

1. Nella scheda **Isolation Groups** (Gruppi di isolamento), fare clic su **Add Isolation Group** (Aggiungi gruppo di isolamento).
2. Immettere un nome e una descrizione per il gruppo di isolamento. Tutti i pacchetti di applicazioni in Citrix Cloud vengono visualizzati nell'elenco **Available Packages** (Pacchetti disponibili).
3. Dall'elenco **Available Packages** (Pacchetti disponibili), selezionare un'applicazione in base alle esigenze, quindi fare clic sulla freccia destra. L'applicazione selezionata dovrebbe ora essere visualizzata nell'elenco **Packages in Isolation Group** (Pacchetti nel gruppo di isolamento).
4. Nel campo **Deployment** (Distribuzione), selezionare **Explicit** (Esplicita) o **Automatic** (Automatica) per l'applicazione.
5. Ripetere i passaggi 2-3 per aggiungere altri pacchetti.
6. Per modificare l'ordine dei pacchetti nell'elenco, fare clic sulla freccia su o giù.
7. Fare clic su **Salva**.

> **Nota:**
>
> Le configurazioni dei gruppi di isolamento determinano la creazione di un gruppo di connessione App-V sul VDA. Gli scenari di distribuzione possono diventare complessi e il client App-V supporta pacchetti che si trovano in un solo gruppo di connessione attivo alla volta. Si consiglia di evitare di aggiungere lo stesso pacchetto a due diversi gruppi di isolamento aggiunti allo stesso gruppo di consegna.

## Autoscale

September 12, 2023

Autoscale offre una soluzione coerente e ad alte prestazioni per la gestione proattiva delle macchine. Punta a raggiungere un equilibrio fra i costi e l'esperienza dell'utente. Autoscale incorpora la tecnologia Smart Scale deprecata nella soluzione di gestione dell'accensione della console **Manage**.

Autoscale consente la gestione proattiva dell'alimentazione di tutte le macchine con sistema operativo a sessione singola e multisessione registrate in un gruppo di consegna.

Le funzionalità di Autoscale includono:

- Impostazioni basate sulla pianificazione e sul carico
- Timeout dinamici delle sessioni
- Scalabilità automatica delle macchine con tag (cloud burst)
- Provisioning dinamico delle macchine
- Notifiche di scollegamento dell'utente

### Piattaforme di hosting VDA supportate

Autoscale supporta tutte le piattaforme supportate da Citrix DaaS. Ciò include varie piattaforme di infrastruttura tra cui Citrix Hypervisor, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere e molte altre. Per un elenco completo delle piattaforme supportate, consultare Requisiti di sistema per Citrix DaaS.

### Carichi di lavoro supportati

Autoscale supporta sia i gruppi di consegna di sistemi operativi sia multisessione che a sessione singola. Ci sono tre interfacce utente di cui essere a conoscenza:

- Interfaccia utente Autoscale per gruppi di consegna di sistemi operativi multisessione (in precedenza gruppi di consegna RDS)
- Interfaccia utente con scalabilità automatica per gruppi di consegna casuali (in pool) di sistemi operativi a sessione singola (in precedenza gruppi di consegna VDI in pool)
- Interfaccia utente Autoscale per gruppi di consegna statici di sistemi operativi a sessione singola (in precedenza gruppi di consegna VDI statici)

Per ulteriori informazioni sulle interfacce utente per diversi gruppi di consegna, vedere Interfacce utente di Autoscale.

### Vantaggi

La funzione Autoscale offre i seguenti vantaggi:

- Fornire un meccanismo unico e coerente per la gestione dell'accensione delle macchine di un gruppo di consegna.
- Garantire la disponibilità e controllare i costi alimentando le macchine con una gestione dell'accensione basata sul carico o su una pianificazione, o una combinazione di entrambi.
- Per monitorare parametri come il risparmio sui costi e l'utilizzo della capacità e per abilitare le notifiche, utilizzare Director, disponibile nella scheda **Monitor**.

### Video di 2 minuti

Il seguente video fornisce una panoramica rapida di Autoscale.

Si tratta di un video incorporato. Fare clic sul collegamento per guardare il video

## Introduzione ad Autoscale

October 30, 2023

Autoscale funziona a livello di gruppo di consegna. Gestisce in modo proattivo le macchine di un gruppo di consegna in base alle pianificazioni impostate.

Autoscale si applica a tutti i tipi di gruppo di consegna:

- Sistema operativo statico a sessione singola
- Sistema operativo casuale a sessione singola
- Sistema operativo casuale multisessione

Questo articolo descrive i concetti di base relativi ad Autoscale e fornisce indicazioni su come abilitare e configurare Autoscale per un gruppo di consegna.

### Concetti di base

Prima di iniziare, è bene apprendere i seguenti concetti di base di Autoscale:

- Pianificazioni
- Capacity buffer (Buffer di capacità)
- Indice di carico

#### Pianificazioni

Autoscale accende e spegne le macchine di un gruppo di consegna in base a una pianificazione impostata dall'utente.

Una pianificazione include il numero di macchine attive per ogni fascia oraria, con orari di punta e non di punta definiti.

Le impostazioni di pianificazione variano in base al tipo di gruppo di consegna. Per ulteriori informazioni, vedere:

- Gruppi di consegna di sistemi operativi multisessione

- Gruppi di consegna casuale di sistemi operativi a sessione singola
- Gruppi di consegna statici di sistemi operativi a sessione singola

#### Capacity buffer (Buffer di capacità)

Il buffer di capacità viene utilizzato per aggiungere capacità di riserva alla domanda corrente per tenere conto degli aumenti dinamici del carico. Ci sono due scenari da tenere presenti:

- Per i gruppi di consegna di sistemi operativi multisessione, il buffer di capacità è definito come una percentuale della capacità totale del gruppo di consegna in termini di indice di carico.
- Per i gruppi di consegna di sistemi operativi a sessione singola, il buffer di capacità è definito come una percentuale del numero totale di macchine incluse nel gruppo di consegna.

#### Indice di carico

> **IMPORTANTE:**
>
> L'indice di carico si applica solo ai gruppi di consegna multisessione.

La metrica dell'indice di carico determina la probabilità che una macchina riceva le richieste di accesso degli utenti. Viene calcolata utilizzando le impostazioni dei **criteri di gestione del carico Citrix** configurate per l'uso simultaneo di accesso, sessione, CPU, disco e memoria.

L'indice di carico varia da 0 a 10.000. Per impostazione predefinita, una macchina è considerata a pieno carico quando ospita 250 sessioni:

- La cifra "0"indica una macchina non caricata. Una macchina con un valore di indice di carico pari a 0 si trova a un carico di base.
- La cifra "10.000"indica una macchina a pieno carico che non può eseguire nessun'altra sessione.

### Abilitare o disabilitare Autoscale per un gruppo di consegna

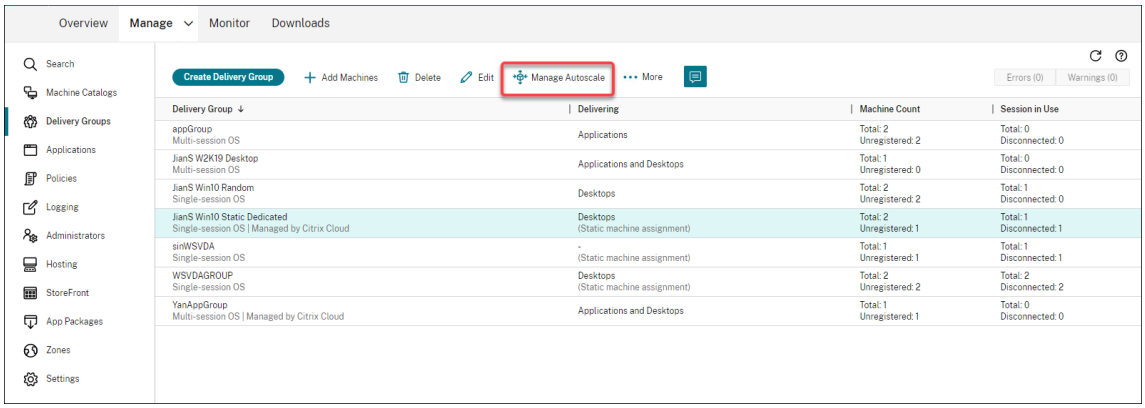
Autoscale è disabilitato per impostazione predefinita quando si crea un gruppo di consegna. Per abilitare e configurare Autoscale per un gruppo di consegna utilizzando l'interfaccia Full Configuration, seguire questi passaggi:

È inoltre possibile utilizzare i comandi PowerShell per abilitare e configurare Autoscale per un gruppo di consegna. Per ulteriori informazioni, vedere Comandi dell'SDK Broker PowerShell.

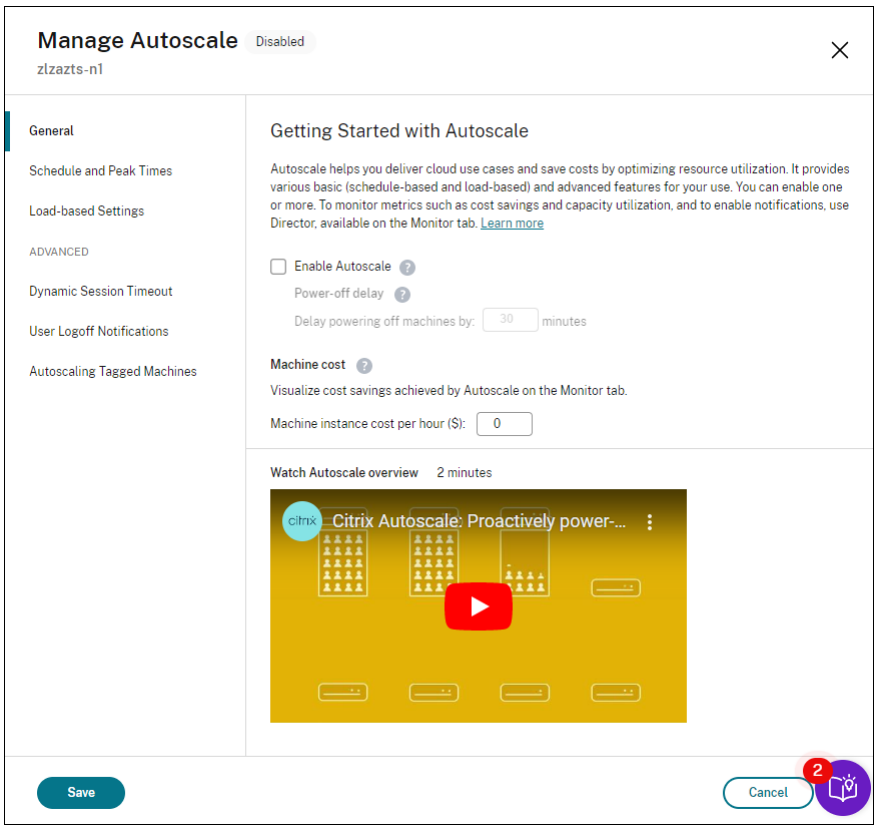
1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra.

2. Selezionare il gruppo di consegna da gestire, quindi fare clic su **Manage Autoscale** (Gestione Autoscale).




3. Nella pagina **Manage Autoscale**, selezionare la casella di controllo **Enable Autoscale** per abilitare Autoscale. Dopo aver abilitato Autoscale, le opzioni presenti nella pagina sono abilitate.




4. Per modificare le impostazioni predefinite in base alle esigenze dell'organizzazione, completare le seguenti impostazioni:

   - Set up schedules (Imposta le pianificazioni)
   - Per spegnere i computer inattivi in modo più efficiente, utilizzare i Dynamic session timeouts (Timeout dinamici delle sessioni) e le User logoff notifications (Notifiche di scollega-

mento degli utenti)

- Per gestire in modo efficiente un sottoinsieme di macchine del gruppo di consegna, utilizzare l'impostazione Autoscaling tagged machines (Scalabilità automatica delle macchine con tag)

Per disattivare Autoscale, deselezionare la casella di controllo **Autoscale**. Le opzioni presenti nella pagina diventano grigie per indicare che l'opzione Autoscale è disabilitata per il gruppo di consegna selezionato.

> **Importante:**
>
> - Se si disabilita Autoscale, tutte le macchine gestite da Autoscale rimangono nello stato in cui si trovavano al momento della disattivazione.
> - Dopo aver disabilitato Autoscale, le macchine in stato di scarico vengono rimosse dallo stato di svuotamento. Per ulteriori informazioni sullo stato di svuotamento, vedere Stato di svuotamento.

È possibile effettuare il provisioning dinamico delle macchine per il gruppo utilizzando uno script PowerShell. Per ulteriori informazioni, vedere Provisioning dinamico delle macchine.

### Monitorare le metriche

Dopo aver abilitato Autoscale per un gruppo di consegna, è possibile monitorare le seguenti metriche delle macchine gestite da Autoscala dalla scheda **Monitor**.

- Utilizzo della macchina
- Risparmio stimato
- Notifiche di avviso per macchine e sessioni
- Stato della macchina
- Tendenze di valutazione del carico

> **Nota:**
>
> La prima volta che si abilita Autoscale per un gruppo di consegna, potrebbero essere necessari alcuni minuti per visualizzare i dati di monitoraggio per quel gruppo di consegna.
> I dati di monitoraggio rimangono disponibili se l'opzione Autoscale è abilitata e quindi disabilitata per il gruppo di consegna. Autoscale raccoglie i dati di monitoraggio a intervalli di 5 minuti.

Per ulteriori informazioni sulle metriche, vedere Monitorare le macchine gestite da Autoscale.

## Considerazioni importanti

Autoscale funziona a livello di gruppo di consegna. Viene configurato un gruppo di consegna alla volta. Gestisce l'accensione delle sole macchine del gruppo di consegna selezionato.

### Registrazione della capacità e della macchina

Autoscale include solo le macchine registrate presso il sito al momento della determinazione della capacità. Le macchine accese non registrate non possono accettare richieste di sessione. Di conseguenza, non sono incluse nella capacità complessiva del gruppo di consegna.

### Scalabilità su più cataloghi di macchine

In alcuni siti, potrebbero esserci più cataloghi di macchine associati a un singolo gruppo di consegna. Autoscale accende in modo casuale le macchine di ciascun catalogo per soddisfare i requisiti della pianificazione o della domanda di sessioni.

Ad esempio, un gruppo di consegna ha due cataloghi di macchine: il catalogo A ha tre macchine accese e il catalogo B ha una macchina accesa. Se Autoscale deve accendere una macchina aggiuntiva, potrebbe accendere una macchina del catalogo A o del catalogo B.

### Provisioning di macchine e domanda di sessioni

Il catalogo di macchine associato al gruppo di consegna deve avere un numero sufficiente di macchine da accendere e spegnere all'aumentare e al diminuire della domanda. Se la domanda di sessioni supera il numero totale di macchine registrate nel gruppo di consegna, Autoscale garantisce che tutte le macchine registrate siano accese. Tuttavia, **Autoscale non effettua il provisioning di macchine aggiuntive**.

Per ovviare a questo collo di bottiglia, è possibile utilizzare uno script PowerShell per creare macchine ed eliminarle dinamicamente. Per ulteriori informazioni, vedere Provisioning dinamico delle macchine.

### Considerazioni sulle dimensioni delle istanze

È possibile ottimizzare i costi se si dimensionano correttamente le istanze nei cloud pubblici. Consigliamo di eseguire il provisioning di istanze più piccole, fintanto che corrispondano ai requisiti di capacità e prestazioni del carico di lavoro.

Le istanze più piccole ospitano meno sessioni utente rispetto alle istanze più grandi. Pertanto Autoscale mette le macchine in stato di svuotamento molto più velocemente, perché lo scollegamento

dell'ultima sessione utente impiega meno tempo. Di conseguenza, Autoscale spegne prima le istanze più piccole, riducendo così i costi.

#### Stato di svuotamento

Autoscale tenta di ridurre il numero di macchine accese del gruppo di consegna in base alla dimensione del pool configurato e al buffer di capacità.

Per raggiungere questo obiettivo, Autoscale mette le macchine in eccesso con il minor numero di sessioni in "stato di svuotamento"e le spegne quando tutte le sessioni vengono scollegate. Questo comportamento si verifica quando la domanda di sessioni diminuisce e la pianificazione richiede meno computer di quanti ne siano accesi.

Autoscale mette le macchine in eccesso in "stato di svuotamento"una per una, in base ai seguenti criteri:

- Se due o più macchine hanno lo stesso numero di sessioni attive, Autoscale scarica la macchina che è stata accesa per il ritardo di spegnimento specificato.

  In questo modo si evita di mettere le macchine accese di recente in stato di svuotamento perché è più probabile che quelle macchine abbiano il minor numero di sessioni.
- Se due o più macchine sono state accese per il ritardo di spegnimento specificato, Autoscale mette in stato di svuotamento tali macchine una in ordine casuale.

Le macchine in stato di svuotamento non ospitano più nuovi avvii di sessioni e sono in attesa che le sessioni esistenti vengano scollegate. Una macchina diventa candidata per l'arresto solo quando tutte le sessioni sono scollegate. Tuttavia, se non ci sono macchine immediatamente disponibili per l'avvio delle sessioni, Autoscale preferisce dirigere gli avvii di sessione su una macchina in stato di svuotamento piuttosto che accendere una macchina.

Una macchina viene tolta dallo stato di svuotamento quando viene soddisfatta una delle seguenti condizioni:

- La macchina è spenta.
- Autoscale è disabilitato per il gruppo di consegna a cui appartiene la macchina.
- Autoscale utilizza la macchina per soddisfare i requisiti di pianificazione o di domanda di carico. Questo caso si verifica quando la pianificazione (ridimensionamento basato su pianificazione) o la domanda corrente (ridimensionamento basato sul carico) richiede più macchine rispetto al numero di macchine attualmente accese.

> **Importante:**
>
> Se nessuna macchina è immediatamente disponibile per gli avvii delle sessioni, Autoscale preferisce dirigere gli avvii di sessione su una macchina in stato di svuotamento piuttosto che

> accendere una macchina. Una macchina in stato di svuotamento che ospita l'avvio di una sessione rimane in stato di svuotamento.

Per scoprire quali macchine sono in stato di svuotamento, utilizzare il comando `Get-BrokerMachine` di PowerShell. Ad esempio: `Get-BrokerMachine -DrainingUntilShutdown $true`. In alternativa, è possibile utilizzare la console Manage (Gestisci). Vedere Visualizzare le macchine in stato di svuotamento.

**Visualizzare le macchine in stato di svuotamento**

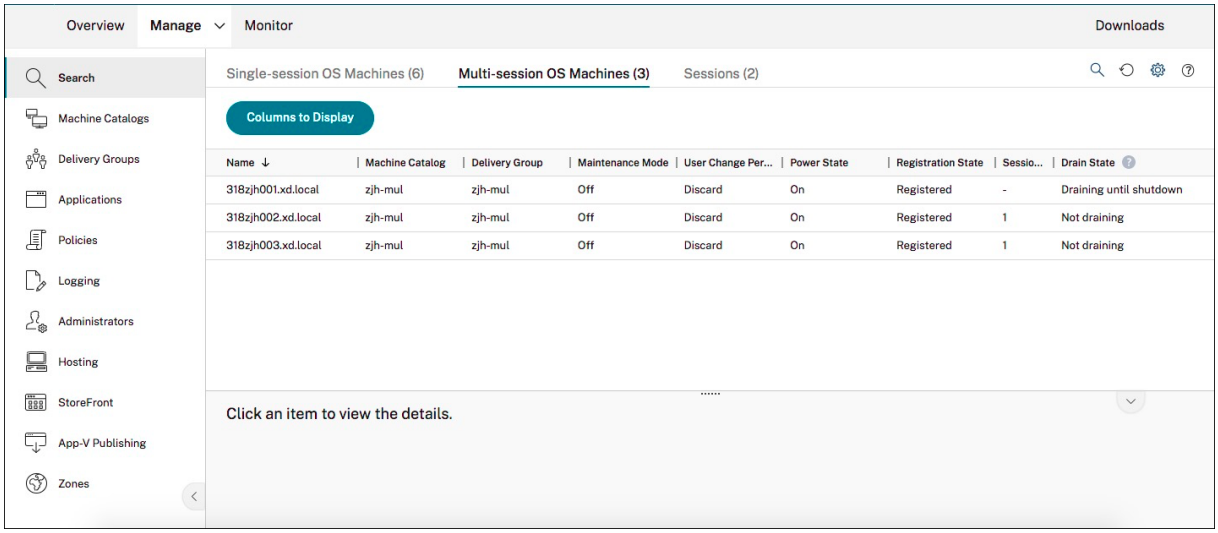
> **Nota:**
>
> Questa funzione si applica solo alle macchine multisessione.

In **Manage > Full Configuration** (Gestione > Configurazione completa), è possibile visualizzare le macchine in stato di svuotamento, per sapere quali macchine stanno per essere arrestate. Completare i seguenti passaggi:

1. Passare al nodo **Search** e quindi fare clic su **Columns to Display** (Colonne da visualizzare).
2. Nella finestra **Colonne da visualizzare**, selezionare la casella di controllo accanto a **Drain State** (Stato di svuotamento).
3. Fare clic su **Save** (Salva) per uscire dalla finestra **Columns to Display**.

La colonna **Drain State** può visualizzare le seguenti informazioni:

- **Draining until shutdown.** Viene visualizzato quando le macchine sono in stato di svuotamento finché non vengono spente.
- **Not draining.** Appare quando le macchine non sono ancora in stato di svuotamento.



### Ulteriori informazioni

Per ulteriori informazioni sul Autoscale, vedere Citrix Autoscale in Tech Zone.

## Impostazioni basate sulla pianificazione e sul carico

October 30, 2023

### Come Autoscale gestisce l'alimentazione delle macchine

Autoscale accende e spegne le macchine in base alla pianificazione selezionata. Autoscale consente di impostare più pianificazioni che includono giorni specifici della settimana e di regolare il numero di macchine disponibili in tali orari. Se ci si aspetta che un gruppo di utenti consumi le risorse macchina in un momento specifico in giorni specifici, Autoscale aiuta a fornire un'esperienza ottimizzata. Si noti che tali macchine saranno accese durante la pianificazione, indipendentemente dal fatto che ci siano o meno sessioni in esecuzione su di esse.

> **Nota:**
>
> Autoscale supporta qualsiasi macchina con alimentazione gestita.

La pianificazione si basa sul **fuso orario** del gruppo di consegna. Per modificare il fuso orario, è possibile modificare le impostazioni utente di un gruppo di consegna. Per ulteriori informazioni, vedere Gestire i gruppi di consegna.

Autoscale ha due orari predefiniti: *Weekdays* (da lunedì a venerdì) e *Weekend* (sabato e domenica). Per impostazione predefinita, la pianificazione **Weekdays** mantiene accesa una macchina dalle 07:00 alle 18:30 durante le ore di punta e non ne mantiene accesa nessuna durante le ore non di punta. Il buffer di capacità predefinito è impostato al 10% durante le ore di punta e non di punta. Per impostazione predefinita, la pianificazione **Weekend** non mantiene acceso nessun computer.

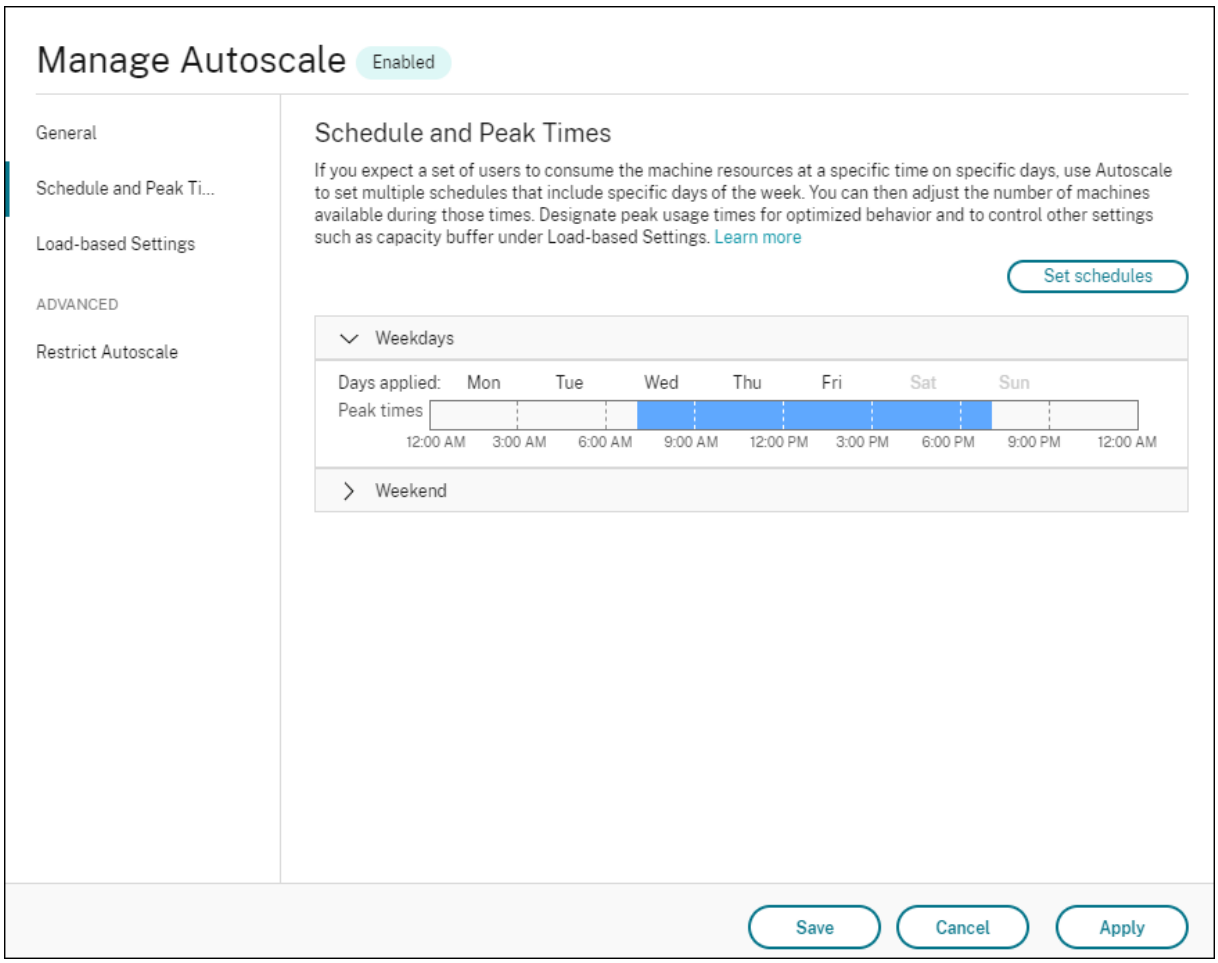
> **Nota:**
>
> Autoscale considera solo le macchine registrate nel sito come parte della capacità disponibile nei calcoli che effettua. "Registered"(Registrata) significa che la macchina è disponibile per l'uso o già in uso. In questo modo si garantisce che solo le macchine in grado di accettare sessioni utente siano incluse nella capacità del gruppo di consegna.

### Interfacce utente

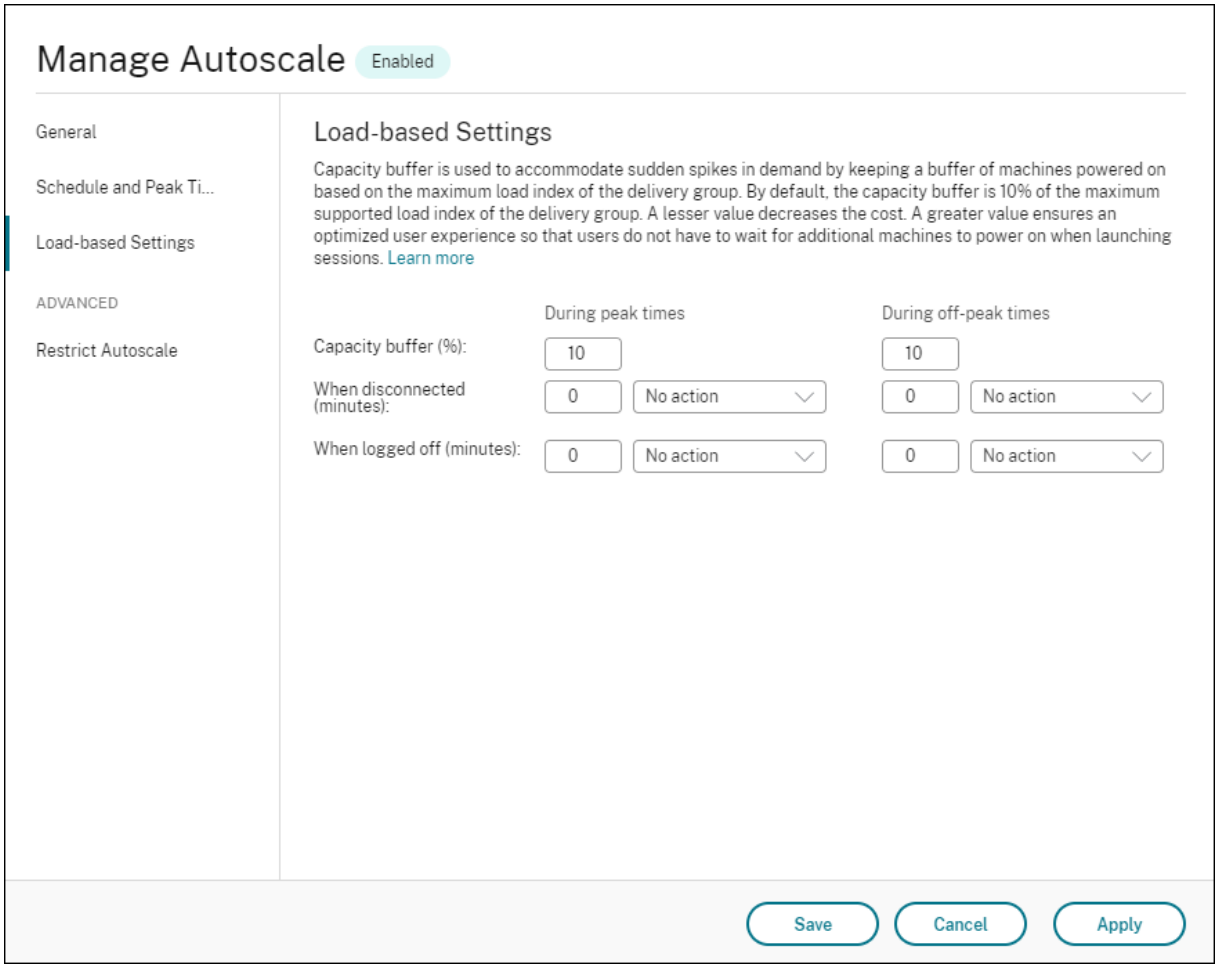
Esistono tre tipi di interfacce utente da tenere presenti.

Interfaccia utente per *gruppi di consegna statici con sistema operativo a sessione singola*:

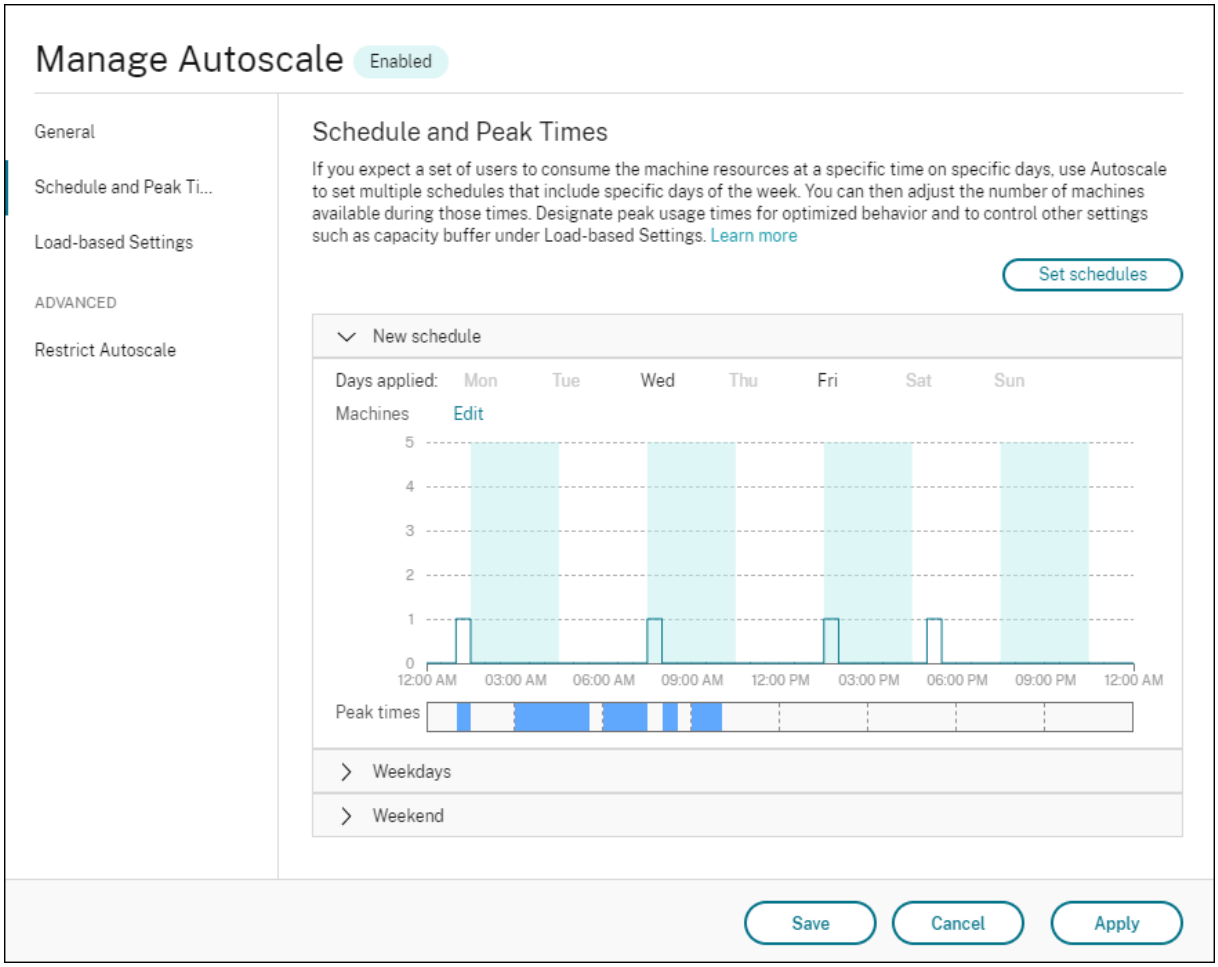


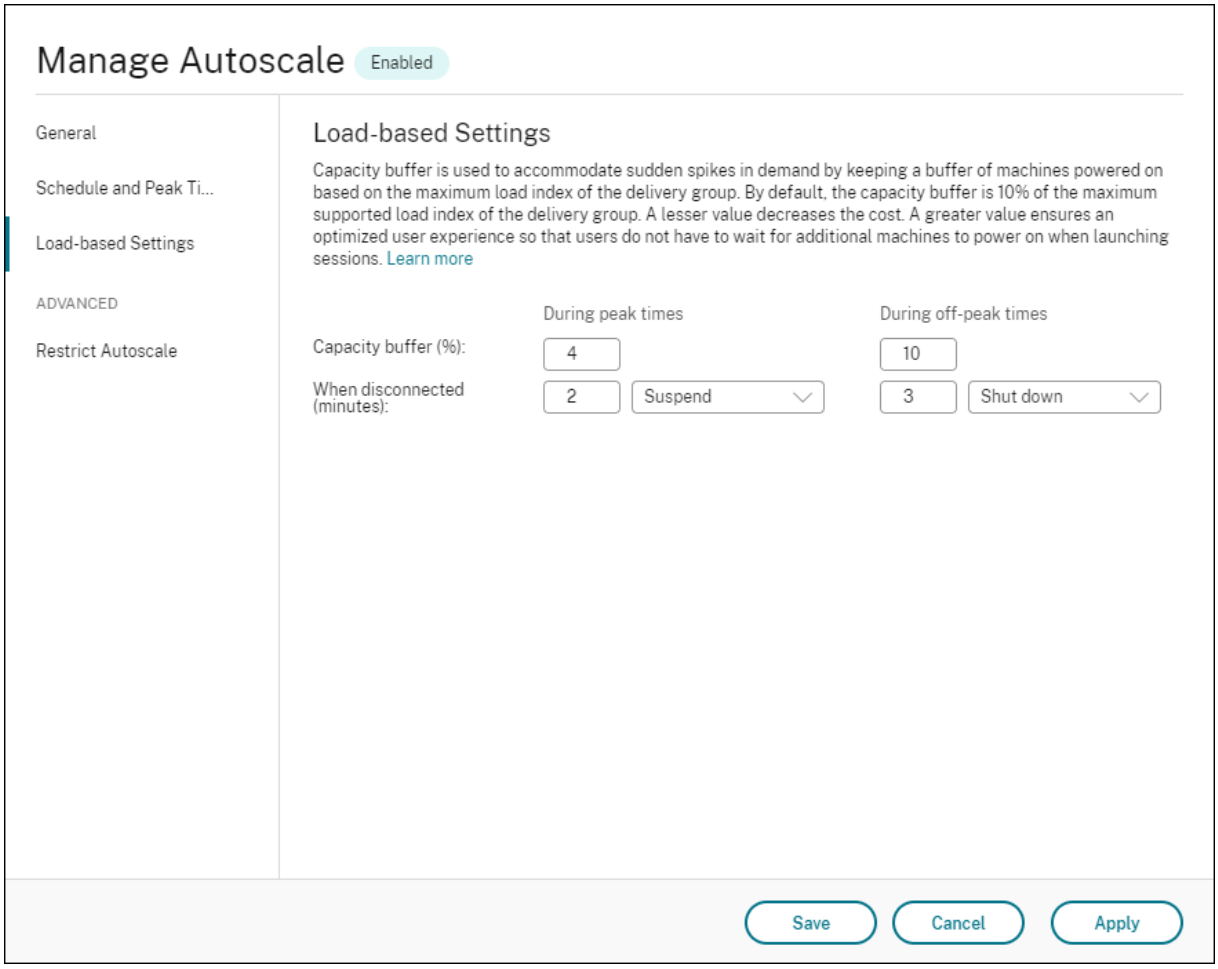



Interfaccia utente Autoscale per *gruppi di consegna casuali con sistema operativo a sessione singola*:

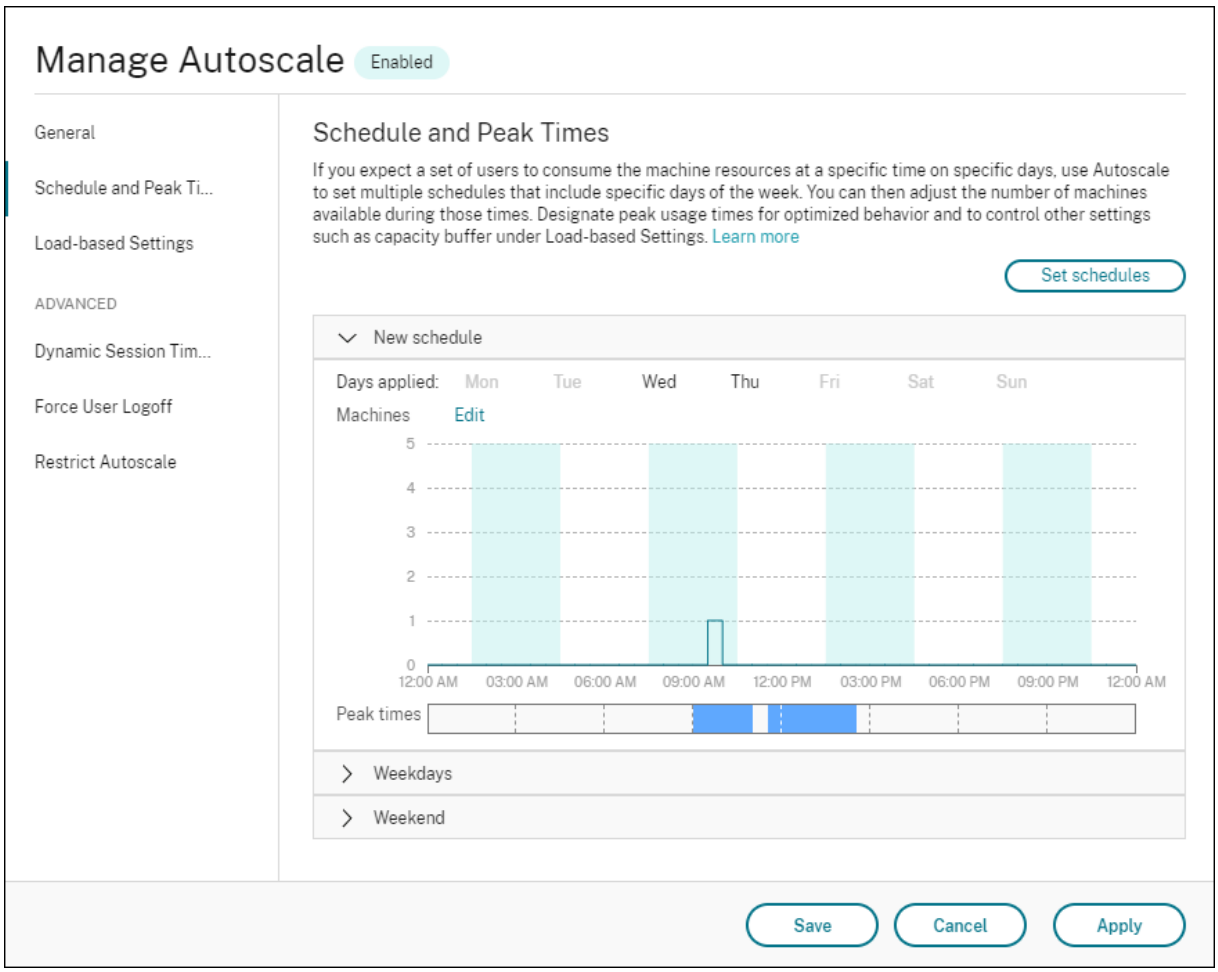


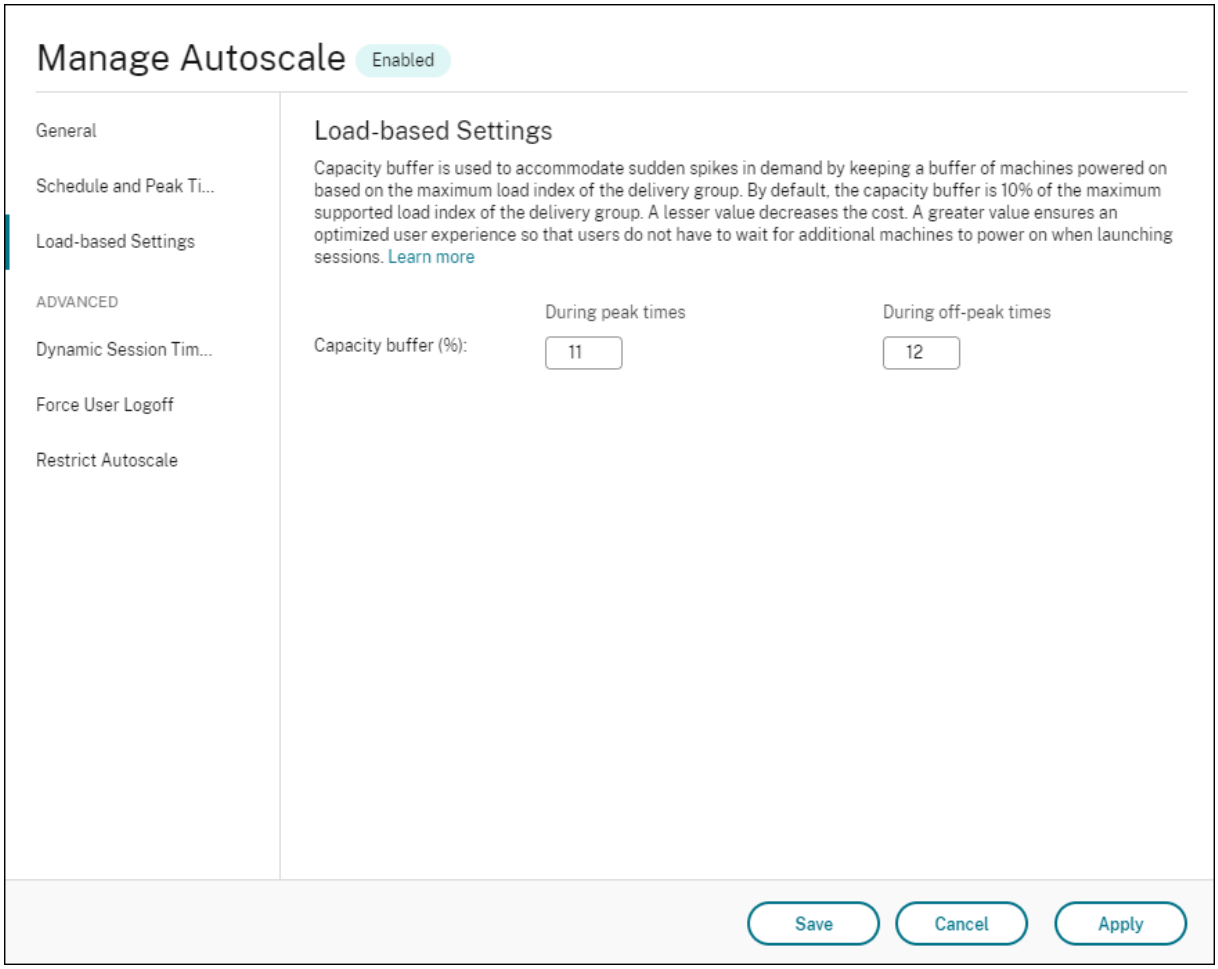



Interfaccia utente Autoscale per *gruppi di consegna di sistemi operativi multisessione*:






### Impostazioni basate sulla pianificazione

**Pianificazione Autoscale**. Consente di aggiungere, modificare, selezionare ed eliminare le pianificazioni.

**Giorni applicati**. Evidenzia i giorni applicati alla pianificazione selezionata. I giorni rimanenti sono in grigio.

**Edit**. Consente di assegnare le macchine rispetto a ciascuna ora esatta o mezz'ora. È possibile assegnare le macchine in base ai numeri e alle percentuali.

> **Nota:**
>
> - Questa opzione è disponibile solo nelle interfacce utente di Autoscale per i gruppi di consegna casuali con sistema operativo multisessione e a sessione singola.
> - L'istogramma accanto a **Edit** rappresenta il numero o la percentuale di macchine in esecuzione in diverse fasce orarie.
> - È possibile **assegnare macchine** rispetto a ciascuna fascia oraria facendo clic su **Edit** al di

sopra di **Peak times**. A seconda dell'opzione selezionata dal menu nella finestra **Machines to start** (Macchine da avviare), è possibile assegnare le macchine in base ai numeri o alle percentuali.
- Per i gruppi di consegna di sistemi operativi multisessione, è possibile impostare il numero minimo di macchine in esecuzione separatamente con incrementi granulari di 30 minuti nell'arco di ogni giorno. Per i gruppi di consegna casuale con sistema operativo a sessione singola, è possibile impostare il numero minimo di macchine in esecuzione separatamente con incrementi granulari di 60 minuti nell'arco di ogni giorno.

Per definire le proprie pianificazioni, attenersi alla seguente procedura:

1. Nella pagina **Schedule and Peak Times** (Pianificazione e orari di punta) della finestra **Manage Autoscale**, fare clic su **Set schedules** (Imposta pianificazioni).
2. Nella finestra **Edit Autoscale Schedules** (Modifica pianificazioni Autoscale), selezionare i giorni che si desidera applicare a ciascuna pianificazione. È inoltre possibile eliminare le pianificazioni secondo necessità.
3. Fare clic su **Done** (Fine) per salvare le pianificazioni e tornare alla pagina **Schedule and Peak Times**(Pianificazione e orari di punta).
4. Selezionare la pianificazione applicabile e configurarla secondo necessità.
5. Fare clic su **Apply** per uscire dalla finestra **Manage Autoscale** o per configurare le impostazioni su altre pagine.

**Importante:**

- Autoscale non consente che lo stesso giorno si sovrapponga in pianificazioni diverse. Ad esempio, se si seleziona il lunedì nella pianificazione2 dopo aver selezionato il lunedì nella pianificazione1, il lunedì viene cancellato automaticamente nella pianificazione1.
- Il nome di una pianificazione non fa distinzione tra maiuscole e minuscole.
- Il nome di una pianificazione non deve essere vuoto o contenere solo spazi.
- Autoscale consente di inserire spazi vuoti tra i caratteri.
- Il nome di una pianificazione non deve contenere i seguenti caratteri: \ / ; : # . * ? = < > | [ ] ( ) { } “‘.
- Autoscale non supporta nomi di pianificazione duplicati. Inserire un nome diverso per ciascuna pianificazione.
- Autoscale non supporta le pianificazioni vuote. Ciò significa che le pianificazioni senza giorni selezionati non vengono salvate.

**Nota:**

I giorni inclusi nel programma selezionato sono evidenziati, mentre quelli non inclusi sono in

> grigio.

### Impostazioni basate sul carico

**Ore di punta**. Consente di definire le ore di punta per i giorni applicati nella pianificazione selezionata. È possibile farlo facendo clic con il pulsante destro del mouse sul grafico a barre orizzontale. Dopo aver definito le ore di punta, le restanti ore non definite vengono impostate automaticamente su ore non di punta. Per **impostazione predefinita**, la fascia oraria dalle 7:00 alle 19:00 è definita orario di punta per i giorni inclusi nella pianificazione selezionata.

> **Importante:**
>
> - Nel caso dei gruppi di consegna di sistemi operativi multisessione, il grafico a barre delle ore di punta viene utilizzato per il buffer di capacità.
> - Nel caso dei gruppi di consegna di sistemi operativi a sessione singola, il grafico a barre delle ore di punta viene utilizzato per il buffer di capacità e controlla le azioni da attivare dopo lo scollegamento e/o la disconnessione.
> - È possibile definire gli orari di punta per i giorni inclusi in una pianificazione a un livello granulare di 30 minuti per i gruppi di consegna di sistemi operativi multisessione e a sessione singola. In alternativa, è possibile utilizzare il comando `New-BrokerPowerTimeScheme PowerShell`. Per ulteriori informazioni, vedere Comandi dell'SDK Broker PowerShell.

**Buffer di capacità**. Consente di mantenere un buffer di macchine accese. Un valore inferiore riduce il costo. Un valore superiore garantisce un'esperienza utente ottimizzata in modo che, all'avvio delle sessioni, gli utenti non debbano attendere l'accensione di altre macchine. Per impostazione predefinita, il buffer di capacità è del 10% per le ore di punta e non di punta. Se si imposta il buffer di capacità su 0 (zero), gli utenti potrebbero dover attendere l'accensione di altre macchine all'avvio delle sessioni. Autoscale consente di determinare il buffer di capacità separatamente per le ore di punta e non di punta.

### Impostazioni varie

> **Suggerimento:**
>
> - È possibile scegliere di configurare le impostazioni varie utilizzando l'SDK Broker PowerShell. Per ulteriori informazioni, vedere Comandi dell'SDK Broker PowerShell.
> - Per comprendere i comandi dell'SDK associati alle impostazioni di disconnessione e disconnessione, vedere https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

**Quando si è disconnessi**. Consente di specificare per quanto tempo una macchina disconnessa e bloccata rimane accesa dopo la disconnessione della sessione prima della sospensione o la chiusura della sessione. Se viene specificato un valore temporale, il computer viene sospeso o arrestato allo scadere del tempo di disconnessione specificato, a seconda dell'azione configurata. Per impostazione predefinita, non viene assegnata alcuna azione alle macchine disconnesse. È possibile definire separatamente azioni per le ore di punta e non di punta. A tale scopo, fare clic sulla freccia rivolta verso il basso e quindi selezionare una delle seguenti opzioni dal menu:

- **No action**. Se è selezionata questa opzione, dopo la disconnessione della sessione la macchina rimane accesa. Autoscale non agisce su di essa.
- **Suspend** Se è selezionata questa opzione, Autoscale mette in pausa la macchina senza spegnerla allo scadere del tempo di disconnessione specificato. Dopo aver selezionato **Suspend** si rende disponibile la seguente opzione.
  - **When no reconnection in (minutes)**. Le macchine sospese rimangono disponibili per gli utenti disconnessi quando questi si riconnettono, ma non sono disponibili per i nuovi utenti. Per rendere nuovamente disponibili le macchine a gestire tutti i carichi di lavoro, arrestarle. Specificare il timeout, in minuti, dopo il quale Autoscale le spegne.
- **Shut down**. Se è selezionata questa opzione, Autoscale arresta la macchina allo scadere del tempo di disconnessione specificato.

> **Nota:**
>
> Questa opzione è disponibile solo nelle interfacce utente di Autoscale per gruppi di consegna casuali e statici di sistemi operativi a sessione singola.

**When logged off**. Consente di specificare per quanto tempo una macchina rimane accesa dopo lo scollegamento della sessione prima di essere sospesa o arrestata. Se viene specificato un valore temporale, la macchina viene sospesa o arrestata allo scadere del tempo di disconnessione specificato, a seconda delle azioni configurate. Per impostazione predefinita, non viene assegnata alcuna azione alle macchine scollegate. È possibile definire separatamente azioni per le ore di punta e non di punta. A tale scopo, fare clic sulla freccia rivolta verso il basso e quindi selezionare una delle seguenti opzioni dal menu:

- **No action**. Se è selezionata questa opzione, dopo lo scollegamento della sessione la macchina rimane accesa. Autoscale non agisce su di essa.
- **Suspend** Se è selezionata questa opzione, Autoscale mette in pausa la macchina senza spegnerla allo scadere del tempo di scollegamento specificato.
- **Shut down**. Se è selezionata questa opzione, Autoscale arresta la macchina allo scadere del tempo di scollegamento specificato.

> **Nota:**
>
> Questa opzione è disponibile solo nell'interfaccia utente Autoscale per gruppi di consegna statici di sistemi operativi a sessione singola.

### Gestire l'alimentazione di macchine con sistema operativo a sessione singola che passano a un periodo di tempo diverso con sessioni disconnesse

> **Importante:**
>
> - Questo miglioramento si applica solo alle macchine con sistema operativo a sessione singola con sessioni disconnesse. Non si applica alle macchine con sistema operativo a sessione singola con sessioni scollegate.
> - Affinché questo miglioramento abbia effetto, è necessario abilitare l'opzione Autoscale per il gruppo di consegna applicabile. In caso contrario, le azioni dei criteri di disconnessione non vengono attivate durante la transizione da un periodo all'altro.

Nelle versioni precedenti, una macchina con sistema operativo a sessione singola che passava a un periodo di tempo in cui era necessaria un'azione (azione di disconnessione= "**Suspend**"o "**Shutdown"** ) rimaneva alimentata. Questo scenario si verificava se la macchina si disconnetteva durante un periodo di tempo (di punta o non di punta) in cui non era richiesta alcuna azione (azione di disconnessione = "**Nothing**").

A partire da questa versione, Autoscale mette in sospensione o arresta la macchina al termine del tempo di disconnessione specificato, a seconda dell'azione di disconnessione configurata per il periodo di tempo di destinazione.

Ad esempio, è possibile configurare i criteri di risparmio energia seguenti per un gruppo di consegna di sistemi operativi a sessione singola:

- Impostare `PeakDisconnectAction` su "Nothing"
- Impostare `OffPeakDisconnectAction` su "Shutdown"
- Impostare "OffPeakDisconnectTimeout"su "10"

> **Nota:**
>
> Per ulteriori informazioni sui criteri di risparmio energia per l'azione di disconnessione, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy e https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Nelle versioni precedenti, una macchina con sistema operativo a sessione singola con una sessione disconnessa durante i periodi di punta rimaneva accesa quando passava dai periodi di punta a quelli

non di punta. A partire da questa versione, le azioni dei criteri `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` vengono applicate alla macchina con sistema operativo a sessione singola durante la transizione da un periodo all'altro. Di conseguenza, la macchina viene spenta 10 minuti dopo la transizione al periodo fuori picco.

Nel caso in cui si desideri ripristinare il comportamento precedente (ovvero, non eseguire alcuna azione su macchine che passano dal periodo di punta a quello fuori picco o al periodo di punta con sessioni disconnesse), effettuare una delle seguenti operazioni:

- Impostare il valore del Registro di sistema "LegacyPeakTransitionDisconnectedBehaviour"su 1, (true; abilita il comportamento precedente). Per impostazione predefinita, il valore è 0 (false; attiva la disconnessione delle azioni dei criteri di risparmio energia durante la transizione da un periodo all'altro).
  - Percorso: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nome: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG_DWORD
  - Dati: 0x00000001 (1)
- Configurare l'impostazione utilizzando il comando PowerShell`Set-BrokerServiceConfigurationD` . Ad esempio:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Una macchina deve soddisfare i seguenti criteri prima che le possano essere applicate le azioni dei criteri di risparmio energia durante la transizione da un periodo all'altro:

- Ha una sessione disconnessa.
- Non ha azioni di alimentazione in sospeso.
- Appartiene a un gruppo di consegna di sistemi operativi a sessione singola che passa a un periodo di tempo diverso.
- Ha una sessione che si disconnette durante un determinato periodo di tempo (di punta o non di punta) e passa a un periodo in cui viene assegnata un'azione di alimentazione.

### Come funziona il buffer di capacità

Il buffer di capacità viene utilizzato per aggiungere capacità di riserva alla domanda corrente per tenere conto degli aumenti dinamici del carico. Ci sono due scenari da tenere presenti:

- Per i gruppi di consegna di sistemi operativi multisessione, il buffer di capacità è definito come una percentuale della capacità totale del gruppo di consegna in termini di indice di carico. Per ulteriori informazioni sull'indice di carico, vedere Indice di carico.

- Per i gruppi di consegna di sistemi operativi a sessione singola, il buffer di capacità è definito come una percentuale della capacità totale del gruppo di consegna in termini di numero di macchine.

> **Nota:**
>
> Negli scenari in cui si limita Autoscale alle macchine con tag, il buffer di capacità è definito come una percentuale della capacità totale delle macchine con tag del gruppo di consegna in termini di indice di carico.

Autoscale consente di impostare il buffer di capacità separatamente per le ore di punta e non di punta. Un valore inferiore nel campo del buffer di capacità riduce il costo perché Autoscale alimenta una minore capacità di riserva. Un valore superiore garantisce un'esperienza utente ottimizzata in modo che gli utenti non debbano attendere l'accensione di altre macchine all'avvio delle sessioni. Per impostazione predefinita, il buffer di capacità è del 10%.

> **Importante:**
>
> Il buffer di capacità fa sì che le macchine vengano accese quando la capacità di riserva totale scende a un livello inferiore a "X"per cento della capacità totale del gruppo di consegna. In questo modo si riserva la percentuale richiesta di capacità di riserva.

### Gruppi di consegna di sistemi operativi multisessione

#### Quando vengono accese le macchine?

> **Importante:**
>
> Se viene selezionata una pianificazione, Autoscale accende tutte le macchine configurate per essere accese nella pianificazione. Autoscale mantiene acceso questo numero specificato di macchine durante la pianificazione, indipendentemente dal carico.

Quando il numero di macchine accese nel gruppo di consegna non è più in grado di soddisfare il buffer necessario per onorare la capacità del buffer in termini di indice di carico, Autoscale si alimenta su macchine aggiuntive. Ad esempio, supponiamo che il proprio gruppo di consegna disponga di 20 macchine e che 3 macchine siano programmate per essere accese come parte del ridimensionamento basato su pianificazione con un buffer di capacità del 20%. Alla fine, 4 macchine verranno accese quando non c'è carico. Questo perché è necessario un indice di carico 4 x 10.000 come buffer; quindi è necessario accendere almeno 4 macchine. Questo caso può verificarsi durante le ore di punta, durante l'aumento del carico sulle macchine, durante l'avvio di nuove sessioni e quando si aggiungono nuove macchine al gruppo di consegna. Notare che Autoscale funziona solo sulle macchine che soddisfano i seguenti criteri:

- Le macchine non sono in modalità di manutenzione.

- L'hypervisor su cui sono in esecuzione le macchine non è in modalità di manutenzione.
- Le macchine sono attualmente spente.
- Le macchine non hanno azioni relative all'alimentazione in sospeso.

#### Quando vengono spente le macchine?

> **Importante:**
>
> - Se viene selezionata una pianificazione, Autoscale spegne le macchine in base alla pianificazione.
> - Autoscale non spegne le macchine che nella pianificazione sono configurate per essere accese durante la pianificazione.

Quando ci sono macchine più che sufficienti a supportare il numero target di macchine accese (incluso il buffer) per il gruppo di consegna, Autoscale spegne le macchine aggiuntive. Questo caso può verificarsi durante le ore non di punta, durante la riduzione del carico sui computer, durante lo scollegamento delle sessioni e quando si rimuovono macchine dal gruppo di consegna. Autoscale spegne solo le macchine che soddisfano i seguenti criteri:

- Le macchine e l'hypervisor su cui sono in esecuzione le macchine non sono in modalità di manutenzione.
- Le macchine sono attualmente accese.
- Le macchine sono registrate come disponibili o in attesa di registrazione dopo l'avvio.
- Le macchine non hanno sessioni attive.
- Le macchine non hanno azioni relative all'alimentazione in sospeso.
- Le macchine soddisfano il ritardo di spegnimento specificato. Ciò significa che le macchine sono state accese per almeno "X"minuti, dove "X"è il ritardo di spegnimento specificato per il gruppo di consegna.

#### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del gruppo di consegna**. Il gruppo di consegna la cui alimentazione si desidera venga gestita da Autoscale contiene 10 macchine (da M1 a M10).
- **Configurazione di Autoscale**
  - Il buffer di capacità è impostato al 10%.

  - Nessuna macchina è inclusa nella pianificazione selezionata.

Lo scenario viene eseguito nella seguente sequenza:

1. Nessun utente effettua l'accesso.
2. Le sessioni utente aumentano.
3. Vengono avviate altre sessioni utente.
4. Il carico della sessione utente diminuisce a causa della chiusura della sessione.
5. Il carico della sessione utente diminuisce ulteriormente fino a quando il carico della sessione non viene gestito solo da risorse locali.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

- Nessun carico utente (stato iniziale)
  - Una macchina (ad esempio M1) è accesa. La macchina viene accesa a causa del buffer di capacità configurato. In questo caso, 10 (numero di macchine) x 10.000 (indice di carico) x 10% (buffer di capacità configurato) equivale a 10.000. Pertanto, viene accesa una macchina.
  - Il valore dell'indice di carico della macchina accesa (M1) è a un carico di base (l'indice di carico è uguale a 0).
- Il primo utente esegue l'accesso
  - La sessione è indirizzata a essere ospitata sulla macchina M1.
  - L'indice di carico della macchina accesa M1 aumenta e la macchina M1 non è più a un carico di base.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M2) per soddisfare la domanda a causa del buffer di capacità configurato.
  - Il valore dell'indice di carico della macchina M2 è a un carico di base.
- Gli utenti aumentano il carico
  - Le sessioni hanno il carico distribuito fra le macchine M1 e M2. Di conseguenza, l'indice di carico delle macchine accese (M1 e M2) aumenta.
  - La capacità di riserva totale è ancora a un livello superiore a 10.000 in termini di indice di carico.
  - Il valore dell'indice di carico della macchina M2 non è più a un carico di base.
- Avvio di altre sessioni utente
  - Le sessioni hanno il carico distribuito su tutte le macchine (M1 e M2). Di conseguenza, l'indice di carico delle macchine alimentate (M1 e M2) aumenta ulteriormente.

  - Quando la capacità di riserva totale scende a un livello inferiore a 10.000 in termini di indice di carico, Autoscale inizia ad accendere una macchina aggiuntiva (M3) per soddisfare la domanda, dato il buffer di capacità configurato.
  - Il valore dell'indice di carico della macchina M3 è a un carico di base.

- Vengono avviate ancora più sessioni utente
  - Le sessioni hanno il carico distribuito su tutte le macchine (da M1 a M3). Di conseguenza, l'indice di carico delle macchine accese (da M1 a M3) aumenta.
  - La capacità di riserva totale è a un livello superiore a 10.000 in termini di indice di carico.
  - Il valore dell'indice di carico della macchina M3 non è più a un carico di base.

- Il carico della sessione utente diminuisce a causa della chiusura della sessione
  - Dopo che gli utenti si sono disconnessi dalle sessioni o dopo il timeout delle sessioni inattive, la capacità che si è liberata sulle macchine da M1 a M3 viene riutilizzata per ospitare sessioni avviate da altri utenti.
  - Quando la capacità di riserva totale aumenta fino a un livello superiore a 10.000 in termini di indice di carico, Autoscale mette una delle macchine (ad esempio M3) in stato di svuotamento. Di conseguenza, le sessioni avviate da altri utenti non vengono più indirizzate a quel computer a meno che non vi siano nuovi cambiamenti. Ad esempio, il carico dell'utente finale aumenta nuovamente o altre macchine diventano meno cariche.

- Il carico della sessione utente continua a diminuire
  - Dopo che tutte le sessioni sulla macchina M3 sono terminate e il ritardo di spegnimento specificato è scaduto, Autoscale spegne la macchina M3.
  - Dopo che più utenti hanno terminato le sessioni, la capacità liberata sulle macchine accese (M1 e M2) viene riutilizzata per ospitare sessioni avviate da altri utenti.
  - Quando la capacità di riserva totale aumenta fino a un livello superiore a 10.000 in termini di indice di carico, Autoscale mette una delle macchine (ad esempio M2) in stato di svuotamento. Di conseguenza, le sessioni avviate da altri utenti non vengono più indirizzate a quella macchina.

- Il carico della sessione utente continua a diminuire fino a quando non ci sono sessioni
  - Dopo che tutte le sessioni sulla macchina M2 sono terminate e il ritardo di spegnimento specificato è scaduto, Autoscale spegne la macchina M2.
  - Il valore dell'indice di carico della macchina accesa (M1) è a un carico di base. Autoscale non mette la macchina M1 in stato di svuotamento a causa del buffer di capacità configurato.

> **Nota:**
>
> Per i gruppi di consegna di sistemi operativi multisessione, tutte le modifiche al desktop vengono

> perse quando gli utenti si scollegano dalle sessioni. Tuttavia, se configurate, le impostazioni specifiche dell'utente vengono spostate insieme al profilo utente.

### Gruppi di consegna casuale di sistemi operativi a sessione singola

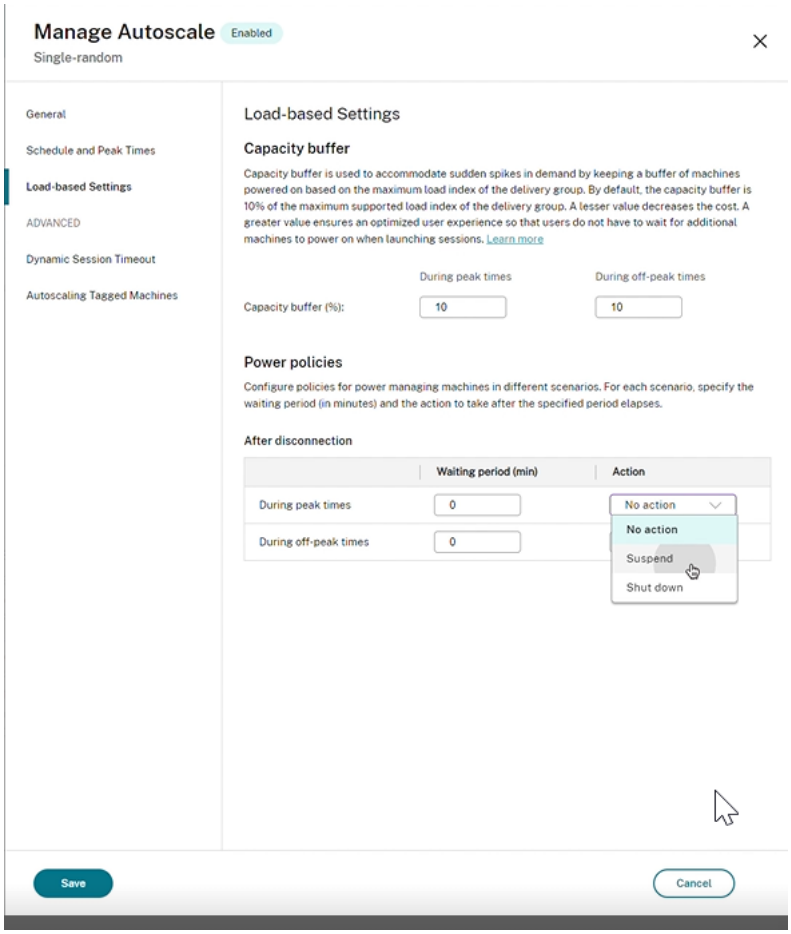
Il buffer di capacità viene utilizzato per gestire i picchi improvvisi della domanda mantenendo un buffer di macchine accese in base al numero totale di macchine incluse nel gruppo di consegna. Per impostazione predefinita, il buffer di capacità è pari al 10% del numero totale di macchine incluse nel gruppo di consegna.

Se il numero di macchine (incluso il buffer di capacità) supera il numero totale di macchine attualmente accese, vengono accese macchine aggiuntive per soddisfare la domanda. Se il numero di macchine (incluso il buffer di capacità) è inferiore al numero totale di macchine attualmente accese, le macchine in eccesso vengono arrestate o sospese, a seconda delle azioni configurate.

#### Criteri di alimentazione

Configurare i criteri per gestire la potenza delle macchine per diversi scenari. Per ciascuno scenario, è possibile specificare il tempo di attesa (in minuti) e l'azione da intraprendere allo scadere del tempo specificato. I criteri di alimentazione sono applicabili ai gruppi di consegna casuale di sistemi operativi a sessione singola e ai gruppi di consegna statici di sistemi operativi a sessione singola.

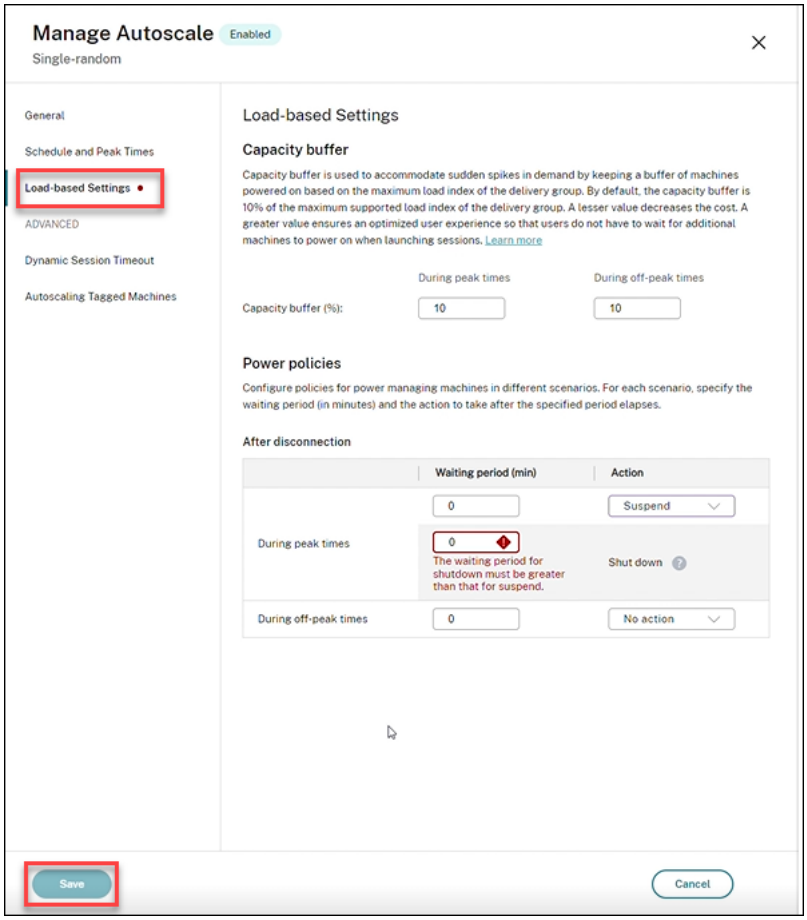



Dopo la disconnessione, le seguenti impostazioni sono applicabili sia nelle ore di punta che in quelle non di punta:

- È possibile impostare il tempo di attesa in minuti e azioni come nessuna azione, sospensione o arresto dal menu a discesa.
- Se si seleziona l'azione di sospensione, configurare un tempo di attesa aggiuntivo per arrestare la macchina.

> **Nota:**
>
> - Durante le ore di punta e non di punta, il tempo di attesa per l'azione di arresto deve essere superiore al tempo di attesa per la sospensione.
> - Le macchine sospese sono accessibili solo agli utenti disconnessi quando si riconnettono. Per rendere le macchine sospese disponibili ai nuovi utenti, arrestarle.
> - Se le impostazioni dell'ora nei campi di sospensione e chiusura sono configurate in modo incorretto, l'opzione **Save** è disabilitata e accanto agli elementi di navigazione viene visualizzato anche un punto rosso che indica gli errori di impostazione.




Ad esempio

- Se si imposta il tempo di attesa su 12 minuti e si sceglie la prima azione come nessuna azione, dopo la fine dei 12 minuti, la macchina rimarrà accesa.
- Se si imposta il tempo di attesa su 15 minuti e si sceglie come prima azione la sospensione e il secondo tempo di attesa su 20 minuti, dopo la fine dei 15 minuti, la macchina verrà sospesa. Dopo la fine del secondo tempo di attesa, la macchina verrà arrestata.
- Se si imposta il tempo di attesa su 18 minuti e si sceglie come prima azione l'arresto, dopo la fine dei 18 minuti, la macchina verrà arrestata.

### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del gruppo di consegna**. Il gruppo di consegna la cui alimentazione si desidera venga gestita da Autoscale contiene 10 macchine (da M1 a M10).
- **Configurazione di Autoscale**
  - Il buffer di capacità è impostato al 10%.

  - Nessuna macchina è inclusa nella pianificazione selezionata.

Lo scenario viene eseguito nella seguente sequenza:

1. Nessun utente effettua l'accesso.
2. Le sessioni utente aumentano.
3. Vengono avviate altre sessioni utente.
4. Il carico della sessione utente diminuisce a causa della chiusura della sessione.
5. Il carico della sessione utente diminuisce ulteriormente fino a quando il carico della sessione non viene gestito solo da risorse locali.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

- Nessun carico utente (stato iniziale)
  - Viene accesa una macchina (M1). La macchina viene accesa a causa del buffer di capacità configurato. In questo caso, 10 (numero di macchine) x 10% (buffer di capacità configurato) equivale a 1. Pertanto, viene accesa una macchina.
- Un primo utente esegue l'accesso
  - La prima volta che un utente esegue l'accesso per utilizzare un desktop, gli viene assegnato un desktop che fa parte di un pool di desktop ospitati su macchine accese. In questo caso, all'utente viene assegnato un desktop proveniente dalla macchina M1.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M2) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un secondo utente esegue l'accesso
  - All'utente viene assegnato un desktop proveniente dalla macchina M2.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M3) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un terzo utente esegue l'accesso
  - All'utente viene assegnato un desktop proveniente dalla macchina M3.
  - Autoscale inizia ad accendere una macchina aggiuntiva (M4) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un utente si scollega
  - Dopo lo scollegamento di un utente o il timeout del desktop dell'utente, la capacità liberata (ad esempio M3) è disponibile come buffer. Di conseguenza, Autoscale inizia a spegnere la macchina M4 perché il buffer di capacità è configurato al 10%.
- Altri utenti si scollegano finché non ci sono più utenti

- Dopo che più utenti si sono scollegati, Autoscale spegne le macchine (ad esempio M2 o M3).
- Anche se non ci sono più utenti, Autoscale non spegne la macchina rimanente (ad esempio M1) perché quella macchina è riservata come capacità di riserva.

> **Nota:**
>
> Per i gruppi di consegna casuali di sistemi operativi a sessione singola, tutte le modifiche al desktop vengono perse quando gli utenti si scollegano dalle sessioni. Tuttavia, se configurate, le impostazioni specifiche dell'utente vengono spostate insieme al profilo utente.

### Gruppi di consegna statici di sistemi operativi a sessione singola

Il buffer di capacità viene utilizzato per gestire i picchi improvvisi della domanda mantenendo un buffer di macchine accese non assegnate in base al numero totale di macchine non assegnate incluse nel gruppo di consegna. Per impostazione predefinita, il buffer di capacità è pari al 10% del numero totale di macchine non assegnate incluse nel gruppo di consegna.

> **Importante:**
>
> Dopo che tutte le macchine del gruppo di consegna sono state assegnate, il buffer di capacità non svolge un ruolo nell'accensione o nello spegnimento delle macchine.

Se il numero di macchine (incluso il buffer di capacità) supera il numero totale di macchine attualmente accese, altre macchine non assegnate vengono accese per soddisfare la domanda. Se il numero di macchine (incluso il buffer di capacità) è inferiore al numero totale di macchine attualmente accese, le macchine in eccesso vengono spente o sospese, a seconda delle azioni configurate.

Per i gruppi di consegna statici di sistemi operativi a sessione singola, Autoscale:

- Accende le macchine assegnate durante le ore di punta e si spegne durante le ore non di punta solo quando la proprietà `AutomaticPowerOnForAssigned` del gruppo di consegna di sistemi operativi a sessione singola applicabile è impostata su true.
- Accende automaticamente una macchina nelle ore di punta se è spenta e la proprietà `AutomaticPowerOnForAssignedDuringPeak` del gruppo di consegna a cui appartiene è impostata su true.

Per capire come funziona il buffer di capacità con le macchine assegnate, considerare quanto segue:

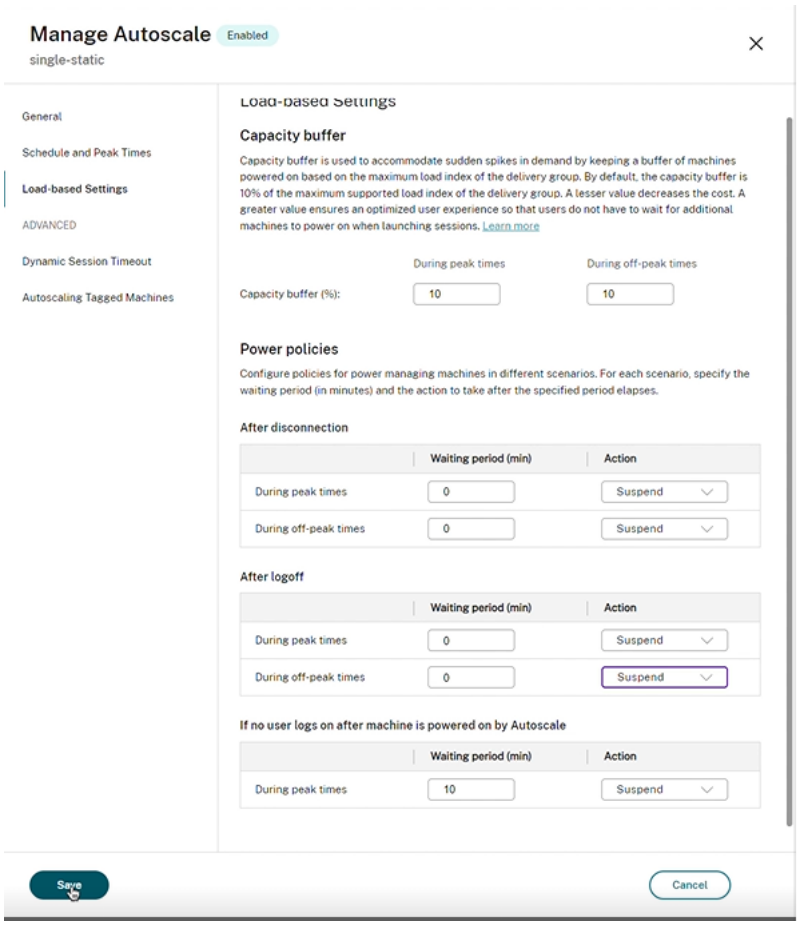
- Il buffer di capacità funziona solo quando il gruppo di consegna ha una o più macchine non assegnate.
- Se il gruppo di consegna non ha macchine non assegnate (tutte le macchine nel gruppo di consegna sono state assegnate), il buffer di capacità non svolge un ruolo nell'accensione o nello spegnimento delle macchine.

- La proprietà `AutomaticPowerOnForAssignedDuringPeak` determina se le macchine assegnate vengono accese durante le ore di punta. Se è impostato su true, Autoscale mantiene le macchine accese durante le ore di punta. Autoscale le accende anche se sono spente.

### Criteri di alimentazione

Configurare i criteri per gestire la potenza delle macchine per diversi scenari. Per ciascuno scenario, è possibile specificare il tempo di attesa (in minuti) e l'azione da intraprendere allo scadere del tempo specificato. I criteri di alimentazione sono applicabili ai gruppi di consegna casuale di sistemi operativi a sessione singola e ai gruppi di consegna statici di sistemi operativi a sessione singola.




In **After disconnection** (Dopo la disconnessione) e **After logoff** (Dopo lo scollegamento), le seguenti impostazioni sono applicabili sia nelle ore di punta che in quelle non di punta:
è possibile impostare il tempo di attesa in minuti e azioni quali nessuna azione, sospensione o spegnimento dal menu a discesa.

**Se nessun utente effettua l'accesso dopo l'accensione della macchina tramite Autoscale**, le seguenti impostazioni sono applicabili solo nelle ore di punta:
È possibile impostare il tempo di attesa in minuti e azioni quali nessuna azione, sospensione o

spegnimento dal menu a discesa durante le ore di punta.

#### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del gruppo di consegna**. Il gruppo di consegna la cui alimentazione si desidera venga gestita da Autoscale contiene 10 macchine (da M1 a M10).
- **Configurazione di Autoscale**
  - Le macchine da M1 a M3 sono assegnate e le macchine da M4 a M10 non sono assegnate.
  - Buffer di capacità impostato al 10% per le ore di punta e non di punta.
  - Secondo il programma selezionato, l'alimentazione Autoscale gestisce le macchine tra le 09:00 e le 18:00.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

- Inizio del programma —09:00
  - Autoscale accende le macchine da M1 a M3.
  - Autoscale accende una macchina aggiuntiva (ad esempio M4) a causa del buffer di capacità configurato. La macchina M4 non è assegnata.
- Un primo utente esegue l'accesso
  - La prima volta che un utente esegue l'accesso per utilizzare un desktop, gli viene assegnato un desktop che fa parte di un pool di desktop ospitati su macchine accese non assegnate. In questo caso, all'utente viene assegnato un desktop proveniente dalla macchina M4. Gli accessi successivi di tale utente si connettono allo stesso desktop assegnato al primo utilizzo.
  - Autoscale inizia ad accendere una macchina aggiuntiva (ad esempio M5) per soddisfare la domanda a causa del buffer di capacità configurato.
- Un secondo utente esegue l'accesso
  - All'utente viene assegnato un desktop proveniente dalle macchine accese non assegnate. In questo caso, all'utente viene assegnato un desktop proveniente dalla macchina M5. Gli accessi successivi di tale utente si connettono allo stesso desktop assegnato al primo utilizzo.
  - Autoscale inizia ad accendere una macchina aggiuntiva (ad esempio M6) per soddisfare la domanda a causa del buffer di capacità configurato.
- Gli utenti si scollegano

  - Quando gli utenti si scollegano dai propri desktop o questi vanno in timeout, Autoscale mantiene accese le macchine da M1 a M5 nel periodo fra le 09:00 le 18:00. Quando questi utenti eseguono l'accesso la volta successiva, si connettono allo stesso desktop assegnato al primo utilizzo.
  - La macchina non assegnata M6 è in attesa di servire un desktop a un utente non assegnato in arrivo.

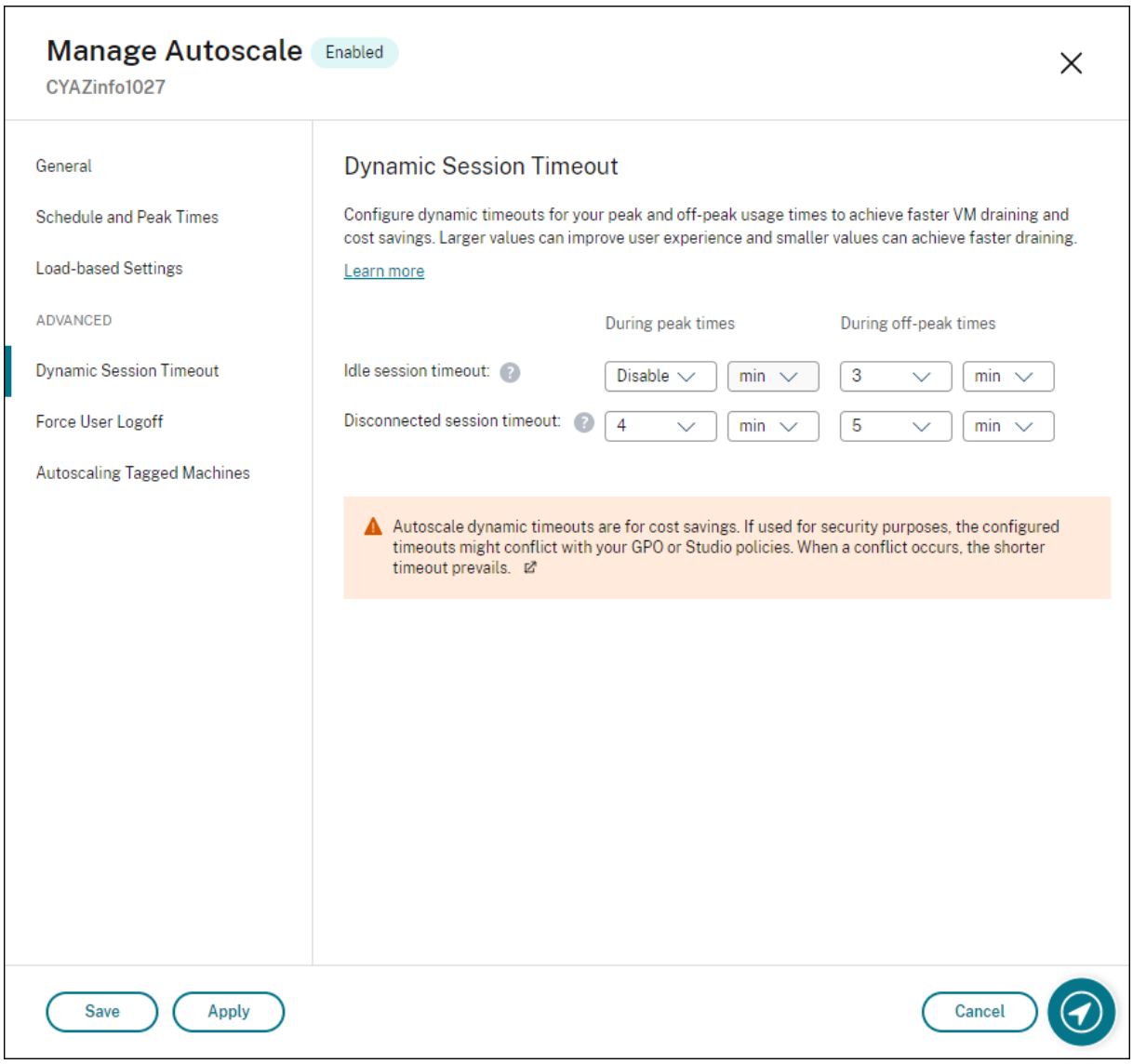
- Fine della pianificazione: 18:00
  - Alle 18:00, Autoscale spegne le macchine da M1 a M5.
  - Autoscale mantiene accesa la macchina non assegnata M6 a causa del buffer di capacità configurato. Quella macchina è in attesa di servire un desktop a un utente non assegnato in arrivo.
  - Nel gruppo di consegna, le macchine da M6 a M10 sono macchine non assegnate.

## Timeout dinamici delle sessioni

June 20, 2023

Questa funzione consente di configurare timeout di sessione disconnessa e inattiva per le ore di utilizzo di punta e non di punta per ottenere uno svuotamento della macchina più rapido e risparmi sui costi. Questa funzionalità si applica alle macchine con sistema operativo a sessione singola e multisessione. Un VDA segnala i tempi di inattività per le sessioni che sono rimaste inattive per più di 10 minuti, quindi i timeout dinamici delle sessioni non saranno in grado di disconnettere le sessioni inattive prima di 10 minuti di inattività. Un valore inferiore rimuove prima le sessioni persistenti, riducendo così i costi.

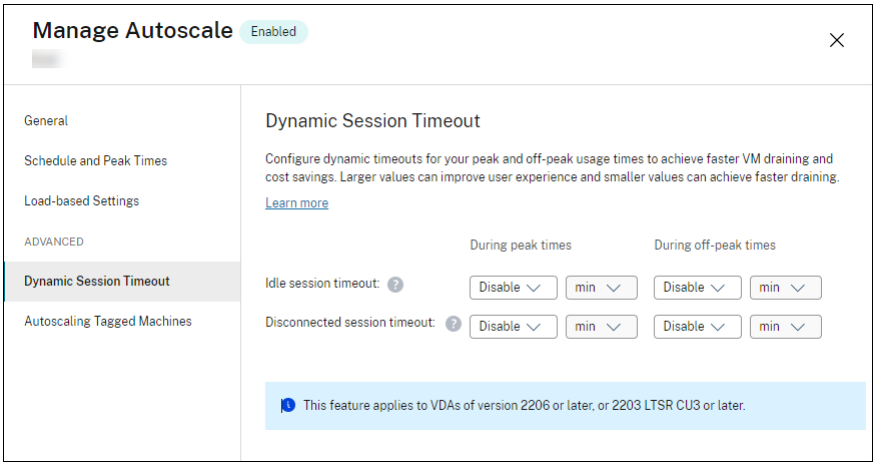
 




**Nota:**

- Questa funzionalità è sempre disponibile per i gruppi di consegna con sistema operativo multisessione.
- Per i gruppi di consegna di sistemi operativi a sessione singola, questa funzionalità si applica ai VDA della versione 2206 CR o successiva o 2203 LTSR CU3 o successiva. Verificare che i VDA siano stati registrati su Citrix Cloud almeno una volta. Quando non è disponibile, viene visualizzata la seguente interfaccia utente:



(Timeout dinamico della sessione non disponibile)

- I timeout dinamici di Autoscale consentono di risparmiare sui costi. Se utilizzati per scopi di sicurezza, i timeout configurati potrebbero entrare in conflitto con l'oggetto Criteri di gruppo o i criteri della console Manage. Quando si verifica un conflitto, prevale il timeout più breve.

**Timeout della sessione inattiva**. Abilita o disabilita un timer che specifica per quanto tempo viene mantenuta ininterrotta una connessione utente in assenza di input da parte dell'utente. Quando il timer scade, la sessione viene posizionata nello stato disconnesso e si applica il **Disconnected session timeout** (Tempo di scadenza di una sessione disconnessa). Se l'opzione **Disconnected session timeout** è disabilitata, la sessione non viene disconnessa.

**Importante:**

- Se si specifica un valore inferiore o uguale a 10 minuti (600 secondi), Autoscale disconnette le sessioni pertinenti dopo che sono rimaste inattive per 10 minuti. Questo perché Autoscale si basa sui tempi di inattività delle sessioni riportati dai VDA. I VDA segnalano i tempi di inattività solo per le sessioni che sono rimaste inattive per più di 10 minuti.
- Una sessione inattiva verrà comunque messa in uno stato di disconnessione se l'utente interagisce con essa negli ultimi 5 minuti dal raggiungimento del timeout della sessione inattiva.

**Disconnected session timeout**. Abilita o disabilita un timer che specifica per quanto tempo un desktop disconnesso debba rimanere bloccato prima che la sessione venga terminata. Se è abilitato, la sessione disconnessa viene terminata alla scadenza del timer.

## Scalabilità automatica delle macchine con tag (cloud burst)

March 3, 2023

> **Nota:**
>
> Questa funzionalità in precedenza era chiamata Restrict Autoscale (Limita Autoscale).

## Introduzione

Autoscale offre la flessibilità necessaria per gestire solo un sottoinsieme di macchine di un gruppo di consegna. Per raggiungere questo obiettivo, applicare un tag a una o più macchine e quindi configurare Autoscale per gestire solo le macchine con tag.

Questa funzione può essere utile nei casi d'uso del cloud bursting, in cui si desidera utilizzare risorse locali (o istanze di cloud pubblico riservate) per gestire i carichi di lavoro prima che le risorse basate sul cloud soddisfino la domanda aggiuntiva (ovvero carichi di lavoro burst). Per consentire alle macchine locali (o alle istanze riservate) di affrontare prima i carichi di lavoro, è necessario utilizzare la restrizione tag insieme alla preferenza di zona.

La restrizione tag specifica che le macchine devono avere l'alimentazione gestita da Autoscale. La preferenza di zona specifica i computer presenti nella zona preferita che gestiscono le richieste di avvio degli utenti. Per maggiori informazioni, vedere Tag e Preferenza di zona.

Per la scalabilità automatica di determinate macchine con tag, è possibile utilizzare la console Manage (Gestione) o PowerShell.

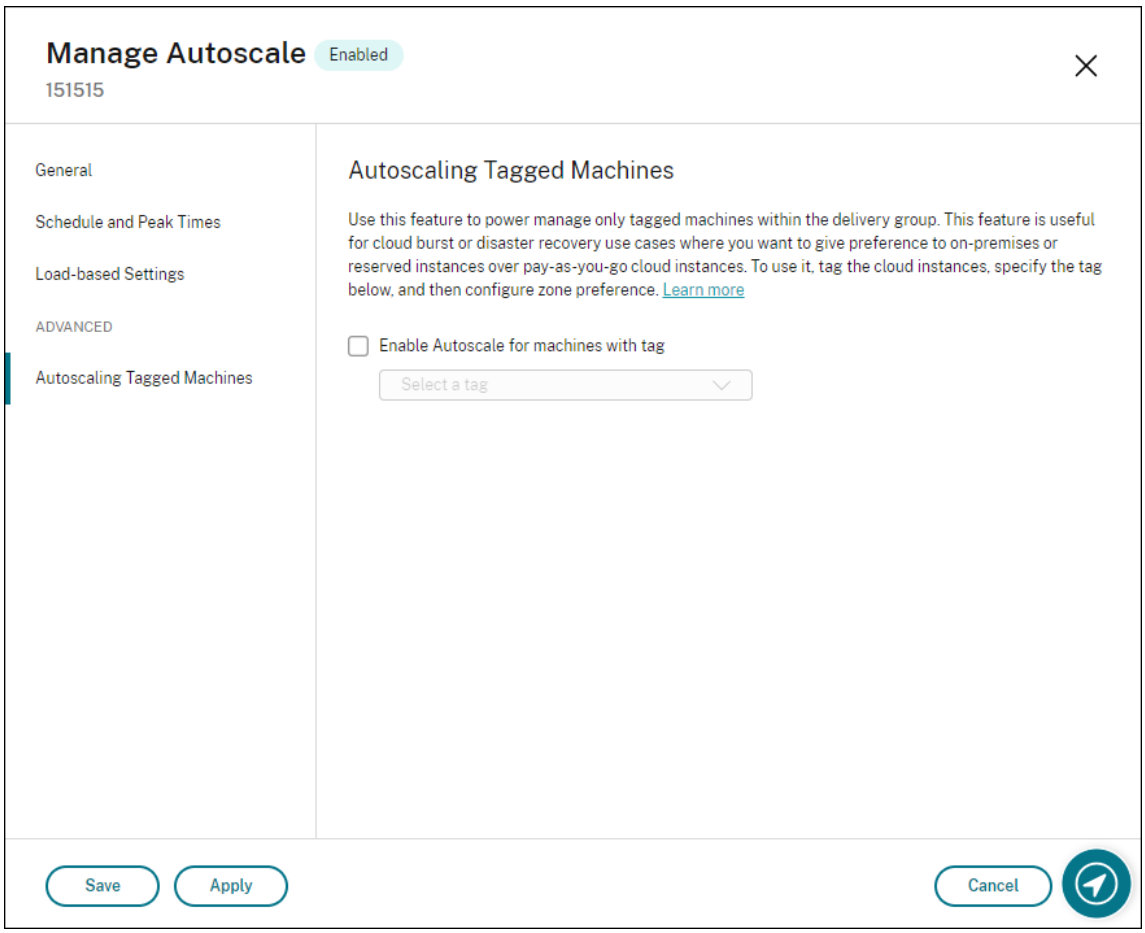
## Utilizzare la console Manage (Gestione) per scalare automaticamente determinate macchine con tag

Per scalare automaticamente alcune macchine con tag, completare i seguenti passaggi:

1. Creare un tag e applicarlo alle macchine pertinenti del gruppo di consegna. Per maggiori informazioni, vedere Gestire i tag e le restrizioni tag.
2. Selezionare il gruppo di consegna e quindi aprire la procedura guidata **Manage Autoscale**.
3. Nella pagina **Autoscaling Tagged Machines** (Scalabilità automatica delle macchine con tag), selezionare **Enable Autoscale for machines with tag** (Abilita Autoscale per le macchine con tag), selezionare un tag dall'elenco, quindi fare clic su **Apply** (Applica) per salvare le modifiche.

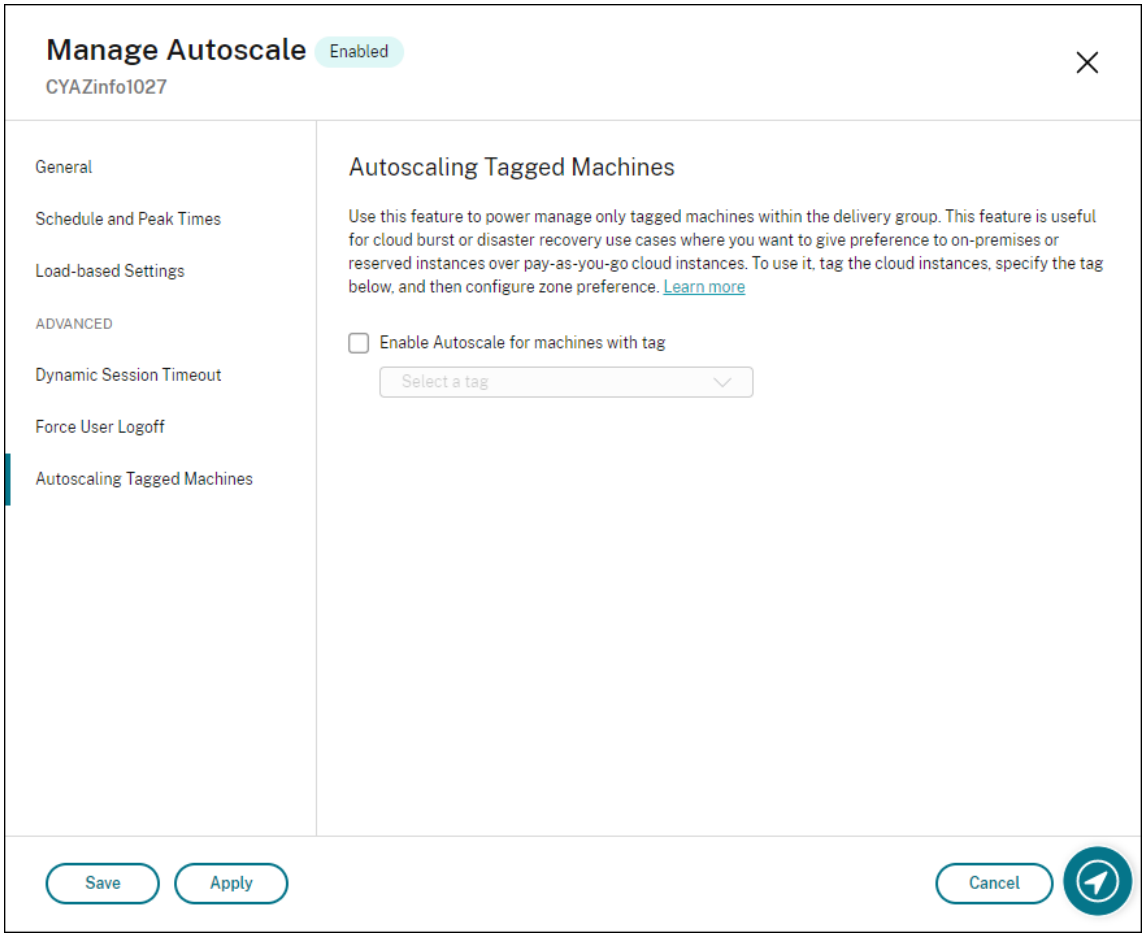
   Interfaccia utente per gruppi di consegna *statici* e *casuali* dei sistemi operativi a sessione singola:




Interfaccia utente per *gruppi di consegna di sistemi operativi multisessione*:




> **Avviso:**
>
> - La scalabilità automatica delle macchine con un tag specifico potrebbe causare l'aggiornamento automatico dell'istogramma per riflettere il numero di macchine in base al tag. Nella pagina **Schedule and Peak Times** (Pianificazione e orari di punta), è possibile assegnare manualmente le macchine rispetto a ogni fascia oraria, se necessario.
> - Non è possibile eliminare un tag che viene utilizzato sulle macchine con tag. Per eliminare il tag, è necessario prima rimuovere la limitazione tag.

Dopo aver applicato la limitazione tag, in un secondo momento si potrebbe decidere di rimuoverla dal gruppo di consegna. A tale scopo, andare alla pagina **Manage Autoscale > Autoscaling Tagged Machines** (Gestisci scalabilità automatica > Scalabilità automatica macchine con tag) e quindi deselezionare **Enable Autoscale for machines with tag** (Abilita Autoscale per macchine con tag).

> **Avviso:**
>
> - Se si rimuove il tag dalle macchine interessate senza deselezionare **Enable Autoscale for machines with tag** (Abilita Autoscale per macchine con tag), si potrebbe ricevere un avviso

> quando si apre la procedura guidata **Manage Autoscale** (Gestici Autoscale). Rimuovendo i tag dalle macchine, potrebbero non rimanere macchine da gestire con Autoscale perché il tag specificato in Autoscale è diventato non valido. Per risolvere l'avviso, andare alla pagina **Autoscaling Tagged Machines** (Scalabilità automatica delle macchine con tag), rimuovere il tag non valido, quindi fare clic su **Apply** (Applica) per salvare le modifiche.

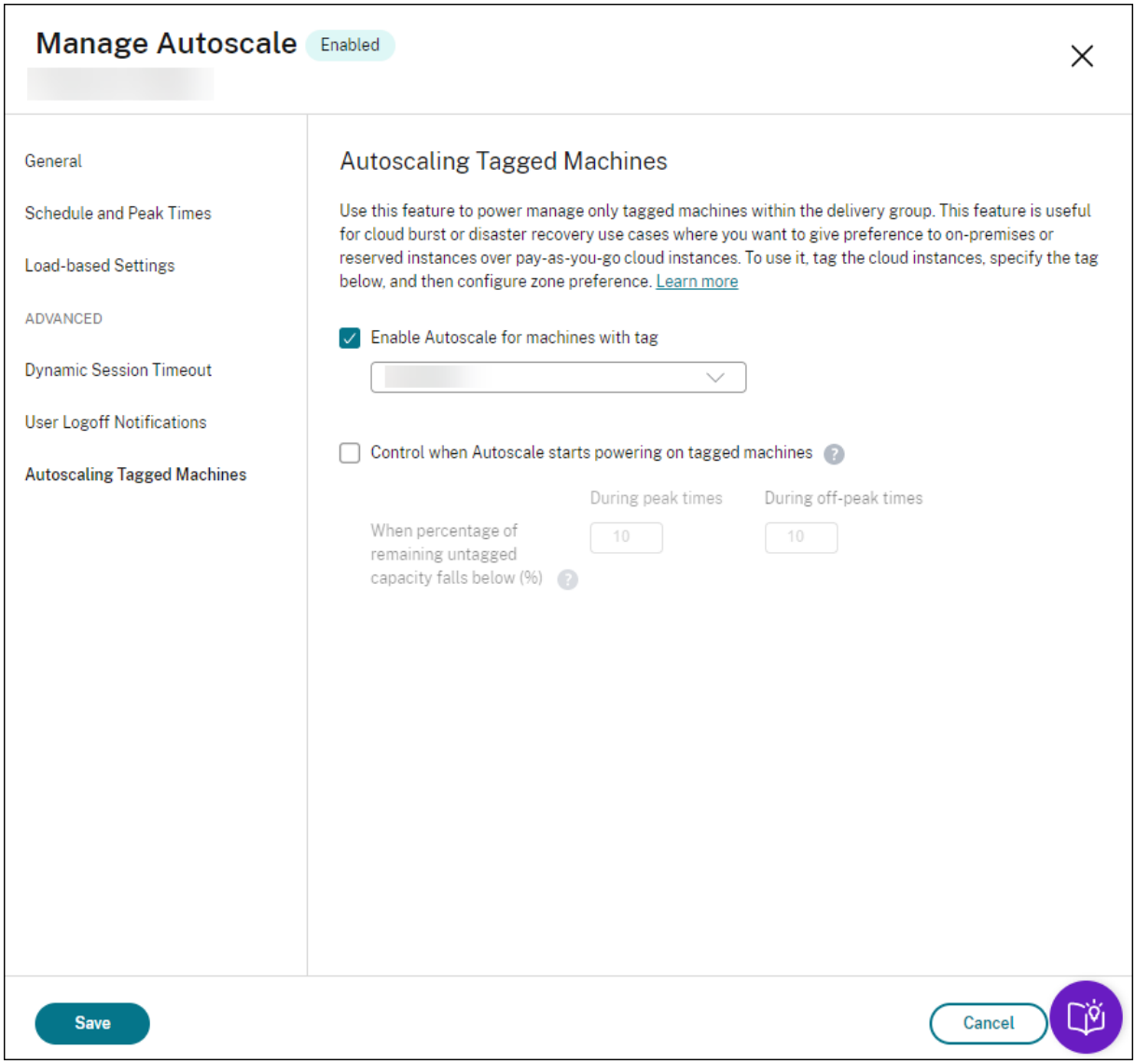
#### Controllare quando Autoscale attiva le risorse

È anche possibile controllare quando Autoscale inizia ad attivare le macchine con tag in base all'utilizzo di macchine senza tag. Ciò consente di ottimizzare ulteriormente il consumo dei carichi di lavoro del cloud pubblico o con tag.

A tale scopo, completare i seguenti passaggi:

1. Nella pagina **Autoscaling Tagged Machines** (Scalabilità automatica delle macchine con tag), selezionare **Control when Autoscale starts powering on tagged machines** (Controlla quando Autoscale inizia ad attivare le macchine con tag).
2. Immettere la quantità percentuale di utilizzo delle macchine senza tag che si desidera raggiungere sia per le ore di punta che per le ore non di punta, quindi fare clic su **Apply** (Applica). Valori supportati: 0-100.




(Controlla quando Autoscale inizia ad attivare le macchine con tag)

> **Suggerimento:**
>
> La percentuale controlla quando Autoscale inizia ad accendere i computer con tag. Quando la percentuale scende al di sotto della soglia (impostazione predefinita 10%), Autoscale inizia ad accendere i computer con tag. Quando la percentuale supera la soglia, Autoscale passa alla modalità di spegnimento. Quando si inserisce la percentuale, considerare due scenari:
>
> - Per gruppi di consegna con sistema operativo a sessione singola: il valore è definito come percentuale del numero totale di macchine senza tag in stato di inattività. Esempio: ci sono 10 macchine con sistema operativo a sessione singola senza tag. Quando ne rimane solo una senza sessione, Autoscale avvia l'accensione di una macchina con tag.
> - Per i gruppi di distribuzione con sistema operativo multisessione: il valore è definito come

> percentuale della capacità totale (in termini di indice di carico) delle macchine senza tag disponibili. Esempio: ci sono 10 macchine con sistema operativo multisessione senza tag. Quando sono caricate al 90%, Autoscale avvia l'alimentazione di una macchina con tag.

### Utilizzare PowerShell per scalare automaticamente alcune macchine con tag

Per utilizzare direttamente l'SDK di PowerShell, completare i seguenti passaggi:

1. **Creare un tag.** Utilizzare il comando PowerShell New-Brokertag per creare un tag.
   - Ad esempio: `$managed = New-BrokerTag Managed`. In questo caso, il tag è denominato "Managed". Per ulteriori informazioni sul comando PowerShell New-Brokertag, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Applicare il tag alle macchine**. Utilizzare il comando PowerShell Get-Brokermachine per applicare il tag alle macchine di un catalogo da sottoporre alla gestione dell'alimentazione con Autoscale.
   - Ad esempio: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. In questo caso, il catalogo è denominato "cloud".
   - Per ulteriori informazioni sul comando PowerShell Get-Brokermachine, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Nota:**
   >
   > È possibile aggiungere nuove macchine al catalogo dopo aver applicato il tag. Il tag *NON* viene applicato automaticamente a quelle nuove macchine.

3. **Aggiungere macchine con tag al gruppo di consegna da sottoporre alla gestione dell'alimentazione con Autoscale.** Utilizzare il comando PowerShell Get-BrokerDesktopGroup per aggiungere una restrizione tag al gruppo di consegna che contiene le macchine (in altre parole, "limitare i lanci alle macchine con tag X").
   - Ad esempio: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. In questo caso, l'UID del gruppo di consegna è 1.
   - Per ulteriori informazioni sul comando Get-BrokerDesktopGroup PowerShell, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Dopo aver applicato la limitazione tag, in un secondo momento si potrebbe decidere di rimuoverla dal gruppo di consegna. A tale scopo, utilizzare il comando PowerShell Get-BrokerDesktopGroup.

Esempio: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscal $null`. In questo caso, l'UID del gruppo di consegna è 1.

> **Nota:**
>
> I computer senza tag si riavviano automaticamente dopo che gli utenti li hanno spenti Questo comportamento garantisce che si rendano disponibili più presto per gestire i carichi di lavoro. Questo può essere abilitato o disabilitato su un gruppo per desktop utilizzando la proprietà `AutomaticRestartForUntaggedMachines` di `Set-BrokerDesktopGroup`. Per ulteriori informazioni, vedere https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

### Esempio di scenario

Supponiamo di avere il seguente scenario:

- **Configurazione del catalogo di macchine**. Esistono due cataloghi di macchine (C1 e C2).
  - Il catalogo C1 contiene 5 macchine (da M1 a M5) che sono locali nelle distribuzioni locali.
  - Il catalogo C2 contiene 5 macchine (da M6 a M10) che sono remote nelle distribuzioni cloud.
- **Restrizioni tag**. Viene creato Un tag denominato "Cloud", che viene applicato alle macchine da M6 a M10 del catalogo C2.
- **Configurazione della zona**. Vengono create due zone (Z1 e Z2).
  - La zona Z1 contenente il catalogo C1 corrisponde alle distribuzioni locali.
  - La zona Z2 contenente il catalogo C2 corrisponde alle distribuzioni cloud.
- **Configurazione del gruppo di consegna**
  - Il gruppo di consegna contiene 10 macchine (da M1 a M10), 5 macchine dei cataloghi C1 (da M1 a M5) e 5 del catalogo C2 (da M6 a M10).
  - Le macchine da M1 a M5 vengono accese manualmente e rimangono accese per tutta la durata della programmazione.
- **Configurazione di Autoscale**
  - Il buffer di capacità è impostato al 10%.
  - Autoscale gestisce l'alimentazione delle sole macchine con il tag "Cloud". In questo caso, Autoscale gestisce l'alimentazione delle macchine cloud da M6 a M10.
- **Configurazione dell'applicazione o del desktop pubblicati**. Le preferenze di zona sono configurate per i desktop pubblicati (ad esempio), dove la Zona Z1 è preferita rispetto alla Zona Z2 per una richiesta di avvio dell'utente.

  - La zona Z1 è configurata come zona preferita (zona home) per i desktop pubblicati.

Lo scenario viene eseguito nella seguente sequenza:

1. Nessun utente effettua l'accesso.
2. Le sessioni utente aumentano.
3. Le sessioni utente aumentano ulteriormente fino a quando non vengono consumate tutte le macchine locali disponibili.
4. Vengono avviate altre sessioni utente.
5. La sessione utente diminuisce a causa della chiusura della sessione.
6. La sessione utente diminuisce ulteriormente fino a quando il carico della sessione non viene gestito solo da macchine locali.

Vedere sotto per i dettagli di come funziona Autoscale nello scenario di cui sopra.

- Nessun carico utente (stato iniziale)
  - Le macchine locali da M1 a M5 sono tutte accese.
  - Una macchina del cloud (ad esempio M6) viene accesa. La macchina viene accesa a causa del buffer di capacità configurato. In questo caso, 10 (numero di macchine) x 10.000 (indice di carico) x 10% (buffer di capacità configurato) equivale a 10.000. Pertanto, viene accesa una macchina.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M6) è a un carico di base (l'indice di carico è uguale a 0).
- Gli utenti effettuano l'accesso
  - Le sessioni sono indirizzate a essere ospitate su macchine da M1 a M5 tramite la preferenza di zona configurata e sono bilanciate dal carico su queste macchine locali.
  - Il valore dell'indice di carico delle macchine accese (da M1 a M5) aumenta.
  - Il valore dell'indice di carico della macchina accesa M6 è a un carico di base.
- Gli utenti aumentano il carico, consumando tutte le risorse locali
  - Le sessioni sono indirizzate a essere ospitate sulle macchine da M1 a M5 tramite la preferenza di zona configurata e il loro carico viene distribuito in modo equilibrato su queste macchine locali.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.
  - Il valore dell'indice di carico della macchina accesa M6 rimane a un carico di base.
- Un altro utente accede
  - La sessione supera la preferenza di zona e viene indirizzata a essere ospitata sulla macchina cloud M6.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.

  - Il valore dell'indice di carico della macchina accesa M6 aumenta e non è più a un carico di base. Quando la capacità di riserva totale scende a un livello inferiore a 10.000 in termini di indice di carico, Autoscale inizia ad accendere una macchina aggiuntiva (M7) per soddisfare la domanda, dato il buffer di capacità configurato. Si noti che potrebbe essere necessario del tempo per accendere la macchina M7. Quindi potrebbe esserci un ritardo fino a quando la macchina M7 non sarà pronta.

- Accedono altri utenti
  - Le sessioni vengono indirizzate a essere ospitate sulla macchina M6.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.
  - Il valore dell'indice di carico della macchina accesa M6 aumenta ulteriormente, ma la capacità di riserva totale è a un livello superiore a 10.000 in termini di indice di carico.
  - Il valore dell'indice di carico della macchina accesa M7 rimane a un carico di base.

- Accedono ancora più utenti
  - Dopo che la macchina M7 è pronta, le sessioni vengono indirizzate a essere ospitate sulle macchine M6 e M7 e il carico viene distribuito fra queste macchine.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) ha raggiunto 10.000.
  - Il valore dell'indice di carico della macchina M7 non è più a un carico di base.
  - Il valore dell'indice di carico delle macchine accese (M6 e M7) aumenta.
  - La capacità di riserva totale è ancora a un livello superiore a 10.000 in termini di indice di carico.

- Il carico della sessione utente diminuisce a causa della chiusura della sessione
  - Dopo che gli utenti si sono disconnessi dalle sessioni o dopo il timeout delle sessioni inattive, la capacità che si è liberata sulle macchine da M1 a M7 viene riutilizzata per ospitare sessioni avviate da altri utenti.
  - Quando la capacità di riserva totale aumenta fino a un livello superiore a 10.000 in termini di indice di carico, Autoscale mette una delle macchine cloud (da M6 a M7) in stato di svuotamento. Di conseguenza, le sessioni avviate da altri utenti non vengono più indirizzate a quella macchina (ad esempio M7) a meno che non vi siano nuovi cambiamenti; ad esempio se il carico dell'utente aumenta nuovamente o altre macchine cloud hanno un carico inferiore.

- Il carico della sessione utente diminuisce ulteriormente fino a quando una o più macchine cloud non sono più necessarie
  - Dopo che tutte le sessioni sulla macchina M7 sono terminate e il ritardo di spegnimento specificato è scaduto, Autoscale spegne la macchina M7.
  - Il valore dell'indice di carico di tutte le macchine accese (da M1 a M5) potrebbe scendere a un livello inferiore a 10.000.

  - Il valore dell'indice di carico della macchina accesa (M6) diminuisce.

- La sessione utente diminuisce ulteriormente fino a quando non sono necessarie macchine cloud.
  - Anche se non ci sono sessioni utente sulla macchina M6, Autoscale non la spegne perché è riservata come capacità di riserva.
  - Autoscale mantiene accesa la rimanente macchina cloud M6 dato il buffer di capacità configurato. Quella macchina è in attesa di servire un desktop a un utente in arrivo.
  - Le sessioni non sono indirizzate a essere ospitate sulla macchina M6 fintanto che le macchine locali hanno capacità disponibile.

## Provisioning dinamico delle macchine

November 28, 2022

Autoscale offre la possibilità di creare macchine ed eliminarle dinamicamente. È possibile sfruttare questa funzionalità utilizzando uno script PowerShell. Lo script consente di aumentare o diminuire dinamicamente il numero di macchine incluse nel gruppo di consegna in base alle condizioni di carico correnti.

Lo script offre i seguenti vantaggi (e non solo):

- **Riduzione dei costi di archiviazione**. Diversamente da Autoscale, che aiuta a ridurre i costi di elaborazione, lo script fornisce una soluzione più economica per il provisioning delle macchine.
- **Gestione efficace delle variazioni di carico**. Lo script consente di gestire le modifiche al carico aumentando o diminuendo automaticamente il numero di macchine in base al carico del gruppo di consegna corrente.

### Scarica lo script

Lo script PowerShell è disponibile all'indirizzo https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs.

### Come funziona lo script

> **Importante:**
>
> - Non è possibile specificare un catalogo macchine in più di un gruppo di consegna che deve essere gestito dallo script. In altre parole, se più gruppi di consegna condividono lo stesso

> catalogo macchine, lo script non funziona con nessuno di questi gruppi di consegna.
> - Non è possibile eseguire contemporaneamente lo script per lo stesso gruppo di consegna da più posizioni.

Lo script funziona a livello di gruppo di consegna. Misura il carico (in termini di indice di carico) e quindi determina se creare o eliminare macchine.

Le macchine create tramite questo script sono dotate di tag univoci (tramite il parametro `ScriptTag`) in modo che possano essere identificate in seguito. La creazione o l'eliminazione di macchine si basa su:

- **Carico percentuale massimo di un gruppo di consegna**. Specifica il livello massimo al quale creare macchine per le quali Autoscale affronta i carichi aggiuntivi. Quando questa soglia viene superata, vengono create macchine in batch per garantire che il carico corrente diminuisca fino o al di sotto della soglia.
- **Carico percentuale minimo di un gruppo di consegna**. Specifica il livello minimo al quale eliminare le macchine create tramite questo script che non hanno sessioni attive. Quando questa soglia viene superata, le macchine create tramite questo script che non hanno sessioni attive vengono eliminate.

Questo script ha lo scopo di effettuare il monitoraggio di un intero gruppo di consegna e di creare o eliminare macchine quando viene soddisfatto il criterio di attivazione. Viene eseguito per ogni esecuzione. Ciò significa che è necessario eseguire lo script regolarmente in modo che possa funzionare come previsto. Si consiglia di eseguire lo script a un intervallo minimo di cinque minuti. In questo modo si migliora la reattività complessiva.

Lo script si basa sui seguenti parametri per funzionare:

| Parametro | Tipo | Valore predefinito | Descrizione |
| --- | --- | --- | --- |
| DeliveryGroupName | Stringa | X | Nome del gruppo di consegna da monitorare per determinare il carico corrente. È possibile fornire un elenco di nomi separati da punto e virgola. Ad esempio: `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`. |
| XdProfileName | Stringa | X | Nome del profilo da utilizzare per l'autenticazione su server remoti. Per informazioni dettagliate sull'autenticazione su server remoti utilizzando questo parametro, vedere Authentication API. |
| HighWatermark | Intero | 80 | Carico percentuale massimo (in termini di indice di carico) al quale creare macchine per le quali Autoscale affronti i carichi aggiuntivi. |

| Parametro | Tipo | Valore predefinito | Descrizione |
|---|---|---|---|
| LowWatermark | Intero | 15 | Carico percentuale minimo (in termini di indice di carico) al quale eliminare le macchine create tramite questo script che non hanno sessioni attive. |
| MachineCatalogName | Stringa | X | Nome del catalogo macchine in cui devono essere create le macchine. |
| MaximumCreatedMachines | Intero | -1 | Quantità massima di macchine che possono essere create in un gruppo di consegna specificato. Se il valore è uguale o inferiore a 0, lo script non elabora questo parametro. |
| ScriptTag | Stringa | AutoscaledScripted | Tag che si applica alle macchine create tramite lo script. |
| EventLogSource | Stringa | X | Nome di origine visualizzato nel Visualizzatore eventi di Windows. |

> **Nota:**
>
> Una "X"indica che non è specificato alcun valore predefinito per quel parametro.

Per impostazione predefinita, lo script richiede tutti i parametri (tranne il parametro `ScriptTag`) la prima volta che viene eseguito. Nelle esecuzioni successive, sono richiesti solo i parametri `DeliveryGroupName` e `XdProfileName`. Facoltativamente, è possibile scegliere di aggiornare la percentuale minima e massima di carichi.

Si noti che è necessario specificare un singolo gruppo di consegna la prima volta che si esegue lo script. Ad esempio, lo script *non* funziona se si utilizza il seguente comando PowerShell per specificare due

gruppi di consegna la prima volta che si esegue lo script:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Invece, specificare prima un singolo gruppo di consegna (in questo esempio, dg1) usando il seguente comando:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Quindi, utilizzare il seguente comando per eseguire lo script per il secondo gruppo di consegna (in questo esempio, dg 2):

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

### Prerequisiti

Per eseguire lo script, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- La macchina risiede nello stesso dominio in cui vengono create le macchine.
- L'SDK Remote PowerShell è installato su quella macchina. Per ulteriori informazioni sull'SDK Remote PowerShell, vedere SDK e API.
- Altri prerequisiti:
  - Un gruppo di consegna da monitorare
  - Un catalogo macchine creato tramite Machine Creation Services (MCS) a cui è associato uno schema di provisioning (modello)
  - Un pool di identità associato allo schema di provisioning
  - Un'origine del registro eventi da creare in modo che lo script possa scrivere informazioni nel registro eventi di Windows
  - Un client sicuro che consenta di autenticarsi su server remoti

### Autorizzazioni, consigli e avvisi

Quando si esegue lo script, tenere presente quanto segue:

- Per eseguire l'autenticazione su server remoti utilizzando il parametro `XdProfileName`, è necessario definire un profilo di autenticazione utilizzando un client sicuro di accesso API, creato nella console Citrix Cloud. Per i dettagli, vedere Authentication API.

- È necessario disporre delle autorizzazioni per creare ed eliminare account computer in Active Directory.
- Si consiglia di automatizzare lo script PowerShell con l'Utilità di pianificazione di Windows. Per informazioni dettagliate, vedere Creare un'attività automatica utilizzando l'Utilità di pianificazione di Windows.
- Se si desidera che lo script scriva informazioni (ad esempio errori e azioni) nel registro eventi di Windows, è necessario prima specificare un nome di origine utilizzando il cmdlet `New-EventLog`. Ad esempio, `New-EventLog -LogName Application –Source <sourceName>`. È quindi possibile visualizzare gli eventi nel riquadro **Applicazione** del Visualizzatore eventi di Windows.
- Se si sono verificati errori durante l'esecuzione dello script, eseguire lo script manualmente e quindi risolvere i problemi eseguendo controlli dello script.

### API di autenticazione

Prima di eseguire lo script, è necessario definire un profilo di autenticazione utilizzando un client sicuro di accesso API. È necessario creare un client sicuro utilizzando lo stesso account da cui verrà eseguito lo script.

Il client sicuro deve disporre delle seguenti autorizzazioni:

- Creare ed eliminare macchine utilizzando MCS.
- Modificare i cataloghi delle macchine (per aggiungere e rimuovere macchine).
- Modificare i gruppi di consegna (per aggiungere e rimuovere macchine).

Quando si crea un client sicuro, assicurarsi che il proprio account disponga delle autorizzazioni sopra indicate, perché il client sicuro eredita automaticamente le autorizzazioni dal proprio account corrente.

Per creare un client sicuro, completare questi passaggi:

1. Accedere a Citrix Cloud, quindi passare a **Identity and Access Management > API Access**.
2. Digitare il nome del client sicuro e quindi fare clic su **Create client**.

Per autenticarsi su server remoti, utilizzare il comando `Set-XDCredentials` di PowerShell. Ad esempio:

- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

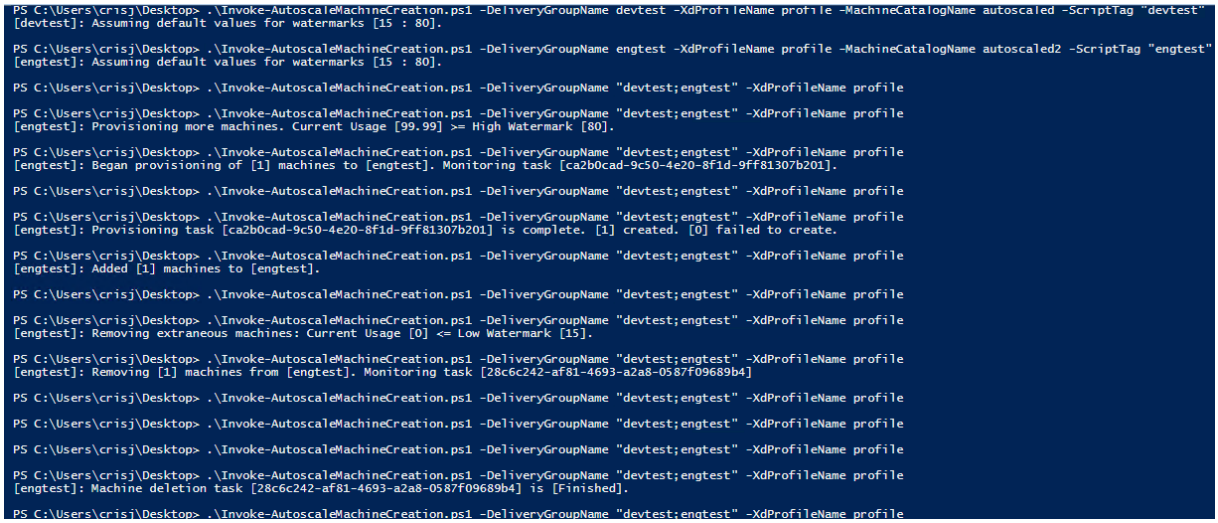
 

### Creare un'attività automatica utilizzando l'Utilità di pianificazione di Windows

È possibile automatizzare lo script PowerShell con l'Utilità di pianificazione di Windows. In questo modo lo script viene eseguito automaticamente a determinati intervalli o quando vengono soddisfatte determinate condizioni. Per eseguire questo script con l'Utilità di pianificazione di Windows, assicurarsi di selezionare **Non avviare una nuova istanza** nella scheda **Crea attività > Impostazioni**. In questo modo si impedisce all'Utilità di pianificazione di Windows di eseguire una nuova istanza dello script se lo script è già in esecuzione.

### Esempio di esecuzione di script

Vedere di seguito un esempio di esecuzione dello script. Si noti che il file di script viene richiamato più volte. In questo esempio, per simulare il carico, viene avviata e quindi terminata una sessione.




### Elenco di controllo di risoluzione dei problemi per lo script

Lo script scrive informazioni (ad esempio errori e azioni) nel registro eventi di Windows. Le informazioni consentono di risolvere i problemi riscontrati durante l'esecuzione dello script. Potrebbe essere utile tenere presente il seguente elenco di controllo per la risoluzione dei problemi:

- Mancata comunicazione con i server remoti. Azioni possibili:
  - Verificare la propria connessione al server.
  - Verificare che la chiave API che si utilizza sia valida.
- Mancata creazione di macchine. Azioni possibili:
  - Verificare che l'account utente che esegue lo script disponga di autorizzazioni sufficienti per creare account utente nel dominio.

  - Verificare che l'utente che ha creato la chiave API disponga di autorizzazioni sufficienti per utilizzare MCS per il provisioning delle macchine.
  - Verificare la validità del catalogo macchine (ovvero se la sua immagine esiste ancora ed è in buono stato).

- Mancata aggiunta di macchine a un catalogo macchine o a un gruppo di consegna. Azione possibile:

  - Verificare che l'utente che ha creato la chiave API disponga di autorizzazioni sufficienti per aggiungere e rimuovere macchine da e verso cataloghi di macchine e gruppi di consegna.

## Notifiche di disconnessione dell'utente (in precedenza scollegamento forzato dell'utente)

June 8, 2023

> **Importante:**
>
> Questa funzionalità è disponibile solo nell'interfaccia utente di Autoscale per gruppi di consegna basati su app multisessione.

Per ottenere risparmi sui costi, Autoscale consente di forzare lo scollegamento dalle sessioni persistenti consentendo di inviare una notifica personalizzata agli utenti e specificare un periodo di prova dopo il quale le sessioni vengono disconnesse forzatamente. Questo viene fatto solo per le macchine in modalità di svuotamento e non per tutte le macchine accese. Per evitare potenziali perdite di dati causate dalla forzatura degli scollegamenti degli utenti, è possibile configurare questa funzionalità in modo che invii solo promemoria di scollegamento senza forzare lo scollegamento degli utenti.

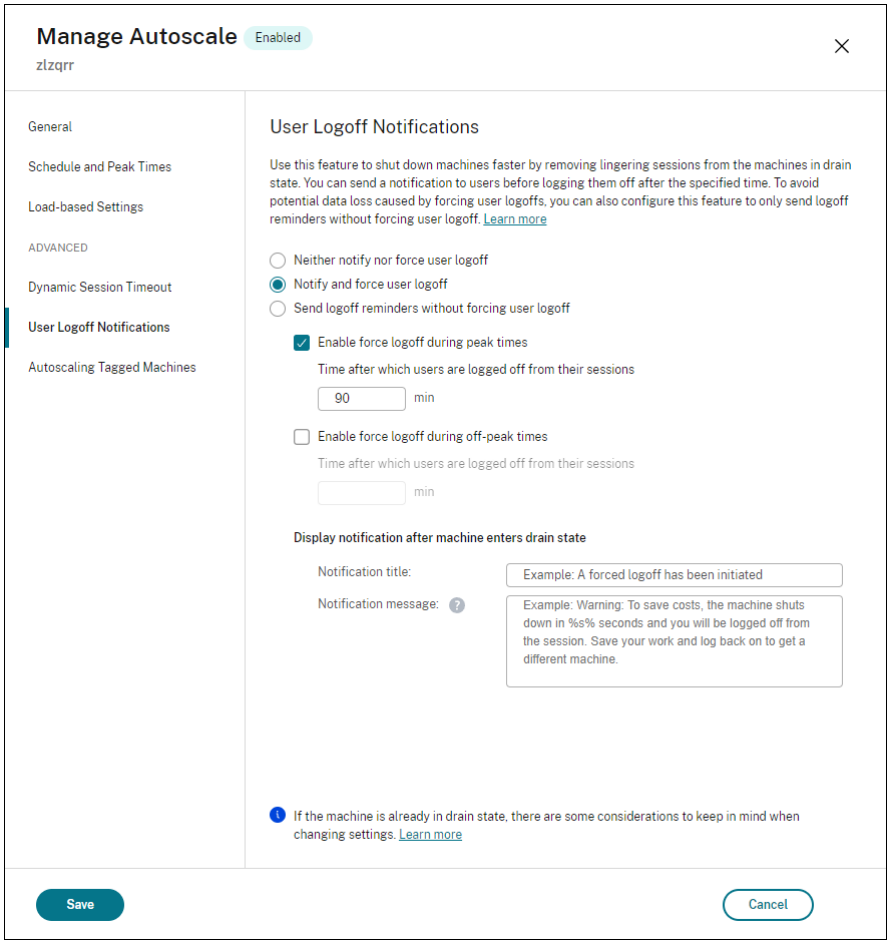
Sono disponibili le opzioni seguenti:

- **Notify and force user logoff (Invia notifiche e forzare lo scollegamento degli utenti)**
- **Send logoff reminders without forcing user logoff (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti)**
- **Neither notify nor force user logoff (Né notificare né forzare la disconnessione dell'utente)**

### Notify and force user logoff (Invia notifiche e forzare lo scollegamento degli utenti)

Se questa opzione è selezionata, Autoscale disconnette gli utenti dalle loro sessioni dopo gli orari specificati di seguito.




**Enable force logoff during peak times** (Abilita lo scollegamento forzato durante le ore di punta). Se questa opzione è selezionata, Autoscale scollega quegli utenti dalle loro sessioni durante le ore di punta allo scadere del tempo specificato.

**Enable force logoff during off-peak times** (Abilita lo scollegamento forzato durante le ore non di punta). Se questa opzione è selezionata, Autoscale scollega quegli utenti dalle loro sessioni durante le ore non di punta allo scadere del tempo specificato.

**Display notification after machine enters drain state** (Visualizza notifiche dopo che la macchina entra nello stato di svuotamento) Consente di inviare notifiche agli utenti dopo che la macchina entra in stato di svuotamento.

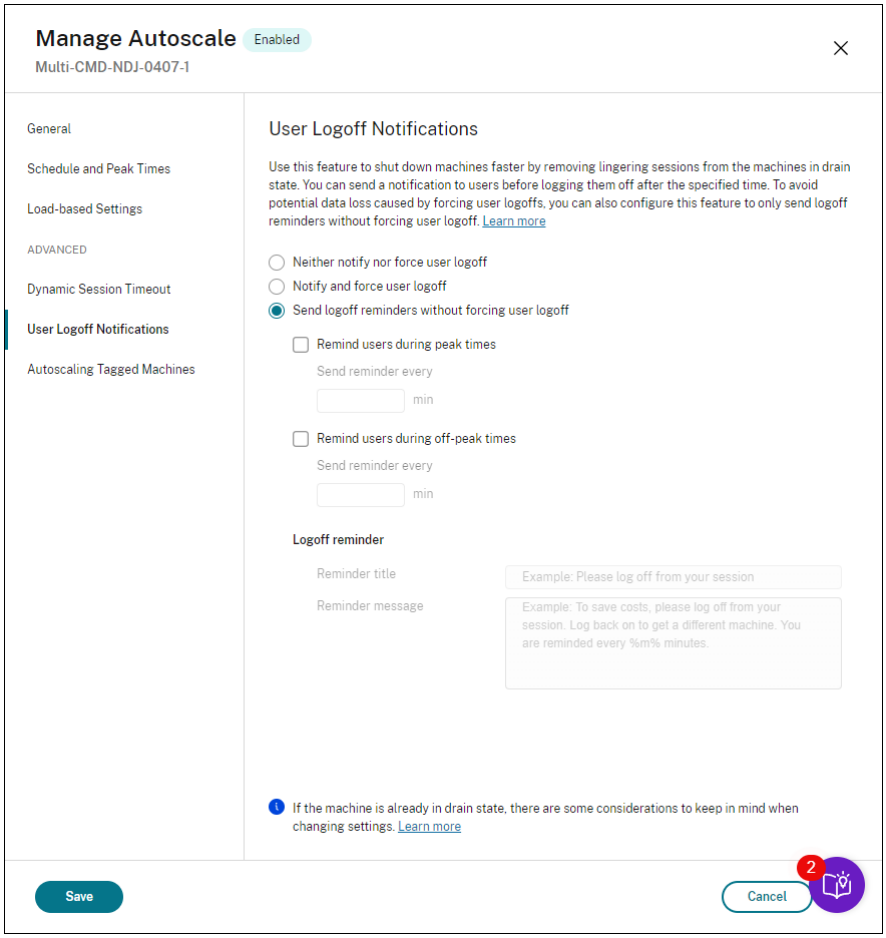
- **Notification title** (Titolo notifica). Consente di specificare un titolo della notifica da inviare agli utenti. Esempio: `A forced logoff has been initiated`.
- **Notification message** (Messaggio di notifica). Consente di specificare il contenuto della notifica da inviare agli utenti. È possibile utilizzare %s% o %m% come variabili per indicare l'ora specificata nel messaggio. Per esprimere il tempo in secondi, utilizzare %s%. Per esprimere il tempo in minuti, utilizzare %m%. Esempio: `Warning: To save costs , the machine shuts down in %s% seconds and you will be logged`

```
 off from the session. Save your work and log back on to get a
different machine.
```

### Send logoff reminders without forcing user logoff (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti)

Se questa opzione è selezionata, gli utenti riceveranno un promemoria per scollegarsi dalla propria macchina dopo che è entrata nello stato di svuotamento. Questo promemoria può essere configurato per essere inviato all'intervallo specificato di seguito.




**Remind users during peak times** (Avvisa gli utenti durante le ore di punta). Se questa opzione è selezionata, gli utenti ricevono un promemoria per scollegarsi dalle proprie sessioni durante le ore di punta ogni X minuti (X indica il tempo specificato).

**Remind users during off-peak times** (Avvisa gli utenti durante le ore non di punta). Se questa opzione è selezionata, gli utenti ricevono un promemoria per scollegarsi dalle proprie sessioni durante le ore non di punta ogni X minuti (X indica il tempo specificato).

**Logoff reminder** (Promemoria di scollegamento). Consente di configurare il promemoria inviato agli

utenti dopo che la loro macchina è entrata in stato di svuotamento.

- **Reminder title** (Titolo del promemoria). Consente di specificare un titolo per il promemoria da inviare agli utenti. Esempio: `Please log off from your session`.
- **Reminder message** (Messaggio di promemoria). Consente di specificare un messaggio da inviare agli utenti. Esempio: `Please log off from your session and log back on to save costs`.

### Neither notify nor force user logoff

Se selezionato, Autoscale non obbliga gli utenti a scollegarsi dai computer in stato di scarico né notifica agli utenti di passare manualmente a un'altra macchina.

### Considerazioni

Se la macchina è già in stato di svuotamento, considerare quanto segue quando si modificano le impostazioni:

- Se si modifica l'impostazione da **Send logoff reminders without forcing user logoff** (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti) a **Notify and force user logoff** (Invia notifiche e forza lo scollegamento degli utenti), la nuova impostazione ha effetto immediato.
- Se si modifica l'impostazione da **Notify and force user logoff** (Invia notifica e forza lo scollegamento degli utenti) a **Send logoff reminders without forcing user logoff** (Invia promemoria di scollegamento senza forzare la disconnessione degli utenti), la nuova impostazione non avrà effetto fino alla volta successiva in cui la macchina entra in stato di svuotamento. L'utente è comunque costretto a scollegarsi.

## Analizzare l'efficacia delle impostazioni di Autoscale

December 18, 2023

È possibile analizzare l'efficacia delle impostazioni di Autoscale in base all'utilizzo della macchina a partire dalla settimana precedente. Attraverso l'analisi, è possibile ottenere queste informazioni sull'efficacia delle impostazioni di Autoscale:

- Identificare gli sprechi finanziari derivanti dall'eccesso di provisioning.
- Determinare se l'esperienza utente è influenzata negativamente a causa di un provisioning insufficiente.

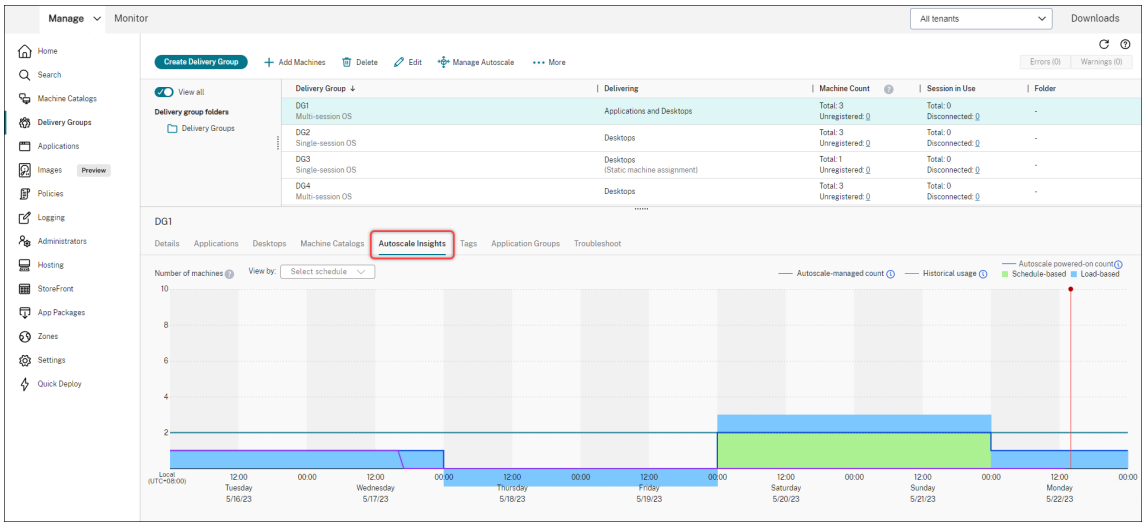
 

- Assicurarsi che la capacità fornita sia correttamente allineata con l'utilizzo della macchina.

Per raggiungere questo obiettivo, procedere nel modo seguente:

1. Selezionare un gruppo di consegna abilitato per Autoscale.
2. Nel riquadro inferiore, fare clic sulla scheda **Autoscale Insights** (Informazioni dettagliate su Autoscale).

   Viene visualizzato il seguente grafico, che mostra il confronto tra i dati di utilizzo delle macchine a partire dalla settimana precedente e il numero di macchine da alimentare in base alle impostazioni di Autoscale.




* La linea verticale rossa identifica l'ora corrente.

La tabella seguente fornisce le descrizioni delle metriche illustrate in questo grafico.

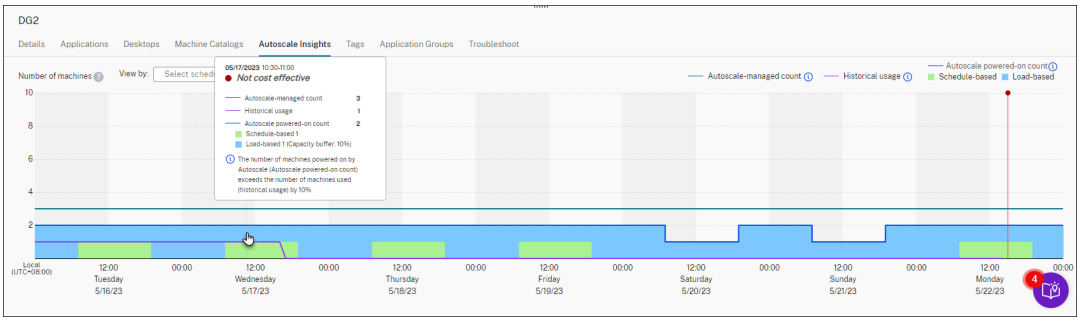
| Metrica | Descrizione |
|---|---|
| Conteggio gestito da Autoscale | Numero totale di macchine gestite da Autoscale. Conteggio gestito da Autoscale= Numero totale di macchine del gruppo di consegna - Numero di macchine in modalità manutenzione - Numero di macchine non contrassegnate per Autoscale (se la funzione Autoscale contrassegnata è abilitata). |
| Numero di accensioni a cura di Autoscale | Numero totale di macchine accese da Autoscale. Numero di accensioni a cura di Autoscale= Conteggio macchine basato sulla pianificazione + Conteggio macchine basato sul carico. |

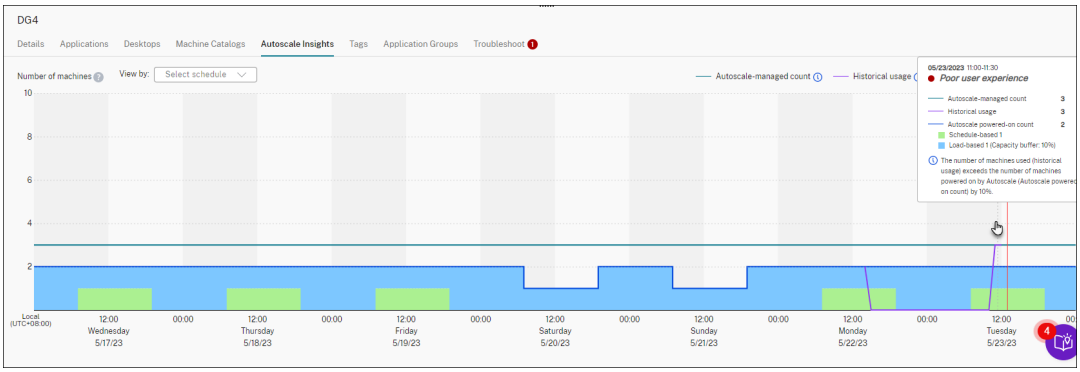
| Metrica | Descrizione |
| --- | --- |
| Utilizzo storico | Numero di macchine che sono state consegnate agli utenti. |
| Basato sulla pianificazione | Numero di macchine alimentate in base alle impostazioni basate sulla pianificazione di Autoscale ( **Nota:** le impostazioni basate sulla pianificazione non si applicano ai gruppi di consegna del tipo di sistema operativo statico a sessione singola). |
| Basato sul carico | Numero di macchine alimentate in base alle impostazioni basate sul carico di Autoscale. |

3. Per verificare l'efficacia delle impostazioni di Autoscale in una fascia oraria specifica, posizionare il mouse sul grafico in corrispondenza di quella fascia oraria. Viene visualizzata una finestra informativa che mostra i risultati del confronto e i conteggi dettagliati delle macchine:

   - **Non conveniente**. L'utilizzo storico è inferiore al 90% delle impostazioni di Autoscale (Autoscale powered-on count). Di conseguenza, potrebbe esistere uno spreco di capacità.

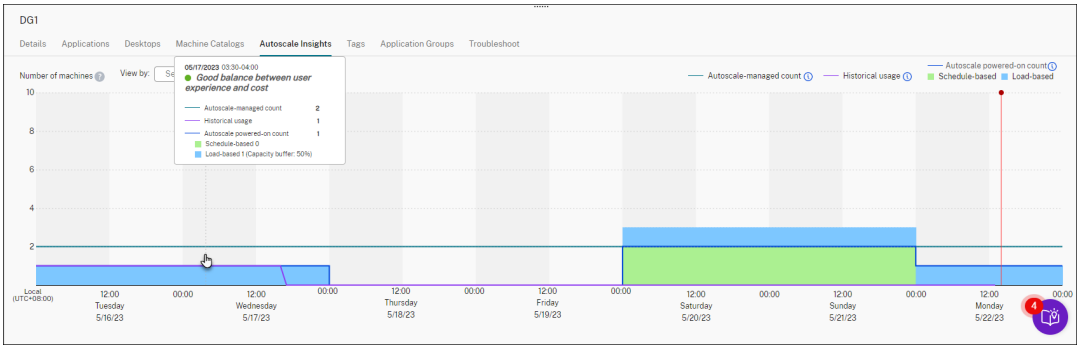



   - **Poor user experience** (Esperienza utente scadente). L'utilizzo storico è superiore al 110% delle impostazioni di Autoscale (Autoscale powered-on count). Di conseguenza, gli utenti potrebbero riscontrare tempi di attesa più lunghi per l'accensione dei computer.

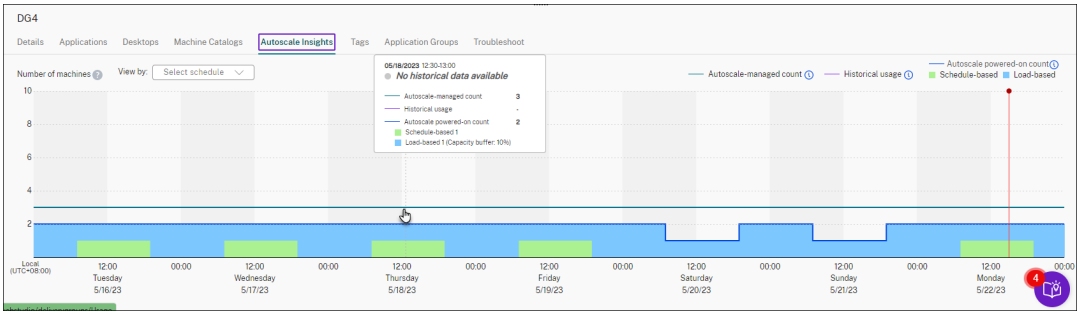


- **Good balance between user experience and cost** (Buon equilibrio tra esperienza utente e costi). La differenza tra l'utilizzo storico e le impostazioni di Autoscale (Autoscale powered-on count) è inferiore al 10%. Le impostazioni di Autoscale sono allineate all'utilizzo storico.




- **Nessun dato storico disponibile**. Non sono disponibili dati storici. Fra le possibili cause, Autoscale potrebbe essere stato abilitato per il gruppo di consegna meno di una settimana fa.




4. Per evidenziare un intervallo di date basato su una pianificazione in Autoscale, selezionare il campo**View by** (Visualizza per).
5. Regolare le impostazioni di Autoscale in base all'analisi effettuata. Per ulteriori informazioni, vedere Impostazioni basate sulla pianificazione e sul carico.

## Comandi dell'SDK Broker PowerShell

November 21, 2023

È possibile configurare Autoscale per i gruppi di consegna utilizzando l'SDK Broker PowerShell. Per configurare Autoscale utilizzando i comandi di PowerShell, è necessario utilizzare l'SDK Remote PowerShell versione 7.21.0.12 o successiva. Per ulteriori informazioni sull'SDK Remote PowerShell, vedere SDK e API.

### Set-BrokerDesktopGroup

Disabilita o abilita un BrokerDesktopGroup esistente o ne modifica le impostazioni. Per ulteriori informazioni su questo cmdlet, vedere https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

#### Esempi

Per ulteriori informazioni su come utilizzare i cmdlet PowerShell per reimpostare un profilo, vedere gli esempi seguenti:

Abilitare Autoscale

- Supponiamo di voler abilitare Autoscale per il gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled $true
  ```

Configurare il buffer di capacità separatamente per le ore di punta e non di punta

- Si supponga di voler impostare il buffer di capacità al 20% per le ore di punta e al 10% per le ore non di punta per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10
  ```

Configurare l'impostazione del **timeout alla disconnessione**

- Si supponga di voler impostare il valore del **timeout alla disconnessione** su 60 minuti per le ore di punta e 30 minuti per le ore non di punta per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30
  ```

Configurare l'impostazione del **timeout allo scollegamento**

- Si supponga di voler impostare il valore del **timeout allo scollegamento** su 60 minuti per le ore di punta e 30 minuti per le ore non di punta per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30
  ```

Configurare l'impostazione del **ritardo di spegnimento**

- Supponiamo di voler impostare il ritardo di spegnimento su 15 minuti per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15`

Configurare un periodo di tempo durante il quale il ritardo di spegnimento non ha effetto

- Supponiamo che si voglia che il ritardo di spegnimento non abbia effetto finché non sono passati 30 minuti per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh 30.`

Configurare il **costo dell'istanza della macchina**

- Supponiamo di voler impostare il costo orario dell'istanza della macchina a 0,2 dollari per un gruppo di consegna dal nome "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2`

### New-BrokerPowerTimeScheme

Crea un BrokerPowerTimeScheme per un gruppo di consegna. Per ulteriori informazioni, vedere https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

#### Esempio

Si supponga di voler creare uno schema dei tempi di accensione per un gruppo di consegna il cui valore UID è 3. Il nuovo schema copre il fine settimana, il lunedì e il martedì. La fascia oraria dalle 8:00 alle 18:30 è definita come ora di punta per i giorni inclusi nello schema. Per le ore di punta, la dimensione del pool (il numero di macchine mantenute accese) è 20. Per le ore non di punta è 5. È possibile utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

```
PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )
PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )
PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48
```

### Parametri per i timeout dinamici delle sessioni

I seguenti cmdlet Broker PowerShell SDK sono stati estesi per i timeout dinamici delle sessioni supportando svariati nuovi parametri:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Tali parametri comprendono:

- **DisconnectPeakIdleSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione inattiva viene disconnessa durante le ore di punta. Questa proprietà ha un valore predefinito pari a 0, che indica la disattivazione del comportamento a essa associato durante le ore di punta. Un valore maggiore di 0 consente il comportamento associato al gruppo di consegna solo nelle ore di punta.
- **DisconnectOffPeakIdleSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione inattiva viene disconnessa durante le ore non di punta. Il valore predefinito di questa proprietà è 0, che indica la disattivazione del comportamento a essa associato durante le ore non di punta. Un valore maggiore di 0 abilita il comportamento associato al gruppo di consegna solo nelle ore non di punta.
- **LogoffPeakDisconnectedSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione disconnessa viene terminata durante le ore di punta. Il valore predefinito di questa proprietà è 0, che indica la disattivazione del comportamento a essa associato durante le ore di punta. Un valore maggiore di 0 abilita il comportamento associato al gruppo di consegna solo nelle ore di punta.
- **LogoffOffPeakDisconnectedSessionAfterSeconds**: rappresenta il tempo in secondi dopo il quale una sessione disconnessa viene terminata durante le ore non di punta. Il valore predefinito di questa proprietà è 0, che indica la disattivazione del comportamento a essa associato durante le ore non di punta. Un valore maggiore di 0 abilita il comportamento associato al gruppo di consegna solo nelle ore non di punta.

#### Esempio

Supponiamo di voler impostare il timeout della sessione di inattività a 3.600 secondi durante le ore di punta per un gruppo di consegna il cui nome è "MyDesktop". Utilizzare il comando `Set-BrokerDesktopGroup` di PowerShell. Ad esempio:

- ```
  C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte
    3600
  ```

 
  ```

In questo modo si disconnettono le sessioni che sono rimaste inattive per più di 1 ora nelle ore non di punta per il gruppo desktop il cui nome è "MyDesktop".

## Cloud Health Check

December 12, 2022

> **Nota:**
>
> Cloud Health Check è integrato in Citrix DaaS. L'integrazione è disponibile come azione Run Health Check (Esegui controllo di integrità) nell'interfaccia di gestione Full Configuration. Per ulteriori informazioni, vedere Risolvere i problemi relativi alla registrazione VDA e all'avvio della sessione.

Cloud Health Check consente di eseguire controlli che misurano l'integrità e la disponibilità del sito e dei suoi componenti. È possibile eseguire controlli di integrità per i Virtual Delivery Agent (VDA), i server StoreFront e Profile Management. I controlli di integrità dei VDA identificano le possibili cause di problemi comuni di registrazione e avvio della sessione dei VDA.

Se sono presenti problemi durante i controlli, Cloud Health Check fornisce un rapporto dettagliato e le azioni per risolverli. A ogni avvio, Cloud Health Check cerca la versione più recente degli script sulla CDN (Content Delivery Network) e scarica automaticamente gli script se non esistono sul computer locale. Cloud Health Check sceglie sempre la versione locale più recente degli script per eseguire i controlli di integrità.

> **Nota:**
>
> Cloud Health Check non si aggiorna ogni volta che viene eseguito.

In un ambiente Citrix Cloud, eseguire Cloud Health Check da una macchina aggiunta a un dominio per eseguire controlli su uno o più server VDA o StoreFront.

> **Nota:**
>
> Non è possibile installare o eseguire Cloud Health Check su un Cloud Connector.

Il registro per l'applicazione Cloud Health Check è archiviato in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`. È possibile utilizzare questo file per la risoluzione dei problemi.

Ecco un'introduzione a Cloud Health Check.

Ecco quando utilizzare Cloud Health Check.

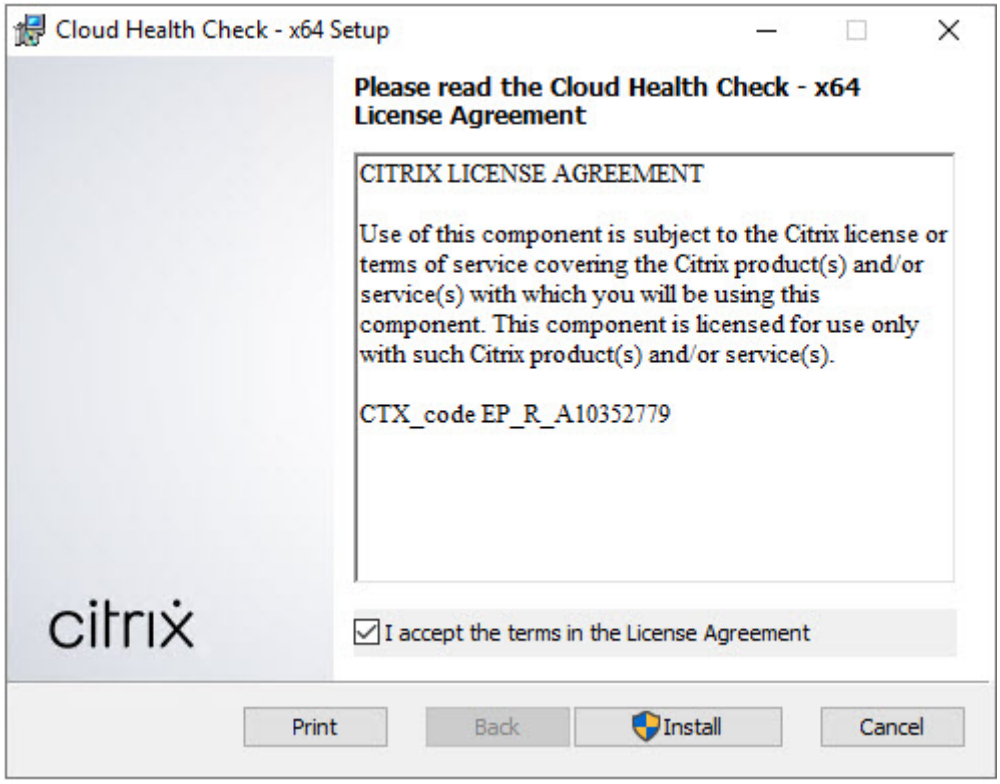
### Installazione

Per preparare il proprio ambiente per l'installazione di Cloud Health Check, è necessario disporre di una macchina Windows aggiunta al dominio.

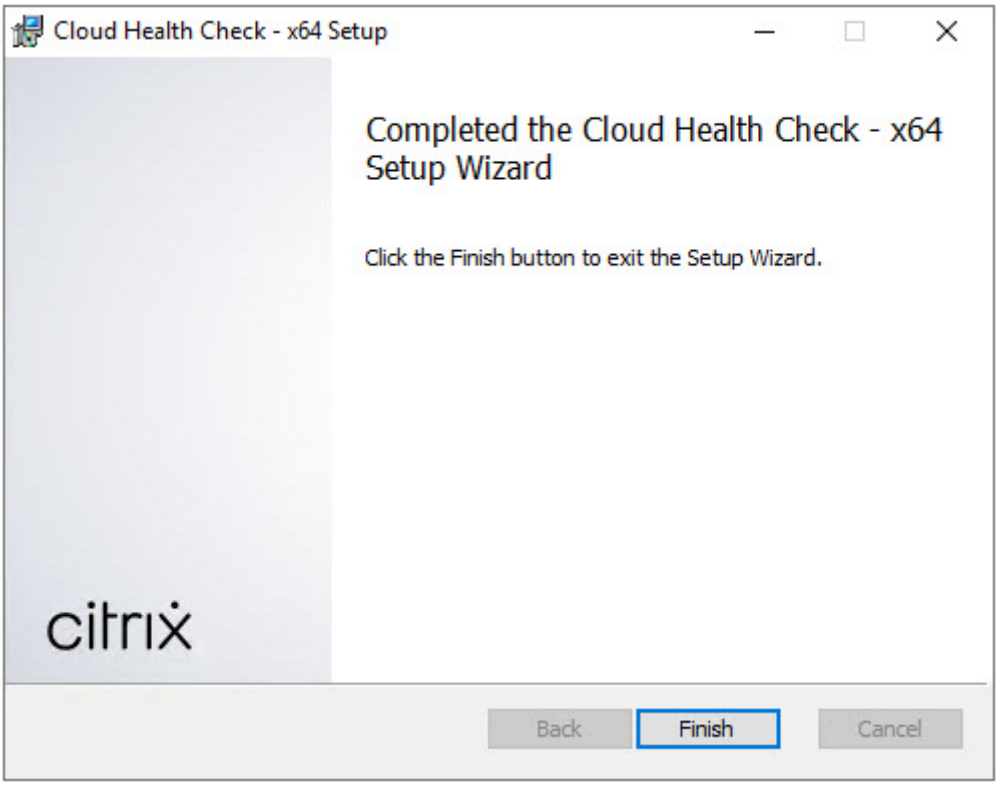
> **Nota:**
>
> Non è possibile installare o eseguire Cloud Health Check su Cloud Connector.

1. Sulla macchina aggiunta al dominio, scaricare il programma di installazione di Cloud Health Check.
2. Fare doppio clic sul file CloudHealthCheckInstaller_x64.msi.
3. Fare clic sulla casella per accettare le condizioni d'uso.
4. Fare clic su Installa.




5. Una volta completata l'installazione, fare clic su **Fine**.




### Autorizzazioni e requisiti

Autorizzazioni:

- Per eseguire i controlli di integrità:
  - È necessario appartenere al gruppo di utenti del dominio.
  - È necessario essere un amministratore completo o disporre di un ruolo personalizzato con autorizzazioni di sola lettura e autorizzazioni **Run Environment Tests** (di esecuzione test ambiente) nel sito.
  - Impostare il criterio di esecuzione degli script su almeno `RemoteSigned` per consentire l'esecuzione degli script. Ad esempio: `Set-ExecutionPolicy RemoteSigned`. **Nota:** possono essere valide anche altre autorizzazioni per l'esecuzione degli script.
- Utilizzare **Run as administrator** (Esegui come amministratore) all'avvio di Cloud Health Check.

Per ciascun computer VDA o StoreFront su cui si eseguono controlli di integrità:

- Il sistema operativo deve essere a 64 bit.
- Cloud Health Check deve essere in grado di comunicare con la macchina.
- La condivisione di file e stampanti deve essere attivata.
- PSRemoting e WinRM devono essere abilitati. Il computer deve anche avere in esecuzione PowerShell 3.0 o versione successiva.

- L'accesso a Windows Management Infrastructure (WMI) deve essere abilitato sul computer.

### Informazioni sui controlli di integrità

I dati del controllo di integrità sono memorizzati nelle cartelle alla voce `C:\ProgramData\Citrix\TelemetryService\`.

#### Controlli di integrità dei VDA

Per la registrazione sul VDA, Cloud Health Check verifica:

- Installazione del software VDA
- Appartenenza al dominio macchina VDA
- Disponibilità delle porte di comunicazione VDA
- Stato del servizio VDA
- Configurazione del firewall di Windows
- Comunicazione con il controller
- Sincronizzazione temporale con il controller
- Stato di registrazione del VDA

Per i lanci delle sessioni sui VDA, Cloud Health Check verifica:

- Disponibilità della porta di comunicazione di avvio della sessione
- Stato dei servizi di avvio della sessione
- Configurazione di Windows firewall all'avvio della sessione
- Licenze di accesso client di VDA Remote Desktop Services
- Percorso di avvio dell'applicazione VDA
- Impostazioni del registro di avvio della sessione
- Stato di Citrix Universal Injection Driver (CTXUVI)

Per Profile Management su VDA, Cloud Health Check verifica:

- Rilevamento di Hypervisor
- Rilevamento di Provisioning
- Citrix Virtual Apps and Desktops
- Configurazione del vDisk personale
- Store utenti
- Rilevamento dello stato del servizio Profile Management
- Test di hook di Winlogon.exe

Per eseguire controlli sul Profile Management, è necessario installare e abilitare Profile Management sul VDA. Per ulteriori informazioni sui controlli di configurazione Profile Management, vedere l'articolo CTX132805del Knowledge Center.

### Controlli di integrità di StoreFront

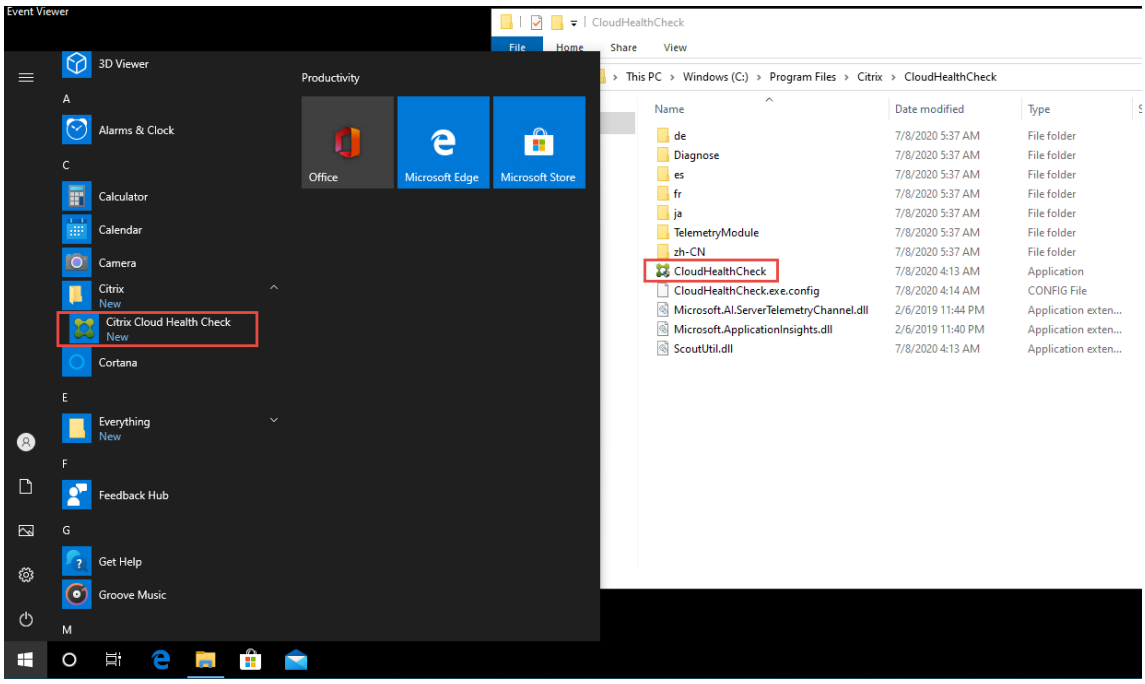
I controlli di StoreFront verificano se:

- Il servizio Citrix Default Domain è in esecuzione
- Il servizio Citrix Credential Wallet è in esecuzione
- La connessione dal server StoreFront ad Active Directory è la porta 88
- La connessione dal server StoreFront ad Active Directory è la porta 389
- La connessione dal server StoreFront ad Active Directory è la porta 464
- L'URL di base ha un nome di dominio completo valido
- È possibile recuperare l'indirizzo IP corretto dall'URL di base
- Il pool di applicazioni IIS utilizza .NET 4.0
- Il certificato è associato alla porta SSL per l'URL dell'host
- La catena di certificati è completa
- I certificati sono scaduti
- Un certificato scade nei prossimi 30 giorni

## Eseguire Cloud Health Check

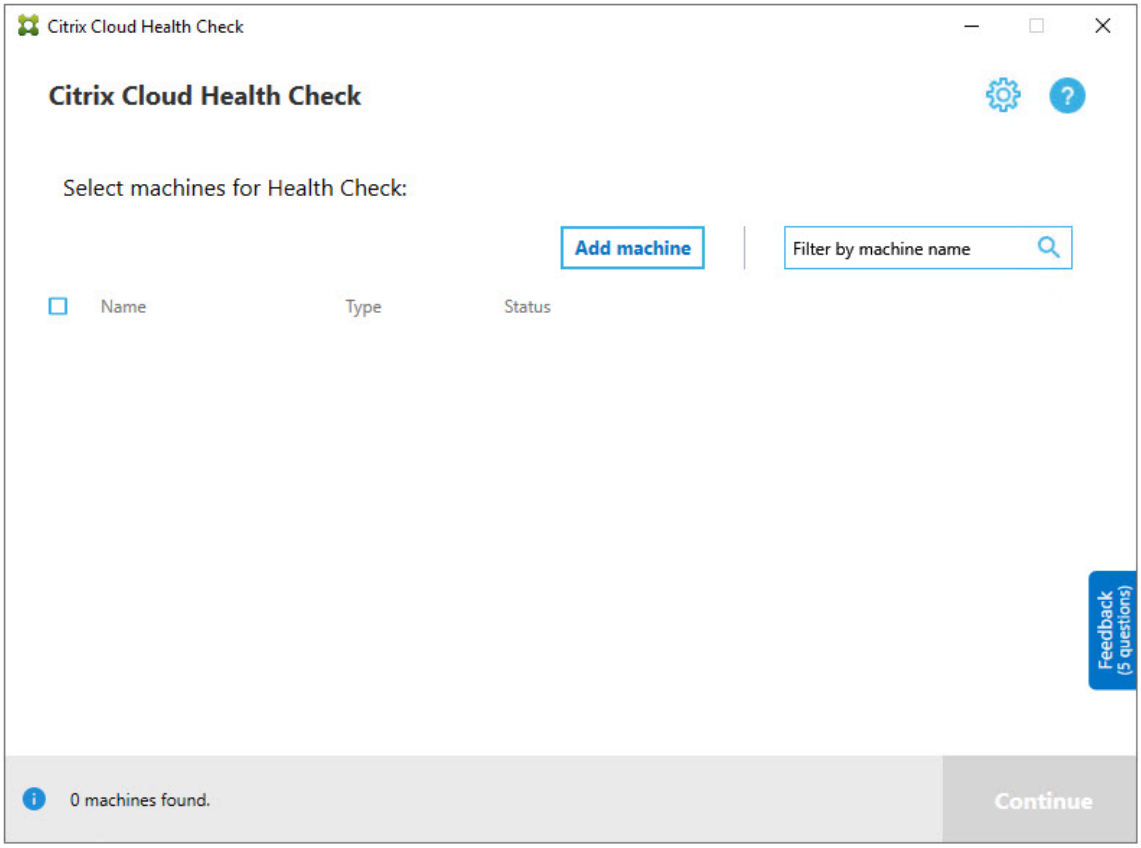
Per eseguire Citrix Cloud Health Check:

1. Selezionare **Citrix > Citrix Cloud Health Check** dal menu Start della macchina o eseguire `CloudHealthCheck.exe` in `C:\Program Files\Citrix\CloudHealthCheck`.



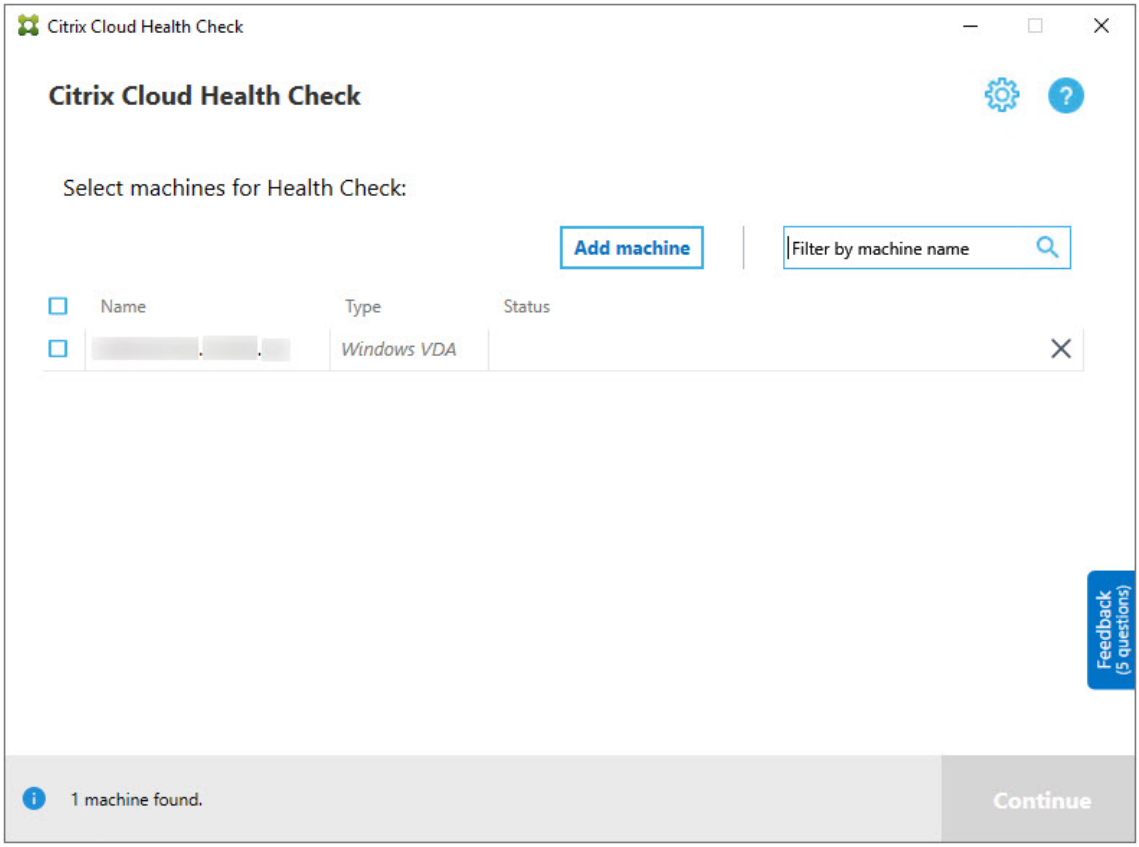

2. Nella schermata principale di Cloud Health Check, fare clic su **Add machine**.




3. Digitare il nome di dominio completo della macchina che si desidera aggiungere. **Nota:** sebbene l'immissione di un alias DNS invece di un FQDN possa sembrare valida, i controlli di integrità potrebbero non riuscire.
4. Fare clic su **Continue** (Continua).
5. Ripetere l'operazione per aggiungere altre macchine, secondo necessità.




6. Per rimuovere una macchina aggiunta manualmente, fare clic sulla **X** all'estremità destra della riga e confermare l'eliminazione. Ripetere l'operazione per eliminare altre macchine aggiunte manualmente.

Cloud Health Check ricorda le macchine aggiunte manualmente finché non vengono eliminate. Quando si chiude e poi si riapre Cloud Health Check, le macchine aggiunte manualmente sono ancora elencate in cima all'elenco.

### Importare macchine VDA

È possibile importare macchine VDA nella distribuzione durante l'esecuzione dei controlli di integrità.

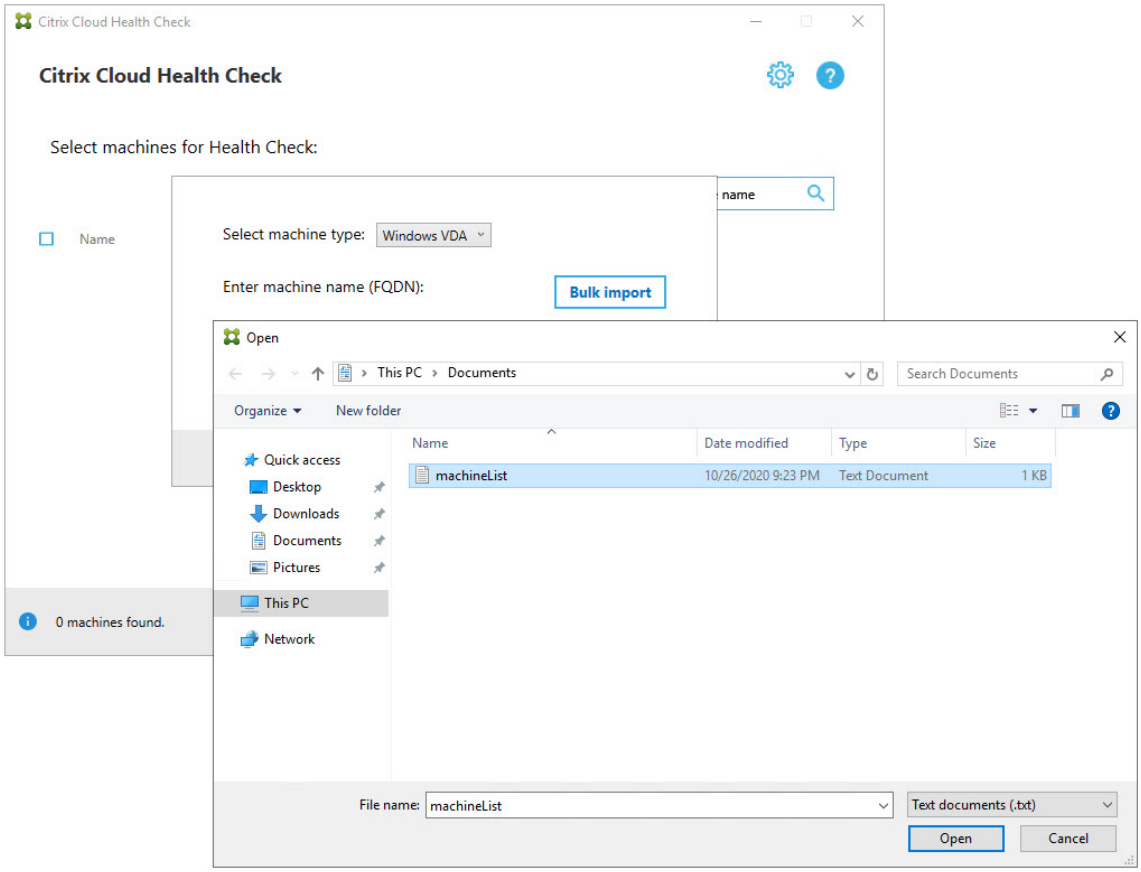
1. Su Connector, generare il file dell'elenco dei computer con il comando PowerShell seguente. Su Connector è necessario inserire le credenziali Citrix e selezionare il cliente nella finestra di dialogo a comparsa.

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.
txt
```

1. Copiare il file machineList.txt nel computer aggiunto al dominio su cui si desidera eseguire Cloud Health Check.

2. Nella pagina Cloud Health Check, fare clic su **Add Machine**.
3. Selezionare il tipo di macchina Windows VDA.
4. Fare clic su **Import VDA machines** (Importa macchine VDA).
5. Selezionare il file machineList.txt.
6. Fare clic su **Open**.




Le macchine VDA importate sono elencate nella pagina Cloud Health Check.

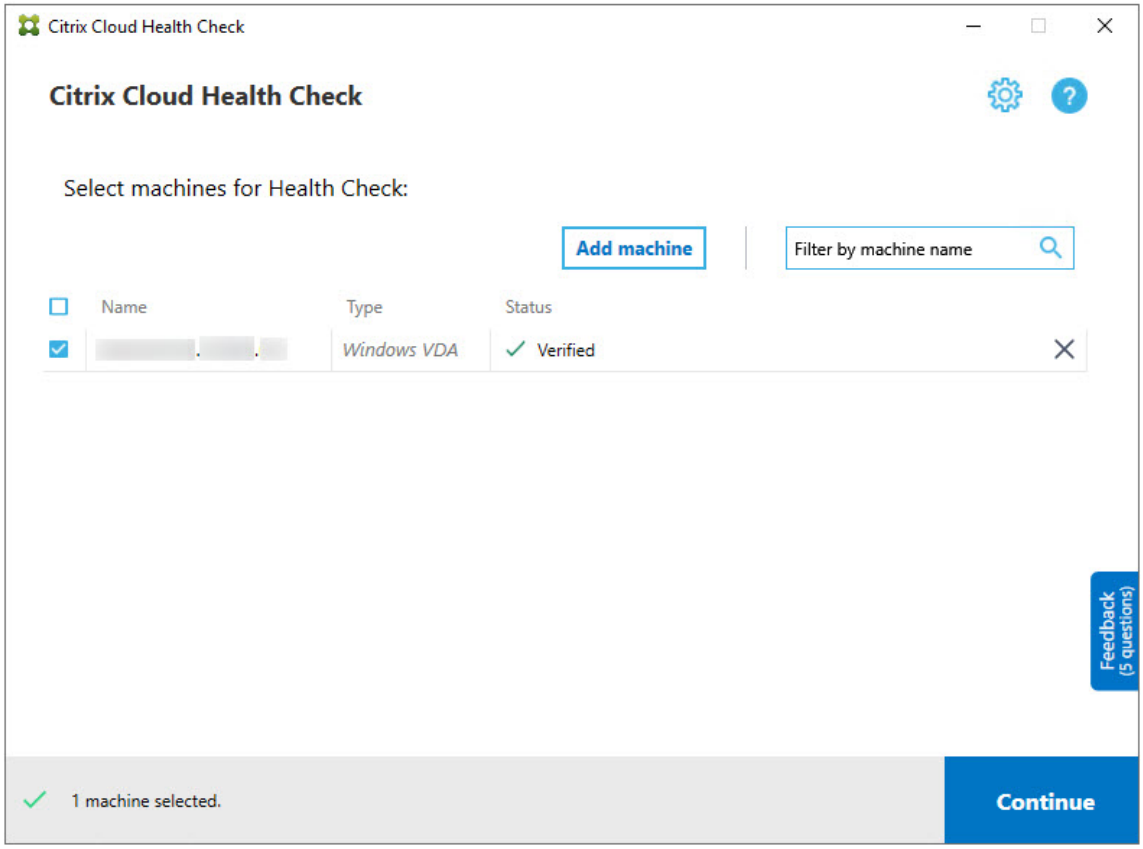
7. Selezionare la casella di controllo accanto a ciascun computer su cui si desidera eseguire i controlli di integrità.

   Cloud Health Check avvia automaticamente i test di verifica su ogni macchina selezionata, assicurandosi che soddisfi i criteri elencati fra i test di verifica. Se la verifica non riesce, viene visualizzato un messaggio nella colonna **Status** e la casella di controllo della macchina viene deselezionata. È quindi possibile:

   - Risolvere il problema e quindi selezionare di nuovo la casella di controllo del computer. Questo innesca un nuovo tentativo dei test di verifica.
   - Saltare quella macchina lasciando deselezionata la casella di controllo. I controlli di integrità non vengono eseguiti su quella macchina.

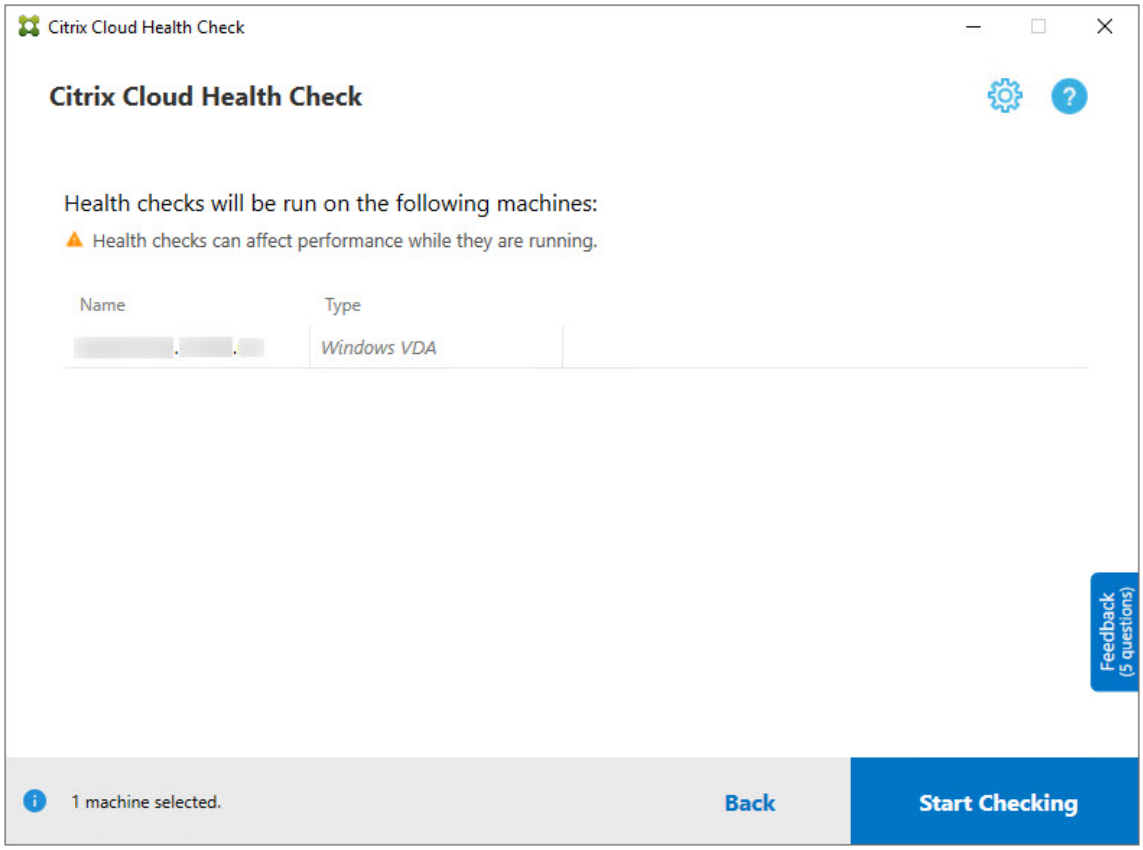
 

8. Al completamento dei test di verifica, fare clic su **Continue**.




9. Eseguire i controlli di integrità sulle macchine selezionate. Il riepilogo elenca le macchine in cui vengono eseguiti i test (i computer selezionati che hanno superato i test di verifica).
10. Fare clic su **Start Checking** (Avvia controlli).

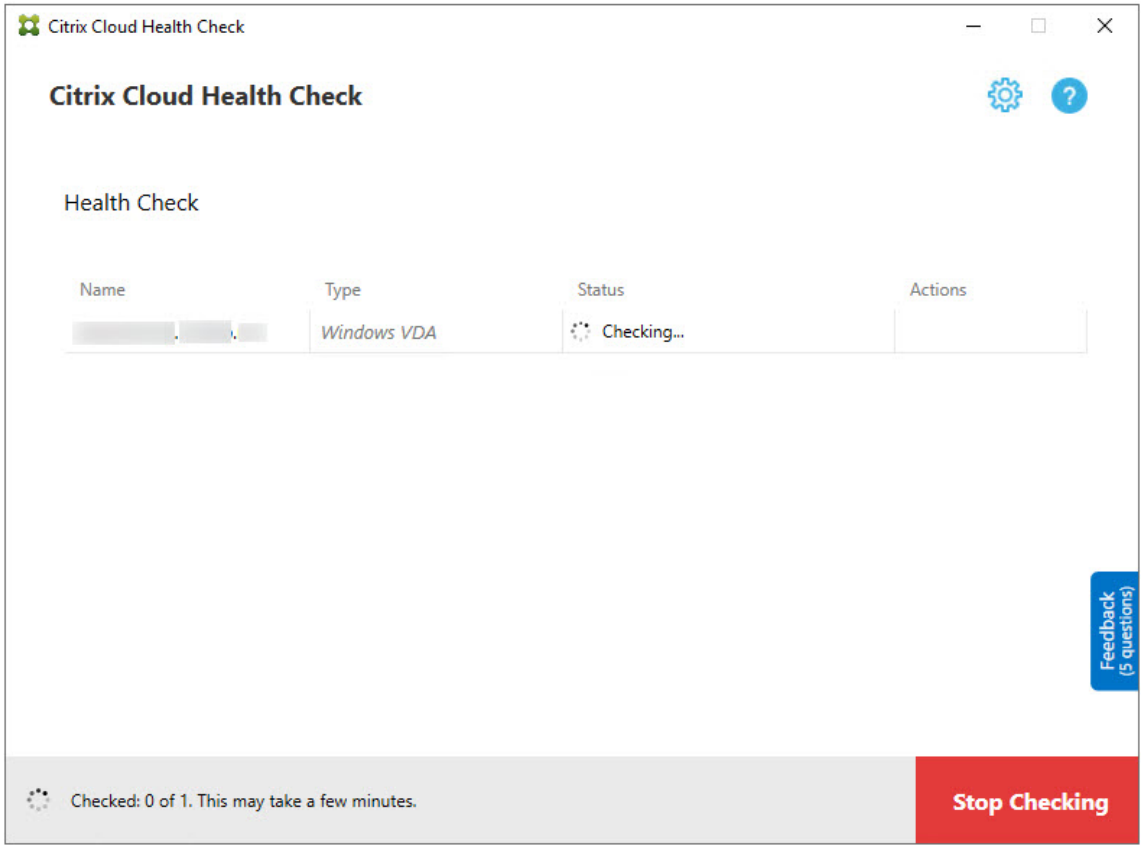
 




Durante e dopo il controllo, la colonna **Status** indica lo stato del controllo corrente di una macchina.

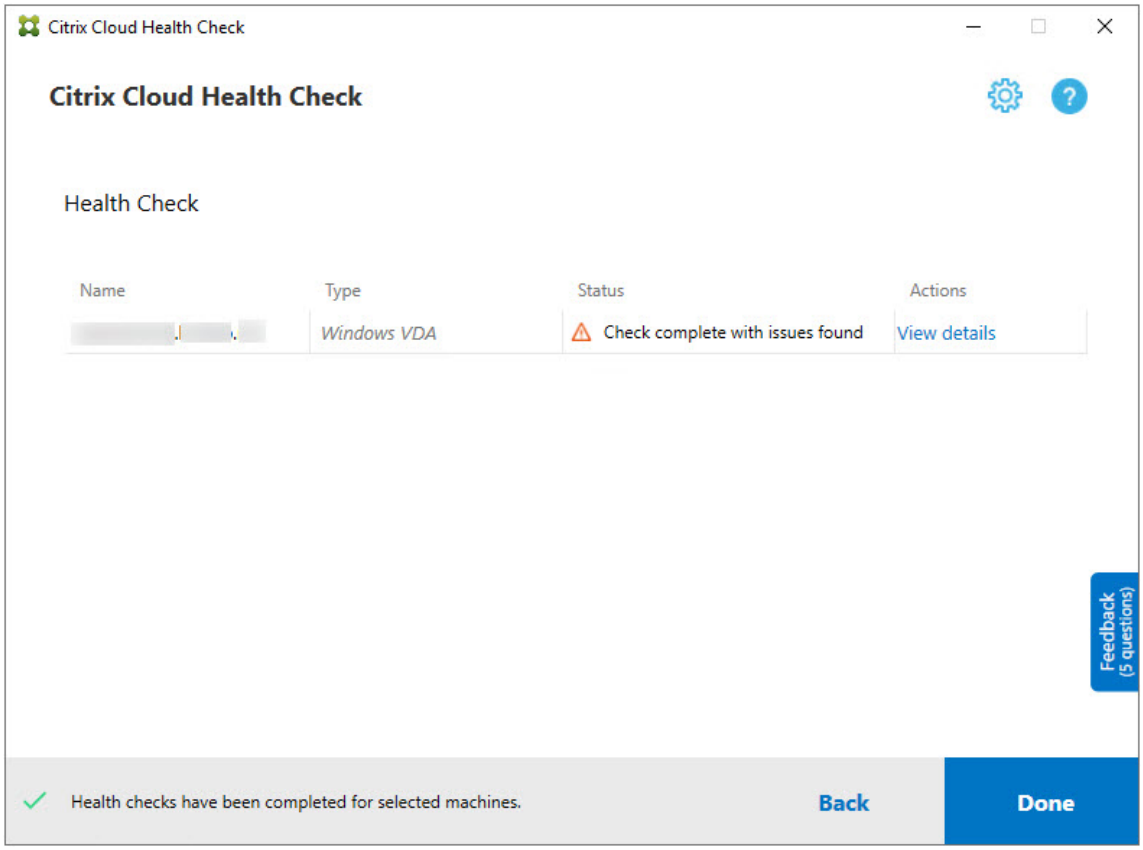
11. Per interrompere tutti i controlli in corso, fare clic su **Stop Checking** (Interrompi controlli) nell'angolo in basso a destra della pagina. Non è possibile annullare il controllo di integrità di una singola macchina, ma solo annullare il controllo di tutte le macchine selezionate.

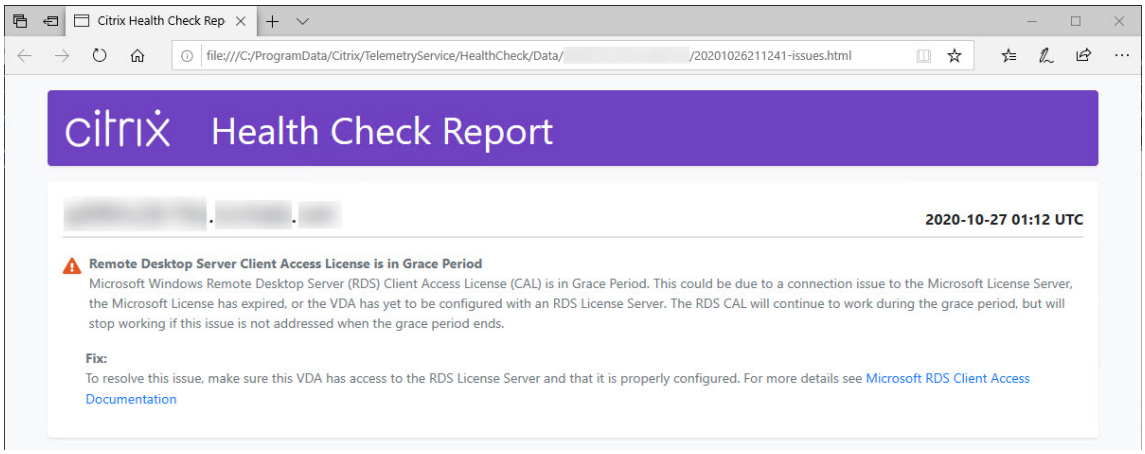



12. Al completamento dei controlli su tutte le macchine selezionate, il pulsante **Stop Checking** nell'angolo in basso a destra diventa **Done** (Fatto).

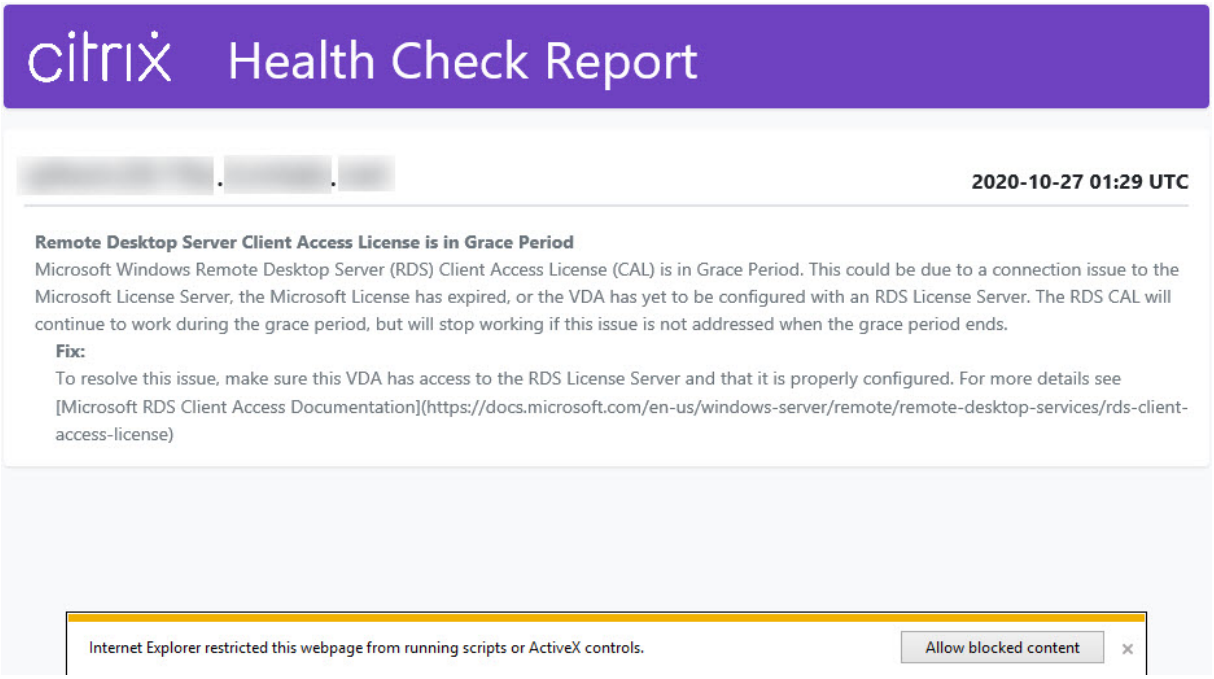



- Se un controllo non riesce, è possibile fare clic su **Retry** (Riprova) nella colonna **Action**.
- Se un controllo viene completato senza rilevare problemi, la colonna **Action** è vuota.
- Se un controllo rileva problemi, fare clic su **View Details** per visualizzare i risultati.




Se si utilizza Internet Explorer per visualizzare il rapporto, è necessario fare clic su **Allow blocked content** (Consenti contenuto bloccato) per visualizzare il collegamento ipertestuale.




Una volta completato il controllo per tutte le macchine selezionate, facendo clic su **Back** (Indietro) si perdono i risultati del controllo.

Una volta completati i controlli, fare clic su **Done** per tornare alla schermata principale di Cloud Health Check.

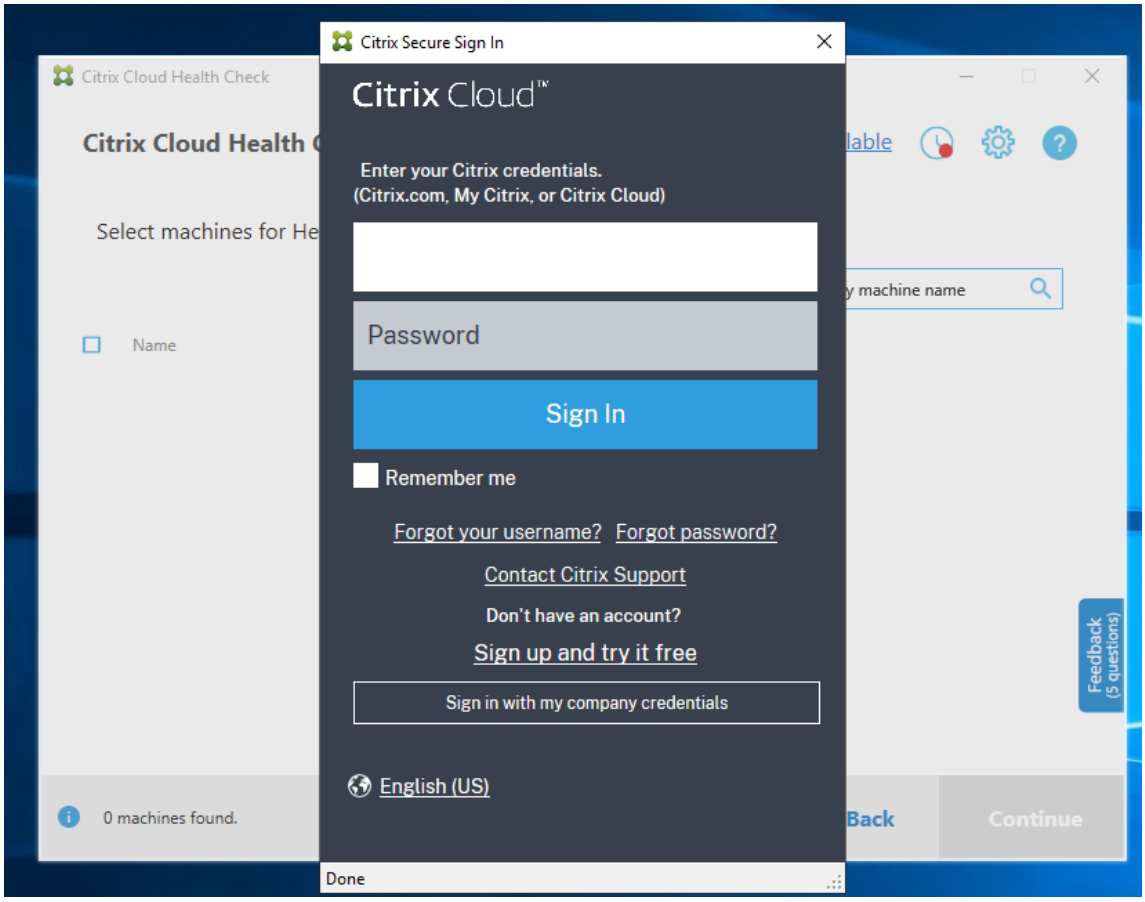
### Recuperare macchine VDA

Cloud Health Check è in grado di rilevare e recuperare automaticamente i VDA dalle distribuzioni Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops).

Per recuperare i propri VDA:

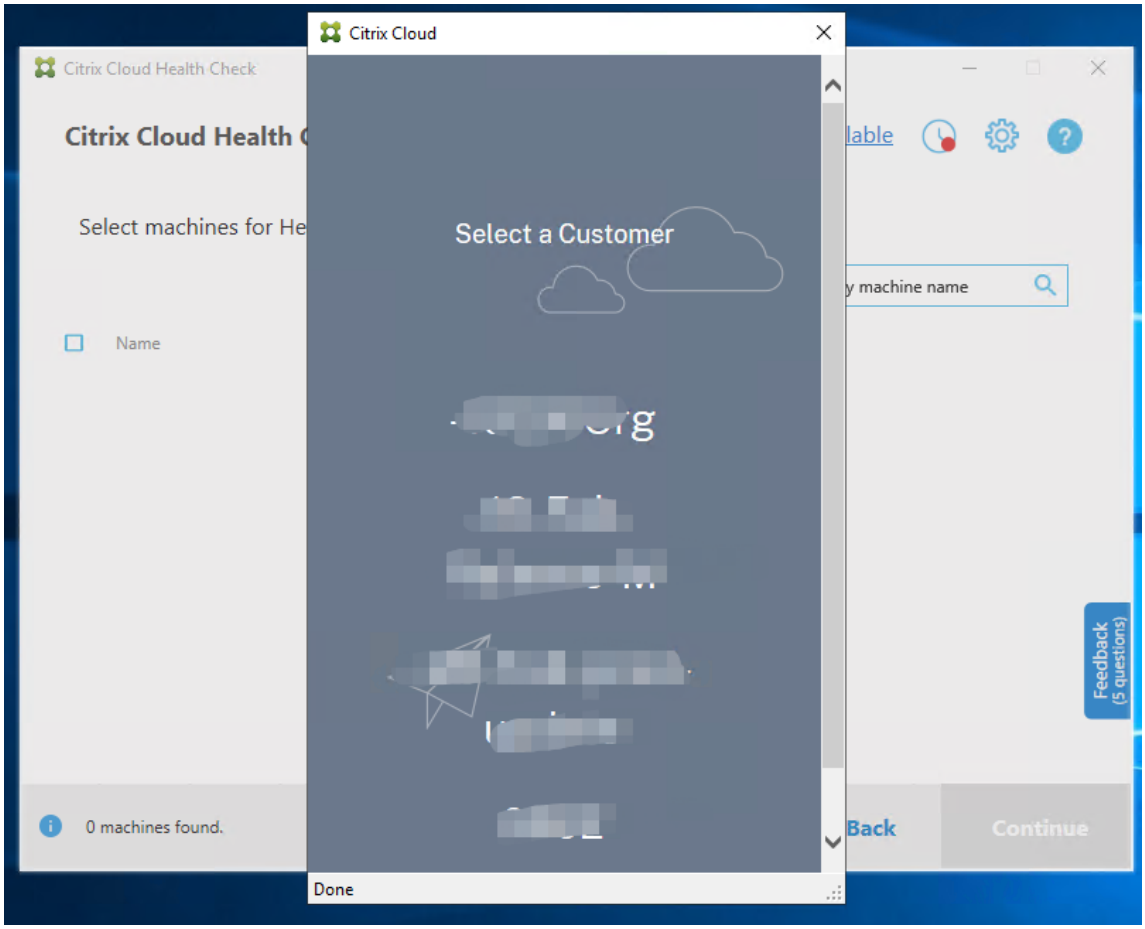
1. Preparare una nuova macchina aggiunta alla stessa foresta di domini su cui viene eseguito Cloud Health Check.
2. Aprire Cloud Health Check e fare clic su **Find machine** (Trova macchina) per accedere a Citrix Cloud.



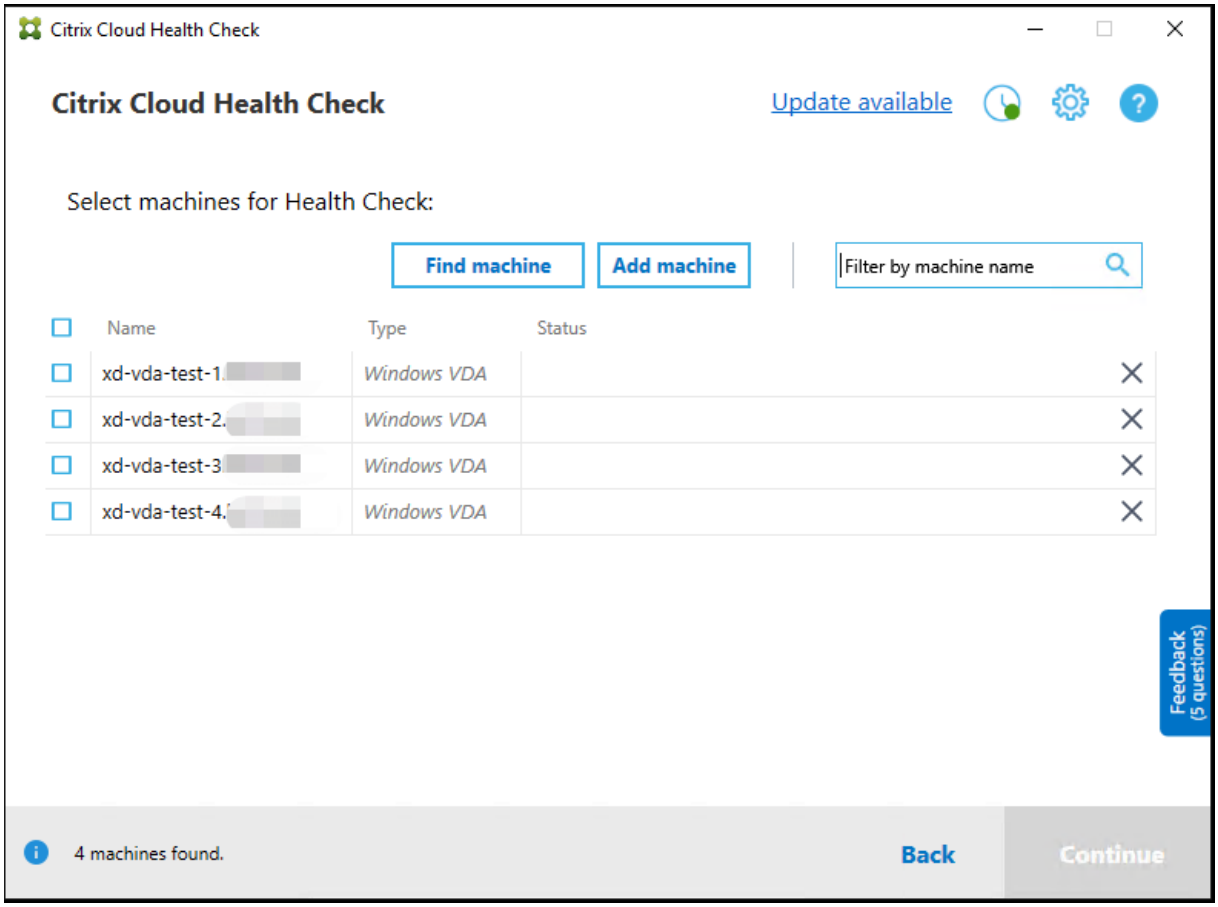

3. Selezionare il cliente con il sito cloud che si desidera recuperare.




Viene visualizzato l'elenco dei VDA in Cloud Health Check. L'elenco viene salvato anche in un file locale che si trova in `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json`.

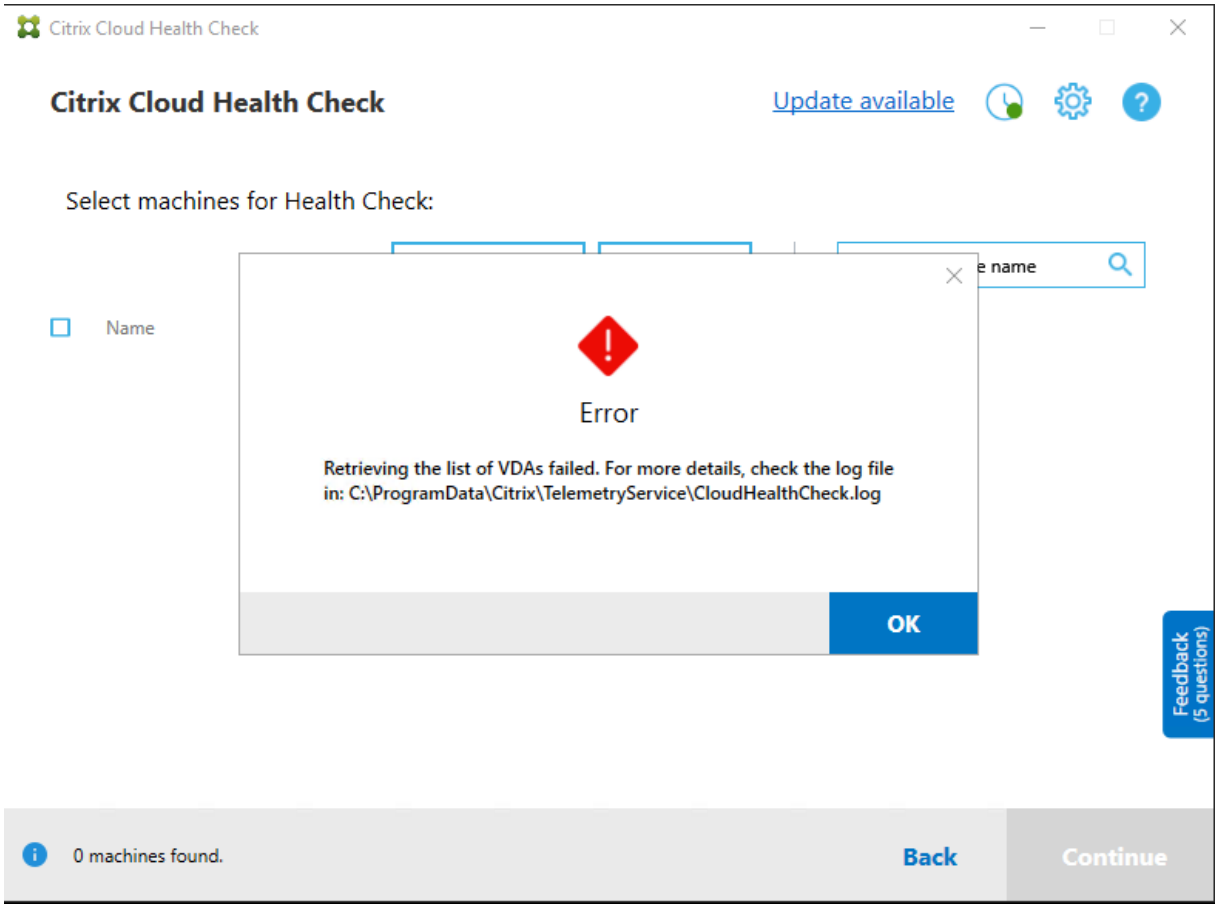
 




L'elenco delle macchine carica la cache locale quando si apre di nuovo Cloud Health Check. Se sono stati effettuati aggiornamenti della distribuzione, è necessario fare clic su **Find machine** per aggiornare l'elenco delle macchine.

> **Nota:**
>
> - Cloud Health Check trova le macchine solo nella stessa foresta di domini su cui viene eseguito Cloud Health Check.
> - Le sessioni Citrix Cloud scadono dopo un'ora. Dopo un'ora, è necessario fare nuovamente clic su **Find machine** per ottenere l'elenco di VDA più recente.
> - Se il recupero dell'elenco VDA non riesce, viene visualizzato un messaggio di errore. È possibile controllare i dettagli in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.




### Risultati del controllo di integrità

I controlli di integrità che generano report contengono i seguenti elementi:

- Ora e data in cui è stato generato il report dei risultati
- FQDN delle macchine che sono state controllate
- Condizioni verificate sulle macchine di destinazione

### Esecuzione di Cloud Health Check dalla riga di comando

Cloud Health Check può essere eseguito dalla riga di comando per aiutare i clienti a eseguire controlli di integrità. Per utilizzare Cloud Health Check dalla riga di comando, è necessario essere un amministratore sulla macchina su cui è in esecuzione Cloud Health Check.

> **Nota:**
>
> Quando si utilizza Cloud Health Check dalla riga di comando, è possibile controllare solo una macchina alla volta. È possibile eseguire una sola istanza di `CloudHealthCheck.exe` con-

> temporaneamente sulla macchina di destinazione. Se si desidera controllare più macchine, è necessario controllarle una per una, racchiudendo i cmdlet in un ciclo negli script di cmdlet/PowerShell. Anche eventuali istanze dell'interfaccia utente aperta di Cloud Health Check devono essere chiuse.

#### Cmdlet

I cmdlet della riga di comando supportati sono:

- `MachineFQDN` - Questo cmdlet è **obbligatorio**. Questo è il nome di dominio completo del computer di destinazione.
- `MachineType` - Questo cmdlet è facoltativo. Il valore del cmdlet può essere il VDA Windows (valore predefinito) o StoreFront.
- `ReportName` - Questo cmdlet è facoltativo. Il valore del cmdlet deve essere un nome di file valido in Windows. Il valore predefinito è `HealthCheckReport`.
- `SkipAdminCheck` - Questo cmdlet è facoltativo. Questo può essere aggiunto per saltare i controlli che richiedono autorizzazioni di amministratore.
- `UpdateScripts` - Questo cmdlet è facoltativo. Questo può essere aggiunto per aggiornare gli script di controllo provenienti dal server CDN.
- `DisableCeip` - Questo cmdlet è facoltativo se CEIP è abilitato nell'interfaccia utente; aggiungerlo per disabilitare CEIP.
- `Help` - Mostra informazioni di guida sui parametri.

Esempi:

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName
checkreport
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts
```

```
HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain
.local,machine3.domain.local
```

```
HealthCheckCLI.exe -Help
```

> **Nota:**
>
> I nomi dei parametri non fanno distinzione tra maiuscole e minuscole.

Per impostazione predefinita, l'output della console non viene visualizzato nella finestra della console della riga di comando. È possibile visualizzare manualmente l'output aggiungendo `|more` al

cmdlet.

Esempio: `HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

L'impostazione predefinita della riga di comando richiede autorizzazioni di amministratore per l'esecuzione. Aggiungere il parametro `-SkipAdminCheck` per ignorare la necessità di autorizzazioni di amministratore.

### Codici di uscita

I codici di uscita spiegano il risultato dei controlli di Cloud Health Check all'interno della riga di comando. Per ottenere il codice di uscita, è necessario aggiungere `start /wait` prima del cmdlet.

Esempio: `start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

I codici di uscita sono:

- 0 - Normale, controllo completato e superato.
- 1 - Errore, controllo completato con problemi.
- 2 - Errore, controllo non completato con errori.

È inoltre possibile utilizzare il cmdlet `echo %errorlevel%` per ottenere il codice di uscita per l'ultimo comando eseguito.

### Report

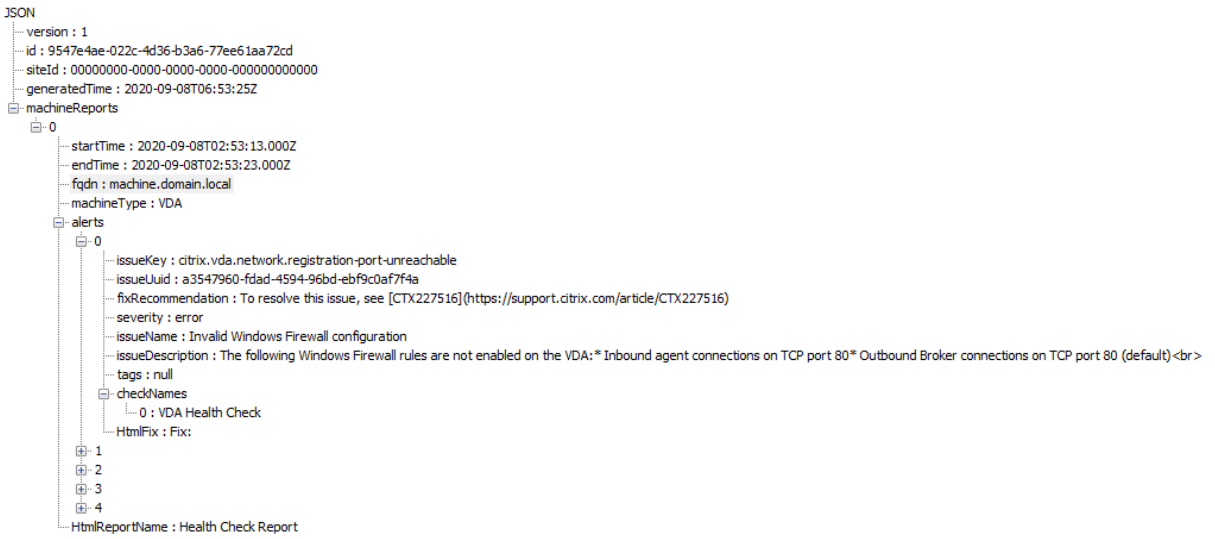
Cloud Health Check crea cartelle con il nome della macchina in `HealthCheckDataFolder` della macchina di destinazione. Vengono creati un file .html e un file .json sulla macchina in cui è installato Cloud Health Check. I report del controlli di integrità si trovano nella cartella `HealthCheckDataFolder` all'interno di `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

I report vengono creati solo quando esistono problemi sul computer di destinazione.

> **Nota:**
>
> I file di report vengono sovrascritti se il nome del report specificato è già esistente.

Gli avvisi e le informazioni di base vengono memorizzati nel report in formato .json.



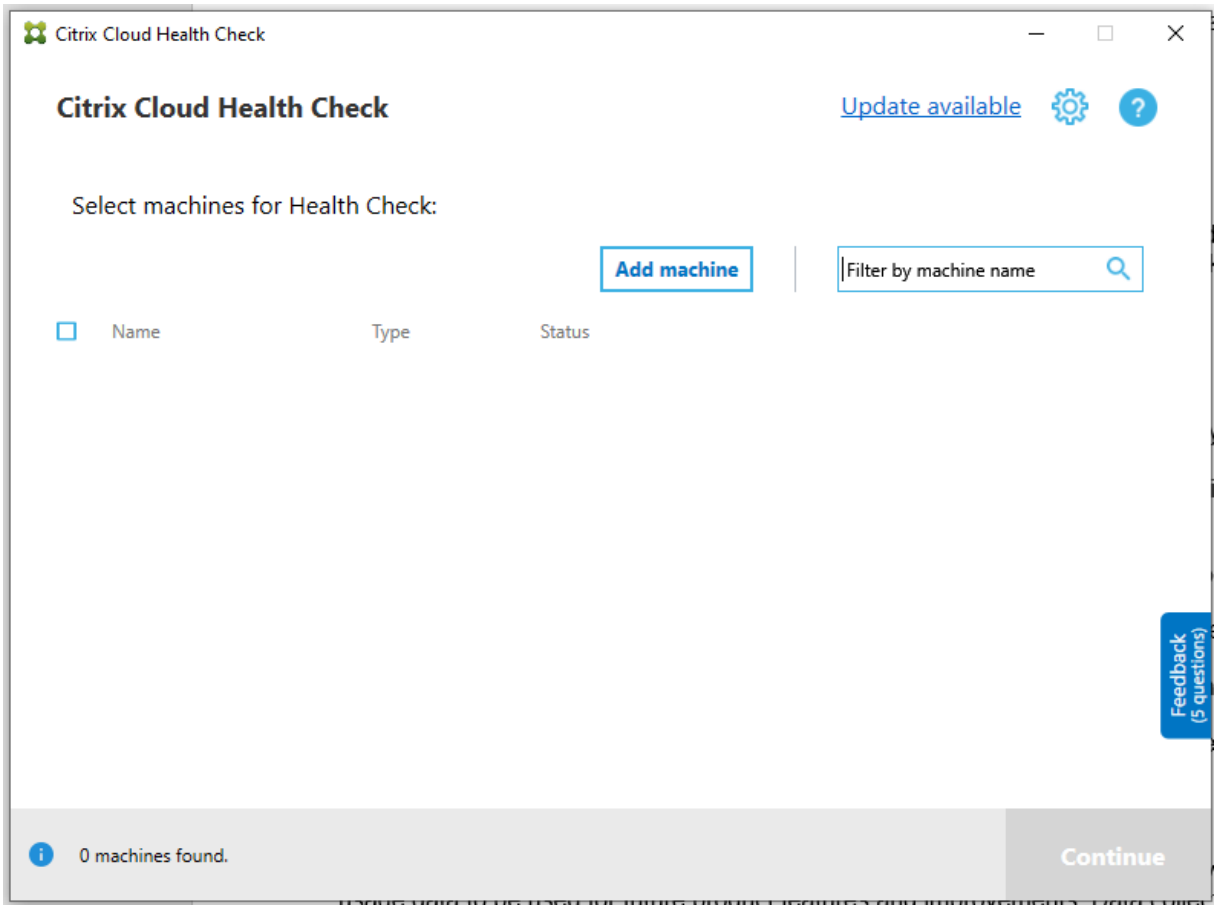

I codici dei report sono:

- **issueKey**: descrizione in solo testo del problema.
- **issueUuid**: stringa identificativa univoca del problema.
- **fixRecommendation**: suggerimento di correzione del problema.
- **severity**: indica se il problema deve essere risolto. Un errore può indicare che il componente (VDA o StoreFront) non funziona correttamente e un avviso indica che il componente può funzionare ma potrebbe presentare alcuni potenziali problemi.
- **issueName**: titolo del problema.
- **issueDescription**: descrizione dettagliata del problema.

## Aggiornare Cloud Health Check

Se è disponibile una nuova versione di Cloud Health Check, viene visualizzato un collegamento Update available in alto a destra nella finestra Cloud Health Check. Fare clic sul collegamento per accedere a Citrix Downloads e ottenere la nuova versione.



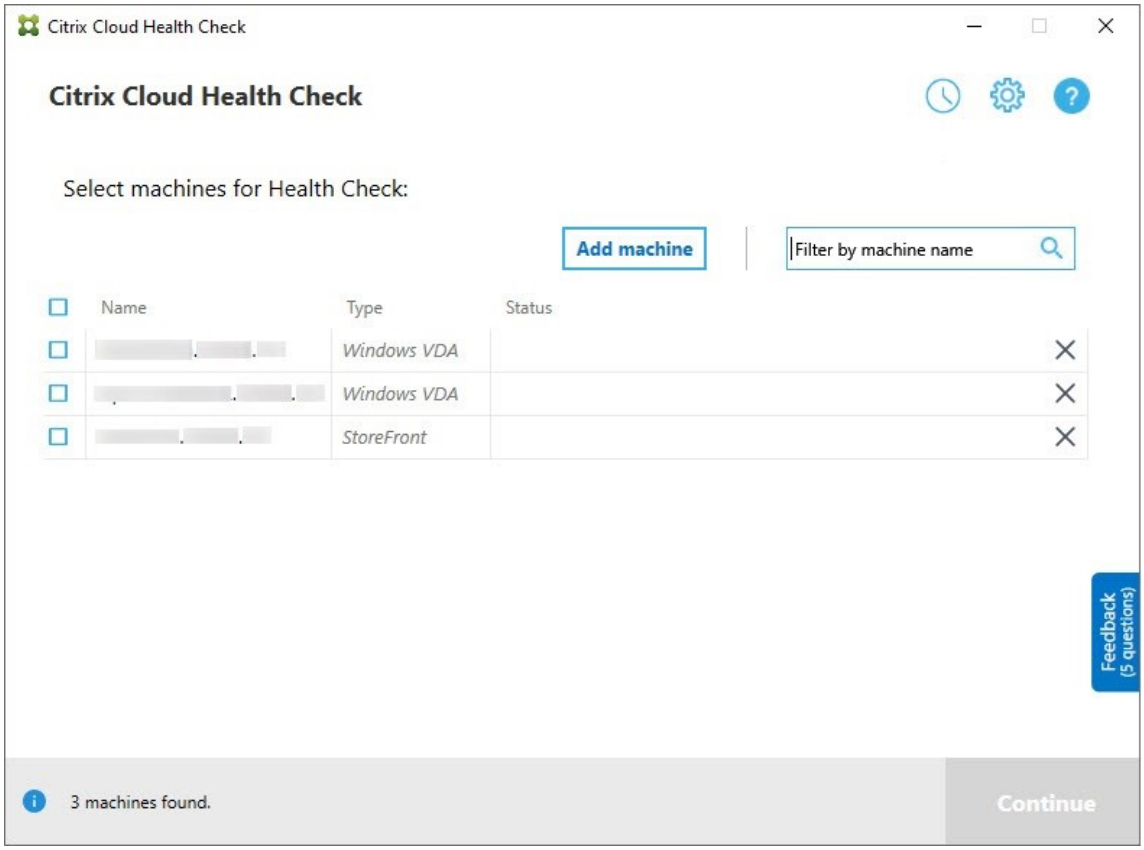

## Utilità di pianificazione di Cloud Health Check

Utilizzare l'utilità di pianificazione di Cloud Health Check per eseguire controlli di integrità periodici.

### Impostare la pianificazione

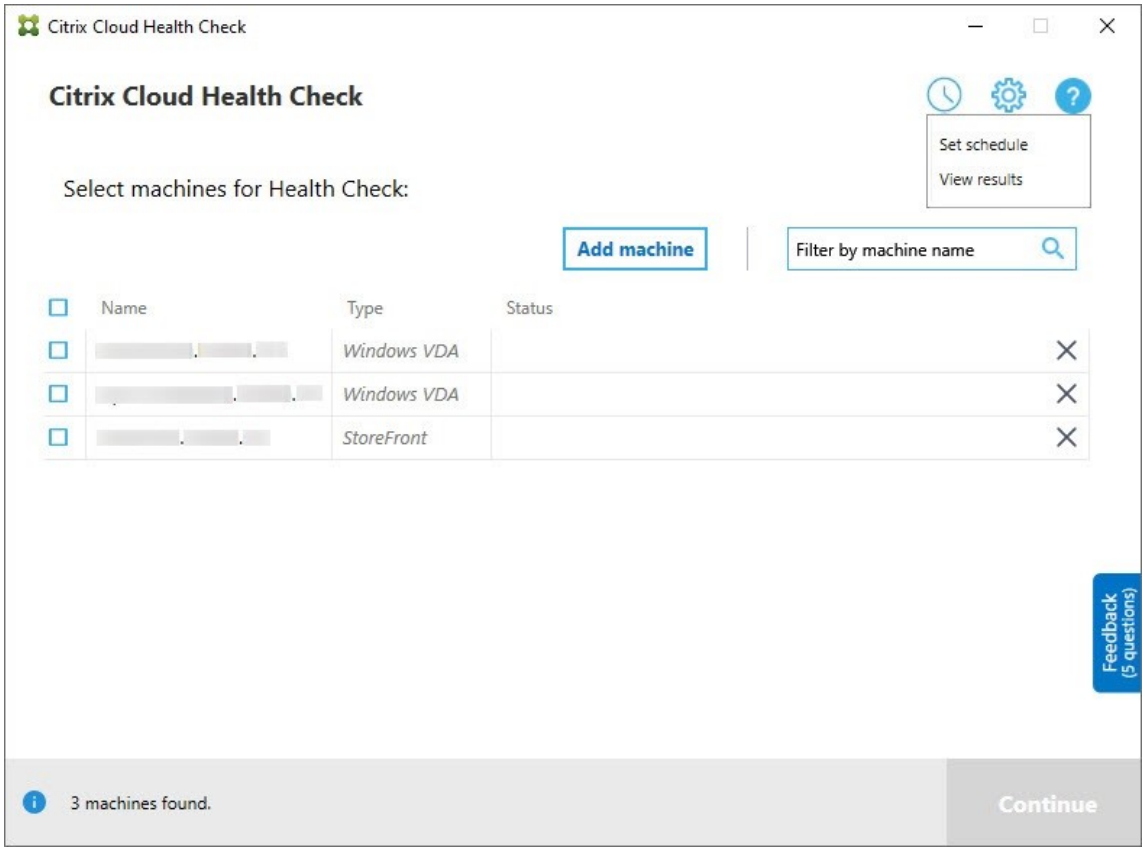
1. Fare clic su **Add machine** nella finestra principale di Cloud Health Check per aggiungere macchine su cui si desidera eseguire controlli periodici.




2. Fare clic sull'icona dell'orologio, quindi su **Set schedule** (Imposta pianificazione).




3. Selezionare un orario per la pianificazione, quindi fare clic su **Next**. L'attività può essere impostata per la ripetizione selezionando la casella di controllo **Repeat task every** (Ripeti attività ogni).
4. Scegliere di visualizzare i risultati nel registro eventi di Windows. L'attività può essere impostata per scrivere i risultati nel registro eventi di Windows.
5. Scegliere di attivare uno script PowerShell personalizzato al termine del controllo pianificato, quindi fare clic su **Next**.

    - Fare clic su **Edit** per modificare il contenuto dello script in Windows PowerShell ISE, se necessario.
    - Fare clic su **Locate** (Individua) per aprire il percorso del file e utilizzare un editor diverso per aprire il file e modificare lo script.
    - Fare clic su **Reset** per ripristinare l'impostazione originale dello script.

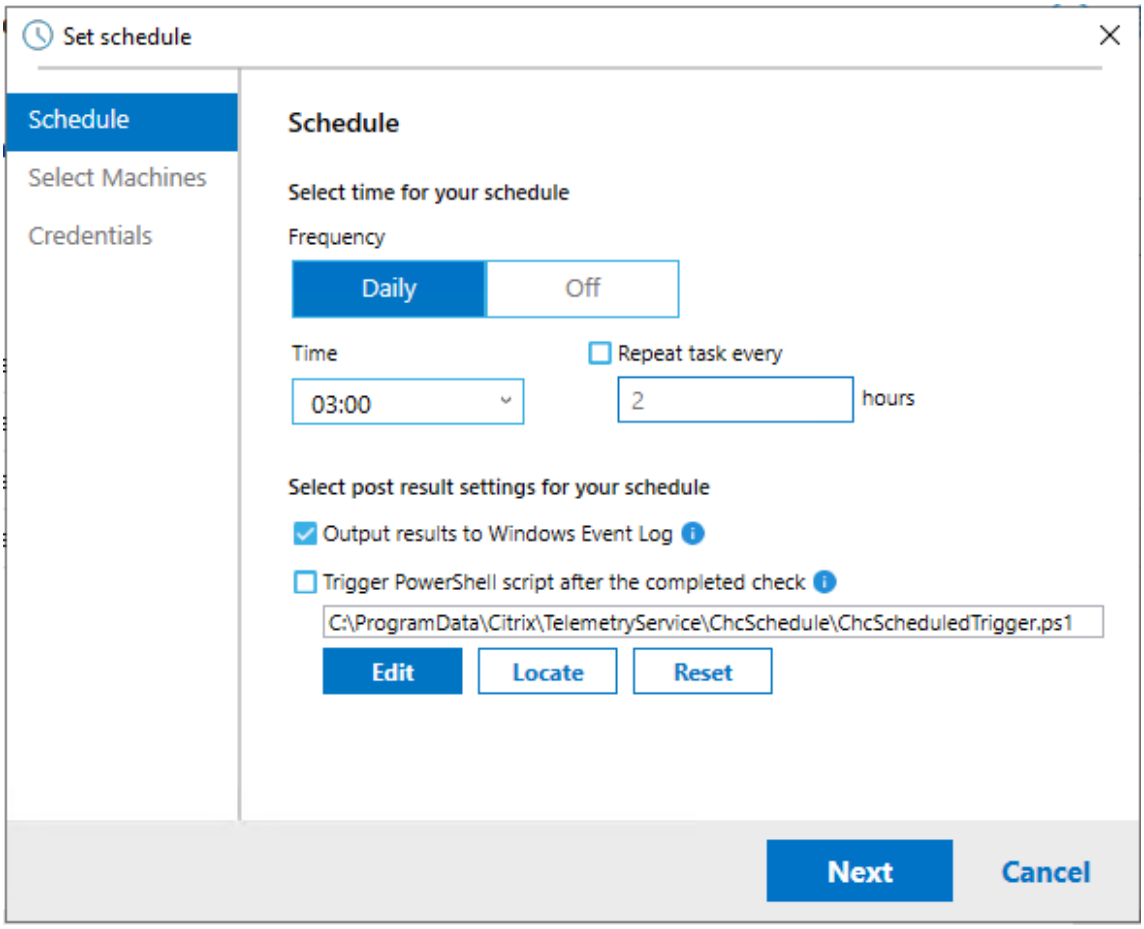
    > **Nota:**
    >
    > – Non è possibile modificare il nome e il percorso dello script.
    > – Utilizzando lo script ChcShceduledTrigger.ps1, è possibile implementare azioni personalizzate, ad esempio l'invio di un'e-mail dopo che il rapporto di controllo

> pianificato è pronto. Aggiungere il seguente codice alla fine dello script. Personalizzare il codice per aggiungere gli account e-mail e l'indirizzo del server SMTP corretti. Viene inviata una notifica e-mail utilizzando le credenziali dell'account da cui viene eseguita l'attività pianificata.

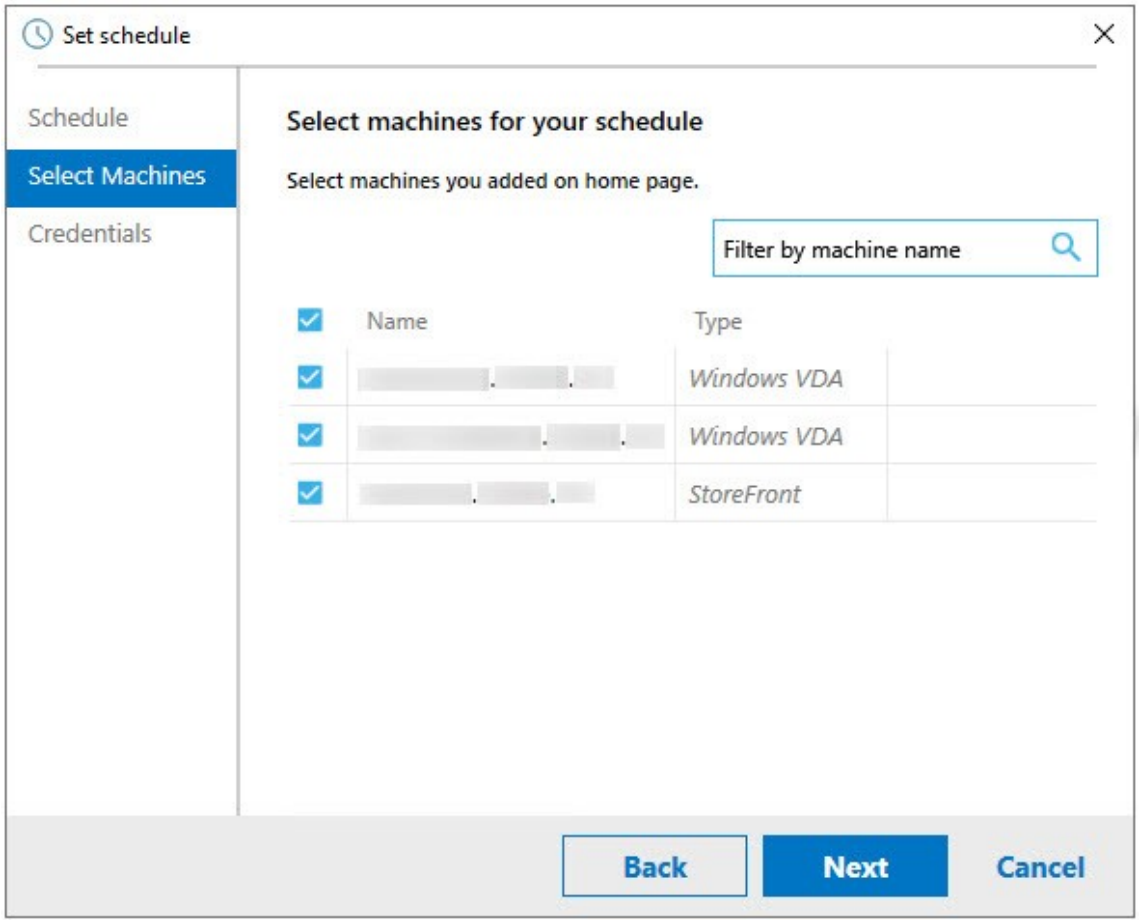
```
#Sending email example code:
$body = "CreatedTime: $($report.CreatedTime)"
$body = $body + "`nStatusCode: $($report.StatusCode)"
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"
$from = "mock_email_accout"
$to = "mock_email_accout"
$smtpServer = "mock_smtp_server"

Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler
    Report" -Body $body -From $from -To $to -SmtpServer $smtpServer
<!--NeedCopy-->
```



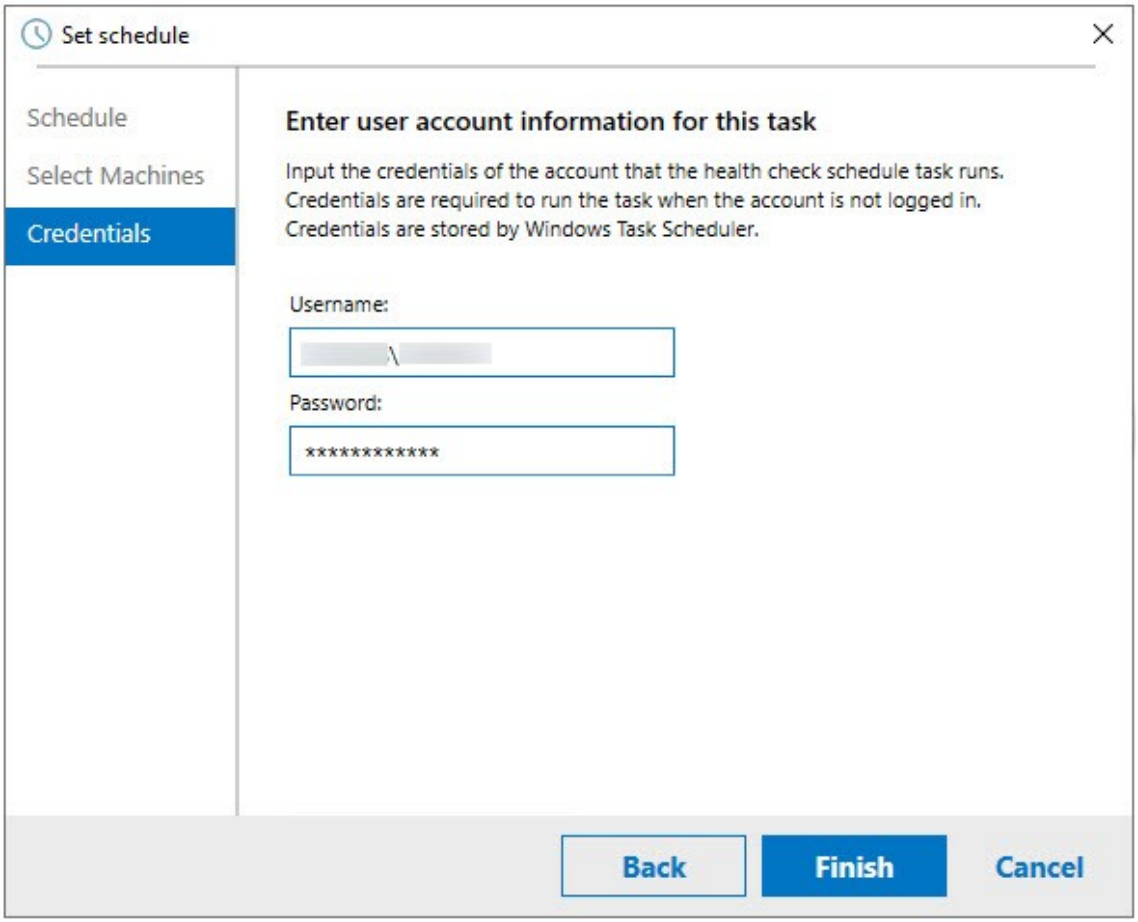

6. Selezionare le macchine per la pianificazione, quindi fare clic su **Next**.

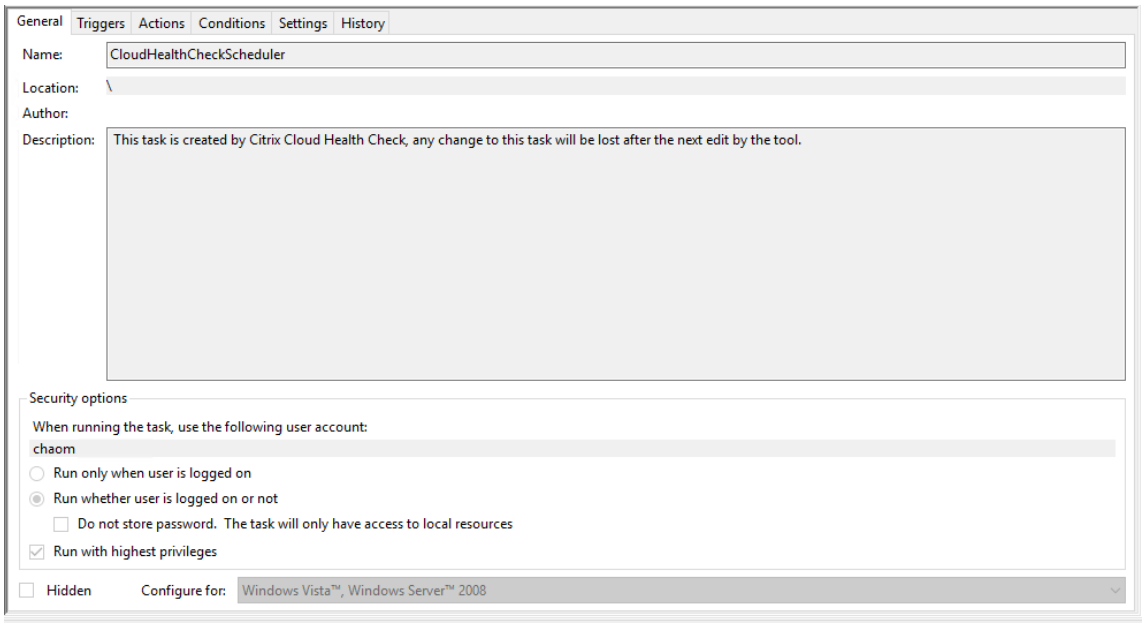



7. Immettere le credenziali dell'account su cui viene eseguita l'attività, quindi fare clic su **Finish**.



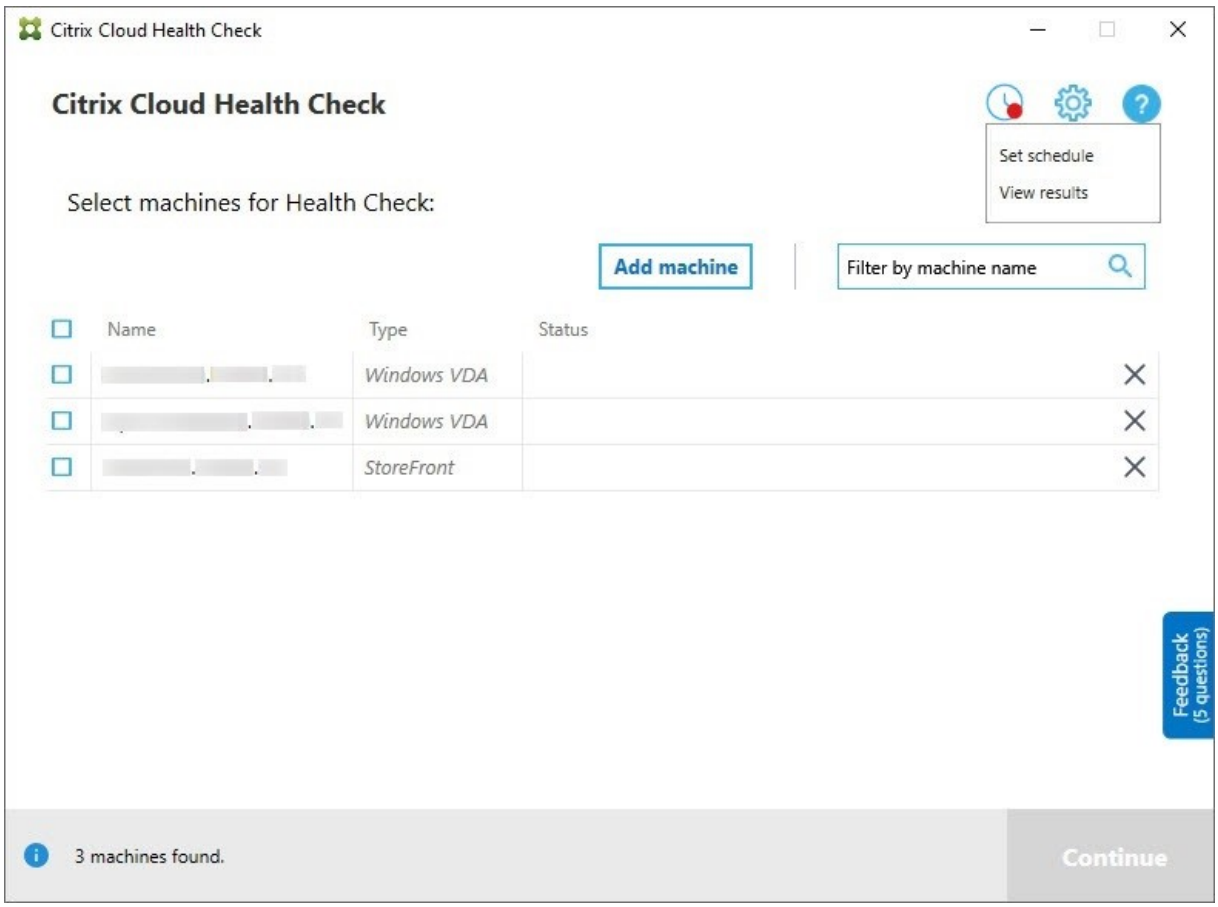

8. Viene creata un'attività CloudHealthCheckScheduler nell'Utilità di pianificazione di Windows.



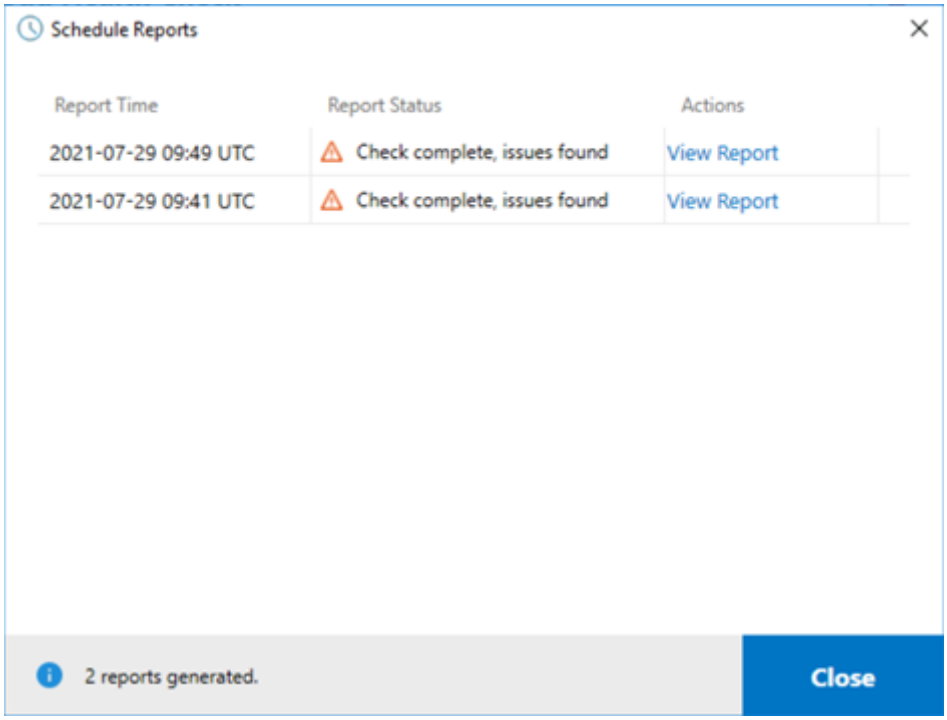
### Visualizzare i risultati della pianificazione

L'icona dell'orologio con un punto rosso indica che sono stati rilevati problemi nell'ultimo controllo. Per visualizzare i risultati, fare clic sull'icona dell'orologio, quindi su **View results** (Visualizza risultati).

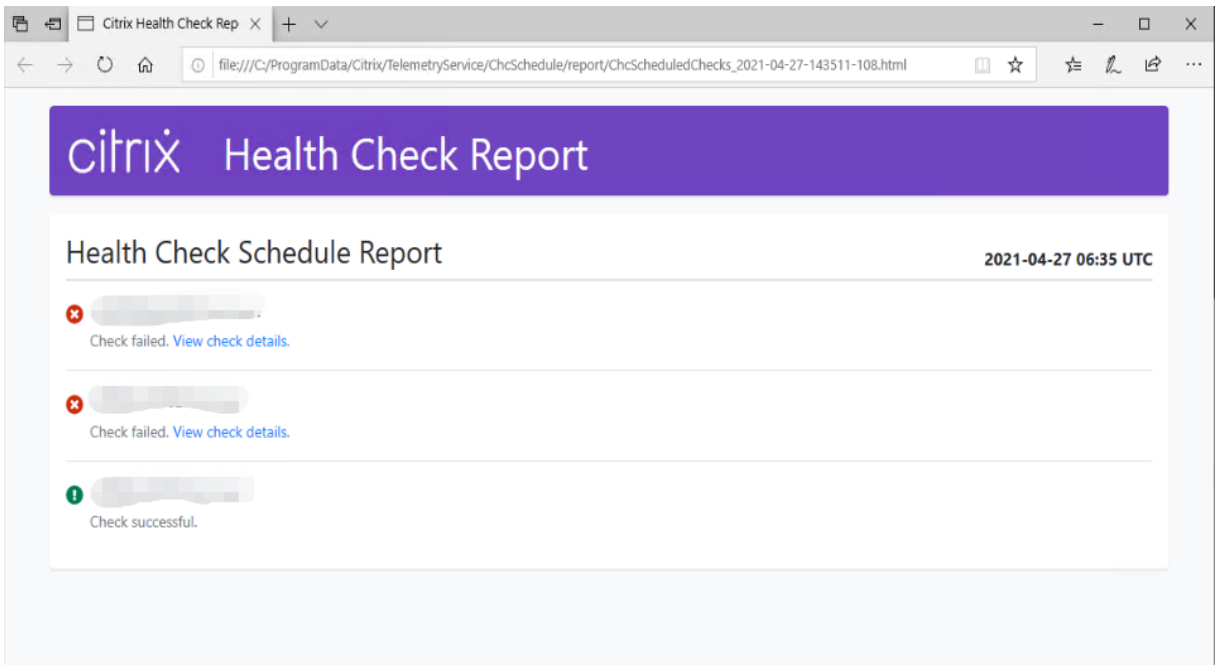



La pagina Schedule Reports mostra i risultati per tutte le attività di controllo di integrità pianificate. Fare clic su **View Report** per visualizzare il report di ogni pianificazione.

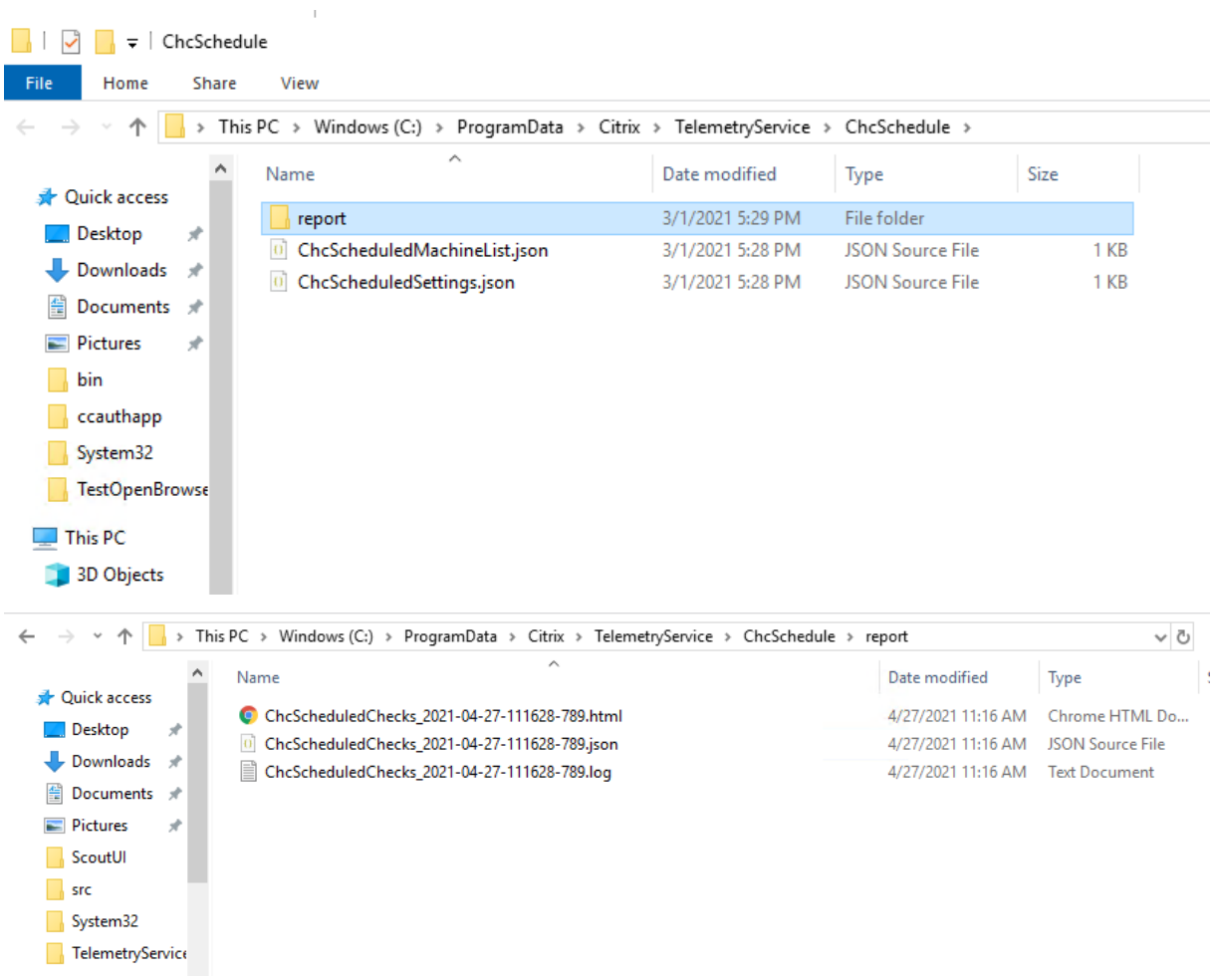



Il report html contiene il rapporto complessivo per ogni pianificazione. Di seguito è riportato un esempio di report:

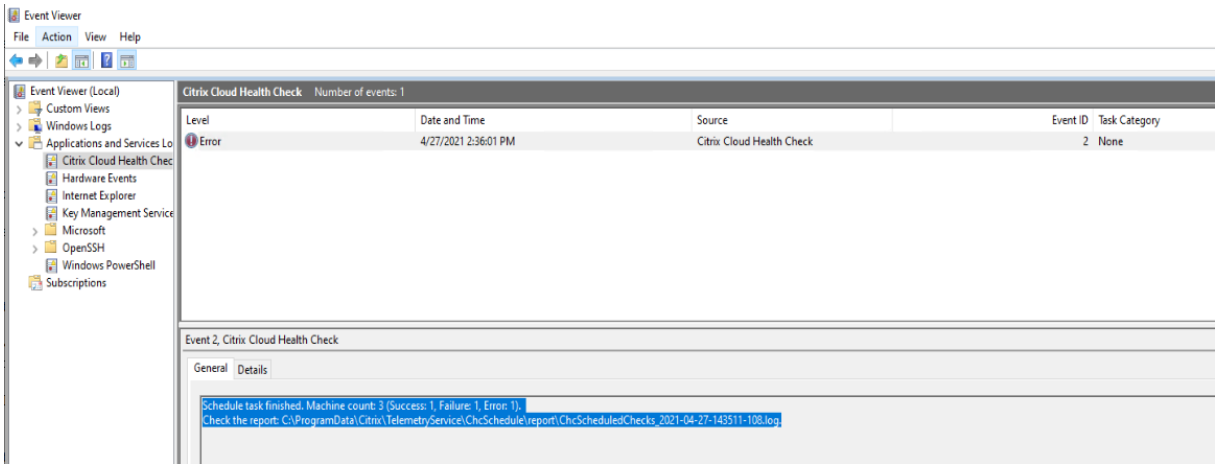



Tutti i risultati del controllo di integrità sono memorizzati in una cartella denominata ChcSchedule. Cloud Health Check crea tre file a ogni esecuzione di controllo. Sono conservati fino a 500 log di iterazione.



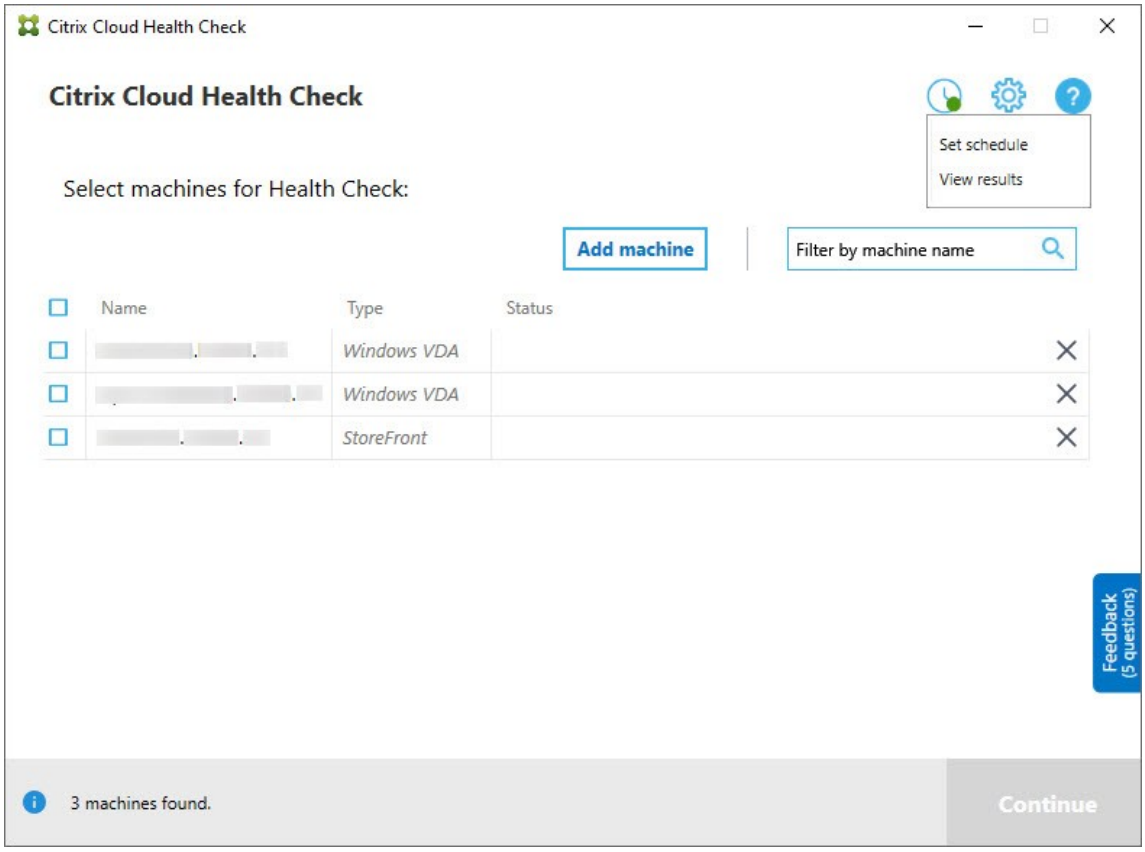

Se la casella di controllo **Output results to Windows Event Log** (Output dei risultati nel Registro eventi di Windows) è selezionata, il risultato del controllo viene inviato anche al Registro eventi di Windows.



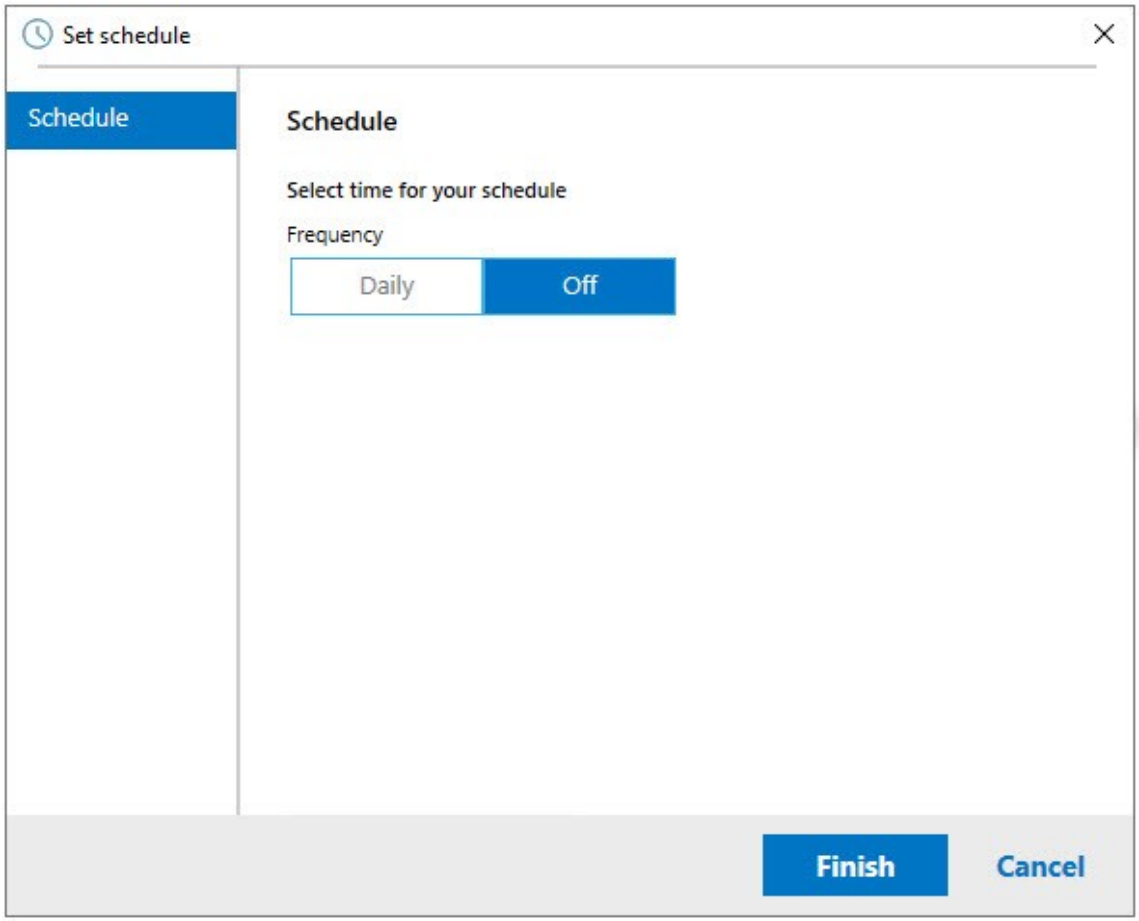
### Disabilitare le pianificazioni

1. Fare clic sull'icona dell'orologio, quindi su **Set schedule** (Imposta pianificazione).




2. Fare clic su **Off**, quindi fare clic su **Finish** per disattivare il pianificatore.




**Ulteriori informazioni**

- È prima necessario aggiungere o importare i VDA in Cloud Health Check. Per ulteriori informazioni, vedere Importare macchine VDA.
- Il pianificatore di Cloud Health Check può pianificare solo un'attività alla volta su una macchina aggiunta a un dominio. Se si imposta la pianificazione più volte, avrà effetto solo l'ultima.

## Test di verifica

Prima dell'avvio di un controllo di integrità, vengono automaticamente eseguiti test di verifica su ogni macchina selezionata. Questi test assicurano che siano soddisfatti i requisiti per l'esecuzione di un controllo di integrità. Se un test non riesce per una macchina, Cloud Health Check visualizza un messaggio con le azioni correttive suggerite.

- **Cloud Health Check cannot reach this machine** (Cloud Health Check non può raggiungere questa macchina); assicurarsi che:
  - La macchina sia accesa.

  - La connessione di rete funzioni correttamente. Ciò può includere la verifica che il firewall sia configurato correttamente.
  - La condivisione di file e stampanti sia attivata. Per istruzioni, vedere la documentazione Microsoft.

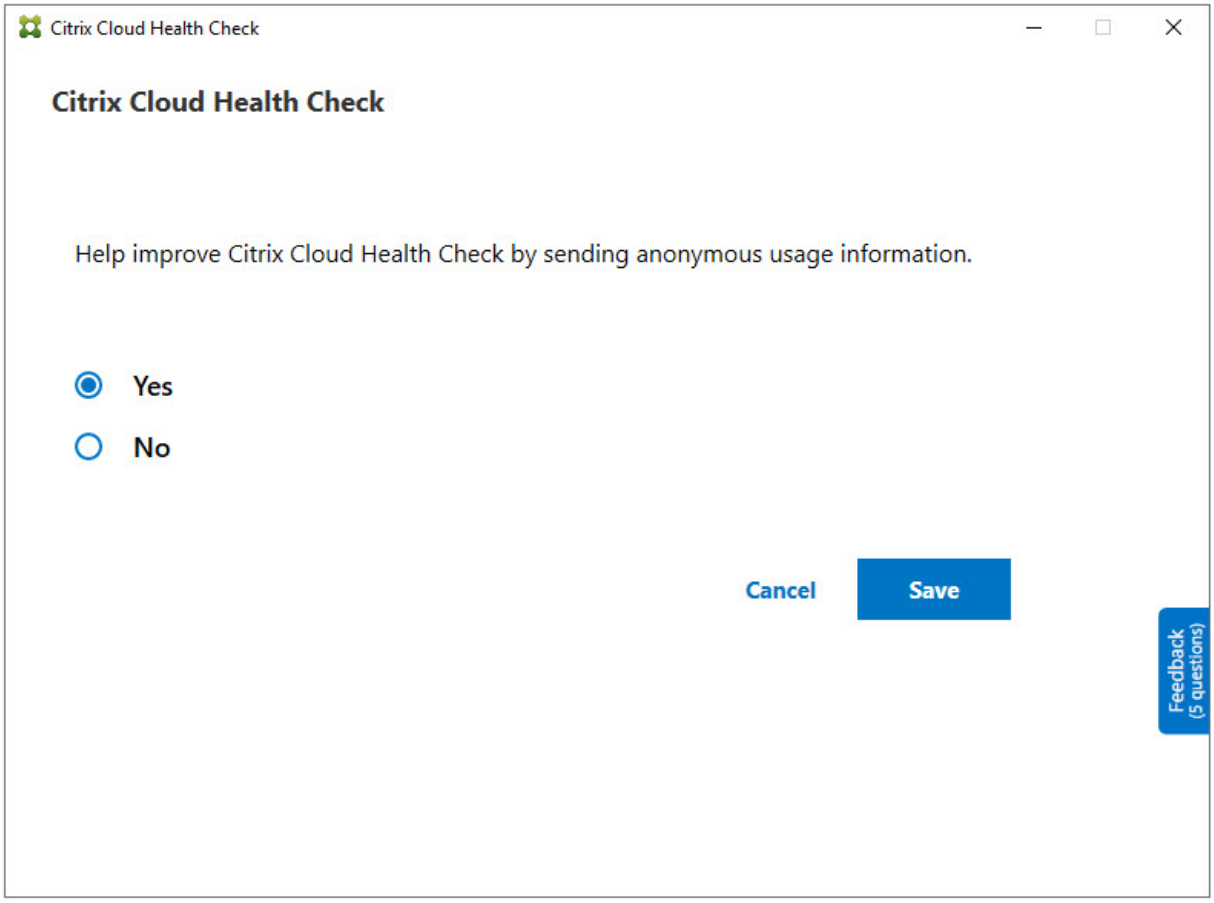
- **Enable PSRemoting and WinRM** (Abilitare PSRemoting e WinRM): è possibile abilitare la comunicazione remota di PowerShell e WinRM eseguendo PowerShell come amministratore, quindi eseguendo il cmdlet Enable-PSRemoting. Per ulteriori informazioni, vedere la Guida di Microsoft relativa al cmdlet.
- **Cloud Health Check richiede PowerShell 3.0 o versione successiva**: installare PowerShell 3.0 o versione successiva sulla macchina, quindi abilitare la comunicazione remota di PowerShell.
- **WMI is not running on the machine** (WMI non è in esecuzione sul computer): assicurarsi che l'accesso a Windows Management Instrumentation (WMI) sia abilitato.
- **WMI connections blocked** (Connessioni WMI bloccate): abilitare WMI nel servizio Windows Firewall.

### Raccolta dei dati di utilizzo

Quando si utilizza Cloud Health Check, Citrix impiega Google Analytics per raccogliere dati anonimi sull'utilizzo finalizzati allo sviluppo di funzionalità e di miglioramenti futuri dei prodotti. La raccolta dei dati è abilitata per impostazione predefinita.

Per modificare la raccolta e il caricamento dei dati di utilizzo, fare clic sul simbolo dell'ingranaggio **Settings** (Impostazioni) nell'interfaccia utente di Cloud Health Check. È quindi possibile scegliere se inviare le informazioni selezionando **Sì** o **No** e quindi facendo clic su **Save**.




### Correzione automatica

La correzione automatica consente a Cloud Health Check di rilevare e risolvere automaticamente determinati problemi modificando le impostazioni o riavviando i servizi.

La correzione automatica controlla i seguenti elementi di registrazione VDA, con le correzioni consigliate:

- Appartenenza al dominio macchina VDA
  - Correzione: verificare il canale di sicurezza della connessione con un modello di "riparazione"per correggere
- Stato dei servizi VDA
  - Correzione: riavviare il servizio BrokerAgent
- Comunicazione con il controller
  - Correzione: riavviare il servizio BrokerAgent
- Sincronizzazione temporale con il controller

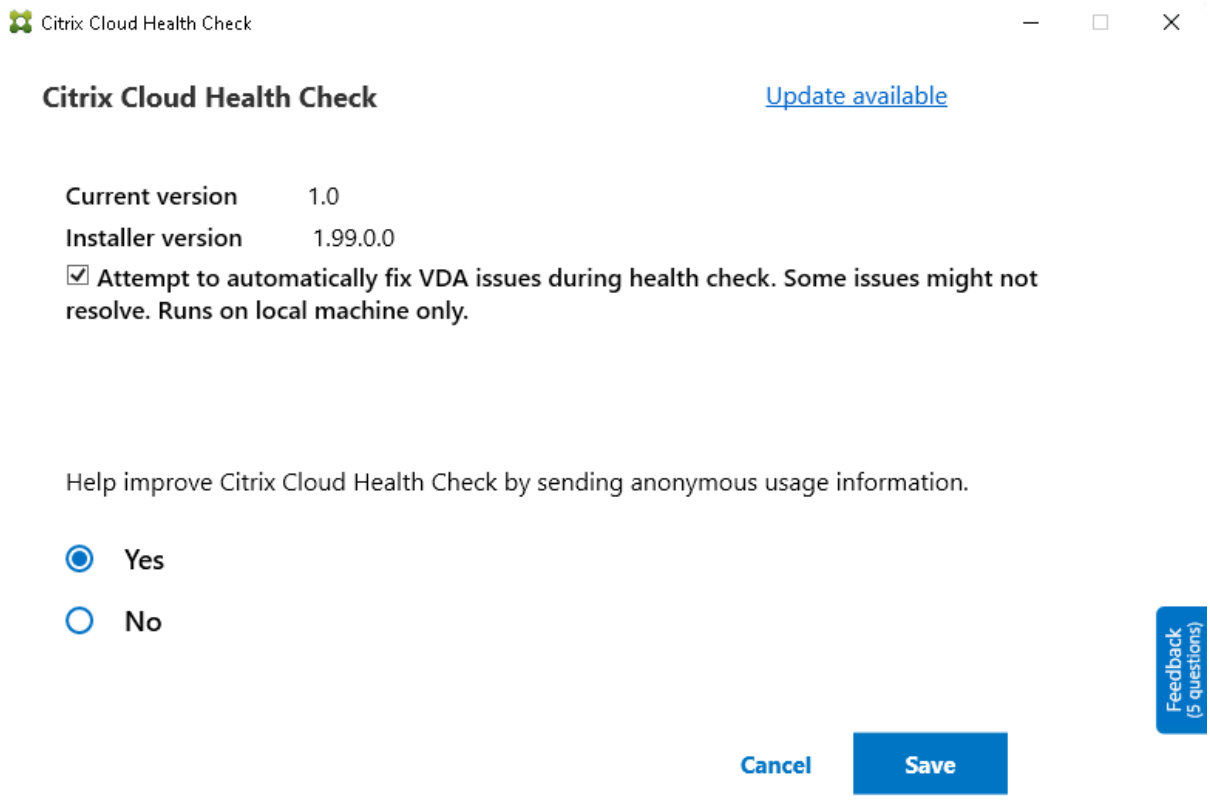
 

  - Correzione: eseguire il comando W32tm

Per l'avvio delle sessioni, la correzione automatica controlla il seguente elemento, con la correzione consigliata:

- Stato dei servizi di avvio della sessione
  - Correzione: riavviare il servizio BrokerAgent

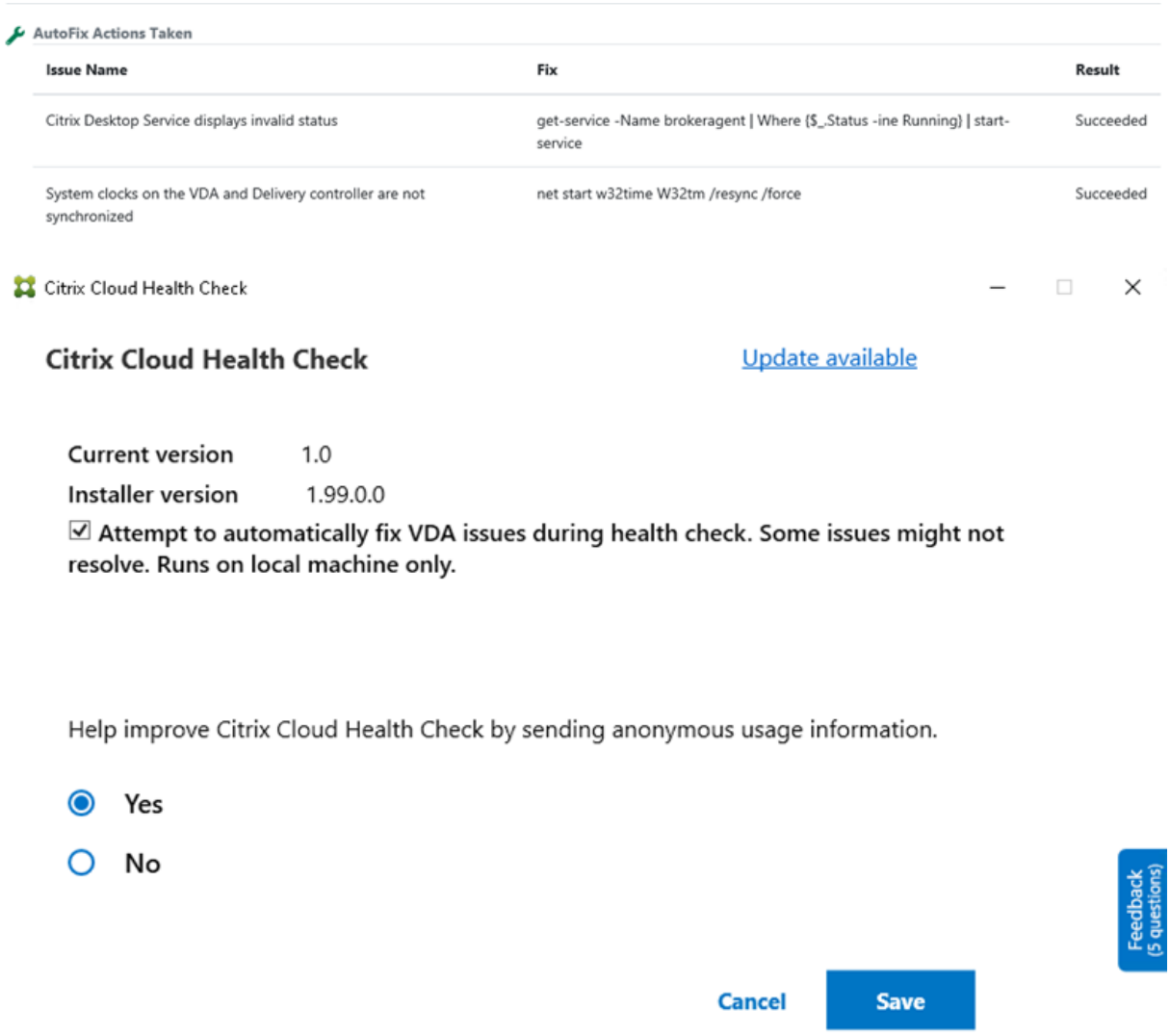
Questa funzionalità è abilitata per impostazione predefinita. Per disabilitarlo, fare clic sull'icona a forma di ingranaggio nell'angolo in alto a destra della finestra principale di Cloud Health Check, quindi deselezionare **Attempt to automatically fix VDA issues during health check** (Tenta di risolvere automaticamente i problemi VDA durante il controllo di integrità).




**Rapporto sui risultati**

Dopo aver eseguito la correzione automatica, c'è una sezione nel rapporto dei risultati del controllo che visualizza tutti i dettagli:




## Risoluzione dei problemi

Quando l'esecuzione di Cloud Health Check non riesce o si verifica un'eccezione, controllare il registro di Cloud Health Check in `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

Il registro di Cloud Health Check per ogni computer di destinazione è in `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

Per abilitare il registro di debug:

Modificare `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`, aggiornare `<add name="TraceLevelSwitch"value="3"/>` to `<add name="TraceLevelSwitch"value="4"/>`, salvare il file e riaprire Cloud Health Check.

### Commenti e suggerimenti

Per lasciare commenti su Cloud Health Check, compilare il sondaggio Citrix.

## Registrazione della configurazione

December 18, 2023

> **Nota:**
>
> I record del registro di configurazione vengono visualizzati solo in inglese, indipendentemente dalla lingua selezionata per il proprio account Citrix Cloud. Le date e le ore associate a tali record sono in formato MM/GG/AA, espresso in Coordinated Universal Time (UTC).

La registrazione della configurazione è una funzionalità che acquisisce le modifiche alla configurazione di distribuzione e le attività amministrative di Citrix Virtual Apps and Desktops e Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) in un database di registrazione in Citrix Cloud. È possibile utilizzare il contenuto registrato per:

- Diagnosticare e risolvere i problemi dopo aver apportato modifiche alla configurazione. Il log fornisce una traccia degli spostamenti.
- Facilitare la gestione delle modifiche e tenere traccia delle configurazioni.
- Segnalare le attività amministrative.

In questo Citrix DaaS, la registrazione della configurazione è sempre abilitata. Non è possibile disabilitarla.

Dall'interfaccia di gestione della configurazione completa, è possibile visualizzare il contenuto del registro di configurazione, filtrato per intervalli di date o per ricerca full-text. È inoltre possibile generare un report CSV utilizzando PowerShell. Da questa console, non è possibile modificare o eliminare il contenuto del registro. È possibile utilizzare l'SDK Remote PowerShell per pianificare l'eliminazione periodica dei dati dal registro.

Autorizzazioni richieste (vedere Amministrazione delegata):

- Gli amministratori completi di Citrix Cloud, nonché gli amministratori Cloud di Citrix DaaS e gli amministratori di sola lettura possono visualizzare i log di configurazione nella console **Manage** (Gestione).
- Gli amministratori completi e gli amministratori cloud possono anche scaricare un rapporto CSV dell'attività di registrazione, utilizzando PowerShell.

### Cosa viene registrato

Le seguenti operazioni vengono registrate:

- Modifiche alla configurazione e attività amministrative avviate dalle schede **Manage** e **Monitor**
- Script PowerShell
- Richieste API REST

> **Nota:**
>
> Non è possibile visualizzare le voci di registro per le operazioni interne della piattaforma Citrix Cloud, come la configurazione e la gestione del database.

Esempi di modifiche alla configurazione registrate includono l'utilizzo (creazione, modifica, eliminazione, assegnazione) di quanto segue:

- Cataloghi di macchine
- Gruppi di consegna (inclusa la modifica delle impostazioni di gestione dell'alimentazione)
- Ruoli e ambiti dell'amministratore
- Risorse e connessioni host
- Criteri Citrix tramite la console **Manage**

Esempi di modifiche amministrative registrate includono:

- Gestire l'alimentazione di una macchina virtuale o di un desktop utente
- Gestire o monitorare le funzioni inviando un messaggio a un utente

Le seguenti operazioni non vengono registrate: (molte di queste non sono disponibili per gli amministratori dei clienti)

- Operazioni automatizzate come l'attivazione della gestione in pool delle macchine virtuali.
- Azioni derivanti da criteri implementate tramite la console di gestione dei criteri di gruppo (GPMC). Utilizzare gli strumenti Microsoft per visualizzare i registri di tali azioni.
- Modifiche apportate tramite il Registro di sistema o da fonti diverse dall'interfaccia di gestione della configurazione completa, Monitor o PowerShell.

### Visualizzare il contenuto del registro di configurazione

Per visualizzare il contenuto del registro di configurazione, attenersi alla seguente procedura:

1. Accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Logging > Events** (Registrazione > Eventi) nel riquadro a sinistra.

Per impostazione predefinita, nel riquadro centrale sono elencati cronologicamente i contenuti del registro (prima le voci più recenti), separati per data. È possibile effettuare le seguenti operazioni:

- Ordinare la visualizzazione per intestazione di colonna.
- Filtra la visualizzazione specificando un intervallo di giorni o un periodo di tempo personalizzato oppure inserendo del testo nella casella di ricerca. Per tornare alla visualizzazione standard dopo aver utilizzato la ricerca, eliminare il testo nella casella Search.

Caratteristiche del display:

- Le operazioni di alto livello create durante la gestione e il monitoraggio sono elencate nel riquadro centrale superiore. Un'operazione di alto livello comporta una o più chiamate ai servizi e all'SDK PowerShell, che sono operazioni di basso livello. Quando si seleziona un'operazione di alto livello nel riquadro centrale, il riquadro inferiore visualizza le operazioni di basso livello.
- Se si crea un'operazione di basso livello in PowerShell senza specificare un'operazione padre di alto livello, la registrazione della configurazione crea un'operazione surrogata di alto livello.
- Se un'operazione non riesce prima del completamento, l'operazione di log potrebbe non essere completata nel database. Ad esempio, un record di avvio non ha alcun record di arresto corrispondente. In questi casi, il log indica che mancano informazioni. Quando si visualizzano i log in base a intervalli di tempo, vengono visualizzati i registri incompleti se i dati nei log corrispondono ai criteri. Ad esempio, se si richiedono i registri degli ultimi cinque giorni e un log con un'ora di inizio negli ultimi cinque giorni non ha un'ora di fine, questo viene incluso.
- Ricorda: non è possibile visualizzare le voci di registro per le operazioni interne della piattaforma Citrix Cloud, come la configurazione e la gestione del database.

### Visualizzare le attività relative alle operazioni del catalogo macchine

Per visualizzare le operazioni relative alle operazioni del catalogo macchine, accedere a **Manage > Full Configuration > Logging > Tasks** (Gestione > Configurazione completa > Registrazione > Attività). La scheda **Task** visualizza solo le attività relative ai cataloghi creati tramite Machine Creation Services (MCS) o Provisioning Services (PVS). In particolare, vengono visualizzate le attività associate alle seguenti operazioni del catalogo macchine:

- Create catalogs (Crea cataloghi)
- Clone catalogs (Clona cataloghi)
- Add machines (Aggiungi macchine)
- Remove machines (Rimuovi macchine)
- Update a catalog (update images or machines) [Aggiorna un catalogo (aggiorna immagini o macchine)]
- Roll back machine updates (Esegui rollback degli aggiornamenti macchine)

> **Suggerimento:**
>
> La scheda **Tasks** visualizza solo le attività relative alle modifiche dello schema di provisioning (creazione o modifica di uno schema di provisioning).

Un'attività può trovarsi nel seguente stato:

- Completed (Completata)
- Not started (Non avviata)
- Running (In esecuzione)
- Canceled (Annullata)
- Failed (Non riuscita)
- Unknown (Sconosciuto)

Per annullare un'operazione in esecuzione, selezionare l'attività e quindi fare clic su **Cancel**. La cancellazione richiede un po'di tempo per essere completata.

Esempi di attività registrate includono:

- Aggiornamento dell'immagine completato per un determinato catalogo
- Errore durante l'aggiornamento dell'immagine per un determinato catalogo
- Aggiornamento dell'immagine annullato per un determinato catalogo
- Provisioning di macchine virtuali in un determinato catalogo
- Rimozione di macchine virtuali da un determinato catalogo
- Creazione di un determinato catalogo

Per impostazione predefinita, nel riquadro centrale sono elencate cronologicamente le attività inserite nel registro (prima le voci più recenti), separate per data. È possibile ordinare la visualizzazione per intestazione di colonna. Per cancellare le attività completate, fare clic su **Clear Completed Tasks** (Cancella attività completate) nella scheda **Tasks**.

### Visualizzare i log delle API

Per visualizzare i log delle API REST, passare a **Manage > Full Configuration > Logging > APIs** (Gestisci > Configurazione completa > Registrazione > API). La scheda **API** visualizza le richieste API REST effettuate durante un determinato periodo di tempo.

Tenere presente le seguenti considerazioni:

- I registri dell'API REST vengono cancellati dopo che ci si scollega dalla console (vengono cancellati anche se si aggiorna la finestra del browser).
- Tutte le operazioni che si svolgono nella console e comportano chiamate API hanno le corrispondenti richieste API visualizzate nella scheda **APIs**.

- Il display elenca le richieste API in ordine cronologico (prima le voci più recenti), separate per data. Il numero massimo di richieste API sul display è 1.000.

### Associare i metadati ai registri di configurazione

È possibile allegare metadati ai registri di configurazione associando una coppia di `name-value` denominata `MetadataMap` ai record di registro.

> **Nota:**
>
> - È possibile allegare metadati solo a oggetti operativi di alto livello.
> - I metadati sono associati ai record esistenti al momento dell'esecuzione.

#### Impostare i metadati

Eseguire il comando PowerShell `Set-LogHighLevelOperationMetadata` per associare un record di registro a `MetadataMap`.
`Set-LogHighLevelOperationMetadata` accetta i seguenti parametri:

- **Id**: ID dell'operazionedi alto livello.
- **InputObject**: leoperazioni di alto livello a cui si aggiungono i metadati. Si tratta di un'alternativa al parametro `Id` in cui un oggetto operativo di alto livello o un elenco di oggetti viene passato al comando PowerShell.
- **Name**: nome della proprietà dei metadati da aggiungere. La proprietà deve essere univoca per l'operazione di alto livello specificata. La proprietà non può contenere nessuno dei seguenti caratteri:
  `()\/;:#.*?=<>|[]"'`
- **Value**: valore della proprietà.
- **Map**: dizionario delle coppie (nome, valore) per le proprietà. Si tratta di un'alternativa all'impostazione dei metadati utilizzando i parametri `-Name` e `-Value`.

Ad esempio, per allegare i metadati a tutti i record di registro di alto livello con Id 40, eseguire il seguente comando PowerShell:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

Per allegare i metadati al record di alto livello con l'utente `abc@example.com`, eseguire il seguente comando PowerShell:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

#### Effettuare il recupero utilizzando i metadati

Per recuperare i record di registro utilizzando i metadati associati, eseguire i seguenti comandi PowerShell:

- Cercare per chiave e valore:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Cercare per valore e per qualsiasi chiave:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Cercare per chiave e qualsiasi valore:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

#### Rimuovere i metadati

Eseguire il comando PowerShell `Remove-LogHighLevelOperationMetadata` per rimuovere i metadati associati.
`Remove-LogHighLevelOperationMetadata` accetta i seguenti parametri:

- **Id**: ID dell'operazionedi alto livello.
- **InputObject**: leoperazioni di alto livello a cui si aggiungono i metadati. Si tratta di un'alternativa al parametro `Id`‘ in cui un oggetto operativo di alto livello o un elenco di oggetti viene passato al comando PowerShell.
- **Name**: nome della proprietà dei metadati da rimuovere. Impostare su $null per rimuovere tutti i metadati per l'oggetto specificato.
- **Map**: dizionario delle coppie (nome, valore) per le proprietà. Può essere una hashtable (creata con @{“name1”= “val1”; “name2”= “val2”}) o un dizionario di stringhe (creato con la stringa “System.Collections.Generic.Dictionary[String, String]”) del nuovo oggetto. Le proprietà con i nomi corrispondenti alle chiavi nella mappa vengono rimosse.

### Generare report

Per generare un report CSV o HTML contenente i dati del registro di configurazione, utilizzare i cmdlet PowerShell per il servizio ConfigLogging nell'SDK Remote PowerShell di Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

### Pianificare l'eliminazione dati periodica

Utilizzare l'SDK Remote PowerShell per specificare per quanto tempo i dati vengono conservati nel database di registrazione della configurazione (questa funzionalità non è disponibile nell'interfaccia di gestione Full Configuration [Configurazione completa]). In Citrix DaaS è necessario disporre dell'accesso completo.

Nel cmdlet `Set-LogSite`, il parametro `-LoggingDBPurgeDurationDays` specifica per quanti giorni i dati vengono conservati nel database di registrazione della configurazione prima di essere eliminati automaticamente.

- Per impostazione predefinita, il valore di questo parametro è 0. Un valore zero indica che i dati nel database di registrazione della configurazione non vengono mai eliminati automaticamente.
- Quando si imposta un valore diverso da zero, il database viene controllato una volta ogni 120 minuti. I dati più vecchi del periodo di conservazione vengono eliminati.

Utilizzare `Get-LogSite` per visualizzare il valore corrente del parametro.

### Differenze rispetto a Citrix Virtual Apps and Desktops locale

Se si ha familiarità con la registrazione della configurazione nel prodotto Virtual Apps and Desktops locale, la versione per Citrix Cloud presenta svariate differenze. In Citrix Cloud:

- La registrazione della configurazione è sempre abilitata. Non è possibile disabilitarla. La registrazione obbligatoria non è disponibile.
- Non è possibile modificare la posizione del database di registrazione della configurazione, poiché il database è gestito nella piattaforma Citrix Cloud.
- Le visualizzazioni del registro di configurazione non includono le operazioni e le attività eseguite all'interno della piattaforma Citrix Cloud.
- PowerShell è l'unica scelta disponibile per creare un report CSV o HTML delle operazioni registrate. Nel prodotto locale, i report possono essere generati da Citrix Studio o PowerShell.
- Non è possibile eliminare il contenuto del registro di configurazione

## Amministrazione delegata

October 30, 2023

## Panoramica

Con l'amministrazione delegata in Citrix Cloud, è possibile configurare le autorizzazioni di accesso di cui tutti gli amministratori hanno bisogno, in base al loro ruolo nella vostra organizzazione.

Per impostazione predefinita, gli amministratori hanno l'accesso completo. Questa impostazione consente l'accesso a tutte le funzioni di amministrazione e gestione dei clienti disponibili in Citrix Cloud, oltre a tutti i servizi in abbonamento. Per personalizzare l'accesso di un amministratore:

- Configurare l'accesso personalizzato per le autorizzazioni di gestione generali di un amministratore in Citrix Cloud.
- Configurare l'accesso personalizzato per i servizi in abbonamento. In Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops), è possibile configurare l'accesso personalizzato quando si invita un nuovo amministratore. È possibile modificare l'accesso di un amministratore in un secondo momento.

Per informazioni sulla visualizzazione dell'elenco degli amministratori e sulla definizione delle autorizzazioni di accesso, vedere Manage administrator access to Citrix Cloud.

Questo articolo descrive come configurare l'accesso personalizzato in Citrix DaaS.

## Amministratori, ruoli e ambiti

L'amministrazione delegata utilizza tre concetti per l'accesso personalizzato: amministratori, ruoli e ambiti.

- **Amministratori:** un amministratore rappresenta una persona identificata dall'accesso a Citrix Cloud, che in genere è un indirizzo e-mail. Ogni amministratore è associato a una o più coppie di ruoli e di ambiti.
- **Ruoli:** un ruolo rappresenta una funzione lavorativa e a esso sono associate autorizzazioni. Queste autorizzazioni consentono determinate attività esclusive di Citrix DaaS. Ad esempio, il ruolo Delivery Group Administrator (Amministratore del gruppo di consegna) dispone dell'autorizzazione per creare un gruppo di consegna e rimuovere un desktop da un gruppo di consegna, oltre ad altre autorizzazioni associate. Un amministratore può avere più ruoli. Un amministratore può essere amministratore del gruppo di consegna e amministratore del catalogo di macchine.

  Citrix DaaS offre diversi ruoli di accesso personalizzati integrati. Non è possibile modificare le autorizzazioni all'interno di questi ruoli incorporati né eliminare tali ruoli.

  È possibile creare ruoli di accesso personalizzati per soddisfare i requisiti dell'organizzazione e delegare le autorizzazioni con maggiori dettagli. Utilizzare ruoli personalizzati per allocare

le autorizzazioni in base alla granularità di un'azione o di un'attività. È possibile eliminare un ruolo personalizzato solo se non è assegnato a un amministratore.

È possibile modificare i ruoli di un amministratore.

Un ruolo è sempre associato a un ambito.

- **Ambiti:** un ambito rappresenta una raccolta di oggetti. Gli ambiti vengono utilizzati per raggruppare gli oggetti in modo rilevante per l'organizzazione. Gli oggetti possono rientrare in più di un ambito.

  C'è un ambito incorporato: Tutto, che contiene tutti gli oggetti. Gli amministratori di Citrix Cloud e dell'Help Desk sono sempre associati all'ambito All. Tale ambito non può essere modificato per tali amministratori.

  Quando si invita (aggiunge) un amministratore per questo servizio, un ruolo viene sempre associato a un ambito (per impostazione predefinita, l'ambito Tutto).

  È possibile creare ed eliminare gli ambiti nell'interfaccia **Manage > Full Configuration** (Gestisci > Configurazione completa) del servizio. Assegnare coppie ruolo/ambito nella console Citrix Cloud.

  Un ambito non viene mostrato per gli amministratori con accesso completo. Per definizione, questi amministratori possono accedere a tutti gli oggetti Citrix Cloud e ai servizi in abbonamento gestiti dal cliente.

### Ruoli e ambiti integrati

Citrix DaaS ha i seguenti ruoli integrati.

- **Amministratore cloud:** può eseguire tutte le attività che possono essere avviate da Citrix DaaS.

  Può vedere le schede **Manage** (Gestisci) e **Monitor** nella console. Questo ruolo è sempre combinato con l'ambito All. Non è possibile modificare l'ambito.

  Non lasciarsi confondere dal nome di questo ruolo. Un amministratore cloud con accesso personalizzato non può eseguire attività a livello di Citrix Cloud (le attività Citrix Cloud richiedono l'accesso completo).

- **Read Only Administrator (Amministratore di sola lettura):** può vedere tutti gli oggetti negli ambiti specificati (oltre alle informazioni globali), ma non può modificare nulla. Ad esempio, un amministratore di sola lettura con ambito Londra può vedere tutti gli oggetti globali e tutti gli oggetti che rientrano nell'ambito di Londra (ad esempio i gruppi di consegna di Londra). Tuttavia, tale amministratore non può visualizzare gli oggetti nell'ambito di New York (supponendo che gli ambiti Londra e New York non si sovrappongano).

Può vedere la scheda **Manage** (Gestisci) nella console. Non può visualizzare la scheda **Monitor**. È possibile modificare l'ambito.

- **Help Desk Administrator (Amministratore dell'Help Desk):** può visualizzare i gruppi di consegna e gestire le sessioni e i computer associati a tali gruppi. Può visualizzare il catalogo macchine e le informazioni sull'host per i gruppi di consegna che segue. Può inoltre eseguire operazioni di gestione delle sessioni e gestione dell'alimentazione della macchina per le macchine di tali gruppi di consegna.

  Può vedere la scheda **Monitor** nella console. Non può visualizzare la scheda **Manage** (Gestisci). Questo ruolo è sempre combinato con l'ambito All. Non è possibile modificare l'ambito.

- **Machine Catalog Administrator (Amministratore del catalogo macchine):** può creare e gestire cataloghi di macchine ed effettuare il provisioning delle macchine al loro interno. Può gestire immagini di base e installare software, ma non può assegnare applicazioni o desktop agli utenti.

  Può vedere la scheda **Manage** (Gestisci) nella console. Non può visualizzare la scheda **Monitor**. È possibile modificare l'ambito.

- **Delivery Group Administrator (Amministratore del gruppo di consegna):** può fornire applicazioni, desktop e macchine. Può anche gestire le sessioni associate. Può gestire le configurazioni di applicazioni e desktop, ad esempio criteri e impostazioni di risparmio energia.

  Può vedere la scheda **Manage** (Gestisci) nella console. Non può visualizzare la scheda **Monitor**. È possibile modificare l'ambito.

- **Host Administrator (Amministratore host):** può gestire le connessioni host e le impostazioni delle risorse associate. Non può distribuire macchine, applicazioni o desktop agli utenti.

  Può vedere la scheda **Manage** (Gestisci) nella console. Non può visualizzare la scheda **Monitor**. È possibile modificare l'ambito.

- **Session Administrator (Amministratore di sessione):** può visualizzare i gruppi di consegna monitorati e gestire le sessioni e i computer associati.

  Può vedere la scheda **Monitor** nella console. Non può visualizzare la scheda **Manage** (Gestisci). Non è possibile modificare l'ambito.

- **Full Administrator (Amministratore completo):** può eseguire tutte le attività e le operazioni. Un amministratore completo viene sempre combinato con l'ambito **All scope**.

  Può vedere le schede **Manage** (Gestisci) e **Monitor** nella console. Questo ruolo è sempre combinato con **All scope**. Non è possibile modificare l'ambito.

- **Full Monitor Administrator (Amministratore monitor completo):** ha pieno accesso a tutte le viste e i comandi della scheda **Monitor**.

Può vedere la scheda **Monitor** nella console. Non può visualizzare la scheda **Manage** (Gestisci). Non è possibile modificare l'ambito.

- **Probe Agent Administrator (Amministratore Probe Agent):** ha accesso alle API di Probe Agent.

  Può vedere la scheda **Monitor** nella console. Non può visualizzare la scheda **Manage** (Gestisci). Ha accesso in sola lettura alla pagina **Applications** (Applicazioni) ma non può accedere a nessun'altra visualizzazione.

Nella tabella seguente vengono riepilogate le schede della console visibili per ciascun ruolo di accesso personalizzato in Citrix DaaS e se il ruolo può essere utilizzato con ambiti personalizzati.

| Ruolo di amministratore di accesso personalizzato | Può vedere la scheda **Manage** (Gestisci) nella console? | Può vedere la scheda **Monitor** nella console? | Il ruolo può essere utilizzato con ambiti personalizzati? |
|---|---|---|---|
| Cloud Administrator (Amministratore cloud) | Sì | Sì | No |
| Read Only Administrator (Amministratore di sola lettura) | Sì | No | Sì |
| Help Desk Administrator (Amministratore dell'helpdesk) | No | Sì | No |
| Machine Catalog Administrator (Amministratore del catalogo macchine) | Sì | No | Sì |
| Delivery Group Administrator (Amministratore di gruppo di consegna) | Sì | No | Sì |
| Host Administrator (Amministratore host) | Sì | No | Sì |
| Session Administrator (Amministratore della sessione) | No | Sì | No |

| Ruolo di amministratore di accesso personalizzato | Può vedere la scheda **Manage** (Gestisci) nella console? | Può vedere la scheda **Monitor** nella console? | Il ruolo può essere utilizzato con ambiti personalizzati? |
|---|---|---|---|
| Full Administrator (Amministratore completo) | Sì | Sì | No |
| Full Monitor Administrator (Amministratore di Monitor completo) | No | Sì | No |
| Probe Agent Administrator (Amministratore di Probe Agent) | No | Sì | No |

> **Nota:**
>
> I ruoli di amministratore degli accessi personalizzati (a eccezione di Cloud Administrator e Help Desk Administrator) non sono disponibili per Citrix Virtual Apps and Desktops Standard for Azure, Virtual Apps Essentials e Virtual Desktops Essentials.

Per visualizzare le autorizzazioni associate a un ruolo:

1. Accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Da **Manage > Full Configuration**, selezionare **Administrators** nel riquadro a sinistra.
3. Seleziona la scheda **Roles**.
4. Selezionare un ruolo nel riquadro centrale in alto. La scheda **Role definition** (Definizione ruolo) nel riquadro inferiore elenca le categorie e le autorizzazioni. Selezionare una categoria per vedere le autorizzazioni specifiche. La scheda **Administrators** (Amministratori) elenca gli amministratori a cui è stato assegnato il ruolo selezionato.

   Problema noto: una voce Full Administrator (Amministratore completo) non visualizza il set corretto di autorizzazioni per un amministratore di Citrix DaaS ad accesso completo.

### Quanti amministratori occorrono

Il numero di amministratori e la granularità delle autorizzazioni in genere dipendono dalle dimensioni e dalla complessità della distribuzione.

- Nelle distribuzioni di piccole dimensioni o quelle prova di concetto, uno o pochi amministratori fanno tutto. Non esistono deleghe di accesso personalizzate. In questo caso, ogni amministratore ha accesso completo, che ha sempre l'ambito All.
- Nelle distribuzioni più grandi con più macchine, applicazioni e desktop, è necessario delegare di più. Diversi amministratori potrebbero avere responsabilità funzionali (ruoli) più specifiche. Ad esempio, due hanno accesso completo e altri sono amministratori dell'helpdesk. Inoltre, un amministratore può gestire solo determinati gruppi di oggetti (ambiti), ad esempio i cataloghi di macchine di un particolare reparto. In questo caso, creare nuovi ambiti, oltre agli amministratori con il ruolo e gli ambiti di accesso personalizzati appropriati.

### Riepilogo della gestione degli amministratori

La configurazione degli amministratori per Citrix DaaS segue questa sequenza:

1. Se l'amministratore deve avere un ruolo diverso da quello di amministratore completo (che copre tutti i servizi in abbonamento di Citrix Cloud) o un ruolo integrato, creare un ruolo personalizzato.
2. Se l'amministratore dovrà avere un ambito diverso da All (e un ambito diverso è consentito per il ruolo previsto e non è già stato creato), creare degli ambiti.
3. Da Citrix Cloud, invitare un amministratore. Se si desidera che il nuovo amministratore abbia qualcosa di diverso dall'accesso completo predefinito, specificare una coppia di ruolo di accesso e ambito personalizzata.

In seguito, se si desidera modificare l'accesso di un amministratore (ruoli e ambito), vedere Configurare l'accesso personalizzato.

### Aggiungere un amministratore

Per aggiungere (invitare) amministratori, seguire le indicazioni fornite in Add administrators to a Citrix Cloud account. Un sottoinsieme di tali informazioni viene ripetuto qui.

> **Importante:**
>
> Non confondere il modo in cui vengono utilizzati i termini "custom"(personalizzato) e "custom access"(accesso personalizzato).
>
> - Quando si creano amministratori e si assegnano ruoli per Citrix DaaS nella console Citrix Cloud, il termine "custom access"(accesso personalizzato) include sia i ruoli incorporati che eventuali ruoli personalizzati aggiuntivi creati nell'interfaccia **Manage > Full Configuration** del servizio.
> - Nell'interfaccia **Manage > Full Configuration** del servizio, "custom"differenzia semplice-

> mente quel ruolo da un ruolo incorporato.

Il flusso di lavoro generale per l'aggiunta di amministratori è il seguente:

1. Accedere a Citrix Cloud e selezionare **Identity and Access Management** nel menu in alto a sinistra.
2. Nella pagina **Identity and Access Management**, selezionare **Administrators**. La scheda **Administrators** elenca tutti gli attuali amministratori dell'account.
3. Nella scheda **Administrators**, selezionare il tipo di identità, inserire l'indirizzo email dell'amministratore, quindi fare clic su **Invite**.

- Selezionare **Full access** se si desidera che l'amministratore abbia l'accesso completo. In questo modo, l'amministratore può accedere a tutte le funzioni di amministratore del cliente in Citrix Cloud e in tutti i servizi in abbonamento.
- Selezionare **Custom access** se si desidera che l'amministratore abbia accesso limitato. È quindi possibile selezionare una coppia di ruolo di accesso e ambito personalizzata. In questo modo, l'amministratore dispone delle autorizzazioni previste per l'accesso a Citrix Cloud.

1. Fare clic su **Send Invite**. Citrix Cloud invia un invito all'indirizzo e-mail e aggiunge l'amministratore all'elenco dopo che l'amministratore ha completato l'onboarding.

Quando riceve l'e-mail, l'amministratore fa clic sul collegamento **Sign In** per accettare l'invito.

Per ulteriori informazioni sull'aggiunta di amministratori, vedere Manage Citrix Cloud administrators.

In alternativa, passare a **Manage > Full Configuration > Administrators > Administrators** e fare clic su **Add Administrator**. Si passerà direttamente a **Identity and Access Management > Administrators**, che si apre in una nuova scheda del browser. Dopo aver completato l'aggiunta di amministratori, chiudere la scheda e tornare alla console per procedere alle altre attività di configurazione.

### Creare e gestire ruoli

Quando gli amministratori creano o modificano un ruolo, possono abilitare solo le autorizzazioni di cui dispongono essi stessi. Questo controllo impedisce agli amministratori di creare un ruolo con più autorizzazioni di quelle di cui dispongono attualmente e di assegnarlo a se stessi (o modificare un ruolo già assegnato).

I nomi di ruolo personalizzati possono contenere fino a 64 caratteri Unicode. I nomi non possono contenere: barra rovesciata, barra, punto e virgola, due punti, cancelletto, virgola, asterisco, punto interrogativo, segno di uguale, freccia sinistra o destra, barra verticale, parentesi quadra aperta o chiusa, parentesi tonda aperta o chiusa, virgolette e apostrofo.

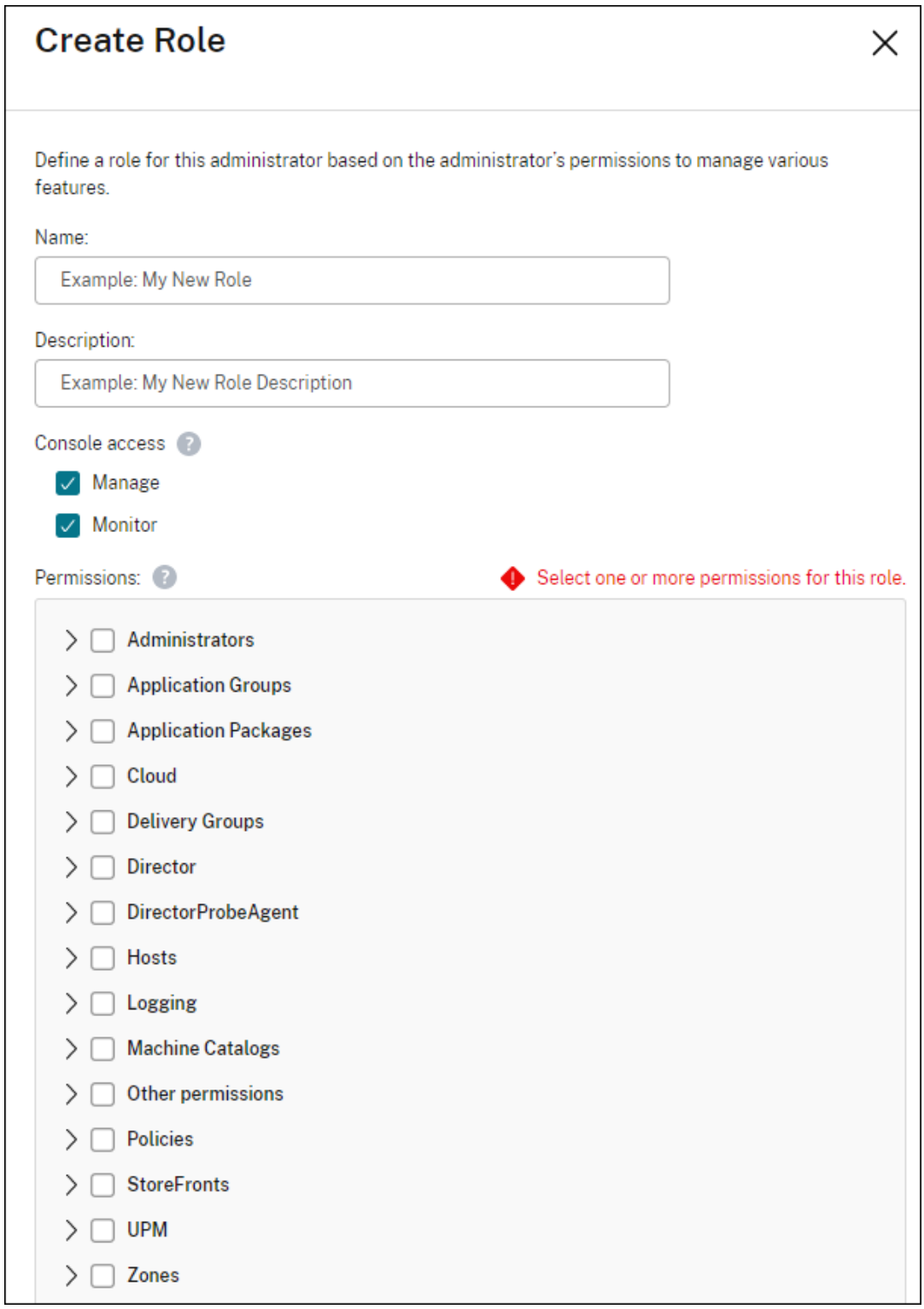
Le descrizioni dei ruoli possono contenere fino a 256 caratteri Unicode.

1. Se non lo si è già fatto, accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Da **Manage > Full Configuration**, selezionare **Administrators** nel riquadro a sinistra.
3. Seleziona la scheda **Roles**.
4. Seguire le istruzioni per l'attività da completare:

    - **Visualizzare i dettagli del ruolo:** selezionare il ruolo nel riquadro centrale. Nella parte inferiore del riquadro centrale sono elencati i tipi di oggetto e le autorizzazioni associate al ruolo. Selezionare la scheda **Administrators** nel riquadro inferiore per visualizzare un elenco degli amministratori che attualmente dispongono di questo ruolo.
    - **Creare un ruolo personalizzato:** selezionare **Create role** nella barra delle azioni. Configurare le impostazioni come segue:
        - Immettere un nome e una descrizione.
        - Configurare l'accesso alla console. Determinare quali console sono visibili agli amministratori. È possibile procedere senza selezionare alcuna console. In tal caso, gli amministratori con quel ruolo non possono accedere a **Manage** e **Monitor** ma possono accedere, visualizzare o gestire gli oggetti tramite SDK e API.
        - Selezionare i tipi di oggetto e le autorizzazioni. Per concedere l'autorizzazione di accesso completo a un tipo di oggetto, selezionare la relativa casella di controllo. Per concedere l'autorizzazione a livello granulare, espandere il tipo di oggetto e quindi selezionare **Read Only** o singoli oggetti in **Manage** all'interno del tipo.




- **Copiare un ruolo:** selezionare il ruolo nel riquadro centrale, quindi selezionare **Copy Role** nella barra delle azioni. Modificare il nome, la descrizione, i tipi di oggetto e le autorizzazioni in base alle esigenze. Al termine, selezionare **Save** (Salva).

- **Modificare un ruolo personalizzato:** selezionare il ruolo nel riquadro centrale e quindi selezionare **Edit Role** nella barra delle azioni. Modificare il nome, la descrizione, i tipi di oggetto e le autorizzazioni in base alle esigenze. Non è possibile modificare un ruolo incorporato. Al termine, selezionare **Save** (Salva).
- **Eliminare un ruolo personalizzato:** selezionare il ruolo nel riquadro centrale e quindi selezionare **Delete Role** nella barra delle azioni. Quando richiesto, confermare l'eliminazione. Non è possibile eliminare un ruolo predefinito. Non è possibile eliminare un ruolo personalizzato se è assegnato a un amministratore.

### Creare e gestire ambiti

Per impostazione predefinita, tutti i ruoli hanno l'ambito All per gli oggetti rilevanti. Ad esempio, un Delivery Group Administrator (Amministratore di gruppo di consegna) può gestire tutti i Delivery Groups (Gruppi di consegna). Per alcuni ruoli di amministratore, è possibile creare un ambito che consenta a tale ruolo di amministratore di accedere a un sottoinsieme degli oggetti pertinenti. Ad esempio, si potrebbe voler dare a un Machine Catalog Administrator (Amministratore di catalogo macchine) l'accesso ai soli cataloghi che contengono un certo tipo di macchine, piuttosto che a tutti i cataloghi.

- I Full Access Administrators (Amministratori con accesso completo) o i Cloud Administrators con accesso personalizzato possono creare ambiti per i ruoli Read Only Administrator (Amministratore di sola lettura), Machine Catalog Administrator (Amministratore catalogo macchine), Delivery Group Administrator (Amministratore di gruppo di consegna) e Host Administrator (Amministratore host).
- Non possono essere creati ambiti né per i Full access administrators, né per i Cloud Administrator né gli Help Desk Administrators. Questi amministratori hanno sempre l'ambito All.

Regole per la creazione e la gestione degli ambiti:

- I nomi di ambito possono contenere fino a 64 caratteri Unicode. I nomi non possono contenere: barra rovesciata, barra, punto e virgola, due punti, cancelletto, virgola, asterisco, punto interrogativo, segno di uguale, freccia sinistra o destra, barra verticale, parentesi quadra aperta o chiusa, parentesi tonda aperta o chiusa, virgolette e apostrofo.
- Le descrizioni degli ambiti possono contenere fino a 256 caratteri Unicode.
- Quando si copia o si modifica un ambito, tenere presente che la rimozione di oggetti dall'ambito può rendere tali oggetti inaccessibili a un amministratore. Se l'ambito modificato è associato a uno o più ruoli, assicurarsi che i propri aggiornamenti dell'ambito non rendano inutilizzabile alcuna coppia ruolo/ambito.

Per creare e gestire ambiti:

1. Accedere a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS).
2. Da **Manage > Full Configuration**, selezionare **Administrators** nel riquadro a sinistra.
3. Selezionare la scheda **Scopes**.
4. Seguire le istruzioni per l'attività da completare:

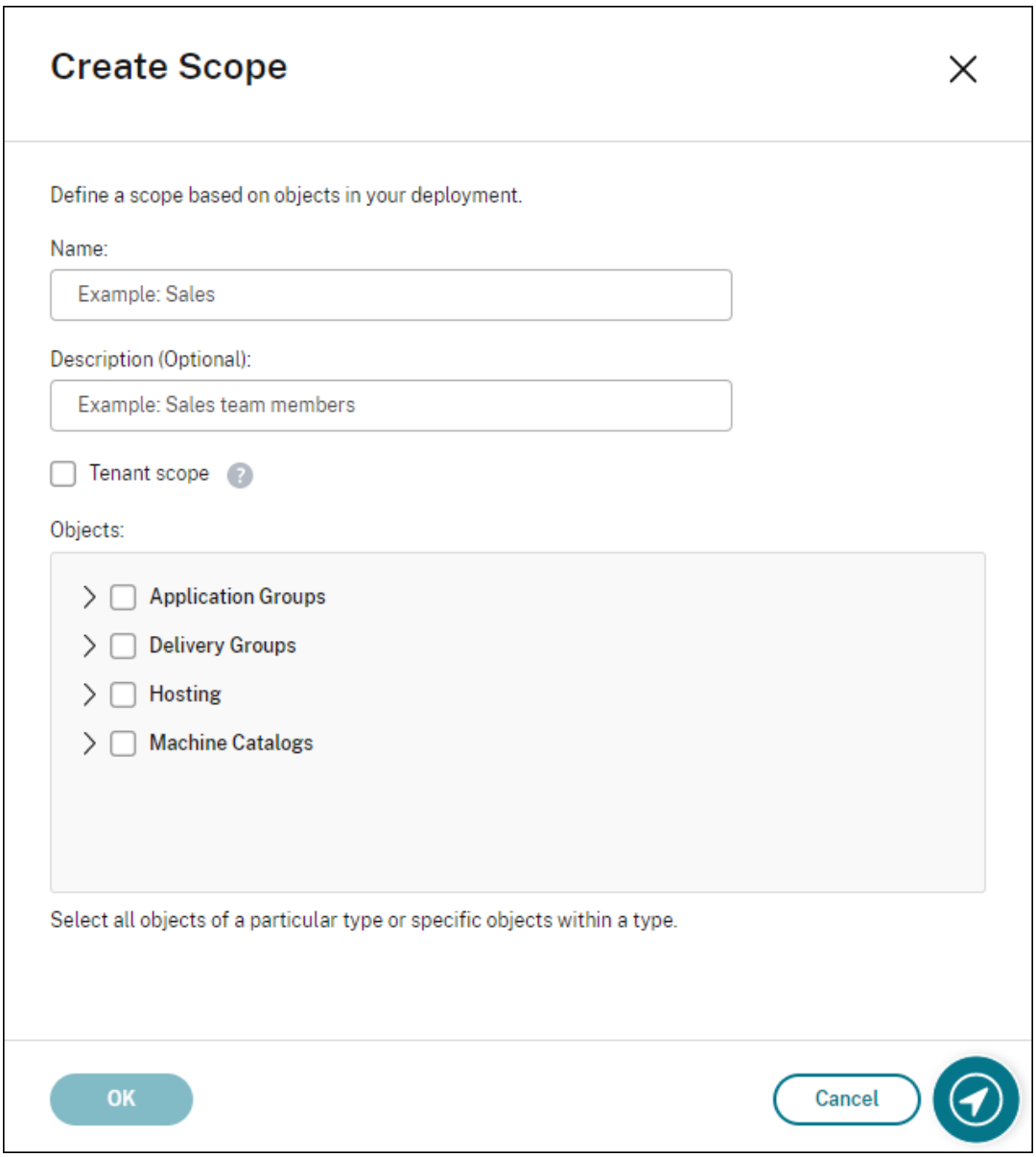
   - **Visualizzare dettagli dell'ambito:** selezionare l'ambito. Nella parte inferiore del riquadro sono elencati gli oggetti e gli amministratori che hanno tale ambito.
   - **Creare un ambito:** selezionare **Create scope** nella barra delle azioni. Immettere un nome e una descrizione. Gli oggetti sono elencati per tipo, ad esempio gruppo di consegna e catalogo macchine.
     - Per includere tutti gli oggetti di un tipo particolare (ad esempio tutti i gruppi di consegna), selezionare la casella di controllo del tipo di oggetto.
     - Per includere singoli oggetti all'interno di un tipo, espandere il tipo e selezionare le caselle di controllo degli oggetti (ad esempio gruppi di consegna specifici).

       > **Nota:**
       >
       > I gruppi di applicazioni, i gruppi di consegna o i cataloghi di macchine vengono visualizzati in strutture di cartelle allineate alla loro gestione in DaaS. È possibile selezionare una cartella per selezionare tutti i relativi oggetti o espandere una cartella per selezionare oggetti specifici.

     - Per creare un cliente tenant, selezionare la casella di controllo **Tenant scope** (Ambito tenant). Se viene selezionata, il nome immesso per l'ambito è il nome del tenant. Per ulteriori informazioni sull'ambito del tenant, vedere Gestione dei tenant.

   Al termine, selezionare **OK**.




- **Copiare un ambito:** selezionare l'ambito nel riquadro centrale e quindi selezionare **Copy Scope** nella barra delle azioni. Cambiare il nome e/o la descrizione. Modificare i tipi di oggetto e gli oggetti in base alle esigenze. Al termine, selezionare **Save** (Salva).
- **Modificare un ambito:** selezionare l'ambito nel riquadro centrale e quindi selezionare **Edit Scope** nella barra delle azioni. Modificare il nome, la descrizione, i tipi di oggetto e gli oggetti in base alle esigenze. Al termine, selezionare **Save** (Salva).
- **Eliminare un ambito:** selezionare l'ambito nel riquadro centrale e quindi selezionare **Delete Scope** nella barra delle azioni. Quando richiesto, confermare l'eliminazione.

  Non è possibile eliminare un ambito se è assegnato a un ruolo. Se si tenta di farlo, un messaggio di errore indica che non si dispone dell'autorizzazione. In effetti, l'errore si verifica

perché la coppia ruolo/ambito che utilizza questo ambito è assegnata a un amministratore. Innanzitutto, rimuovere l'assegnazione della coppia ruolo/ambito da tutti gli amministratori che la utilizzano. Quindi eliminare l'ambito nella console **Manage**.

Dopo aver creato un ambito, questo viene visualizzato nell'elenco di **Custom access** (Accesso personalizzato) nella console Citrix Cloud. È quindi possibile selezionarlo quando si assegna un ruolo a un amministratore.

Ad esempio, supponiamo di creare un ambito denominato CAD e di selezionare i cataloghi che contengono macchine adatte alle applicazioni CAD. Quando si torna alla console Citrix Cloud e si seleziona **Edit scopes** (Modifica ambiti) per un ruolo, l'elenco degli ambiti disponibili contiene l'ambito CAD creato in precedenza.

Il Cloud Administrator e l'Help Desk Administrator hanno sempre l'ambito All, quindi l'ambito CAD non si applica a loro.

#### Gestione dei tenant

Utilizzando l'interfaccia di gestione Full Management (Configurazione completa), è possibile creare tenant che si escludono a vicenda in un singolo Citrix DaaS. È possibile ottenere questo risultato creando ambiti tenant in **Administrators > Scopes** (Amministratori > Ambiti) e associando gli oggetti di configurazione correlati, ad esempio cataloghi macchine e gruppi di consegna, a tali tenant. Di conseguenza, gli amministratori con accesso a un tenant possono gestire solo gli oggetti associati al tenant.

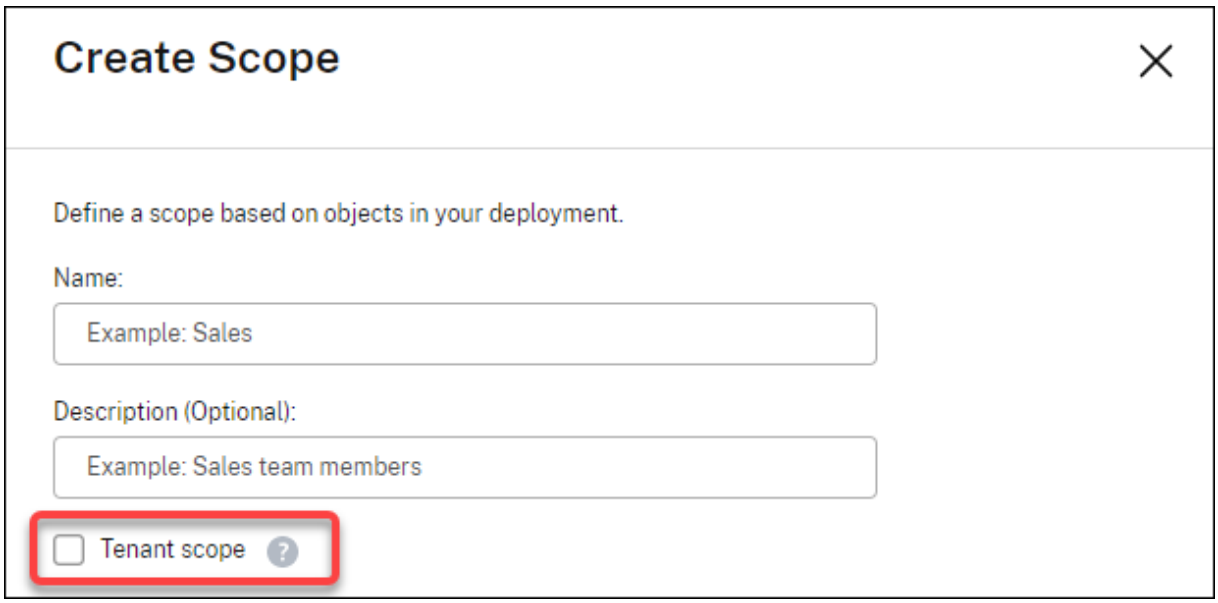
Questa funzione è utile, ad esempio, se la propria organizzazione:

- Dispone di silos aziendali diversi (divisioni indipendenti o team di gestione IT separati) o
- Dispone di più siti locali e desidera mantenere la stessa configurazione in una singola istanza di Citrix DaaS.

L'interfaccia consente di filtrare i clienti tenant in base al nome. Per impostazione predefinita, l'interfaccia visualizza informazioni su tutti i clienti tenant. Per visualizzare le informazioni su un tenant specifico, selezionarlo dall'elenco nell'angolo in alto a destra.

**Creare un cliente tenant** Per creare un cliente tenant, selezionare **Tenant scope** (Ambito tenant) durante la creazione di un ambito. Selezionando l'opzione, si crea un tipo di ambito univoco che si applica agli oggetti negli scenari in cui si condivide un'istanza Citrix DaaS tra diverse unità organizzative, ognuna delle quali è indipendente dalle altre. Dopo aver creato un ambito tenant, non è possibile modificare il tipo di ambito.




La scheda **Scopes** (Ambiti) visualizza tutti gli elementi dell'ambito. L'unica differenza tra ambiti regolari e ambiti tenant è nella colonna **Type** (Tipo). Un campo colonna vuoto indica un ambito regolare. È possibile fare clic sulla colonna **Type** (Tipo) per ordinare gli elementi dell'ambito, se necessario.

Per visualizzare le risorse (oggetti) associate a un ambito, selezionare **Administrators** (Amministratori) nel riquadro di sinistra. Nella scheda **Scopes** (Ambiti), selezionare l'ambito, quindi selezionare **Edit Scope** (Modifica ambito) nella barra delle azioni.

> **Suggerimento:**
>
> La proprietà tenant viene assegnata a livello di ambito. I cataloghi di macchine, i gruppi di consegna, le applicazioni e le connessioni ereditano la proprietà del tenant dall'ambito applicabile.

Quando si utilizza un ambito tenant, tenere presente le seguenti considerazioni:

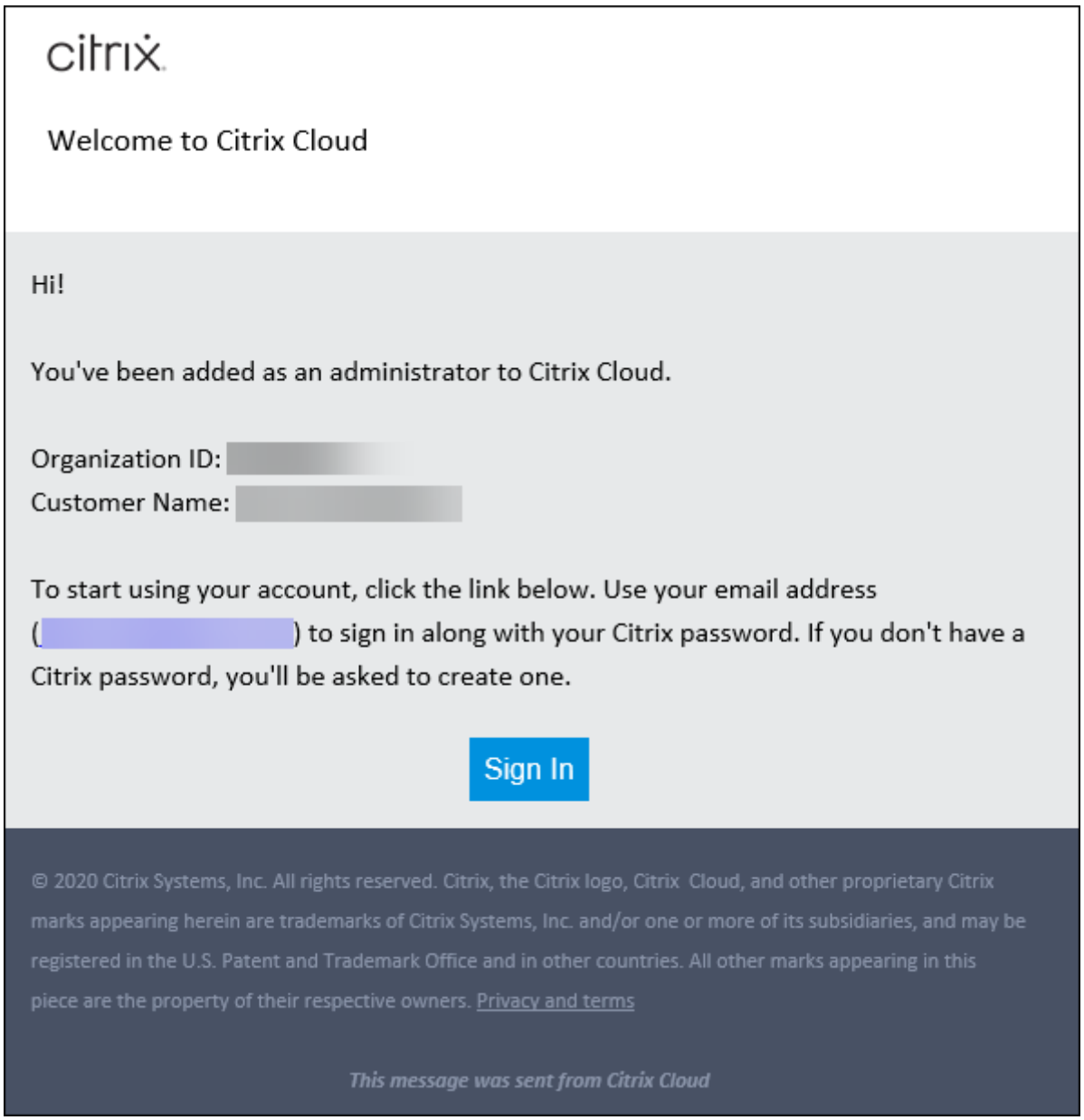
- La proprietà del tenant viene assegnata nel seguente ordine: **Hosting > Machine Catalogs > Delivery Groups > Applications** (Hosting > Cataloghi di macchine > Gruppi di consegna > Applicazioni). Gli oggetti di livello inferiore si basano sugli oggetti di livello superiore da cui ereditare la proprietà tenant. Ad esempio, quando si seleziona un gruppo di consegna, è necessario selezionare l'hosting e il catalogo delle macchine associati. In caso contrario, il gruppo di consegna non può ereditare la proprietà tenant.
- Dopo aver creato un ambito tenant, è possibile modificare le assegnazioni dei tenant modificando gli oggetti. Quando l'assegnazione di un tenant viene modificata, è ancora soggetta al vincolo in base al quale deve essere assegnata agli stessi tenant o a un sottoinsieme di tali tenant. Tuttavia, gli oggetti di livello inferiore non vengono rivalutati quando cambiano le assegnazioni dei tenant. Assicurarsi che gli oggetti siano limitati correttamente quando si modificano le assegnazioni dei tenant. Ad esempio, se un catalogo delle macchine è disponibile per `TenantA` e `TenantB`, è possibile creare un gruppo di consegna per `TenantA` e uno per

`TenantB` (`TenantA` e `TenantB` sono entrambi associati a quel catalogo delle macchine). È quindi possibile modificare il catalogo delle macchine in modo che sia associato solo a `TenantA`. Di conseguenza, il gruppo di consegna associato a `TenantB` non è più valido.

**Configurare l'accesso personalizzato per gli amministratori** Dopo aver creato gli ambiti tenant, configurare l'accesso personalizzato per i rispettivi amministratori. Per ulteriori informazioni, consultare Configurare l'accesso personalizzato per un amministratore. Citrix Cloud invia un invito agli amministratori dei clienti specificati e li aggiunge all'elenco. Quando ricevono l'e-mail, fanno clic su **Sign In** (Accedi) per accettare l'invito. Quando accedono all'interfaccia di gestione **Full Configuration** (Configurazione completa), vedono le risorse contenute nelle coppie di ruolo e ambito assegnate.




Gli amministratori con accesso a un tenant possono gestire solo gli oggetti (ad esempio catalogo delle macchine, gruppo di consegna) associati al tenant.

### Configurare l'accesso personalizzato per un amministratore

Questa funzione consente di definire le autorizzazioni di accesso degli amministratori esistenti o degli amministratori che si invitano in modo appropriato al loro ruolo nell'organizzazione.

Le modifiche apportate alle autorizzazioni di accesso richiedono 5 minuti per avere effetto. Scollegandosi dall'interfaccia di gestione Full Configuration e accedendo di nuovo, le modifiche abbiano effetto immediato. Negli scenari in cui gli amministratori utilizzano ancora l'interfaccia di gestione dopo che

le modifiche sono diventate effettive senza riconnettersi a essa, viene visualizzato un avviso quando essi tentano di accedere agli elementi per i quali non dispongono più delle autorizzazioni.

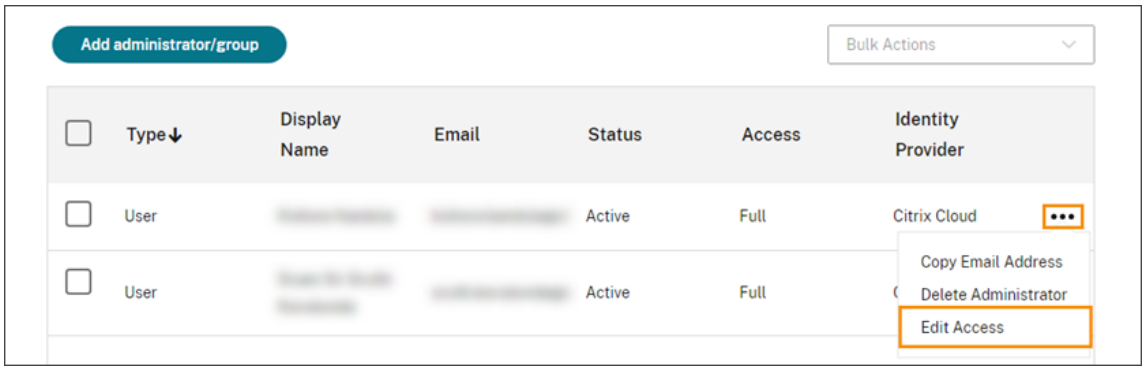
Per impostazione predefinita, quando si invitano amministratori, questi hanno accesso completo. L'accesso completo consente all'amministratore di gestire tutti i servizi in abbonamento e tutte le operazioni Citrix Cloud (quale invitare più amministratori). Una distribuzione Citrix Cloud richiede almeno un amministratore con accesso completo.

È anche possibile concedere un accesso personalizzato quando si invita un amministratore. L'accesso personalizzato consente all'amministratore di gestire solo i servizi e le operazioni specificati.

Quando si crea un ruolo o un ambito in Citrix DaaS, questo viene visualizzato nell'elenco di accesso personalizzato e può essere selezionato. Quando si seleziona un ruolo per un amministratore, è possibile modificare gli ambiti in base come necessario in base al ruolo dell'amministratore nell'organizzazione.

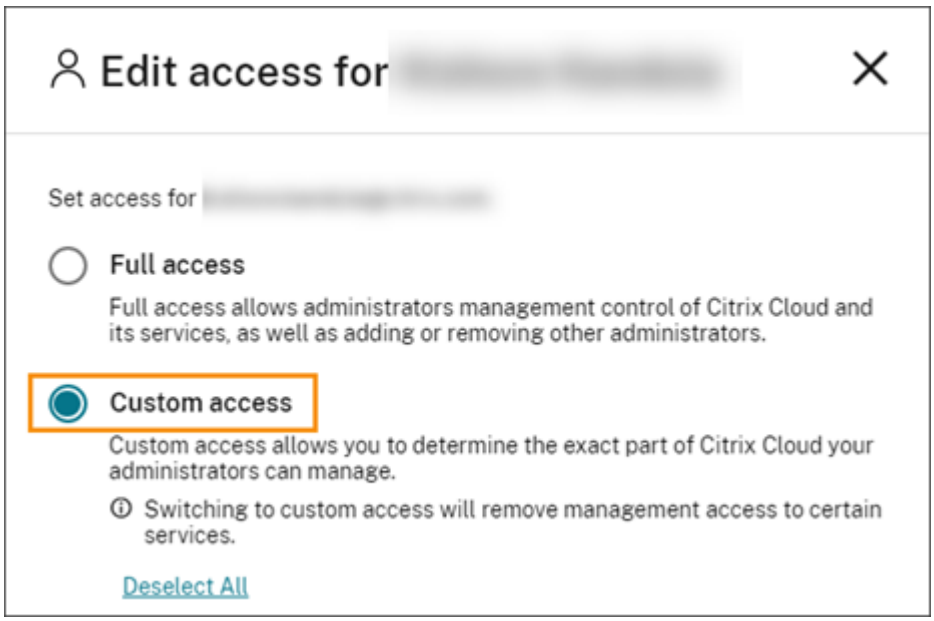
Per configurare l'accesso personalizzato per un amministratore:

1. Accedere a Citrix Cloud. Selezionare **Identity and Access Management** > **Administrators** nel menu in alto a sinistra.
2. Individuare l'amministratore che si desidera gestire, selezionare il menu con i puntini di sospensione e selezionare **Edit access**.



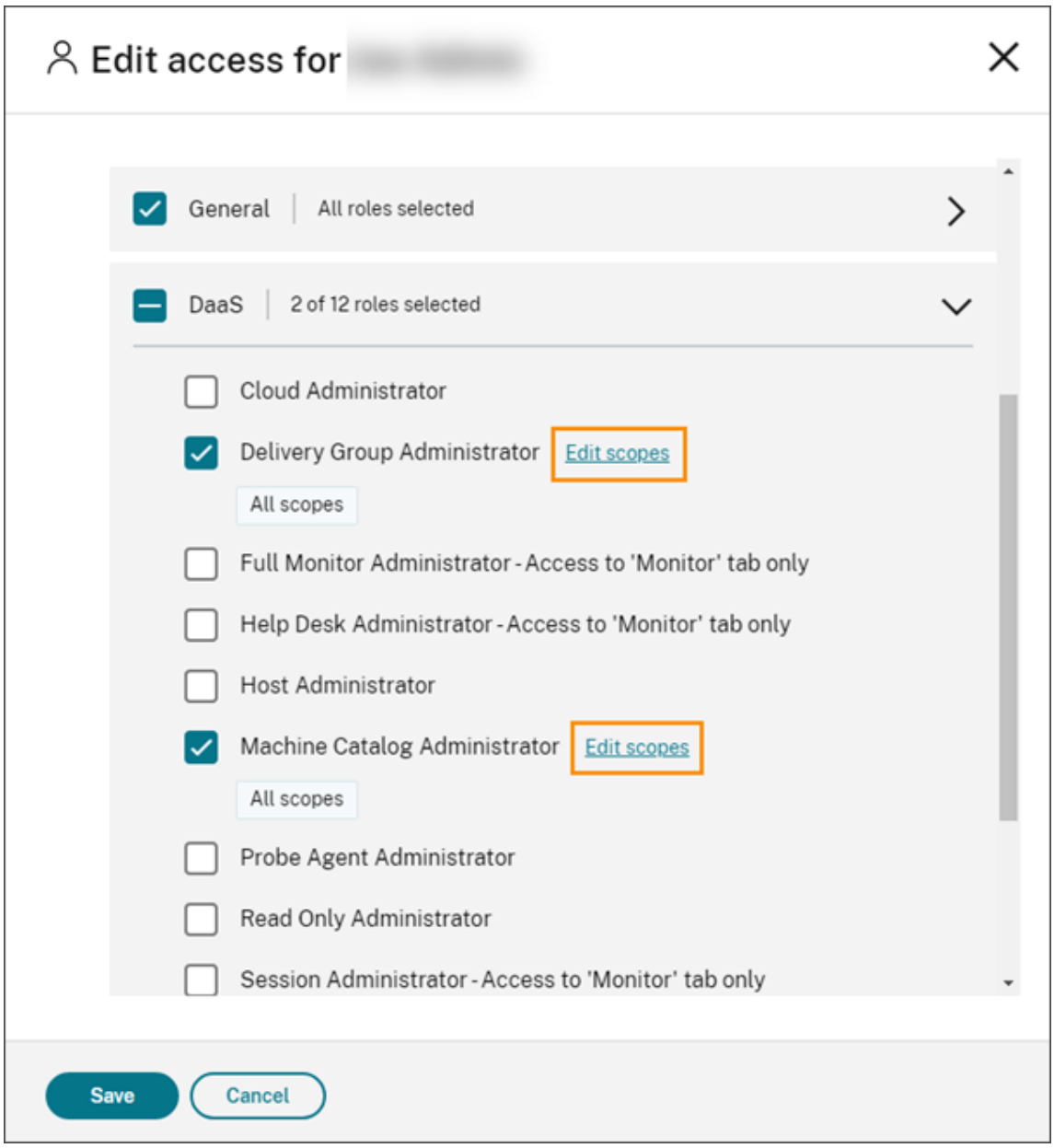

3. Selezionare **Custom access**.




4. In **DaaS**, selezionare o deselezionare i segni di spunta accanto a uno o più ruoli. Per modificare gli ambiti associati a un ruolo assegnato, selezionare **Edit scopes** (Modifica ambiti).

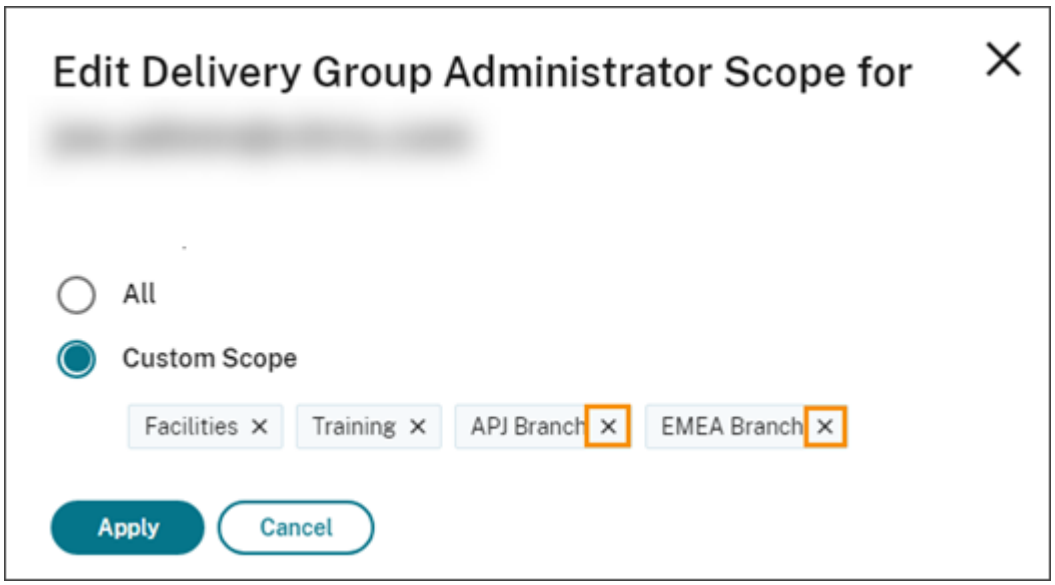
 



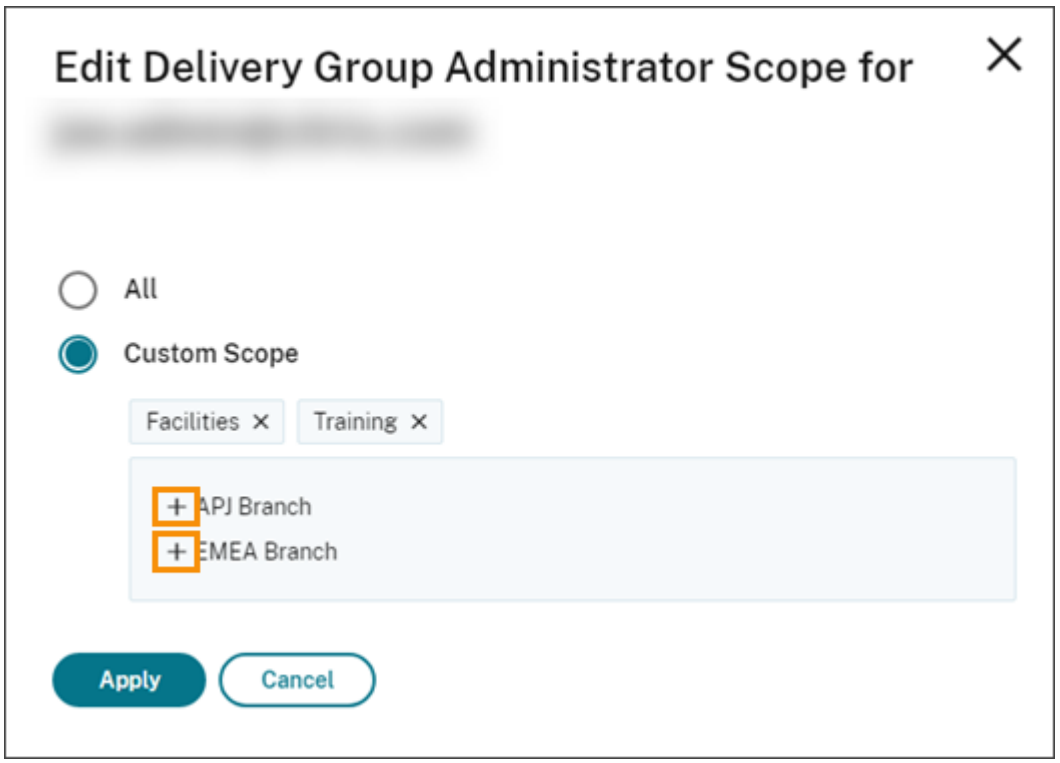

Per impostazione predefinita, ogni ruolo selezionato ha tutti gli ambiti selezionati, come indicato dall'etichetta **All scopes** (Tutti gli ambiti).

5. Per specificare gli ambiti di un ruolo selezionato, selezionare **Custom Scope** (IAmbito personalizzato) e quindi aggiungere o rimuovere gli ambiti appropriati. Per impostazione predefinita, tutti gli ambiti personalizzati vengono aggiunti a un ruolo. Per rimuovere un ambito, fare clic sull'icona X sull'ambito.




Gli ambiti che sono stati rimossi e sono disponibili per essere aggiunti a un ruolo vengono visualizzati in un elenco sotto gli ambiti già aggiunti. Per aggiungere un ambito al ruolo, selezionare l'icona con il segno più dell'ambito.




6. Quando si è finito di selezionare gli ambiti, selezionare **Apply**.
7. Selezionare **Save** per salvare i ruoli selezionati per l'amministratore.

### Differenze rispetto a Citrix Virtual Apps and Desktops locale

Se si ha familiarità con l'amministrazione delegata nel prodotto Citrix Virtual Apps and Desktops on-premise, la versione di Citrix DaaS presenta diverse differenze.

In Citrix Cloud:

- Gli amministratori sono identificati dal loro accesso Citrix Cloud, piuttosto che dal loro account Active Directory. È possibile creare coppie di ruolo/ambito per singoli utenti di Active Directory, ma non per gruppi.
- Gli amministratori vengono creati, configurati ed eliminati nella console Citrix Cloud, anziché in Citrix DaaS.
- Le coppie ruolo/ambito vengono assegnate agli amministratori nella console Citrix Cloud anziché in Citrix DaaS.
- I report non sono disponibili. È possibile visualizzare le informazioni relative all'amministratore, al ruolo e all'ambito nell'interfaccia **Manage > Full Configuration** del servizio.
- Il Cloud Administrator con accesso personalizzato è simile a un amministratore completo della versione locale. Entrambi dispongono di autorizzazioni complete di gestione e monitoraggio per la versione Citrix Virtual Apps and Desktops utilizzata.

  Tuttavia, in Citrix DaaS non esiste un ruolo Full Administrator (Amministratore completo) specifico. Non equiparare "Full access"di Citrix Cloud con "Full administrator"in Citrix Virtual Apps and Desktops locale. Full access in Citrix Cloud comprende i domini a livello di piattaforma, la libreria, le notifiche e le posizioni delle risorse, oltre a tutti i servizi in abbonamento.

### Differenze rispetto alle versioni precedenti di Citrix DaaS

Prima del rilascio della funzionalità di accesso personalizzato estesa (settembre 2018), esistevano due ruoli di amministratore con accesso personalizzato: Full Administrator e Help Desk Administrator. Quando la distribuzione ha l'amministrazione delegata abilitata (che è un'impostazione della piattaforma), tali ruoli vengono mappati automaticamente.

- Un amministratore precedentemente configurato come **Virtual Apps and Desktops (o XenApp e XenDesktop) Service: Full Administrator** con accesso personalizzato è ora un **Cloud Administrator** con accesso personalizzato.
- Un amministratore precedentemente configurato come **Virtual Apps and Desktops (o XenApp e XenDesktop) Service: Help Desk Administrator** con accesso personalizzato è ora un **Help Desk Administrator** con accesso personalizzato.

### Ulteriori informazioni

Vedere Amministrazione e monitoraggio delegati per informazioni su amministratori, ruoli e ambiti utilizzati nella console **Monitor** del servizio.

## Home page per l'interfaccia Full Configuration (Configurazione completa)

October 30, 2023

Fornisce una panoramica della distribuzione e dei carichi di lavoro di Citrix DaaS insieme a informazioni che consentono di ottenere il massimo dalla propria sottoscrizione. La pagina comprende le seguenti parti:

- Panoramica del servizio
- Avvisi sullo stato del servizio
- Consigli
- Novità
- Funzionalità di anteprima
- Per iniziare

Per accedere alla Home page, attenersi alla seguente procedura:

1. Accedere a Citrix Cloud.
2. Nel riquadro **DaaS**, fare clic su **Manage** (Gestisci).
3. Selezionare **Manage > Full Configuration** (Gestisci > Configurazione completa). Viene visualizzata la Home page.

### Panoramica del servizio

Fornisce una panoramica della distribuzione e dei carichi di lavoro di Citrix DaaS:

- **Risorse**. Mostra il numero di risorse distribuite e i relativi conteggi per categoria.

| Risorsa | Per visualizzare i conteggi per categoria |
| --- | --- |
| Macchine | Fare clic su **Machines** (Macchine), selezionare uno stato, quindi passare il mouse sul grafico ad anello per i dettagli. Opzioni disponibili: **Availability state** (Stato di disponibilità) (Available, In use, Off, and Unavailable [Disponibile, In uso, Disattivato e Non disponibile]), **Registration state** (Stato di registrazione) (Registered and Unregistered [Registrato e Non registrato]) e **Maintenance state** (Stato di manutenzione) (In maintenance or Not in maintenance [In manutenzione o Non in manutenzione]). Quando si visualizzano i conteggi delle macchine per stato di disponibilità, è possibile fare clic su uno stato per visualizzare i dettagli della macchina corrispondente. |
| Applicazioni | Fare clic su **Applications** (Applicazioni) e passare il mouse sul grafico ad anello per i dettagli. |
| Gruppi di consegna | Fare clic su **Delivery Groups** (Gruppi di consegna) e passare il mouse sul grafico ad anello per i dettagli. |
| Cataloghi di macchine | Fare clic su **Machine Catalogs** (Cataloghi delle macchine) e passare il mouse sopra il grafico ad anello per i dettagli. |

- **Sessioni avviate negli ultimi 7 giorni**. Mostra il numero di sessioni desktop e app avviate ogni giorno negli ultimi sette giorni. Per visualizzare ulteriori dettagli, fare clic su **Go to Monitor** (Vai al monitoraggio).

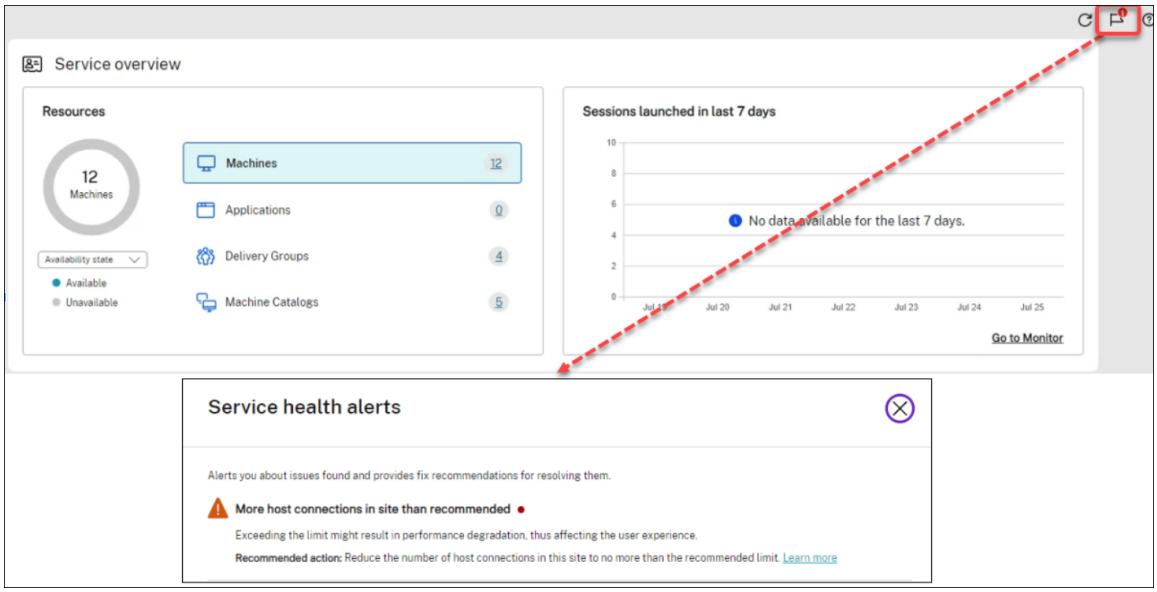
### Avvisi sullo stato del servizio

Avvisa dei problemi rilevati e fornisce consigli per risolverli. Gli avvisi vengono visualizzati con simboli di avviso e di errore.

> **Nota:**
>
> La diagnostica viene aggiornata ogni ora.

Esempio di avviso:




## Consigli

Consiglia le funzionalità disponibili con la propria sottoscrizione, ad esempio Workspace Environment Management e Autoscale. Per interagire con noi, è possibile aggiungere "mi piace"o "non mi piace"a un consiglio e lasciare feedback.

> **Nota:**
>
> Se una raccomandazione non ti piace, la raccomandazione scompare. Se si contrassegnano con "non mi piace"tutti i consigli o il widget dei consigli, il widget dei consigli scompare.

## Novità

Mostra un elenco selezionato delle più recenti funzionalità di Citrix DaaS più importanti per la propria azienda. L'utilizzo di queste funzionalità aiuta a ottenere il massimo dalla propria sottoscrizione. Per un elenco completo delle nuove funzionalità, vedere Novità.

## Funzionalità di anteprima

Mostra le funzionalità attualmente in anteprima. In qualità di amministratore di Citrix Cloud con accesso completo, si possono attivare o disattivare le funzionalità di anteprima senza contattare Citrix. Sono necessari fino a 15 minuti affinché le modifiche abbiano effetto.

Le funzionalità di anteprima sono consigliate per l'uso in ambienti non di produzione. I problemi riscontrati nelle funzionalità di anteprima non sono supportati dal supporto tecnico Citrix.

### Per iniziare

Mostra i passaggi che guidano l'utente nella configurazione iniziale di app e desktop.

Le fasi di configurazione sono le seguenti:

1. Creare posizioni delle risorse

   Per "posizioni delle risorse" si intendono posizioni che contengono applicazioni e desktop che si desidera fornire agli utenti. Questo passaggio consente di aggiungere le posizioni delle risorse a DaaS e di installare Cloud Connector al loro interno. I Cloud Connector fungono da canali che autenticano e crittografano tutte le comunicazioni tra Citrix Cloud e le proprie risorse.

2. Creare una connessione host

   Gli host sono hypervisor o servizi cloud utilizzati nelle posizioni delle risorse. Questo passaggio consente di specificare le informazioni che DaaS utilizza per comunicare con le VM su un host. Le informazioni dettagliate includono la posizione delle risorse, il tipo di host, le credenziali di accesso, il metodo di archiviazione da utilizzare e le reti che possono essere utilizzate dalle VM sull'host.

3. Preparare un'immagine master

   Un'immagine master include il sistema operativo, tutte le applicazioni richieste e il Virtual Delivery Agent (VDA). I VDA stabiliscono e gestiscono le connessioni tra le VM e i dispositivi degli utenti.

4. Creare un catalogo di macchine

   Un catalogo di macchine è una raccolta di macchine virtuali identiche a sessione singola o multisessione assegnate agli utenti. Questo passaggio consente di creare un catalogo di macchine specificando la tecnologia di provisioning, l'immagine master e la dimensione della VM.

5. Assegnare utenti

   Un gruppo di consegna è una raccolta di macchine selezionate da uno o più cataloghi di macchine. Questo passaggio consente di creare gruppi di consegna per specificare quali macchine possono essere utilizzate dai diversi team, reparti o tipi di utenti.

6. Configurare Workspace

   Condividere l'URL dell'area di lavoro da **Workspace Configuration > Access** con i propri utenti.

## Licenze

October 6, 2022

Questo articolo tratta le attività e le risorse necessarie per le licenze Microsoft e le licenze Citrix.

## Configurare un server di licenze Servizi Desktop remoto Microsoft per i carichi di lavoro di Windows Server

Queste informazioni si applicano quando si distribuiscono carichi di lavoro di Windows Server.

Questo servizio consente di accedere alle funzionalità di sessione remota di Windows Server quando viene consegnato un carico di lavoro di Windows Server, ad esempio Windows 2019. Questa operazione richiede in genere una licenza di accesso client (CAL) di Servizi Desktop remoto. Il VDA deve essere in grado di contattare un server licenze di Servizi Desktop remoto per richiedere licenze CAL di Servizi Desktop remoto.

Installare e attivare il server licenze. Per ulteriori informazioni, vedere il documento Microsoft Attivare il server licenze di Servizi Desktop remoto. Per gli ambienti Proof of Concept (POC), è possibile utilizzare il periodo di prova fornito da Microsoft.

Con questo metodo, è possibile fare in modo che questo servizio applichi le impostazioni del server licenze. È possibile configurare il server licenze e la modalità per utente nella console di Servizi Desktop remoto sull'immagine. È inoltre possibile configurare il server licenze utilizzando le impostazioni di Criteri di gruppo Microsoft. Per ulteriori informazioni, vedere il documento Microsoft Concedere licenze CAL (Client Access License) per la distribuzione di Servizi Desktop remoto.

Per configurare il server licenze di Servizi Desktop remoto utilizzando le impostazioni di Criteri di gruppo Microsoft:

1. Installare un server licenze di Servizi Desktop remoto in una macchina virtuale disponibile. La macchina virtuale deve essere sempre disponibile. I carichi di lavoro dei servizi Citrix devono essere in grado di raggiungere questo server licenze.
2. Specificare l'indirizzo del server licenze e la modalità di licenza per utente utilizzando Criteri di gruppo Microsoft. Per ulteriori informazioni, vedere il documento Microsoft Specify the Remote Desktop Licensing Model for an RD Session Host Server (Specificare il modello di gestione licenze Desktop remoto per un server Host sessione Desktop remoto).

I carichi di lavoro di Windows 10 richiedono l'adeguata attivazione della licenza di Windows 10. Si consiglia di seguire la documentazione Microsoft per attivare i carichi di lavoro di Windows 10.

## Utilizzo della licenza Citrix

Per informazioni sull'uso della licenza Citrix, vedere:

- Monitor license and active usage for cloud services
- Monitorare la licenza e l'utilizzo attivo per Citrix DaaS

# Licenze multi-tipo

August 17, 2023

Le licenze multi-tipo supportano il consumo di diversi diritti di licenza in un'unica distribuzione di Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). Questo articolo si applica a chi dispone di più di un diritto di licenza Citrix. Una licenza Citrix è una combinazione dei seguenti elementi:

- Prodotto, che nell'attuale contesto di DaaS è sempre Citrix DaaS
- Edizione del servizio (ad esempio: Advanced, Advanced Plus, Premium o Premium Plus)
- Modello di licenza (ad esempio: utente/dispositivo o simultanea)

## Regole per combinare i diritti

Le regole per combinare le edizioni dei servizi sono le seguenti:

- È consentito solo combinare DaaS Advanced e Advanced Plus
- È consentito solo combinare DaaS Premium e Premium Plus
- DaaS Standard non può essere combinato con altre edizioni

È possibile combinare i modelli di licenza quando vengono seguite le regole della precedente edizione del servizio.

## Autorizzazione a livello di sede e di gruppo di consegna

È possibile configurare e utilizzare i diritti di licenza ai due livelli seguenti:

- Sito (la propria implementazione del prodotto Citrix DaaS)
- Gruppo di consegna

Se non si sono ancora configurate le autorizzazioni per il sito o il gruppo di consegna, tenere presente il seguente comportamento predefinito:

- Se si dispone di più di un diritto, viene selezionato quello con più funzionalità tra i diritti disponibili a livello di sito, a condizione che siano stati ordinati contemporaneamente. Altrimenti il primo che viene visualizzato diventa l'impostazione predefinita a livello di sito a meno che tale impostazione non venga modificata esplicitamente in seguito.
- Viene utilizzato il diritto al sito a meno che non sia configurato un diritto a un gruppo di consegna.

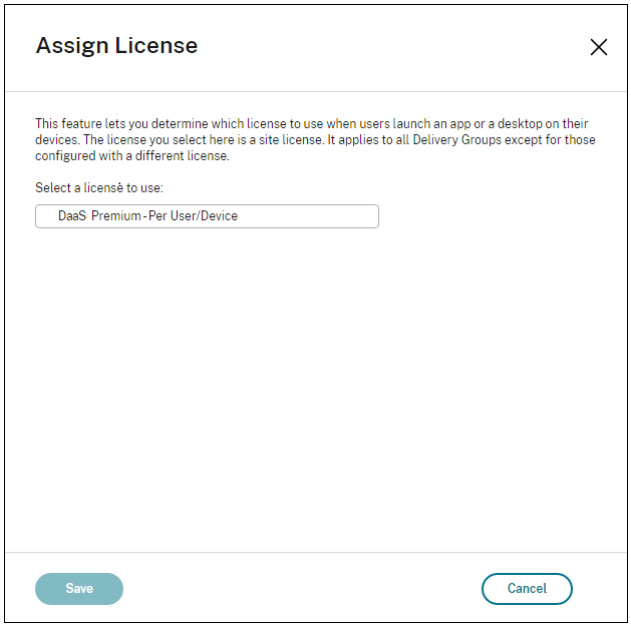
 

> **Nota:**
>
> La configurazione dei diritti per un sito o un gruppo di consegna influisce sul modo in cui viene conteggiato il consumo delle licenze nelle visualizzazioni dell'utilizzo delle licenze in Citrix Cloud

### Visualizzare e aggiornare il diritto a livello di sito

Per specificare quale diritto di licenza utilizzare in tutto il sito, andare a **Full Configuration > Settings > Assign license** (Configurazione completa > Impostazioni > Assegna licenza) e fare clic su **Edit**. Viene visualizzato il pannello **Assign License**. Per informazioni su come accedere alla pagina **Full Configuration**, vedere la documentazione di Citrix DaaS.

Nel pannello **Assign Licence**, selezionare una licenza che si desidera venga utilizzata dal sito. La licenza selezionata si applica a tutti i gruppi di consegna del sito, ma non ai gruppi di consegna configurati con una licenza diversa.




Le licenze disponibili da selezionare sono le seguenti:

- Citrix DaaS Premium - Per utente/dispositivo
- Citrix DaaS Premium - Simultanea
- Citrix DaaS Premium per Google Cloud - Per utente/dispositivo
- Citrix DaaS Premium per Google Cloud —Simultanea
- Citrix DaaS Advanced - Per utente/dispositivo
- Citrix DaaS Advanced - Simultanea
- Citrix DaaS Advanced Plus - Per utente/dispositivo
- Citrix DaaS Advanced Plus - Simultanea
- Citrix DaaS Standard per Azure - Per utente/dispositivo

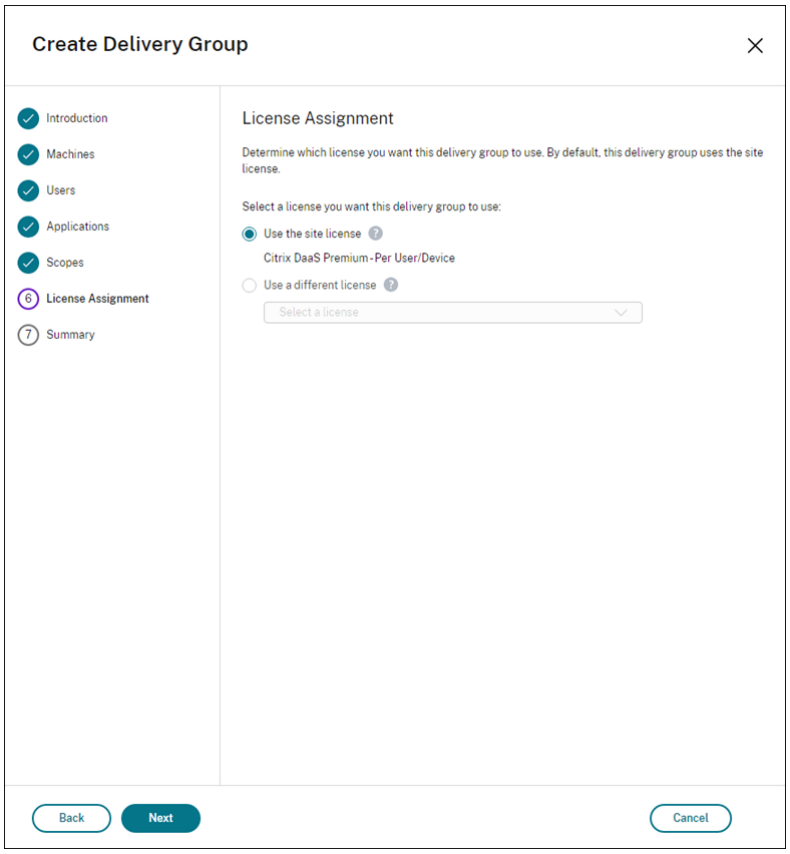
 

- Citrix DaaS Standard per Azure - Simultanea
- Citrix DaaS Standard per Google Cloud - Per utente/dispositivo
- Citrix DaaS Standard per Google Cloud —Simultanea

Se la propria licenza è scaduta, contattare il proprio rappresentante di vendita Citrix per rinnovarla o per acquistare nuove licenze.

### Visualizzare e aggiornare un diritto a livello di gruppo di consegna

È possibile specificare la licenza che si desidera venga utilizzata da un gruppo di consegna per la creazione o la modifica di un gruppo di consegna. Nella pagina **License Assignment** (Assegnazione licenza), selezionare un'opzione.




Opzioni:

- **Use the site license** (Utilizzare la licenza per sito). Una licenza per sito si applica a tutti i gruppi di consegna, a eccezione dei gruppi di consegna configurati con una licenza diversa. La licenza che appare sotto questa opzione è la licenza del sito in uso. Per configurare la licenza del sito, passare a **Manage > Full Configuration**, selezionare il nodo **Settings** (Impostazioni) e quindi modificare **Assign license** (Assegna licenza).

- **Use a different license** (Utilizzare una licenza diversa). Questa opzione consente di configurare questo gruppo di consegna per l'utilizzo di una licenza diversa dalla licenza del sito. Ricordare che il diritto della licenza è una combinazione di codice prodotto, edizione e modello di licenza. Il gruppo di consegna deve utilizzare la stessa edizione di licenza (Standard, Premium o Advanced) del sito. Se configurato, il gruppo di consegna consuma solo la licenza selezionata. Anche se la licenza selezionata viene completamente consumata o è diventata non valida, il gruppo di consegna non torna alla licenza del sito.

Per impostazione predefinita, il gruppo di consegna utilizza la licenza del sito.

Quando una licenza del gruppo di consegna scade e non è più valida, utilizzare una licenza diversa.

> **Nota:**
>
> Se in seguito si configura un gruppo di consegna per l'utilizzo di una licenza diversa, gli utenti connessi che utilizzano la licenza corrente potrebbero perdere temporaneamente l'accesso ai desktop e alle applicazioni.

### Un esempio di combinazione di diritti

Ad esempio, si consideri che il Cliente A abbia acquistato inizialmente l'edizione Advanced e successivamente l'edizione Advanced Plus. In questo caso, il Cliente A dispone ancora di una licenza valida solo per l'edizione Advanced per l'intero sito. Citrix non modifica l'impostazione inizialmente effettuata a livello di sito dal Cliente A. È responsabilità del Cliente A modificare l'edizione della licenza in Advanced Plus a livello di sito.

Analogamente, il Cliente A può aggiornare l'edizione della licenza ad Advanced Plus anche nel gruppo di consegna. Se questa impostazione non è configurata, il gruppo di consegna eredita l'edizione della licenza impostata a livello di sito.

L'amministratore del cliente A può aggiornare l'edizione della licenza nei seguenti modi:

- Aggiornare l'edizione della licenza a livello di sito: passare a **Manage > Full Configuration**, selezionare il nodo **Settings**, quindi modificare **Assign license** (Assegna licenza).
- Aggiornare l'edizione della licenza a livello di gruppo di consegna: passare a **Manage > Full Configuration**, selezionare il nodo **Delivery groups** (Gruppi di consegna). Modificare il gruppo di consegna target per apportare modifiche.

#### Aggiornare il gruppo di consegna utilizzando il comando PowerShell

Il comando PowerShell per aggiornare il gruppo di consegna è il seguente:

```
Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
    code> -LicenseModel <The type of license model>
```

```
<!--NeedCopy-->
```

Aggiornare il comando precedente, in base ai propri dati.

Ad esempio, considerare quanto segue:

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`
- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null` (imposta la configurazione a livello di gruppo di consegna sulla configurazione impostata a livello di sito)
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

Tenere presente che il modello di licenza e il codice del prodotto non sono impostati a livello di gruppo di consegna. In questo scenario, queste due proprietà impostate a livello di sito vengono utilizzate per il gruppo di consegna.

Per ulteriori informazioni sull'SDK Remote PowerShell Citrix DaaS, vedere la documentazione di SDK e API.

### Ulteriori informazioni

- Licenze
- Creare gruppi di consegna
- Gestire i gruppi di consegna

## Bilanciare il carico delle macchine

December 5, 2023

> **Nota:**
>
> Questa funzione si applica a tutti i cataloghi: cataloghi di sistemi operativi a sessione singola o a più sessioni. Il bilanciamento del carico verticale si applica solo alle macchine con sistema operativo multisessione.

Il bilanciamento del carico può essere configurato a livello di sito e a livello di gruppo di consegna. Sono disponibili due opzioni: verticale e orizzontale. Per impostazione predefinita, il bilanciamento del carico orizzontale è abilitato.

### Impostazioni di bilanciamento del carico a livello di sito

- **Bilanciamento del carico verticale**. Assegna una sessione utente in arrivo alla macchina più caricata che non ha ancora raggiunto il carico massimo. Questo processo satura le macchine esistenti prima di passare a nuove macchine. Gli utenti che si disconnettono dalle macchine esistenti liberano capacità su tali macchine. I carichi in entrata vengono quindi assegnati a tali macchine. Il bilanciamento del carico verticale peggiora l'esperienza dell'utente, ma riduce i costi (le sessioni utilizzano al massimo la capacità delle macchine accese).

  Esempio: si dispone di due macchine configurate per 10 sessioni ciascuna. La prima macchina gestisce le prime 10 sessioni simultanee. La seconda macchina gestisce l'undicesima sessione.

  > **Suggerimento:**
  >
  > Per specificare il numero massimo di sessioni che una macchina può ospitare, utilizzare l'impostazione del criterio Maximum number of sessions (Numero massimo di sessioni).

  In alternativa, è possibile utilizzare PowerShell per abilitare o disabilitare il bilanciamento del carico verticale a livello di sito. Utilizzare l'impostazione `UseVerticalScalingForRdsLaunches` nel cmdlet `Set-BrokerSite`. Utilizzare `Get-BrokerSite` per visualizzare il valore dell'impostazione `UseVerticalScalingForRdsLaunches`. Per ulteriori informazioni, vedere la guida dei cmdlet.

- **Bilanciamento del carico orizzontale** Assegna una sessione utente in arrivo alla macchina accesa meno caricata disponibile. Il bilanciamento del carico orizzontale migliora l'esperienza dell'utente, ma aumenta i costi (perché vengono mantenute accese più macchine). Per impostazione predefinita, il bilanciamento del carico orizzontale è abilitato.

  Esempio: si dispone di due macchine configurate per 10 sessioni ciascuna. La prima macchina gestisce cinque sessioni simultanee. Anche la seconda macchina ne gestisce cinque.

Per configurare questa funzione, da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Hosting** nel riquadro di sinistra. Selezionare un'opzione in **Load balance multi-session catalogs** (Cataloghi multisessione di bilanciamento del carico).

### Impostazioni di bilanciamento del carico a livello di gruppo di consegna

La configurazione del bilanciamento del carico a livello del gruppo di consegna consente di sovrascrivere le impostazioni di bilanciamento del carico ereditate dal livello del sito. È possibile ottenere il massimo utilizzo per ogni macchina selezionando il bilanciamento del carico verticale a livello del gruppo di consegna. Ciò contribuirà a ridurre i costi nei cloud pubblici. Questa configurazione può essere eseguita durante la creazione di un nuovo gruppo di consegna o la modifica di un gruppo di consegna esistente.

**Bilanciamento del carico orizzontale**. Le sessioni vengono distribuite tra le macchine accese. Ad esempio, se vi sono due macchine configurate per 10 sessioni ciascuna, la prima macchina gestisce cinque sessioni simultanee e anche la seconda ne gestisce cinque.

**Bilanciamento del carico verticale**. Le sessioni sfruttano al massimo la capacità della macchina accesa e consentono di risparmiare sui costi macchina. Ad esempio, se vi sono due macchine configurate per 10 sessioni ciascuna, la prima macchina gestisce le prime 10 sessioni simultanee. La seconda macchina gestisce l'undicesima sessione.

## Cache host locale

November 21, 2023

> **Suggerimento:**
>
> In **Full Configuration > Home**, la funzionalità di avvisi sullo stato del servizio fornisce avvisi proattivi per garantire che la cache e le zone dell'host locale siano configurate correttamente. Pertanto, quando si verifica un'interruzione, la cache host locale funziona e gli utenti non ne risentono. Gli avvisi sono a due livelli: avvisi a livello di sito visualizzati in Home (icona a forma di bandiera) e avvisi relativi alla zona visualizzati nella scheda Troubleshoot (Risoluzione dei problemi) di ciascuna area. Per ulteriori informazioni, vedere Zone.

La cache host locale consente di continuare le operazioni di intermediazione delle connessioni in una distribuzione di Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops) quando un Cloud Connector non è in grado di comunicare con Citrix Cloud. La cache host locale si attiva quando la connessione di rete viene persa per 60 secondi.

Con Local Host Cache, gli utenti che sono connessi quando si verifica un'interruzione possono continuare a lavorare senza interruzioni. Le riconnessioni e le nuove connessioni subiscono ritardi di connessione minimi.

> **Importante:**
>
> Se si utilizza una distribuzione StoreFront locale, è necessario aggiungere tutti i Cloud Connector che hanno (o possono avere) VDA registrati allo StoreFront come Delivery Controller. Un Cloud Connector che non viene aggiunto a StoreFront non può passare alla modalità di interruzione, con possibili conseguenti errori di avvio dell'utente.
>
> Per le distribuzioni senza StoreFront on-premise, utilizzare la funzionalità di continuità del servizio della piattaforma Citrix Workspace per consentire agli utenti di connettersi alle risorse durante le interruzioni. Per ulteriori informazioni, vedere Continuità del servizio.

### Contenuto di dati

La cache host locale include le seguenti informazioni, che sono un sottoinsieme delle informazioni contenute nel database principale:

- Identità degli utenti e dei gruppi a cui vengono assegnati diritti sulle risorse pubblicate dal sito.
- Identità degli utenti che attualmente utilizzano o che hanno recentemente utilizzato le risorse pubblicate dal sito.
- Identità delle macchine VDA (incluse le macchine Accesso remoto PC) configurate nel sito.
- Identità (nomi e indirizzi IP) delle macchine client dell'app Citrix Workspace utilizzate attivamente per connettersi alle risorse pubblicate.

Contiene inoltre informazioni per le connessioni attualmente attive che sono state stabilite mentre il database principale non era disponibile:

- Risultati di tutte le analisi endpoint della macchina client eseguite dall'app Citrix Workspace.
- Identità delle macchine dell'infrastruttura (quali Citrix Gateway e server StoreFront) coinvolte nel sito.
- Date, orari e tipi delle attività recenti svolte dagli utenti.

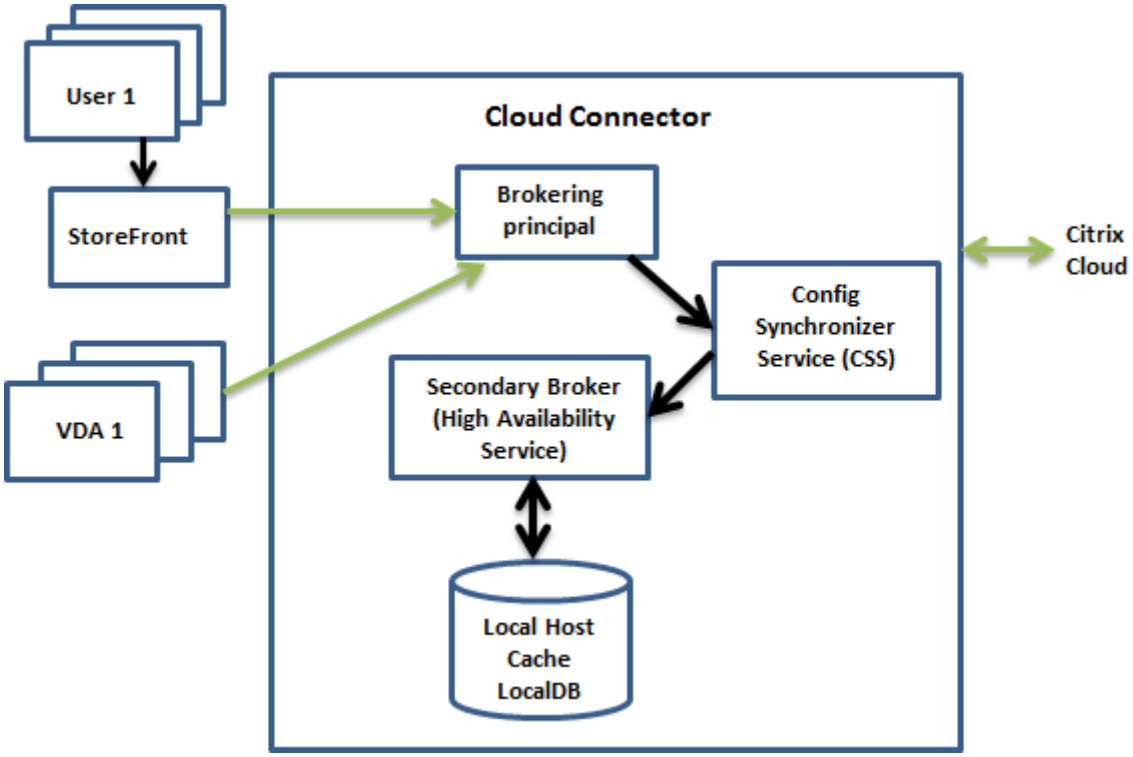
### Come funziona

Ecco come Local Host Cache interagisce con Citrix Cloud.

Si tratta di un video incorporato. Fare clic sul collegamento per guardare il video

**Durante le normali operazioni**




- Il Brokering Principal (noto anche come Citrix Remote Broker Provider Service) presente su un Cloud Connector accetta le richieste di connessione da StoreFront. Il broker principale comunica con Citrix Cloud per connettere gli utenti con VDA che sono registrati con Cloud Connector.
- Citrix Config Synchronizer Service (CSS) controlla il broker di Citrix Cloud circa ogni 5 minuti per verificare se sono state apportate modifiche alla configurazione. Tali modifiche possono essere avviate dall'amministratore (ad esempio la modifica di una proprietà di un gruppo di consegna) o le azioni di sistema (come le assegnazioni di macchine).
- Se la configurazione è cambiata dopo il controllo precedente, CSS sincronizza (copia) le informazioni con un broker secondario presente nel Cloud Connector. Il broker secondario è anche noto come servizio High Availability o broker HA, come mostrato nella figura precedente.

  Vengono copiati tutti i dati di configurazione, non solo gli elementi che sono cambiati dopo il controllo precedente. Il CSS importa i dati di configurazione in un database Microsoft SQL Server Express LocalDB sul Cloud Connector. Questo database viene denominato database della cache host locale. CSS assicura che le informazioni contenute nel database della cache host locale corrispondano alle informazioni presenti nel database del sito in Citrix Cloud. Il database della cache host locale viene ricreato a ogni sincronizzazione.

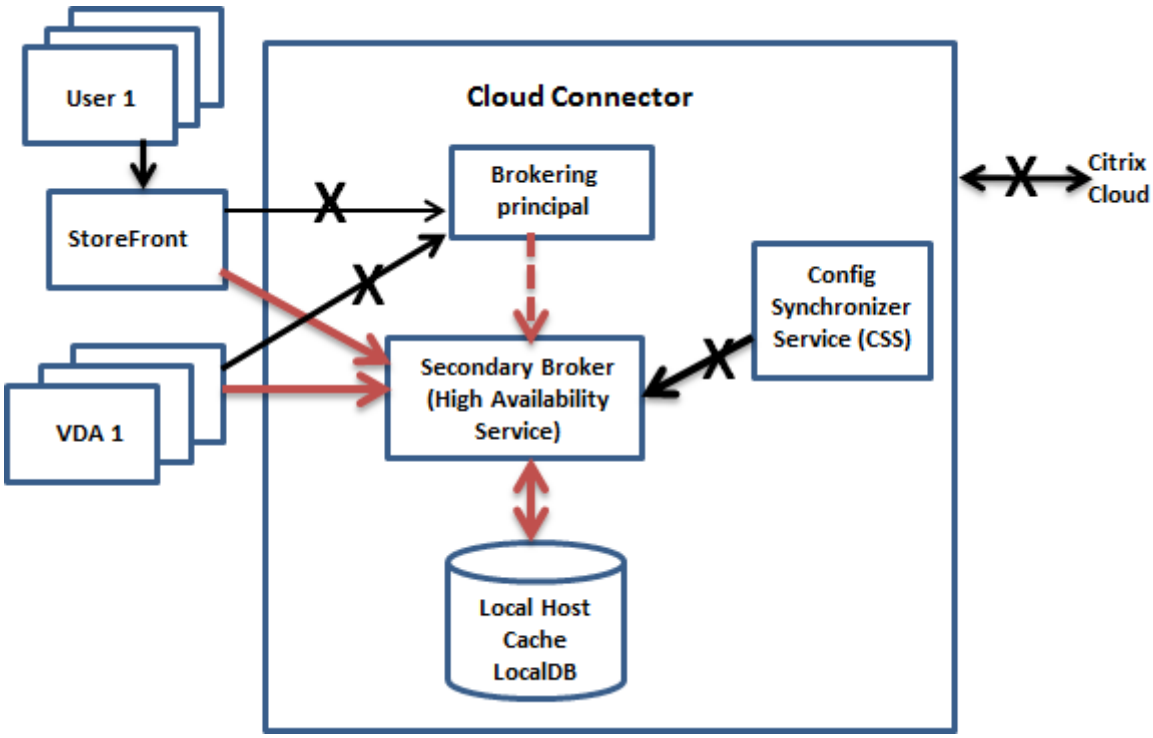
  Microsoft SQL Server Express LocalDB (utilizzato dal database della cache host locale) viene installato automaticamente quando si installa un Cloud Connector. Il database Local Host Cache

non può essere condiviso tra più Cloud Connector. Non è necessario eseguire il backup del database della cache host locale. Viene ricreato ogni volta che viene rilevata una modifica della configurazione.

- Se non vi sono state modifiche dopo l'ultimo controllo, i dati di configurazione non vengono copiati.

**Durante un'interruzione**




Quando inizia un'interruzione:

- Il broker secondario inizia l'ascolto e l'elaborazione delle richieste di connessione.
- Quando inizia l'interruzione, il broker secondario non dispone dei dati di registrazione VDA correnti, ma quando un VDA comunica con esso, viene attivato un processo di registrazione. Durante tale processo, il broker secondario riceve anche le informazioni sulla sessione corrente relative a quel VDA.
- Mentre il broker secondario gestisce le connessioni, il broker principale continua a monitorare la connessione a Citrix Cloud. Quando la connessione viene ripristinata, il broker principale chiede al broker secondario di interrompere l'ascolto delle informazioni sulla connessione e ricomincia a svolgere le operazioni di mediazione. La volta successiva che un VDA comunica con il broker principale, viene attivato un processo di registrazione. Il broker secondario rimuove le registrazioni VDA che sono rimaste dall'interruzione precedente. Il CSS riprende la sincronizzazione delle informazioni quando rileva che sono state apportate modifiche della configurazione in

Citrix Cloud.

Nell'improbabile caso in cui un'interruzione inizi durante una sincronizzazione, l'importazione corrente viene eliminata e viene utilizzata l'ultima configurazione nota.

Il registro degli eventi indica quando si verificano sincronizzazioni e interruzioni.

Non è previsto alcun limite di tempo per il funzionamento in modalità di interruzione.

È inoltre possibile attivare intenzionalmente un'interruzione. Per dettagli su perché e come farlo, vedere Forzare un'interruzione.

#### Posizioni delle risorse con più Cloud Connector

Tra le altre attività che svolge, il CSS fornisce regolarmente al broker secondario informazioni su tutti i Cloud Connector della posizione delle risorse. Avendo queste informazioni, ogni broker secondario è a conoscenza di tutti i broker secondari peer che sono in esecuzione su altri Cloud Connector nella posizione della risorsa.

I broker secondari comunicano tra loro su un canale separato. Questi broker utilizzano un elenco alfabetico di nomi FQDN delle macchine su cui sono in esecuzione per determinare (scegliere) quale broker secondario medierà le operazioni nella zona in caso di interruzione. Durante l'interruzione, tutti i VDA si registrano di nuovo presso il broker secondario scelto. I broker secondari non scelti della zona rifiutano attivamente le richieste di connessione e di registrazione VDA in entrata.

Se un broker secondario scelto si arresta durante un'interruzione, viene scelto un altro broker secondario al suo posto e i VDA si registrano presso il broker secondario appena scelto.

Durante un'interruzione, se un Cloud Connector viene riavviato:

- Se quel Cloud Connector non è il broker scelto, il riavvio non ha alcun impatto.
- Se il Cloud Connector è il broker scelto, ne viene scelto un altro, facendo registrare i VDA. Dopo l'accensione, il Cloud Connector riavviato assume automaticamente il ruolo di mediazione, facendo nuovamente registrare i VDA. In questo scenario, durante le registrazioni le prestazioni possono risentirne.

Nel registro eventi sono disponibili informazioni sulla scelta dei broker.

### Cosa non è disponibile durante un'interruzione e altre differenze

Non è previsto alcun limite di tempo per il funzionamento in modalità di interruzione. Tuttavia, se l'interruzione è dovuta alla perdita della connettività a Citrix Cloud dalla posizione delle risorse, Citrix consiglia di ripristinare la connettività dalla posizione della risorsa al più presto possibile.

Durante un'interruzione:

- Non è possibile utilizzare le interfacce di **Manage**.
- È disponibile un accesso limitato all'SDK Remote PowerShell.
  - È necessario innanzitutto:
    * Aggiungere una chiave `EnableCssTestMode` del Registro di sistema con un valore di 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Impostare l'autenticazione SDK su `OnPrem` in modo che il proxy SDK non tenti di reindirizzare le chiamate ai cmdlet: `$XDSDKAuth="OnPrem"`
    * Usare la porta 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - Dopo aver eseguito questi comandi, è possibile accedere a:
    * Tutti i cmdlet `Get-Broker*`.
- I dati di monitoraggio non vengono inviati a Citrix Cloud durante un'interruzione. Pertanto, le funzioni di **Monitor** non evidenziano attività a partire da un intervallo di interruzione.
- Le credenziali Hypervisor non possono essere ottenute dal servizio host. Tutte le macchine sono in stato di alimentazione sconosciuto e non è possibile emettere operazioni di alimentazione. Tuttavia, le macchine virtuali dell'host che sono alimentate possono essere utilizzate per le richieste di connessione.
- Una macchina assegnata può essere utilizzata solo se l'assegnazione si è verificata durante le normali operazioni. Non è possibile effettuare nuove assegnazioni durante un'interruzione.
- La registrazione e la configurazione automatica delle macchine Accesso remoto al PC non sono possibili. Tuttavia, le macchine che sono state registrate e configurate durante il normale funzionamento sono utilizzabili.
- Le applicazioni ospitate da server e gli utenti desktop potrebbero utilizzare più sessioni rispetto ai limiti di sessione configurati, se le risorse si trovano in zone diverse.
- Gli utenti possono avviare applicazioni e desktop solo da VDA registrati nella zona contenente il broker attualmente attivo/scelto. Gli avvii tra una zona e l'altra (da un broker che si trova in una zona a un VDA che si trova in una zona diversa) non sono supportati durante un'interruzione.
- Se si verifica un'interruzione del database del sito prima dell'inizio di un riavvio pianificato per i VDA di un gruppo di consegna, i riavvii iniziano al termine dell'interruzione. Questo scenario può dare risultati imprevisti. Per ulteriori informazioni, vedere Riavvii pianificati ritardati a causa di un'interruzione del database.
- La preferenza di zona non può essere configurata. Se è configurata, le preferenze non vengono prese in considerazione per l'avvio della sessione.

- Le restrizioni sui tag in cui i tag vengono utilizzati per designare le posizioni risorsa non sono supportate per l'avvio delle sessioni. Quando sono configurate restrizioni di tag e l'opzione di controllo avanzato di integrità di uno store StoreFront è abilitata, alcune delle sessioni potrebbero non avviarsi.

## Requisiti di StoreFront

Se si utilizza una distribuzione StoreFront locale, è necessario aggiungere tutti i Cloud Connector che hanno (o possono avere) VDA registrati allo StoreFront come Delivery Controller. Un Cloud Connector che non viene aggiunto a StoreFront non può passare alla modalità di interruzione, con possibili conseguenti errori di avvio dell'utente.

### Disponibilità delle risorse

Durante un'interruzione è possibile garantire la disponibilità di risorse (app e desktop) in due modi:

- Pubblicare le risorse in ogni posizione delle risorse della distribuzione.
- Se si utilizza StoreFront 1912 CU4 o versione successiva, pubblicare le risorse in almeno una posizione di risorse e attivare il controllo avanzato dello stato su tutti i server StoreFront. Per le versioni precedenti a StoreFront 2308, il controllo di integrità avanzato è disattivato per impostazione predefinita e deve essere abilitato da un amministratore. Per StoreFront versione 2308 e successive, questa funzionalità è abilitata per impostazione predefinita. Per ulteriori informazioni e istruzioni sull'attivazione del controllo di integrità avanzato, vedere Controllo di integrità avanzato.

## Supporto di applicazioni e desktop

La cache host locale supporta applicazioni e desktop ospitati da server e desktop statici (assegnati).

La cache host locale supporta i VDA desktop (a sessione singola) nei gruppi di consegna in pool, come indicato di seguito.

- Per impostazione predefinita, i VDA desktop con gestione dell'alimentazione in gruppi di consegna in pool (creati da MCS o Citrix Provisioning) con la proprietà `ShutdownDesktopsAfterUse` abilitata non sono disponibili per le nuove connessioni durante un evento della cache host locale. È possibile modificare questa impostazione predefinita per consentire l'utilizzo di tali desktop durante l'evento della cache host locale.

  Tuttavia, non è necessariamente possibile fare affidamento sulla gestione dell'alimentazione durante l'interruzione. La gestione dell'alimentazione riprende dopo il ripresa delle normali

operazioni. Inoltre, tali desktop potrebbero contenere dati dell'utente precedente, perché non sono stati riavviati.

- Per ignorare il comportamento predefinito, è necessario abilitarlo in tutto il sito e per ogni gruppo di consegna interessato, utilizzando i comandi di PowerShell.

  Per intervenire su tutto il sito, eseguire il seguente comando:

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  Per impostazione predefinita, tutti i gruppi di consegna non sono abilitati per questa funzione. Esistono due opzioni per abilitarla a livello di gruppo di consegna:

  - **Abilitare per gruppi di consegna selezionati:** per ciascun gruppo di consegna interessato, eseguire il seguente comando.

    ```
    Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOuta
     $true
    ```

  - **Abilitare per tutti i gruppi di consegna:** per abilitare l'impostazione predefinita a livello di gruppo di consegna, eseguire il seguente comando. Questa impostazione si applica a tutti i gruppi di consegna di nuova creazione (ovvero, a tutti i gruppi di consegna creati dopo aver abilitato l'impostazione).

    ```
    Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage
    $true
    ```

    Per abilitare questa opzione per i gruppi di consegna esistenti, eseguire il comando indicato in precedenza (`Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutS $true`).

  L'attivazione di questa funzione nel sito e nei gruppi di consegna non influisce sul funzionamento della proprietà `ShutdownDesktopsAfterUse` configurata durante le normali operazioni.

> **Importante:**
>
> Senza abilitare ReuseMachinesWithoutShutdownInOutageAllowed a livello di sito e ReuseMachinesWithoutShutdownInOutage a livello di gruppo di consegna, tutti i tentativi di avvio della sessione di VDA desktop ad alimentazione gestita in gruppi di consegna in pool non riusciranno durante un evento Local Host Cache.

### Verificare che la cache dell'host locale funzioni

Ecco come verificare che Local Host Cache sia configurata correttamente.

Si tratta di un video incorporato. Fare clic sul collegamento per guardare il video

Per verificare che la cache host locale sia correttamente configurata e in funzione:

- Se si utilizza StoreFront, verificare che la distribuzione locale di StoreFront punti a tutti i Cloud Connector in quella posizione risorsa.
- Assicurarsi che le importazioni di sincronizzazione siano completate correttamente. Controllare i registri degli eventi.
- Assicurarsi che sia stato creato il database Local Host Cache su ogni Cloud Connector. Ciò conferma che il servizio High Availability può subentrare, se necessario.
  - Sul server Cloud Connector, passare a `c:\Windows\ServiceProfiles\NetworkService`.
  - Verificare che vengano creati `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf`.
- Selezionare Force an outage su tutti i Cloud Connector nella posizione della risorsa. Dopo aver verificato che la cache locale host funziona, ricordare di rimettere tutti i Cloud Connector in modalità normale. Questa operazione può richiedere circa 15 minuti.

## Registri eventi

I registri eventi indicano quando si verificano sincronizzazioni e interruzioni. Nei registri del visualizzatore eventi, la modalità di interruzione viene definita *modalità HA*.

### Servizio Config Synchronizer

Durante le normali operazioni, possono verificarsi gli eventi di cui sotto quando il CSS importa i dati di configurazione nel database della cache host locale utilizzando il broker cache host locale.

- 503: Citrix Config Sync Service ha ricevuto una configurazione aggiornata. Questo evento si verifica ogni volta che viene ricevuta una configurazione aggiornata da Citrix Cloud. Indica l'inizio del processo di sincronizzazione.
- 504: Citrix Config Sync Service ha importato una configurazione aggiornata. L'importazione della configurazione è stata completata correttamente.
- 505: Citrix Config Sync Service non è riuscito a effettuare un'importazione. L'importazione della configurazione non è stata completata correttamente. Se è disponibile, viene utilizzata una precedente configurazione riuscita in caso di interruzione. Tuttavia, sarà obsoleta rispetto alla configurazione corrente. Se non è disponibile alcuna configurazione precedente, il servizio non può partecipare alla mediazione della sessione durante un'interruzione. In questo caso, consultare la sezione Risoluzione dei problemi e contattare il Supporto Citrix.
- 507: Citrix Config Sync Service ha abbandonato un'importazione perché il sistema è in modalità di interruzione e viene utilizzato il broker cache host locale per la mediazione. Il servizio ha ricevuto una nuova configurazione, ma l'importazione è stata abbandonata a causa di un'interruzione. Questo è un comportamento previsto.

- 510: nessun dato di configurazione del Configuration Service ricevuto dal servizio di configurazione principale.
- 517: si è verificato un problema di comunicazione con il Broker principale.
- 518: lo script Config Sync si è interrotto perché il Broker secondario (High Availability Service) non è in esecuzione.

#### Servizio High Availability

Questo servizio è noto anche come broker cache host locale.

- 3502: si è verificata un'interruzione e il broker cache host locale sta eseguendo operazioni di mediazione.
- 3503: è stata risolta un'interruzione e sono riprese le normali operazioni.
- 3504: indica quale broker cache host locale viene scelto, oltre ad altri broker cache host locale coinvolti nella scelta.
- 3507: fornisce un aggiornamento dello stato della cache host locale ogni 2 minuti; questo indica che la modalità Cache host locale è attiva sul broker selezionato. Contiene un riepilogo dell'interruzione, inclusa la durata dell'interruzione, la registrazione del VDA e le informazioni sulla sessione.
- 3508: annuncia che la cache host locale non è più attiva sul broker scelto e le normali operazioni sono state ripristinate. Contiene un riepilogo dell'interruzione che include la durata dell'interruzione, il numero di macchine registrate durante l'evento della cache host locale e il numero di avvii riusciti durante l'evento LHC.
- 3509: notifica che la cache host locale è attiva sui broker non scelti. Contiene una durata di interruzione ogni 2 minuti e indica il broker scelto.
- 3510: annuncia che la cache host locale non è più attiva sui broker non scelti. Contiene la durata dell'interruzione e indica il broker scelto.

### Forzare un'interruzione

Potrebbe essere utile forzare deliberatamente un'interruzione.

- Se la rete continua a disattivarsi e riattivarsi. Forzare un'interruzione fino a quando non vengono risolti i problemi di rete impedisce la transizione continua tra modalità normale e di interruzione (e le frequenti tempeste di registrazione VDA che ne derivano).
- Per verificare un piano di ripristino di emergenza.
- Per aiutare a garantire che cache host locale funzioni correttamente.

Sebbene un Cloud Connector possa essere aggiornato durante un'interruzione forzata, possono verificarsi problemi imprevisti. Consigliamo di impostare una pianificazione per gli aggiornamenti di Cloud Connector che eviti gli intervalli di modalità di interruzione forzata.

Per forzare un'interruzione, modificare il registro di ciascun server Cloud Connector. In `HKLM\Software\Citrix\DesktopServer\LHC`, creare e impostare `OutageModeForced` come `REG_DWORD` su `1`. Questa impostazione indica al broker Local Host Cache di entrare in modalità di interruzione, indipendentemente dallo stato della connessione a Citrix Cloud. Impostando il valore su `0` si fa uscire il broker cache host locale dalla modalità di interruzione.

Per verificare gli eventi, monitorare il file di log `Current_HighAvailabilityService` al percorso `C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAvailabilityService`.

### Risoluzione dei problemi

Sono disponibili diversi strumenti per la risoluzione dei problemi quando un'importazione di sincronizzazione nel database della cache host locale non riesce e viene pubblicato un evento 505.

**CDF tracing**: contiene opzioni per i moduli ConfigSyncServer e BrokerLHC. Queste opzioni, insieme ad altri moduli broker, possono identificare il problema.

**Report:** se un'importazione di sincronizzazione non riesce, è possibile generare un rapporto. Questo rapporto si arresta all'oggetto che causa l'errore. Questa funzione di report influisce sulla velocità di sincronizzazione, pertanto Citrix consiglia di disabilitarla quando non è in uso.

Per abilitare e produrre un report di traccia CSS, immettere il seguente comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

Il report HTML è pubblicato all'indirizzo: `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`

Dopo aver generato il report, immettere il seguente comando per disabilitare la funzione di reporting:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

#### Comandi PowerShell della cache host locale

È possibile gestire la cache host locale sui Cloud Connector utilizzando i comandi PowerShell.

Il modulo PowerShell si trova nella seguente posizione sui Cloud Connectors:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Importante:**
>
> Eseguire questo modulo solo sui Cloud Connector.

**Importare il modulo PowerShell** Per importare il modulo, eseguire la procedura seguente sul proprio Cloud Connector:

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-
Module .\HighAvailabilityServiceControl.psm1
```

**Comandi PowerShell per gestire LHC** I seguenti cmdlet consentono di attivare e gestire la modalità LHC sui Cloud Connector.

| Cmdlet | Funzione |
| --- | --- |
| `Enable-LhcForcedOutageMode` | Mettere il broker in modalità LHC. I file di database della cache host locale devono essere stati creati correttamente dal servizio ConfigSync per assicurare che `Enable-LhcForcedOutageMode` funzioni correttamente. Questo cmdlet forza LHC solo sul Cloud Connector su cui è stato eseguito. Per rendere attivo LHC, questo cmdlet deve essere eseguito su tutti i Cloud Connector all'interno della posizione risorsa. |
| `Disable-LhcForcedOutageMode` | Consente di escludere il Broker dalla modalità LHC. Questo cmdlet disabilita solo la modalità LHC sul Cloud Connector su cui è stato eseguito. `Disable-LhcForcedOutageMode` deve essere eseguito su tutti i Cloud Connector all'interno della posizione della risorsa. |

| Cmdlet | Funzione |
| --- | --- |
| `Set-LhcConfigSyncIntervalOverride` | Impostare l'intervallo con cui Citrix Config Synchronizer Service (CSS) verifica se sono state apportate modifiche alla configurazione all'interno del sito Citrix DaaS. L'intervallo di tempo può variare da 60 secondi (un minuto) a 3600 secondi (un'ora). Questa impostazione si applica solo al Cloud Connector su cui è stata eseguita. Per garantire la coerenza tra i Cloud Connector, considerare l'esecuzione di questo cmdlet su ogni Cloud Connector. Ad esempio: `Set-LhcConfigSyncIntervalOverride -Seconds 1200` |
| `Clear-LhcConfigSyncIntervalOverride` | Imposta l'intervallo con cui Citrix Config Synchronizer Service (CSS) verifica le modifiche alla configurazione all'interno del sito Citrix DaaS sul valore predefinito di 300 secondi (cinque minuti). Questa impostazione si applica solo al Cloud Connector su cui è stata eseguita. Per garantire la coerenza tra i Cloud Connector, considerare l'esecuzione di questo cmdlet su ogni Cloud Connector. |
| `Enable-LhcHighAvailabilitySDK` | Abilita l'accesso a tutti i cmdlet `Get-Broker*` all'interno del Cloud Connector in cui è stato eseguito. |
| `Disable-LhcHighAvailabilitySDK` | Disabilita l'accesso ai comandi PowerShell Broker all'interno del Cloud Connector in cui è stato eseguito. |

> **Nota:**
>
> - Utilizzare la porta 89 quando si eseguono i cmdlet `Get-Broker*` sul Cloud Connector. Ad esempio:
>
>   ```
>   - Get-BrokerMachine -AdminAddress localhost:89
>   ```
>
> - Quando non è in modalità LHC, l'LHC Broker sul Cloud Connector contiene solo le informazioni di configurazione.
> - Durante la modalità LHC, il broker LHC presente sul Cloud Connector selezionato contiene

> le seguenti informazioni:
>
> - Stati delle risorse
> - Dettagli della sessione
> - Registrazioni dei VDA
> - Informazioni sulla configurazione

### Ulteriori informazioni

Vedere Considerazioni sulla scalabilità e sul dimensionamento per la cache host locale per informazioni su:

- Metodologie e risultati di test
- Considerazioni sulle dimensioni della RAM
- Considerazioni sulla configurazione del core e del socket della CPU
- Considerazioni sull'archiviazione

## Gestire le chiavi di sicurezza

April 14, 2023

> **Nota:**
>
> - È necessario utilizzare questa funzione in combinazione con StoreFront 1912 LTSR CU2 o versioni successive.
> - La funzionalità Secure XML è supportata solo su Citrix ADC e Citrix Gateway versione 12.1 e successive.

Mediante questa funzione è possibile consentire solo alle macchine StoreFront e Citrix Gateway approvati di comunicare con i Citrix Delivery Controller. Dopo aver attivato questa funzione, tutte le richieste che non contengono la chiave vengono bloccate. Utilizzare questa funzione per aggiungere un ulteriore livello di sicurezza per proteggere dagli attacchi provenienti dalla rete interna.

Un flusso di lavoro generale per utilizzare questa funzione è il seguente:

1. Visualizzare le impostazioni della chiave di sicurezza nell'interfaccia Full Configuration. (Utilizzare l'SDK Remote PowerShell)
2. Configurare le impostazioni per la propria distribuzione. Utilizzare l'interfaccia Full Configuration o l'SDK Remote PowerShell.
3. Configurare le impostazioni in StoreFront (utilizzare PowerShell).

4. Configurare le impostazioni in Citrix ADC.

### Visualizzare le impostazioni della chiave di sicurezza nell'interfaccia Full Configuration

Per impostazione predefinita, le impostazioni per le chiavi di sicurezza non sono visibili nell'interfaccia Full Configuration. Per visualizzarle in quell'interfaccia, utilizzare l'SDK Remote PowerShell. Per ulteriori informazioni sull'SDK Remote PowerShell, vedere SDK e API.

I passaggi dettagliati sono i seguenti:

1. Eseguire l'SDK Remote PowerShell.
2. In una finestra di comando, eseguire i comandi seguenti:
   - `Add-PSSnapIn Citrix*`. Questo comando aggiunge gli snap-in Citrix.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

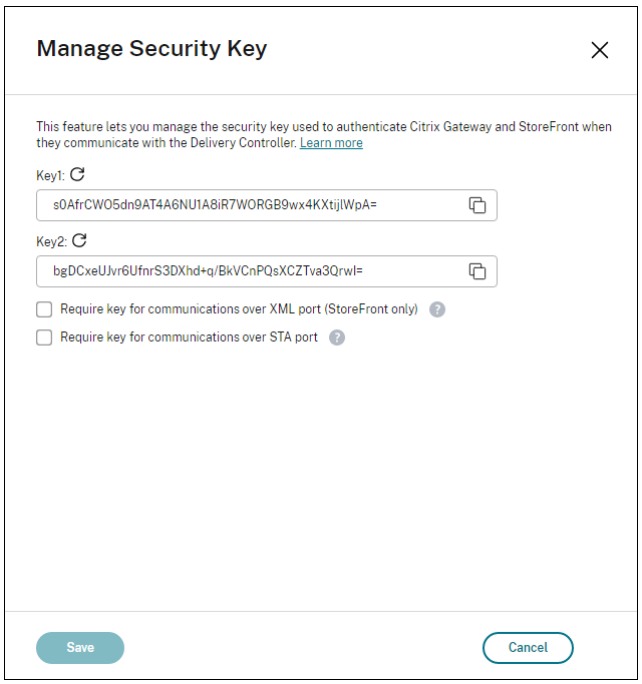
### Configurare le impostazioni per la propria distribuzione

È possibile configurare le impostazioni per la distribuzione utilizzando Full Configuration o PowerShell.

#### Utilizzare l'interfaccia Full Configuration

Dopo aver abilitato la funzionalità, accedere a **Full Configuration > Settings > Manage Security Key** e fare clic su **Edit**. Viene visualizzato il pannello **Manage Security Key**. Fare clic su **Save** per applicare le modifiche e uscire dal pannello.




> **Importante:**
>
> - Vi sono due chiavi disponibili per l'uso. È possibile utilizzare la stessa chiave o chiavi diverse per le comunicazioni tramite le porte XML e STA. Si consiglia di utilizzare solo una chiave alla volta. La chiave non utilizzata viene utilizzata solo per la rotazione delle chiavi.
> - Non fare clic sull'icona di aggiornamento per aggiornare la chiave già in uso, altrimenti vi sarà un'interruzione del servizio.

Fare clic sull'icona di aggiornamento per generare nuove chiavi.

**Require key for communications over XML port (solo StoreFront)**. Se questa opzione è selezionata, viene richiesta una chiave per autenticare le comunicazioni tramite la porta XML. StoreFront comunica con Citrix Cloud su questa porta. Per informazioni sulla modifica della porta XML, vedere l'articolo CTX127945 del Knowledge Center.

**Require key for communications over STA port**. Se questa opzione selezionata, è richiesta una chiave per autenticare le comunicazioni sulla porta STA. Citrix Gateway e StoreFront comunicano con Citrix Cloud su questa porta. Per informazioni sulla modifica della porta STA, vedere l'articolo CTX101988 del Knowledge Center.

Dopo aver applicato le modifiche, fare clic su **Close** per uscire dal pannello **Manage Security Key**.

### Utilizzare l'SDK Remote PowerShell

Di seguito sono riportati i passaggi di PowerShell equivalenti alle operazioni eseguite nell'interfaccia Full Configuration.

1. Eseguire l'SDK Remote PowerShell.
2. In una finestra di comando, eseguire il comando seguente:
   - `Add-PSSnapIn Citrix*`
3. Eseguire i seguenti comandi per generare una chiave e impostare Key1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Eseguire i seguenti comandi per generare una chiave e impostare Key2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Eseguire uno o entrambi i comandi seguenti per abilitare l'utilizzo di una chiave nell'autenticazione delle comunicazioni:
   - Per autenticare le comunicazioni tramite la porta XML:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Per autenticare le comunicazioni tramite la porta STA:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Per indicazioni guida e sintassi, vedere la Guida dei comandi di PowerShell.

### Configurare le impostazioni in StoreFront

Dopo aver completato le impostazioni per la distribuzione, è necessario configurare le impostazioni pertinenti in StoreFront utilizzando PowerShell.

Sul server StoreFront eseguire i seguenti comandi di PowerShell:

- Per configurare la chiave per le comunicazioni tramite la porta XML, utilizzare i comandi `Get-STFStoreServie` e `Set-STFStoreService`. Ad esempio:
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>`
- Per configurare la chiave per le comunicazioni tramite la porta STA, utilizzare il comando `New-STFSecureTicketAuthority`. Ad esempio:
  - `PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL > -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>`

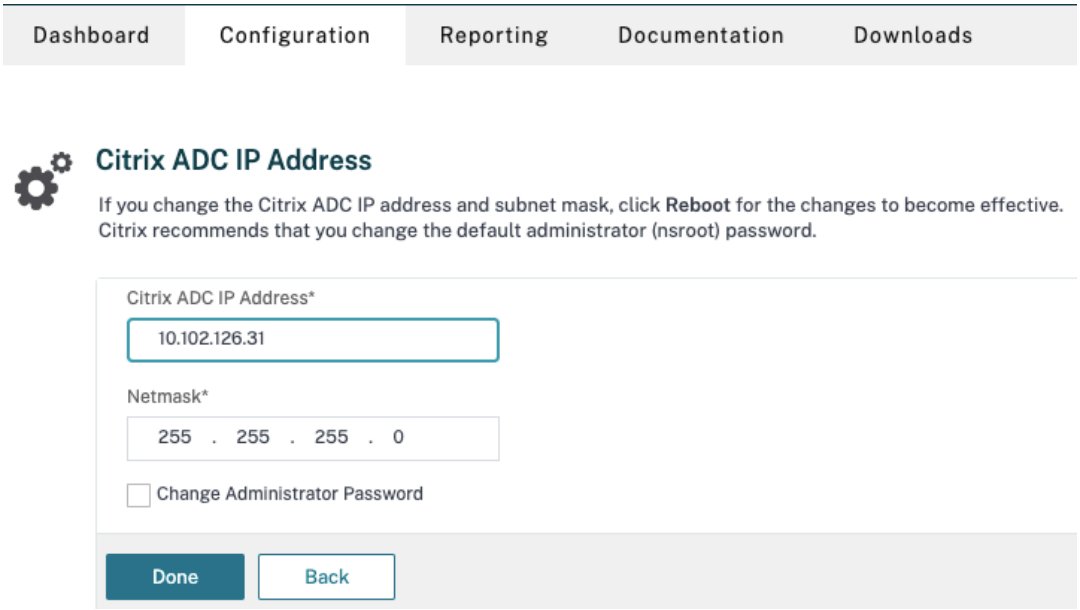
 

Per indicazioni guida e sintassi, vedere la Guida dei comandi di PowerShell.

### Configurare le impostazioni in Citrix ADC

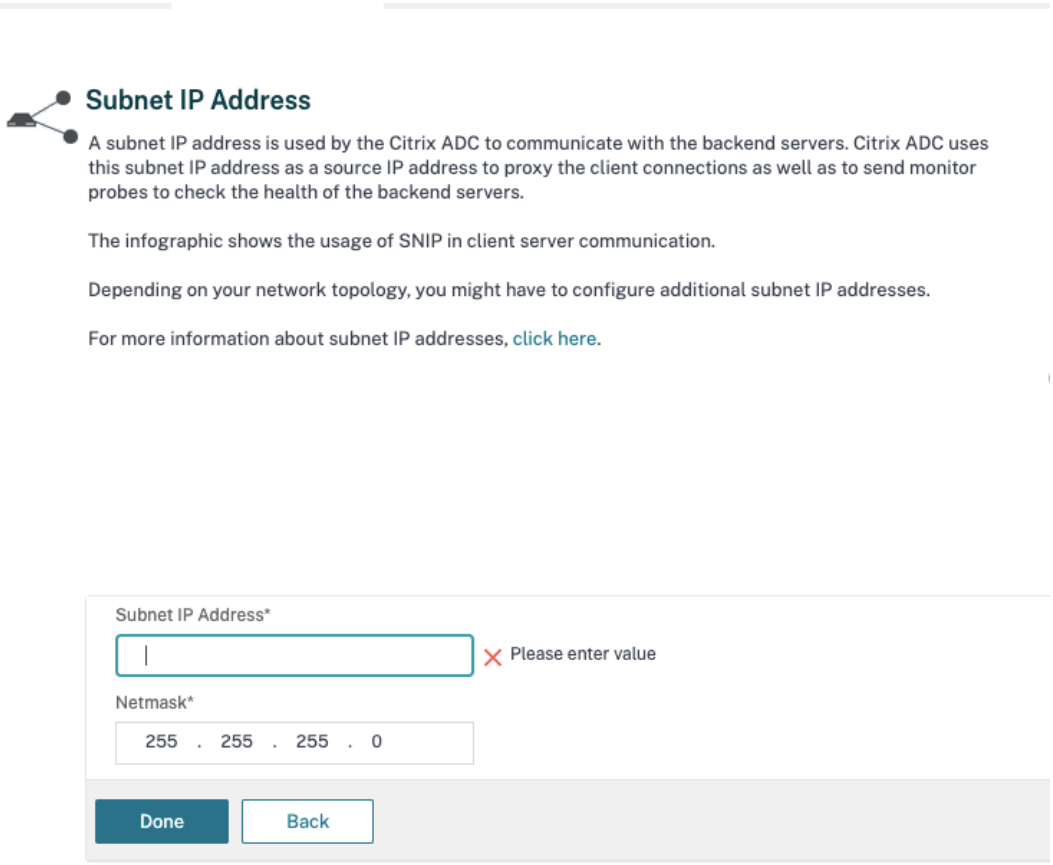
> **Nota:**
>
> La configurazione di questa funzionalità in Citrix ADC non è necessaria a meno che non si utilizzi Citrix ADC come gateway. Se si utilizza Citrix ADC, seguire la procedura riportata di seguito.

1. Assicurarsi che sia stata applicata la seguente configurazione dei prerequisiti:
   - Sono configurati i seguenti indirizzi IP relativi a Citrix ADC.
     - Indirizzo Citrix ADC Management IP (NSIP) per l'accesso alla console Citrix ADC. Per ulteriori informazioni, vedere Configurazione dell'indirizzo NSIP.



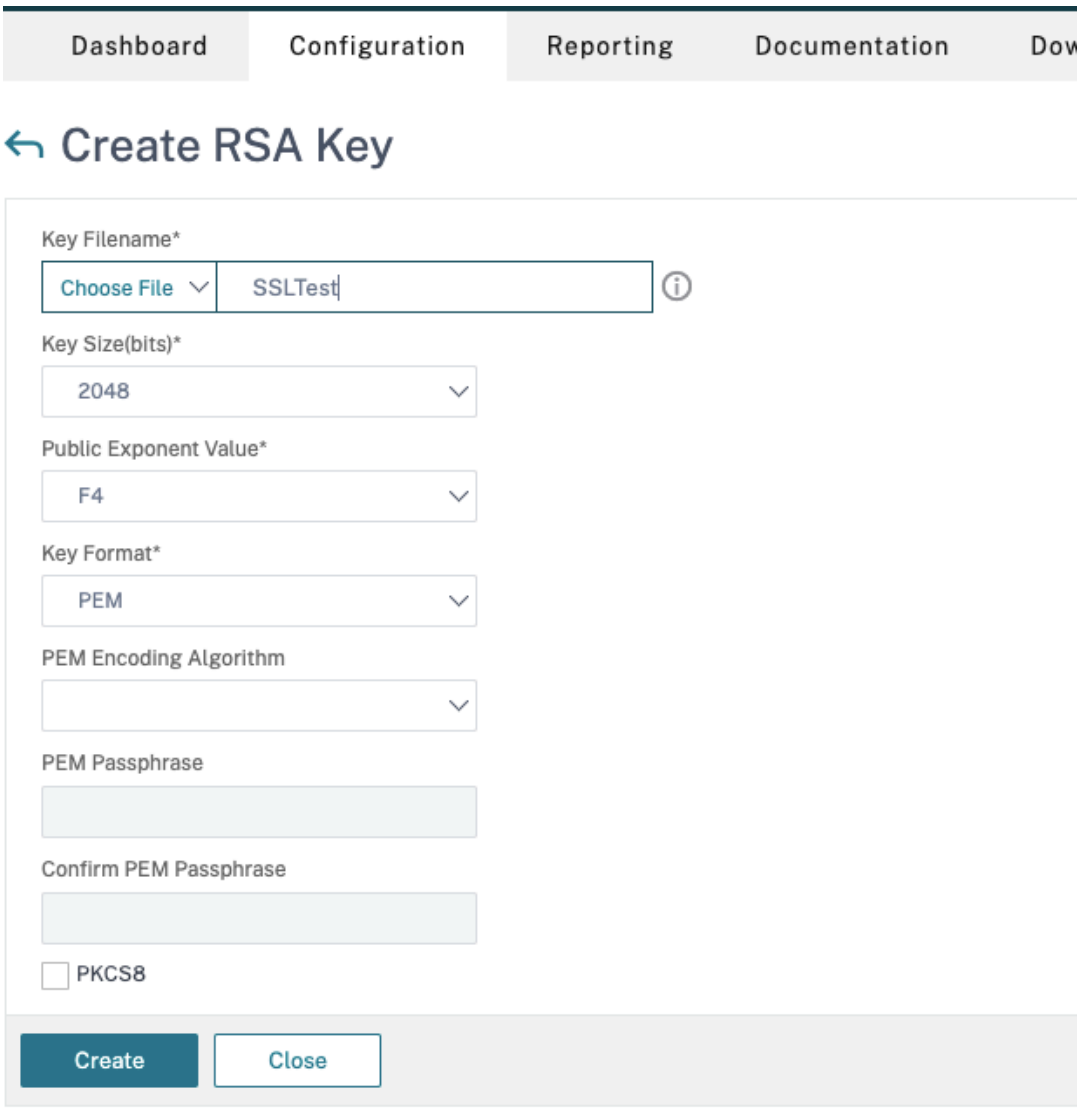

     - Indirizzo IP della subnet (SNIP) per abilitare la comunicazione tra l'appliance Citrix ADC e i server back-end. Per ulteriori informazioni, vedere Configurazione degli indirizzi IP delle subnet.
     - Indirizzo IP virtuale Citrix Gateway e indirizzo IP virtuale dell'unità di bilanciamento del carico per accedere all'appliance ADC per l'avvio della sessione. Per ulteriori informazioni, vedere Creare un server virtuale.



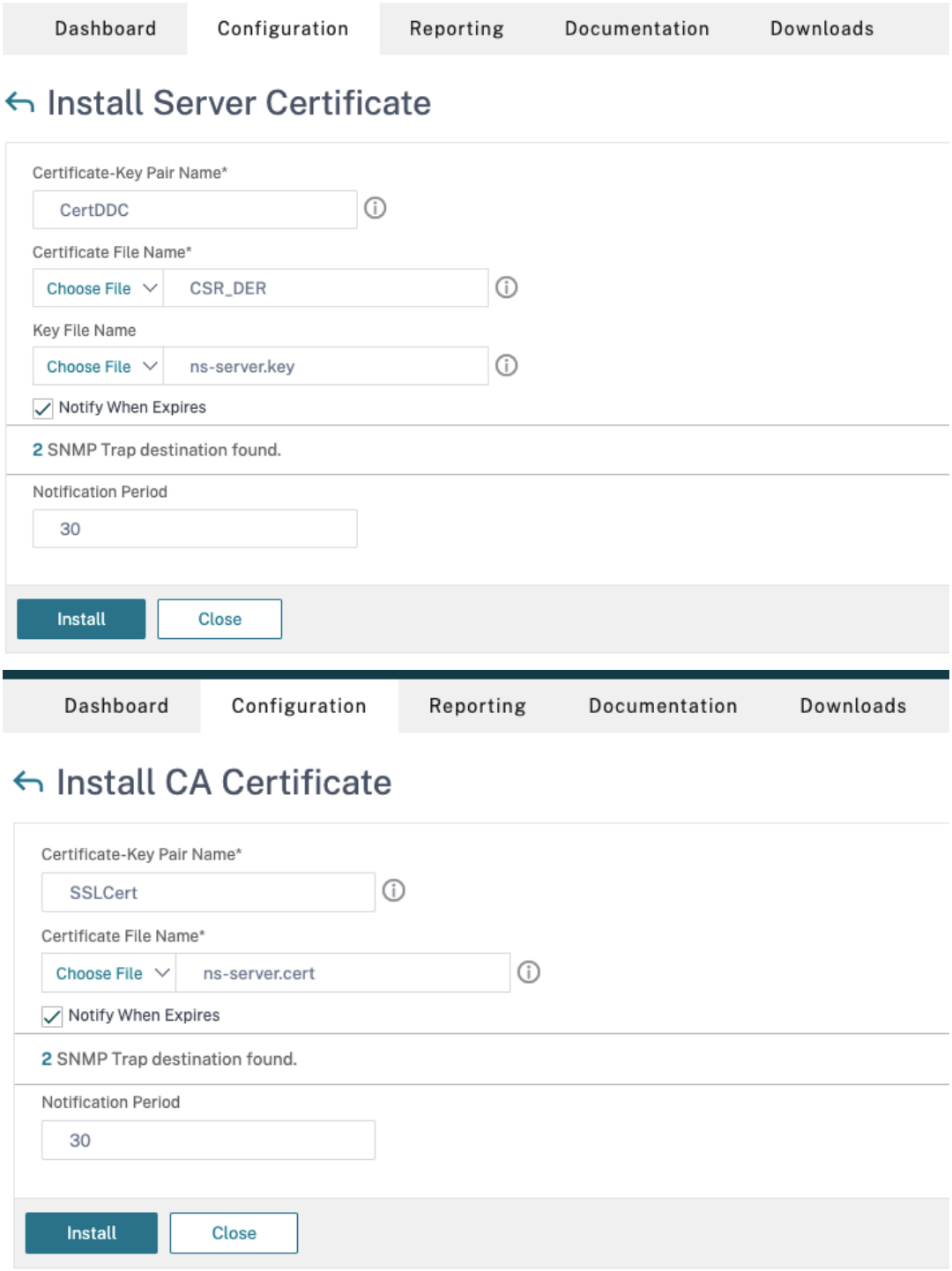

- Le modalità e le funzionalità richieste nell'appliance Citrix ADC sono abilitate.
  - Per abilitare le modalità, nella GUI di Citrix ADC andare a **System (Sistema) > Settings (Impostazioni) > Configure Mode (Configura modalità)**.
  - Per abilitare le funzionalità, nella GUI di Citrix ADC andare a **System (Sistema) > Settings (Impostazioni) > Configure Basic Features (Configura funzionalità di base)**.
- Le configurazioni relative ai certificati sono complete.
  - Viene creata la richiesta di firma del certificato (CSR). Per ulteriori informazioni, vedere Creare un certificato.



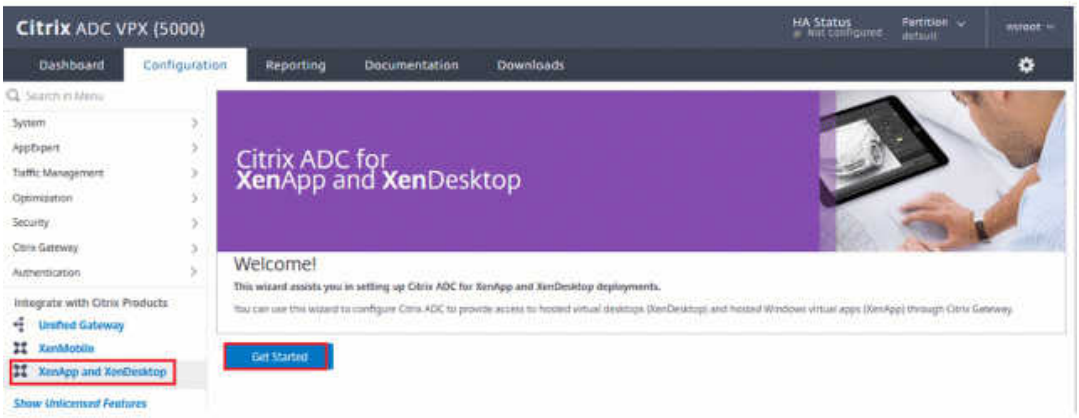

- I certificati del server e CA e i certificati radice sono installati. Per ulteriori informazioni, vedere Installazione, collegamento e aggiornamenti.



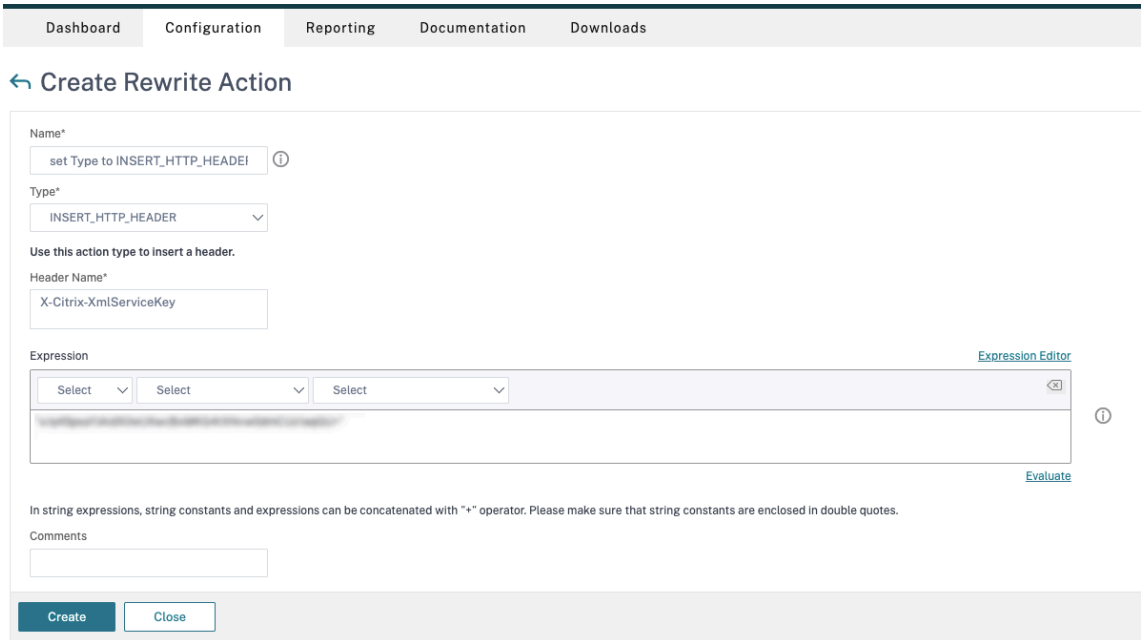

- È stato creato un Citrix Gateway per Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops). Verificare la connettività facendo clic sul pulsante **Test STA Connectivity** (Verifica connettività STA) per confermare che i server virtuali sono online. Per ulteriori informazioni, vedere Configurazione di Citrix ADC per Citrix Virtual Apps and Desktops.




2. Aggiungere un'azione di riscrittura. Per ulteriori informazioni, vedere Configurazione di un'azione di riscrittura.

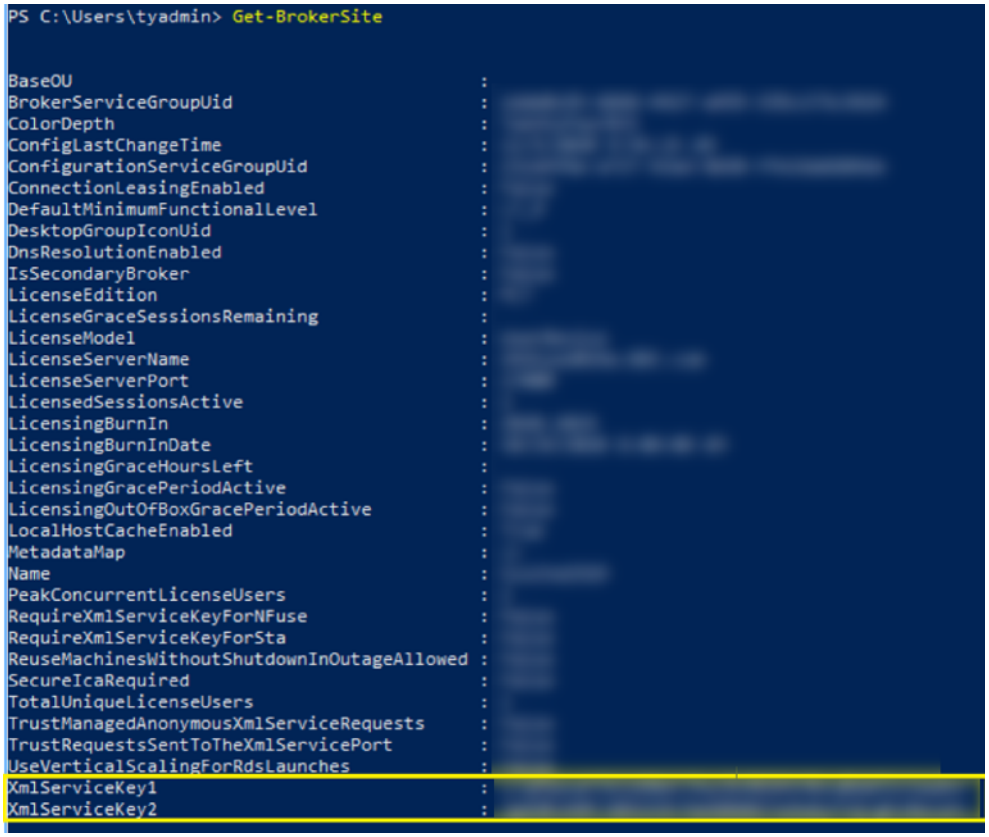
   a) Accedere ad **AppExpert > Rewrite (Riscrivi) > Actions (Azioni)**.
   b) Fare clic su **Add** (Aggiungi) per aggiungere una nuova azione di riscrittura. È possibile assegnare all'azione un nome come "set Type to INSERT_HTTP_HEADER"(imposta Tipo su INSERT_HTTP_HEADER).




   a) In **Type** (Tipo), selezionare **INSERT_HTTP_HEADER**.
   b) In **Header Name** (Nome intestazione), immettere X-Citrix-XmlServiceKey.

c) In **Expression** (Espressione), aggiungere <`XmlServiceKey1 value`> con le virgolette. È possibile copiare il valore XmlServiceKey1 dalla configurazione del Delivery Controller desktop.

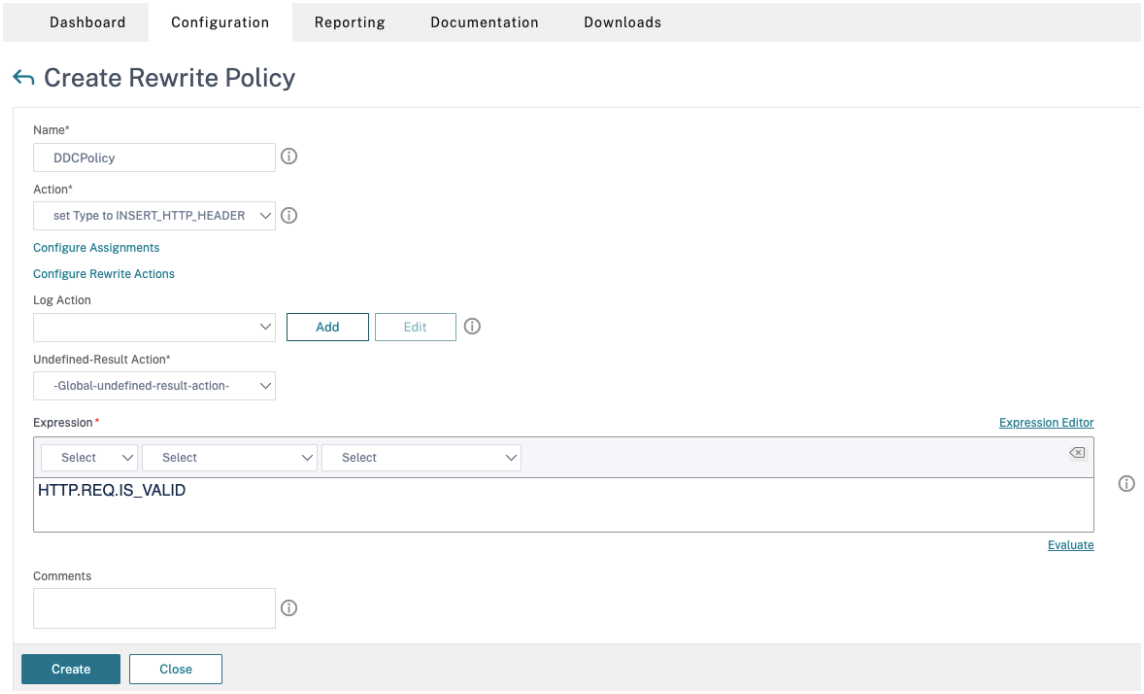



3. Aggiungere un criterio di riscrittura. Per ulteriori informazioni, vedere Configurazione di un criterio di riscrittura.

   a) Accedere ad **AppExpert > Rewrite (Riscrivi) > Policies (Criteri)**.

   b) Fare clic su **Add** (Aggiungi) per aggiungere un nuovo criterio.




a) In **Action** (Azione), selezionare l'azione creata nel passaggio precedente.
b) In **Expression** (Espressione), aggiungere HTTP.REQ.IS_VALID.
c) Fare clic su **OK**.

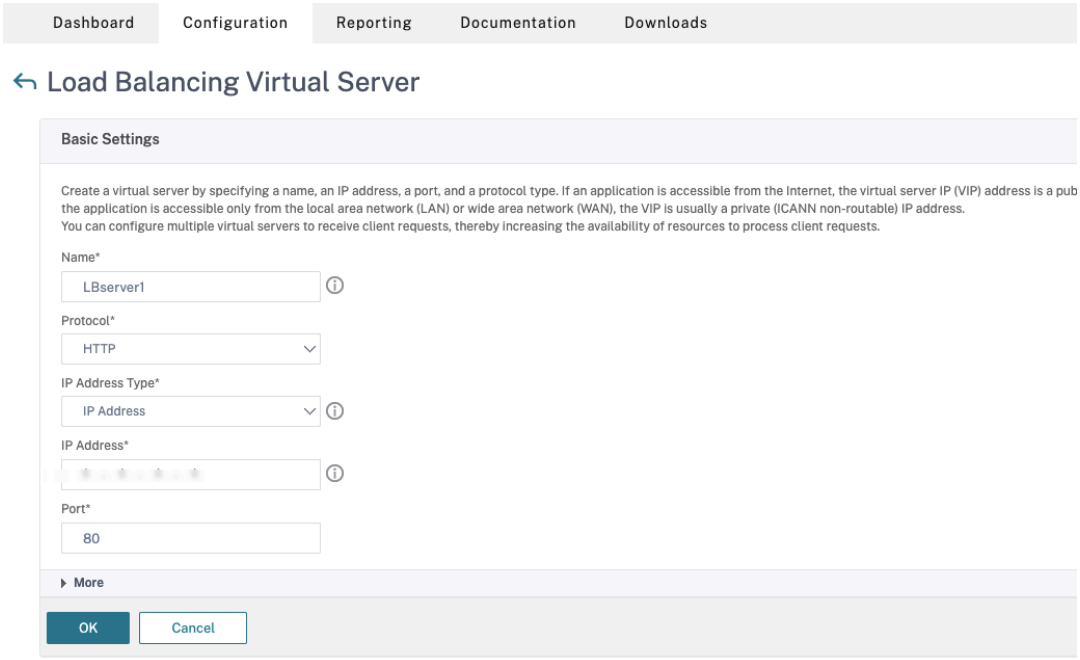
4. Impostare il bilanciamento del carico. È necessario configurare un server virtuale di bilanciamento del carico per ciascun server STA. In caso contrario, le sessioni non vengono avviate.

   Per ulteriori informazioni, vedere Impostare il bilanciamento del carico di base.

   a) Creare un server virtuale di bilanciamento del carico.

      - Andare a **Traffic Management (Gestione del traffico) > Load Balancing (Bilanciamento del carico) > Servers (Server)**.
      - Nella pagina **Virtual Servers** (Server virtuali), fare clic su **Add** (Aggiungi).

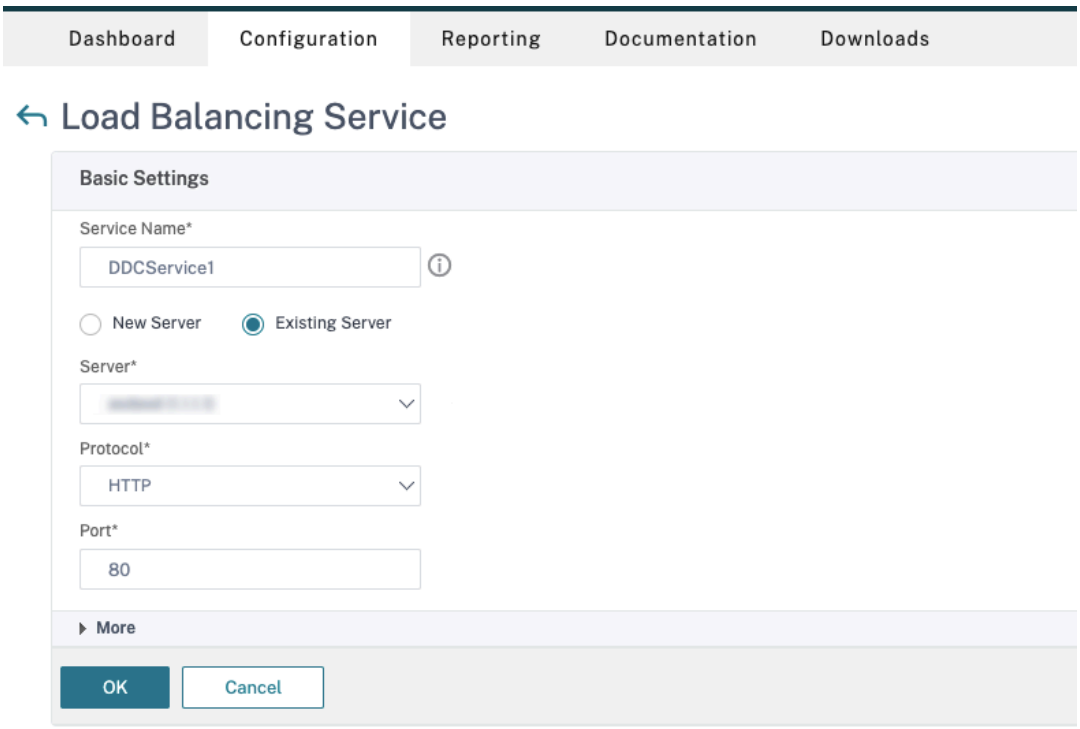



- In **Protocol** (Protocollo), selezionare **HTTP**.
- Aggiungere l'indirizzo IP virtuale di bilanciamento del carico e in **Port** (Porta) selezionare **80**.
- Fare clic su **OK**.

b) Creare un servizio di bilanciamento del carico.

- Andare a **Traffic Management (Gestione del traffico) > Load Balancing (Bilanciamento del carico) > Services (Servizi)**.

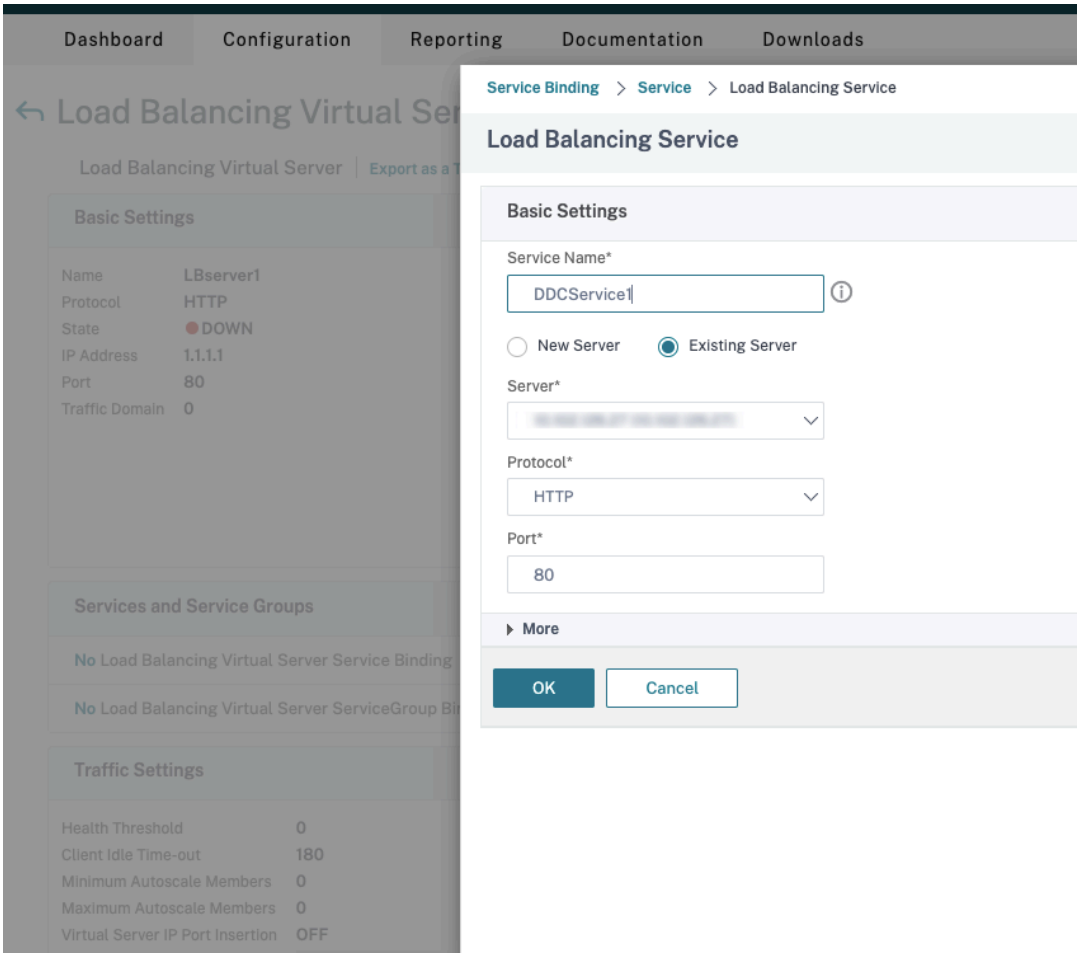



- In **Existing Server** (Server esistente), selezionare il server virtuale creato nel passaggio precedente.
- In **Protocol** (Protocollo), selezionare **HTTP** e in **Port** (Porta) selezionare **80**.
- Fare clic su **OK** e quindi su **Done** (Fine).

c) Associare il servizio al server virtuale.

- Selezionare il server virtuale creato in precedenza e fare clic su **Edit** (Modifica).
- In **Services and Service Groups** (Servizi e gruppi di servizi), fare clic su **No Load Balancing Virtual Server Service Binding** (Nessuna associazione del servizio del server virtuale con bilanciamento del carico).

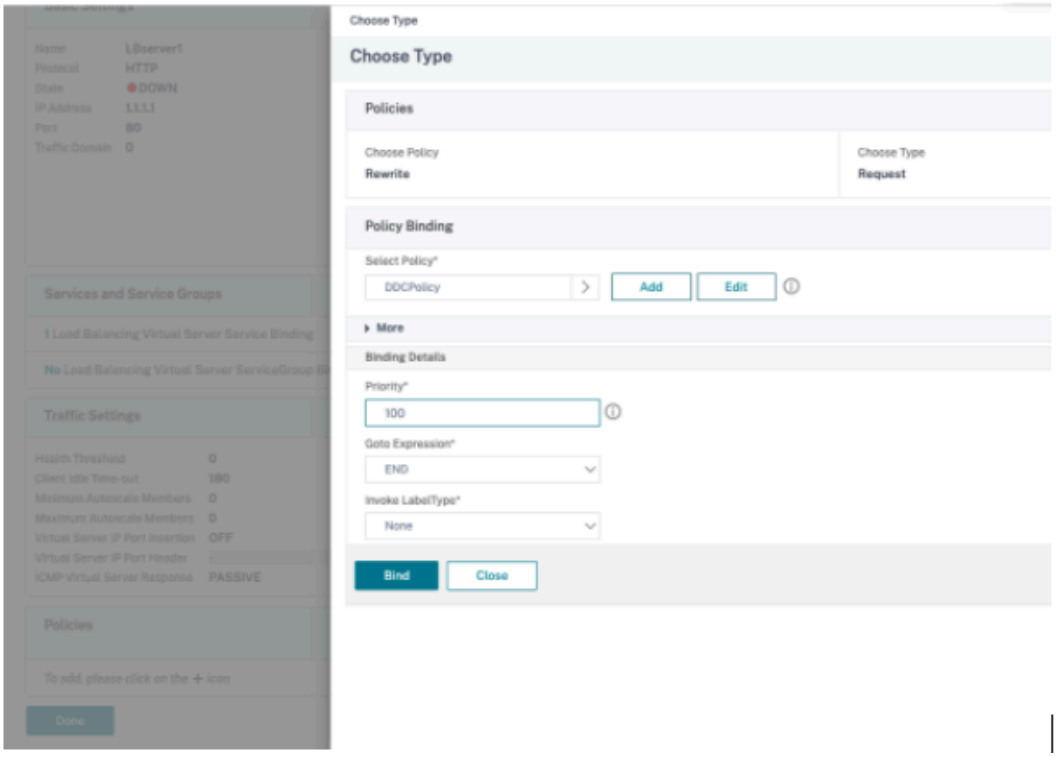



- In **Service Binding** (Associazione del servizio), selezionare Citrix DaaS creato in precedenza.
- Fare clic su **Bind** (Associa).

d) Associare il criterio di riscrittura creato in precedenza al server virtuale.

- Selezionare il server virtuale creato in precedenza e fare clic su **Edit** (Modifica).
- In **Advanced Settings** (Impostazioni avanzate), fare clic su **Policies** (Criteri), quindi nella sezione **Policies** (Criteri) fare clic su **+**.

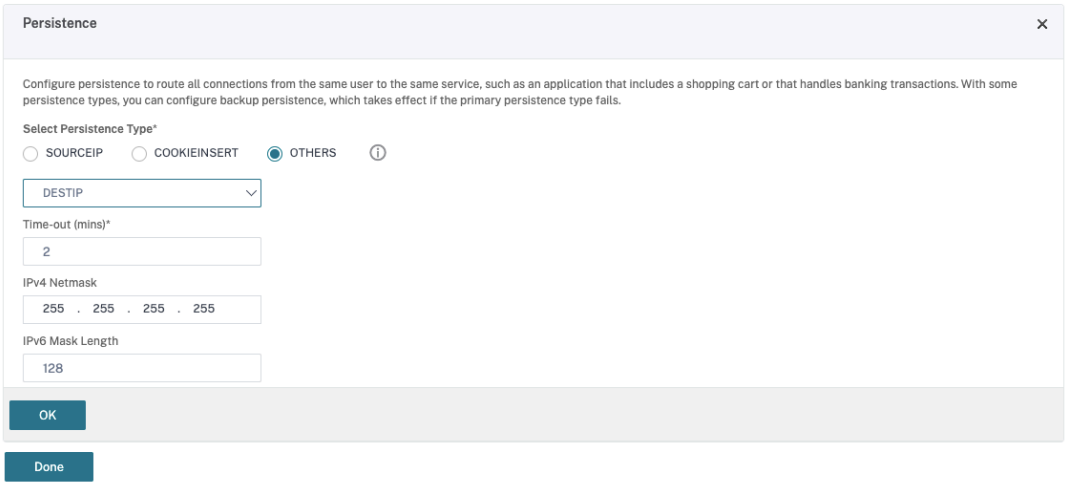



- In **Choose Policy** (Scegli criterio), selezionare **Rewrite** (Riscrivi) e in **Choose Type** (Scegli tipo) selezionare **Request** (Richiesta).
- Fare clic su **Continue** (Continua).
- In **Select Policy** (Seleziona criterio), selezionare il criterio di riscrittura creato in precedenza.
- Fare clic su **Bind** (Associa).
- Fare clic su **Done** (Fine).

e) Impostare la persistenza per il server virtuale, se necessario.

- Selezionare il server virtuale creato in precedenza e fare clic su **Edit** (Modifica).
- In **Advanced Settings** (Impostazioni avanzate), fare clic su **Persistence** (Persistenza).




- Selezionare il tipo di persistenza **Others** (Altro).
- Selezionare **DESTIP** per creare sessioni di persistenza in base all'indirizzo IP del servizio selezionato dal server virtuale (l'indirizzo IP di destinazione).
- In **IPv4 Netmask** (Netmask IPv4), aggiungere la stessa maschera di rete del DDC.
- Fare clic su **OK**.

f) Ripetere questi passaggi anche per l'altro server virtuale.

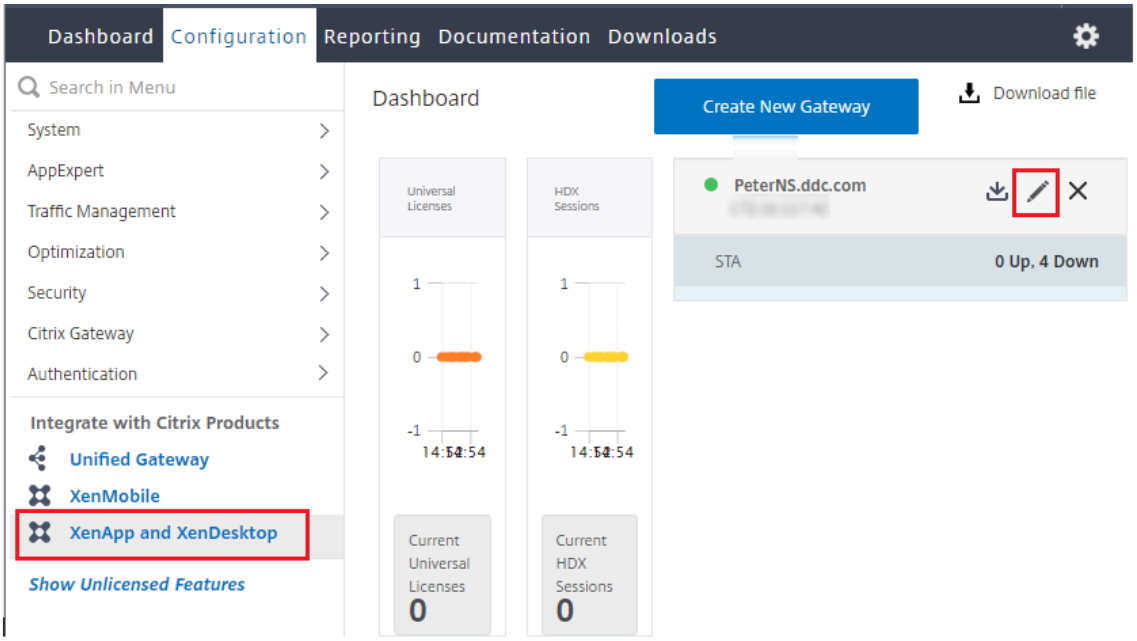
**La configurazione cambia se l'appliance Citrix ADC è già configurata con Citrix DaaS**

Se è già stata configurata l'appliance Citrix ADC con Citrix DaaS, per utilizzare la funzionalità Secure XML è necessario apportare le seguenti modifiche alla configurazione.

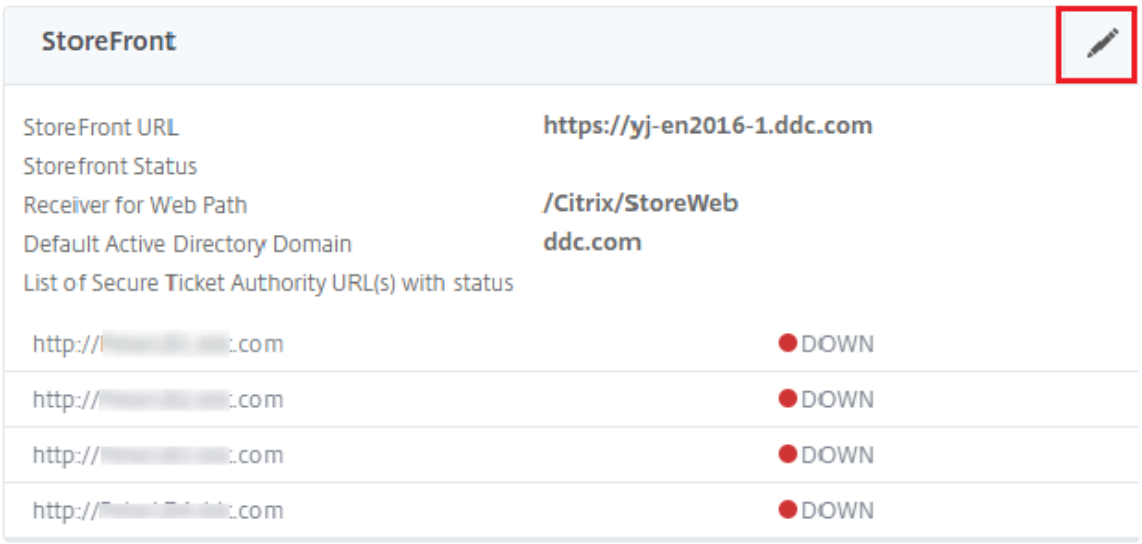
- Prima dell'avvio della sessione, modificare l'**URL Security Ticket Authority** del gateway per utilizzare i nomi di dominio completi dei server virtuali di bilanciamento del carico.
- Assicurarsi che il parametro `TrustRequestsSentToTheXmlServicePort` sia impostato su False. Per impostazione predefinita, il parametro `TrustRequestsSentToTheXmlServicePort` è impostato su False. Tuttavia, se il cliente ha già configurato Citrix ADC per Citrix DaaS, `TrustRequestsSentToTheXmlServicePort` è impostato su True.

1. Nella GUI di Citrix ADC, accedere a **Configuration (Configurazione) > Integrate with Citrix Products (Integra con i prodotti Citrix)** e fare clic su **XenApp and XenDesktop** (XenApp e XenDesktop).
2. Selezionare l'istanza del gateway e fare clic sull'icona di modifica.



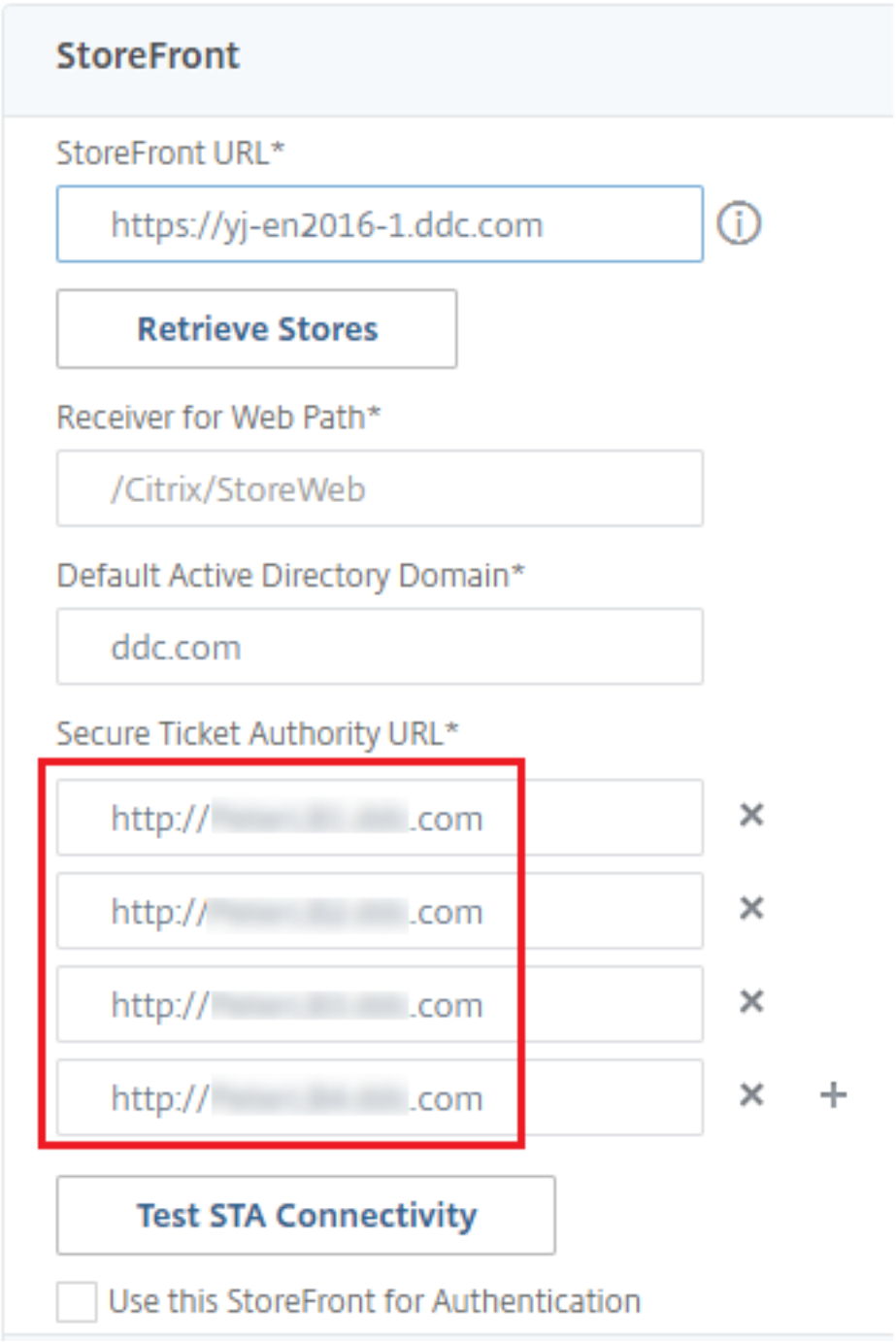

3. Nel riquadro StoreFront, fare clic sull'icona di modifica.




4. Aggiungere l'**URL Secure Ticket Authority**.

   - Se la funzionalità Secure XML è abilitata, l'URL STA deve essere l'URL del servizio di bilanciamento del carico.
   - Se la funzionalità Secure XML è disabilitata, l'URL STA deve essere l'URL di STA (indirizzo del DDC) e il parametro TrustRequestsSentToTheXmlServicePort sul DDC deve essere impostato su True.




## Sessioni

May 9, 2023

Mantenere l'attività della sessione è fondamentale per fornire la migliore esperienza utente. La

perdita di connettività dovuta a reti inaffidabili, latenza di rete altamente variabile e limitazioni di portata dei dispositivi wireless può essere frustrante per l'utente. La possibilità di spostarsi rapidamente tra una workstation e l'altra e di accedere allo stesso insieme di applicazioni ogni volta che accedono è una priorità per molti lavoratori mobili, come ad esempio gli operatori sanitari in un ospedale.

Le funzionalità descritte in questo articolo ottimizzano l'affidabilità delle sessioni, riducono gli inconvenienti, i tempi di inattività e la perdita di produttività; utilizzando queste funzionalità, gli utenti mobili possono spostarsi rapidamente e facilmente tra i dispositivi.

È inoltre possibile scollegare un utente da una sessione, disconnettere una sessione e configurare il prelancio e la permanenza della sessione; vedere Gestire i gruppi di consegna

## Affidabilità della sessione

Session Reliability (Affidabilità delle sessioni) mantiene attive le sessioni e le mantiene sullo schermo dell'utente quando la connettività di rete viene interrotta. Gli utenti continuano a visualizzare l'applicazione che stanno utilizzando fino al ripristino della connettività di rete.

Questa funzione è particolarmente utile per gli utenti mobili con connessioni wireless. Ad esempio, un utente con connessione wireless entra in una galleria ferroviaria e perde momentaneamente la connettività. Normalmente, la sessione viene disconnessa, scomparendo dallo schermo dell'utente e l'utente deve riconnettersi alla sessione disconnessa. Con la funzione di affidabilità della sessione, la sessione rimane attiva sulla macchina. Per indicare che la connettività è stata persa, lo schermo dell'utente si blocca e il cursore diventa una clessidra rotante fino a quando la connettività non riprende al termine della galleria. L'utente continua ad accedere allo schermo durante l'interruzione e può riprendere l'interazione con l'applicazione quando viene ripristinata la connessione di rete. La funzione di affidabilità della sessione riconnette gli utenti senza richieste di riautenticazione.

Gli utenti dell'app Citrix Workspace non possono ignorare l'impostazione del controller.

È possibile utilizzare la funzione di affidabilità della sessione con Transport Layer Security (TLS). TLS crittografa solo i dati inviati tra il dispositivo utente e Citrix Gateway.

Abilitare e configurare l'affidabilità della sessione con le seguenti impostazioni dei criteri:

- L'impostazione dei criteri di connessione per l'affidabilità della sessione consente o impedisce l'affidabilità della sessione.
- L'impostazione del criterio di timeout per l'affidabilità della sessione ha un valore predefinito di 180 secondi o tre minuti. Sebbene sia possibile estendere la quantità di tempo in cui l'affidabilità della sessione mantiene aperta una sessione, questa funzione è progettata per la comodità dell'utente e pertanto non richiede all'utente di eseguire nuovamente l'autenticazione. Più si prolunga il tempo in cui una sessione viene mantenuta aperta, più aumentano le probabilità

che un utente possa distrarsi e allontanarsi dal proprio dispositivo, lasciando potenzialmente la sessione accessibile a utenti non autorizzati.
- Le connessioni di affidabilità della sessione in entrata utilizzano la porta 2598, a meno che non si modifichi il numero di porta nell'impostazione del criterio del numero di porta di affidabilità della sessione.
- Se non si desidera che gli utenti siano in grado di riconnettersi alle sessioni interrotte senza dover eseguire nuovamente l'autenticazione, utilizzare la funzione di riconnessione automatica del client. È possibile configurare l'impostazione dei criteri di autenticazione di riconnessione automatica del client per richiedere agli utenti di riconnettersi nuovamente durante la riconnessione a sessioni interrotte.

Se si utilizza sia l'affidabilità della sessione che la riconnessione automatica del client, le due funzionalità funzionano in sequenza. L'affidabilità della sessione chiude (o disconnette) la sessione utente dopo il periodo di tempo specificato nell'impostazione del timeout dell'affidabilità della sessione. A quel punto avranno effetto le impostazioni di riconnessione automatica del client, che tentano di riconnettere l'utente alla sessione disconnessa.

### Riconnessione automatica del client

Con la funzione di riconnessione automatica del client, l'app Citrix Workspace è in grado di rilevare disconnessioni involontarie delle sessioni ICA e di ricollegare automaticamente gli utenti alle sessioni interessate. Quando questa funzione è abilitata sul server, gli utenti non devono riconnettersi manualmente per continuare a lavorare.

L'app Citrix Workspace tenta di riconnettersi alla sessione finché la connessione non viene ristabilita o fino a quando l'utente annulla i tentativi di riconnessione.

Per le sessioni desktop, l'app Citrix Workspace tenta di riconnettersi alla sessione per un intervallo di tempo specificato, se non nel caso in cui vi è una riconnessione corretta o l'utente annulla i tentativi di riconnessione. Per impostazione predefinita, questo intervallo di tempo è di cinque minuti. Per modificare questo intervallo di tempo, modificare questo registro sul dispositivo dell'utente:

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

dove `seconds` è il numero di secondi dopo i quali non vengono più effettuati tentativi di riconnessione alla sessione.

Abilitare e configurare la riconnessione automatica del client con le seguenti impostazioni dei criteri:

- **Auto client reconnect:** abilita o disabilita la riconnessione automatica tramite l'app Citrix Workspace dopo che una connessione è stata interrotta.

- **Auto client reconnect authentication:** abilita o disabilita l'obbligo di autenticazione utente dopo la riconnessione automatica.
- **Auto client reconnect logging:** abilita o disabilita la registrazione degli eventi di riconnessione nel registro eventi. La registrazione è disabilitata per impostazione predefinita. Quando la registrazione è abilitata, il log di sistema del server acquisisce informazioni sugli eventi di riconnessione automatica riusciti e non riusciti. Ogni server memorizza le informazioni sugli eventi di riconnessione nel proprio registro di sistema. Il sito non fornisce un registro combinato degli eventi di riconnessione per tutti i server.

La riconnessione automatica utente incorpora un meccanismo di autenticazione basato sulle credenziali utente crittografate. All'inizio, quando un utente accede, il server crittografa e memorizza le credenziali dell'utente e crea e invia un cookie contenente la chiave di crittografia all'app Citrix Workspace. L'app Citrix Workspace invia la chiave al server per la riconnessione. Il server decrittografa le credenziali e le invia all'accesso di Windows per l'autenticazione. Quando i cookie scadono, gli utenti devono autenticarsi nuovamente per riconnettersi alle sessioni.

I cookie non vengono utilizzati se si abilita l'impostazione di autenticazione della riconnessione automatica del client. Viene invece visualizzata una finestra di dialogo per gli utenti che richiedono le credenziali quando l'app Citrix Workspace tenta di riconnettersi automaticamente.

Per la massima protezione delle credenziali e delle sessioni utente, utilizzare la crittografia per tutte le comunicazioni tra i client e il sito.

Disabilitare la riconnessione automatica del client sull'app Citrix Workspace per Windows utilizzando il file icaclient.adm. Per ulteriori informazioni, vedere la documentazione dell'app Citrix Workspace per Windows.

Le impostazioni delle connessioni influiscono anche sulla riconnessione automatica del client:

- Per impostazione predefinita, la riconnessione automatica del client è abilitata tramite le impostazioni dei criteri a livello di sito, come descritto sopra. La riautenticazione dell'utente non è richiesta. Tuttavia, se la connessione TCP ICA di un server è configurata per reimpostare le sessioni quando si interrrompe un collegamento di comunicazione, la riconnessione automatica non avviene. La riconnessione automatica del client funziona solo se il server disconnette le sessioni quando è presente una connessione interrotta o scaduta. In questo contesto, la connessione TCP ICA fa riferimento alla porta virtuale di un server (anziché a un'effettiva connessione di rete) che viene utilizzata per le sessioni su reti TCP/IP.
- Per impostazione predefinita, la connessione TCP ICA su un server è impostata per disconnettere le sessioni in caso di connessioni interrotte o scadute. Le sessioni disconnesse rimangono intatte nella memoria di sistema e sono disponibili per la riconnessione tramite l'app Citrix Workspace.
- La connessione può essere configurata per ripristinare o disconnettere le sessioni con connessioni interrotte o scadute. Quando una sessione viene reimpostata, il tentativo di riconnessione

avvia una nuova sessione. Invece di riportare un utente nello stesso punto dell'applicazione in uso, l'applicazione viene riavviata.
- Se il server è configurato per reimpostare le sessioni, la riconnessione automatica del client crea una sessione. In questo processo gli utenti dovranno immettere le proprie credenziali per accedere al server.
- La riconnessione automatica può non riuscire se l'app Citrix Workspace o il plug-in inviano informazioni di autenticazione errate, problema che potrebbe verificarsi durante un attacco, o se il server determina che è trascorso troppo tempo da quando ha rilevato la connessione interrotta.

### ICA Kep-Alive

L'abilitazione della funzione ICA Keep-Alive impedisce la disconnessione delle connessioni interrotte. Se la funzione è abilitata, quando il server non rileva attività (ad esempio, nessun cambio di orologio, nessun movimento del mouse, nessun aggiornamento dello schermo), viene impedito a Servizi Desktop remoto di disconnettere la sessione. Il server invia pacchetti keep-alive ogni pochi secondi per rilevare se la sessione è attiva. Se la sessione non è più attiva, il server contrassegna la sessione come disconnessa.

> **Importante:**
>
> ICA Keep-Alive funziona solo se non si utilizza l'affidabilità della sessione. L'affidabilità della sessione ha i propri meccanismi per impedire la disconnessione delle connessioni interrotte. Configurare ICA Keep-Alive solo per le connessioni che non utilizzano l'affidabilità della sessione.

Le impostazioni ICA Keep-Alive sostituiscono le impostazioni keep-alive configurate in Criteri di gruppo Microsoft Windows.

Abilitare e configurare ICA Keep-Alive con le seguenti impostazioni dei criteri:

- **ICA keep-alive timeout:** (Timeout ICA keep-alive) specifica l'intervallo (1-3600 secondi) utilizzato per inviare messaggi ICA keep-alive. Non configurare questa opzione se si desidera che il software di monitoraggio della rete chiuda le connessioni inattive in ambienti in cui le connessioni interrotte sono così rare che consentire agli utenti di riconnettersi alle sessioni non è un problema.

  L'intervallo predefinito è 60 secondi: i pacchetti ICA Keep-Alive vengono inviati ai dispositivi utente ogni 60 secondi. Se un dispositivo utente non risponde in 60 secondi, lo stato delle sessioni ICA diventa disconnesso.
- **ICA keep alives:** invia o impedisce l'invio di messaggi ICA keep-alive.

### Controllo di Workspace

Il controllo di Workspace consente a desktop e applicazioni di seguire un utente da un dispositivo all'altro. Questa possibilità di roaming consente all'utente di accedere a tutti i desktop o di aprire le applicazioni da qualsiasi luogo semplicemente effettuando l'accesso, senza dover riavviare i desktop o le applicazioni su ciascun dispositivo. Ad esempio, il controllo dell'area di lavoro può aiutare gli operatori sanitari di un ospedale che devono spostarsi rapidamente tra diverse workstation e accedere allo stesso insieme di applicazioni a ogni accesso. Se si configurano le opzioni di controllo dell'area di lavoro per consentirlo, questi lavoratori possono disconnettersi da più applicazioni su un dispositivo client e quindi riconnettersi per aprire le stesse applicazioni su un dispositivo client diverso.

Il controllo dell'area di lavoro influisce sulle seguenti attività:

- **Accesso:** per impostazione predefinita, il controllo dell'area di lavoro consente agli utenti di riconnettersi automaticamente a tutti i desktop e le applicazioni in esecuzione durante l'accesso, senza doverli riaprire manualmente. Attraverso il controllo dell'area di lavoro, gli utenti possono aprire desktop o applicazioni disconnessi, oltre a quelli che sono attivi su un altro dispositivo client. La disconnessione da un desktop o da un'applicazione li lascia in esecuzione sul server. Se si hanno utenti in roaming che devono mantenere alcuni desktop o applicazioni in esecuzione su un dispositivo client mentre si riconnettono a un sottoinsieme dei loro desktop o applicazioni su un altro dispositivo client, è possibile configurare il comportamento di riconnessione di accesso per aprire solo i desktop o le applicazioni precedentemente disconnessi dall'utente.
- **Riconnessione:** dopo aver effettuato l'accesso al server, gli utenti possono riconnettersi a tutti i desktop o alle applicazioni in qualsiasi momento facendo clic su Riconnetti. Per impostazione predefinita, Reconnect apre i desktop o la applicazioni che sono disconnessi, oltre a quelli attualmente in esecuzione su un altro dispositivo client. È possibile configurare Reconnect per aprire solo i desktop o le applicazioni da cui l'utente si è disconnesso in precedenza.
- **Scollegamento:** per gli utenti che aprono desktop o applicazioni tramite StoreFront, è possibile configurare il comando Log Off perché scolleghi l'utente da StoreFront e da tutte le sessioni attive insieme o lo scolleghi solo da StoreFront.
- **Disconnessione:** gli utenti possono disconnettersi da tutti i desktop e le applicazioni in esecuzione contemporaneamente, senza dover disconnettersi da ciascuno individualmente.

Il controllo dell'area di lavoro è disponibile per gli utenti che accedono a desktop e applicazioni tramite una connessione Citrix StoreFront o tramite l'app Citrix Workspace. Per impostazione predefinita, il controllo dell'area di lavoro è disabilitato per le sessioni di desktop virtuale, ma è abilitato per le applicazioni in hosting. La condivisione delle sessioni non avviene per impostazione predefinita tra i desktop pubblicati e le applicazioni pubblicate in esecuzione all'interno di tali desktop.

I criteri utente, le mappature delle unità client e le configurazioni stampante cambiano come nec-

essario quando un utente si sposta su un nuovo dispositivo client. I criteri e le mappature vengono applicati nel modo corretto per il dispositivo client in cui l'utente ha effettuato l'accesso alla sessione. Ad esempio, se un operatore sanitario si scollega da un dispositivo client nel Pronto Soccorso di un ospedale e quindi accede a una workstation nel laboratorio radiologico dell'ospedale, i criteri, le mappature delle stampanti e le mappature delle unità client appropriate per la sessione nel laboratorio radiologico entrano in vigore all'avvio della sessione.

È possibile personalizzare la scelta delle stampanti visibili agli utenti quando cambiano posizione. È inoltre possibile controllare se gli utenti possono stampare su stampanti locali, quanta larghezza di banda viene consumata quando gli utenti si connettono in remoto e altri aspetti della loro esperienza di stampa.

Per informazioni sull'attivazione e la configurazione del controllo dell'area di lavoro per gli utenti, vedere la documentazione di StoreFront.

### Roaming di sessione

> **Nota:**
>
> Le seguenti informazioni guidano l'utente nella configurazione del roaming delle sessioni utilizzando PowerShell. È possibile anche utilizzare invece l'interfaccia di gestione di Full Configuration. Per ulteriori informazioni, vedere Gestire i gruppi di consegna.

Per impostazione predefinita, le sessioni sono in roaming fra i dispositivi client con l'utente. Quando l'utente avvia una sessione e si sposta su un altro dispositivo, viene utilizzata la stessa sessione e le applicazioni sono disponibili simultaneamente su entrambi i dispositivi. È possibile visualizzare le applicazioni su più dispositivi. Seguono le applicazioni, indipendentemente dal dispositivo o dall'esistenza di sessioni correnti. Spesso seguono anche stampanti e altre risorse assegnate all'applicazione.

Sebbene questo comportamento predefinito offra molti vantaggi, potrebbe non essere l'ideale in tutti i casi. È possibile impedire il roaming di sessione utilizzando PowerShell SDK.

Esempio 1: un professionista medico utilizza due dispositivi, un PC desktop su cui compila un modulo assicurativo e un tablet su cui esamina le informazioni sul paziente.

- Se il roaming di sessione è abilitato, entrambe le applicazioni vengono visualizzate su entrambi i dispositivi (un'applicazione avviata su un dispositivo è visibile su tutti i dispositivi in uso). Ciò potrebbe non soddisfare i requisiti di sicurezza.
- Se il roaming di sessione è disabilitato, il registro paziente non viene visualizzato sul PC desktop e il modulo assicurativo non viene visualizzato sul tablet.

Esempio 2: un responsabile della produzione lancia un'applicazione sul PC nel suo ufficio. Il nome e la posizione del dispositivo determinano quali stampanti e altre risorse sono disponibili per quella

sessione. Più tardi, si reca in un ufficio nell'edificio accanto per una riunione che gli richiederà l'uso di una stampante.

- Se il roaming di sessione è abilitato, il responsabile della produzione probabilmente non sarebbe in grado di accedere alle stampanti più vicine alla sala riunioni, perché le applicazioni lanciate in precedenza nel suo ufficio hanno determinato l'assegnazione di stampanti e altre risorse vicino a quella posizione.
- Se il roaming di sessione è disabilitato e accede a un altro computer (utilizzando le stesse credenziali), viene avviata una nuova sessione e le stampanti e le risorse che si trovano nelle vicinanze sono disponibili.

#### Configurare il roaming di sessione

Per configurare il roaming di sessione, utilizzare i cmdlet delle regole dei criteri di autorizzazione riportati di seguito con la proprietà "SessionReconnection". Facoltativamente, è anche possibile specificare la proprietà "LeasingBehavior".

Per le sessioni di desktop:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Per le sessioni delle applicazioni:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Dove `value` può essere uno dei valori seguenti:

- **Always** (Sempre): le sessioni sono sempre in roaming, indipendentemente dal dispositivo client e dal fatto che la sessione sia connessa o disconnessa. Questo è il valore predefinito.
- **DisconnectedOnly** (Solo disconnnesse): riconnettersi solo alle sessioni già disconnesse; in caso contrario, avviare una nuova sessione Le sessioni possono eseguire il roaming tra i dispositivi client prima disconnettendoli o utilizzando il controllo dell'area di lavoro per eseguire il roaming esplicitamente. Non viene mai utilizzata una sessione attiva connessa da un altro dispositivo client. Viene invece lanciata una nuova sessione.
- **SameEndpointOnly** (Solo stesso endpoint): un utente riceve una sessione univoca per ciascun dispositivo client che utilizza. Questo disabilita completamente il roaming. Gli utenti possono riconnettersi solo allo stesso dispositivo utilizzato in precedenza nella sessione.

La proprietà "LeasingBehavior"è descritta di seguito.

**Effetti di altre impostazioni:**

La disattivazione del roaming di sessione è influenzata dal limite dell'applicazione "Allow only one instance of the application per user"(Consenti solo un'istanza dell'applicazione per utente) impostato nelle proprietà dell'applicazione nel gruppo di consegna.

- Se si disabilità il roaming di sessione, disabilitare il limite di applicazione "Allow only one instance…".
- Se si abilita il limite di applicazione "Allow only one instance…", non configurare nessuno dei due valori che consentono nuove sessioni su nuovi dispositivi.

### Intervallo di accesso

Se una macchina virtuale contenente un VDA desktop si chiude prima del completamento del processo di accesso, è possibile assegnare più tempo al processo. Il valore predefinito per la versione 7.6 e le successive è 180 secondi (il valore predefinito per le versioni 7.0-7.5 è 90 secondi).

Sul computer (o sull'immagine master utilizzata in un catalogo di macchine), impostare la seguente chiave di registro:

Chiave: `HKLM\SOFTWARE\Citrix\PortICA`

- Valore: `AutoLogonTimeout`
- Tipo: `DWORD`
- Specificare un tempo decimale in secondi, nell'intervallo 0-3600.

Se si modifica l'immagine master, distribuire la nuova immagine nel catalogo. Per ulteriori informazioni, vedere Cambiare l'immagine master.

Questa impostazione si applica solo alle macchine virtuali con VDA desktop (workstation) a sessione singola. Microsoft controlla il timeout di accesso sulle macchine con server VDA multisessione.

## Tag

November 21, 2023

### Introduzione

I tag sono stringhe che identificano elementi come macchine, applicazioni, desktop, gruppi di consegna, gruppi di applicazioni e criteri. Dopo aver creato un tag e averlo aggiunto a un elemento, è possibile personalizzare determinate operazioni per applicarle solo agli elementi che hanno un tag specificato.

- La ricerca su misura viene visualizzata nell'interfaccia di gestione Full Configuration.

  Ad esempio, per visualizzare solo le applicazioni ottimizzate per i tester, creare un tag denominato "test"e quindi aggiungerlo (applicarlo) a tali applicazioni. A quel punto è possibile filtrare la ricerca con il tag "test".

- Pubblicare applicazioni da un gruppo di applicazioni o desktop specifici da un gruppo di consegna, considerando solo un sottoinsieme di macchine in gruppi di consegna selezionati. Questa funzionalità è denominata *restrizione tag*.

  Con le restrizioni tag, è possibile utilizzare le macchine esistenti per più di un'attività di pubblicazione, risparmiando i costi associati alla distribuzione e alla gestione di macchine aggiuntive. Una restrizione tag può essere spiegata come una suddivisione (o la creazione di partizioni) delle macchine che fanno parte di un gruppo di consegna. La sua funzionalità è simile, ma non identica, ai gruppi di lavoro nelle versioni di XenApp precedenti alla 7.x.

  L'utilizzo di un gruppo di applicazioni o di desktop con una restrizione tag può essere utile per isolare e risolvere i problemi di un sottoinsieme di macchine in un gruppo di consegna.

  I dettagli e gli esempi d'uso di una restrizione tag sono descritti più avanti in questo articolo.

- Pianificare riavvii periodici per un sottoinsieme di macchine inclusi in un gruppo di consegna.

  L'utilizzo di una restrizione di tag per le macchine consente di utilizzare nuovi cmdlet PowerShell per configurare più pianificazioni di riavvio per sottoinsiemi di macchine inclusi in un gruppo di consegna. Per esempi e dettagli, vedere Gestire i gruppi di consegna.

- Personalizza l'applicazione (assegnazione) dei criteri Citrix in base alle macchine in gruppi di consegna, tipi di gruppo di consegna o OU che hanno (o non hanno) un tag specificato.

  Ad esempio, se si desidera applicare un criterio Citrix solo alle workstation più potenti, aggiungere un tag denominato "high power"a tali macchine. Quindi, nella pagina **Assign Policy** (Assegna criterio) della creazione guidata criteri, selezionare il tag e la casella di controllo **Enable** (Abilita). È inoltre possibile aggiungere un tag a un gruppo di consegna e quindi applicare un criterio Citrix a tale gruppo. Per i dettagli, vedere Creare criteri.

È possibile applicare tag a:

- Macchine
- Applicazioni
- Cataloghi di macchine
- Gruppi di consegna
- Gruppi di applicazioni

È possibile configurare una restrizione tag durante la creazione o la modifica di quanto segue nell'interfaccia di gestione Full Configuration:

- Un desktop in un gruppo di consegna condiviso

- Un gruppo di applicazioni

### Restrizioni tag per un desktop o un gruppo di applicazioni

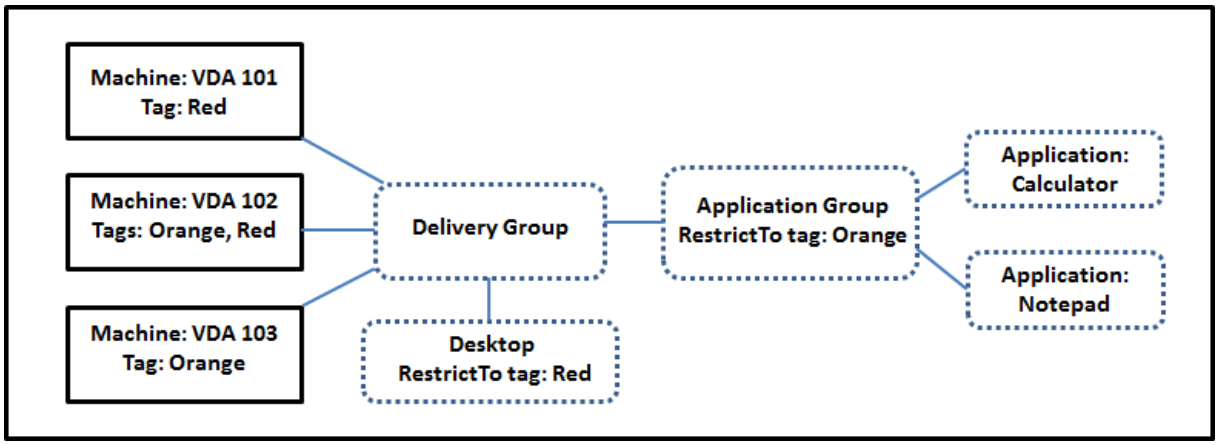
Una restrizione tag prevede diversi passaggi:

- Creare il tag e aggiungerlo (applicarlo) alle macchine.
- Creare o modificare un gruppo con la restrizione tag (in altre parole, limitare i lanci alle macchine con tag *x*).

Una restrizione tag estende il processo di selezione della macchina del Controller. Il Controller seleziona una macchina da un gruppo di consegna associato soggetto a criteri di accesso, a elenchi di utenti configurati, a preferenze di zona e a prontezza di avvio, oltre alla limitazione di tag (se presente). Per le applicazioni, il Controller torna ad altri gruppi di consegna in ordine di priorità, applicando le stesse regole di selezione delle macchine per ciascun gruppo di consegna considerato.

#### Esempio 1: layout semplice

Questo esempio presenta un semplice layout che utilizza restrizioni di tag per limitare le macchine che vengono considerate per l'avvio di alcuni desktop e applicazioni. Esiste un gruppo di consegna condiviso, un desktop pubblicato e un gruppo di applicazioni configurato con due applicazioni.




- Sono stati aggiunti tag a ciascuna delle tre macchine (VDA 101-103).
- Il desktop del gruppo di consegna è stato creato con una restrizione tag denominata `Red`. In questo modo quel desktop può essere lanciato solo su macchine di quel gruppo di consegna che hanno il tag `Red`: VDA 101 e 102.
- Il gruppo di applicazioni è stato creato con la restrizione tag `Orange`. Ciascuna delle sue applicazioni (`Calculator` e `Notepad`) viene lanciata solo su macchine che fanno parte di quel gruppo di consegna e che hanno il tag `Orange`: VDA 102 e 103.

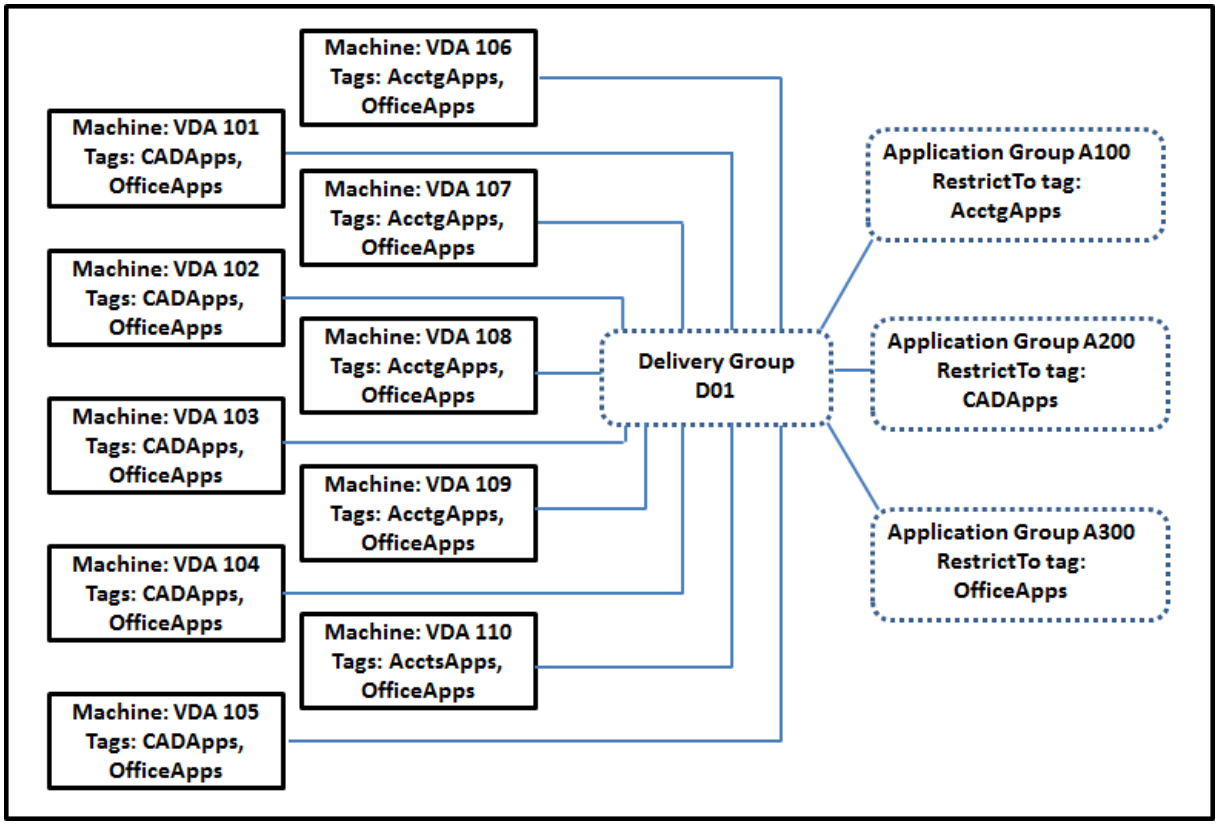
 

La macchina VDA 102 ha entrambi i tag (`Red` e `Orange`), quindi può essere presa in considerazione per l'avvio delle applicazioni e del desktop.

#### Esempio 2: layout più complesso

Questo esempio contiene diversi gruppi di applicazioni creati con restrizioni tag. Ciò si traduce nella capacità di fornire più applicazioni con meno macchine di quante sarebbero altrimenti necessarie se si utilizzassero solo gruppi di consegna.

Come configurare l'esempio 2 mostra i passaggi utilizzati per creare e applicare i tag, quindi configurare le restrizioni tag in questo esempio.




Questo esempio utilizza 10 macchine (VDA 101-110), un gruppo di consegna (`D01`) e tre gruppi di applicazioni (`A100`, `A200`, `A300`). Applicando tag a ciascuna macchina e specificando le restrizioni tag durante la creazione di ciascun gruppo di applicazioni:

- Gli utenti contabili del gruppo possono accedere alle app di cui hanno bisogno su cinque macchine (VDA 101—105)
- I progettisti CAD del gruppo possono accedere alle app di cui hanno bisogno su cinque macchine (VDA 106-110)
- Gli utenti del gruppo che necessitano di applicazioni Office possono accedere alle app Office su 10 computer (VDA 101-110)

Vengono utilizzate solo 10 macchine, con un solo gruppo di consegna. L'utilizzo dei gruppi di consegna da soli (senza gruppi di applicazioni) richiederebbe un numero doppio di macchine, poiché una macchina può appartenere a un solo gruppo di consegna.

## Gestire i tag e le restrizioni tag

I tag vengono creati, aggiunti (applicati), modificati ed eliminati dagli elementi selezionati tramite l'azione **Manage Tags** nell'interfaccia di gestione Full Configuration.

Eccezione: i tag utilizzati per le assegnazioni dei criteri vengono creati, modificati ed eliminati tramite l'azione **Manage Tags**. Tuttavia, si applicano (assegnano) tag quando si crea il criterio. Vedere Creare criteri per i dettagli.

Le restrizioni tag vengono configurate quando si creano o modificano desktop nei gruppi di consegna e quando si creano e modificano gruppi di applicazioni.

### Usare la funzione di gestione tag

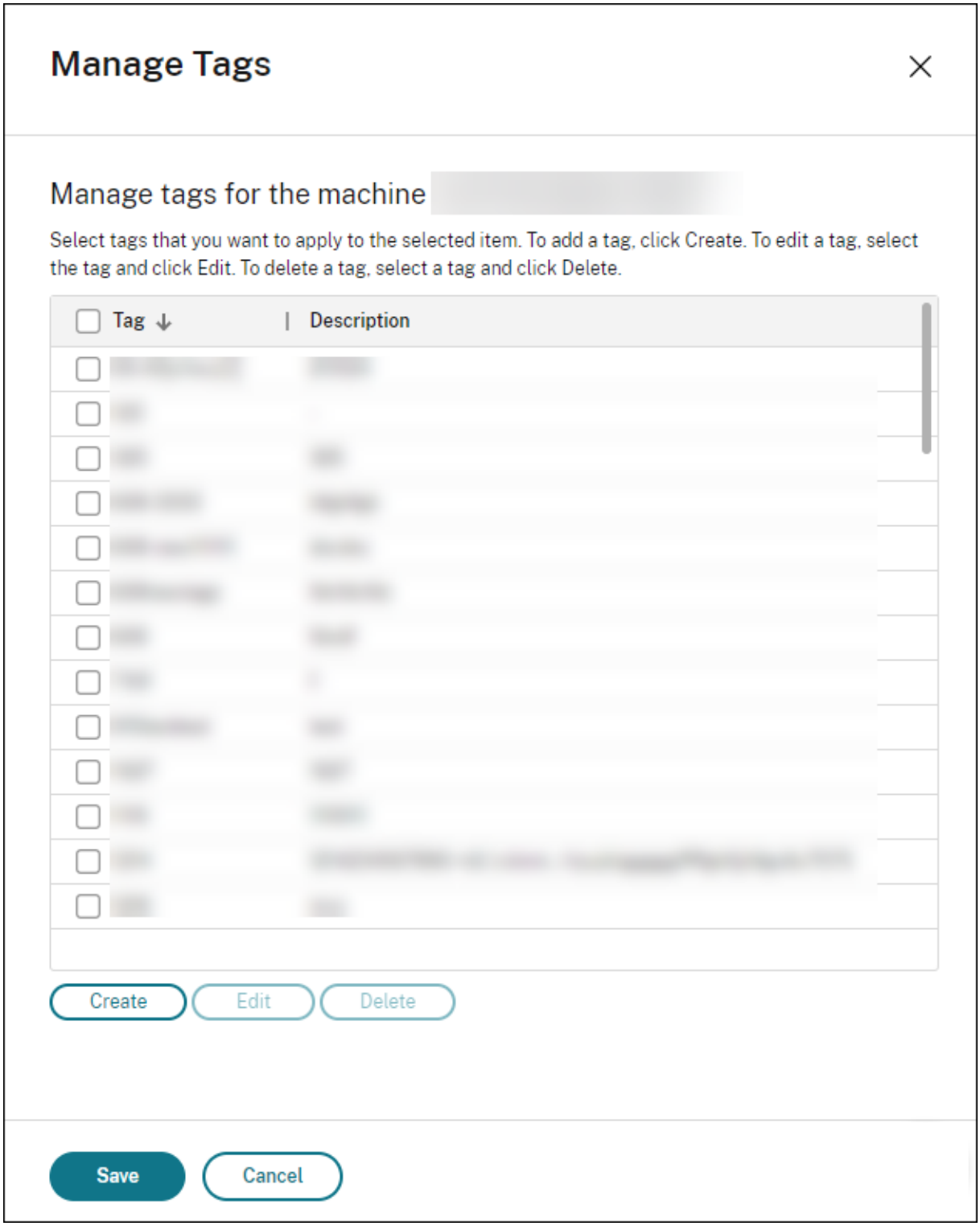
Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare gli elementi a cui si desidera applicare un tag. Gli elementi includono:

- Una o più macchine
- Una o più applicazioni
- Un desktop, un gruppo di consegna o un gruppo di applicazioni
- Un catalogo di macchine

Selezionare **Manage Tags** (Gestisci tag) nella barra delle azioni. Nella finestra di dialogo **Manage Tags** sono elencati tutti i tag esistenti, non solo quelli relativi agli elementi selezionati.

- Una casella di controllo abilitata indica che il tag è già stato aggiunto agli elementi selezionati. Nell'acquisizione dello schermo sottostante, alla macchina selezionata viene applicato un tag denominato "Tag1".
- Se vengono selezionati più elementi, una casella di controllo contenente un trattino indica che alcuni, ma non tutti gli elementi selezionati, hanno aggiunto quel tag.




Le seguenti azioni sono disponibili nella finestra di dialogo **Manage Tags** . Leggere Avvertenze per quando si lavora con i tag.

- **Per creare un tag:**

Selezionare **Create**. Immettere un nome e una descrizione. I nomi dei tag devono essere univoci e non fanno distinzione tra maiuscole e minuscole Quindi selezionare **Save** (Salva).

La creazione di un tag non lo applica automaticamente agli elementi selezionati. Utilizzare le caselle di controllo per applicare il tag.

- **Per aggiungere (applicare) uno o più tag:**

  Abilitare la casella di controllo accanto al nome del tag. Una casella di controllo contenente un trattino indica che ad alcuni, ma non a tutti gli elementi selezionati, è già stato applicato quel tag. Quando si selezionano più elementi e la casella di controllo di un tag ha un trattino, la modifica in un segno di spunta riguarda tutte le macchine selezionate.

  Se si tenta di aggiungere un tag a delle macchine e tale tag viene utilizzato come restrizione in un gruppo di applicazioni, tale azione può rendere tali macchine disponibili per l'avvio. Se è quello che si intendeva fare, procedere.

- **Per rimuovere uno o più tag:**

  Deselezionare la casella di controllo accanto al nome del tag. Una casella di controllo contenente un trattino indica che ad alcuni, ma non a tutti gli elementi selezionati, è già stato applicato quel tag. Quando si selezionano più elementi e la casella di controllo di un tag contiene un trattino, la deselezione della casella di controllo rimuove il tag da tutte le macchine selezionate.

  Se si tenta di rimuovere una restrizione di tag da una macchina, si viene avvertiti che l'azione può influire sulle macchine considerate per il lancio. Se è quello che si intendeva fare, procedere.

- **Per modificare un tag:**

  Selezionare un tag e selezionare **Edit**. Immettere un nuovo nome, una descrizione o entrambi. È possibile modificare solo un tag alla volta.

- **Per eliminare uno o più tag:**

  Selezionare i tag e selezionare **Delete**. La finestra di dialogo **Delete Tag** indica quanti elementi utilizzano attualmente i tag selezionati (ad esempio "2 macchine"). Selezionare un elemento per visualizzare ulteriori informazioni (ad esempio i nomi delle due macchine a cui è applicato il tag). Confermare se si desidera eliminare i tag.

  Non è possibile eliminare un tag utilizzato come restrizione. Innanzitutto, modificare il gruppo di applicazioni e rimuovere la restrizione tag o selezionare un tag diverso.

Quando si è finito di utilizzare la finestra di dialogo **Manage Tags**, selezionare **Save**.

Per verificare se a una macchina sono stati applicati dei tag: selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro di sinistra. Selezionare un gruppo di consegna, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni. Selezionare una macchina e quindi selezionare la scheda **Tags** nel riquadro **Details**.

### Gestire le restrizioni tag

La configurazione di una restrizione tag è un processo in più passaggi: prima si crea il tag e lo si aggiunge/applica alle macchine. Quindi, si aggiunge la restrizione al gruppo di applicazioni o al desktop.

- **Creare e applicare il tag:**

  Creare il tag e quindi aggiungerlo (applicarlo) alle macchine interessate dalla restrizione tag, utilizzando le azioni disponibili in **Manage Tags**.

- **Per aggiungere una restrizione tag a un gruppo di applicazioni:**

  Creare o modificare il gruppo di applicazioni. Nella pagina **Delivery Groups**, selezionare **Restrict launches to machines with the tag** (Limita avvii alle macchine con il tag) e quindi selezionare il tag dall'elenco.

- **Per modificare o rimuovere la restrizione tag relativa a un gruppo di applicazioni:**

  Modificare il gruppo. Nella pagina **Delivery Groups** selezionare un tag diverso dall'elenco o rimuovere completamente la restrizione tag deselezionando **Restrict launches to machines with the tag**.

- **Per aggiungere una restrizione tag a un desktop:**

  Creare o modificare un gruppo di consegna. Selezionare **Add** o **Edit** nella pagina **Desktop**. Nella finestra di dialogo **Add Desktop** (Aggiungi desktop), selezionare **Restrict launches to machines with the tag** (Limita avvii alle macchine con il tag) e quindi selezionare il tag dal menu.

- **Per modificare o rimuovere la limitazione tag relativa a un gruppo di consegna:**

  Modificare il gruppo. Nella pagina **Desktop**, selezionare **Edit**. Nella finestra di dialogo selezionare un tag diverso dall'elenco o rimuovere completamente la restrizione tag deselezionando **Restrict launches to machines with the tag**.

### Avvertenze per quando si lavora con i tag

Un tag applicato a un elemento può essere utilizzato per scopi diversi. Tenere quindi presente che l'aggiunta, la rimozione e l'eliminazione di un tag può avere effetti non voluti. È possibile utilizzare un tag per ordinare le visualizzazioni delle macchine quando si utilizza la ricerca nell'interfaccia di gestione Full Configuration. È possibile utilizzare lo stesso tag di una restrizione durante la configurazione di un gruppo di applicazioni o di un desktop. Tale azione limita le macchine prese in considerazione per l'avvio solo a quelle di gruppi di consegna specificati che hanno quel tag.

Se si aggiunge un tag alle macchine dopo che quel tag è stato configurato come restrizione tag per un desktop o un gruppo di applicazioni, si viene avvisati che ciò potrebbe rendere i computer disponibili per l'avvio di più applicazioni o desktop. Se è quello che si intendeva fare, procedere. In caso contrario, annullare l'operazione.

Ad esempio, supponiamo che si crei un gruppo di applicazioni con la restrizione tag Red. Successivamente, si aggiungono diverse altre macchine negli stessi gruppi di consegna utilizzati da quel gruppo di applicazioni. Se poi si tenta di aggiungere il tag Red a tali macchine, viene visualizzato un messaggio simile al seguente: "The tag Red is used as a restriction on the following application groups. L'aggiunta di questo tag potrebbe rendere le macchine selezionate disponibili all'avvio delle applicazioni di questo gruppo di applicazioni."È quindi possibile confermare o annullare l'aggiunta di quel tag a quelle macchine aggiuntive.

Analogamente, quando un tag viene utilizzato in un gruppo di applicazioni per limitare gli avvii, non è possibile eliminare il tag finché non si modifica il gruppo rimuovendo il tag come restrizione. Se è stato consentito eliminare quel tag, ciò potrebbe comportare l'avvio delle applicazioni su tutti i computer inclusi nei gruppi di consegna associati al gruppo di applicazioni. Lo stesso divieto di eliminare un tag si applica se il tag viene utilizzato come restrizione per gli avvii di desktop. Dopo aver modificato il gruppo di applicazioni o i desktop del gruppo di consegna per rimuovere la restrizione tag, è possibile eliminare il tag.

Le macchine potrebbero non avere tutte lo stesso insieme di applicazioni. Un utente può appartenere a più di un gruppo di applicazioni, ognuno con una restrizione tag diversa e insiemi di computer diversi o sovrapposti inclusi in gruppi di consegna. La tabella seguente elenca come viene deciso quali macchine prendere in considerazione.

| **Quando è stata aggiunta un'applicazione a** | **Queste macchine incluse nei gruppi di consegna selezionati sono prese in considerazione per l'avvio.** |
|---|---|
| Un gruppo di applicazioni senza restrizioni tag | Qualsiasi macchina. |
| Un gruppo di applicazioni con restrizione tag A | Macchine a cui è applicato il tag A. |
| Due gruppi di applicazioni, uno con restrizione tag A e l'altro con restrizione tag B | Macchine con tag A e tag B. Se non ne è disponibile nessuna, le macchine con tag A o tag B. |
| Due gruppi di applicazioni, uno con restrizione tag A e l'altro senza restrizioni tag | Macchine che hanno il tag A. Se non ne è disponibile nessuna, allora qualsiasi macchina. |

Se si è utilizzata una restrizione tag in una pianificazione di riavvio del computer, eventuali modifiche apportate che influiscono sulle applicazioni di tag o sulle restrizioni influiscono sul successivo ciclo di riavvio del computer. Non influisce sui cicli di riavvio in corso durante le modifiche.

#### Come configurare l'esempio 2

La sequenza seguente mostra i passaggi da seguire per creare e applicare tag, quindi per configurare le restrizioni tag per i gruppi di applicazioni illustrati nel secondo esempio precedente.

VDA e applicazioni sono già stati installati sulle macchine e il gruppo di consegna è stato creato.

Creare e applicare tag alle macchine:

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Delivery Groups** (Gruppi di consegna) nel riquadro a sinistra. Selezionare il gruppo di consegna `D01`, quindi selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
2. Selezionare le macchine VDA 101-105 e quindi selezionare **Manage Tags** nella barra delle azioni.
3. Nella finestra di dialogo **Manage Tags** selezionare **Create**. Creare un tag denominato `CADApps`. Selezionare **OK**.
4. Selezionare nuovamente **Create** e creare un tag con il nome `OfficeApps`. Selezionare **OK**.
5. Aggiungere (applicare) i tag appena creati alle macchine selezionate abilitando le caselle di controllo accanto al nome di ciascun tag (`CADApps` e `OfficeApps`). Quindi chiudere la finestra di dialogo.
6. Selezionare il gruppo di consegna `D01`. Selezionare **View Machines** (Visualizza macchine) nella barra delle azioni.
7. Selezionare le macchine VDA 106-110 e quindi selezionare **Manage Tags** nella barra delle azioni.
8. Nella finestra di dialogo **Manage Tags** selezionare **Create**. Creare un tag denominato `AcctgApps`. Selezionare **OK**.
9. Applicare il tag `AcctgApps` appena creato e il tag `OfficeApps` alle macchine selezionate selezionando le caselle di controllo accanto al nome di ciascun tag. Quindi chiudere la finestra di dialogo.

Creare i gruppi di applicazioni con restrizioni tag.

1. Andare a **Manage > Full Configuration**, quindi selezionare **Applications** nel riquadro di sinistra.
2. Selezionare **Create Application Group** (Crea gruppo di applicazioni) nella barra delle azioni. Viene avviata la procedura guidata.
3. Nella pagina **Delivery Groups**, selezionare il gruppo di consegna `D01`. Selezionare **Restrict launches to machines with tag** (Limita lanci su macchine con tag), quindi selezionare il tag `AcctgApps` dall'elenco.
4. Completare la procedura guidata, specificando gli utenti contabili e le applicazioni di contabilità. Quando si aggiunge l'applicazione, scegliere l'origine **From Start menu** (Dal menu Start), che cerca l'applicazione sulle macchine che hanno il tag `AcctgApps`. Nella pagina **Summary**, assegnare al gruppo il nome `A100`.
5. Ripetere i passaggi precedenti per creare il gruppo di applicazioni `A200`, specificando le macchine che hanno il tag `CADApps`, oltre agli utenti e alle applicazioni appropriati.

6. Ripetere i passaggi per creare il gruppo di applicazioni `A300`, specificando le macchine che hanno il tag `OfficeApps`, oltre agli utenti e alle applicazioni appropriati.

#### Applicare i tag ai cataloghi di macchine

È possibile utilizzare **Manage > Full Configuration** oppure PowerShell per applicare tag ai cataloghi di macchine.

- L'uso dell'interfaccia di gestione è descritto in Gestire i tag. Le visualizzazioni del catalogo non indicano se sono applicati tag.
- Per utilizzare PowerShell, vedere Use PowerShell to apply tags to catalogs.

Ecco un esempio di utilizzo dei tag con i cataloghi:

- Un gruppo di consegna contiene macchine provenienti da diversi cataloghi, ma si desidera che un'operazione (ad esempio una pianificazione di riavvio) riguardi solo le macchine di un catalogo specifico. Tale obiettivo si può ottenere applicando un tag a quel catalogo.

#### Utilizzare PowerShell per applicare tag ai cataloghi

Sono disponibili i seguenti cmdlet PowerShell:

- È possibile passare oggetti catalogo a cmdlet come `Add-BrokerTag` e `Remove-BrokerTag` .
- `Get-BrokerTagUsage` mostra quanti cataloghi contengono tag.
- `Get-BrokerCatalog` ha una proprietà denominata `Tags`.

Ad esempio, i cmdlet seguenti aggiungono un tag creato in precedenza denominato `fy2018` al catalogo denominato `acctg`:`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018` .

Per informazioni e per la sintassi, vedere la guida dei cmdlet PowerShell.

### Tag automatici (anteprima)

Il tagging automatico consente agli amministratori di impostare e rimuovere automaticamente i tag su vari oggetti DaaS, in base a regole personalizzate. Questo miglioramento elimina la necessità di mantenere più script diversi che vengono eseguiti periodicamente per l'ottimizzazione dell'ambiente.

### Casi d'uso

Con il tagging automatico, è possibile implementare regole pertinenti ai motori economici per la propria attività, come la riduzione dei costi, l'ottimizzazione dell'infrastruttura e l'aumento dei consumi. Di seguito sono riportati alcuni dei casi d'uso:

- **Reclaim unused VDIs** (Recupera i VDI non utilizzati): per rilasciare i carichi di lavoro dedicati che non sono stati utilizzati per più di un numero preconfigurato di giorni nel pool disponibile.
- **Remove App clutter** (Rimuovi l'ingombro di app): per ridurre l'eccesso di applicazioni identificando le applicazioni che non sono state utilizzate per più di un numero preconfigurato di giorni.
- **DGs with less than X functional level** (DG con un livello funzionale inferiore a X): per trovare i gruppi di consegna con un livello funzionale inferiore a livello specifico.
- **Inactive users** (Utenti inattivi): per recuperare le risorse degli utenti che non hanno effettuato l'accesso per più di un numero preconfigurato di giorni.

### Comandi PowerShell

È possibile creare tag automatici utilizzando i comandi PowerShell. Una volta creata, una regola di tagging automatico viene valutata con una frequenza di 600 secondi. Per ulteriori informazioni, vedere New-BrokerAutoTagRule.

**Esempi** `New-BrokerAutoTagRule` utilizza lo stesso tipo di oggetto e gli stessi parametri di filtro del commandlet `Get-BrokerMachine`. Per ulteriori informazioni, vedere GetBrokerMachine.

1. Etichetta i VDI dedicati che non sono stati utilizzati per più di 30 giorni con un ID 123:

    a) Definire un tag con cui etichettare i VDI non utilizzati, ad esempio **unused-VDI.**

    - Nome tag: unused-VDI
    - ID del tag : 123

    b) Creare la regola di tagging automatico per applicare tag alle macchine non utilizzate. Definire i parametri della regola:

    - Nome : nome generico della regola.
    - Tipo di oggetto: macchina.
    - Testo della regola : macchine statiche assegnate connesse l'ultima volta più di 30 giorni prima o nessun valore.
    - Tag Uid : l'ID del tag a cui si desidera associarsi, 123.

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine' -
RuleText "-AllocationType Static -IsAssigned $true -Filter {
SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt '-30'
 -or LastConnectionTime -eq `$null )} " -TagUid 123
```

c) Controllare le macchine contrassegnate con il tag **unused-VDI** e rilasciarle.

2. Per assegnare tag ai gruppi di consegna con un livello funzionale inferiore a X (utilizzando **L7_20** come livello funzionale di soglia):

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-
RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid
 123
```

3. Per assegnare tag alle app visibili all'utente pubblicate senza una cartella:

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-
TagUid 123
```

### Ulteriori informazioni

Post del blog: Come assegnare desktop a server specifici.

## Impostazione del fuso orario

October 30, 2023

L'impostazione **Date and time** (data e ora) in **Settings** (Impostazioni) nella console di gestione consente di personalizzare il formato di data e ora in base alle proprie preferenze.

Fare clic su **Edit** (Modifica) per configurare le seguenti opzioni:

- **Time format** (Formato ora):
  - Selezionare questa opzione per visualizzare l'ora utilizzando un orologio a 12 ore (09:00pm, ad esempio) o un orologio a 24 ore (21:00, ad esempio).

> **Nota:**
>
> Selezionare l'opzione **Same as local** (Uguale a quella locale) se si desidera che il formato sia allineato al fuso orario del browser.

- **Date format** (Formato data):

  - Configurare il formato della data in base alle proprie preferenze, ad esempio gg/MM/aaaa.

> **Nota:**
>
> Selezionare l'opzione **Same as local** (Uguale a quella locale) se si desidera che il formato sia allineato al fuso orario del browser.

- **Time zone** (Fuso orario):
  - **UTC:** visualizza la data e l'ora in UTC in tutta l'interfaccia utente. Passando il mouse sulla data e l'ora vengono visualizzate le informazioni nel fuso orario locale.
  - **Local time zone** (Fuso orario locale): consente di visualizzare la data e l'ora nel fuso orario locale in tutta l'interfaccia utente. Passando il mouse sulla data e l'ora vengono visualizzate le informazioni in UTC.

## Risolvere i problemi relativi alla registrazione VDA e all'avvio della sessione

October 6, 2022

Offriamo una funzione di controllo di integrità che consente di valutare l'integrità dei VDA. La funzione consente di identificare le possibili cause dei problemi comuni di registrazione VDA e di avvio della sessione tramite l'interfaccia di gestione Full Configuration.

A differenza di Cloud Health Check, strumento autonomo per valutare l'integrità e la disponibilità del sito e degli altri suoi componenti, la funzione è disponibile come azione **Run Health Check** (Esegui controllo di integrità) nell'interfaccia di gestione Full Configuration.

L'azione **Run Health Check** può eseguire gli stessi controlli di Cloud Health Check tranne i seguenti:

- Per la registrazione VDA:
  - Disponibilità delle porte di comunicazione VDA
- Per i lanci delle sessioni sui VDA:
  - Disponibilità della porta di comunicazione di avvio della sessione
  - Percorso di avvio dell'applicazione VDA

### Prerequisiti

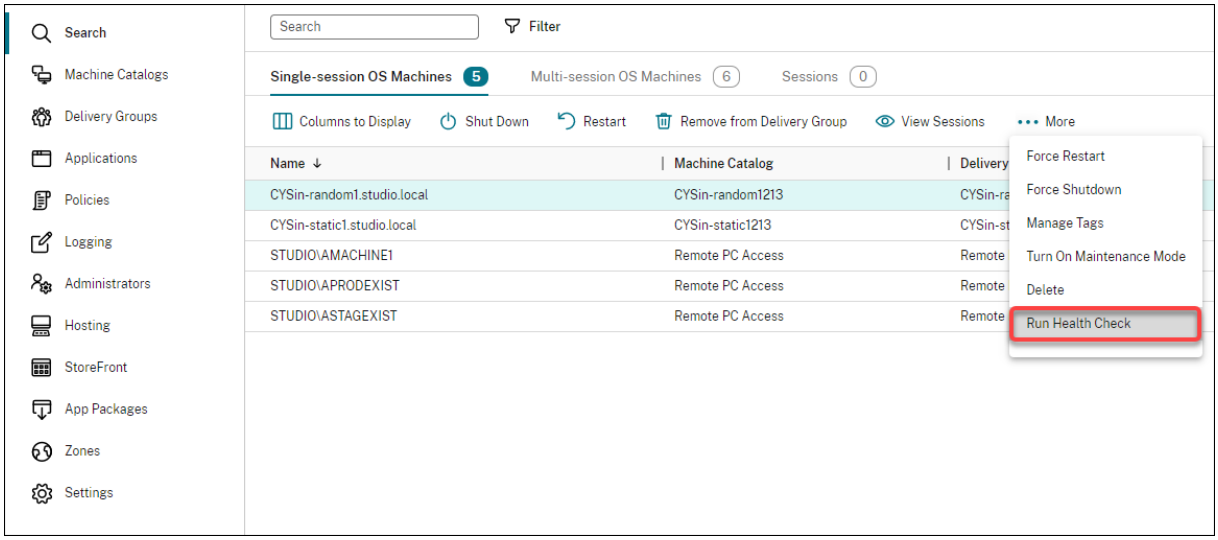
Prima di utilizzare la funzione, verificare che siano soddisfatti i seguenti prerequisiti:

- VDA Windows
- VDA versione 2109 o successiva
- I VDA sono registrati

### Eseguire controlli di integrità per i VDA

1. Nell'interfaccia di gestione Full Configuration, passare al nodo **Search**.
2. Selezionare una o più macchine, quindi selezionare **Run Health Check** nella barra delle azioni.




> **Nota:**
>
> Attualmente, è possibile eseguire controlli di integrità solo per i VDA registrati. L'azione **Run Health Check** (Esegui controllo di integrità) non è disponibile per i VDA non registrati.

Dopo aver selezionato **Run Health Check**, viene visualizzata una finestra che mostra lo stato di avanzamento dei controlli di integrità. Attendere il completamento dei controlli di integrità o fare clic su **Cancel** per annullare i controlli. Se necessario, è possibile spostare la finestra.

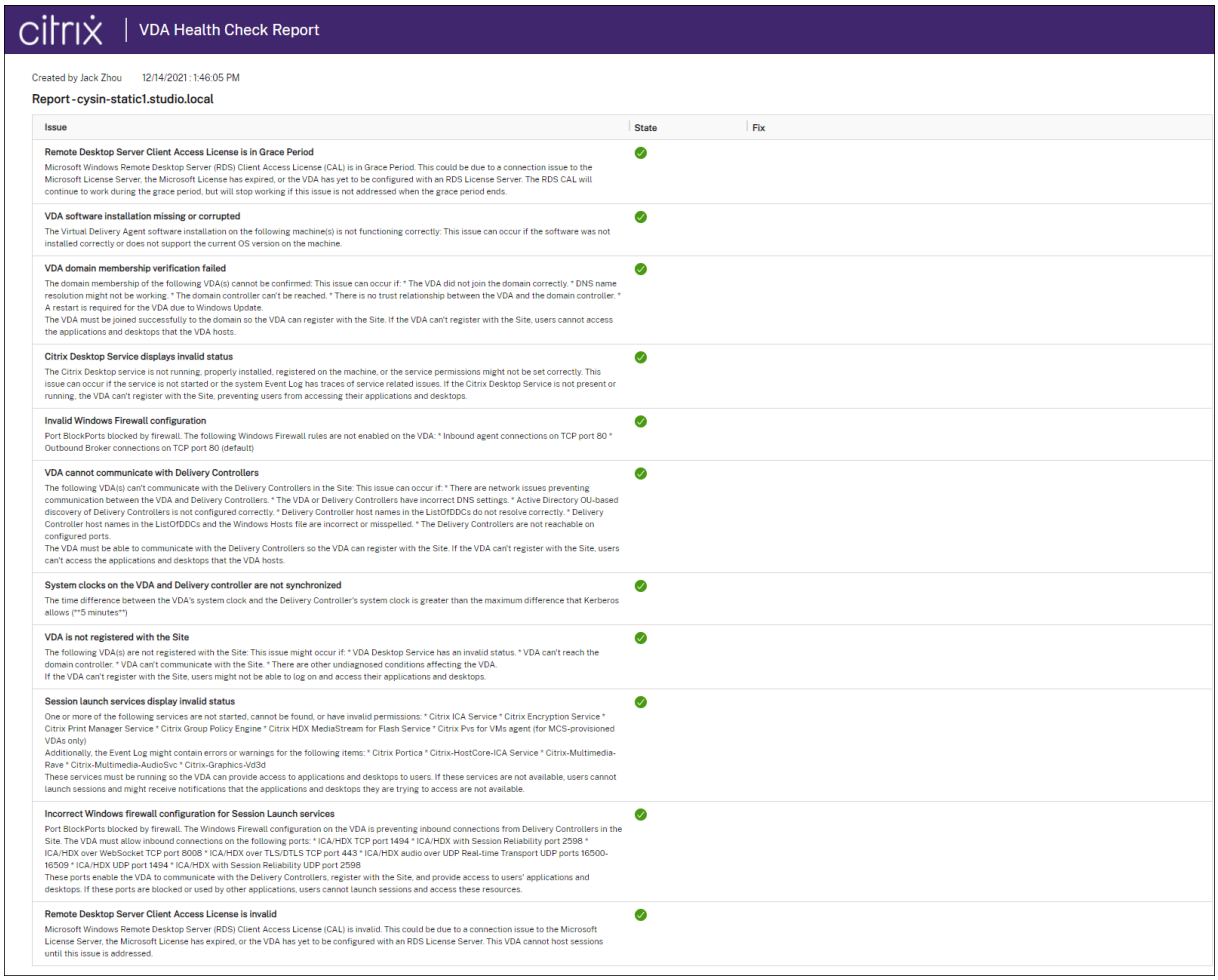

> **Nota:**
>
> Negli scenari in cui esiste già una finestra "health checks in progress"(controlli di integrità in corso), non è possibile eseguire controlli di integrità aggiuntivi fino al completamento di quelli esistenti.

Al termine dei controlli di integrità, vengono visualizzati i seguenti due pulsanti: **View report** e **Close**. Per visualizzare i risultati dei controlli di integrità, fare clic su **View report**.


Il rapporto del controllo di integrità si apre in una nuova scheda del browser. Il rapporto contiene i seguenti elementi:

- Ora e data in cui è stato generato il report dei risultati
- La persona che ha eseguito i controlli di integrità
- I controlli vengono eseguiti sui computer di destinazione
- Problemi riscontrati, insieme a consigli di correzione




È possibile eseguire controlli di integrità singolarmente e in batch.

> **Nota:**
>
> Quando si eseguono controlli di integrità in batch, selezionare non più di 10 macchine. In caso contrario, l'azione **Run Health Check** non è disponibile.

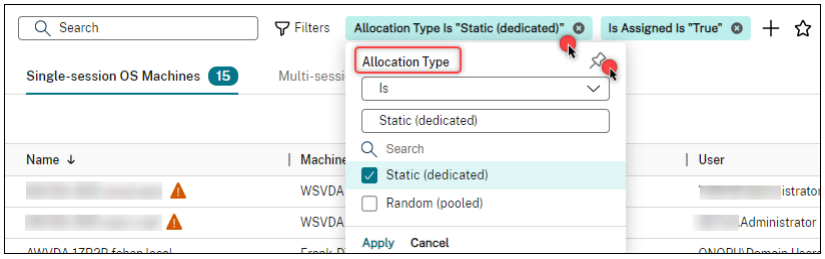
# Utilizzare la funzione di ricerca nell'interfaccia di gestione Full Configuration

December 18, 2023

## Introduzione

Utilizzare la funzione di ricerca per visualizzare informazioni su macchine, sessioni, cataloghi di macchine, applicazioni, gruppi di consegna specifici e altro.
In **Full Configuration > Search**, sono disponibili diverse opzioni:

- Utilizzare le schede per elencare i computer in base al tipo (sistema operativo a sessione singola o multisessione) o per elencare tutte le sessioni.
- Inserire il nome nella casella di ricerca per eseguire una ricerca rapida senza applicare filtri.
- Perfezionare la ricerca utilizzando i filtri.
  - Selezionare **Match all** (Corrispondi a tutti) (operatore AND) se si desidera che la ricerca restituisca risultati che corrispondono a tutti i criteri di filtro. Seleziona **Match any** (Corrispondi a qualsiasi) (operatore OR) se si desidera che la ricerca restituisca risultati che corrispondono a uno qualsiasi dei criteri di filtro.
  - Selezionare l'icona dei filtri per aprire il pannello dei filtri. È possibile selezionare più criteri di filtro all'interno del pannello.
  - Fare clic sul filtro per aprire il pannello con la puntina. Fai clic sull'icona della **puntina** per bloccare il campo del filtro utilizzato per la ricerca. È possibile aggiungere i campi di filtro utilizzati di frequente per una facile accessibilità.




  - Salvare i filtri in uso facendo clic sul simbolo della stella. L'elemento salvato è noto come set di filtri. Gli elementi salvati vengono visualizzati nei **Saved filter sets** (set di filtri salvati) (per accedere all'elenco, selezionare la casella di ricerca). È possibile fare clic su un set di filtri salvato per applicare i filtri alla propria ricerca. Per eliminare un set di filtri salvato, passarci sopra con il mouse e selezionare l'icona **X**. Per gestire i set di filtri salvati, selezionare **Manage**.

> **Nota:**
>
> I set di filtri vengono salvati suddivisi per amministratore, garantendo un'esperienza di filtraggio personalizzata e personalizzata per ogni amministratore.

### Ricerca senza filtri

Digitare nella casella di ricerca e premere **Invio** per eseguire una ricerca generale senza applicare filtri.

Eseguendo una ricerca generale, DaaS cerca le corrispondenze in base ai seguenti criteri e fornisce risultati pertinenti:

- **Name**. Ricerca per nome della macchina o nome DNS.
- **Machine Catalog**. Ricerca per nome del catalogo di macchine.
- **Delivery Group**. Ricerca per nome del gruppo di consegna.
- **User**. Ricerca per nome utente della sessione.
- **Client**. Ricerca per nome del client di sessione.
- **VM**. Ricerca per nome della macchina ospitata. È il nome intuitivo della macchina ospitata utilizzato dal suo hypervisor.
- **Hosting Server Name**. Ricerca in base al nome del server di hosting.

Quando si cerca un elemento particolare, ad esempio un utente, un gruppo di desktop, un catalogo o una macchina, la ricerca generale è un modo pratico per trovare le informazioni necessarie.

### Cercare cataloghi di macchine o gruppi di consegna

È possibile cercare e individuare le risorse all'interno dei nodi **Machine Catalogs** e **Delivery Groups**. La funzionalità di ricerca in questi nodi fornisce la stessa interfaccia del nodo **Search**, offrendo un'esperienza di ricerca senza interruzioni in tutto DaaS.

È possibile eseguire ricerche generali e ricerche basate su filtri. Nel nodo **Machine Catalogs**, sono disponibili i seguenti filtri:

- **Catalog Name**. Ricerche in base al nome del catalogo di macchine.
- **Allocation Type**. Filtra per allocazione statica (dedicata) o casuale (in pool) o entrambe.
- **Provisioning Type**. Filtra per metodo di provisioning manuale o MCS o entrambi.
- **Session Support**. Filtri per macchina a sessione singola o multisessione o entrambe.
- **Allocated Count**. Filtra in base al numero di macchine allocate.
- **Persistence**. Filtra in base alle modifiche della macchina non persistenti (scarta) o persistenti (su disco locale) o entrambe.
- **Machine Type**. Filtra per tipo di macchina fisica o virtuale o entrambi.

Nel nodo **Delivery Groups** (Gruppi di consegna), sono disponibili i seguenti filtri:

- **Group Name**. Esegue la ricerca in base al nome del gruppo di consegna.
- **Description**. Filtra in base alla descrizione del gruppo di consegna specificata durante la sua creazione.
- **Session Support**. Filtri per macchina a sessione singola o multisessione o entrambe.
- **Machine Identity**. Filtra in base all'identità della macchina.
- **Remote PC Access**. Filtri per macchina Accesso remoto PC.
- **Maintenance mode**. Filtri per macchine in modalità di manutenzione (accesa o spenta o entrambe).
- **Group State**. Filtra in base allo stato del gruppo. L'opzione **Enable delivery group** (Abilita gruppo di consegna) in **Edit Delivery Group > User Settings** (Modifica gruppo di consegna > Impostazioni utente) controlla se interrompere la consegna di applicazioni e desktop.
- **Allocation Type**. Filtra per tipo statico (dedicato) o casuale (in pool) o entrambi.

Eseguendo una ricerca generale, DaaS cerca le corrispondenze in base ai seguenti criteri e fornisce risultati pertinenti:

- **Cataloghi di macchine**:
  - Name: cerca il catalogo delle macchine per nome, incluso il percorso della cartella.
  - Machine catalog: cerca i cataloghi di macchine per nome.
  - Description: cerca in base alla descrizione del catalogo di macchine specificata durante la creazione del catalogo.
- **Gruppi di consegna**:
  - Delivery group name: cerca i gruppi di consegna per nome.
  - Description: cerca in base alla descrizione del gruppo di consegna specificata durante la creazione del gruppo di consegna.

### Personalizzare le colonne da visualizzare

Quando si personalizzano le colonne, è possibile visualizzare le colonne contrassegnate con l'etichetta **Degrades performance** (Riduce le prestazioni). La selezione di tali colonne potrebbe ridurre le prestazioni della console. Dopo aver completato la personalizzazione, la tabella si aggiorna per visualizzare le colonne selezionate. La loro presenza potrebbe causare ritardi quando si aggiorna la tabella.

Se la personalizzazione contiene colonne che riducono le prestazioni, viene richiesto di determinare se conservarle. Il messaggio viene visualizzato dopo che si aggiorna la finestra del browser o ci si scollega dalla console e quindi si accede. Se si decide di conservare le colonne, tenere presente le seguenti considerazioni:

- Per garantire le prestazioni della console, non è possibile aggiornare la tabella più di una volta al minuto. Questa restrizione si applica a tutte le schede: **Single-session OS Machines** (Macchine con sistema operativo a sessione singola), **Multi-session OS Machines** (Macchine con sistema operativo multisessione) e **Sessions** (Sessioni). Se si ha necessità di aggiornamenti più frequenti, rimuovere tutte le colonne che riducono le prestazioni.

### Esportare i risultati della ricerca in un file CSV

È possibile esportare i risultati della ricerca (fino a 30,000 elementi) in un file CSV. Il file viene salvato nella posizione di download predefinita del browser.

Questa funzionalità è disponibile sia per le macchine che per le sessioni. Per esportare i risultati della ricerca, fare clic sull'icona di esportazione nell'angolo in alto a destra. Il completamento dell'esportazione potrebbe richiedere alcuni minuti.

In ogni scheda del nodo Search (Cerca), non è possibile eseguire un'altra esportazione mentre è in corso un'esportazione.

### Suggerimenti per migliorare una ricerca

Tenere presenti i seguenti suggerimenti quando si utilizza la funzione di ricerca:

- Nel nodo **Search**, selezionare una colonna qualsiasi per ordinare gli elementi.
- Per visualizzare più caratteristiche da includere nella visualizzazione in cui è possibile cercare e ordinare, selezionare **Columns to Display** (Colonne da visualizzare) o fare clic su qualsiasi colonna e selezionare **Columns to Display**. Nella finestra **Columns to Display**, selezionare la casella di controllo accanto agli elementi da visualizzare e selezionare **Save** per uscire.

  > **Nota:**
  >
  > Gli elementi che riducono le prestazioni sono contrassegnati dall'etichetta **Degrades performance** .

- Per individuare un dispositivo utente connesso a una macchina, utilizzare **Client (IP)** e **Is**, quindi immettere l'indirizzo IP del dispositivo.
- Per individuare le sessioni attive, utilizzare **Session State**, **Is** e **Connected**.
- Per elencare tutte le macchine di un gruppo di consegna, selezionare **Delivery Groups** nel riquadro di sinistra. Selezionare il gruppo, quindi selezionare **View Machines** (Visualizza macchine) dalla barra delle azioni o dal menu di scelta rapida.

Quando si eseguono operazioni di ordinamento, tenere presenti le seguenti considerazioni:

- Se il numero di elementi non supera 5.000, è possibile fare clic su qualsiasi colonna per ordinare gli elementi in essa contenuti. Quando il numero supera 5.000, è possibile ordinare solo per nome o per utente corrente (a seconda della scheda in cui ci si trova). Per abilitare l'ordinamento, utilizzare i filtri per ridurre il numero di elementi a 5.000 o meno.
- Quando il numero di elementi è superiore a 500 ma non superiore a 5.000:
  - Tutti i dati vengono memorizzati nella cache locale per migliorare le prestazioni di ordinamento. Nelle schede **Single-session OS Machines** e**Multi-session OS Machines** si memorizzano nella cache i dati la prima volta che si fa clic su una colonna (qualsiasi colonna tranne la colonna **Name**) per l'ordinamento. Nella scheda **Sessions**, si memorizzano i dati nella cache la prima volta che si fa clic su una colonna (qualsiasi colonna tranne la colonna **Current User** (Utente corrente)) per ordinare. Di conseguenza, il completamento dell'ordinamento richiede più tempo. Per prestazioni più veloci, ordinare per nome o utente corrente oppure utilizzare i filtri per ridurre il numero di elementi.
  - Il seguente messaggio sotto la tabella indica che i dati sono memorizzati nella cache: Last refreshed: <`the time when you refreshed the table`>. In tal caso, le operazioni di ordinamento si basano su elementi che sono stati caricati in precedenza. Questi elementi potrebbero non essere aggiornati. Per aggiornarli, fare clic sull'icona di aggiornamento.

## Accesso utente

May 9, 2023

Esistono due componenti principali che forniscono l'accesso ad applicazioni e desktop in una distribuzione Citrix DaaS (precedentemente chiamato servizio Citrix Virtual Apps and Desktops):

- **Piattaforma Citrix Workspace**: la piattaforma Citrix Workspace è una soluzione digitale completa che consente di fornire un accesso sicuro alle informazioni, alle app e ad altri contenuti rilevanti per il ruolo di una persona nell'organizzazione. Gli utenti si abbonano ai servizi che l'amministratore rende disponibili e possono accedervi da qualsiasi luogo, su qualsiasi dispositivo. La piattaforma Citrix Workspace aiuta a organizzare e automatizzare i dettagli più importanti di cui gli utenti hanno bisogno per collaborare, prendere decisioni migliori e concentrarsi completamente sul loro lavoro.

  Non vi è alcuno sforzo per distribuire Citrix Workspace ed è mantenuto "sempreverde"da Citrix. La piattaforma Citrix Workspace è consigliata per clienti nuovi ed esistenti, anteprime e Proof of Concept (POC).

- **Uno StoreFront locale**: i clienti possono anche utilizzare uno StoreFront esistente per aggregare applicazioni e desktop in Citrix Cloud. Questo caso d'uso offre una maggiore sicurezza, incluso il supporto per l'autenticazione a due fattori, e impedisce agli utenti di inserire la propria password nel servizio cloud. Consente inoltre ai clienti di personalizzare i propri nomi di dominio e URL. Questo tipo di distribuzione è consigliato a tutti i clienti Citrix Virtual Apps and Desktops che hanno già installato StoreFront.

  Vedere anche Local Host Cache and StoreFront.

Quando gli utenti si connettono dall'esterno del firewall aziendale, Citrix Cloud può utilizzare la tecnologia Citrix Gateway (precedentemente NetScaler Gateway) per proteggere queste connessioni con SSL. Citrix Gateway o l'appliance virtuale Citrix VPX è un'appliance VPN SSL distribuita nella zona demilitarizzata (DMZ). Fornisce un unico punto di accesso sicuro attraverso il firewall aziendale.

### Utilizzare Citrix Workspace

L'accesso agli spazi di lavoro avviene tramite `https://<customername>.cloud.com`. Se necessario, è possibile personalizzare la parte `<customername>` dell'URL dell'area di lavoro. È quindi possibile configurare la connettività per ogni posizione di risorse che si desidera utilizzare, in modo che gli utenti finali possano accedere alle risorse nella propria area di lavoro. Gli utenti finali accedono alla propria area di lavoro utilizzando l'ultima versione dell'app Citrix Workspace.

Per ulteriori informazioni sull'utilizzo di Citrix Workspace, vedere:

- Configurare le aree di lavoro: per configurare l'accesso e le personalizzazioni.
- Proteggere le aree di lavoro: per configurare l'autenticazione.
- Gestire l'esperienza Workspace: per capire come gli utenti finali accedono alla propria area di lavoro e l'aspetto che ha.

Per fornire l'accesso remoto agli utenti finali tramite Citrix Workspace, è possibile utilizzare il servizio Citrix Gateway o il proprio Citrix Gateway.

- Per utilizzare il servizio Citrix Gateway:

  1. In **Citrix Cloud > Resource Locations** (Citrix Cloud > Posizioni delle risorse) selezionare **Gateway** per la posizione delle risorse che si desidera utilizzare.
  2. Selezionare **Gateway Service** e fare clic su **Save**.
  3. In **Citrix Cloud > Workspace Configuration > Service Integrations** (Citrix Cloud > Configurazione dell'area di lavoro > Integrazioni di servizi), individuare il servizio Gateway e selezionare **Enable** dal menu con i puntini di sospensione.

- Per utilizzare il proprio Citrix Gateway:

1. Configuraree Citrix Gateway come proxy ICA (non sono necessari autenticazione o criteri di sessione).
2. Configurare un percorso di risorse per utilizzare Citrix Gateway:
   a) In **Citrix Cloud > Resource Locations** (Citrix Cloud > Posizioni delle risorse) selezionare **Gateway** per la posizione delle risorse che si desidera utilizzare.
   b) Selezionare **Traditional Gateway** e immettere il nome di dominio completo esterno. Non aggiungere un protocollo. Le porte sono facoltative. La combinazione di accesso remoto e interno non è supportata in Citrix Workspace.
3. Associare Citrix Cloud Connectors come server STA (Secure Ticket Authority) a Citrix Gateway. Per ulteriori informazioni, vedere CTX232640.

   > **Nota:**
   >
   > Solo le macchine Citrix Cloud Connector sono supportate per l'uso come server STA con Citrix Gateway. L'uso di altri connettori come server STA, ad esempio Connector Appliance, non è supportato.

Per ulteriori informazioni sul servizio Citrix Gateway e su Citrix Gateway, vedere Citrix Gateway.

### Utilizzare uno StoreFront locale

Per informazioni sulla configurazione di uno StoreFront locale, vedere la documentazione di StoreFront.

Uno dei vantaggi dell'uso di uno StoreFront esistente è che Citrix Cloud Connector fornisce la crittografia delle password degli utenti. Cloud Connector crittografa le credenziali utilizzando AES-256, mediante una chiave monouso generata casualmente. Questa chiave viene restituita direttamente all'app Citrix Workspace e non viene mai inviata al cloud. L'app Citrix Workspace la fornisce quindi al VDA durante l'avvio della sessione per decrittografare le credenziali e fornire un'esperienza Single Sign-On in Windows.

- Per il trasporto, selezionare HTTP e la porta 80. La macchina StoreFront deve essere in grado di accedere direttamente al Cloud Connector tramite il nome di dominio completo (FQDN) fornito. Il Cloud Connector deve essere in grado di raggiungere l'URL Cloud NFuse/STA su (`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` e `ctxsta.dll`).
- Aggiungere Cloud Connector come controller di consegna per un'elevata disponibilità.

Utilizzare la versione più recente di StoreFront.

#### Accesso esterno

Per fornire accesso esterno tramite Citrix Gateway e StoreFront in locale:

- Configurare Citrix Gateway come di consueto, con criteri di autenticazione e sessione. Vedere la documentazione di Citrix Gateway.
- Indirizzare i Delivery Controller dello store StoreFront locale ai Citrix Cloud Connector. Associare i Cloud Connector come server STA a Citrix Gateway.
- Citrix Gateway deve utilizzare gli stessi URL STA di StoreFront. Se il gateway non è già configurato per utilizzare l'STA di un ambiente Citrix Virtual Apps and Desktops esistente, i Cloud Connector possono essere utilizzati come STA.

#### Accesso interno

Per fornire l'accesso interno tramite uno StoreFront locale, indirizzare i Delivery Controller dello store StoreFront locale ai Citrix Cloud Connector.

#### Accesso esterno e interno

Per fornire accesso esterno e interno tramite Citrix Gateway e StoreFront in locale:

- Configurare Citrix Gateway come di consueto, con criteri di autenticazione e sessione. Vedere la documentazione di Citrix Gateway.
- Associare i Cloud Connector come server STA a Citrix Gateway.
- Indirizzare i Delivery Controller del proprio store StoreFront locale ai Cloud Connector.

### Cache host locale e StoreFront

La cache host locale consente di continuare le operazioni di intermediazione delle connessioni in una distribuzione Citrix DaaS quando i Cloud Connector non sono in grado di comunicare con Citrix Cloud.

La funzionalità della cache host locale funziona solo nelle posizioni delle risorse che contengono uno StoreFront locale distribuito dal cliente. La funzionalità della cache host locale non è supportata per l'uso con Citrix Workspace.

Ogni postazione di risorse deve avere uno StoreFront locale distribuito dal cliente. Verificare che la posizione della risorsa contenga uno StoreFront locale che punti a tutti i Cloud Connector presenti in quella posizione della risorsa.

Per ulteriori informazioni, vedere Cache host locale.

# IP virtuale e loopback virtuale

October 6, 2022

> **Importante:**
>
> Windows 10 Enterprise multisessione non supporta la virtualizzazione IP di Desktop remoto (IP virtuale) e Citrix non supporta né l'IP virtuale né il loopback virtuale in Windows 10 Enterprise multisessione.

Le funzionalità Virtual IP e di loopback virtuale sono supportate sulle macchine Windows Server 2016. Queste funzionalità non si applicano alle macchine con sistema operativo desktop Windows.

La funzionalità di indirizzo IP virtuale di Microsoft fornisce a un'applicazione pubblicata un indirizzo IP univoco assegnato dinamicamente per ciascuna sessione. La funzione di loopback virtuale Citrix consente di configurare applicazioni che dipendono dalle comunicazioni con localhost (127.0.0.1 per impostazione predefinita) per l'uso di un indirizzo di loopback virtuale univoco compreso nell'intervallo localhost (127.*).

Alcune applicazioni, quali CRM e Computer Telephony Integration (CTI), utilizzano un indirizzo IP per indirizzamento, licenza, identificazione o altri scopi e quindi richiedono un indirizzo IP univoco o un indirizzo di loopback nelle sessioni. Altre applicazioni potrebbero essere collegate a una porta statica, quindi i tentativi di avviare istanze aggiuntive di un'applicazione in un ambiente multiutente non riescono perché la porta è già in uso. Per assicurare che tali applicazioni funzionino correttamente in un ambiente Citrix Virtual Apps, è necessario un indirizzo IP univoco per ciascun dispositivo.

L'IP virtuale e il loopback virtuale sono funzionalità indipendenti. È possibile utilizzare una delle due o entrambe.

Sinossi dell'azione dell'amministratore:

- Per utilizzare Microsoft Virtual IP, abilitarlo e configurarlo sul server Windows (Le impostazioni dei criteri Citrix non sono necessarie).
- Per utilizzare il loopback virtuale Citrix, configurare due impostazioni in un criterio Citrix.

## IP virtuale

Quando l'IP virtuale è abilitato e configurato sul server Windows, ogni applicazione configurata in esecuzione in una sessione sembra avere un indirizzo univoco. Gli utenti accedono a queste applicazioni su un server Citrix Virtual Apps nello stesso modo in cui accedono a qualsiasi altra applicazione pubblicata. Un processo richiede un IP virtuale in uno dei seguenti casi:

- Il processo utilizza un numero di porta TCP hardcoded

- Il processo utilizza socket Windows e richiede un indirizzo IP univoco o un numero di porta TCP specificato

Per determinare se un'applicazione deve utilizzare indirizzi IP virtuali:

1. Ottenete lo strumento TCPView da Microsoft. Questo strumento elenca tutte le applicazioni che collegano indirizzi IP e porte specifici.
2. Disabilitare la funzione Risolvi indirizzi IP in modo da visualizzare gli indirizzi anziché i nomi host.
3. Avviare l'applicazione e utilizzare TCPView per vedere quali indirizzi IP e quali porte vengono aperte dall'applicazione e quali nomi di processo stanno aprendo queste porte.
4. Configurare tutti i processi che aprono l'indirizzo IP del server, 0.0.0.0 o 127.0.0.1.
5. Per garantire che un'applicazione non apra lo stesso indirizzo IP su una porta diversa, avviare un'istanza aggiuntiva dell'applicazione.

#### Come funziona la virtualizzazione IP di Microsoft Remote Desktop (RD)

- Sul server Microsoft deve essere abilitato l'indirizzamento IP virtuale.

  Ad esempio, in un ambiente Windows Server 2016, da Server Manager espandere **Servizi Desktop remoto > Connessioni host sessione Desktop remoto** per abilitare la funzionalità di virtualizzazione IP Desktop remoto e configurare le impostazioni per assegnare dinamicamente gli indirizzi IP utilizzando il server DHCP (Dynamic Host Configuration Protocol) per quella sessione o per quel programma. Per istruzioni, vedere la documentazione Microsoft.

- Dopo aver attivato la funzione, all'avvio della sessione il server richiede gli indirizzi IP assegnati dinamicamente dal server DHCP.

- La funzione Virtualizzazione IP Desktop remoto assegna indirizzi IP alle connessioni desktop remote per sessione o per programma. Se si assegnano indirizzi IP a più programmi, questi hanno lo stesso indirizzo IP per sessione.

- Dopo aver assegnato un indirizzo a una sessione, la sessione utilizza l'indirizzo virtuale anziché l'indirizzo IP principale del sistema ogni volta che vengono effettuate le seguenti chiamate: `bind`¸`closesocket`¸`connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Quando si utilizza la funzionalità di virtualizzazione IP Microsoft all'interno della configurazione di hosting di sessione Desktop remoto, le applicazioni vengono associate a specifici indirizzi IP inserendo un componente "filtro"tra l'applicazione e le chiamate di funzione Winsock. L'applicazione vede quindi solo l'indirizzo IP che deve utilizzare. Qualsiasi tentativo da parte dell'applicazione di ascoltare le comunicazioni TCP o UDP è associato automaticamente all'indirizzo IP virtuale allocato

(o indirizzo di loopback) e qualsiasi connessione di origine aperta dall'applicazione ha origine dall'indirizzo IP associato all'applicazione.

Nelle funzioni che restituiscono un indirizzo (ad esempio `GetAddrInfo()`, controllato da un criterio di Windows), se viene richiesto l'indirizzo IP dell'host locale, l'IP virtuale esamina l'indirizzo IP restituito e lo modifica per corrispondere all'indirizzo IP virtuale della sessione. Le applicazioni che tentano di ottenere l'indirizzo IP del server locale tramite tali funzioni di nome vedono solo l'indirizzo IP virtuale univoco assegnato a quella sessione. Questo indirizzo IP viene spesso utilizzato nelle chiamate socket successive, quali bind o connect. Per ulteriori informazioni sui criteri di Windows, vedere Virtualizzazione IP RDS in Windows Server.

Spesso, un'applicazione richiede di collegarsi a una porta per l'ascolto sull'indirizzo 0.0.0.0. Quando un'applicazione esegue questa operazione e utilizza una porta statica, non è possibile avviare più istanze dell'applicazione. La funzione di indirizzo IP virtuale cerca anche 0.0.0.0 in questi tipi di chiamata e modifica la chiamata in ascolto sull'indirizzo IP virtuale specifico, che consente a più di un'applicazione di ascoltare sulla stessa porta dello stesso computer perché sono tutte in ascolto su indirizzi diversi. La chiamata viene modificata solo se si trova in una sessione ICA e se la funzione di indirizzo IP virtuale è abilitata. Ad esempio, se due istanze di un'applicazione in esecuzione in sessioni diverse provano entrambe a collegarsi a tutte le interfacce (0.0.0.0) e a una porta specifica (ad esempio 9000), queste si associano a VIPAddress1:9000 e a VIPAddress2:9000 e non vi sono conflitti.

### Loopback virtuale

L'abilitazione delle impostazioni dei criteri di loopback IP virtuale Citrix consente a ogni sessione di disporre del proprio indirizzo di loopback per la comunicazione. Quando un'applicazione utilizza l'indirizzo localhost (impostazione predefinita= 127.0.0.1) in una chiamata Winsock, la funzione di loopback virtuale sostituisce semplicemente 127.0.0.1 con 127.X.X.X, dove X.X.X è una rappresentazione dell'ID sessione + 1. Ad esempio, un ID di sessione 7 è 127.0.0.8. Nell'improbabile caso in cui l'ID di sessione superi il quarto ottetto (più di 255), l'indirizzo passa all'ottetto successivo (127.0.1.0), fino al massimo di 127.255.255.255.

Un processo richiede il loopback virtuale in uno dei seguenti casi:

- Il processo utilizza l'indirizzo di loopback del socket Windows (localhost) (127.0.0.1)
- Il processo utilizza un numero di porta TCP hardcoded

Utilizzare le impostazioni dei criteri di loopback virtuale per le applicazioni che utilizzano un indirizzo di loopback per la comunicazione tra processi. Non è richiesta alcuna configurazione aggiuntiva. Il loopback virtuale non dipende dall'IP virtuale, quindi non è necessario configurare il server Microsoft.

- Supporto loopback IP virtuale. Se abilitata, questa impostazione dei criteri consente a ogni sessione di avere il proprio indirizzo di loopback virtuale. Questa impostazione è disabilitata

per impostazione predefinita. La funzionalità si applica solo alle applicazioni specificate con l'impostazione dei criteri di elenco dei programmi di loopback virtuale Virtual IP.
- Elenco dei programmi di loopback virtuale Virtual IP. Questa impostazione dei criteri specifica le applicazioni che utilizzano la funzione di loopback IP virtuale. Questa impostazione si applica solo quando è abilitata l'impostazione del criterio di supporto per il loopback Virtual IP.

#### Funzionalità correlata

È possibile utilizzare le seguenti impostazioni del Registro di sistema per garantire che il loopback virtuale abbia la preferenza rispetto all'IP virtuale; si tratta del cosiddetto loopback preferito. Tuttavia, procedere con cautela:

- Utilizzare il loopback preferito solo se sono abilitati sia l'IP virtuale che il loopback virtuale; altrimenti si potrebbero ottenere risultati indesiderati.
- La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Eseguire regedit sui server in cui risiedono le applicazioni.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Nome: PreferLoopback, Tipo: REG_DWORD, Data: 1
- Nome: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Dati: <elenco dei processi>

## Zone

December 18, 2023

### Introduzione

Le distribuzioni di Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops) che si estendono su posizioni ampiamente disperse connesse da una WAN possono affrontare sfide dovute alla latenza e all'affidabilità della rete. L'uso delle zone può aiutare gli utenti che si trovano in regioni remote a connettersi alle risorse senza necessariamente costringere le loro connessioni ad attraversare grandi segmenti della WAN. Nell'ambiente Citrix DaaS, ogni posizione risorsa è considerata una zona.

Le zone possono essere utili per implementazioni di tutte le dimensioni. È possibile utilizzare le zone per mantenere le applicazioni e i desktop più vicini agli utenti, migliorando le prestazioni. Le zone possono essere utilizzate per il ripristino d'emergenza, i data center distanti geograficamente, le filiali, un cloud o una zona di disponibilità in un cloud.

In questo articolo il termine locale si riferisce alla zona in discussione. Ad esempio, "Un VDA si registra con un Cloud Connector"significa che un VDA si registra con un Cloud Connector nella zona in cui si trova il VDA.

### Differenze rispetto alle zone negli ambienti Citrix Virtual Apps and Desktops locali

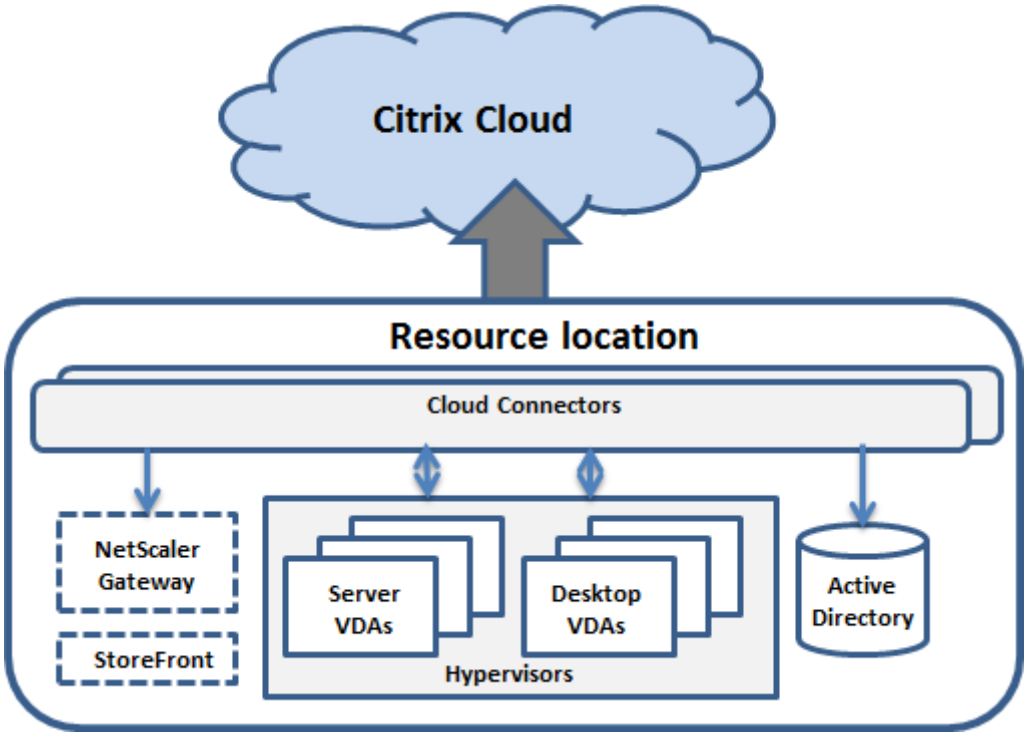
Le zone in un ambiente Citrix DaaS sono simili, ma non identiche alle zone in una distribuzione on-premise di Citrix Virtual Apps and Desktops.

- In Citrix DaaS, le zone vengono create automaticamente quando si crea una posizione risorsa e si aggiunge un Cloud Connector. A differenza di una distribuzione on-premise, un ambiente Citrix DaaS non classifica le zone come primarie o satellite.
- In XenApp versione 6.5 e precedenti, le zone includevano raccoglitori di dati. Citrix DaaS non utilizza agenti di raccolta dati per le zone. Inoltre, il failover e le zone preferite funzionano in modo diverso.

### Cosa c'è in una zona

Una zona è equivalente a una posizione di risorse. Quando si crea una posizione di risorse e si installa un Cloud Connector, viene creata automaticamente una zona. Ogni zona può avere un insieme diverso di risorse, in base alle esigenze specifiche e all'ambiente dell'utente.




Ogni zona deve avere sempre almeno un Cloud Connector, e preferibilmente due o più, per la ridondanza.

È possibile inserire cataloghi di macchine, hypervisor, connessioni host, utenti e applicazioni in una zona. Una zona può contenere anche server Citrix Gateway e StoreFront. Per utilizzare la funzionalità della cache host locale, una zona deve disporre di un server StoreFront.

Le zone sono supportate con Citrix Workspace e il servizio Citrix Gateway.

L'inserimento di elementi in una zona influisce sul modo in cui Citrix DaaS interagisce con essi e con altri oggetti a essi correlati.

- Quando una connessione hypervisor viene posizionata in una zona, si presume che tutti gli hypervisor gestiti tramite quella connessione risiedano anche in quella zona.
- Quando un catalogo di macchine viene inserito in una zona, si presume che tutti i VDA nel catalogo si trovino nella zona.
- È possibile aggiungere istanze di Citrix Gateway alle zone. Quando si crea una posizione di risorse, viene offerta la possibilità di aggiungere un Citrix Gateway. Quando un Citrix Gateway è associato a una zona, questo viene preferito per l'uso quando si utilizzano connessioni a VDA di quella zona.
- Idealmente, Citrix Gateway viene utilizzato in una zona per le connessioni utente che entrano in quella zona da altre zone o posizioni esterne. È inoltre possibile utilizzarlo per le connessioni all'interno della zona.
- Dopo aver creato più posizioni di risorse e aver installato dei Cloud Connector al loro interno (azione che crea automaticamente più zone), è possibile spostare le risorse da una zona all'al-

tra. Questa flessibilità comporta il rischio di separare gli elementi che funzionano meglio nelle immediate vicinanze. Ad esempio, lo spostamento di un catalogo in una zona diversa dalla connessione (host) che crea le macchine del catalogo può influire sulle prestazioni. Considerare quindi i potenziali effetti non voluti prima di spostare elementi da una zona all'altra. Mantenere un catalogo e la connessione host che utilizza nella stessa zona.

Se la connessione tra una zona e Citrix Cloud non riesce, la funzione della cache host locale consente a un Cloud Connector della zona di continuare a mediare le connessioni alle VDA in quella zona. La zona deve avere StoreFront installato. Ad esempio, questo è efficace in un ufficio in cui gli impiegati utilizzano il sito StoreFront locale per accedere alle risorse locali, anche se il collegamento WAN che collega il proprio ufficio alla rete aziendale non funziona. Per ulteriori informazioni, vedere Cache host locale.

### Dove si registrano i VDA

I VDA devono essere come minimo versione 7.7 per utilizzare queste funzionalità di registrazione delle zone:

- Un VDA che si trova in una zona viene registrato con un Cloud Connector locale.
  - Finché il Cloud Connector è in grado di comunicare con Citrix Cloud, le normali operazioni continuano.
  - Se quel Cloud Connector è operativo ma non è in grado di comunicare con Citrix Cloud (e quella zona ha uno StoreFront locale), entra in modalità di interruzione della cache host locale.
  - Se un Cloud Connector si guasta, i VDA di quella zona tentano di registrarsi con altri Cloud Connector locali. Un VDA che si trova in una zona non tenta mai di registrarsi con un Cloud Connector di un'altra zona.
- Se si aggiunge o si rimuove un Cloud Connector in una zona (utilizzando la console di gestione Citrix Cloud) e l'aggiornamento automatico è abilitato, i VDA di quella zona ricevono elenchi aggiornati dei Cloud Connector locali disponibili, in modo che sappiano con chi possono registrarsi e da chi possono accettare le connessioni.
- Se si sposta un catalogo in un'altra zona (utilizzando l'interfaccia di gestione Full Configuration), i VDA del catalogo si registrano nuovamente con i Cloud Connector nella zona in cui è stato spostato il catalogo. Quando si sposta un catalogo, è bene assicurarsi di spostare anche tutte le eventuali connessioni host associate alla stessa zona.
- Durante un'interruzione (quando i Cloud Connector di una zona non possono comunicare con Citrix Cloud), sono disponibili solo le risorse associate alle macchine registrate in quella zona.

## Preferenza di zona

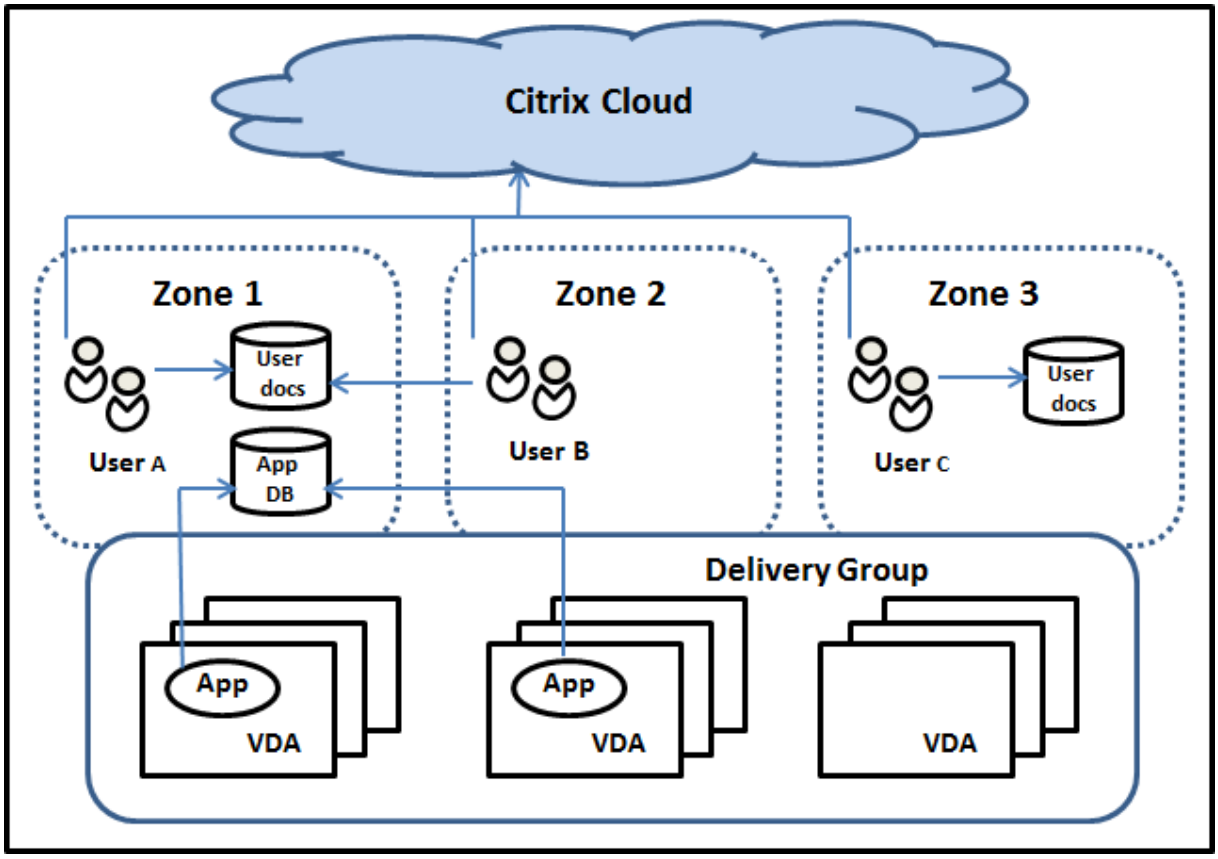
In un sito multi-zona, la funzione di preferenza di zona offre all'amministratore maggiore flessibilità per controllare quale VDA viene utilizzato per avviare un'applicazione o un desktop.

### Come funziona la preferenza di zona

Esistono tre forme di preferenza di zona. Potrebbe essere preferibile utilizzare un VDA in una determinata zona, a seconda dei fattori seguenti:

- Dove sono memorizzati i dati dell'applicazione. Tale posizione viene denominata posizione home dell'applicazione.
- La posizione in cui sono memorizzati i dati home dell'utente, ad esempio un profilo o una condivisione domestica. Questa è denominata home utente.
- La posizione corrente dell'utente (in cui è in esecuzione l'app Citrix Workspace). Questa viene denominata posizione dell'utente. La posizione dell'utente richiede almeno StoreFront 3.7 e Citrix Gateway (precedentemente NetScaler Gateway) 11.0-65.x.

L'immagine seguente mostra un esempio di configurazione multi-zona.




In questo esempio, i VDA sono distribuiti tra tre zone, ma sono tutti nello stesso gruppo di consegna.

Pertanto, il broker Citrix DaaS potrebbe scegliere quale VDA utilizzare per una richiesta di avvio dell'utente. Questo esempio illustra che gli utenti possono eseguire i propri endpoint dell'app Citrix Workspace in posizioni diverse. L'utente A sta utilizzando un dispositivo con l'app Citrix Workspace nella zona 1. L'utente B sta utilizzando un dispositivo nella zona 2. Allo stesso modo, i documenti di un utente possono essere archiviati in posizioni diverse. Gli utenti A e B utilizzano una condivisione situata nella zona 1. L'utente C utilizza una condivisione nella zona 3. Inoltre, una delle applicazioni pubblicate utilizza un database situato nella zona 1.

È possibile associare un utente o un'applicazione a una zona, configurando una zona home per l'utente o l'applicazione. Il broker utilizza quindi tali associazioni per aiutare a selezionare la zona in cui verrà avviata una sessione, se sono disponibili risorse. L'utente deve:

- Configurare la zona home di un utente aggiungendo un utente a una zona.
- Configurare la zona home di un'applicazione modificando le proprietà dell'applicazione.

Un utente o un'applicazione possono disporre di una sola zona home alla volta. Un'eccezione per gli utenti può essere quando vi sono abbonamenti a più zone a causa dell'appartenenza al gruppo di utenti. Tuttavia, anche in questo caso, il broker utilizza una sola zona home.

Sebbene le preferenze di zona per utenti e applicazioni possano essere configurate, il broker seleziona solo una zona preferita per un avvio. L'ordine di priorità predefinito per la selezione della zona preferita è applicazioni home > home utente > posizione utente. Quando un utente avvia un'applicazione:

- Se tale applicazione ha un'associazione di zona configurata (una home dell'applicazione), la zona preferita è la zona home per quell'applicazione.
- Se l'applicazione non dispone di un'associazione di zona configurata, ma ce l'ha l'utente (una home utente), la zona preferita è la zona home di quell'utente.
- Se né l'applicazione né l'utente hanno un'associazione di zona configurate, la zona preferita è la zona in cui l'utente esegue un'istanza dell'app Citrix Workspace (la posizione utente). Se tale zona non è definita, viene utilizzata una selezione casuale di VDA e zona. Viene applicato il bilanciamento del carico a tutti i VDA che si trovano nella zona preferita. Se non esiste una zona preferita, il bilanciamento del carico viene applicato a tutti i VDA che si trovano nel gruppo di consegna.

#### Personalizzare la preferenza della zona

Quando si configura (o si rimuove) una zona home di un utente o un'applicazione, è inoltre possibile limitare ulteriormente il modo in cui viene utilizzata (o meno) la preferenza di zona.

- **Uso obbligatorio della zona home utente:** in un gruppo di consegna, è possibile specificare "Launch the session in the user's home zone (if the user has a home zone), with no failover to a different zone if resources are not available in the home zone."[Avvia la sessione nella zona

home dell'utente (se l'utente ne dispone) senza failover su un'altra zona se la zona home non ha risorse disponibili]. Questa restrizione è utile se si desidera evitare il rischio di copiare profili di grandi dimensioni o file di dati tra una zona e l'altra. In altre parole, quando è preferibile negare l'avvio di una sessione piuttosto che avviare la sessione in un'altra zona.

- **Uso obbligatorio della zona home dell'applicazione:** analogamente, quando si configura una zona home per un'applicazione, è possibile specificare "launch the application only in that zone, with no failover to a different zone if resources are not available in the application's home zone"(Avvia l'applicazione solo in quella zona, senza failover su una zona diversa se non sono disponibili risorse nella zona home dell'applicazione).
- **Nessuna area home dell'applicazione e ignora la zona home utente configurata:** se non si specifica una zona home per un'applicazione, è inoltre possibile specificare "do not consider any configured user zones when launching that application"(non considerare eventuali zone utente configurate quando si avvia quell'applicazione). Ad esempio, utilizzare la preferenza della zona di posizione dell'utente se si desidera che gli utenti eseguano un'applicazione specifica su un VDA vicino alla propria macchina, anche se alcuni utenti potrebbero avere una zona home diversa.

#### In che modo le zone preferite influenzano l'uso della sessione

Quando un utente avvia un'applicazione o un desktop, il broker preferisce utilizzare la zona preferita anziché utilizzare una sessione esistente.

Se l'utente che avvia un'applicazione o un desktop dispone già di una sessione adatta per la risorsa che viene avviata (ad esempio può utilizzare la condivisione di sessione per un'applicazione o una sessione che sta già eseguendo la risorsa che si sta avviando), ma tale sessione è su un VDA in una zona diversa dalla zona preferita per l'utente/applicazione, il sistema potrebbe creare una nuova sessione. Questa azione soddisfa l'avvio nella zona corretta (se questa ha capacità disponibile), prima di riconnettersi a una sessione in una zona meno preferita per i requisiti di sessione di quell'utente.

Per evitare una sessione orfana che non può più essere raggiunta, è consentita la riconnessione alle sessioni disconnesse esistenti, anche se si trovano in una zona non preferita.

L'ordine di desiderabilità perché le sessioni soddisfino un avvio è il seguente:

1. Riconnettere a una sessione esistente nella zona preferita.
2. Riconnettersi a una sessione disconnessa esistente in una zona non preferita.
3. Avviare una nuova sessione nella zona preferita.
4. Riconnettersi a una sessione esistente connessa in una zona non preferita.
5. Avviare una nuova sessione in una zona non preferita.

#### Altre considerazioni sulle preferenze di zona

- Se si configura una zona home per un gruppo di utenti (ad esempio un gruppo di sicurezza), gli utenti di quel gruppo (tramite l'appartenenza diretta o indiretta) vengono associati alla zona specificata. Tuttavia, un utente può essere membro di più gruppi di sicurezza e pertanto potrebbe avere una zona principale diversa configurata tramite l'appartenenza ad altri gruppi. In questi casi, la determinazione della zona home dell'utente può essere ambigua.

  Se un utente dispone di una zona home configurata che non è stata acquisita tramite l'appartenenza al gruppo, tale zona viene utilizzata per le preferenze di zona. Tutte le associazioni di zona acquisite tramite l'appartenenza al gruppo vengono ignorate.

  Se l'utente ha più associazioni di zone diverse acquisite esclusivamente tramite l'appartenenza al gruppo, il broker ne sceglie una in modo casuale. Dopo che il broker ha fatto questa scelta, questa zona viene utilizzata per i successivi avviamenti delle sessioni, fino a quando l'appartenenza al gruppo dell'utente non cambia.

- La preferenza della zona di posizione utente richiede il rilevamento dell'app Citrix Workspace sul dispositivo endpoint da parte del Citrix Gateway attraverso il quale tale dispositivo si sta connettendo. Citrix deve essere configurato per associare intervalli di indirizzi IP a zone particolari. L'identità della zona rilevata deve essere trasferita a Citrix DaaS tramite StoreFront.

Sebbene sia stato scritto per l'uso locale delle zone, il post del blog Elementi interni della preferenza zona contiene dettagli tecnici pertinenti.

### Permessi per gestire le zone

Un amministratore completo può eseguire tutte le attività di gestione delle zone supportate. Lo spostamento di elementi tra le zone non richiede autorizzazioni relative alla zona (a eccezione dell'autorizzazione di lettura della zona). Tuttavia, è necessario disporre dell'autorizzazione di modifica per gli elementi che si stanno spostando. Ad esempio, per spostare un catalogo di macchine da una zona a un'altra, è necessario disporre dell'autorizzazione di modifica per quel catalogo.

**Se si utilizza Citrix Provisioning:** l'attuale console di Citrix Provisioning non tiene conto delle zone, pertanto Citrix consiglia di utilizzare l'interfaccia **Manage > Full Configuration** per creare cataloghi di macchine che si desidera collocare in zone specifiche. Dopo aver creato il catalogo, è possibile utilizzare la console Citrix Provisioning per eseguire il provisioning delle macchine che si trovano in quel catalogo.

### Creazione di zone

Quando si crea una posizione risorsa in Citrix Cloud e quindi vi si aggiunge un Cloud Connector, Citrix DaaS crea automaticamente una zona e le assegna un nome. È possibile aggiungere una descrizione

in un secondo momento.

Dopo aver creato più di una posizione di risorse (e dopo che le zone sono state create automaticamente), è possibile spostare le risorse da una zona all'altra.

Le posizioni e le zone delle risorse vengono sincronizzate periodicamente, in genere circa ogni cinque minuti. Pertanto, se si modifica il nome di una posizione di risorse in Citrix Cloud, tale modifica viene propagata alla zona associata entro cinque minuti.

### Aggiungere o modificare la descrizione di una zona

Sebbene non sia possibile modificare il nome di una zona, è possibile aggiungervi una descrizione e modificarla.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Zones** nel riquadro di sinistra.
2. Selezionare una zona nel riquadro centrale e quindi selezionare **Edit Zone** nella barra delle azioni.
3. Aggiungere o modificare la descrizione della zona.
4. Selezionare **OK** o **Apply**.

### Spostare le risorse da una zona a un'altra

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Zones** nel riquadro di sinistra.
2. Selezionare una zona nel riquadro centrale, quindi selezionare uno o più elementi.
3. Trascinare gli elementi nell'area di destinazione o selezionare **Move Items** (Sposta elementi) nella barra delle azioni, quindi specificare la zona in cui spostarli. Sebbene sia possibile selezionare i Cloud Connector, non è possibile spostarli in una zona diversa.

Un messaggio di conferma elenca gli elementi selezionati e chiede se si è sicuri di volerli spostare tutti.

Ricordare: quando un catalogo di macchine utilizza una connessione host a un hypervisor o a un servizio cloud, assicurarsi che sia il catalogo che la connessione siano nella stessa zona. In caso contrario, le prestazioni potrebbero risentirne. Quando se ne sposta uno, spostare anche l'altro.

### Eliminazione delle zone

Non è possibile eliminare una zona. Tuttavia, è possibile eliminare una posizione di risorse (dopo aver rimosso i suoi Cloud Connector). L'eliminazione della posizione della risorsa comporta l'eliminazione automatica della zona.

- Se la zona non contiene elementi (ad esempio cataloghi, connessioni, applicazioni o utenti), questa viene eliminata durante la successiva sincronizzazione tra le zone e le posizioni di risorse. La sincronizzazione avviene ogni cinque minuti.
- Se contiene elementi, la zona viene eliminata automaticamente dopo che tutti gli elementi sono stati rimossi.

### Aggiungere una zona home per un utente

La configurazione di una zona home per un utente è anche nota come *aggiunta di un utente a una zona*.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Zones** nel riquadro di sinistra.
2. Selezionare una zona nel riquadro centrale e quindi selezionare **Add Users to Zone** (Aggiungi utenti alla zona) nella barra delle azioni.
3. Nella finestra di dialogo **Add Users to Zone** selezionare **Add** e quindi selezionare gli utenti e i gruppi di utenti da aggiungere alla zona. Se si specificano utenti che hanno già una zona home, un messaggio offre due opzioni: **Yes**= aggiungere solo gli utenti specificati che non dispongono di una zona home; **No**= tornare alla finestra di dialogo di selezione utente.
4. Selezionare **OK**.

Per gli utenti che dispongono di una zona home configurata, è possibile richiedere che le sessioni vengano avviate solo dalla loro zona home:

1. Creare o modificare un gruppo di consegna.
2. Nella pagina **Users** (Utenti), selezionare la casella di controllo **Sessions must launch in a user's home zone, if configured** (Le sessioni devono essere avviate nella zona home di un utente, se configurata).

Tutte le sessioni avviate da un utente in quel gruppo di consegna devono essere avviate dai computer nella zona home di quell'utente. Se un utente del gruppo di consegna non dispone di una zona home configurata, questa impostazione non ha alcun effetto.

### Rimuovere una zona home per un utente

Questa procedura è nota anche come rimozione di un utente da una zona.

1. Da **Manage > Full Configuration** (Gestisci > Configurazione completa), selezionare **Zones** nel riquadro di sinistra.
2. Selezionare una zona nel riquadro centrale e quindi selezionare **Remove Users from Zone** (Rimuovi utenti dalla zona) nella barra delle azioni.

3. Nella finestra di dialogo **Add Users to Zone** selezionare **Remove** e quindi selezionare gli utenti e i gruppi da rimuovere dalla zona. Questa azione rimuove solo gli utenti dalla zona. Tali utenti rimangono nei gruppi di consegna a cui appartengono.
4. Confermare la rimozione quando richiesto.

### Gestione delle zone home per le applicazioni

La configurazione di una zona home per un'applicazione è nota anche come aggiunta di un'applicazione a una zona. Per impostazione predefinita, in un ambiente multi-zona, un'applicazione non dispone di una zona principale.

La zona home di un'applicazione è specificata nelle proprietà dell'applicazione. È possibile configurare le proprietà dell'applicazione quando si aggiunge l'applicazione a un gruppo o in seguito.

- Quando si crea un gruppo di consegna o si aggiungono applicazioni a gruppi esistenti, selezionare **Properties** nella pagina **Applications** della procedura guidata.
- Per modificare le proprietà di un'applicazione dopo l'aggiunta dell'applicazione, selezionare **Zones** nel riquadro di sinistra. Selezionare un'applicazione e quindi selezionare **Properties** nella barra delle azioni.

Nella pagina **Zones** delle proprietà/impostazioni dell'applicazione:

- Se si desidera che l'applicazione abbia una zona home:
  - Selezionare il pulsante di opzione **Use the selected zone to decide per decidere** (Usa la zona selezionata) e quindi selezionare la zona.
  - Se si desidera che l'applicazione venga avviata solo dalla zona selezionata (e non da nessun'altra zona), selezionare la casella di controllo sotto la selezione della zona.
- Se non si desidera che l'applicazione disponga di una zona home:
  - Selezionare il pulsante di opzione **Do not configure a home zone** (Non configurare una zona home).
  - Se non si desidera che il broker consideri alcuna delle zone utente configurate all'avvio di questa applicazione, selezionare la casella di controllo sotto il pulsante di opzione. In questo caso, non vengono utilizzate le zone home né dell'applicazione né dell'utente per determinare dove avviare l'applicazione.

### Altre azioni che richiedono di specificare zone

Se si dispone di più zone, è possibile specificare una zona quando si aggiunge una connessione host o si crea un catalogo. Le zone sono elencate in ordine alfabetico negli elenchi di selezione. Per impostazione predefinita, è selezionato il primo nome in ordine alfabetico.

## Risoluzione dei problemi

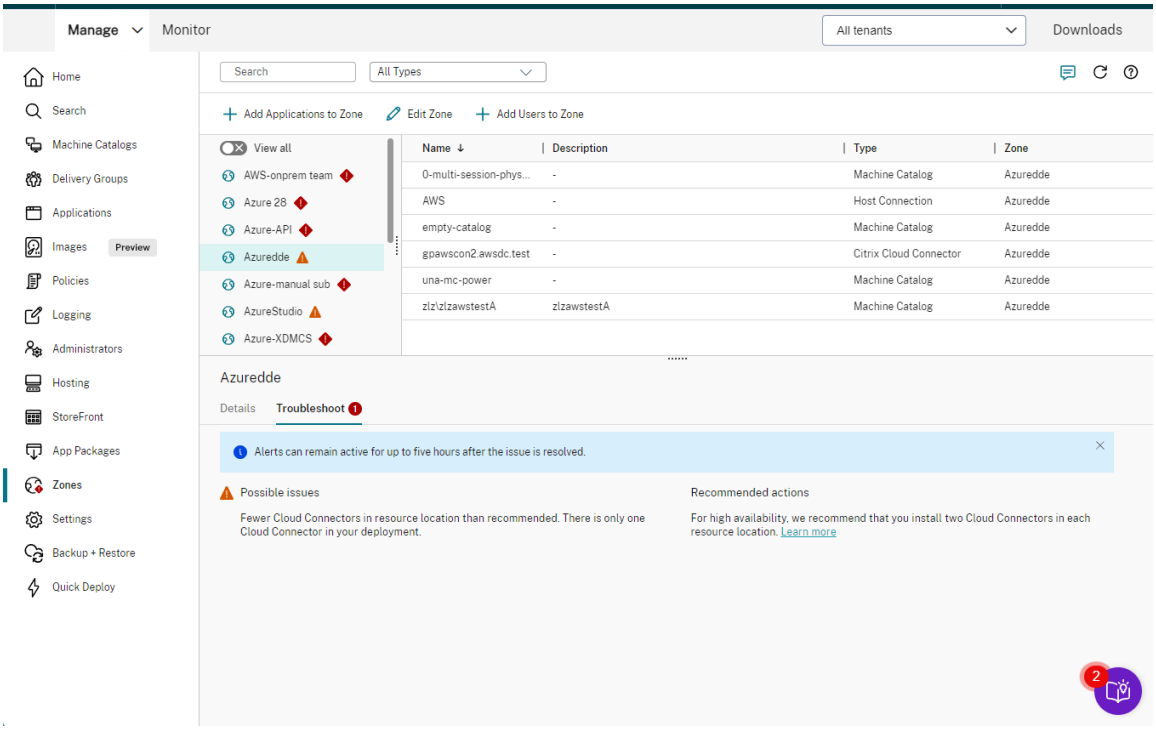
Full Configuration offre avvisi proattivi per garantire che la cache host locale e le zone siano configurate correttamente in modo da poter risolvere i problemi in tempo prima che un'interruzione abbia ripercussioni sugli utenti. Questa funzionalità aiuta a mantenere continuo l'accesso degli utenti ai carichi di lavoro mission critical.

Viene visualizzata una scheda **Troubleshoot** (Risoluzione dei problemi) per ogni zona che presenta problemi.

Per verificare i problemi correlati alle zone, effettuare le seguenti operazioni:

1. Passare a **Full Configuration > Zones** e fare clic sulla zona con l'icona di avviso.
2. Passare alla scheda **Troubleshoot** nel riquadro inferiore e leggere le informazioni che contiene.

> **Nota:**
>
> La diagnostica viene aggiornata ogni ora.
>
> Esempio di informazioni di risoluzione problemi:




La tabella seguente fornisce un elenco completo degli avvisi e degli errori correlati alle zone:

| Gravità | Titolo del problema | Descrizione del problema | Azione consigliata |
|---|---|---|---|
| Avviso | La posizione risorsa contiene più domini | Con più domini in una posizione risorsa, se le relazioni di trust non sono configurate correttamente, la registrazione dei VDA potrebbe richiedere più tempo. Inoltre, i VDA potrebbero non riuscire a registrarsi in modalità ad alta disponibilità. | Assicurarsi che le relazioni di trust tra i domini in questa posizione di risorse siano configurate correttamente. Vedere Citrix Cloud Connector Technical Details. |
| Avviso | Più connessioni host nella posizione risorsa rispetto a quelle consigliate | Il superamento del limite potrebbe comportare un peggioramento delle prestazioni, con conseguente impatto sull'esperienza utente. | Ridurre il numero di connessioni host in questa posizione risorsa a non più del limite consigliato. Vedere Limiti. |
| Avviso | Meno processori CPU logici di quelli consigliati | In modalità ad alta disponibilità, potrebbe verificarsi un peggioramento delle prestazioni. | Assicurarsi che ciascun Cloud Connector soddisfi i requisiti minimi del processore logico della CPU. Vedere Cache host locale. |
| Avviso | Meno Cloud Connector nella posizione delle risorse rispetto a quelli consigliati | Nella propria implementazione è presente un solo Cloud Connector. | Per un'elevata disponibilità, consigliamo di installare due Cloud Connector in ciascuna posizione risorsa. Vedere Citrix Cloud Connector Technical Details. |

| Gravità | Titolo del problema | Descrizione del problema | Azione consigliata |
|---|---|---|---|
| Errore | Numero di VDA nella posizione delle risorse superiore a quello consigliato | In modalità ad alta disponibilità, la cache host locale consente la registrazione di soli 10.000 VDA. I tentativi di registrazione da parte di VDA aggiuntivi non riusciranno. | Ridurre il numero di VDA in questa posizione risorsa a non più del limite consigliato. Vedere Limiti. |
| Errore | I Cloud Connector nella zona non sono raggiungibili. | Nessuno dei Cloud Connector della zona è raggiungibile. I VDA di questa posizione di risorse potrebbero non essere disponibili a meno che la cache host locale o la continuità del servizio non siano configurati per la distribuzione. | Controllare la connettività dei Cloud Connector nella zona e controllare nel registro se la modalità LHC è forzata tramite il registro. Se il registro non forza l'LHC, prendere in considerazione l'esecuzione della Cloud Connector Connectivity Check Utility. Se il problema persiste, aprire un ticket di supporto. |

## Monitoraggio

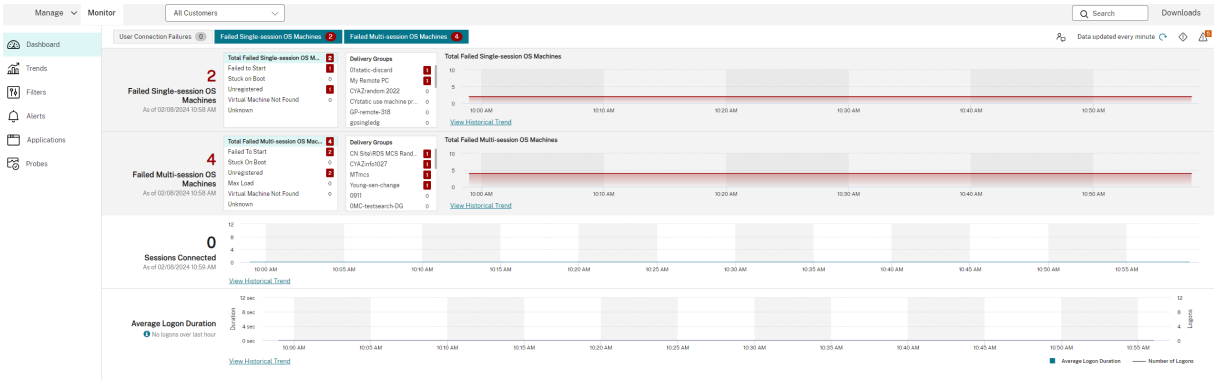
October 6, 2022

Gli amministratori e il personale dell'helpdesk possono monitorare Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) da **Monitor**, la console di monitoraggio e risoluzione dei problemi. La scheda **Monitor** visualizza una dashboard per monitorare, risolvere i problemi ed eseguire attività di supporto per gli abbonati.

> **Nota:**
>
> Monitor è disponibile come console Director per monitorare e risolvere i problemi delle implementazioni di Citrix Virtual Apps and Desktops versione corrente e LTSR .

Per accedere a **Monitor**, effettuare l'accesso a Citrix Cloud. Nel menu in alto a sinistra, selezionare **My Services > DaaS** (I miei servizi > DaaS). Fare clic su **Monitor**.




> **Nota:**
>
> La risoluzione ottimale dello schermo consigliata per la visualizzazione di Monitor è 1366 x 1024.

Il monitor offre:

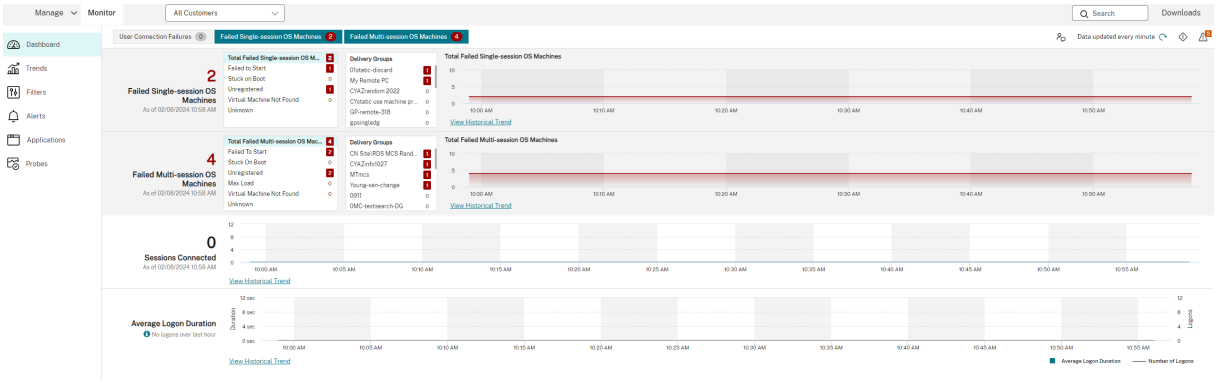
- Dati in tempo reale provenienti dal Broker Agent mediante una console unificata integrata con Analytics e Performance Manager.
- Analisi, comprendente la gestione delle prestazioni per la garanzia del funzionamento e della capacità e le tendenze storiche per identificare i colli di bottiglia dell'ambiente Citrix DaaS.
- Dati storici memorizzati nel database Monitor per accedere al database di registrazione della configurazione.
- Visibilità sull'esperienza dell'utente finale per applicazioni virtuali, desktop e utenti per Citrix DaaS.
- Monitor utilizza una dashboard di risoluzione dei problemi che fornisce il monitoraggio storico e in tempo reale dello stato di Citrix DaaS. Questa funzione consente di vedere i guasti in tempo reale, fornendo una migliore idea dell'esperienza degli utenti finali.

## Analisi del sito

January 18, 2023

La dashboard Monitor fornisce una posizione centralizzata per monitorare lo stato e l'utilizzo di un sito.



Se al momento non ci sono errori e non si sono verificati errori negli ultimi 60 minuti, i pannelli rimangono compressi. In caso di errori, viene visualizzato automaticamente il pannello dell'errore specifico.

| Pannello | Descrizione |
| --- | --- |
| User Connection Failures (Errori di connessione utente) | Errori di connessione negli ultimi 60 minuti. Fare clic sulle categorie accanto al numero totale per visualizzare le metriche per quel tipo di errore. Nella tabella adiacente, tale numero viene suddiviso per gruppi di consegna. Gli errori di connessione includono errori causati dal raggiungimento dei limiti dell'applicazione. Per ulteriori informazioni sui limiti delle applicazioni, vedere Applicazioni. |
| Failed Single-session OS Machines (Macchine con sistema operativo a sessione singola che presentano errori) o Failed Multi-session OS Machines (Macchine con sistema operativo multisessione che presentano errori) | Errori totali negli ultimi 60 minuti suddivisi per gruppi di consegna. Errori suddivisi per tipo, tra cui avvio non riuscito, blocco all'avvio e mancata registrazione. Per le macchine con sistema operativo multisessione, gli errori includono anche le macchine che raggiungono il carico massimo. |
| Sessions Connected (Sessioni connesse) | Sessioni connesse per tutti i gruppi di consegna negli ultimi 60 minuti. |
| Average Logon Duration (Durata media dell'accesso) | Dati di accesso per gli ultimi 60 minuti. Il numero elevato a sinistra è la durata media dell'accesso nel corso dell'ora. I dati di accesso per VDA precedenti a XenDesktop 7.0 non sono inclusi in questa media. Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti. |

> **Nota:**
>
> Se non viene visualizzata alcuna icona per una determinata metrica, questo indica che tale metrica non è supportata dal tipo di host in uso. Ad esempio, non sono disponibili informazioni sullo stato per gli host System Center Virtual Machine Manager (SCVMM), AWS e CloudStack.

Continuare a risolvere i problemi utilizzando queste opzioni (che sono documentate di seguito):

- Controllare l'alimentazione della macchina dell'utente
- Prevent connections to machines (Impedisci le connessioni alle macchine)

### Monitorare le sessioni

Se una sessione viene disconnessa, è ancora attiva e le relative applicazioni continuano a essere eseguite, ma il dispositivo utente non comunica più con il server.

| Azione | Descrizione |
| --- | --- |
| Visualizzare la macchina o la sessione di un utente attualmente connesso | Dalle viste Activity Manager (Gestione attività) e User Details (Dettagli utente), visualizzare la macchina o la sessione attualmente connessa dell'utente e un elenco di tutte le macchine e le sessioni a cui l'utente ha accesso. Per accedere a questo elenco, fare clic sull'icona del commutatore di sessione nella barra del titolo dell'utente. Per ulteriori informazioni, vedere Ripristinare le sessioni. |
| Visualizzare il numero totale di sessioni connesse in tutti i gruppi di consegna | Dalla dashboard, nel riquadro **Sessions Connected** (Sessioni connesse), visualizzare il numero totale di sessioni connesse in tutti i gruppi di consegna negli ultimi 60 minuti. Quindi, fare clic sul numero totale elevato, che apre la vista Filters (Filtri), in cui è possibile visualizzare i dati della sessione sotto forma di grafici in base ai gruppi di consegna e agli intervalli selezionati e all'utilizzo nei gruppi di consegna. |

| Azione | Descrizione |
| --- | --- |
| Terminare le sessioni inattive | La vista Sessions Filters (Filtri sessioni) visualizza i dati relativi a tutte le sessioni attive. Filtrare le sessioni in base all'utente associato, al gruppo di consegna, allo stato della sessione e al tempo di inattività superiore a un periodo di soglia. Dall'elenco filtrato, selezionare le sessioni da scollegare o disconnettere. Per ulteriori informazioni, vedere Risolvere i problemi relativi alle applicazioni. |
| Visualizza i dati per un periodo più lungo | Nella vista Trends (Tendenze), selezionare la scheda **Sessions** (Sessioni) per eseguire il drill down dei dati di utilizzo più specifici per le sessioni connesse e disconnesse per un periodo di tempo più lungo (ovvero i totali delle sessioni precedenti agli ultimi 60 minuti). Per visualizzare queste informazioni, fare clic su **View historical trends** (Visualizza tendenze storiche). |

> **Nota:**
>
> Se il dispositivo utente esegue un Virtual Delivery Agent (VDA) legacy, ad esempio un VDA precedente alla versione 7 o un VDA Linux, Monitor non è in grado di visualizzare informazioni complete sulla sessione. Visualizza invece un messaggio che indica che le informazioni non sono disponibili.

**Limitazione delle regole di assegnazione del desktop** la console di gestione consente l'assegnazione di più regole di assegnazione del desktop (DAR) per utenti o gruppi di utenti diversi a un singolo VDA nel gruppo di consegna. StoreFront visualizza il desktop assegnato con il **Display Name** (Nome visualizzato) corrispondente in base al DAR dell'utente che ha effettuato l'accesso. Tuttavia, Monitor non supporta le DAR e visualizza il desktop assegnato utilizzando il nome del gruppo di consegna indipendentemente dall'utente connesso. Di conseguenza, non è possibile mappare un desktop specifico a una macchina in Monitor.

È possibile mappare il desktop assegnato visualizzato in StoreFront al nome del gruppo di consegna visualizzato in Monitor utilizzando il seguente comando PowerShell. Eseguire il comando PowerShell utilizzando l'SDK Remote PowerShell come descritto nel blog.

| | | | |
|---|---|---|---|
| Get-BrokerDesktopGroup | Where-Object { $_.Uid -eq (Get-BrokerAssignmentPolicyRule).DesktopGroupUid } | Where-Object { $_.PublishedName -eq "[1]" } | Select-Object -Property Name, Uid |

**Disabilitare la visibilità delle applicazioni in esecuzione in Activity Manager**

Per impostazione predefinita, Activity Manager visualizza un elenco di tutte le applicazioni in esecuzione per la sessione di un utente. Queste informazioni possono essere visualizzate da tutti gli amministratori che hanno accesso alla funzionalità Activity Manager. Per i ruoli Delegated Administrator (Amministratore delegato) sono compresi i ruoli Full Administrator (Amministratore completo), Delivery Group Administrator (Amministratore del gruppo di consegna) e Help Desk Administrator (Amministratore dell'helpdesk).

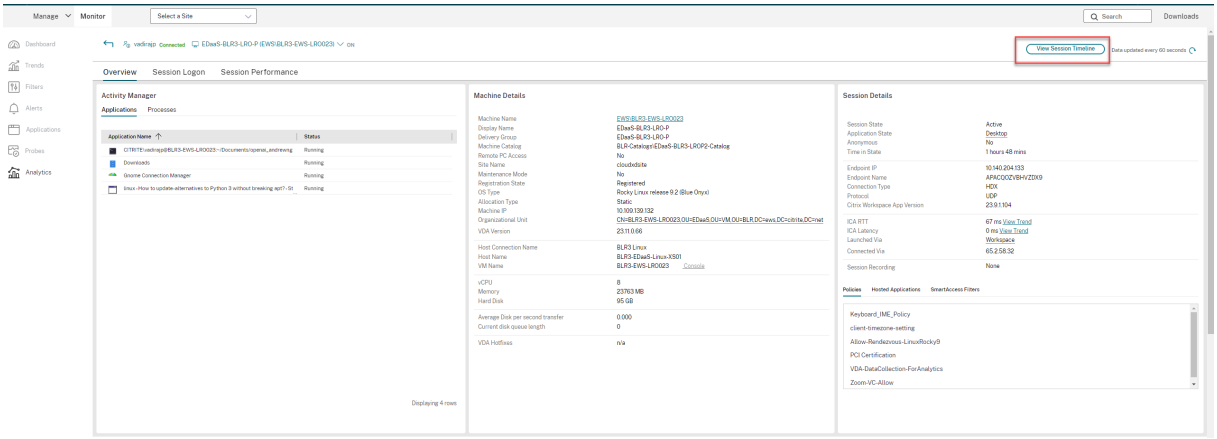
Per proteggere la privacy degli utenti e delle applicazioni che eseguono, è possibile disattivare l'elenco delle applicazioni in esecuzione nella scheda Applications. A questo scopo, sul VDA, modificare la chiave del Registro di sistema in HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. Per impostazione predefinita, la chiave è impostata su 1. Modificare il valore su 0, il che significa che le informazioni non vengono raccolte dal VDA e quindi non vengono visualizzate in Activity Manager (Gestione attività).

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

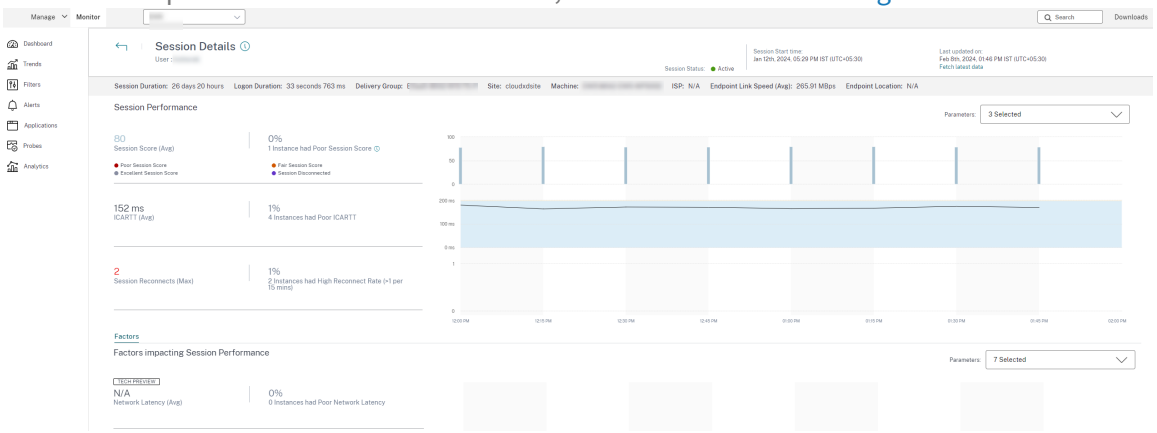
**Accedere a Citrix Analytics for Performance - Session Details (Dettagli della sessione)**

È possibile accedere alla pagina Session Details (Dettagli della sessione) di Citrix Analytics for Performance da Monitor. Fare clic su **View Session Timeline** (Visualizza cronologia della sessione) nella sezione Sessions Details di Activity Manager per aprire la pagina dei dettagli delle sessioni di Citrix Analytics for Performance in Monitor.



> **Nota:**
>
> questa funzione richiede che si disponga di un'autorizzazione valida per Citrix Analytics for Performance.
>
> I dettagli della sessione sono disponibili per le sessioni classificate da Citrix Analytics for Performance come eccellenti, accettabili o scadenti. Per ulteriori informazioni sui motivi per cui una sessione potrebbe non essere classificata, vedere l'articolo Not Categorized.



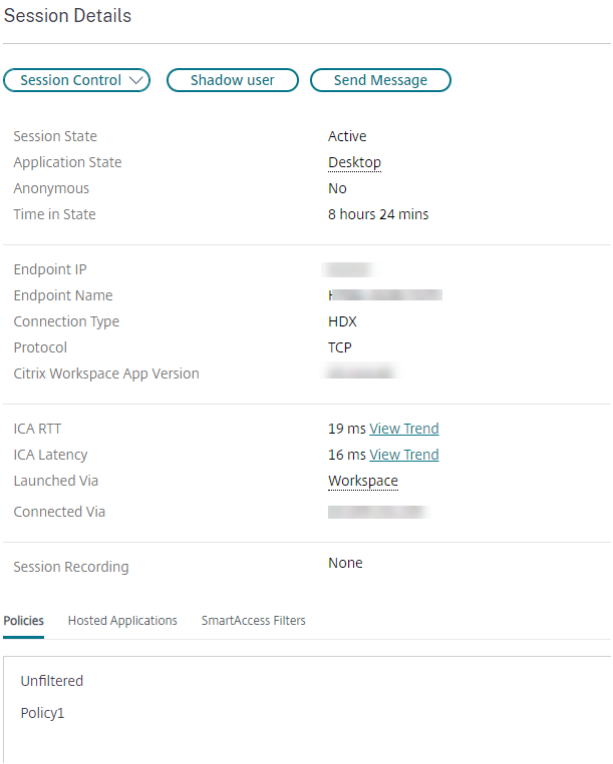
È possibile visualizzare l'andamento dell'esperienza di sessione per un massimo di tre giorni insieme ai fattori che contribuiscono all'esperienza della sessione. Queste informazioni integrano i dati in tempo reale disponibili in Monitor, utilizzati dall'amministratore dell'help desk per la risoluzione dei problemi relativi all'esperienza di sessione.

Per ulteriori informazioni sulla pagina Dettagli della sessione, vedere Session Details.

### Protocollo di trasporto della sessione

Visualizzare il protocollo di trasporto in uso per il tipo di connessione HDX per la sessione corrente nel pannello **Session Details** (Dettagli sessione). Queste informazioni sono disponibili per le sessioni avviate sui VDA versione 7.13 o successiva.




Utilizzare l'elenco a discesa Controllo sessione nel riquadro **Dettagli sessione** per scollegarsi o disconnettere una sessione.

- Per il tipo di connessione **HDX**:
  - Il protocollo viene visualizzato come **UDP** se viene utilizzato EDT per la connessione HDX.
  - Il protocollo viene visualizzato come **TCP** se viene utilizzato TCP per la connessione HDX.
- Per il tipo di connessione **RDP**, il protocollo viene visualizzato come **n/a** (n/d).

Quando è configurato il trasporto adattivo, il protocollo di trasporto della sessione passa dinamicamente da EDT (su UDP) a TCP e viceversa, in base alle condizioni di rete. Se la sessione HDX non può essere stabilita utilizzando EDT, ritorna al protocollo TCP.

Per ulteriori informazioni sulla configurazione del trasporto adattivo, vedere Trasporto adattivo.

## Esportare i report

È possibile esportare i dati delle tendenze per generare rapporti regolari di utilizzo e gestione della capacità. L'esportazione supporta i formati di report PDF, Excel e CSV. I report in formato PDF ed Excel contengono tendenze rappresentate come grafici e tabelle. I report in formato CSV contengono dati tabulari che possono essere elaborati per generare viste o possono essere archiviati.

Per esportare un report:

1. Andare alla scheda **Trends** (Tendenze).
2. Impostare i criteri del filtro e il periodo di tempo e fare clic su **Apply** (Applica). Il grafico e la tabella delle tendenze vengono popolati con dati.
3. Fare clic su **Export** (Esporta) e immettere il nome e il formato del report.

Monitor genera il report in base ai criteri del filtro selezionati. Se si modificano i criteri del filtro, fare clic su **Apply** (Applica) prima di fare clic su **Export** (Esporta).

> **Nota:**
>
> L'esportazione di una grande quantità di dati provoca un aumento significativo del consumo di memoria e CPU sul server di Monitor, sul Delivery Controller e sui server SQL. Il numero supportato di operazioni di esportazione simultanee e la quantità di dati che è possibile esportare sono impostati su limiti predefiniti per ottenere prestazioni ottimali per l'esportazione.

#### Limiti di esportazione supportati

I report PDF ed Excel esportati contengono grafici completi per i criteri del filtro selezionati. Tuttavia, i dati tabulari in tutti i formati di report vengono troncati oltre i limiti predefiniti per il numero di righe o record nella tabella. Il numero predefinito di record supportati è definito in base al formato del report.

| Formato del report | Numero predefinito di record supportati |
|---|---|
| PDF | 500 |
| Excel | 100,000 |
| CSV | 100.000 (10.000.000 nella scheda **Sessions** [Sessioni]) |

#### Gestione degli errori

Errori che si potrebbero riscontrare durante un'operazione di esportazione:

- **Director has timed out** (Timeout di Director): questo errore può verificarsi a causa di problemi di rete o di utilizzo elevato delle risorse sul server di Director o con il servizio di monitoraggio.
- **Monitor has timed out:** (Timeout di Monitor): questo errore potrebbe verificarsi a causa di problemi di rete o di utilizzo elevato delle risorse con il servizio di monitoraggio o sul server SQL.

- **Max concurrent Export or Preview operations ongoing** (Max operazioni simultanee di esportazione o anteprima in corso): solo un'istanza di esportazione o anteprima può essere eseguita in un momento specifico. Se viene visualizzato l'errore **Max concurrent Export or Preview operations ongoing**, riprovare la successiva operazione in un secondo momento.

### Aggiornamenti rapidi per il monitor

Per visualizzare gli aggiornamenti rapidi installati su una specifica macchina VDA (fisica o VM), scegliere la vista **Machine Details** (Dettagli macchina).

### Controllare gli stati di alimentazione della macchina utente

Per controllare lo stato delle macchine selezionate in Monitor, utilizzare le opzioni Power Control (Controllo dell'alimentazione). Queste opzioni sono disponibili per le macchine con sistema operativo a sessione singola, ma potrebbero non essere disponibili per le macchine con sistema operativo multisessione.

> **Nota:**
>
> Questa funzionalità non è disponibile per macchine fisiche o macchine che utilizzano Remote PC Access (Accesso remoto PC).

| Comando | Funzione |
| --- | --- |
| **Restart (Riavvia)** | Esegue un arresto ordinato della VM e tutti i processi in esecuzione vengono arrestati singolarmente prima di riavviare la VM. Ad esempio, selezionare le macchine che appaiono in Monitor come "Failed to start"(Impossibile eseguire l'avvio) e utilizzare questo comando per riavviarle. |
| **Force Restart (Forza riavvio)** | Riavvia la VM senza prima eseguire alcuna procedura di arresto. Questo comando equivale a scollegare un server fisico dalla corrente, quindi a ricollegarlo e riaccenderlo. |
| **Shut Down (Arresta)** | Esegue un arresto ordinato della VM. Tutti i processi in esecuzione vengono interrotti singolarmente. |

| Comando | Funzione |
| --- | --- |
| **Force Shutdown (Imponi arresto)** | Spegne la VM senza prima eseguire alcuna procedura di arresto. Questo comando equivale a scollegare un server fisico dalla corrente. Potrebbe non sempre arrestare tutti i processi in esecuzione e se si spegne una VM in questo modo si rischia di perdere dati. |
| **Suspend** | Sospende una VM in esecuzione nello stato corrente e memorizza tale stato in un file nel repository di archiviazione predefinito. Questa opzione consente di spegnere il server host della VM e successivamente, dopo il riavvio, riattivare la VM, riportandola allo stato di esecuzione originale. |
| **Resume** (Riprendi) | Riprende una VM sospesa e ripristina lo stato di esecuzione originale. |
| **Start (Avvia)** | Avvia una VM quando è spenta (chiamato anche avvio a freddo). |

Se le azioni di controllo dell'alimentazione non vanno a buon fine, passare il mouse sopra l'avviso e viene visualizzato un messaggio a comparsa con i dettagli dell'errore.

### Prevent connections to machines (Impedisci le connessioni alle macchine)

Utilizzare la modalità di manutenzione per impedire temporaneamente nuove connessioni mentre l'amministratore appropriato esegue attività di manutenzione sull'immagine.

Quando si abilita la modalità di manutenzione sulle macchine, non sono consentite nuove connessioni fino a quando non viene disabilitata. Se gli utenti sono attualmente connessi, la modalità di manutenzione ha effetto non appena tutti gli utenti vengono disconnessi. Per gli utenti che non si disconnettono, inviare un messaggio che li informa che le macchine verranno spente in un determinato momento e utilizzare i controlli di alimentazione per forzare l'arresto delle macchine.

1. Selezionare la macchina, ad esempio dalla vista User Details (Dettagli utente), o un gruppo di macchine nella vista Filters (Filtri).
2. Selezionare **Maintenance Mode** (Modalità di manutenzione) e attivare l'opzione.

Se un utente tenta di connettersi a un desktop assegnato mentre è in modalità di manutenzione, viene visualizzato un messaggio che indica che il desktop non è attualmente disponibile. Non è possibile stabilire nuove connessioni fino a quando non si disabilita la modalità di manutenzione.

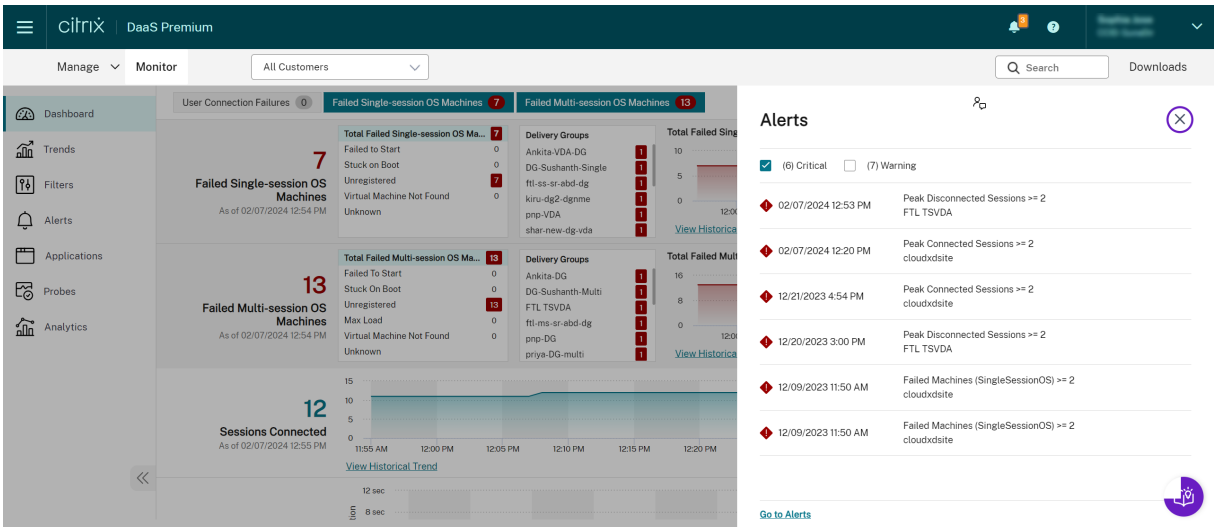
### Analisi delle applicazioni

La scheda **Applications** (Applicazioni) visualizza le analisi basate sulle applicazioni in un'unica vista consolidata per facilitare l'analisi e la gestione efficienti delle prestazioni delle applicazioni. È possibile ottenere importanti dettagli approfonditi sulle informazioni sullo stato e sull'utilizzo di tutte le applicazioni pubblicate sul sito. Questa scheda mostra metriche come i risultati del probe, il numero di istanze per applicazione e gli errori e i guasti associati alle applicazioni pubblicate. Per ulteriori informazioni, vedere la sezione Analisi delle applicazioni in **Risolvere i problemi relativi alle applicazioni**.

## Avvisi e notifiche

November 21, 2023

Gli avvisi vengono visualizzati in Monitor nella dashboard e in altre viste di alto livello con simboli di avvertimento e avviso critico. Gli avvisi si aggiornano automaticamente ogni minuto; è inoltre possibile aggiornarli su richiesta.



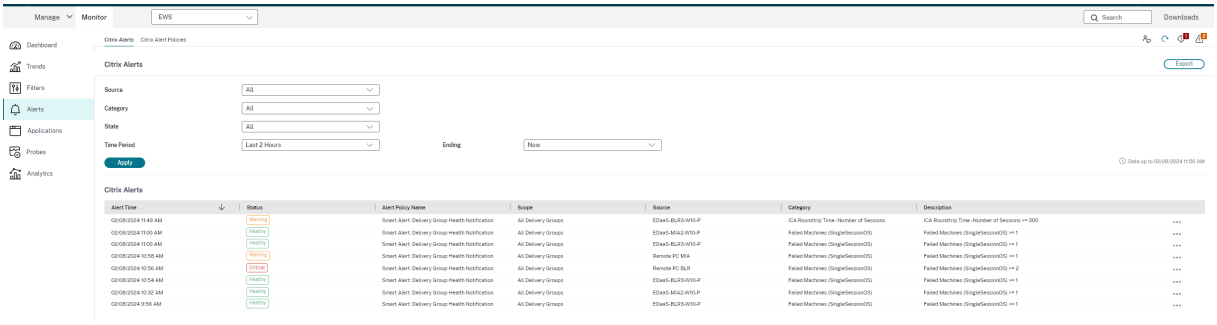

Un avviso di avvertimento (triangolo ambrato) indica che la soglia di avvertimento di una condizione è stata raggiunta o superata.

Un avviso critico (cerchio rosso) indica che la soglia critica di una condizione è stata raggiunta o superata.

È possibile visualizzare informazioni più dettagliate sugli avvisi selezionando un avviso dalla barra laterale, facendo clic sul collegamento **Go to Alerts** (Vai agli avvisi) nella parte inferiore della barra laterale o selezionando **Alerts** (Avvisi) nella parte superiore della pagina di Monitor.

Nella vista Alerts (Avvisi), è possibile filtrare ed esportare avvisi. Ad esempio, è possibile filtrare le macchine con sistema operativo multisessione che presentano problemi per un gruppo di consegna specifico nell'ultimo mese o tutti gli avvisi per un utente specifico. Per ulteriori informazioni, vedere Esportare i report.




## Avvisi Citrix

Gli avvisi Citrix sono quelli che provengono dai componenti Citrix. È possibile configurare gli avvisi Citrix in Monitor in **Alerts** (Avvisi) > **Citrix Alerts Policy** (Criterio per gli avvisi Citrix). Come parte della configurazione, è possibile impostare notifiche da inviare via e-mail a individui e gruppi quando gli avvisi superano le soglie impostate. Per ulteriori informazioni sulla configurazione di Citrix Alerts, vedere Creare criteri per gli avvisi.

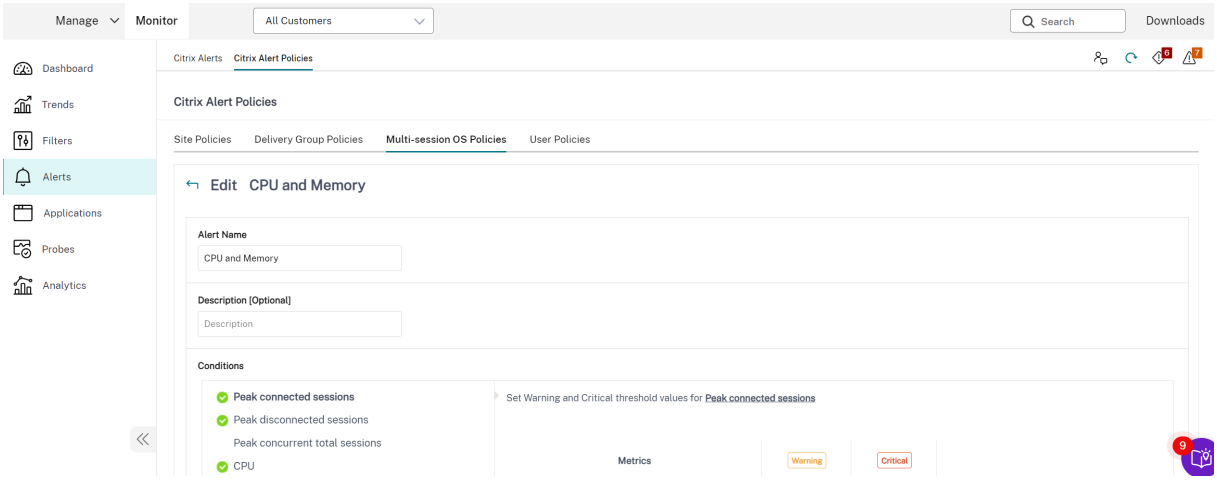
## Criteri intelligenti per gli avvisi

È disponibile un set di criteri incorporati per gli avvisi con valori di soglia predefiniti per i gruppi di consegna e l'ambito dei VDA con sistema operativo multisessione. È possibile modificare i parametri di soglia dei criteri incorporati per gli avvisi in **Alerts** (Avvisi) > **Citrix Alerts Policy** (Criterio per gli avvisi Citrix).
Questi criteri vengono creati quando è presente almeno un target per gli avvisi: un gruppo di consegna o un VDA con sistema operativo multisessione definito nel sito. Inoltre, questi avvisi incorporati vengono aggiunti automaticamente a un nuovo gruppo di consegna o a un VDA con sistema operativo multisessione.

I criteri incorporati per gli avvisi vengono creati solo se non esistono regole di avviso corrispondenti nel database di monitoraggio.

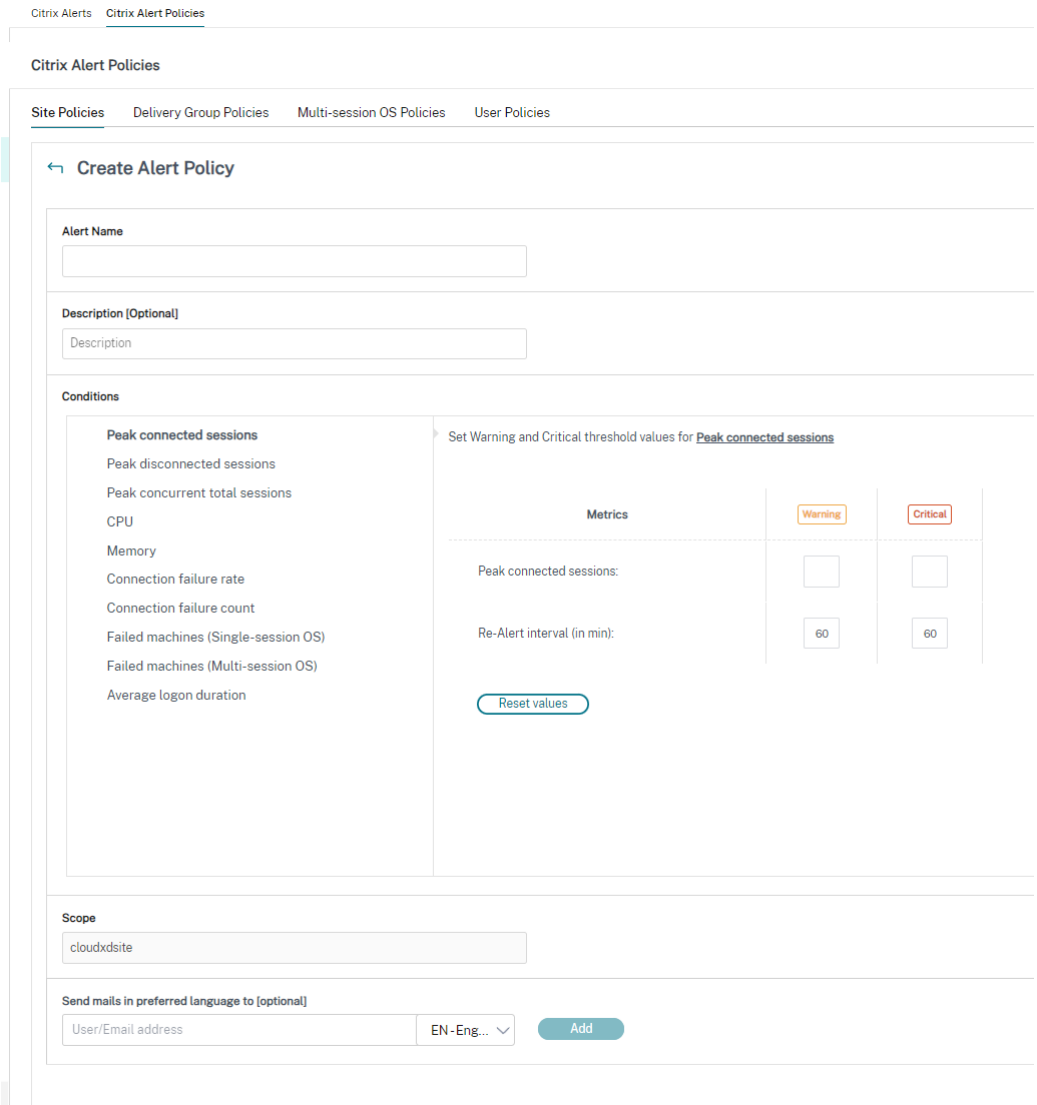
Per i valori di soglia dei criteri per gli avvisi incorporati, vedere la sezione Condizioni dei criteri per gli avvisi.



## Creare criteri per gli avvisi




Per creare un nuovo criterio per gli avvisi, ad esempio per generare un avviso quando viene soddisfatta una serie specifica di criteri di conteggio delle sessioni:

1. Andare ad **Alerts** (Avvisi) > **Citrix Alerts Policy** (Criterio per gli avvisi Citrix) e selezionare, ad esempio, Multi-session OS Policy (Criterio del sistema operativo multisessione).
2. Fare clic su **Create**.
3. Assegnare un nome al criterio e descriverlo, quindi impostare le condizioni che devono essere soddisfatte per l'attivazione dell'avviso. Ad esempio, specificare i conteggi Warning (Avvertimento) e Critical (Critico) per Peak Connected Sessions (Sessioni di picco connesse), Peak Disconnected Sessions (Sessioni di picco disconnesse) e Peak Concurrent Total Sessions (Sessioni di picco simultanee totali). I valori di avvertimento non devono essere superiori ai valori di avviso critico. Per ulteriori informazioni, vedere Condizioni dei criteri per gli avvisi.

4. Impostare l'intervallo Re-alert (Visualizza nuovamente avviso). Se le condizioni per l'avviso sono ancora soddisfatte, l'avviso viene riattivato a questo intervallo di tempo e viene generata una notifica via e-mail, se impostata nel criterio di avviso. Un avviso ignorato non genera una notifica via e-mail all'intervallo di riavviso.
5. Impostare il campo Scope (Ambito). Ad esempio, impostare un gruppo di consegna specifico.
6. In Notification preferences (Preferenze di notifica), specificare chi deve essere avvisato via e-mail quando viene attivato l'avviso. Le notifiche e-mail vengono inviate tramite SendGrid. Assicurarsi che l'indirizzo email "donotreplynotifications@citrix.com"sia inserito nella white-list della configurazione e-mail.
7. Fare clic su **Salva**.

La creazione di un criterio con 20 o più gruppi di consegna definiti in Scope (Ambito) potrebbe richiedere circa 30 secondi per completare la configurazione. Durante questo periodo viene visualizzata una rotellina.

La creazione di più di 50 criteri per un massimo di 20 gruppi di consegna univoci (1000 target di gruppi di consegna in totale) potrebbe comportare un aumento del tempo di risposta (oltre 5 secondi).

Lo spostamento di una macchina contenente sessioni attive da un gruppo di consegna a un altro potrebbe causare avvisi errati del gruppo di consegna definiti utilizzando i parametri della macchina.

> **Nota:**
> dopo aver eliminato un criterio di avviso, potrebbero essere necessari fino a 30 minuti prima che le notifiche di avviso generate dalla politica si interrompano.

## Condizioni dei criteri per gli avvisi

Di seguito sono riportate le categorie di avvisi, le azioni consigliate per mitigare l'avviso e le condizioni dei criteri incorporate, se definite. I criteri incorporati per gli avvisi sono definiti per intervalli di avviso e riavviso di 60 minuti.

### Peak Connected Sessions (Sessioni di picco connesse)

- Controllare la vista Monitor Session Trends (Tendenze della sessione di Monitor) per verificare se sono presenti sessioni di picco connesse.
- Verificare che vi sia capacità sufficiente per supportare il carico della sessione.
- Aggiungere nuove macchine, se necessario.

**Peak Disconnected Sessions (Sessioni di picco disconnesse)**

- Controllare la vista Monitor Session Trends (Tendenze della sessione di Monitor) per verificare se sono presenti sessioni di picco disconnesse.
- Verificare che vi sia capacità sufficiente per supportare il carico della sessione.
- Aggiungere nuove macchine, se necessario.
- Disconnettere le sessioni disconnesse, se necessario.

**Peak Concurrent Total Sessions (Sessioni di picco simultanee totali)**

- Controllare la vista Monitor Session Trends (Tendenze della sessione di Monitor) per verificare se sono presenti sessioni di picco simultanee.
- Verificare che vi sia capacità sufficiente per supportare il carico della sessione.
- Aggiungere nuove macchine, se necessario.
- Disconnettere le sessioni disconnesse, se necessario.

**CPU**

La percentuale di utilizzo della CPU indica il consumo complessivo della CPU sul VDA, incluso quello dei processi. È possibile ottenere maggiori informazioni sull'utilizzo della CPU da parte dei singoli processi dalla pagina **Machine details** (Dettagli macchina) del VDA corrispondente.

- Andare a **Machine Details (Dettagli macchina) > View Historical Utilization (Visualizza utilizzo storico) > Top 10 Processes (Primi 10 processi)** e identificare i processi che consumano CPU. Assicurarsi che il criterio di monitoraggio dei processi sia abilitato per avviare la raccolta delle statistiche sull'utilizzo delle risorse a livello di processo.
- Terminare il processo, se necessario.
- L'interruzione del processo causa la perdita dei dati non salvati.
- Se tutto funziona come previsto, aggiungere altre risorse CPU in futuro.

  > **Nota:**
  >
  > L'impostazione dei criteri **Enable resource monitoring** (Abilita il monitoraggio delle risorse) è consentita per impostazione predefinita per il monitoraggio dei contatori delle prestazioni della CPU e della memoria su macchine con VDA. Se questa impostazione dei criteri è disabilitata, gli avvisi con condizioni relative alla CPU e alla memoria non vengono attivati. Per ulteriori informazioni, vedere Impostazioni dei criteri di monitoraggio.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione

- **Threshold values** (Valori soglia): Warning (Avvertimento) - 80%, Critical (Avviso critico) - 90%

#### Memory (Memoria)

La percentuale di utilizzo della memoria indica il consumo complessivo di memoria sul VDA, incluso quello dei processi. È possibile ottenere maggiori informazioni sull'utilizzo della memoria da parte dei singoli processi dalla pagina **Machine details** (Dettagli macchina) del VDA corrispondente.

- Andare a **Machine Details (Dettagli macchina) > View Historical Utilization (Visualizza utilizzo storico) > Top 10 Processes (Primi 10 processi)** e identificare i processi che consumano memoria. Assicurarsi che il criterio di monitoraggio dei processi sia abilitato per avviare la raccolta delle statistiche sull'utilizzo delle risorse a livello di processo.
- Terminare il processo, se necessario.
- L'interruzione del processo causa la perdita dei dati non salvati.
- Se tutto funziona come previsto, aggiungere ulteriore memoria in futuro.

> **Nota:**
>
> L'impostazione dei criteri **Enable resource monitoring** (Abilita monitoraggio delle risorse) è consentita per impostazione predefinita per il monitoraggio dei contatori delle prestazioni della CPU e della memoria sulle macchine con VDA. Se questa impostazione dei criteri è disabilitata, gli avvisi con condizioni relative alla CPU e alla memoria non vengono attivati. Per ulteriori informazioni, vedere Impostazioni dei criteri di monitoraggio.

**Condizioni dei criteri intelligenti:**

- **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
- **Threshold values** (Valori soglia): Warning (Avvertimento) - 80%, Critical (Avviso critico) - 90%

#### Connection Failure Rate (Frequenza dei problemi di connessione)

Percentuale di problemi di connessione nell'ultima ora.

- Calcolata in base al totale delle connessioni non riuscite rispetto al numero totale di tentativi di connessione.
- Controllare la vista Monitor Connection Failures Trend (Tendenze degli errori di connessione di Monitor) per visualizzare gli eventi registrati dal log di configurazione.
- Determinare se le applicazioni o i desktop sono raggiungibili.

#### Connection Failure Count (Conteggio degli errori di connessione)

Numero di problemi di connessione nell'ultima ora.

- Controllare la vista Monitor Connection Failures Trend (Tendenze degli errori di connessione di Monitor) per visualizzare gli eventi registrati dal log di configurazione.
- Determinare se le applicazioni o i desktop sono raggiungibili.

#### ICA RTT (Average) (Tempo di round trip ICA [media])

Tempo medio di round trip ICA.

- Controllare Citrix ADM per i dettagli del tempo di round trip ICA, per determinare la causa principale. Per ulteriori informazioni, vedere la documentazione di Citrix ADM.
- Se Citrix ADM non è disponibile, controllare la vista Monitor User Details (Dettagli utente di Monitor) per il tempo di round trip ICA e la latenza e per determinare se si tratta di un problema di rete o di un problema delle applicazioni o dei desktop.

#### ICA RTT (No. of Sessions) (Tempo di round trip ICA [numero di sessioni])

Numero di sessioni che superano la soglia per il tempo di round trip ICA.

- Controllare Citrix ADM per visualizzare il numero di sessioni con tempo di round trip ICA elevato. Per ulteriori informazioni, vedere la documentazione di Citrix ADM.
- Se Citrix ADM non è disponibile, rivolgersi al team di rete per determinare la causa principale.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento): 300 ms per 5 o più sessioni, Critical (Avviso critico): 400 ms per 10 o più sessioni

#### ICA RTT (% of Sessions) (Tempo di round trip ICA [% delle sessioni])

Percentuale di sessioni che superano il tempo medio di round trip ICA.

- Controllare Citrix ADM per visualizzare il numero di sessioni con tempo di round trip ICA elevato. Per ulteriori informazioni, vedere la documentazione di Citrix ADM.
- Se Citrix ADM non è disponibile, rivolgersi al team di rete per determinare la causa principale.

#### ICA RTT (User) (Tempo di round trip ICA [utente])

Tempo di round trip ICA applicato alle sessioni avviate dall'utente specificato. L'avviso viene attivato se il tempo di round trip ICA è maggiore della soglia in almeno una sessione.

#### Failed Machines (Single-session OS) (Macchine che presentano problemi [sistema operativo a sessione singola])

Numero di macchine con sistema operativo a sessione singola che presentano problemi. Gli errori possono verificarsi per vari motivi, come mostrato nella dashboard di Monitor e nelle viste Filters (Filtri).

- Eseguire la diagnostica Citrix Scout per determinare la causa principale. Per ulteriori informazioni, vedere Risoluzione dei problemi degli utenti.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): ambito del gruppo di consegna
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 1, Critial (Avviso critico) - 2

#### Failed Machines (Multi-session OS) (Macchine che presentano problemi [sistema operativo multisessione])

Numero di macchine con sistema operativo multisessione che presentano problemi. Gli errori possono verificarsi per vari motivi, come mostrato nella dashboard di Monitor e nelle viste Filters (Filtri).

- Eseguire la diagnostica Citrix Scout per determinare la causa principale.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 1, Critial (Avviso critico) - 2

#### Computer con errori (in %)

Percentuale di computer con sistema operativo a sessione singola e multisessione che hanno riportato errori in un gruppo di consegna calcolata in base al numero di macchine con errore. Questa condizione di avviso consente di configurare le soglie di avviso in termini di percentuale di macchine con errori all'interno di un gruppo di consegna e viene calcolata ogni 30 secondi.
Gli errori possono verificarsi per vari motivi, come mostrato nella dashboard di Director e nelle viste Filters (Filtri). Eseguire la diagnostica Citrix Scout per determinare la causa principale. Per ulteriori informazioni, vedere Risoluzione dei problemi degli utenti.

#### Average Logon Duration (Durata media dell'accesso)

Durata media dell'accesso per gli accessi avvenuti nell'ultima ora.

- Controllare la dashboard di Monitor per ottenere metriche aggiornate sulla durata dell'accesso. Un numero elevato di utenti che effettuano l'accesso in un breve periodo di tempo può aumentare la durata dell'accesso.
- Controllare la linea di base e la ripartizione degli accessi per restringere la causa. Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti.

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 45 secondi, Critical (Avviso critico) - 60 secondi

#### Logon Duration (User) (Durata dell'accesso [utente])

Durata dell'accesso per gli accessi dell'utente specificato che si sono verificati nell'ultima ora.

#### Load Evaluator Index (Indice di valutazione del carico)

Valore dell'indice di valutazione del carico negli ultimi 5 minuti.

- Controllare Monitor per verificare la presenza di macchine con sistema operativo multisessione che potrebbero avere un carico di picco (carico massimo). Visualizzare sia la dashboard (errori) che il report Trends Load Evaluator Index (Indice delle tendenze per la valutazione del carico).

  **Condizioni dei criteri intelligenti:**

  - **Scope** (Ambito): gruppo di consegna, ambito del sistema operativo multisessione
  - **Threshold values** (Valori soglia): Warning (Avvertimento) - 80%, Critical (Avviso critico) - 90%

### Monitoraggio degli avvisi di Hypervisor

Monitor visualizza avvisi per monitorare lo stato dell'hypervisor. Gli avvisi di Citrix Hypervisor e VMware vSphere aiutano a monitorare i parametri e gli stati dell'Hypervisor. Viene monitorato anche lo stato della connessione all'hypervisor per fornire un avviso se il cluster o il pool di host viene riavviato o non è disponibile.

Per ricevere avvisi per l'hypervisor, assicurarsi che venga creata una connessione di hosting nella scheda Manage. Per ulteriori informazioni, vedere Connessioni e risorse. Solo queste connessioni

sono monitorate per gli avvisi dell'hypervisor. Nella tabella seguente vengono descritti i vari parametri e stati degli avvisi di Hypervisor.

| Avviso | Hypervisor supportati | Attivato da | Condizione | Configurazione |
|---|---|---|---|---|
| CPU usage (Utilizzo della CPU) | Citrix Hypervisor, VMware vSphere | Hypervisor | Soglia di avviso di utilizzo della CPU raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |
| Memory usage (Utilizzo della memoria) | Citrix Hypervisor, VMware vSphere | Hypervisor | Soglia di avviso di utilizzo della memoria raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |
| Network usage (Utilizzo della rete) | Citrix Hypervisor, VMware vSphere | Hypervisor | Soglia di avviso di utilizzo della rete raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |
| Disk usage (Utilizzo del disco) | VMware vSphere | Hypervisor | Soglia di avviso di utilizzo del disco raggiunta o superata | Le soglie di avviso devono essere configurate in Hypervisor. |
| Host connection or power state (Connessione host o stato di alimentazione) | VMware vSphere | Hypervisor | L'host di Hypervisor è stato riavviato o non è disponibile | Gli avvisi sono predefiniti in VMware vSphere. Non sono necessarie configurazioni aggiuntive. |

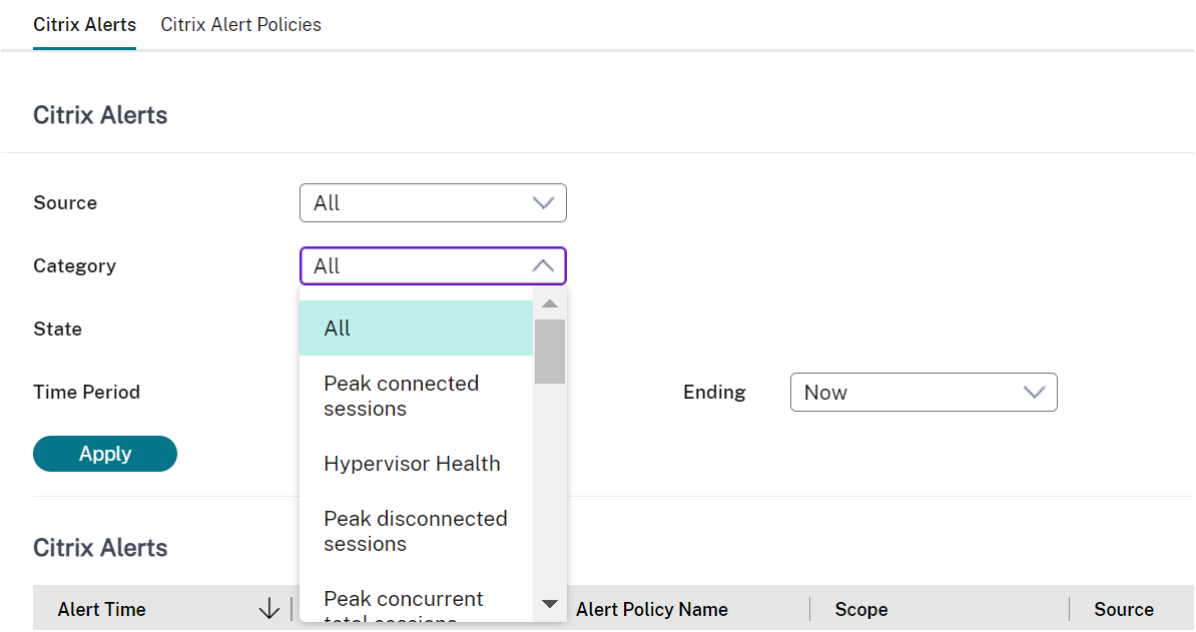
| Avviso | Hypervisor supportati | Attivato da | Condizione | Configurazione |
|---|---|---|---|---|
| Hypervisor connection unavailable (Connessione all'Hypervisor non disponibile) | Citrix Hypervisor, VMware vSphere | Delivery Controller | La connessione all'hypervisor (pool o cluster) viene persa, interrotta o riavviata. Questo avviso viene generato ogni ora finché la connessione non è disponibile. | Gli avvisi sono predefiniti nel Delivery Controller. Non sono necessarie configurazioni aggiuntive. |

> **Nota:**
>
> Per ulteriori informazioni sulla configurazione degli avvisi, vedere Avvisi di Citrix XenCenter o consultare la documentazione di Avvisi di VMware vCenter.

La preferenza per le notifiche e-mail può essere configurata in **Citrix Alerts Policy (Criteri per gli avvisi Citrix) > Site Policy (Criterio del sito) > Hypervisor Health (Stato dell'Hypervisor)**. Le condizioni di soglia per i criteri di avviso di Hypervisor possono essere configurate, modificate, disabilitate o eliminate solo dall'hypervisor e non da Monitor. Tuttavia, in Monitor è possibile modificare le preferenze e-mail e ignorare un avviso.

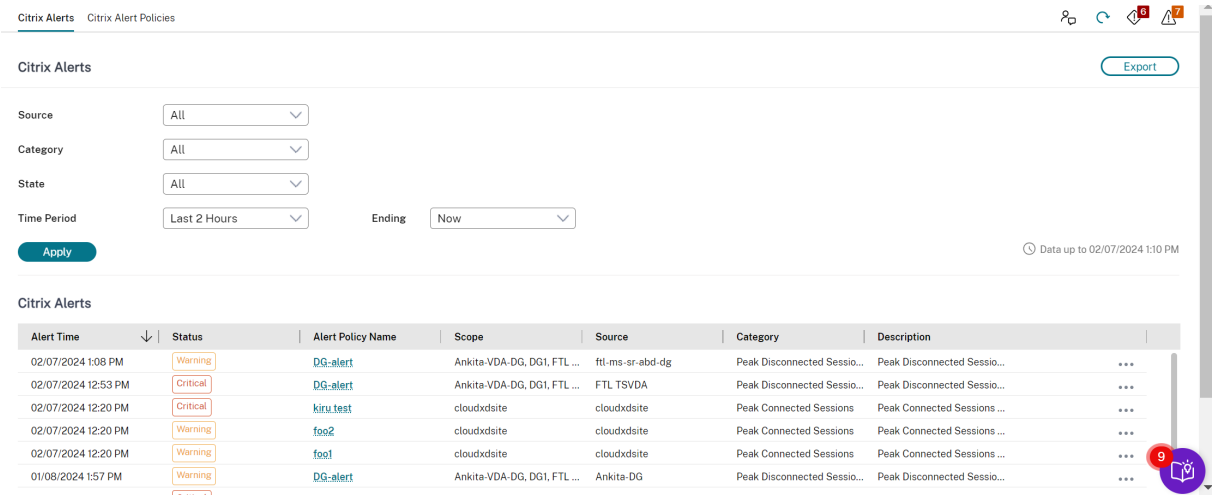
> **Importante:**
>
> - Tutti gli avvisi dell'hypervisor più vecchi di un giorno vengono automaticamente ignorati.
> - Gli avvisi attivati dall'Hypervisor vengono recuperati e visualizzati in Monitor. Tuttavia, i cambiamenti nel ciclo di vita/stato degli avvisi dell'Hypervisor non si riflettono in Monitor.
> - Gli avvisi integri o ignorati o disabilitati nella console di Hypervisor continueranno a essere visualizzati in Monitor e dovranno essere ignorati esplicitamente.
> - Gli avvisi che vengono ignorati in Monitor non vengono automaticamente ignorati nella console dell'Hypervisor.




È stata aggiunta una nuova categoria di avvisi denominata **Hypervisor Health** (Stato di Hypervisor) per abilitare il filtraggio solo degli avvisi di Hypervisor. Questi avvisi vengono visualizzati una volta raggiunte o superate le soglie. Gli avvisi di Hypervisor possono essere:

- Critical (Avviso critico): soglia critica del criterio di allarme dell'hypervisor raggiunta o superata
- Warning (Avvertimento): soglia di avvertimento del criterio di allarme dell'hypervisor raggiunta o superata
- Dismissed (Ignorato): avviso non più visualizzato come avviso attivo



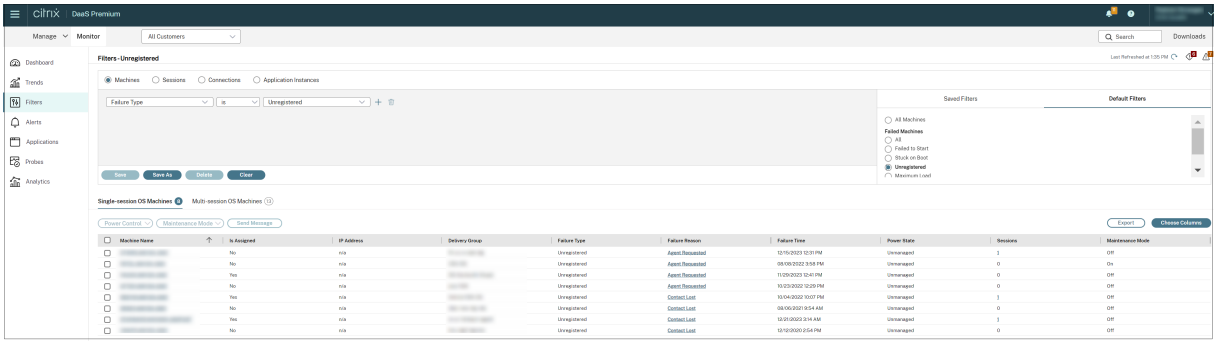

 

# Filtrare i dati per risolvere i problemi

August 17, 2023

Quando si fa clic sui numeri nella Dashboard o si seleziona un filtro Default predefinito dalla scheda **Filters** (Filtri), si apre la vista Filters (Filtri) in cui sono visualizzati i dati in base al tipo di macchina o guasto selezionato.

È possibile creare viste filtrate personalizzate di macchine, connessioni, sessioni e istanze di applicazioni in tutti i gruppi di consegna e salvare la ricerca per accedervi in seguito. È possibile modificare un filtro predefinito e salvarlo come filtro salvato.



1. Selezionare una vista:

    - **Machines** (Macchine). Selezionare Single-session OS Machines (Macchine con sistema operativo a sessione singola) o Multi-session OS Machines (Macchine con sistema operativo multisessione). Queste viste mostrano il numero di macchine configurate. La scheda Multi-session OS Machines (Macchine con sistema operativo multisessione) include anche l'indice di valutazione del carico, che indica la distribuzione dei contatori delle prestazioni e le descrizioni dei comandi del conteggio delle sessioni se si passa il mouse sul collegamento.
    - **Sessions** (Sessioni). È inoltre possibile visualizzare il conteggio delle sessioni dalla vista Sessions (Sessioni). Utilizzare le misurazioni del tempo di inattività per identificare le sessioni inattive oltre un periodo di soglia. Fare clic sull'**utente associato** per aprire l'Activity Manager per l'utente. Facendo clic sul nome dell'**endpoint** si apre l'Activity Manager relativo all'endpoint. Facendo clic su **View Details** (Visualizza dettagli), si apre rispettivamente la pagina **User Details** (Dettagli utente) o **Endpoint Details** (Dettagli endpoint). Per ulteriori informazioni, vedere Dettagli utente.
    - **Connections** (Connessioni). Filtrare le connessioni in base a diversi periodi di tempo, inclusi gli ultimi 60 minuti, le ultime 24 ore o gli ultimi 7 giorni.
    - **Application Instances** (Istanze dell'applicazione). Questa vista visualizza le proprietà di tutte le istanze delle applicazioni sui VDA con sistema operativo multisessione e a sessione singola. Le misurazioni del tempo di inattività della sessione sono disponibili per le istanze delle applicazioni sui VDA con sistema operativo multisessione.

2. Selezionare un filtro dall'elenco dei filtri salvati o predefiniti.
3. Utilizzare gli elenchi a discesa per selezionare ulteriori criteri di filtro.
4. Selezionare colonne aggiuntive, se necessario, per continuare con la risoluzione dei problemi.
5. Salvare il filtro e assegnarvi un nome.
6. Per aprire il filtro in un secondo momento, nella vista Filters (Filtri) selezionare View (Machines, Sessions, Connections, or Application Instances) (Visualizza [macchine, sessioni, connessioni o istanze delle applicazioni]) e selezionare il filtro salvato.
7. Fare clic su **Export** (Esporta) per esportare i dati in file in formato CSV. È possibile esportare fino a 100.000 record di dati.
8. Se necessario, per le viste **Machines** (Macchine) o **Connections** (Connessioni), utilizzare i controlli di alimentazione per tutte le macchine selezionate nell'elenco filtrato. Per la vista Sessions (Sessioni), utilizzare i controlli di sessione o l'opzione per inviare messaggi.
9. Nelle viste **Machines** (Macchine) e **Connections** (Connessioni), fare clic su **Failure Reason** (Motivo dell'errore) di una macchina che presenta problemi o di una connessione non riuscita per ottenere una descrizione dettagliata dell'errore e delle azioni consigliate per risolverlo. I motivi degli errori e le azioni consigliate per gli errori delle macchine e delle connessioni sono disponibili nella Guida alla risoluzione dei problemi per i motivi degli errori di Citrix Director.
10. Nella vista **Machines** (Macchine), fare clic sul collegamento del nome di una macchina per accedere alla pagina **Machine Details** (Dettagli macchina) corrispondente. Questa pagina visualizza i dettagli della macchina, fornisce controlli di alimentazione, visualizza la CPU, la memoria, il monitoraggio del disco e i grafici sul monitoraggio della GPU. Inoltre, fare clic su **View Historical Utilization** (Visualizza utilizzo storico) per visualizzare le tendenze di utilizzo delle risorse per la macchina. Per ulteriori informazioni, vedere Risolvere i problemi relativi alle macchine.
11. Nella vista **Application Instances** (Istanze applicazione), ordinare o filtrare in base al **tempo di inattività** superiore a un periodo di soglia. Selezionare le istanze dell'applicazione inattive da terminare. Lo scollegamento o la disconnessione di un'istanza dell'applicazione termina tutte le istanze dell'applicazione attive nella stessa sessione. Per ulteriori informazioni, vedere Risolvere i problemi relativi alle applicazioni. La pagina dei filtri Application Instances (Istanze delle applicazioni) e le misurazioni del tempo di inattività nelle pagine dei filtri Sessions (Sessioni) sono disponibili nei VDA versione 7.13 o successiva.

> **Nota:**
>
> La console Manage consente l'assegnazione di più regole di assegnazione del desktop (DAR) per diversi utenti o gruppi di utenti a un singolo VDA nel gruppo di consegna. StoreFront visualizza il desktop assegnato con il Display Name (Nome visualizzato) corrispondente in base al DAR dell'utente che ha effettuato l'accesso. Tuttavia, Monitor non supporta le DAR e visualizza il desktop

> assegnato utilizzando il nome del gruppo di consegna indipendentemente dall'utente connesso. Di conseguenza, non è possibile mappare un desktop specifico a una macchina in Monitor. Per mappare il desktop assegnato visualizzato in StoreFront al nome del gruppo di consegna visualizzato in Monitor, utilizzare il seguente comando PowerShell: Eseguire il comando PowerShell utilizzando l'SDK Remote PowerShell come descritto nel blog.

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

## Monitorare le tendenze storiche di un sito

August 17, 2023

La vista Trends (Tendenze) accede alle informazioni sulle tendenze storiche di ciascun sito per i seguenti parametri:

- sessioni
- errori di connessione
- errori della macchina
- prestazioni di accesso
- valutazione del carico
- gestione della capacità
- utilizzo della macchina
- utilizzo delle risorse

Per individuare queste informazioni, fare clic sul menu **Trends** (Tendenze).

La funzione di drill down con zoom avanti consente di spostarsi tra i grafici delle tendenze selezionando un periodo di tempo (facendo clic su un punto dati nel grafico) ed eseguendo il drill down per visualizzare i dettagli associati alla tendenza. Questa funzionalità consente di comprendere meglio i dettagli di chi o cosa è stato influenzato dalle tendenze visualizzate.

Per modificare l'ambito predefinito di ciascun grafico, applicare un filtro diverso ai dati.

> **Nota:**
>
> - Le informazioni sulle sessioni, gli errori e le tendenze delle prestazioni di accesso sono disponibili come grafici e tabelle quando il periodo di tempo è impostato su Last month (**Ending now**) (Ultimo mese [che sta per concludersi]) o un periodo più limitato. Quando il

> periodo di tempo viene impostato come Last month (Ultimo mese) con una data di fine personalizzata o come Last year (Ultimo anno), le informazioni sulle tendenze sono disponibili come grafici, ma non come tabelle.
> - Citrix DaaS, (in precedenza servizio Citrix Virtual Apps and Desktops) supporta la conservazione dei dati storici solo per 90 giorni. Pertanto, le tendenze e i rapporti di un anno in Monitor mostrano gli ultimi 90 giorni di dati.

### Tendenze disponibili

**View trends for sessions** (Visualizza tendenze per le sessioni): dalla scheda Sessions, selezionare il gruppo di consegna e il periodo di tempo per visualizzare informazioni più dettagliate sul conteggio delle sessioni simultanee.

La colonna **Session Auto Reconnect** (Riconnessione automatica sessione) visualizza il numero di riconnessioni automatiche in una sessione. La riconnessione automatica è abilitata quando sono in vigore i criteri Session Reliability (Affidabilità della sessione) o Auto Client Reconnect (Riconnessione automatica client). Quando si verifica un'interruzione della rete sull'endpoint, entrano in vigore i seguenti criteri:

- Session Reliability (Affidabilità della sessione) entra in vigore (per impostazione predefinita per 3 minuti) quando l'app Citrix Receiver o Citrix Workspace tenta di connettersi al VDA.
- Auto Client Reconnect (Riconnessione automatica client) entra in vigore tra 3 e 5 minuti quando il client tenta di connettersi al VDA.

Entrambe queste riconnessioni vengono acquisite e visualizzate all'utente. Queste informazioni possono richiedere un tempo massimo di 5 minuti per apparire nell'interfaccia utente di Director dopo la riconnessione.

Le informazioni di riconnessione automatica consentono di visualizzare le connessioni di rete che presentano interruzioni e risolverne i problemi, nonché di analizzare le reti che presentano un'esperienza senza problemi. È possibile visualizzare il numero di riconnessioni per un gruppo di consegna o un periodo di tempo specifico selezionato in Filters (Filtri).

Il drill down fornisce informazioni aggiuntive come l'affidabilità della sessione o la riconnessione automatica del client, i timestamp, l'IP dell'endpoint e il nome dell'endpoint della macchina su cui è installata l'app Workspace.

Per impostazione predefinita, i log vengono ordinati in base ai timestamp degli eventi in ordine decrescente. Questa funzionalità è disponibile per l'app Citrix Workspace per Windows, l'app Citrix Workspace per Mac, Citrix Receiver per Windows e Citrix Receiver per Mac. Questa funzionalità richiede VDA 1906 o versioni successive.

Per ulteriori informazioni sulle riconnessioni delle sessioni, vedere Sessions. Per ulteriori informazioni sui criteri, vedere Impostazioni dei criteri di riconnessione automatica del client e Impostazioni dei criteri di affidabilità delle sessioni.

A volte, i dati di riconnessione automatica potrebbero non essere visualizzati in Monitor per i seguenti motivi:

- L'app Workspace non invia i dati di riconnessione automatica al VDA.
- Il VDA non invia i dati al servizio Monitor.

> **Nota:**
>
> Talvolta, l'indirizzo IP del client potrebbe non essere ottenuto correttamente se sono impostati determinati criteri di Citrix Gateway.

**View trends for connection failures** (Visualizza tendenze per errori di connessione): dalla scheda Failures (Errori), selezionare la connessione, il tipo di macchina, il tipo di errore, il gruppo di consegna e il periodo di tempo per visualizzare un grafico contenente informazioni più dettagliate sugli errori di connessione utente nel sito.

**View trends for machine failures** (Visualizza tendenze per gli errori delle macchine): dalla scheda Single-session OS Machine Failures (Errori delle macchine con sistema operativo a sessione singola) o dalla scheda Multi-session OS Machines (Macchine con sistema operativo multisessione), selezionare il tipo di errore, il gruppo di consegna e il periodo di tempo per visualizzare un grafico contenente informazioni più dettagliate sugli errori delle macchine nel sito.

**View trends for logon performance** (Visualizza tendenze per le prestazioni di accesso): dalla scheda Logon Performance (Prestazioni di accesso), selezionare il gruppo di consegna e il periodo di tempo per visualizzare un grafico contenente informazioni più dettagliate sulla durata dei tempi di accesso degli utenti nel sito e se il numero di accessi influisce sulle prestazioni. Questa vista mostra anche la durata media delle fasi di accesso, come la durata del brokering e l'ora di avvio della VM.
Questi dati sono specificamente riferiti agli accessi utente e non includono gli utenti che tentano di riconnettersi da sessioni disconnesse.
La tabella sotto il grafico mostra Logon Duration by User Session (Durata dell'accesso per sessione utente). È possibile scegliere le colonne da visualizzare e ordinare il report in base a una qualsiasi delle colonne.
Per ulteriori informazioni, vedere Diagnosticare i problemi di accesso degli utenti.

**View trends for load evaluation** (Visualizza tendenze per la valutazione del carico): dalla scheda Load Evaluator Index (Indice di valutazione del carico), visualizzare un grafico contenente informazioni più dettagliate sul carico distribuito tra le macchine con sistema operativo multisessione. Le opzioni di filtro per questo grafico includono il gruppo di consegna o la macchina con sistema operativo multisessione in un gruppo di consegna, la macchina con sistema operativo multisessione (disponibile solo se è stata selezionata la macchina con sistema operativo multisessione in un

gruppo di consegna) e l'intervallo. L'indice di valutazione del carico viene visualizzato sotto forma di percentuali di CPU, memoria, disco o sessioni totali e viene visualizzato rispetto al numero di utenti connessi nell'ultimo intervallo.

**View hosted applications usage** (Visualizza utilizzo delle applicazioni ospitate): nella scheda Capacity Management (Gestione capacità), selezionare la scheda Hosted Applications Usage(Utilizzo delle applicazioni ospitate), selezionare il gruppo di consegna e il periodo di tempo per visualizzare un grafico che mostra il picco di utilizzo simultaneo e una tabella che visualizza l'utilizzo in base all'applicazione. Dalla tabella Application Based Usage (Utilizzo basato sull'applicazione), è possibile scegliere un'applicazione specifica per visualizzare i dettagli e un elenco di utenti che utilizzano o hanno utilizzato l'applicazione. È possibile visualizzare i valori delle istanze di applicazione simultanee di picco previsti scelti per il periodo di tempo futuro con la previsione dell'istanza dell'applicazione. Per ulteriori informazioni, vedere la sezione Application instance prediction.

**View Single-session and Multi-session OS usage** (Visualizza utilizzo del sistema operativo a sessione singola e multisessione): la vista Trends (Tendenze) mostra l'utilizzo del sistema operativo a sessione singola per sito e per gruppo di consegna. Quando si seleziona il sito, viene visualizzato l'utilizzo per gruppo di consegna. Quando si seleziona il gruppo di consegna, viene visualizzato l'utilizzo per utente.
La vista Trends mostra anche l'utilizzo del sistema operativo multisessione per sito, per gruppo di consegna e per macchina. Quando si seleziona il sito, viene visualizzato l'utilizzo per gruppo di consegna. Quando si seleziona il gruppo di consegna, viene visualizzato l'utilizzo per macchina e per utente. Quando si seleziona Machine (Macchina), viene visualizzato l'utilizzo per utente.

**View virtual machine usage** (Visualizza utilizzo della macchina virtuale): dalla scheda Machine Usage (Utilizzo macchina), selezionare Single-session OS Machines (Macchine con sistema operativo a sessione singola) o Multi-session OS Machines (Macchine con sistema operativo multisessione) per ottenere una visualizzazione in tempo reale dell'utilizzo della VM. La pagina visualizza il numero di macchine con sistema operativo multisessione e sessione singola abilitate per la scalabilità automatica che sono accese per un gruppo di consegna e un periodo di tempo selezionati. Sono disponibili anche i risparmi stimati ottenuti abilitando Autoscale nel gruppo di consegna selezionato; questa percentuale viene calcolata utilizzando i costi per macchina.

Le tendenze di utilizzo delle macchine abilitate per la scalabilità automatica indicano l'utilizzo effettivo delle macchine, consentendo di valutare rapidamente le esigenze di capacità del proprio sito.

- Single-session OS availability (Disponibilità del sistema operativo a sessione singola): visualizza lo stato corrente delle macchine con sistema operativo a sessione singola (VDI) in base alla disponibilità per l'intero sito o per un gruppo di consegna specifico.
- Multi-session OS availability (Disponibilità del sistema operativo multisessione): visualizza lo stato corrente delle macchine con sistema operativo multisessione in base alla disponibilità per l'intero sito o per un gruppo di consegna specifico.

> **Nota:**
>
> La griglia sotto il grafico mostra i dati sull'utilizzo della macchina in base al gruppo di consegna in tempo reale. I dati includono la disponibilità macchina di tutte le macchine indipendentemente dall'abilitazione di Autoscale. Il numero di macchine visualizzate nella colonna Available Counter (Contatore disponibili) nella griglia include le macchine in modalità di manutenzione.

Il consolidamento dei dati di monitoraggio dipende dal periodo di tempo selezionato.

- I dati di monitoraggio per i periodi di un giorno e di una settimana vengono consolidati per ora.
- I dati di monitoraggio per il periodo di un mese vengono consolidati per giorno.

Lo stato della macchina viene letto al momento del consolidamento e non vengono prese in considerazione eventuali variazioni verificatesi durante il periodo intermedio. Per il periodo di consolidamento, fare riferimento alla documentazione dell'API Monitor.

Per ulteriori informazioni sul monitoraggio delle macchine abilitate alla scalabilità automatica, vedere l'articolo Autoscale.

**View resource utilization** (Visualizza utilizzo delle risorse): dalla scheda Resource Utilization (Utilizzo delle risorse), selezionare Single-session OS Machines (Macchine con sistema operativo a sessione singola) o Multi-session OS Machines (Macchine con sistema operativo multisessione) per ottenere informazioni dettagliate sui dati delle tendenze storiche per l'utilizzo di CPU e memoria, nonché su IOPS e sulla latenza del disco per ogni macchina VDI, per una migliore pianificazione della capacità. Questa funzionalità richiede i VDA **versione 7.11** o successiva.
I grafici mostrano i dati relativi alla CPU media, alla memoria media, agli IOPS medi, alla latenza del disco e alle sessioni di picco simultanee. È possibile eseguire il drill down sulla macchina e visualizzare dati e grafici per i primi 10 processi che consumano CPU. Filtrare in base al gruppo di consegna e al periodo di tempo. I grafici della CPU, dell'utilizzo della memoria e delle sessioni di picco simultanee sono disponibili per le ultime 2 ore, le ultime 24 ore, gli ultimi 7 giorni, l'ultimo mese e l'ultimo anno. I grafici sugli IOPS e la latenza del disco medi sono disponibili per le ultime 24 ore, l'ultimo mese e l'ultimo anno.

> **Nota:**
>
> - L'impostazione dei criteri di monitoraggio Enable Process Monitoring (Abilita monitoraggio processo) deve essere impostata su "Allowed"(Consentito) per raccogliere e visualizzare i dati nella tabella Top 10 Processes (Primi 10 processi) della pagina Historic Machine Utilization (Utilizzo storico della macchina). Il criterio è impostato su "Prohibited"(Non consentito) per impostazione predefinita. Tutti i dati di utilizzo delle risorse vengono raccolti per impostazione predefinita. Questa opzione può essere disabilitata utilizzando l'impostazione dei criteri Enable Resource Monitoring (Abilita monitoraggio delle risorse). La tabella sotto i grafici mostra i dati di utilizzo delle risorse per ogni macchina.

> - L'IOPS medio mostra le medie giornaliere. L'IOPS di picco è calcolato come la più alta delle medie IOPS per l'intervallo di tempo selezionato (una media IOPS è la media oraria degli IOPS raccolti nel corso di un'ora sul VDA).
> - Il drill-down della macchina elenca i processi con un utilizzo medio della CPU o un utilizzo medio della memoria superiore all'1%; ciò potrebbe significare che a volte vengono elencati meno di 10 processi.

**View application failures** (Visualizza errori dell'applicazione): nella scheda Application Failures (Errori applicazione) vengono visualizzati gli errori associati alle applicazioni pubblicate sui VDA.

Questa funzionalità richiede i VDA **versione 7.15** o successiva. Sono supportati i VDA con sistema operativo a sessione singola che eseguono Windows Vista e versioni successive e i VDA con sistema operativo multisessione che eseguono Windows Server 2008 e versioni successive.
Per ulteriori informazioni, vedere Monitoraggio storico degli errori delle applicazioni.

Per impostazione predefinita, vengono visualizzati solo gli errori delle applicazioni dei VDA con sistema operativo multisessione. È possibile impostare il monitoraggio degli errori delle applicazioni utilizzando i criteri di monitoraggio. Per ulteriori informazioni, vedere Impostazioni dei criteri di monitoraggio.

**View application probe results** (Visualizza risultati del probe dell'applicazione): la scheda **Probe Results** (Risultati del probe) visualizza i risultati del probe per le applicazioni e i desktop configurati per il probe nella pagina Configuration (Configurazione). Qui viene registrata la fase di avvio durante la quale si è verificato l'errore di avvio dell'applicazione.

Per ulteriori informazioni, vedere Probe delle applicazioni e dei desktop.

**Create customized reports** (Crea report personalizzati): la scheda Custom Reports (Report personalizzati) fornisce un'interfaccia utente per la generazione di report personalizzati contenenti dati storici e in tempo reale del database Monitoring (Monitoraggio) in formato tabulare.

Dall'elenco delle query Custom Report (Report personalizzato) salvate in precedenza, è possibile fare clic su **Run and download** (Esegui e scarica) per esportare il report in formato CSV, fare clic su **Copy OData** (Copia OData) per copiare e condividere la query OData corrispondente oppure fare clic su **Edit** (Modifica) per modificare la query.
È possibile creare una nuova query Custom Report (Report personalizzato) basata su macchine, connessioni, sessioni o istanze dell'applicazione. Specificare le condizioni di filtro in base a campi come macchina, gruppo di consegna o periodo di tempo. Specificare le colonne aggiuntive richieste nel report personalizzato. L'anteprima visualizza un campione dei dati del report. Il salvataggio della query Custom Report (Report personalizzato) la aggiunge all'elenco delle query salvate.

È possibile creare una query Custom Report (Report personalizzato) basata su una query OData copiata. Per farlo, selezionare l'opzione OData Query (Query OData) e incollare la query OData copiata. È possibile salvare la query risultante per eseguirla in un secondo momento.

> **Nota:**
>
> I nomi delle colonne nel report Preview (Anteprima) ed Export (Esporta) generati utilizzando le query OData non sono tradotti, ma vengono visualizzati in inglese.

Le icone a forma di bandierina sul grafico indicano eventi o azioni significativi per l'intervallo di tempo specifico. Passare il mouse sulla bandierina e fare clic per elencare eventi o azioni.

> **Nota:**
>
> - I dati di accesso alla connessione HDX non vengono raccolti per le versioni di VDA precedenti alla 7. Per i VDA precedenti, i dati del grafico vengono visualizzati come 0.
> - I gruppi di consegna eliminati nella console Manage sono disponibili per la selezione nei filtri Trends fino a quando i dati a essi correlati non vengono eliminati Se si seleziona un gruppo di consegna eliminato, vengono visualizzati grafici per i dati disponibili fino alla conservazione. Tuttavia, le tabelle non mostrano dati.
> - Lo spostamento di una macchina contenente sessioni attive da un gruppo di consegna a un altro fa sì che le tabelle **Resource Utilization (Utilizzo delle risorse) e Load Evaluator Index (Indice di valutazione del carico)** del nuovo gruppo di consegna visualizzino le metriche consolidate dei gruppi di consegna vecchi e nuovi.

### Previsione delle istanze dell'applicazione

L'analisi predittiva offre la possibilità di prevedere l'utilizzo futuro delle risorse. Questa funzionalità è particolarmente utile per aiutare gli amministratori a organizzare le risorse e le licenze richieste su ciascuna risorsa.

La prima funzione di analisi predittiva, la previsione delle istanze dell'applicazione, prevede il numero di istanze di applicazioni ospitate che potrebbero essere avviate per sito o gruppo di consegna nel tempo.

La previsione dell'istanza dell'applicazione è disponibile nella scheda **Trends > Capacity Management** (Tendenze > Gestione capacità) in cui è visualizzato l'utilizzo dell'applicazione ospitata per il periodo di tempo scelto. Il grafico storico contiene i valori delle istanze di applicazione simultanee di picco tracciati per il periodo scelto.

Per ottenere il grafico previsto, selezionare la casella di controllo Predict (Previsione). Un grafico di previsione a linee tratteggiate viene visualizzato come estensione del grafico storico. I valori delle istanze di applicazione simultanee di picco previsti vengono tracciati con la linea temporale estesa verso il futuro per il periodo di tempo scelto.

È possibile prevedere le istanze dell'applicazione per i prossimi 7 giorni, il prossimo mese o il prossimo anno. Non sono supportate date di fine personalizzate.

La previsione viene eseguita utilizzando algoritmi ad apprendimento automatico basati su modelli di dati creati con i dati storici esistenti. Le previsioni sono quindi accurate quanto lo è la qualità dei dati esistenti.

L'accuratezza della previsione è indicata dal livello di tolleranza visualizzato come suggerimento sul grafico previsto. Indica la possibile variazione dei valori effettivi rispetto ai valori previsti.

Il livello di tolleranza può essere elevato se i dati disponibili non seguono uno schema regolare o mancano per determinati periodi o sono insufficienti.

La previsione per un anno cattura gli andamenti mensili e trimestrali insieme alla tendenza generale dell'anno. Allo stesso modo, la previsione mensile acquisisce gli andamenti giornalieri e settimanali insieme a tendenze settimanali come la riduzione dell'attività durante i fine settimana.

Per la previsione devono essere disponibili dati storici sufficienti come segue:

- Dati di 14 giorni per la previsione di 7 giorni
- Dati di 35 giorni per la previsione di un mese
- Dati di 84 giorni per la previsione di un anno

> **Nota:**
>
> È possibile esportare solo il grafico storico, ma non il grafico previsto.

## Monitoraggio di macchine gestite dalla scalabilità automatica

October 6, 2022

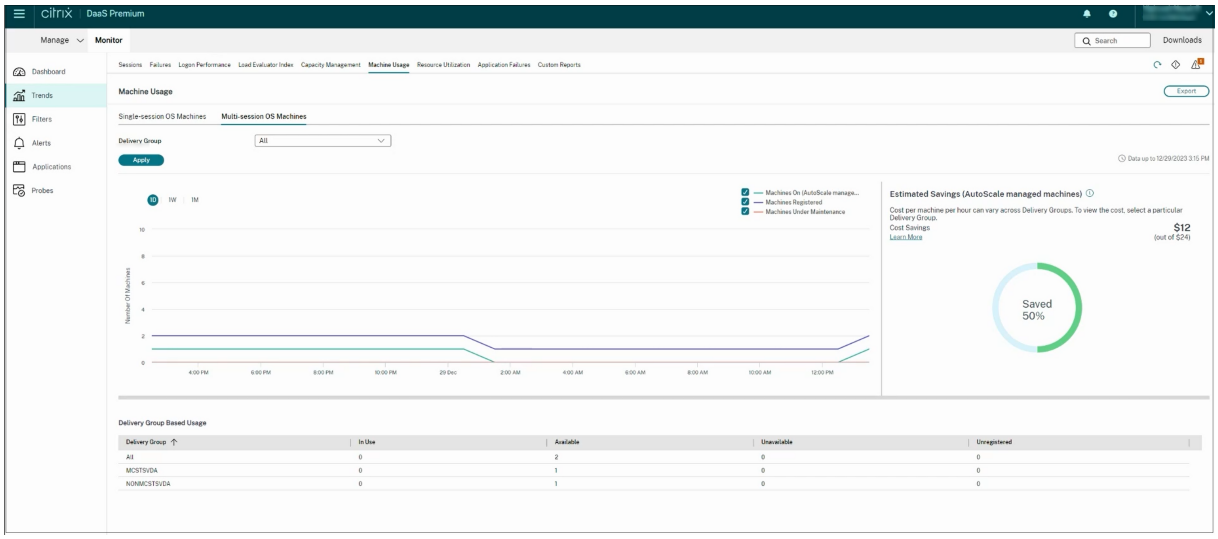
La scalabilità automatica è una funzionalità di gestione dell'alimentazione che consente la gestione proattiva dell'alimentazione di tutte le macchine con sistema operativo multisessione e a sessione singola registrate in un gruppo di consegna. È possibile configurare la scalabilità automatica per un gruppo di consegna selezionato dalla scheda **Manage** (Gestisci). Per ulteriori informazioni, vedere Scalabilità automatica.
È possibile monitorare le metriche chiave delle macchine abilitate alla scalabilità automatica dalla scheda **Monitor**.

### Utilizzo della macchina

La pagina **Monitor** > **Trends** > **Machine Usage** visualizza il numero di macchine con sistema operativo multisessione e sessione singola abilitate per la scalabilità automatica che sono accese per un gruppo di consegna e un periodo di tempo selezionati. Questa metrica indica l'utilizzo effettivo delle macchine incluse nel gruppo di consegna.

Dalla scheda **Single session OS Machines** (Macchine con sistema operativo a sessione singola) o dalla scheda **Multi-session OS Machines** (Macchine con sistema operativo multisessione), selezionare il gruppo di consegna e il periodo di tempo.



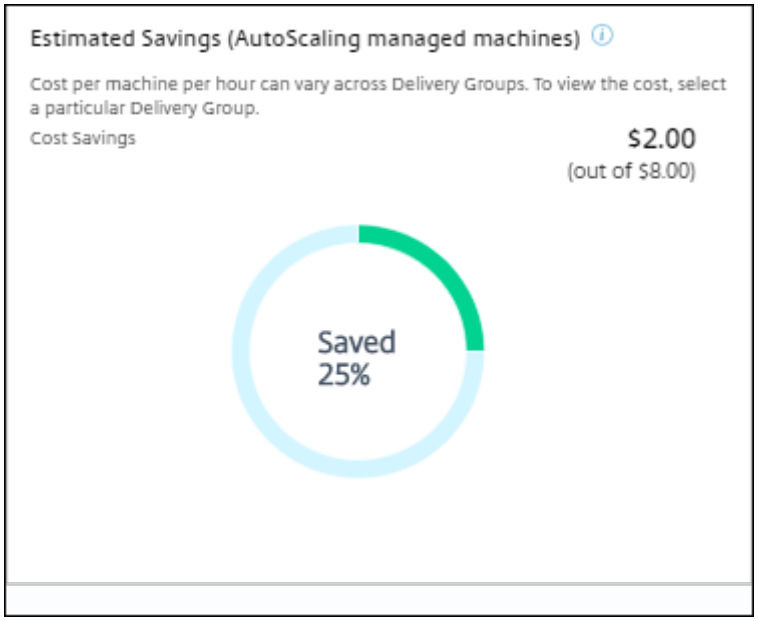

Il grafico illustra le seguenti metriche:

- **Machines On**: il numero di macchine abilitate alla scalabilità automatica che sono accese
- **Machines Registered**: il numero di macchine con sistema operativo multisessione o a sessione singola registrate
- **Machines under Maintenance**: il numero di macchine con sistema operativo multisessione o a sessione singola con modalità di manutenzione attivata

## Risparmio stimato

La pagina **Monitor** > **Trends** > **Machine Usage** visualizza anche i risparmi sui costi stimati ottenuti abilitando la scalabilità automatica nel gruppo di consegna selezionato.




Il risparmio stimato viene calcolato come percentuale di risparmi per macchina all'ora (in dollari USA) come configurato in **Manage** > **Edit Delivery Group** > **Autoscale** (Gestisci > Modifica gruppo di consegna > Scalabilità automatica). Per ulteriori informazioni sulla configurazione dei risparmi per macchina, vedere Autoscale.

Quando si selezionano tutti i gruppi di consegna, viene visualizzato il valore medio del risparmio stimato in tutti i gruppi di consegna.
La stima del risparmio aiuta gli amministratori a consolidare l'infrastruttura esistente e pianificare la capacità per ottenere il massimo risparmio e utilizzo.

### Notifiche di avviso per macchine e sessioni

Il Monitor Dashboard visualizza le notifiche di avviso di cui è possibile effettuare un ulteriore drill-down. I dettagli dell'avviso vengono visualizzati nella pagina **Monitor** > **Alerts**.

- Per creare un criterio di avviso in un gruppo di consegna, andare a **Monitor** > **Alerts** > **Citrix Alerts Policy** > **Delivery Group Policy**.
- Qui è possibile impostare le seguenti soglie di avvertenza e soglie critiche:
  - macchine con errori (sistema operativo a sessione singola) e macchine con errori (sistema operativo multisessione);
  - sessioni connesse di picco, sessioni disconnesse di picco e sessioni totali concorrenti di picco nel gruppo di consegna.
- Vengono generati avvisi quando la metrica corrispondente all'interno del gruppo di consegna raggiunge la soglia.

Per maggiori dettagli sulle condizioni dei criteri di avviso e sulla creazione di nuovi criteri di avviso, vedere Avvisi e notifiche.

### Stato della macchina

- In **Monitor** > **Filters** > **Machines** è visualizzato lo stato di alimentazione di tutte le macchine in un formato tabellare. È possibile filtrare indicando un gruppo di consegna specifico.
- In **Monitor** > **Filters** > **Sessions** è visualizzato il filtro in base al nome della macchina per vedere le sessioni a essa associate e il loro stato in tempo reale.
- In **Monitor** > **Trends** > **Sessions**, selezionare il gruppo di consegna e il periodo di tempo per visualizzare l'andamento delle sessioni e le metriche associate.

Per ulteriori informazioni, vedere Filtrare i dati per risolvere i problemi.

### Tendenze di valutazione del carico

Nella pagina **Monitor** > **Trends** > **Load Evaluator Index** (Indice di valutazione del carico) è visualizzato un grafico con informazioni dettagliate sul carico distribuito tra le macchine con sistema operativo multisessione. Le opzioni di filtro per questo grafico includono il gruppo di consegna o la macchina con sistema operativo multisessione in un gruppo di consegna, la macchina con sistema operativo multisessione (disponibile solo se è stata selezionata la macchina con sistema operativo multisessione in un gruppo di consegna) e l'intervallo. L'indice di valutazione del carico viene visualizzato sotto forma di percentuali di CPU, memoria, disco o sessioni totali e viene visualizzato rispetto al numero di utenti connessi nell'ultimo intervallo.

## Risolvere i problemi relativi alle distribuzioni

October 5, 2022

In qualità di amministratore dell'help desk, è possibile cercare l'utente che segnala un problema e visualizzare i dettagli delle sessioni o delle applicazioni associate a tale utente.

Analogamente, è possibile cercare macchine o endpoint in cui vengono segnalati problemi. È possibile risolvere rapidamente i problemi monitorando le metriche rilevanti ed eseguendo azioni appropriate.

Sono disponibili le seguenti azioni:

- chiudere un'applicazione o un processo che non risponde
- effettuare lo shadowing di operazioni sul computer dell'utente

- scollegare una sessione che non risponde
- riavviare il computer
- mettere la macchina in modalità di manutenzione
- reimpostare il profilo utente

# Risolvere i problemi relativi alle applicazioni

July 28, 2023

## Analisi delle applicazioni

La vista **Applications** (Applicazioni) visualizza le analisi basate sulle applicazioni in un'unica vista consolidata per facilitare l'analisi e la gestione efficienti delle prestazioni delle applicazioni. È possibile ottenere importanti dettagli approfonditi sulle informazioni sullo stato e sull'utilizzo di tutte le applicazioni pubblicate sul sito. La vista predefinita aiuta a identificare le applicazioni più frequentemente eseguite.
Questa funzionalità richiede i VDA versione 7.15 o successiva.


La colonna **Probe Result** (Risultato del probe) visualizza il risultato dell'esecuzione del probe delle applicazioni nelle ultime 24 ore. Fare clic sul collegamento dei risultati del probe per visualizzare ulteriori dettagli nella pagina **Trends** (Tendenze) > **Probe Results** (Risultati del probe). Per ulteriori dettagli su come configurare i probe delle applicazioni e dei desktop, vedere Probe delle applicazioni e dei desktop.

La colonna **Instances** (Istanze) visualizza l'utilizzo delle applicazioni. Indica il numero di istanze delle applicazioni attualmente in esecuzione (istanze connesse e disconnesse). Per risolvere ulteriormente i problemi, fare clic sul campo **Instances** (Istanze) per visualizzare la pagina dei filtri **Application Instances** (Istanze dell'applicazione) corrispondente. Qui è possibile selezionare le istanze dell'applicazione da scollegare o disconnettere.

> **Nota:**
>
> Per gli amministratori di ambiti personalizzati, Monitor non visualizza le istanze delle applicazioni create in gruppi di applicazioni. Per visualizzare tutte le istanze dell'applicazione, è

> necessario essere un amministratore completo. Per ulteriori informazioni, vedere l'articolo CTX256001 del Knowledge Center.

Monitorare lo stato delle applicazioni pubblicate nel sito con le colonne **Application Faults** (Problemi delle applicazioni) e **Application Errors** (Errori delle applicazioni). Queste colonne visualizzano il numero aggregato di problemi ed errori che si sono verificati durante l'avvio dell'applicazione corrispondente nell'ultima ora. Fare clic sul campo **Application Faults** (Problemi delle applicazioni) o **Application Errors** (Errori delle applicazioni) per visualizzare i dettagli degli errori nella pagina **Trends** (Tendenze) > **Application Failures** (Errori delle applicazioni) corrispondente all'applicazione selezionata.

Le impostazioni dei criteri degli errori delle applicazioni regolano la disponibilità e la visualizzazione di problemi ed errori. Per ulteriori informazioni sui criteri e su come modificarli, vedere Criteri per il monitoraggio degli errori delle applicazioni nelle impostazioni dei criteri di Monitoring.

### Monitoraggio delle applicazioni in tempo reale

È possibile risolvere i problemi delle applicazioni e delle sessioni utilizzando la metrica relativa al tempo di inattività per identificare le istanze inattive oltre un limite di tempo specifico.

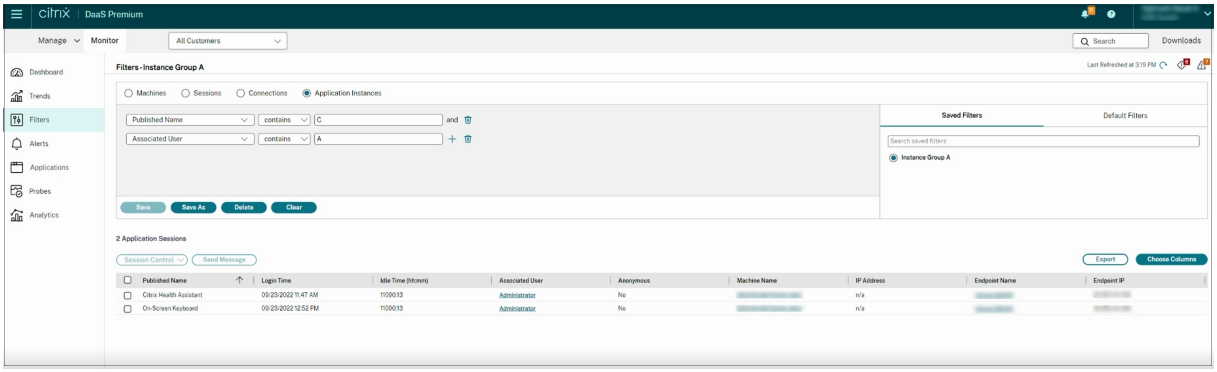
I casi d'uso tipici per la risoluzione dei problemi basati sulle applicazioni sono nel settore sanitario, dove i dipendenti condividono le licenze delle applicazioni. In questo caso è necessario terminare le sessioni inattive e le istanze delle applicazioni per ripulire l'ambiente Citrix Virtual Apps and Desktops, per riconfigurare server con prestazioni insoddisfacenti o per gestire e aggiornare le applicazioni.

La pagina dei filtri **Application Instances** (Istanze delle applicazioni) elenca tutte le istanze delle applicazioni sui VDA con sistema operativo multisessione e a sessione singola. Le misurazioni del tempo di inattività associate vengono visualizzate per le istanze delle applicazioni sui VDA con sistema operativo multisessione che sono rimasti inattivi per almeno 10 minuti.

> **Nota:**
>
> Le metriche Application Instances (Istanze delle applicazioni) sono disponibili sui siti di tutte le edizioni con licenza.

Utilizzare queste informazioni per identificare le istanze delle applicazioni inattive oltre un determinato periodo di tempo e per scollegarle o disconnetterle, a seconda dei casi. A tale scopo, selezionare **Filters (Filtri) > Application Instances (Istanze delle applicazioni)** e selezionare un filtro pre-salvato oppure scegliere **All Application Instances** (Tutte le istanze delle applicazioni) e creare un filtro personalizzato.

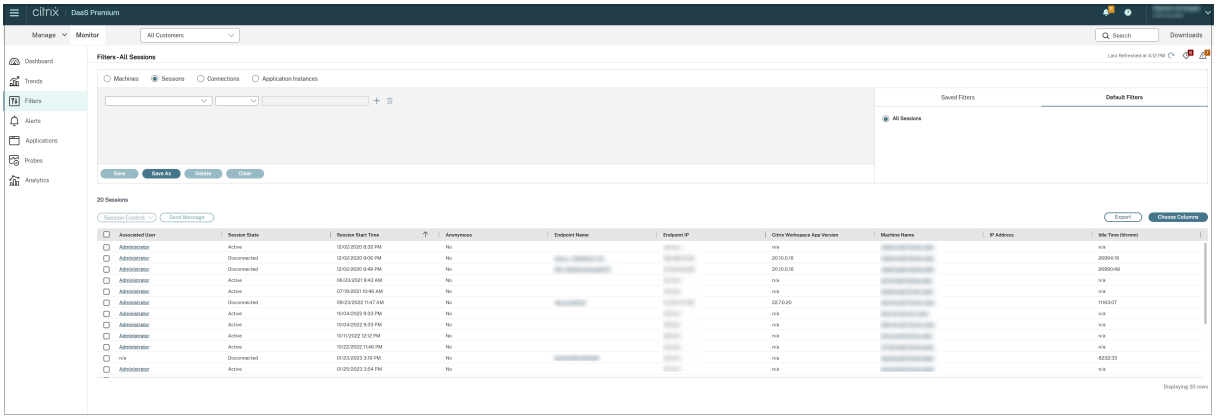
 



Un esempio di filtro è il seguente. Come criteri **Filter by** (Filtra per), scegliere **Published Name** (Nome pubblicato) dell'applicazione e **Idle Time** (Tempo di inattività). Quindi, impostare **Idle Time** (Tempo di inattività) su un valore **maggiore o uguale a** un limite di tempo specifico e salvare il filtro per riutilizzarlo. Dall'elenco filtrato, selezionare le istanze dell'applicazione. Selezionare l'opzione per inviare messaggi o scegliere **Logoff** (Scollega) o **Disconnect** (Disconnetti) dal menu a discesa **Session Control** (Controllo sessione) per terminare le istanze.

> **Nota:**
>
> Lo scollegamento o la disconnessione di un'istanza di un'applicazione scollega o disconnette la sessione corrente, terminando così tutte le istanze dell'applicazione appartenenti alla stessa sessione.

È possibile identificare le sessioni inattive dalla pagina dei filtri **Sessions** (Sessioni) utilizzando lo stato della sessione e la metrica relativa al tempo di inattività della sessione. Ordinare in base alla colonna **Idle Time** (Tempo di inattività) o definire un filtro per identificare le sessioni che sono inattive oltre un limite di tempo specifico. Il tempo di inattività è elencato per le sessioni sui VDA con sistema operativo multisessione che sono rimasti inattivi per almeno 10 minuti.



Il **tempo di inattività** viene visualizzato come **N/A** (N/D) quando la sessione o l'istanza dell'applicazione

- non è rimasta inattiva per più di 10 minuti,

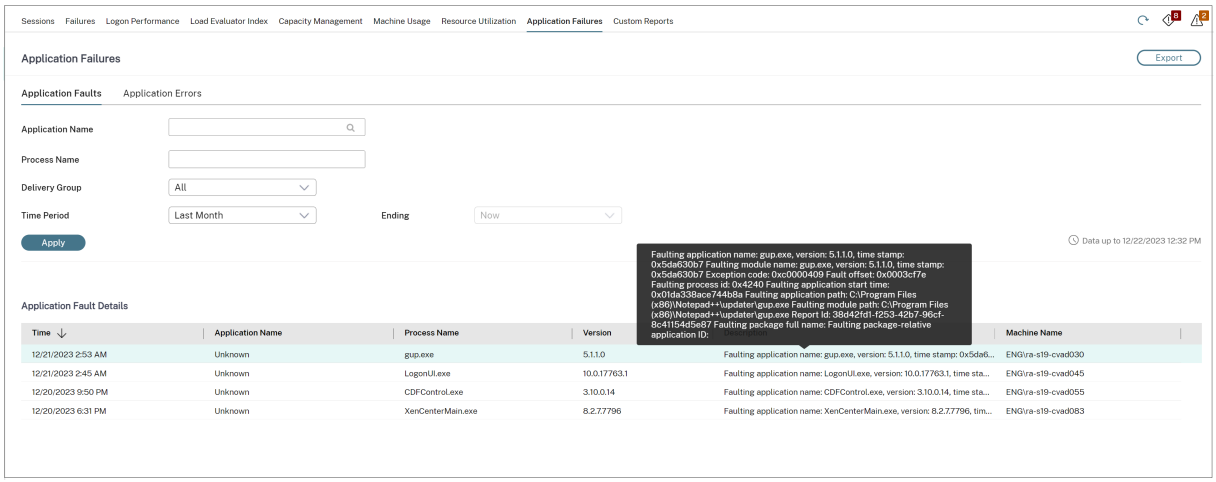
 

- viene avviata su un VDA con sistema operativo a sessione singola oppure
- viene avviata su un VDA versione 7.12 o precedente.

### Monitoraggio storico degli errori delle applicazioni

La scheda **Trends** (Tendenze) -> **Application Failures** (Errori delle applicazioni) visualizza gli errori associati alle applicazioni pubblicate sui VDA.

Per ulteriori informazioni sulla disponibilità delle tendenze relative agli errori delle applicazioni, consultare l'articolo Granularità e conservazione dei dati. Gli errori delle applicazioni registrati in Event Viewer (Visualizzatore eventi) con origine "Application errors"(Errori delle applicazioni) vengono monitorati. Fare clic su **Export** (Esporta) per generare report in formato CSV, Excel o PDF.




Gli errori vengono visualizzati come **Application Faults** (Problemi delle applicazioni) o **Application Errors** (Errori delle applicazioni) in base alla gravità. La scheda Application Faults (Problemi delle applicazioni) visualizza gli errori associati alla perdita di funzionalità o dati. La scheda Application Errors (Errori delle applicazioni) indica problemi che non sono immediatamente rilevanti e che indicano condizioni che potrebbero causare problemi futuri.

È possibile filtrare gli errori in base a **Published Application Name** (Nome dell'applicazione pubblicata), **Process Name** (Nome del processo) o **Delivery Group** (Gruppo di consegna) e **Time Period** (Periodo di tempo). La tabella mostra il codice del problema o dell'errore e una breve descrizione dell'errore. La descrizione dettagliata dell'errore viene visualizzata come una descrizione comando.

> **Nota:**
>
> Il nome dell'applicazione pubblicata viene visualizzato come "Unknown"(Sconosciuto) quando non è possibile derivare il nome dell'applicazione corrispondente. Questo si verifica in genere quando un'applicazione avviata presenta problemi in una sessione desktop o quando presenta problemi a causa di un'eccezione non gestita causata da un file eseguibile dipendente.

Per impostazione predefinita, vengono monitorati solo gli errori delle applicazioni ospitate su VDA con sistema operativo multisessione. È possibile modificare le impostazioni di monitoraggio tramite i criteri di gruppo di monitoraggio: Enable monitoring of application failures (Abilita il monitoraggio degli errori delle applicazioni), Enable monitoring of application failures on Single-session OS VDAs (Abilita il monitoraggio degli errori delle applicazioni sui VDA con sistema operativo a sessione singola) e List of applications excluded from failure monitoring (Elenco delle applicazioni escluse dal monitoraggio degli errori). Per ulteriori informazioni, vedere Criteri per il monitoraggio degli errori delle applicazioni nelle impostazioni dei criteri di monitoraggio.

La pagina **Trends** (Tendenze) **> Application Probe Results** (Risultati del probe delle applicazioni) visualizza i risultati dell'esecuzione del probe delle applicazioni nel sito per le ultime 24 ore e gli ultimi 7 giorni. Per ulteriori dettagli su come configurare i probe delle applicazioni, vedere Probe delle applicazioni.

## Probe delle applicazioni

January 18, 2023

Il probe delle applicazioni automatizza il processo di verifica dello stato delle istanze di Citrix Virtual Apps pubblicate in un sito. I risultati del probe delle applicazioni sono disponibili nella scheda **Monitor** di Citrix DaaS (in precedenza servizio Citrix Virtual Apps and Desktops). Citrix Probe Agent supporta i siti in hosting sui piani di controllo Citrix Cloud Japan e Citrix Cloud Government.

Assicurarsi che le macchine endpoint che eseguono gli agenti di probe siano macchine Windows con Citrix Receiver per Windows versione 4.8 o successiva o l'app Citrix Workspace per Windows (precedentemente chiamata Citrix Receiver per Windows) versione 1808 o successiva. L'app Workspace per Unified Windows Platform (UWP) non è supportata.

Requisiti:

- Le macchine endpoint che eseguono gli agenti di probe sono macchine Windows con Citrix Receiver per Windows versione 4.8 o successiva o l'app Citrix Workspace per Windows (precedentemente chiamata Citrix Receiver per Windows) versione 1906 o successiva. L'app Workspace per Unified Windows Platform (UWP) non è supportata.
- Citrix Probe Agent supporta l'autenticazione predefinita basata su moduli supportata da Citrix WorkSpace. Citrix Probe Agent non supporta altri metodi di autenticazione come Single Sign-On (SSO) o Multi Factor Authentication (MFA). Allo stesso modo, Citrix Probe Agent funziona solo quando non è installato un server proxy o un sistema di bilanciamento del carico come Citrix Gateway o Citrix ADC.
- Verificare che sul computer endpoint in cui si desidera installare l'agente Probe sia installato Microsoft .NET Framework versione 4.7.2 o successiva.

- Per utilizzare l'agente di probe nel piano di controllo Citrix Cloud Japan, impostare il valore del Registro di sistema nel percorso "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\A su 2. Per utilizzare l'agente di probe nel piano di controllo Citrix Cloud Government, impostare il valore del Registro di sistema nel percorso "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Prob su 3.

Account/autorizzazioni utente necessari per eseguire il probe delle applicazioni:

- Un utente unico di Workspace che esegua il probe su ciascuna macchina endpoint. L'utente di Workspace non deve necessariamente essere un amministratore; i probe possono essere eseguiti in un contesto non amministrativo.
- Account utente con autorizzazioni di amministratore Windows per installare e configurare Citrix Probe Agent sulle macchine endpoint.
- Un account utente amministratore completo con le seguenti autorizzazioni. Se si riutilizzano account utente esistenti per il probe delle applicazioni, ci si potrebbe disconnettere dalle sessioni attive degli utenti.
  - Autorizzazioni per il gruppo di consegna:
    - Di sola lettura
  - Autorizzazioni per Director:
    - Create\Edit\Remove Probe Configurations (Creazione, modifica e rimozione delle configurazioni probe)
    - Pagina View Configurations (Visualizza configurazioni)
    - Pagina View Trends (Visualizza tendenze)

### Configurare il probe delle applicazioni

Configurare l'esecuzione dei probe delle applicazioni durante le ore di minor utilizzo in più aree geografiche. I risultati completi del probe possono aiutare a risolvere i problemi relativi alle applicazioni, alla macchina di hosting o alla connessione prima che gli utenti li riscontrino.

Citrix Probe Agent versione 2103 supporta l'aggregazione del sito. Le applicazioni e i desktop possono essere enumerati e avviati da siti aggregati. Quando si configura l'agente di probe, selezionare l'opzione **Workspace (StoreFront) Site Aggregation Enabled** (Aggregazione del sito Workspace [StoreFront] abilitata) per abilitare l'enumerazione di applicazioni e desktop dai siti aggregati. Sono supportate le seguenti combinazioni di siti:

- Più siti locali con un URL StoreFront.
- Siti locali e cloud con un URL StoreFront o Workspace.
- Più siti cloud con un unico URL Workspace.

> **Nota:**
>
> È necessario creare amministratori o utenti separati per configurare i probe che hanno accesso a un solo sito.

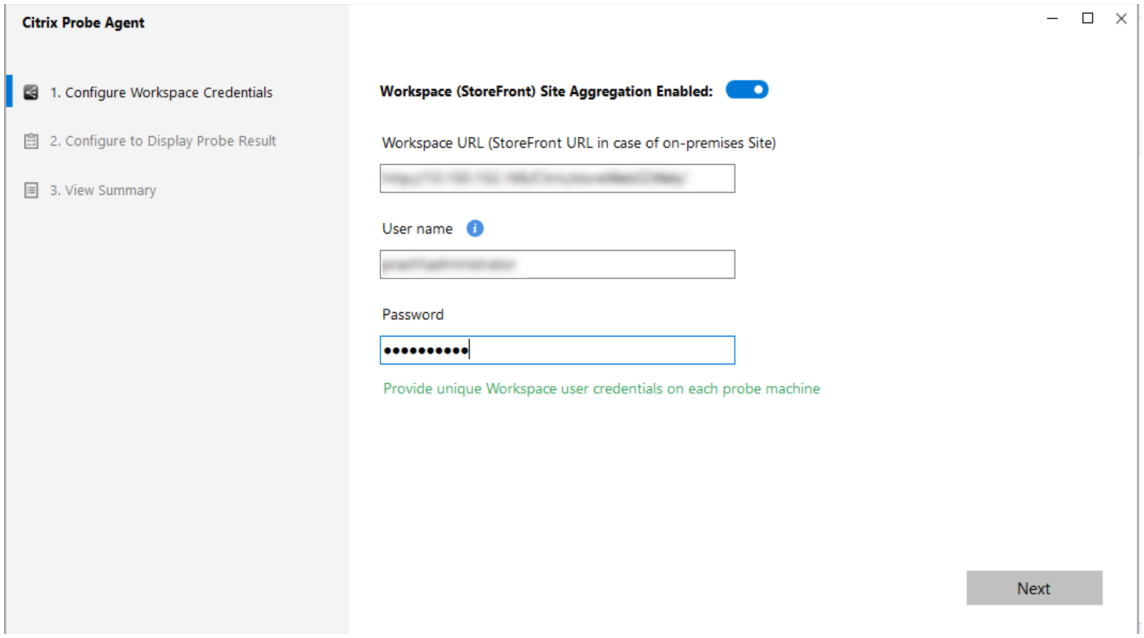
**Passaggio 1: installare e configurare Citrix Probe Agent**

Citrix Probe Agent è un file eseguibile di Windows che simula l'avvio effettivo dell'applicazione da parte dell'utente tramite Citrix Workspace. Verifica gli avvii dell'applicazione in base alla configurazione in Monitor e restituisce i risultati a Monitor.

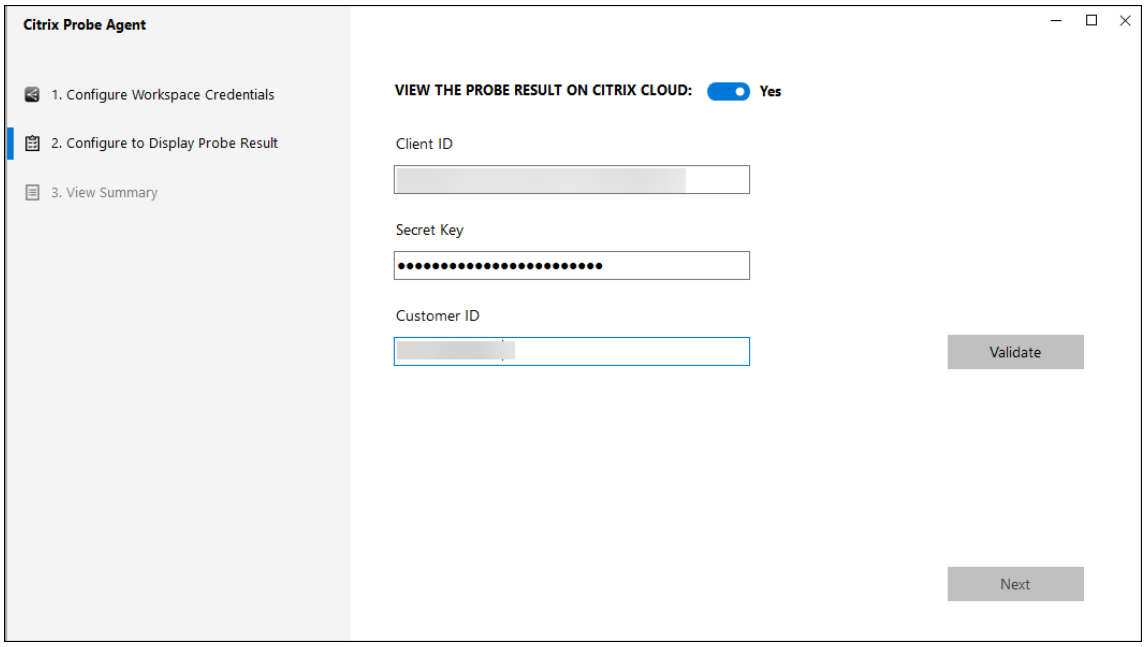
1. Identificare le macchine endpoint da dove si desidera eseguire il probe delle applicazioni.
2. Gli utenti con privilegi amministrativi possono installare e configurare Citrix Probe Agent sulla macchina endpoint. Scaricare il file eseguibile Citrix Probe Agent disponibile all'indirizzo https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Avviare l'agente e configurare le credenziali Citrix Workspace. Configurare un utente Workspace univoco su ogni computer endpoint. Le credenziali sono crittografate e archiviate in modo sicuro.

   > **Note:**
   >
   > - Per accedere al sito da sottoporre a probe dall'esterno della rete, digitare l'URL di accesso a Citrix Gateway nel campo **Workspace URL** (URL Workspace). Citrix Gateway instrada automaticamente la richiesta all'URL Workspace del sito corrispondente.
   > - Utilizzare NetBIOS come nome di dominio nel campo del nome utente. Ad esempio, NetBIOS/nome utente.
   > - Il probe delle app supporta il servizio Citrix Content Collaboration utilizzando l'autenticazione Workspace (solo AD).




4. Nella scheda **Configure To Display Probe Result** (Configura per visualizzare i risultati del probe), immettete le credenziali per accedere a Citrix DaaS. È possibile trovare il nome cliente o l'ID cliente, l'ID client e la chiave segreta dalla pagina di accesso API nella console di Citrix Cloud.




**Passaggio 2: configurare il probe delle applicazioni nella scheda Monitor**

1. In Citrix DaaS, accedere a **Configuration** > **Probe Configuration** (Configurazione del probe) > **Application Probe** (Probe dell'applicazione) e fare clic su **Create Probe** (Crea probe).

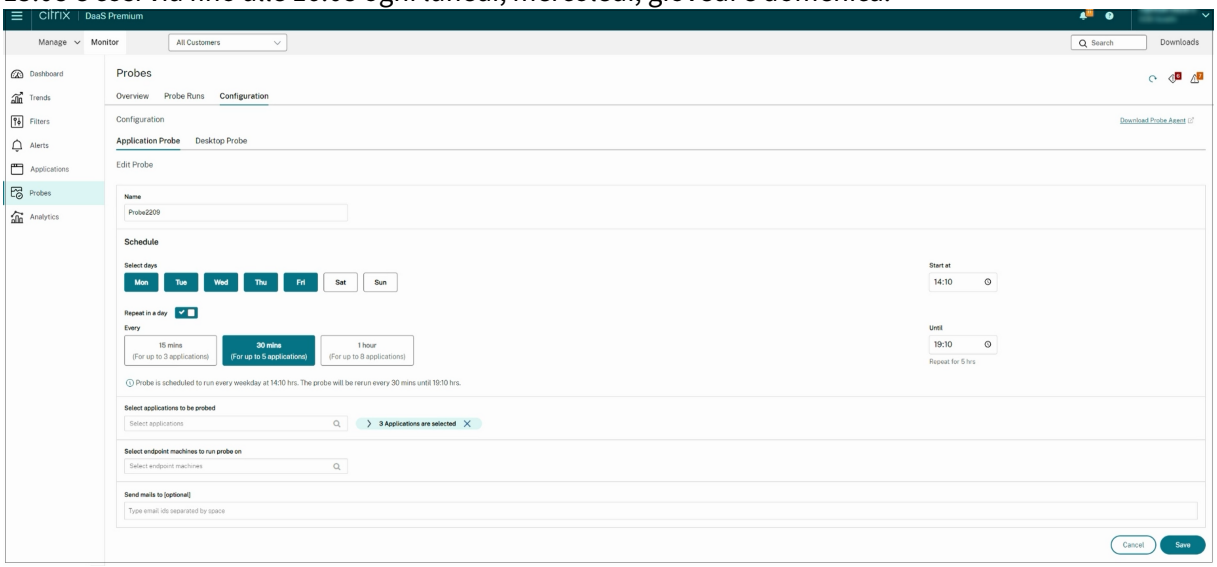
 

2. Nella pagina **Create Probe**, inserire il nome del probe.
3. Seleziona il programma:

    a) Scegliere i giorni della settimana in cui si intende eseguire il probe.
    b) Inserire l'ora di inizio in cui si intende eseguire il probe.
    c) È inoltre possibile scegliere l'opzione **Repeat in a day** (Ripeti in un giorno). Inserire l'ora di fine e l'intervallo in cui si intende ripetere il probe nello stesso giorno. Ad esempio, la configurazione seguente consente di eseguire il probe delle applicazioni dalle 12:08 alle 16:34, con una ripetizione ogni 30 minuti tutti i lunedì, i mercoledì, i giovedì e le domeniche.

4. Selezionare il numero consigliato di applicazioni da sottoporre a probe in base all'intervallo.
5. Selezionare le macchine endpoint su cui deve essere eseguito il probe.
6. Immettere gli indirizzi e-mail a cui vengono inviati i risultati dell'errore di probe e fare clic su **Save**.

In questa configurazione, le sessioni dell'applicazione vengono avviate alle 12:08, alle 12:38, alle 13:08 e così via fino alle 16:08 ogni lunedì, mercoledì, giovedì e domenica.




**Nota:**

- Configurare il server e-mail in **Alerts** (Avvisi) > **Email Server Configuration** (Configurazione server e-mail).
- Dopo la configurazione nella scheda **Monitor**, l'agente esegue i probe configurati a partire dall'ora successiva.
- I probe configurati prima dell'introduzione dell'opzione **Repeat in a day** continuano a essere eseguiti all'ora pianificata. Per impostazione predefinita, l'opzione **Repeat in a day** è disabilitata.

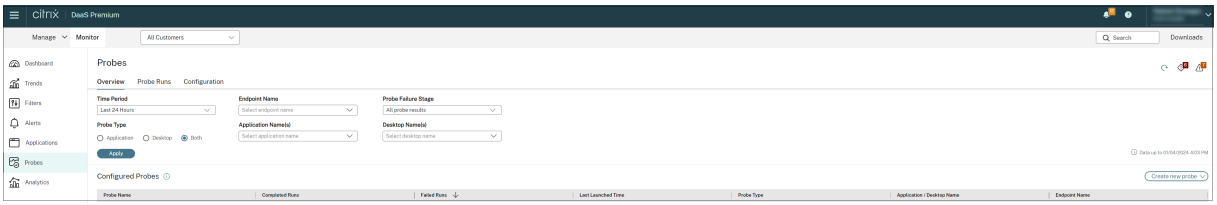
#### Passaggio 3: esecuzione del probe

L'agente esegue il probe dell'applicazione secondo la configurazione di probe che recupera da Monitor ogni ora. Avvia le applicazioni selezionate in serie utilizzando Workspace. L'agente restituisce i risultati a Monitor tramite il database Monitor. Gli errori vengono segnalati in cinque fasi specifiche:

- **Raggiungibilità di Workspace**: l'URL di Workspace configurato non è raggiungibile.
- **Autenticazione di Workspace**: le credenziali configurate di Workspace non sono valide.
- **Enumerazione Workspace**: l'elenco delle applicazioni Workspace enumerate non contiene l'applicazione di cui eseguire il probe.
- **ICA download** (Download ICA): il file ICA non è disponibile.
- **Application launch** (Avvio dell'applicazione): l'applicazione non può essere avviata.

#### Passaggio 4: visualizzare i risultati del probe

È possibile visualizzare i risultati più recenti del probe nella pagina Citrix DaaS > **Applications** (Applicazioni).




Per risolvere ulteriormente i problemi, fare clic sul collegamento dei risultati del probe per visualizzare ulteriori dettagli nella pagina **Trends** (Tendenze) > **Application Probe Results** (Risultati del probe delle applicazioni).

I dati consolidati dei risultati del probe sono disponibili per le ultime 24 ore o gli ultimi 7 giorni in questa pagina. È possibile vedere lo stadio in cui il probe è stato interrotto. È possibile filtrare la tabella per un'applicazione, uno stadio di errore del probe o una macchina endpoint specifici.

## Probe dei desktop

February 13, 2023

Il probe dei desktop automatizza il processo di verifica dello stato delle istanze di Citrix Virtual Desktops pubblicate in un sito. I risultati del probe dei desktop sono disponibili in Monitor. Citrix Probe Agent ora supporta i siti in hosting sui piani di controllo Citrix Cloud Japan e Citrix Cloud Government.

Nella pagina Configuration (Configurazione) di Monitor, configurare i desktop da sottoporre a probe, le macchine endpoint su cui eseguire il probe e l'ora del probe. L'agente verifica l'avvio di desktop selezionati utilizzando Workspace e restituisce i risultati a Monitor. I risultati del probe vengono visualizzati nell'interfaccia utente di Monitor (i dati delle ultime 24 ore nella pagina Applications [Applicazioni] e i dati storici del probe nella pagina **Trends [Tendenze] > Probe Results [Risultati probe] > Desktop Probe Results [Risultati del probe dei desktop]**).

Qui si può vedere la fase in cui si è verificato l'errore del probe: Workspace Reachability (Raggiungibilità di Workspace), Workspace Authentication (Autenticazione di Workspace), Workspace Enumeration (Enumerazione di Workspace), ICA download (Download ICA) o Desktop launch (Avvio desktop). Il report degli errori viene inviato agli indirizzi e-mail configurati.

È possibile pianificare l'esecuzione dei probe dei desktop durante le ore di minor utilizzo in più aree geografiche. I risultati completi possono aiutare a risolvere in modo proattivo i problemi relativi ai desktop di cui è stato eseguito il provisioning, alle macchine di hosting o alle connessioni prima che gli utenti li riscontrino.

Questa funzionalità richiede Probe Agent 1903 o versione successiva.

Requisiti:

- Le macchine endpoint che eseguono gli agenti di probe sono macchine Windows con Citrix Receiver per Windows versione 4.8 o successiva o l'app Citrix Workspace per Windows (precedentemente chiamata Citrix Receiver per Windows) versione 1906 o successiva. L'app Workspace per Unified Windows Platform (UWP) non è supportata.
- Citrix Probe Agent supporta l'autenticazione predefinita basata su moduli supportata da StoreFront e Citrix WorkSpace. Citrix Probe Agent non supporta altri metodi di autenticazione come Single Sign-On (SSO) o Multi Factor Authentication (MFA). Allo stesso modo, Citrix Probe Agent funziona solo quando non è installato un server proxy o un sistema di bilanciamento del carico come Citrix Gateway o Citrix ADC.
- Verificare che sul computer endpoint in cui si desidera installare l'agente Probe sia installato Microsoft .NET Framework versione 4.7.2 o successiva.
- Per utilizzare l'agente di probe nel piano di controllo Citrix Cloud Japan, impostare il valore del Registro di sistema nel percorso "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\A
su 2. Per utilizzare l'agente di probe nel piano di controllo Citrix Cloud Government, impostare il valore del Registro di sistema nel percorso "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Prob
su 3.

Account utente o autorizzazioni necessarie per eseguire il probe dei desktop:

- Un utente unico di Workspace che esegua il probe su ciascuna macchina endpoint. L'utente di Workspace non deve necessariamente essere un amministratore; i probe possono essere eseguiti in un contesto non amministrativo.

- Account utente con autorizzazioni di amministratore Windows per installare e configurare Citrix Probe Agent sulle macchine endpoint.
- Un account utente amministratore completo o un ruolo personalizzato con le seguenti autorizzazioni. Se si riutilizzano normali account utente per il probe dei desktop, le sessioni attive degli utenti potrebbero essere scollegate.
  - Autorizzazioni per il gruppo di consegna:
    - Di sola lettura
  - Autorizzazioni di Monitor:
    - Create, Edit, Remove Alert Email Server Configuration (Creazione, modifica e rimozione della configurazione del server e-mail per gli avvisi), se il server e-mail non è già configurato
    - Create, Edit, Remove Probe Configurations (Creazione, modifica e rimozione delle configurazioni probe)
    - Pagina View Configurations (Visualizza configurazioni)
    - Pagina View Trends (Visualizza tendenze)

## Configurare il probe dei desktop

È possibile pianificare l'esecuzione dei probe dei desktop durante le ore di minor utilizzo in più aree geografiche. I risultati completi del probe possono aiutare a risolvere i problemi relativi ai desktop, alle macchine di hosting o alla connessione prima che gli utenti li riscontrino.

Citrix Probe Agent versione 2103 supporta l'aggregazione del sito. Le applicazioni e i desktop possono essere enumerati e avviati da siti aggregati. Quando si configura l'agente di probe, selezionare l'opzione **Workspace (StoreFront) Site Aggregation Enabled** (Aggregazione del sito Workspace [StoreFront] abilitata) per abilitare l'enumerazione di applicazioni e desktop dai siti aggregati. Sono supportate le seguenti combinazioni di siti:

- Più siti locali con un URL StoreFront.
- Siti locali e cloud con un URL StoreFront o Workspace.
- Più siti cloud con un unico URL Workspace.

> **Nota:**
>
> È necessario creare amministratori o utenti separati per configurare i probe che hanno accesso a un solo sito.

### Passaggio 1: installare e configurare Citrix Probe Agent

Citrix Probe Agent è un file eseguibile di Windows che simula l'effettivo avvio dei desktop da parte dell'utente tramite Workspace. Verifica gli avvii dei desktop in base alla configurazione in Monitor e

restituisce i risultati a Monitor.

1. Identificare le macchine endpoint da dove si desidera eseguire il probe dei desktop.
2. Gli utenti con privilegi amministrativi possono installare e configurare Citrix Probe Agent sulla macchina endpoint. Scaricare il file eseguibile Citrix Probe Agent disponibile all'indirizzo https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Avviare l'agente e configurare il proprio Workspace Receiver per le credenziali Web. Configurare un utente Workspace univoco su ogni computer endpoint. Le credenziali sono crittografate e archiviate in modo sicuro.

   > **Note:**
   >
   > - Per accedere al sito da sottoporre a probe dall'esterno della rete, digitare l'URL della pagina di accesso a Citrix Gateway nel campo Workspace URL. Citrix Gateway instrada automaticamente la richiesta all'URL Workspace del sito corrispondente. Questa funzionalità è disponibile per Citrix Gateway versione 12.1 o successiva.
   > - Utilizzare NetBIOS come nome di dominio nel campo del nome utente. Ad esempio, NetBIOS/nome utente.
   > - Il probe dei desktop supporta il servizio Citrix Content Collaboration utilizzando l'autenticazione Workspace (solo AD).
   > - È necessario abilitare Interactive Logon (Accesso interattivo) per l'utente StoreFront univoco configurato.

4. Nella scheda **Configure To Display Probe Result** (Configura per visualizzare i risultati del probe), immettere le proprie credenziali di Monitor. È possibile trovare il nome cliente o l'ID cliente, l'ID client e la chiave segreta dalla pagina di accesso API nella console di Citrix Cloud.

#### Passaggio 2: configurare il probe dei desktop in Monitor

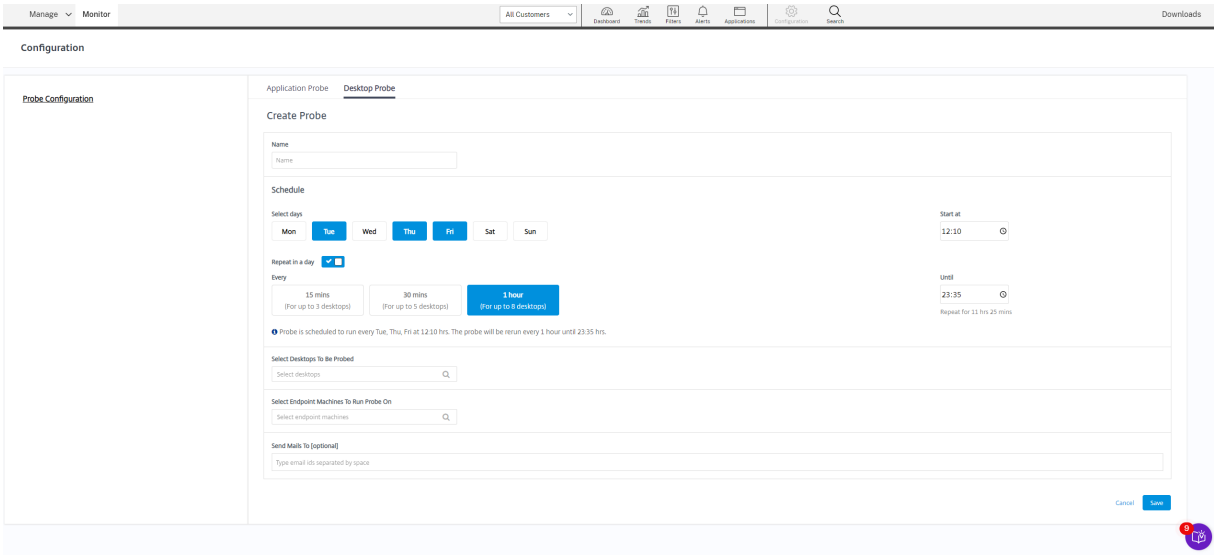
1. In Citrix DaaS, accedere a **Configuration** > **Probe Configuration** (Configurazione del probe) > **Application Probe** (Probe dell'applicazione) e fare clic su **Create Probe** (Crea probe).
2. Nella pagina **Create Probe**, inserire il nome del probe.
3. Seleziona il programma:

   a) Scegliere i giorni della settimana in cui si intende eseguire il probe.
   b) Inserire l'ora di inizio in cui si intende eseguire il probe.
   c) È inoltre possibile scegliere l'opzione **Repeat in a day** (Ripeti in un giorno). Inserire l'ora di fine e l'intervallo in cui si intende ripetere il probe nello stesso giorno. Ad esempio, la configurazione seguente consente di eseguire probe dei desktop dalle 12:10 alle 23:35 con ripetizione ogni ora tutti i martedì, i giovedì e i venerdì.

4. Selezionare il numero consigliato di desktop da sottoporre a probe in base all'intervallo.
5. Selezionare le macchine endpoint su cui deve essere eseguito il probe.
6. Immettere gli indirizzi e-mail a cui vengono inviati i risultati dell'errore di probe e fare clic su **Save**.

In questa configurazione, le sessioni desktop vengono avviate alle 12:10, alle 13:10, alle 14:10 e così via fino alle 23:10 ogni martedì, giovedì e venerdì.




**Nota:**

- Configurare il server e-mail in **Alerts** (Avvisi) > **Email Server Configuration** (Configurazione server e-mail).
- Dopo che la configurazione del probe dei desktop è stata completata, l'agente esegue i probe configurati a partire dall'ora successiva.
- I probe configurati prima dell'introduzione dell'opzione **Repeat in a day** continuano a essere eseguiti all'ora pianificata. Per impostazione predefinita, l'opzione **Repeat in a day** è disabilitata.

### Passaggio 3: esecuzione del probe

L'agente esegue il probe dei desktop in base alla configurazione probe che recupera periodicamente da Monitor. Avvia i desktop selezionati in serie utilizzando Workspace. L'agente restituisce i risultati a Monitor tramite il database Monitor. Gli errori vengono segnalati in cinque fasi specifiche:

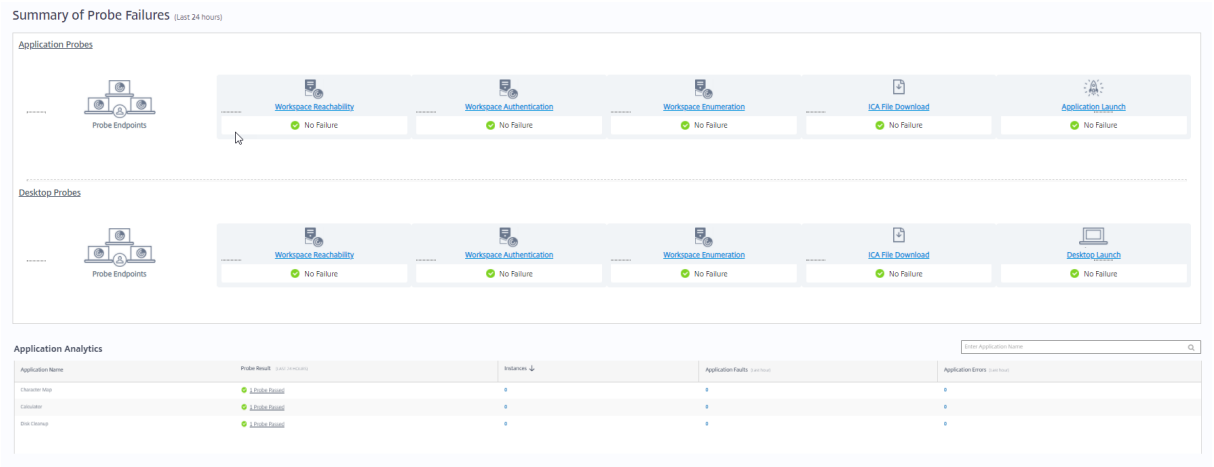
- **Raggiungibilità di Workspace**: l'URL di Workspace configurato non è raggiungibile.
- **Autenticazione di Workspace**: le credenziali configurate di Workspace non sono valide.
- **Enumerazione dell'area di lavoro**: l'elenco dei desktop di Workspace Enumerate non contiene il desktop di cui eseguire il probe.

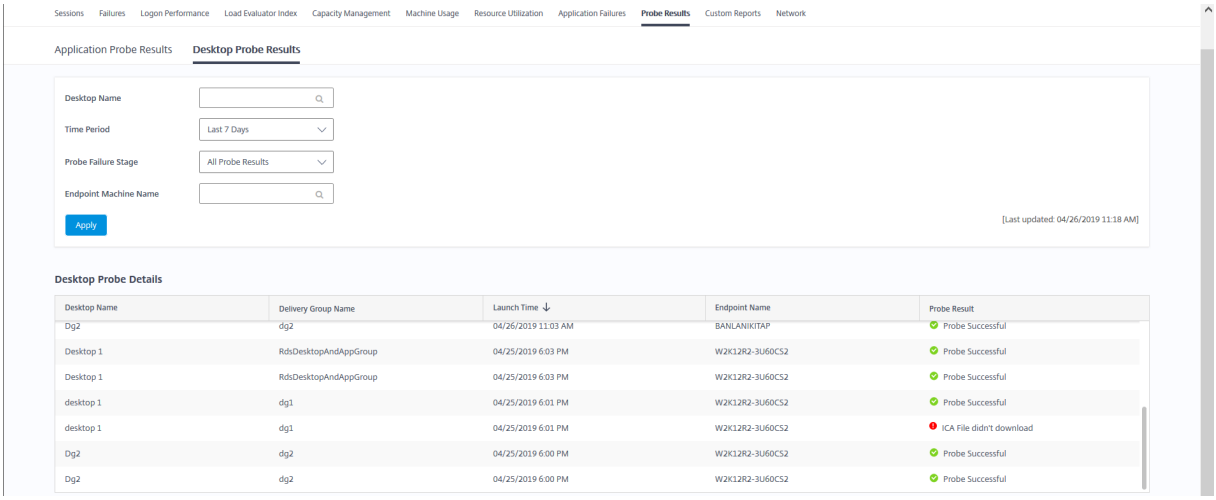
- **ICA download** (Download ICA): il file ICA non è disponibile.
- **Desktop launch** (Avvio desktop): il desktop non può essere avviato.

### Passaggio 4: visualizzare i risultati del probe

È possibile visualizzare i risultati più recenti del probe nella pagina **Desktops**.




Per risolvere ulteriormente i problemi, fare clic sul collegamento dei risultati del probe per visualizzare ulteriori dettagli nella pagina **Trends** (Tendenze) > **Probe Results** (Risultati del probe) > **Desktop Probe Results** (Risultati del probe dei desktop).




I dati consolidati dei risultati del probe sono disponibili per le ultime 24 ore o gli ultimi 7 giorni in questa pagina. È possibile vedere lo stadio in cui il probe è stato interrotto. È possibile filtrare la tabella per un desktop, uno stadio di errore del probe o una macchina endpoint specifici.

# Risolvere i problemi relativi alle macchine

December 18, 2023

> **Nota:**
>
> **Citrix Health Assistant** è uno strumento per risolvere i problemi di configurazione nei VDA non registrati. Lo strumento automatizza una serie di controlli dello stato per identificare le possibili cause principali degli errori di registrazione dei VDA e dei problemi relativi all'avvio della sessione e alla configurazione del reindirizzamento del fuso orario. L'articolo del Knowledge Center Citrix Health Assistant - Risolvere i problemi relativi alla registrazione dei VDA e all'avvio della sessione contiene le istruzioni per il download e l'uso dello strumento **Citrix Health Assistant**.

La vista **Filters (Filtri) > Machines (Macchine)** nella scheda Monitor visualizza le macchine configurate nel sito. La scheda Multi-session OS Machines (Macchine con sistema operativo multisessione) include l'indice di valutazione del carico, che indica la distribuzione dei contatori delle prestazioni e le descrizioni dei comandi del conteggio delle sessioni se si passa il mouse sul collegamento.

Fare clic sulla colonna **Failure Reason** (Motivo dell'errore) di una macchina che presenta un problema per ottenere una descrizione dettagliata dell'errore e delle azioni consigliate per risolverlo. I motivi degli errori e le azioni consigliate per gli errori delle macchine e delle connessioni sono disponibili nella Guida alla risoluzione dei problemi per i motivi degli errori di Citrix Director.

Fare clic sul collegamento del nome della macchina per andare alla pagina **Machine Details** (Dettagli macchina).

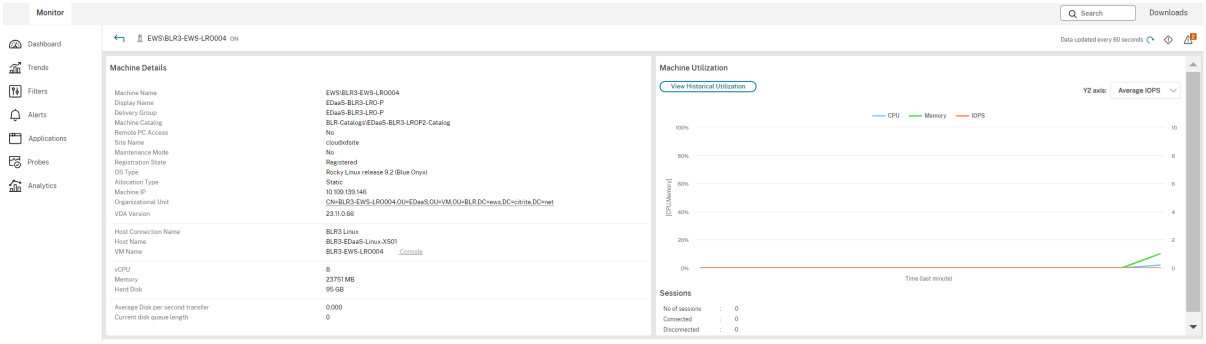
La pagina Machine Details (Dettagli macchina) elenca i dettagli della macchina, i dettagli dell'infrastruttura e i dettagli degli aggiornamenti rapidi applicati alla macchina.

## Utilizzo delle risorse in tempo reale basato sulla macchina

Il pannello **Machine Utilization** (Utilizzo macchina) visualizza grafici che mostrano l'utilizzo in tempo reale di CPU e memoria. Inoltre, i grafici relativi al monitoraggio del disco e della GPU sono disponibili per i VDA versione 7.14 e successive.

I grafici di monitoraggio del disco, gli IOPS medi e la latenza del disco sono importanti misurazioni delle prestazioni che consentono di monitorare e risolvere i problemi relativi ai dischi dei VDA. Il grafico Average IOPS (IOPS medi) visualizza il numero medio di letture e scritture su un disco. Selezionare **Disk Latency** (Latenza del disco) per visualizzare un grafico del ritardo tra una richiesta di dati e il relativo ritorno dal disco, misurato in millisecondi.




### Utilizzo della GPU

Selezionare **GPU Utilization** (Utilizzo della GPU) per visualizzare la percentuale di utilizzo della GPU, della memoria della GPU, del codificatore e del decodificatore per risolvere i problemi relativi alla GPU sui VDA con sistema operativo multisessione o a sessione singola.

**Versioni di GPU supportate:**

- GPU NVIDIA Tesla M60 con Display Driver versione 369.17 o successiva. Per ulteriori informazioni, vedere NVIDIA vGPU Software.
- CPU AMD Radeon Instinct MI25 GPUs e AMD EPYC 7V12(Rome). Per ulteriori informazioni, vedere AMD Drivers and Support.

**Driver:**

Sui VDA devono essere installati i driver o le estensioni appropriati.

- Per le GPU NVIDIA, installare i driver GRID manualmente o tramite estensioni. Per ulteriori informazioni, vedere NVIDIA vGPU Software.
  - Si noti che per NVIDIA sono supportati solo i driver GRID. I driver CUDA non funzionano con la serie NVadsA10 v5 e non sono supportati.
  - Per un processo di esempio di installazione dei driver GPU Nvidia Grid tramite estensioni su macchine basate su Azure, vedere Driver NVIDIA GRID. Estensione del driver GPU NVIDIA - VM Windows di Azure - Macchine virtuali di Azure.
  - Per un processo di esempio di installazione manuale dei driver GPU Nvidia Grid, vedere Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- Per le GPU AMD, installare i driver grafici AMD manualmente o tramite estensioni. Per ulteriori informazioni, vedere AMD Drivers and Support.
  - Per un processo di esempio dell'installazione dei driver GPU AMD tramite estensioni su macchine basate su Azure, vedere AMD GPU Driver Extension - Azure Windows VMs - Macchine virtuali di Azure.

  - Per un processo di esempio dell'installazione manuale dei driver GPU AMD su macchine Azure, vedere Install AMD GPU drivers on N-series VMs running Windows.

**Note d'uso:**

- I grafici di utilizzo della GPU sono disponibili solo per i VDA che eseguono Windows a 64 bit.
- I grafici di utilizzo della GPU AMD sono disponibili solo per i VDA che eseguono Citrix Virtual Apps and Desktops 7 2212 o versioni successive.
- Sui VDA deve essere abilitato HDX 3D Pro per fornire l'accelerazione della GPU. Per ulteriori informazioni, vedere Accelerazione GPU per sistema operativo Windows a sessione singola e Accelerazione GPU per sistema operativo multisessione Windows.
- Quando un VDA accede a più di una GPU, il grafico di utilizzo visualizza la media delle metriche della GPU raccolte dalle singole GPU. Le metriche della GPU vengono raccolte per l'intero VDA e non per i singoli processi.
- Per AMD, l'utilizzo di encoder e decoder non è supportato separatamente. Qualsiasi carico di lavoro di codifica/decodifica che utilizza la GPU verrà segnalato come carico 3D generale sull'utilizzo della GPU.
- Assicurarsi di installare la WMI NVIDIA durante l'installazione. Questa finestra è disponibile solo durante l'installazione manuale.
- Se i driver sono installati ma Director non rileva la GPU
  - Controllare Task Manager (Gestione attività). Se i driver sono installati correttamente, la GPU dovrebbe essere visualizzata in Task Manager.
  - Controllare se la macchina è registrata. A volte può trascorrere del tempo prima che sia rilevata la presenza online delle macchine.
- Se l'utilizzo della GPU non mostra alcuna attività in Director, assicurarsi che il carico di lavoro in esecuzione utilizzi la GPU. Per i carichi di lavoro grafici, questo può essere abilitato da Impostazioni > Sistema > Schermo > Impostazioni grafiche > scegliere l'app di cui impostare le preferenze. Assicurarsi di attivare le prestazioni elevate. A volte, Windows utilizza per impostazione predefinita la CPU per i carichi di lavoro grafici quando questa è impostata sui valori predefiniti del sistema o sul risparmio energetico, in base ad altre impostazioni.
- I dati vengono aggiornati ogni minuto e la visualizzazione dei dati inizia entro un minuto dalla selezione di **GPU Utilization**.

### Utilizzo storico delle risorse basato sulla macchina

Nel pannello **Machine Utilization** (Utilizzo macchina), fare clic su **View Historical Utilization** (Visualizza utilizzo storico) per visualizzare l'utilizzo storico delle risorse sulla macchina selezionata.
I grafici di utilizzo includono contatori critici delle prestazioni di CPU, memoria, sessioni simultanee di picco, IOPS medio e latenza del disco.

> **Nota:**
>
> L'impostazione dei criteri di monitoraggio **Enable Process Monitoring**(Abilita monitoraggio processo) deve essere impostata su Allowed (Consentito) per raccogliere e visualizzare i dati nella tabella Top 10 Processes (Primi 10 processi) della pagina Historic Machine Utilization (Utilizzo storico della macchina). La raccolta è vietata per impostazione predefinita.

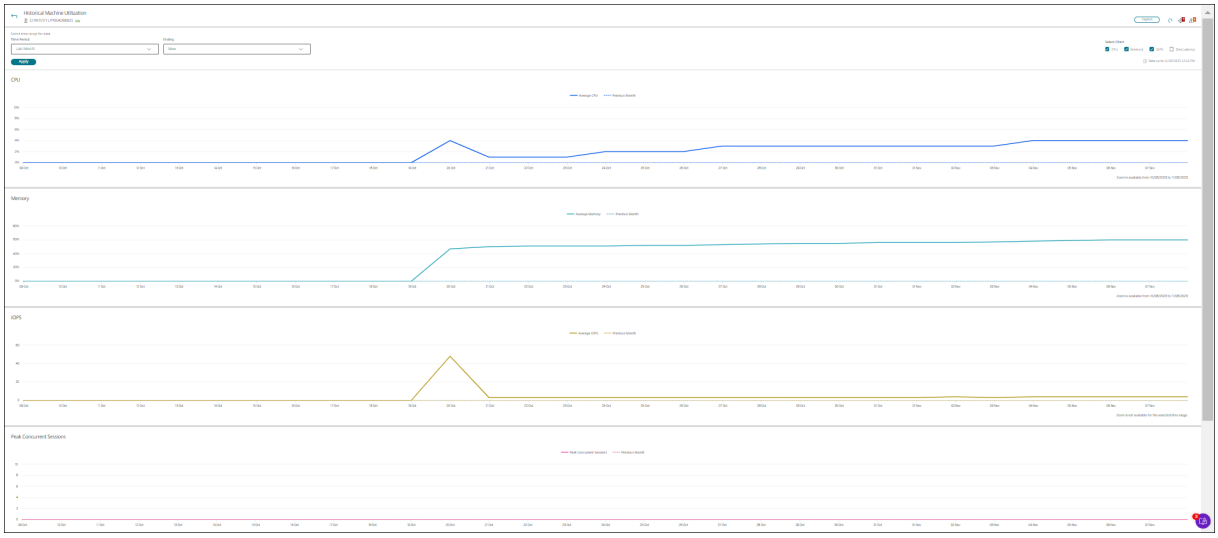
I dati relativi all'utilizzo della CPU e della memoria, agli IOPS medi e alla latenza del disco vengono raccolti per impostazione predefinita. È possibile disabilitare la raccolta utilizzando l'impostazione dei criteri **Enable Resource Monitoring** (Abilita monitoraggio delle risorse).


1. Dal pannello **Machine Utilization** (Utilizzo macchina) nella vista **Machine Details** (Dettagli macchina), selezionare **View Historical Utilization** (Visualizza utilizzo storico).
2. Nella pagina **Historical Machine Utilization** (Utilizzo storico della macchina), impostare **Time Period** (Periodo di tempo) per visualizzare l'utilizzo nelle ultime 2 ore, nelle ultime 24 ore, negli ultimi 7 giorni, nell'ultimo mese o nell'ultimo anno.

   > **Nota:**
   >
   > I dati medi di utilizzo degli IOPS e della latenza del disco sono disponibili solo per le ultime 24 ore, l'ultimo mese e l'anno corrente. L'ora di fine personalizzata non è supportata.

3. Fare clic su **Apply** (Applica) e selezionare i grafici richiesti.
4. Passare il mouse sulle diverse sezioni del grafico per visualizzare ulteriori informazioni per il periodo di tempo selezionato.



Ad esempio, se si seleziona **Last 2 hours** (Ultime 2 ore), il periodo di base sono le 2 ore precedenti l'intervallo di tempo selezionato. Visualizzare le tendenze della CPU, della memoria e della sessione nelle ultime 2 ore e all'ora di base. Se si seleziona **Last month** (Ultimo mese), il periodo di base è il mese precedente. Selezionare questa opzione per visualizzare gli IOPS e la latenza del disco medi nell'ultimo mese e all'ora di base.

1. Fare clic su **Export** (Esporta) per esportare i dati di utilizzo delle risorse per il periodo selezionato. Per ulteriori informazioni, vedere la sezione Esportare i report nella sezione di monitoraggio delle distribuzioni.
2. Sotto i grafici, la tabella elenca i primi 10 processi in base all'utilizzo della CPU o della memoria. È possibile ordinare i dati in base a una qualsiasi delle colonne, che mostrano Application Name (Nome applicazione), User Name (Nome utente), Session ID (ID sessione), Average CPU (CPU media), Peak CPU (CPU di picco), Average Memory (Memoria media) e Peak Memory (Memoria di picco) nell'intervallo di tempo selezionato. Le colonne IOPS e Disk Latency (Latenza del disco) non possono essere ordinate.

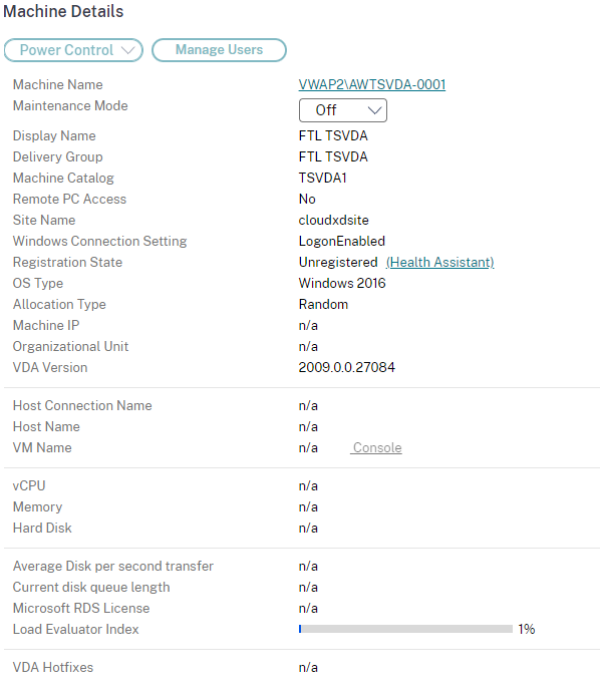
   > **Nota:**
   >
   > - L'ID di sessione per i processi di sistema viene visualizzato come "0000".
   > - Se un sito che appartiene a Citrix Cloud Japan o al piano Citrix Cloud Government contiene più di 5000 macchine, i dati di processo sono disponibili solo per un massimo di 2000 macchine. La politica di monitoraggio dei processi deve essere abilitata su queste macchine.

3. Per visualizzare la tendenza storica sul consumo di risorse di un determinato processo, eseguire il drill down di uno dei primi 10 processi.

### Accesso alla console della macchina

È possibile accedere alle console delle macchine desktop o con sistema operativo multisessione ospitati su XenServer versione 7.3 e successive direttamente da Monitor. In questo modo non è necessario che XenCenter risolva i problemi sui VDA ospitati da XenServer. Perché sia disponibile questa funzionalità, la versione dell'istanza di XenServer che ospita la macchina deve corrispondere a 7.3 o successiva e deve essere accessibile da Monitor.



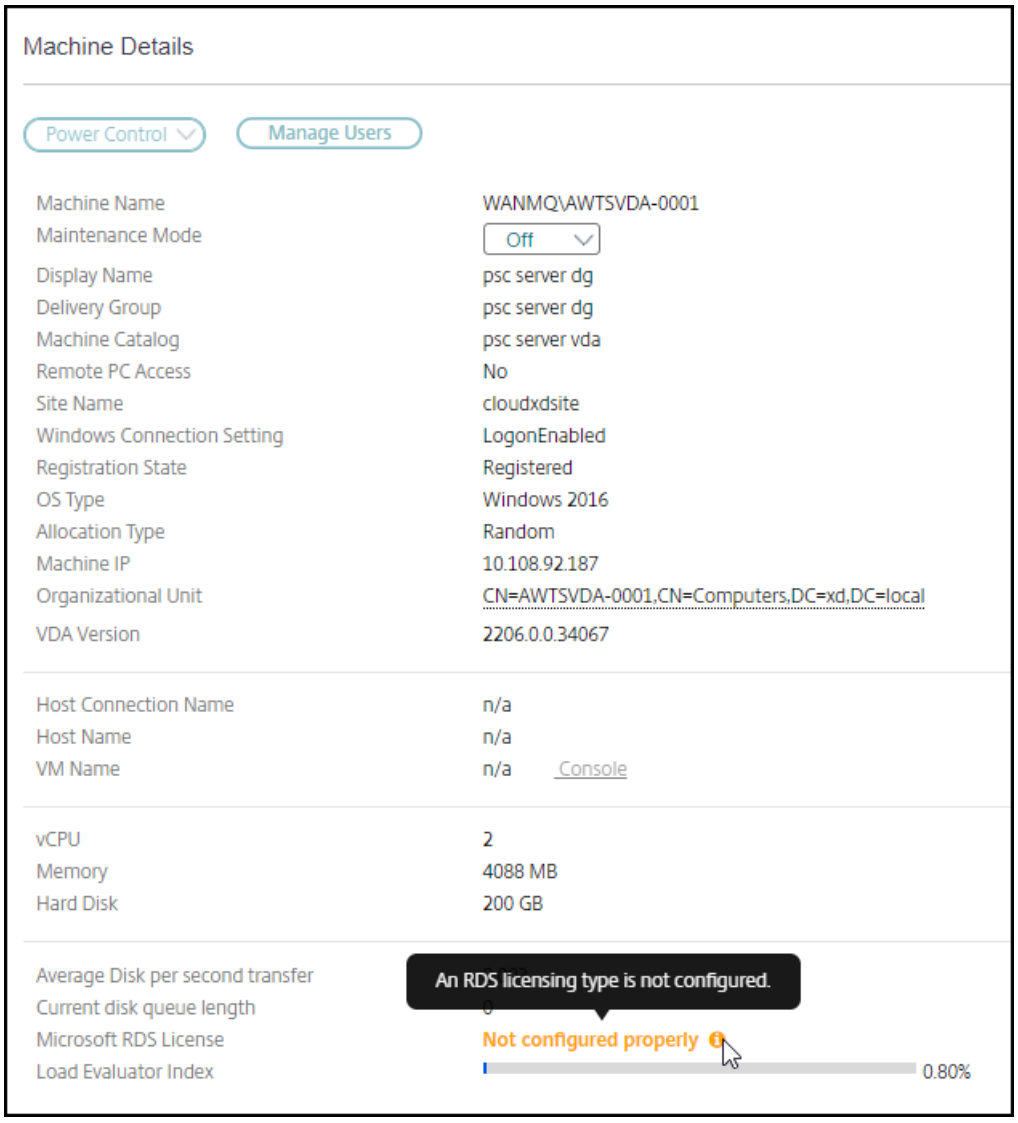

Per risolvere i problemi di una macchina, fare clic sul collegamento **Console** nel pannello Machine Details (Dettagli macchina) corrispondente. Dopo l'autenticazione delle credenziali host fornite, la console della macchina si apre in una scheda separata utilizzando noVNC, un client VNC basato sul Web. Ora si ha accesso alla console con tastiera e mouse.

> **Nota:**
>
> - Questa funzionalità non è supportata su Internet Explorer 11.
> - Se il puntatore del mouse sulla console della macchina non è allineato, vedere la procedura di risoluzione del problema in CTX230727.
> - L'accesso alla console viene avviato in una nuova scheda, assicurando che le impostazioni del browser consentano le finestre a comparsa.
> - Per motivi di sicurezza, Citrix consiglia di installare certificati SSL sul browser.

### Stato licenza Servizi Desktop remoto Microsoft

È possibile visualizzare lo stato della licenza Servizi Desktop remoto Microsoft nel pannello Machine Details (Dettagli macchina) nella pagina **Machine Details** (Dettagli macchina) e nella pagina **User Details** (Dettagli utente) per macchine con sistema operativo multisessione.




Viene visualizzato uno dei seguenti messaggi:

- License available (Licenza disponibile)
- Not configured properly (warning) (Non configurato correttamente [avviso])
- License error (error) (Errore di licenza [errore])
- Incompatible VDA version (error) (Versione VDA incompatibile [errore])

> **Nota:**
>
> Lo stato di integrità della licenza Servizi Desktop remoto per le macchine sottoposte a periodo di tolleranza con licenza valida visualizza un messaggio **License available** (Licenza disponibile) in verde. Rinnovare la licenza prima della scadenza.

Per i messaggi di avviso e di errore, passare il mouse sull'icona delle informazioni per visualizzare informazioni aggiuntive come indicato nella tabella seguente.

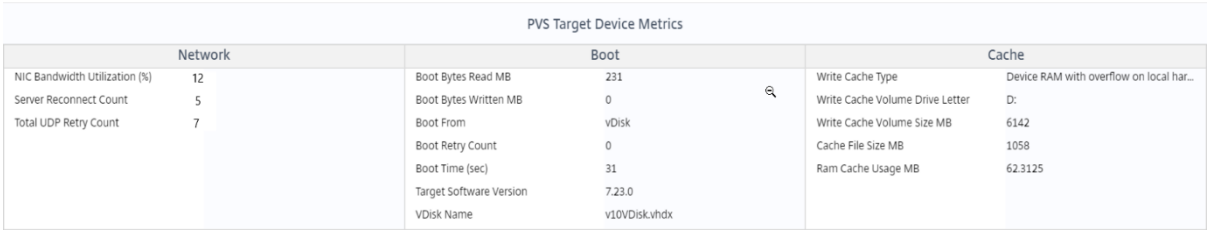
| Tipo di messaggio | Messaggi in Monitor |
|---|---|
| Errore | Disponibile per VDA versione 7.16 e successive. |
| Errore | Non sono consentite nuove connessioni RDS. |
| Errore | La licenza Servizi Desktop remoto ha superato il periodo di tolleranza. |
| Errore | Un License Server non è configurato per il livello di sistema operativo richiesto con il tipo di licenza Accesso client per dispositivo. |
| Errore | Il License Server configurato non è compatibile con il livello del sistema operativo host di Servizi Desktop remoto con il tipo di licenza Accesso client per dispositivo. |
| Avviso | Terminal Server personale non è un tipo di licenza Servizi Desktop remoto valido in una distribuzione Citrix Virtual Apps and Desktops. |
| Avviso | Desktop remoto per amministrazione non è un tipo di licenza valido in una distribuzione Citrix Virtual Apps and Desktops. |
| Avviso | Un tipo di licenza Servizi Desktop remoto non è configurato. |
| Avviso | Il controller di dominio o License Server non è raggiungibile con il tipo di licenza Servizi Desktop remoto Accesso client per utente. |
| Avviso | Con il tipo di licenza Accesso client per dispositivo, la licenza del dispositivo client non poteva essere determinata poiché il server delle licenze per il livello di sistema operativo richiesto non è raggiungibile. |

> **Nota:**
>
> Questa funzionalità è applicabile solo per CAL (licenza di accesso client) di Servizi Desktop remoto Microsoft.

### Metriche del dispositivo di destinazione PVS

È possibile visualizzare lo stato dei dispositivi di destinazione PVS per le macchine con sistema operativo a sessione singola e multisessione nella pagina **Machine Details** di Director. In questo pannello sono disponibili diverse metriche per **Network** (Rete), **Boot** (Avvio) e **Cache**. Queste metriche aiutano a monitorare i dispositivi di destinazione PVS e a risolverne i problemi per assicurarsi che siano attivi e funzionanti.




**Network (Rete):**

- Network Bandwidth Utilization: utilizzo medio della larghezza di banda in tutte le schede NIC.
- Server Reconnect Count: numero di volte in cui il server si è ricollegato a causa di problemi di rete o ribilanciamento del server o arresti e riavvii del Citrix Provisioning Stream Service.
- Total UDP Retry Count: numero di volte in cui il dispositivo di destinazione di provisioning ha tentato di riconnettersi al server di provisioning utilizzando UDP. Questa metrica aiuta a sapere se ci sono problemi di rete in Citrix Provisioning Stream Service (ad esempio, configurazioni di switch errate).

**Boot (Avvio):**

- Boot Bytes Read MB: byte letti durante l'avvio.
- Boot Bytes Written MB: byte scritti durante l'avvio.
- Boot From: supporto di avvio (vDisk, disco locale e così via).
- Boot Retry Count: numero di tentativi di avvio della macchina.
- Boot Time: tempo impiegato per avviare la macchina, in secondi. Per impostazione predefinita, vi è un ritardo di 5 secondi tra un tentativo e il successivo. Se questo ritardo diventa a doppia cifra, si verifica un aumento significativo del tempo di avvio. Controllare la configurazione del provisioning per risolvere il problema.
- Target Software Version: versione del software del dispositivo di destinazione di Provisioning.

- vDisk Name: vDisk da cui si avvia il dispositivo di destinazione di Provisioning.

**Cache:**

- Write Cache Type: vDisk può essere impostato su diversi tipi di cache. Per ulteriori informazioni, vedere l'articolo CTX119469 del Knowledge Center.
- Write Cache Volume Drive Letter: lettera di unità per i tipi di cache di scrittura che interessano le unità.
- Write Cache Volume Size MB: dimensione totale del volume configurato per la cache di scrittura.
- Cache File Size MB: dimensione attuale del file della cache (cache sulla RAM del dispositivo con overflow sul disco rigido).
- Ram Cache Usage MB: dimensione attuale della cache RAM (cache sulla RAM del dispositivo con overflow sul disco rigido). Utilizzare l'overflow su disco solo se necessario. Questa metrica è utile quando si imposta o si ottimizza la dimensione corretta della cache RAM.

Per ulteriori informazioni, vedere Using the Status Tray on a target device.

Le metriche del dispositivo di destinazione di Provisioning sono disponibili solo su:

- Macchine di Provisioning.
- Dispositivo di destinazione di Provisioning versione 7.19 e versioni successive.
- VDA versione 2003 e successive.

> **Nota:**
>
> Le metriche per il conteggio delle riconnessioni server e il conteggio dei tentativi UDP sono disponibili solo per la versione di destinazione di Provisioning 1912 CU2 e successive.

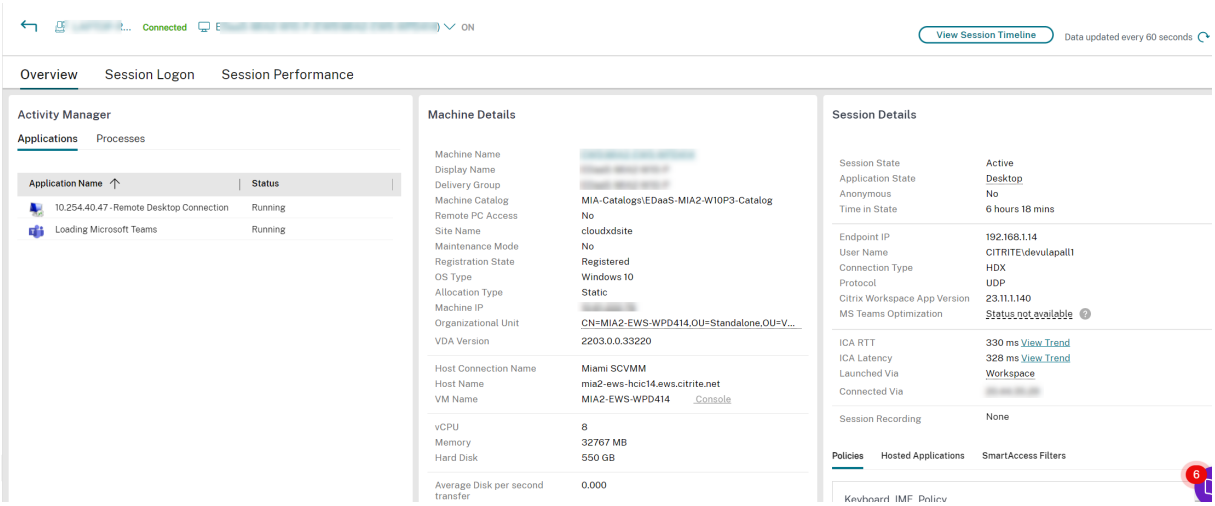
## Risolvere i problemi dell'utente

November 21, 2023

Utilizzare la vista **Help Desk** (Helpdesk) di Monitor (pagina **Activity Manager** [Gestione attività]) per visualizzare le informazioni sull'utente o sull'endpoint.

Facendo clic su **View Details** dall'Activity Manager per l'utente si apre la pagina **User Details** (Dettagli utente).
Facendo clic su **Dettagli utente** dall'Activity Manager dell'endpoint si apre la pagina **Endpoint Details** (Dettagli dell'endpoint).




Se l'utente ha avviato più di una sessione, viene visualizzato il selettore di sessione.


Scegliere una sessione per visualizzarne i dettagli.

- È possibile controllare dettagli sulla sessione, l'esperienza di accesso dell'utente, l'avvio della sessione, la connessione e le applicazioni.
- È possibile oscurare la macchina dell'utente.
- Risolvere il problema con le azioni consigliate nella tabella seguente e, se necessario, segnalare il problema all'amministratore appropriato.

### Suggerimenti per la risoluzione dei problemi

| Problema dell'utente | Suggerimenti |
|---|---|
| L'accesso richiede molto tempo o non riesce in modo intermittente o ripetuto | Diagnosticare i problemi di accesso utente |
| L'avvio della sessione richiede molto tempo o non riesce in modo intermittente o ripetuto | Diagnosticare i problemi di avvio |
| Identificare i componenti coinvolti nello stabilire la sessione | Analizzare la vista Session Topology |
| La risposta della sessione è lenta o la sessione non risponde | Diagnosticare i problemi di prestazione della sessione |
| L'applicazione è lenta o non risponde | Risolvere gli errori delle applicazioni |
| Connessione non riuscita | Ripristinare le connessioni desktop |
| La sessione è lenta o non risponde | Ripristinare le sessioni |
| Il video è lento o di scarsa qualità | Eseguire report sui sistemi di canale HDX |

> **Nota:**
>
> Per assicurarsi che la macchina non sia in modalità di manutenzione, dalla vista User Details (Dettagli utente) esaminare il riquadro Machine details (Dettagli macchina).

### Prestazioni della sessione

La scheda **Session Performance** (Prestazioni della sessione) ha migliorato i flussi di lavoro per la risoluzione dei problemi, a partire dalla capacità di correlare le metriche in tempo reale per identificare i problemi all'interno delle sessioni utente. Il pannello **Session Topology** (Topologia della sessione) fornisce una rappresentazione visiva del percorso all'interno della sessione per le sessioni HDX connesse. Il pannello **Performance Metrics** illustra le tendenze delle metriche di sessione quali ICARTT (Tempo di round trip ICA), ICA Latency (Latenza ICA), Frames Per Second (Fotogrammi per secondo), Output Bandwidth Available (Larghezza di banda in uscita disponibile) e Output Bandwidth Consumed (Larghezza di banda in uscita consumata) aiutano a indicare come queste metriche si sono comportate nel tempo. Per ulteriori informazioni, vedere Diagnosticare i problemi di prestazione della sessione.

### Suggerimenti di ricerca

La ricerca del nome utente viene eseguita in tutte le Active Directory configurate.

Quando si digita il nome di una macchina multiutente in un campo di ricerca, vengono visualizzati i dettagli della macchina specificata.

Quando si digita il nome di un endpoint in un campo di ricerca, vengono elencate le sessioni non autenticate (anonime) e autenticate connesse a un endpoint specifico. Ciò consente la risoluzione dei problemi per le sessioni non autenticate. Assicurarsi che i nomi degli endpoint siano univoci per abilitare la risoluzione dei problemi delle sessioni non autenticate.

I risultati di ricerca includono anche utenti che attualmente non utilizzano una macchina o non sono assegnati a una macchina.

- Le ricerche non fanno distinzione tra maiuscole e minuscole.
- Le voci parziali generano un elenco di possibili corrispondenze.
- Dopo aver digitato alcune lettere di un nome in due parti (nome utente, cognome e nome o nome visualizzato) separate da uno spazio, i risultati includono corrispondenze per entrambe le stringhe. Ad esempio, se si digita"jo rob", i risultati potrebbero includere stringhe come "John Robertson"o "Robert, Jones".

Per tornare alla pagina di destinazione, fare clic sulla scheda Monitor.

## Diagnosticare i problemi di avvio

October 6, 2022

Oltre alle fasi del processo di accesso menzionate nella sezione Diagnosticare i problemi di accesso degli utenti, Monitor visualizza la durata di avvio della sessione. Questa durata è suddivisa nella durata del Workspace App Session Startup (Avvio della sessione dell'app Workspace) e del VDA Session Startup (Avvio della sessione VDA) nelle pagine **User Details** (Dettagli utente) e **Endpoint Details** (Dettagli endpoint). Queste due durate contengono inoltre singole fasi di cui vengono visualizzate le durate dell'avvio. Questi dati aiutano a comprendere e risolvere i problemi di durata elevata dell'avvio delle sessioni. Inoltre, la durata di ogni fase coinvolta nell'avvio della sessione aiuta a risolvere i problemi associati alle singole fasi. Ad esempio, se il tempo di mappatura dell'unità è elevato, è possibile verificare se tutte le unità valide sono mappate correttamente nell'oggetto Criteri di gruppo o nello script.

### Prerequisiti

Assicurarsi che siano soddisfatti i seguenti prerequisiti perché vengano visualizzati i dati relativi alla durata dell'avvio delle sessioni:

- VDA 1903 o versioni successive.

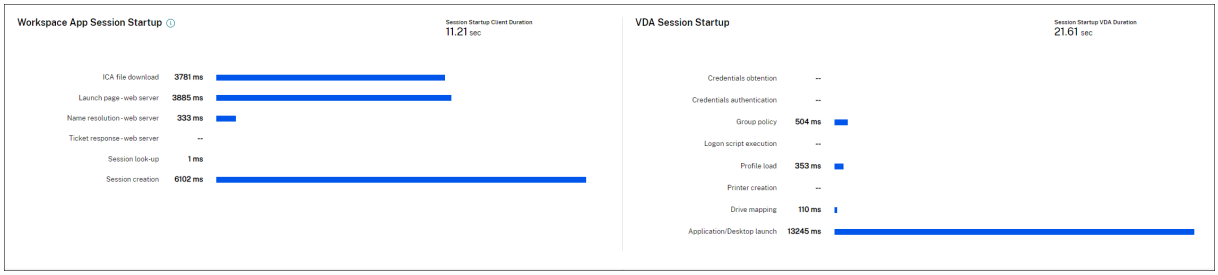
- Il servizio Citrix End User Experience Monitoring (EUEM) deve essere in esecuzione sul VDA.

## Limitazioni

Le seguenti limitazioni si applicano quando Monitor visualizza i dati relativi alla durata dell'avvio delle sessioni.

- La durata dell'avvio delle sessioni è disponibile solo per le sessioni HDX.
- Per gli avvii delle sessioni da iOS e Android OS, è disponibile solo la durata dell'avvio VDA.
- IFDCD è disponibile solo quando viene rilevata l'app Workspace durante l'avvio da un browser.
- Per gli avvii delle sessioni da macOS, IFDCD è disponibile solo per l'app Workspace 1902 e versioni successive.
- Per gli avvii delle sessioni dal sistema operativo Windows, IFDCD è disponibile per l'app Workspace 1902 e versioni successive. Per le versioni precedenti, IFDCD viene visualizzato solo per gli avvii di app da un browser con l'app Workspace rilevata.

> **Note:**
>
> - Se si riscontrano problemi di visualizzazione della durata di avvio delle sessioni dopo aver soddisfatto i prerequisiti, visualizzare i log del server Monitor e del VDA come descritto in CTX130320.
>
>  Per le sessioni condivise (più applicazioni avviate nella stessa sessione), vengono visualizzate le metriche di avvio dell'app Workspace per la connessione più recente o l'avvio dell'applicazione più recente.
> - Alcune metriche in VDA Session Startup (Avvio della sessione VDA) non sono applicabili alle riconnessioni. In questi casi, viene visualizzato un messaggio.




## Fasi di avvio delle sessioni dell'app Workspace

### Session Startup Client Duration (SSCD) (Durata del client di avvio della sessione [SSCD])

Quando questa metrica è alta, indica un problema lato client che causa lunghi tempi di avvio. Esaminare le metriche successive per determinare la probabile causa principale del problema. SSCD inizia

il più vicino possibile all'ora della richiesta (clic del mouse) e termina quando è stata stabilita la connessione ICA tra il dispositivo client e il VDA. Nel caso di una sessione condivisa, questa durata è molto inferiore, poiché gran parte dei costi di configurazione associati alla creazione di una nuova connessione al server non vengono sostenuti. Al livello immediatamente inferiore, sono disponibili diverse metriche dettagliate.

#### ICA File Download Duration (IFDCD) (Durata del download del file ICA [IFDCD])

IFDCD è il tempo necessario perché il client esegua il download del file ICA dal server. Il processo generale è il seguente:

1. L'utente fa clic su una risorsa (applicazione o desktop) nell'applicazione Workspace.
2. Una richiesta dell'utente viene inviata a StoreFront tramite Citrix Gateway (se configurato), che invia la richiesta al Delivery Controller.
3. Il Delivery Controller trova una macchina disponibile per la richiesta e invia le informazioni sulla macchina e altri dettagli a StoreFront. Inoltre, StoreFront richiede e riceve un ticket una tantum dalla Secure Ticket Authority.
4. StoreFront genera un file ICA e lo invia all'utente tramite Citrix Gateway (se configurato).

IFDCD rappresenta il tempo necessario per il processo completo (passaggi 1-4). La durata IFDCD interrompe il conteggio quando il client riceve il file ICA.

LPWD è il componente StoreFront del processo.

Se il valore IFDCD è alto (ma LPWD è normale), l'elaborazione sul lato server dell'avvio è riuscita, ma si sono verificati dei problemi di comunicazione tra il dispositivo client e StoreFront. Questo deriva da problemi di rete tra le due macchine. In questo modo è possibile risolvere prima i problemi di rete potenziali.

#### Launch Page Web Server Duration (LPWD) (Durata del server Web della pagina di avvio [LPWD])

Questo è il tempo necessario per elaborare la pagina di avvio (launch.aspx) su StoreFront. Se il valore LPWD è alto, potrebbe esserci un collo di bottiglia su StoreFront.

Le possibili cause includono:

- Carico elevato su StoreFront. Cercare di identificare la causa del rallentamento controllando i log di Internet Information Services (IIS) e gli strumenti di monitoraggio, Gestione attività, Monitoraggio prestazioni e così via.
- StoreFront sta riscontrando problemi di comunicazione con altri componenti come Delivery Controller. Controllare se la connessione di rete tra StoreFront e Delivery Controller è lenta o alcuni Delivery Controller sono inattivi o sovraccarichi.

#### Name Resolution Web Server Duration (NRWD) (Durata del server Web con risoluzione dei nomi [NRWD])

Questo è il tempo impiegato dal Delivery Controller per risolvere il nome di un'applicazione pubblicata/desktop in un indirizzo IP della macchina VDA.

Quando questa metrica è alta, indica che il Delivery Controller sta impiegando molto tempo per risolvere il nome di un'applicazione pubblicata in un indirizzo IP. Le possibili cause includono:

- un problema del client
- problemi del Delivery Controller, come il sovraccarico del Delivery Controller, o un problema del collegamento di rete tra i due

#### Ticket Response Web Server Duration (TRWD) (Durata del server Web di risposta del ticket [TRWD])

Questa durata indica il tempo necessario per ottenere un ticket (se necessario) dal server Secure Ticket Authority (STA) o dal Delivery Controller. Quando questa durata è elevata, indica che il server STA o il Delivery Controller sono sovraccarichi.

#### Session Look-up Client Duration (SLCD) (Durata del client di ricerca della sessione [SLCD])

Questa durata rappresenta il tempo necessario per interrogare ogni sessione per ospitare l'applicazione pubblicata richiesta. Il controllo viene eseguito sul client per determinare se una sessione esistente può gestire la richiesta di avvio dell'applicazione. Il metodo utilizzato dipende dal fatto che la sessione sia nuova o condivisa.

#### Session Creation Client Duration (SCCD) (Durata del client di creazione della sessione [SCCD])

Questa durata rappresenta il tempo necessario per creare una sessione, dal momento in cui wfica32.exe (o un file equivalente simile) viene avviato al momento in cui viene stabilita la connessione.

### Fasi di avvio della sessione VDA

#### Session Startup VDA Duration (SSVD) (Durata del VDA di avvio della sessione [SSVD])

Questa durata è la metrica di avvio della connessione lato server di alto livello che indica il tempo impiegato dal VDA per eseguire l'intera operazione di avvio. Quando questa metrica è alta, indica che è presente un problema del VDA che aumenta i tempi di avvio della sessione. Questo include il tempo impiegato sul VDA per eseguire l'intera operazione di avvio.

**Credentials Obtention VDA Duration (COVD) (Durata del VDA per l'ottenimento delle credenziali [COVD])**

Il tempo impiegato dal VDA per ottenere le credenziali utente.

Questa durata può essere gonfiata artificialmente se un utente non riesce a fornire tempestivamente le credenziali e, quindi, non essere inclusa nella durata di avvio del VDA. È probabile che questa durata sia significativa solo se viene utilizzato l'accesso manuale e viene visualizzata la finestra di dialogo delle credenziali lato server (o se viene visualizzata una nota legale prima dell'inizio dell'accesso).

**Credentials Authentication VDA Duration (CAVD) (Durata del VDA per l'autenticazione delle credenziali [CAVD])**

Questo è il tempo impiegato dal VDA per autenticare le credenziali dell'utente con il provider di autenticazione, che può essere Kerberos, Active Directory o una Security Support Provider Interface (SSPI).

**Group Policy VDA Duration (GPVD) (Durata del VDA per i Criteri di gruppo [GPVD])**

Questa durata è il tempo necessario per applicare gli oggetti Criteri di gruppo durante l'accesso.

**Login Script Execution VDA Duration (LSVD) (Durata del VDA di esecuzione dello script di accesso [LSVD])**

Questo è il tempo impiegato dal VDA per eseguire gli script di accesso dell'utente.

È possibile rendere asincroni gli script di accesso dell'utente o del gruppo. Ottimizzare eventuali script di compatibilità delle applicazioni o utilizzare variabili d'ambiente.

**Profile Load VDA Duration (PLVD) (Durata del VDA per il caricamento del profilo [PLVD])**

Questo è il tempo impiegato dal VDA per caricare il profilo dell'utente.

Se questa durata è elevata, esaminare la configurazione User Profile (Profilo utente). Le dimensioni e la posizione del profilo mobile contribuiscono a rallentare gli avvii delle sessioni. Quando un utente accede a una sessione in cui sono abilitati i profili mobili e le Home directory di Servizi terminal, il contenuto e l'accesso del profilo mobile a tale cartella vengono mappati durante l'accesso, processo che utilizza risorse aggiuntive. A volte, questo può consumare una quantità significativa dell'utilizzo della CPU. Utilizzare **Home directory di Servizi terminal** con cartelle personali reindirizzate per mitigare questo problema. In generale, utilizzare Citrix Profile Management per gestire i profili utente

negli ambienti Citrix. Se si utilizza Citrix Profile Management e i tempi di accesso sono lenti, verificare se il software antivirus blocca lo strumento Citrix Profile Management.

**Printer Creation VDA Duration (PCVD) (Durata del VDA per la creazione della stampante [PCVD])**

Questo è il tempo impiegato dal VDA per mappare in modo sincrono le stampanti client dell'utente. Se la configurazione è impostata per eseguire la creazione della stampante in modo asincrono, non viene registrato alcun valore per PCVD in quanto non influisce sul completamento dell'avvio della sessione.

Il tempo eccessivo impiegato per la mappatura delle stampanti è spesso il risultato delle impostazioni dei criteri di creazione automatica delle stampanti. Il numero di stampanti aggiunte localmente sui dispositivi client degli utenti e la configurazione di stampa possono influire direttamente sugli orari di inizio della sessione. All'avvio di una sessione, Citrix Virtual Apps and Desktops deve creare tutte le stampanti mappate localmente sul dispositivo client. Riconfigurare i criteri di stampa per ridurre il numero di stampanti create, in particolare quando gli utenti hanno molte stampanti locali. A tale scopo, modificare il criterio Printer Auto creation (Creazione automatica delle stampanti) nel Delivery Controller e in Citrix Virtual Apps and Desktops.

**Drive Mapping VDA Duration (DMVD) (Durata del VDA per la mappatura unità [DMVD])**

Questo è il tempo impiegato dal VDA per mappare le unità client, i dispositivi e le porte dell'utente.

Assicurarsi che i criteri di base includano impostazioni per disabilitare i canali virtuali inutilizzati, come la mappatura delle porte audio o COM, per ottimizzare il protocollo ICA e migliorare le prestazioni complessive della sessione.

**Application/Desktop Launch VDA Duration (ALVD/DLVD) (Durata del VDA per l'avvio di applicazioni/desktop [ALVD/DLVD])**

Questa fase è una combinazione della durata di userinit e Shell. Quando un utente accede a una macchina Windows, Winlogon esegue userinit.exe. Usernit.exe esegue gli script di accesso, ristabilisce le connessioni di rete e quindi avvia explorer.exe, l'interfaccia utente di Windows; userinit rappresenta la durata tra l'avvio di userinit.exe e l'avvio dell'interfaccia utente per il desktop virtuale o l'applicazione. La durata di Shell è il tempo che intercorre tra l'inizializzazione dell'interfaccia utente e il momento in cui l'utente riceve il controllo della tastiera e del mouse.

**Session Creation VDA Duration (SCVD) (Durata del VDA per la creazione di sessioni [SCVD])**

Questa durata include eventuali ritardi vari nella creazione della sessione sul VDA.

# Diagnosticare i problemi di accesso utente

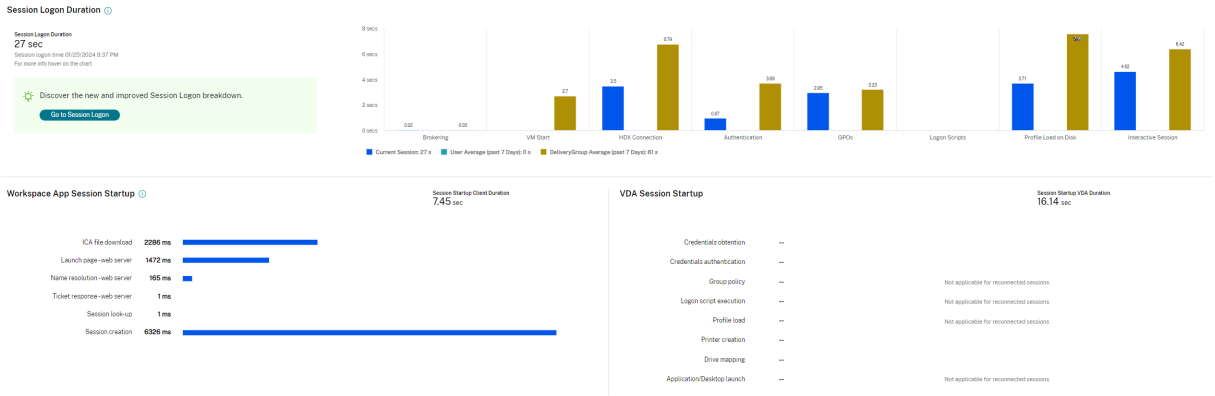
November 21, 2023

Utilizzare i dati Logon Duration (Durata dell'accesso) per risolvere i problemi di accesso degli utenti.

La durata dell'accesso viene misurata solo per le connessioni iniziali a un desktop o un'app che utilizzano HDX. Questi dati non includono utenti che tentano di connettersi con Remote Desktop Protocol o riconnettersi da sessioni disconnesse. In particolare, la durata dell'accesso non viene misurata quando un utente si connette inizialmente utilizzando un protocollo non HDX e si ricollega utilizzando HDX.

Nella visualizzazione Dettagli utente, la durata viene visualizzata sotto forma di valore numerico al di sotto del quale vengono visualizzati l'ora in cui si è verificato l'accesso e un grafico delle fasi del processo di accesso.

Quando gli utenti accedono a Citrix Virtual Apps and Desktops, il servizio di monitoraggio tiene traccia delle fasi del processo di accesso dal momento in cui l'utente si connette dall'app Citrix Workspace al momento in cui il desktop è pronto per l'uso.




Il numero elevato a sinistra è il tempo di accesso totale e viene calcolato combinando il tempo impiegato per stabilire la connessione e ottenere un desktop dal Delivery Controller con il tempo impiegato per l'autenticazione e l'accesso a un desktop virtuale. Le informazioni sulla durata sono presentate in secondi (o frazioni di secondi).

## Prerequisiti

Assicurarsi che siano soddisfatti i seguenti prerequisiti per la visualizzazione dei dati e dei drill-down relativi alla durata degli accessi:

1. Installare **Citrix User Profile Manager** e **Citrix User Profile Manager WMI Plugin** sul VDA.
2. Assicurarsi che il servizio Citrix Profile Management sia in esecuzione.

3. Per i siti XenApp e XenDesktop 7.15 e versioni precedenti, disabilitare l'impostazione dell' oggetto Criteri di gruppo **Non elaborare l'elenco di esecuzione precedente**.
4. L'opzione Controlla traccia processo deve essere abilitata per il drill-down della sessione interattiva.
5. Per il drill-down dell'oggetto Criteri di gruppo, aumentare le dimensioni dei log operativi di Criteri di gruppo.

> **Nota:**
>
> La durata dell'accesso è supportata solo sulla shell predefinita di Windows (explorer.exe) e non su shell personalizzate.

## Procedura per risolvere i problemi di accesso degli utenti

1. Dalla vista **User Details** (Dettagli utente), risolvere il problema dello stato di accesso utilizzando il riquadro Logon Duration (Durata dell'accesso).
    - Se l'utente sta effettuando l'accesso, la vista riflette il processo di accesso.
    - Se l'utente ha effettuato l'accesso, il riquadro Logon Duration (Durata dell'accesso) visualizza il tempo necessario per l'accesso alla sessione corrente.
2. Esaminare le fasi del processo di accesso.

## Fasi del processo di accesso

### Brokering

Tempo necessario per decidere quale desktop assegnare all'utente.

### VM start (Avvio VM)

Se la sessione ha richiesto l'avvio di una macchina, questo è il tempo impiegato per avviare la macchina virtuale.

### HDX connection (Connessione HDX)

Tempo necessario per completare i passaggi necessari per configurare la connessione HDX dal client alla macchina virtuale.

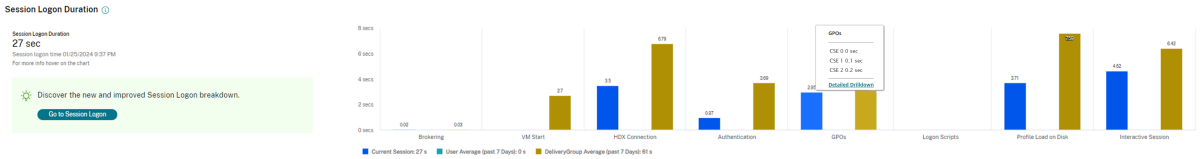
 

### Autenticazione

Tempo necessario per completare l'autenticazione alla sessione remota.

### GPOs (Oggetti Criteri di gruppo)

Se le impostazioni di Criteri di gruppo sono abilitate sulle macchine virtuali, questo è il tempo necessario per applicare gli oggetti Criteri di gruppo durante l'accesso. Il drill-down del tempo impiegato per applicare ogni criterio in base alle CSE (estensioni lato client) è disponibile come descrizione comando quando si passa il mouse sulla barra degli oggetti Criteri di gruppo.




Fare clic su **Espansione dettagliata** per visualizzare una tabella con lo stato dei criteri e il nome dell'oggetto Criteri di gruppo corrispondente. Le durate temporali nel drill-down rappresentano solo il tempo di elaborazione delle CSE e non si sommano al tempo totale dell'oggetto Criteri di gruppo. È possibile copiare la tabella del drill-down per ulteriori risoluzioni dei problemi o per utilizzarla nei report. Il tempo degli oggetti Criteri di gruppo per i criteri viene recuperato dai log del Visualizzatore eventi. I log possono essere sovrascritti a seconda della memoria allocata per i log operativi (la dimensione predefinita è 4 MB). Per ulteriori informazioni sull'aumento delle dimensioni del registro per i registri operativi, vedere l'articolo di Microsoft TechNet https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10).

### Logon scripts (Script di accesso)

Se gli script di accesso sono configurati per la sessione, questo è il tempo necessario per la loro esecuzione.

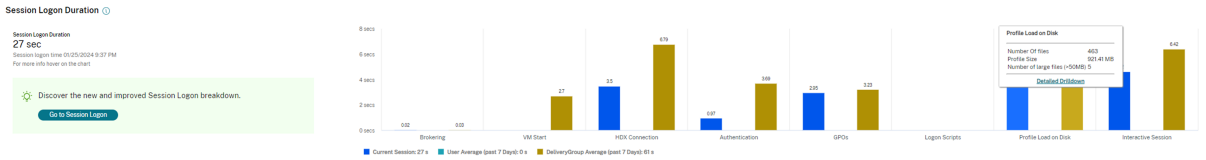
### Profile load (Caricamento del profilo)

Se le impostazioni del profilo sono configurate per l'utente o la macchina virtuale, questo è il tempo necessario per il caricamento del profilo.

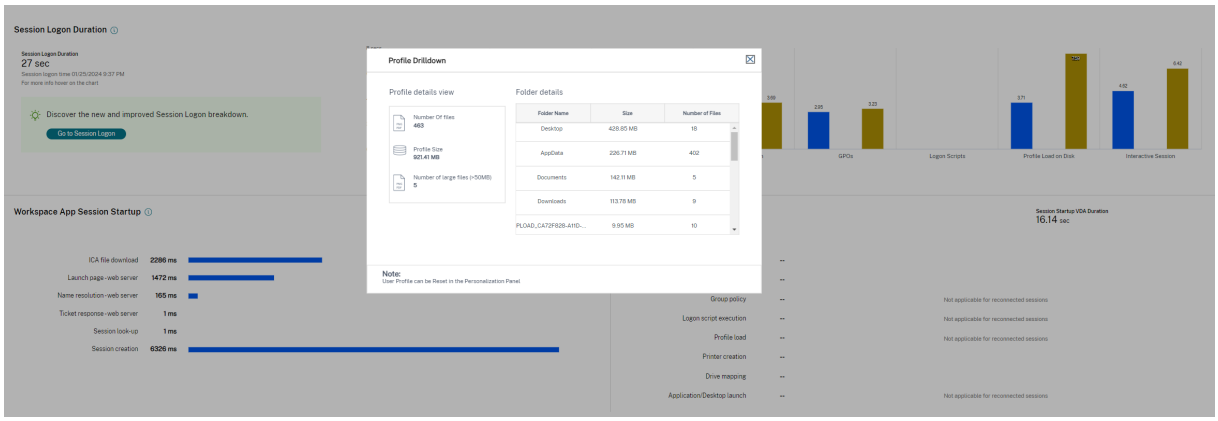
Se Citrix Profile Management è configurato, la barra Profile Load (Caricamento profilo) include il tempo impiegato da Citrix Profile Management per elaborare i profili utente. Queste informazioni aiutano gli amministratori a risolvere i problemi relativi alla durata elevata dell'elaborazione dei profili. Quando Profile Management è configurato, la barra Profile Load (Caricamento profilo) visualizza una durata maggiore. L'aumento è causato da questo miglioramento e non causa un degrado delle prestazioni. Questo miglioramento è disponibile sui VDA 1903 e versioni successive.

Se si passa il mouse sulla barra Profile Load (Caricamento profilo), viene visualizzata una descrizione comando che mostra i dettagli del profilo utente per la sessione corrente. Queste informazioni aggiuntive possono aiutare a risolvere i problemi di carico elevato del profilo.




Fare clic su **Detailed Drilldown** (Drill-down dettagliato) per eseguire il drill-down di ogni singola cartella nella cartella principale del profilo (ad esempio, C:/Users/username), le relative dimensioni e il numero di file (inclusi i file all'interno delle cartelle nidificate).




Il drilldown del profilo è disponibile sui VDA 1811 e versioni successive. Utilizzando le informazioni di drill-down del profilo, è possibile risolvere i problemi relativi a un tempo di caricamento del profilo elevato. È possibile effettuare le seguenti operazioni:

- Reimpostare il profilo utente
- Ottimizzare il profilo rimuovendo file di grandi dimensioni indesiderati
- Ridurre il numero di file per ridurre il carico di rete
- Usare lo streaming dei profili

Per impostazione predefinita, tutti i nomi delle cartelle sono visibili. Per nascondere i nomi delle cartelle, modificare i valori del Registro di sistema sul computer VDA utilizzando i seguenti passaggi:

> **Avviso:**
>
> L'aggiunta e la modifica non corrette del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non garantisce che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

1. Sul VDA, aggiungere un nuovo valore del Registro di sistema **ProfileFoldersNameHidden** in HKEY_LOCAL_MACHINE\Software\Citrix\Director\
2. Impostare il valore su 1. Questo valore deve essere un valore DWORD (32 bit). La visibilità dei nomi delle cartelle ora è disabilitata.
3. Per rendere nuovamente visibili i nomi delle cartelle, impostare il valore su 0.

> **Nota:**
>
> È possibile utilizzare l'oggetto Criteri di gruppo o PowerShell per applicare la modifica del valore del Registro di sistema su più macchine. Per ulteriori informazioni sull'utilizzo di un oggetto Criteri di gruppo per distribuire le modifiche del Registro di sistema, vedere il blog.

#### Informazioni aggiuntive

- Il drill-down del profilo non considera le cartelle reindirizzate.
- I file NTUser.dat nella cartella principale potrebbero non essere visibili agli utenti finali. Tuttavia, sono inclusi nel drill-down del profilo e visualizzati nell'elenco dei file nella **cartella principale**.
- Ci sono alcuni file nascosti nella cartella AppData che non sono inclusi nel drilldown del profilo.
- Il numero di file e i dati relativi alle dimensioni del profilo potrebbero non corrispondere ai dati nel riquadro Personalization (Personalizzazione) a causa di alcune limitazioni di Windows.

#### Interactive Session (Sessione interattiva)

Questo è il tempo necessario per "trasferire"il controllo della tastiera e del mouse all'utente dopo il caricamento del profilo utente. Normalmente è la durata più lunga di tutte le fasi del processo di accesso e viene calcolata come **Interactive Session duration (Durata della sessione interattiva) = Desktop Ready Event Timestamp (Data e ora evento Desktop pronto) (EventId 1000 su VDA) - User Profile Loaded Event Timestamp (Data e ora evento Profilo utente caricato) (EventId 2 su VDA)**. La sessione interattiva è composta da tre sottofasi: Pre-userinit, Userinit e Shell. Passare il mouse su Interactive Session (Sessione interattiva) per visualizzare una descrizione comando che mostra quanto segue:

- sottofasi
- il tempo impiegato per ogni sottofase
- il ritardo totale cumulativo tra queste sottofasi

> **Nota:**
>
> Questa funzionalità è disponibile sui VDA 1811 e versioni successive. Se sono state avviate sessioni su siti precedenti a 7.18 e successivamente è stato eseguito l'aggiornamento a 7.18, viene visualizzato un messaggio "Drilldown unavailable due to server error"(Drill-down non disponibile a causa di un errore del server). Tuttavia, se sono state avviate le sessioni dopo l'aggiornamento,

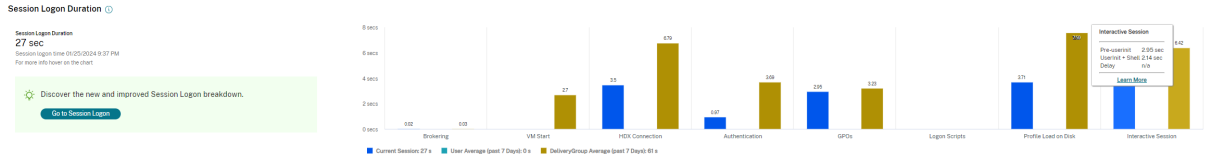
 

> non viene visualizzato alcun messaggio di errore.

Per visualizzare la durata di ogni sottofase, abilitare Controlla traccia processo sulla VM (VDA). Quando l'opzione Controlla traccia processo è disabilitata (impostazione predefinita), vengono visualizzate la durata di Pre-userinit e la durata combinata di Userinit e Shell. È possibile abilitare Controlla traccia processo tramite un oggetto Criteri di gruppo (GPO) come segue:

1. Creare un oggetto Criteri di gruppo e modificarlo utilizzando l'Editor oggetti Criteri di gruppo.
2. Andare a **Configurazione computer > Impostazioni di Windows > Impostazioni di sicurezza > Criteri locali > Criteri di controllo**.
3. Nel riquadro di destra, fare doppio clic su **Controlla traccia processo**.
4. Selezionare **Operazione riuscita** e fare clic su OK.
5. Applicare questo oggetto Criteri di gruppo ai VDA o al gruppo richiesti.

Per ulteriori informazioni sul tracciamento del processo di verifica e sull'abilitazione o disabilitazione del processo, vedere https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10) nella documentazione Microsoft.




Riquadro Logon Duration (Durata dell'accesso) nella vista User Details (Dettagli utente).

- **Interactive Session** —**Pre-userinit** (Sessione interattiva - Pre-userinit): si tratta del segmento di Interactive Session (Sessione interattiva) che si sovrappone a oggetti Criteri di gruppo e script. Questa sottofase può essere ridotta ottimizzando gli oggetti Criteri di gruppo e gli script.
- **Interactive Session** —**Userinit** (Sessione interattiva - Userinit): quando un utente accede a una macchina Windows, Winlogon esegue userinit.exe. Userinit.exe esegue gli script di accesso, ristabilisce le connessioni di rete e quindi avvia Explorer.exe, l'interfaccia utente di Windows. Questa sottofase di Interactive Session (Sessione interattiva) rappresenta la durata tra l'avvio di Userinit.exe e l'avvio dell'interfaccia utente per il desktop virtuale o l'applicazione.
- **Interactive Session** —**Shell** (Sessione interattiva - Shell): nella fase precedente, Userinit avvia l'inizializzazione dell'interfaccia utente di Windows. La sottofase Shell acquisisce la durata tra l'inizializzazione dell'interfaccia utente e il momento in cui l'utente riceve il controllo della tastiera e del mouse.
- **Delay** (Ritardo): si tratta del ritardo temporale cumulativo tra le sottofasi **Pre-userinit e Userinit** e le sottofasi **Userinit e Shell**.

Il tempo di accesso totale non è una somma esatta di queste fasi. Ad esempio, alcune fasi si verificano in parallelo e, in alcune fasi, ha luogo elaborazione aggiuntiva che può comportare una durata dell'accesso più lunga della somma.
Il tempo di accesso totale non include il tempo di inattività ICA, ovvero il tempo tra il download del

file ICA e l'avvio del file ICA per un'applicazione.
Per abilitare l'apertura automatica del file ICA all'avvio dell'applicazione, configurare il browser per l'avvio automatico del file ICA al momento del download di un file ICA. Per ulteriori informazioni, vedere CTX804493.

> **Nota:**
>
> Il grafico Logon Duration (Durata dell'accesso) mostra le fasi di accesso in secondi. Tutti i valori di durata inferiore a un secondo vengono visualizzati come valori secondari. I valori superiori a un secondo sono arrotondati al mezzo secondo più vicino (0,5 s). Il grafico è stato progettato per mostrare il valore dell'asse y più alto come 200 secondi. Qualsiasi valore superiore a 200 secondi viene mostrato con il valore effettivo visualizzato sopra la barra.

### Suggerimenti per la risoluzione dei problemi

Per identificare valori insoliti o imprevisti nel grafico, confrontare il tempo impiegato in ogni fase della sessione corrente con la durata media per questo utente negli ultimi sette giorni e la durata media per tutti gli utenti di questo gruppo di consegna per gli ultimi sette giorni.

Segnalare i problemi secondo necessità. Ad esempio, se l'avvio della VM è lento, potrebbe trattarsi di un problema dell'hypervisor, quindi occorre segnalarlo all'amministratore dell'hypervisor. Oppure, se il tempo di brokering è lento, è possibile segnalare il problema all'amministratore del sito per verificare il bilanciamento del carico sul Delivery Controller.

Esaminare le differenze insolite, tra cui:

- Barre di accesso mancanti (correnti)
- Notevoli discrepanze tra la durata corrente e la durata media di questo utente. Le cause includono:
  - È stata installata una nuova applicazione.
  - Si è verificato un aggiornamento del sistema operativo.
  - Sono state apportate modifiche alla configurazione.
  - Le dimensioni del profilo dell'utente sono elevate. In questo caso, il caricamento del profilo è elevato.
- Notevoli discrepanze tra il log dell'utente per quanto riguarda i numeri (durata corrente e media) e la durata media del gruppo di consegna.

Se necessario, fare clic su **Restart** (Riavvia) per osservare il processo di accesso dell'utente al fine di risolvere i problemi, ad esempio VM Start (Avvio VM) o Brokering.

# Shadowing degli utenti

November 16, 2022

Utilizzare la funzionalità di shadowing degli utenti per visualizzare la macchina virtuale o la sessione di un utente o lavorarci direttamente. È possibile utilizzare la funzionalità di shadowing sia sui VDA Windows che Linux. L'utente deve essere connesso alla macchina di cui si desidera fare lo shadowing. Verificarlo controllando il nome della macchina elencato nella barra del titolo dell'utente.

Shadowing viene avviato in una nuova scheda; aggiornare le impostazioni del browser per consentire i popup dall'URL di Citrix Cloud.

Accedere alla funzionalità di shadowing dalla vista **User Details** (Dettagli utente). Selezionare la sessione utente e fare clic su **Shadow** (Avvia shadowing) nella vista Activity Manager (Gestione attività) o nel riquadro Session Details (Dettagli sessione).

## Shadowing di VDA Linux

Lo shadowing è disponibile per i VDA Linux versione 7.16 o successive con le distribuzioni Linux RHEL7.3 o Ubuntu versione 16.04.

> **Nota:**
>
> - Monitor utilizza il nome di dominio completo per connettersi al VDA Linux di destinazione. Assicurarsi che il client di Monitor (Monitoraggio) sia in grado di risolvere il nome di dominio completo del VDA Linux.
> - Sul VDA devono essere installati i pacchetti python-websockify e x11vnc.
> - La connessione noVNC al VDA utilizza il protocollo WebSocket. Per impostazione predefinita, viene utilizzato il protocollo WebSocket **ws://**. Per motivi di sicurezza, Citrix consiglia di utilizzare il protocollo **wss://** sicuro. Installare i certificati SSL su ciascun client Monitor (Monitoraggio) e VDA Linux.

Seguire le istruzioni riportate in Shadowing delle sessioni per configurare il VDA per lo shadowing.

1. Dopo aver fatto clic su **Shadow** (Avvia shadowing), la connessione di shadowing viene inizializzata e sul dispositivo utente viene visualizzato un prompt di conferma.
2. Chiedere all'utente di fare clic su **Yes** (Sì) per avviare la condivisione della macchina o della sessione.
3. L'amministratore può solo visualizzare la sessione di cui viene eseguito lo shadowing.

### Shadowing dei VDA Windows

Lo shadowing delle sessioni di VDA Windows viene eseguito utilizzando l'Assistenza remota di Windows. Abilitare la funzionalità User Windows Remote Assistance (Assistenza remota di Windows per l'utente) durante l'installazione del VDA. Per ulteriori informazioni, vedere Abilitare o disabilitare funzionalità.

1. Dopo aver fatto clic su **Shadow** (Avvia shadowing), la connessione di shadowing viene inizializzata e una finestra di dialogo richiede di aprire o salvare il file richiesta di supporto .msrc.
2. Aprire il file richiesta di supporto con Remote Assistance Viewer, se non è già selezionato per impostazione predefinita. Sul dispositivo dell'utente viene visualizzato un messaggio di conferma.
3. Chiedere all'utente di fare clic su **Yes** (Sì) per avviare la condivisione della macchina o della sessione.
4. Per un maggiore controllo, chiedere all'utente di condividere il controllo della tastiera e del mouse.

#### Ottimizzare i browser Microsoft Internet Explorer per lo shadowing

Configurare il browser Microsoft Internet Explorer in modo che apra automaticamente il file Microsoft Remote Assistance (.msra) scaricato con il client di Assistenza remota.

A tale scopo, è necessario abilitare l'impostazione Richiesta di conferma automatica per download di file nell'editor Criteri di gruppo:

Configurazione computer > Modelli amministrativi > Componenti di Windows > Internet Explorer > Pannello di controllo Internet > Scheda Sicurezza > Area Internet > Richiesta di conferma automatica per download di file.

## Inviare messaggi agli utenti

October 5, 2022

Da Monitor, inviare un messaggio a un utente connesso a una o più macchine. Ad esempio, utilizzare questa funzionalità per inviare avvisi immediati sulle azioni amministrative, come la manutenzione imminente del desktop, le disconnessioni e i riavvii delle macchine e il ripristino dei profili.

Per inviare un messaggio a un utente, effettuare le seguenti operazioni:

1. Passare a **Monitor** > **Filters** > **Machines** > **All Machines**.

2. Selezionare una macchina a cui si desidera inviare un messaggio e fare clic su **Send Message**(Invia messaggio).
3. Digitare il messaggio e fare clic su **Send** (Invia).

Se il messaggio viene inviato correttamente, viene visualizzato un messaggio di conferma. Se la macchina dell'utente è connessa, il messaggio viene visualizzato su quella macchina.

Se il messaggio non viene inviato correttamente, viene visualizzato un messaggio di errore. Risolvere il problema in base al messaggio di errore. Al termine, digitare di nuovo il testo dell'oggetto e del messaggio e fare clic nuovamente clic su Try (Prova).

## Risolvere gli errori delle applicazioni

February 13, 2023

Nella vista **Activity Manager** (Gestione attività), fare clic sulla scheda **Applications** (Applicazioni). È possibile visualizzare tutte le applicazioni su tutte le macchine a cui l'utente ha accesso, incluse le applicazioni locali e ospitate per la macchina attualmente connessa, e lo stato di ciascuna.

L'elenco include solo le applicazioni avviate all'interno della sessione.

Per le macchine con sistema operativo multisessione e quelle con sistema operativo a sessione singola, le applicazioni sono elencate per ogni sessione disconnessa. Se l'utente non è connesso, non viene visualizzata alcuna applicazione.

| Azione | Descrizione |
| --- | --- |
| Terminare l'applicazione che non risponde | Scegliere l'applicazione che non risponde e fare clic su **End Application** (Termina applicazione). Una volta terminata l'applicazione, chiedere all'utente di avviarla di nuovo. |
| Terminare i processi che non rispondono | Se si dispone dell'autorizzazione richiesta, fare clic sulla scheda **Processes** (Processi). Selezionare un processo correlato all'applicazione o che utilizza una quantità elevata di risorse della CPU o memoria e fare clic su **End Process** (Termina processo). Tuttavia, se non si dispone dell'autorizzazione necessaria per terminare il processo, il tentativo di terminare un processo non riesce. |

| Azione | Descrizione |
| --- | --- |
| Riavviare la macchina dell'utente | Solo per le macchine con sistema operativo a sessione singola, per la sessione selezionata fare clic su **Restart** (Riavvia). In alternativa, dalla vista Machine Details (Dettagli macchina), utilizzare i controlli di alimentazione per riavviare o spegnere la macchina. Chiedere all'utente di effettuare nuovamente l'accesso in modo da poter ricontrollare l'applicazione. Per le macchine con sistema operativo multisessione, l'opzione di riavvio non è disponibile. In questo caso, disconnettersi dall'utente e lasciare che l'utente acceda di nuovo. |
| Mettere la macchina in modalità di manutenzione | Se l'immagine della macchina necessita di manutenzione, ad esempio una patch o altri aggiornamenti, mettere la macchina in modalità di manutenzione. Dalla vista Machine Details (Dettagli macchina), fare clic su **Details** (Dettagli) e attivare l'opzione Maintenance Mode (Modalità di manutenzione). Fare una segnalazione all'amministratore appropriato. |

### Disabilitare la visibilità delle applicazioni in esecuzione

Per impostazione predefinita, Activity Manager visualizza un elenco di tutte le applicazioni in esecuzione per la sessione di un utente. Queste informazioni possono essere visualizzate da tutti gli amministratori che hanno accesso alla funzionalità Activity Manager. Per i ruoli Delegated Administrator (Amministratore delegato) sono compresi i ruoli Full Administrator (Amministratore completo), Delivery Group Administrator (Amministratore del gruppo di consegna) e Help Desk Administrator (Amministratore dell'helpdesk).

Per proteggere la privacy degli utenti e delle applicazioni che eseguono, è possibile disattivare l'elenco delle applicazioni in esecuzione nella scheda Applications. A questo scopo, sul VDA, modificare la chiave del Registro di sistema in HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. Per impostazione predefinita, la chiave è impostata su 1. Modificare il valore su 0, il che significa che le informazioni non vengono raccolte dal VDA e quindi non vengono visualizzate in Activity Manager (Gestione attività).

> **Avviso:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

## Ripristinare le connessioni desktop

October 5, 2022

Da Monitor controllare lo stato della connessione dell'utente per la macchina corrente nella barra del titolo dell'utente.

Utilizzare questa funzionalità per inviare avvisi immediati sulle azioni amministrative, come la manutenzione imminente del desktop, le disconnessioni e i riavvii delle macchine e i ripristini dei profili.

| Azione | Descrizione |
| --- | --- |
| Assicurarsi che la macchina non sia in modalità di manutenzione | Nella pagina User Details (Dettagli utente), assicurarsi che la modalità di manutenzione sia disattivata. |
| Riavviare la macchina dell'utente | Selezionare la macchina e fare clic su **Restart** (Riavvia). Utilizzare questa opzione se la macchina dell'utente non risponde o non è in grado di connettersi, ad esempio quando la macchina utilizza una quantità insolitamente elevata di risorse della CPU, con la possibilità di rendere la CPU inutilizzabile. |

## Ripristinare le sessioni

October 5, 2022

Se una sessione viene disconnessa, è ancora attiva e le relative applicazioni continuano a essere eseguite, ma il dispositivo utente non comunica più con il server.

Nella vista User Details (Dettagli utente), risolvere i problemi relativi alla sessione nel riquadro **Session Details** (Dettagli sessione). È possibile visualizzare i dettagli della sessione corrente, indicati dall'ID della sessione.

| Azione | Descrizione |
| --- | --- |
| Terminare le applicazioni o i processi che non rispondono | Fare clic sulla scheda **Applications** (Applicazioni). Selezionare le applicazioni che non rispondono e fare clic su **End Application** (Termina applicazione). Analogamente, selezionare gli eventuali processi corrispondente che non rispondono e fare clic su **End Process** (Termina processo). Inoltre, terminare i processi che consumano una quantità insolitamente elevata di memoria o risorse della CPU, il che può rendere inutilizzabile la CPU. |
| Disconnettere la sessione di Windows | Fare clic su **Session Control** (Controllo sessione) e quindi selezionare **Disconnect** (Disconnetti). Questa opzione è disponibile solo per macchine con sistema operativo multisessione con broker. Per le sessioni senza broker, l'opzione è disabilitata. |
| Disconnettere l'utente dalla sessione | Fare clic su **Session Control** (Controllo sessione), quindi selezionare **Log Off** (Esci). |

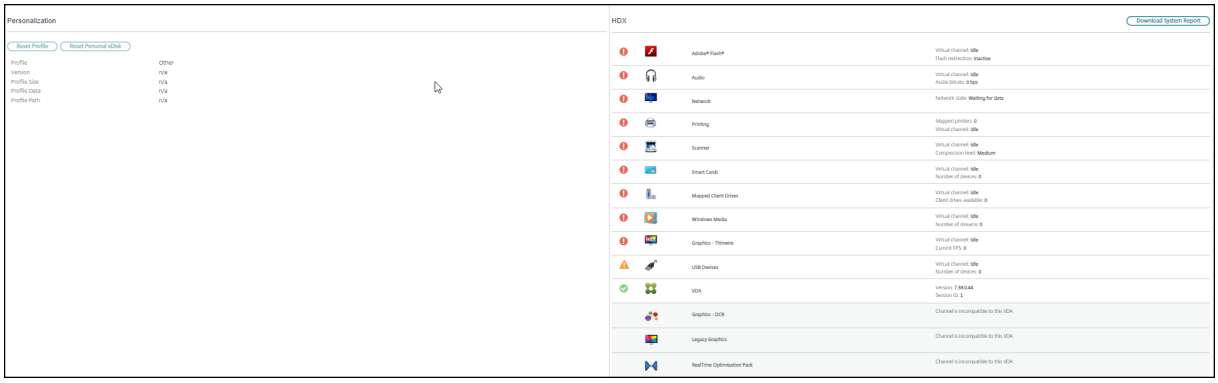
Per testare la sessione, l'utente può tentare di riaccedervi. È inoltre possibile ricorrere allo shadowing dell'utente per monitorare più da vicino questa sessione.

## Eseguire report sui sistemi di canale HDX

November 21, 2023

Nella vista **User Details** (Dettagli utente), controllare lo stato dei canali HDX sulla macchina dell'utente nel riquadro HDX. Questo riquadro è disponibile solo se la macchina dell'utente è collegata utilizzando HDX.




Se viene visualizzato un messaggio che indica che le informazioni non sono attualmente disponibili, attendere un minuto per l'aggiornamento della pagina oppure selezionare il pulsante **Refresh** (Aggiorna). L'aggiornamento dei dati HDX richiede un po'più tempo rispetto ad altri dati.

Fare clic su un'icona di errore o di avviso per ulteriori informazioni.

> Suggerimento:
>
> È possibile visualizzare informazioni sugli altri canali nella stessa finestra di dialogo facendo clic sulle frecce sinistra e destra nell'angolo sinistro della barra del titolo.

I report di sistema del canale HDX vengono utilizzati principalmente dal supporto Citrix per ulteriori risoluzioni dei problemi. Nel riquadro HDX, fare clic su **Download System Report** (Scarica report di sistema).

## Reimpostare un profilo utente

October 5, 2022

> **Attenzione:**
>
> Quando un profilo viene ripristinato, anche se le cartelle e i file dell'utente vengono salvati e copiati nel nuovo profilo, la maggior parte dei dati del profilo utente viene eliminata (ad esempio, il registro viene ripristinato e le impostazioni dell'applicazione potrebbero essere eliminate).

1. Da Monitor, cercare l'utente di cui si desidera reimpostare il profilo e selezionare la sessione di questo utente.
2. Fare clic su **Reset Profile** (Reimposta profilo).
3. Chiedere all'utente di disconnettersi da tutte le sessioni.
4. Chiedere all'utente di accedere di nuovo. Le cartelle e i file salvati dal profilo dell'utente vengono copiati nel nuovo profilo.

> **Importante:**
>
> Se l'utente dispone di profili su più piattaforme (ad esempio Windows 8 e Windows 7), chiedere all'utente di accedere prima allo stesso desktop o alla stessa app segnalati dall'utente come problema. In questo modo viene ripristinato il profilo corretto. Un profilo utente Citrix è già reimpostato quando viene visualizzato il desktop dell'utente. Nel caso di un profilo mobile Microsoft, il ripristino della cartella potrebbe essere ancora in corso per un breve periodo. L'utente deve rimanere connesso fino al completamento del ripristino.

I passaggi precedenti presuppongono l'utilizzo di Citrix Virtual Desktops (Desktop VDA). Se si utilizza Citrix Virtual Desktops (Server VDA), è necessario effettuare l'accesso per eseguire il ripristino del profilo. L'utente deve quindi disconnettersi e accedere nuovamente per completare il ripristino del profilo.

Se il profilo non viene ripristinato correttamente (ad esempio, l'utente non è in grado di accedere nuovamente alla macchina o mancano alcuni file), è necessario ripristinare manualmente il profilo originale.

Le cartelle (e i relativi file) del profilo dell'utente vengono salvate e copiate nel nuovo profilo. Vengono copiate nell'ordine elencato:

- Desktop
- Cookie
- Preferiti
- Documenti
- Immagini
- Musica
- Video

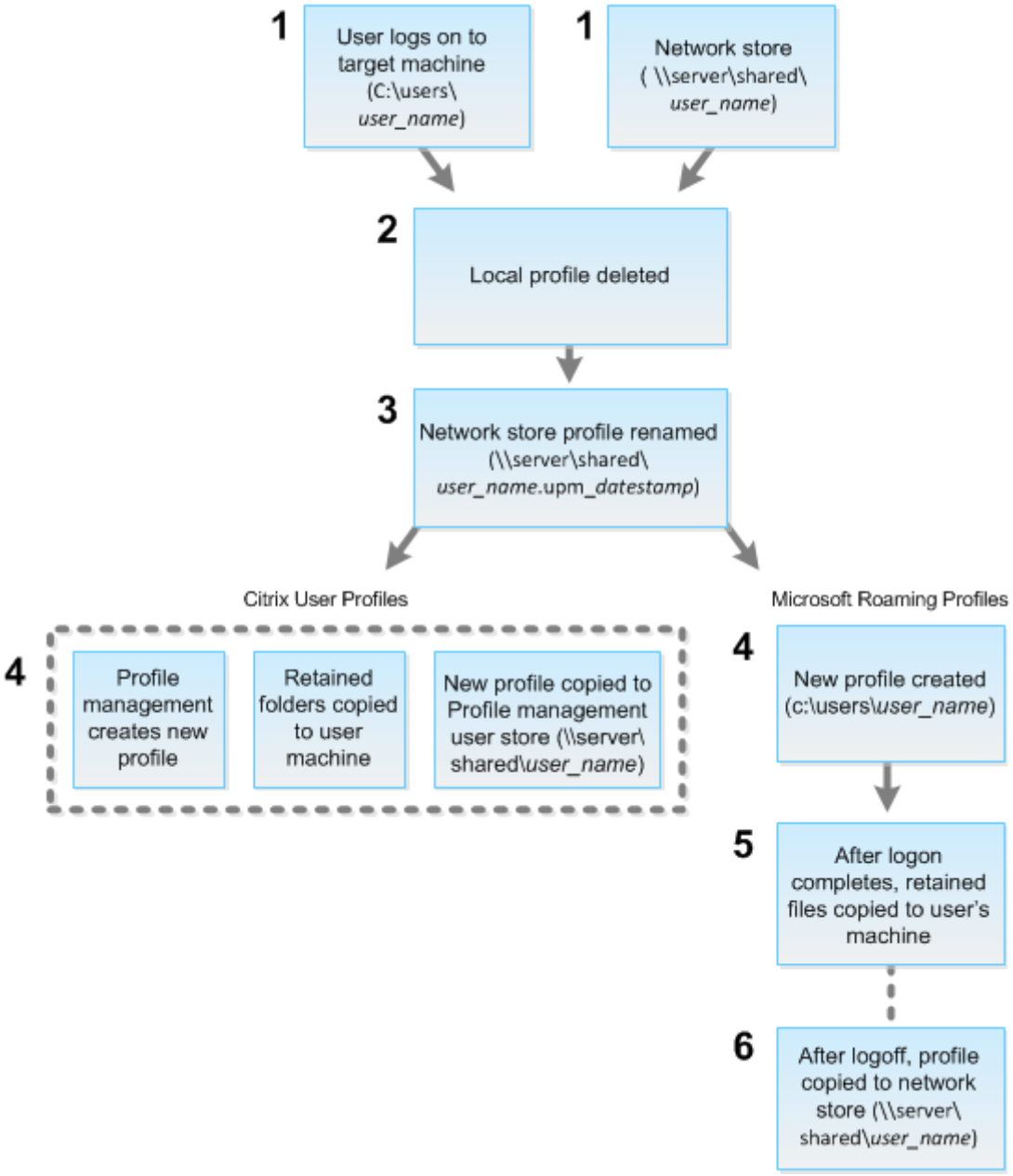
> **Nota:**
>
> In Windows 8 e versioni successive, i cookie non vengono copiati quando i profili vengono reimpostati.

### Come vengono elaborati i profili ripristinati

È possibile reimpostare qualsiasi profilo utente Citrix o profilo mobile Microsoft. Dopo che l'utente si disconnette e si seleziona il comando reset (in Monitor o utilizzando l'SDK di PowerShell), Monitor identifica innanzitutto il profilo utente in uso ed emette un comando di ripristino appropriato. Monitor riceve le informazioni tramite Profile Management, incluse informazioni sulle dimensioni, sul tipo e sui tempi di accesso del profilo.

Questo diagramma illustra il processo successivo all'accesso dell'utente, quando viene reimpostato un profilo utente.




Il comando reset emesso da Monitor specifica il tipo di profilo. Il servizio Profile Management tenta quindi di reimpostare un profilo di quel tipo e cerca la condivisione di rete appropriata (archivio utente). Se l'utente viene elaborato da Profile Management, ma quest'ultimo riceve un comando di profilo mobile, il comando viene rifiutato (o viceversa).

1. Se è presente un profilo locale, viene eliminato.
2. Il profilo di rete viene rinominato.
3. L'azione successiva dipende dal tipo di profilo in fase di reimpostazione: un profilo utente Citrix o un profilo mobile Microsoft.

Nel caso dei profili utente Citrix, il nuovo profilo viene creato utilizzando le regole di importazione di Profile Management, le cartelle vengono copiate nuovamente nel profilo di rete e l'utente può effettuare l'accesso normalmente. Se per il ripristino viene utilizzato un profilo mobile, le eventuali impostazioni del Registro di sistema nel profilo mobile vengono mantenute nel profilo di ripristino. È possibile configurare Profile Management in modo che un profilo del modello sostituisca il profilo mobile, se necessario.

Per i profili mobili Microsoft, Windows crea un nuovo profilo e, quando l'utente effettua l'accesso, le cartelle vengono copiate nuovamente nel dispositivo dell'utente. Quando l'utente si disconnette di nuovo, il nuovo profilo viene copiato nell'archivio di rete.

### Per ripristinare manualmente un profilo dopo un ripristino non riuscito

1. Chiedere all'utente di disconnettersi da tutte le sessioni.
2. Eliminare il profilo locale, se ne esiste uno.
3. Individuare la cartella archiviata nella condivisione di rete contenente la data e l'ora aggiunte al nome della cartella, la cartella con estensione .upm_datestamp.
4. Eliminare il nome del profilo corrente, ossia quello senza l'estensione upm_datestamp.
5. Rinominare la cartella archiviata utilizzando il nome del profilo originale, ossia rimuovere l'estensione di data e ora. Il profilo è stato restituito allo stato originale di pre-ripristino.

## Matrice di compatibilità delle funzionalità

September 12, 2023

Citrix Monitor supporta tre edizioni di Citrix DaaS (in precedenza servizi Citrix Virtual Apps and Desktops). Sono **Premium**, **Citrix DaaS Advanced**e **Citrix DaaS Advanced Plus**. Le funzionalità specifiche di Citrix Monitor, le versioni VDA, i componenti dipendenti e le rispettive edizioni di licenza sono elencati nella tabella seguente.

| Funzionalità | Dipendenze - versione minima richiesta | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Utilizzo della GPU in tempo reale disponibile per le GPU AMD | VDA 7 2212 con Windows a 64 bit | Sì | Sì | Sì |

| Funzionalità | Dipendenze - versione minima richiesta | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Accedere a Citrix Analytics for Performance - Session Details (Dettagli della sessione) | Diritto d'uso di Citrix Analytics for Performance | Sì | Sì | Sì |
| Riconnessione automatica della sessione | VDA 1906 | Sì | Sì | Sì |
| Durata dell'avvio della sessione | VDA 1903 | Sì | Sì | Sì |
| Probe dei desktop | Citrix Probe Agent 1903 | Sì | No | No |
| Durata di Profile Management Citrix nel caricamento del profilo | VDA 1903 | Sì | Sì | Sì |
| Drill-down del profilo | VDA 1811 | Sì | Sì | Sì |
| Monitoraggio degli avvisi di Hypervisor | Nessuna | Sì | No | No |
| Probe delle applicazioni | Citrix Application Probe Agent 1811 | Sì | No | No |
| Stato della licenza Servizi Desktop remoto Microsoft | VDA 7.16 | Sì | Sì | Sì |
| Accedere alla console della macchina da Monitor | XenServer Hypervisor 7.3 | Sì | Sì | Sì |

| Funzionalità | Dipendenze - versione minima richiesta | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Esportazione dei dati dei filtri | Nessuna | Sì | Sì | Sì |
| Drill-down interattivo della sessione | VDA 1808 | Sì | Sì | Sì |
| Drill-down dell'oggetto Criteri di gruppo | VDA 1808 | Sì | Sì | Sì |
| Dati cronologici della macchina disponibili utilizzando l'API OData | Nessuna | Sì | Sì | Sì |
| Criteri intelligenti per gli avvisi | Nessuna | Sì | No | No |
| Collegamento Health Assistant | Nessuna | Sì | Sì | Sì |
| Drill-down interattivo della sessione | Nessuna | Sì | Sì | Sì |
| Analisi delle applicazioni | VDA 7.15 | Sì | Sì | Sì |
| API OData V.4 | Nessuna | Sì | Sì | Sì |
| Shadowing degli utenti di VDA Linux | VDA 7.16 | Sì | Sì | Sì |
| Accesso alla console della macchina | Nessuna | Sì | Sì | Sì |
| Monitoraggio degli errori delle applicazioni | VDA 7.15 | Sì | Sì | Sì |

| Funzionalità | Dipendenze - versione minima richiesta | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Risoluzione dei problemi incentrata sulle applicazioni | VDA 7.13 | Sì | Sì | Sì |
| Monitoraggio disco | VDA 7.14 | Sì | Sì | Sì |
| Monitoraggio GPU | VDA 7.14 | Sì | Sì | Sì |
| Protocollo di trasporto nel riquadro Session Details (Dettagli sessione) | VDA 7.13 | Sì | Sì | Sì |
| Descrizioni in linguaggio accessibile degli errori di connessione e delle macchine | VDA 7.x | Sì | Sì | Sì |
| Conservazione dei dati storici | VDA 7.x | Sì | No | No |
| Reporting personalizzato | VDA 7.x | Sì | No | No |
| Reporting sull' utilizzo delle risorse | VDA 7.11 | Sì | Sì | Sì |
| Avvisi estesi per condizioni legate a CPU, memoria e tempo di round trip ICA | VDA 7.11 | Sì | No | No |

| Funzionalità | Dipendenze - versione minima richiesta | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Miglioramenti dell'esportazione di report | VDA 7.x | Sì | Sì | Sì |
| Suddivisione della durata dell'accesso | VDA 7.x | Sì | Sì | Sì |
| Monitoraggio e avvisi proattivi | VDA 7.x | Sì | No | No |
| Utilizzo delle applicazioni ospitate | VDA 7.x | Sì | No | No |
| Utilizzo del sistema operativo a sessione singola e multisessione | VDA 7.x | Sì | No | No |
| Supporto per il canale virtuale Framehawk | VDA 7.6 | Sì | Sì | Sì |

## Amministrazione e monitoraggio delegati

October 6, 2022

L'amministrazione delegata utilizza tre concetti: amministratori, ruoli e ambiti. Le autorizzazioni si basano sul ruolo di amministratore e sull'ambito di questo ruolo. Ad esempio, a un amministratore potrebbe essere assegnato un ruolo di amministratore dell'helpdesk in cui l'ambito riguarda la responsabilità per gli utenti finali in un solo sito.

Le autorizzazioni amministrative determinano l'interfaccia di monitoraggio che viene visualizzata agli amministratori e le attività che possono eseguire. Le autorizzazioni determinano:

- Le viste a cui l'amministratore può accedere, denominate collettivamente come "vista".

- Desktop, macchine e sessioni che l'amministratore può visualizzare e con cui può interagire.
- I comandi che l'amministratore può eseguire, ad esempio lo shadowing della sessione di un utente o l'abilitazione della modalità di manutenzione.

Il monitoraggio ora supporta i ruoli di amministratore delegato che consentono di assegnare ruoli personalizzati o incorporati agli amministratori. Il ruolo determina le autorizzazioni disponibili e quindi il modo in cui un amministratore utilizza il monitoraggio. È inoltre possibile definire l'ambito applicabile a tali ruoli. L'ambito definisce gli oggetti per i quali è applicabile il ruolo.

Per informazioni sulla creazione di amministratori delegati, vedere l'articolo principale sull'amministrazione delegata.

I ruoli e le autorizzazioni predefiniti determinano il modo in cui gli amministratori utilizzano **Monitor**:

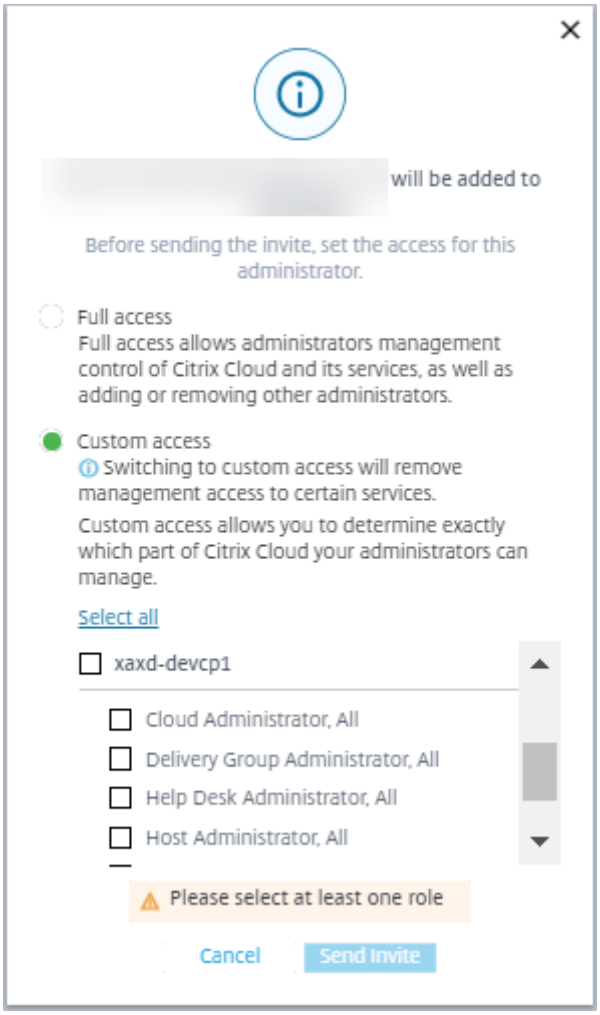
| Ruolo di amministratore | Autorizzazioni in Monitor |
|---|---|
| Full Administrator (Amministratore completo) | Ha accesso completo a tutte le viste e può eseguire tutti i comandi, incluso lo shadowing della sessione di un utente, l'abilitazione della modalità di manutenzione e l'esportazione dei dati delle tendenze. |
| Delivery group Administrator (Amministratore del gruppo di consegna) | Ha accesso completo a tutte le viste e può eseguire tutti i comandi, incluso lo shadowing della sessione di un utente, l'abilitazione della modalità di manutenzione e l'esportazione dei dati delle tendenze. |
| Read Only Administrator (Amministratore di sola lettura) | Può accedere a tutte le viste e visualizzare tutti gli oggetti in ambiti specifici in aggiunta a informazioni globali. Può scaricare report dai canali HDX ed esportare i dati delle tendenze utilizzando l'opzione Export (Esporta) nella vista Trends (Tendenze). Non può eseguire altri comandi o modificare elementi nelle viste. |

| Ruolo di amministratore | Autorizzazioni in Monitor |
|---|---|
| Help Desk Administrator (Amministratore dell'helpdesk) | Può accedere solo alle viste Help Desk (Helpdesk) e User Details (Dettagli utente) e può visualizzare solo gli oggetti che l'amministratore è delegato a gestire. Può fare lo shadowing della sessione di un utente ed eseguire comandi per quell'utente. Può eseguire operazioni in modalità di manutenzione. Può utilizzare le opzioni di controllo dell'alimentazione per macchine con sistema operativo a sessione singola. Non può accedere alle viste Dashboard, Trends (Tendenze), Alerts (Avvisi) o Filters (Filtri). Non può utilizzare le opzioni di controllo dell'alimentazione per macchine con sistema operativo multisessione. |
| Machine catalog administrator (Amministratore del catalogo macchine) | Può accedere solo alla pagina Machine Details (Dettagli macchina) (ricerca basata su macchina). |
| Host Administrator (Amministratore host) | Nessun accesso. Questo amministratore non è supportato per Monitor e non può visualizzare i dati. |
| Probe Agent Administrator (Amministratore di Probe Agent) | Accesso in sola lettura alla pagina Applications; accesso non consentito a nessun'altra visualizzazione. Pensato per eseguire Citrix Probe Agent su macchine endpoint. |
| Monitoring Full Administrator (Amministratore completo del monitoraggio) | Ha l'accesso completo a tutte le viste e i comandi nella scheda **Monitor** . |
| Session Administrator (Amministratore della sessione) | Può visualizzare i gruppi di consegna e gestire le sessioni e i computer associati nella pagina **Filters** della scheda **Monitor**. |

Per assegnare un ruolo (integrato o personalizzato) a un utente, dal menu Citrix Cloud, andare a **Identity and Access Management** (Gestione identità e accessi) > **Administrators**. Lì, quando si aggiunge o si modifica l'accesso di un amministratore, è possibile selezionare **Custom Access** (Accesso personalizzato) e uno dei ruoli elencati.

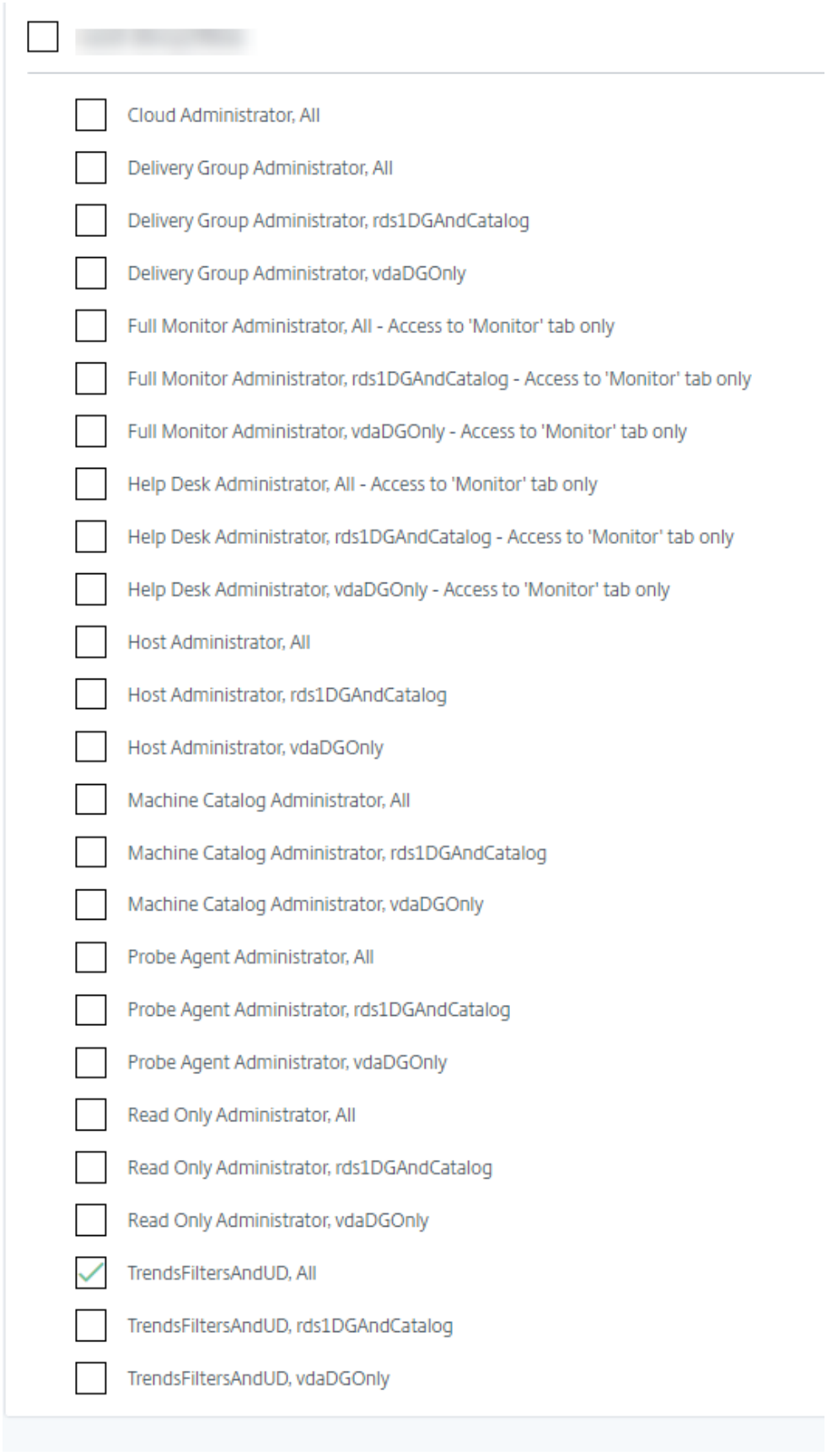
 




È possibile definire ruoli e ambiti personalizzati in **Full Configuration > Administrators > Administrators**.

I ruoli incorporati e i ruoli personalizzati sono elencati per consentirne la selezione con ambito personalizzato.



# Granularità e conservazione dei dati

January 18, 2023

## Aggregazione dei valori dei dati

Il servizio di monitoraggio raccoglie vari dati, tra cui l'utilizzo della sessione utente, i dettagli sulle prestazioni di accesso dell'utente, i dettagli del bilanciamento del carico della sessione e le informazioni relative alla connessione e ai guasti della macchina. I dati vengono aggregati in modo diverso a seconda della categoria. Comprendere l'aggregazione dei valori dei dati presentati utilizzando le API del metodo OData è fondamentale per l'interpretazione dei dati. Ad esempio:

- Per un determinato periodo di tempo si verificano errori relativi alle sessioni connesse e alle macchine. Pertanto, sono espressi come valori massimi in un periodo di tempo.
- Logon Duration (Durata dell'accesso) è una misura della durata del tempo, quindi viene esposta come media in un periodo di tempo.
- Logon Count (Conteggio degli accessi) e Connection Failures (Errori di connessione) sono conteggi di occorrenze in un determinato periodo di tempo, pertanto vengono espressi come somme nell'arco di un periodo di tempo.

## Valutazione simultanea dei dati

Le sessioni devono essere sovrapposte per essere considerate simultanee. Tuttavia, quando l'intervallo di tempo è di 1 minuto, tutte le sessioni in quel minuto (che si sovrappongano o meno) sono considerate simultanee. La dimensione dell'intervallo è così piccola che il sovraccarico delle prestazioni correlato al calcolo della precisione non ha sostanzialmente valore. Se le sessioni si verificano nella stessa ora, ma non nello stesso minuto, non vengono considerate sovrapposte.

## Correlazione delle tabelle di riepilogo con dati non elaborati

Il modello di dati rappresenta le metriche in due modi diversi:

- Le tabelle di riepilogo rappresentano viste aggregate delle metriche in granularità al minuto, ora e giorno.
- I dati non elaborati rappresentano singoli eventi o lo stato corrente individuati nella sessione, nella connessione, nell'applicazione e in altri oggetti.

Quando si tenta di correlare i dati tra le chiamate API o all'interno del modello di dati stesso, è importante comprendere i seguenti concetti e limitazioni:

- **Nessun dato di riepilogo per intervalli parziali.** I riepiloghi delle metriche sono progettati per soddisfare le esigenze delle tendenze storiche per lunghi periodi di tempo. Queste metriche vengono aggregate nella tabella di riepilogo per intervalli completi. Non ci sono dati di riepilogo per un intervallo parziale all'inizio (dati più vecchi disponibili) della raccolta dati né alla fine. Quando si visualizzano aggregazioni di un giorno (Interval=1440), ciò significa che i primi e i più recenti giorni incompleti non hanno dati. Sebbene possano esistere dati non elaborati per questi intervalli parziali, non vengono mai riassunti. Estrarre la SummaryDate minima e massima da una particolare tabella di riepilogo per determinare il primo e l'ultimo intervallo aggregato per una particolare granularità dei dati. La colonna SummaryDate (Data riepilogo) rappresenta l'inizio dell'intervallo. La colonna Granularity (Granularità) rappresenta la lunghezza dell'intervallo per i dati aggregati.
- **Correlazione in base al tempo.** Le metriche vengono aggregate nella tabella di riepilogo per intervalli completi come descritto nella sezione precedente. Possono essere utilizzati per le tendenze storiche, ma gli eventi non elaborati potrebbero essere più attuali nello stato di quanto è stato riassunto per l'analisi delle tendenze. Qualsiasi confronto temporale tra riepilogo e dati non elaborati deve tenere conto che non vi sono dati di riepilogo per intervalli parziali che potrebbero verificarsi o per l'inizio e la fine del periodo di tempo.
- **Eventi mancati e latenti.** Le metriche aggregate nella tabella di riepilogo potrebbero risultare leggermente imprecise se gli eventi non vengono rilevati o sono latenti nel periodo di aggregazione. Sebbene il servizio di monitoraggio cerchi di mantenere uno stato corrente accurato, non torna indietro nel tempo per rielaborare l'aggregazione nelle tabelle di riepilogo per eventi mancanti o latenti.
- **Alta disponibilità della connessione.** Durante l'alta disponibilità della connessione, ci sono lacune nel conteggio dei dati di riepilogo delle connessioni correnti, ma le istanze di sessione sono ancora in esecuzione nei dati non elaborati.
- **Periodi di conservazione dei dati.** I dati nelle tabelle di riepilogo vengono conservati in una pianificazione di pulizia diversa dalla pianificazione per i dati non elaborati relativi agli eventi. I dati potrebbero essere mancanti perché sono stati eliminati dal riepilogo o dalle tabelle non elaborate. Anche i periodi di conservazione potrebbero differire a seconda delle diverse granularità dei dati di riepilogo. I dati con granularità inferiore (minuti) vengono puliti più rapidamente rispetto ai dati con granularità più elevata (giorni). Se i dati mancano da una granularità a causa della pulizia, si potrebbero trovare in una granularità più elevata. Poiché le chiamate API restituiscono solo la granularità specifica richiesta, se non si ricevono dati per una granularità non significa che i dati non esistano per una granularità superiore per lo stesso periodo di tempo.
- **Fusi orari.** Le metriche vengono memorizzate con timestamp UTC. Le tabelle di riepilogo sono aggregate in base ai limiti di un'ora del fuso orario. Per i fusi orari che non utilizzano limiti di un'ora, potrebbe esserci qualche discrepanza riguardo a dove i dati sono aggregati.

### Granularità e conservazione

La granularità dei dati aggregati recuperati da Monitor è una funzione dell'intervallo temporale (T) richiesto. Le regole sono le seguenti:

- 0 < T <= 30 giorni d'uso della granularità all'ora
- T > 31 giorni d'uso della granularità al giorno

I dati richiesti che non provengono da dati aggregati provengono dalle informazioni non elaborate sulla sessione e sulla connessione. Questi dati tendono a crescere rapidamente e quindi hanno le proprie impostazioni di pulizia. La pulizia garantisce che solo i dati rilevanti siano conservati a lungo termine. Ciò garantisce prestazioni migliori pur mantenendo la granularità richiesta per la creazione di report.

| | Nome impostazione | Pulizia interessata | Giorni di conservazione per Premium | Giorni di conservazione per Advanced |
|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays (Giorni di conservazione della pulizia delle sessioni) | Elimina i record sulla sessione e la connessione dopo il termine della sessione | 90 | 31 |
| 2 | GroomFailuresRetentionDays (Giorni di conservazione della pulizia degli errori) | Elimina i record MachineFailureLog (Log degli errori macchina) e ConnectionFailureLog (Log degli errori di connessione) | 90 | 31 |

| | | Nome impostazione | Pulizia interessata | Giorni di conservazione per Premium | Giorni di conservazione per Advanced |
|---|---|---|---|---|---|
| | 3 | GroomLoadIndexesRetentionDays (Giorni di conservazione della pulizia degli indici di caricamento) | PerfCounterLoadIndex (Indice di caricamento) | 90 | 31 |

| | | Nome impostazione | Pulizia interessata | Giorni di conservazione per Premium | Giorni di conservazione per Advanced |
|---|---|---|---|---|---|
| | 4 | GroomDeletedRetentionDays (Giorni di conservazione della pulizia degli elementi eliminati) | Entità Machine (Macchina), Catalog (Catalogo), Desktop-Group (Gruppo desktop) e Hypervisor con stato del ciclo di vita "Deleted" (Eliminato). Questa impostazione elimina anche tutti i record Session (Sessione), SessionDetail (Dettagli sessione), Summary (Riepilogo), Failure (Errore) o LoadIndex (Indice di caricamento) correlati. | 90 | 31 |

| | | Nome impostazione | Pulizia interessata | Giorni di conservazione per Premium | Giorni di conservazione per Advanced |
|---|---|---|---|---|---|
| | 5 | GroomSummariesRetentionDays (Giorni di conservazione della pulizia dei riepiloghi) | Record Desktop-GroupSummary (Riepilogo dei gruppi desktop), FailureLogSummary (Riepilogo dei log degli errori) e LoadIndexSummary (Riepilogo degli indici di caricamento). Dati aggregati: granularità giornaliera | 365 | 31 |
| | 6 | GroomMachineHotfixLogRetentionDays (Giorni di conservazione della pulizia dei log degli hotfix delle macchine) | Hotfix applicati alle macchine con VDA e Controller | 90 | 31 |
| | 7 | GroomHourlyRetentionDays (Giorni di conservazione della pulizia delle ore) | Dati aggregati - granularità oraria | 32 | 31 |

| | Nome impostazione | Pulizia interessata | Giorni di conservazione per Premium | Giorni di conservazione per Advanced |
|---|---|---|---|---|
| 8 | GroomApplicationInstanceLogRetentionDays (Giorni di conservazione della pulizia delle istanze delle applicazioni) | Cronologia dell'istanza dell'applicazione | 90 | Non applicabile |
| 9 | GroomNotificationLogRetentionDays (Giorni di conservazione della pulizia dei log delle notifiche) | Registri delle notifiche | 90 | Non applicabile |
| 10 | GroomResourceUsageRawDataRetentionDays (Giorni di conservazione della pulizia dei dati non elaborati sull'utilizzo delle risorse) | Utilizzo delle risorse - dati non elaborati | 3 | 3 |
| 11 | GroomResourceUsageHourDataRetentionDays (Giorni di conservazione della pulizia dei dati delle ore di utilizzo delle risorse) | Utilizzo riepilogo dell'utilizzo delle risorse - granularità all'ora | 30 | 30 |
| 12 | GroomResourceUsageDayDataRetentionDays (Giorni di conservazione della pulizia dei dati dei giorni di utilizzo delle risorse) | Utilizzo riepilogo dell'utilizzo delle risorse - granularità al giorno | 365 | 31 |

| | | Nome impostazione | Pulizia interessata | Giorni di conservazione per Premium | Giorni di conservazione per Advanced |
|---|---|---|---|---|---|
| | 13 | GroomProcessUsageRawDataRetentionDays (Giorni di conservazione della pulizia dei dati non elaborati di utilizzo dei processi) | Pulizia dei dati non elaborati dei processi - dati non elaborati | 1 | 1 |
| | 14 | GroomProcessUsageHourDataRetentionDays (Giorni di conservazione della pulizia delle ore di utilizzo dei processi) | Pulizia dei dati orari dei processi - granularità all'ora | 7 | 7 |
| | 15 | GroomProcessUsageDayDataRetentionDays (Giorni di conservazione della pulizia dei giorni di utilizzo dei processi) | Pulizia dei dati giornalieri dei processi - granularità al giorno | 30 | 30 |
| | 16 | GroomSessionMetricsDataRetentionDays (Giorni di conservazione della pulizia dei dati delle metriche delle sessioni) | Pulizia dei dati delle metriche delle sessioni | 1 | 1 |
| | 17 | GroomMachineMetricsDataRetentionDays (Giorni di conservazione della pulizia dei dati delle metriche delle macchine) | Pulizia dei dati delle metriche delle macchine | 3 | 3 |

| | Nome impostazione | Pulizia interessata | Giorni di conservazione per Premium | Giorni di conservazione per Advanced |
|---|---|---|---|---|
| 18 | GroomMachineMetricDaily (Giorni di conservazione della pulizia dei dati di riepilogo dei giorni delle metriche delle macchine) | Dati di riepilogo delle metriche delle macchine | 395 DataRetentionDays | 31 |
| 19 | GroomApplicationErrorsRetentionDays (Giorni di conservazione della pulizia degli errori delle applicazioni) | Errori delle applicazioni | 1 | 1 |
| 20 | GroomApplicationFaultsRetentionDays (Giorni di conservazione della pulizia dei problemi delle applicazioni) | Problemi delle applicazioni | 1 | 1 |

> **Attenzione:**
>
> Non è possibile modificare i valori nel database del servizio Monitor.

La conservazione dei dati per lunghi periodi ha le seguenti implicazioni sulle dimensioni della tabella:

- **Dati orari.** Se i dati orari possono rimanere nel database per un massimo di due anni, un sito di 1000 gruppi di consegna può causare la crescita del database come segue:

  1000 gruppi di consegna x 24 ore al giorno x 365 giorni all'anno x 2 anni = 17.520.000 righe di dati. L'impatto sulle prestazioni di una quantità così elevata di dati nelle tabelle di aggregazione è significativo. Poiché i dati della dashboard sono ricavati da questa tabella, i requisiti relativi

al server del database potrebbero essere notevoli. Una quantità eccessiva di dati può avere un impatto significativo sulle prestazioni.

- **Dati di sessioni ed eventi.** Questi sono i dati raccolti ogni volta che viene avviata una sessione e viene effettuata una connessione/riconnessione. Per un sito di grandi dimensioni (100.000 utenti), questi dati crescono rapidamente. Ad esempio, due anni di queste tabelle raccoglierebbero più di un TB di dati, richiedendo un database di livello aziendale di fascia alta.

## Diagnostica di avvio della sessione

September 12, 2023

> **Nota:**
>
> La diagnostica di avvio della sessione è attualmente in anteprima.

I lanci delle sessioni coinvolgono molteplici componenti Citrix. Per diagnosticare gli errori di avvio della sessione, utilizzare Citrix Monitor (ovvero il servizio Citrix Director) per individuare il componente e la fase esatti in cui si è verificato il problema. Applicare le azioni consigliate per risolvere il problema. L'app Citrix Workspace genera un ID transazione di 32 cifre (8-4-4-4-12) che può essere utilizzato per diagnosticare gli errori di avvio della sessione.

> **Nota:**
>
> Questa funzione è disponibile solo per i clienti cloud nelle regioni seguenti: Stati Uniti, AP-S e UE. Non è disponibile in Giappone e nelle regioni governative.

### Prerequisiti

Se si utilizza Citrix DaaS, l'integrazione è automatica. I clienti cloud che utilizzano StoreFront locale devono assicurarsi che sia stata integrata una versione StoreFront supportata.

- Se si utilizza Citrix Analytics for Performance, vedere Data sources per i passaggi per l'integrazione di StoreFront locale.
- Se non si utilizza Citrix Analytics per le prestazioni:
  1. Passare a `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.
  2. Fare clic su **Connect to StoreFront deployment** (Connetti alla distribuzione di StoreFront), inserire i dettagli e scaricare il file di configurazione. Per ulteriori informazioni, vedere Onboarding di siti locali tramite StoreFront.

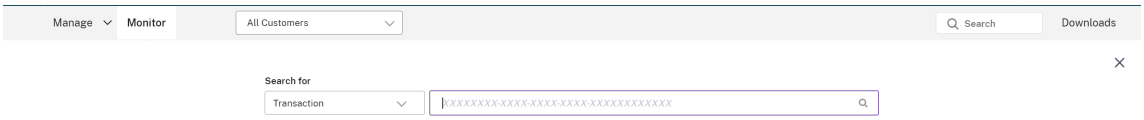
> **Nota:**
>
> Gli amministratori con ruoli di Cloud Administrator possono effettuare l'onboarding delle implementazioni StoreFront, mentre gli amministratori con il ruolo di Full Monitor Administrator possono visualizzare solo le implementazioni StoreFront.

Le versioni minime supportate di altri componenti sono le seguenti:

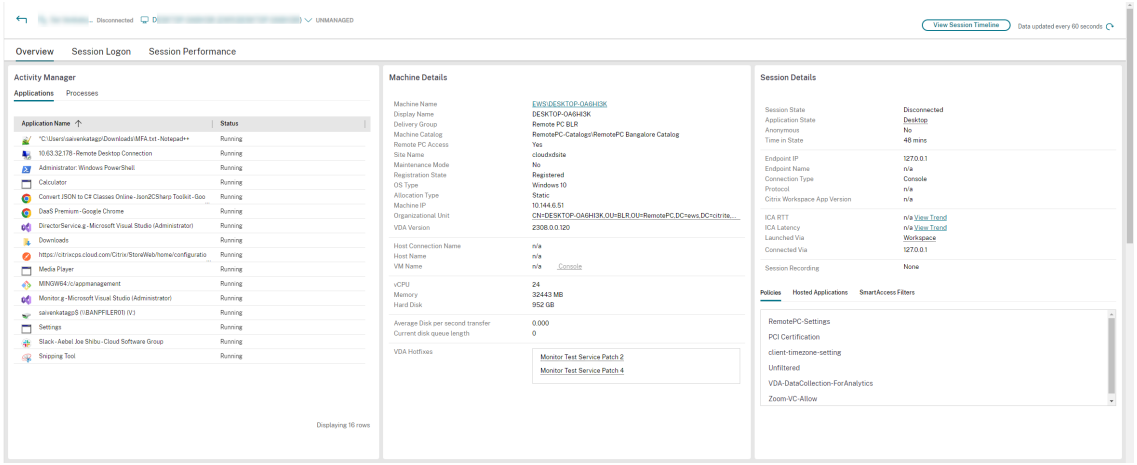
- App Citrix Workspace per Windows 2109
- App Citrix Workspace per Mac 2112
- App Citrix Workspace per Linux versione 2112
- App Citrix Workspace per HTML5 2110
- App Citrix Workspace per Chrome 2110
- App Citrix Workspace per Android 2110
- Versione VDA Citrix Virtual Apps and Desktops 2112
- Citrix StoreFront 1912 LTSR CU4

## Passaggi per diagnosticare un errore di avvio della sessione

1. Copiare l'ID della transazione dell'avvio di sessione non riuscito dall'app Citrix Workspace.
2. Nell'interfaccia utente di Monitor, cercare l'ID della transazione a 32 cifre e fare clic su **Details**.

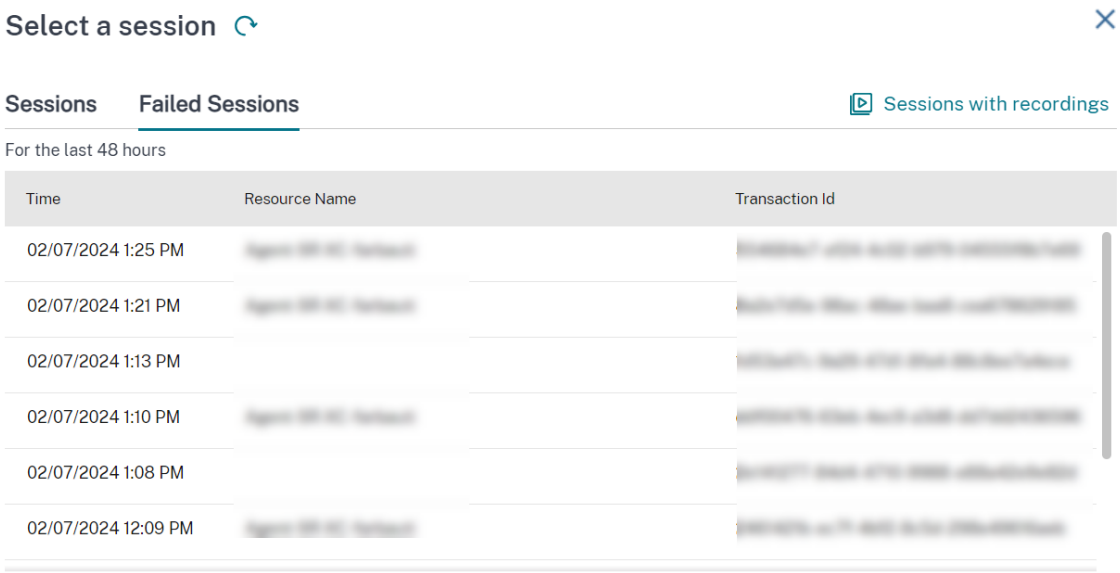



3. Se l'ID della transazione non è disponibile, effettuare la ricerca utilizzando il nome utente. Viene visualizzato l'Activity Manager dell'utente.

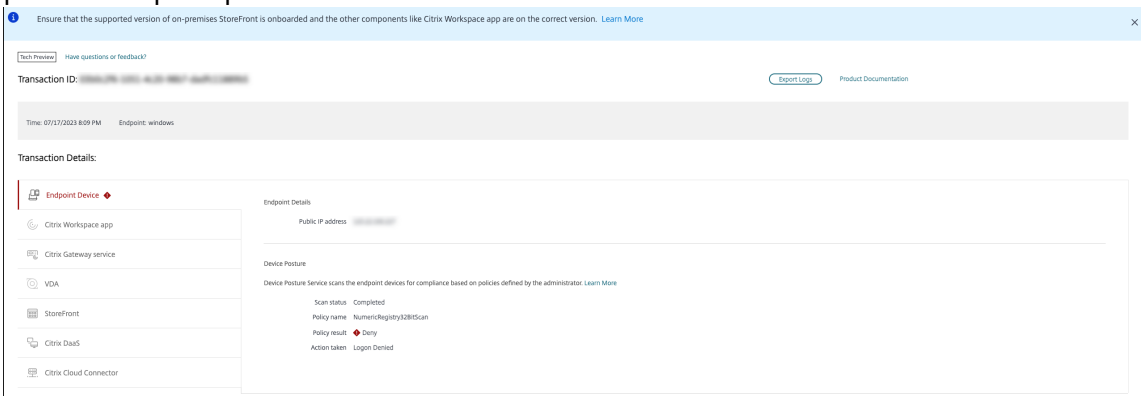


4. Fare clic sul selettore di sessione. Passare alla scheda **Failed sessions** (Sessioni non riuscite). Viene visualizzato un elenco delle sessioni che non sono riuscite nelle ultime 48 ore. Fare clic sulla sessione selezionata.




5. Citrix Monitor visualizza le informazioni chiave relative alla transazione, come il nome utente, l'indicatore data e ora e l'applicazione o il desktop su cui si è verificato l'errore.
6. Il pannello Transaction Details (Dettagli transazione) contiene un elenco di componenti che indicano il verificarsi dell'errore.
7. Fare clic su **Endpoint Device** (Dispositivo endpoint) nell'elenco dei componenti per visualizzare lo stato della scansione di Device Posture. Il servizio Device Posture esegue la scansione del dispositivo endpoint per verificare la conformità in base ai criteri definiti dall'amministratore.




Vengono visualizzati lo stato della scansione, il nome del criterio, il risultato del criterio e l'azione intrapresa. Assicurarsi che il servizio Device Posture sia configurato con DaaS come descritto nell'articolo su Device Posture. Gli errori registrati da Device Posture sono descritti in Device Posture Error Logs.

8. Fare clic sui nomi degli altri componenti per controllare i dettagli del componente e i dettagli

dell'ultimo errore noto.

9. Vengono visualizzati il motivo dell'errore e il codice di errore. Fare clic sul collegamento **Learn more about the error** (Ulteriori informazioni sull'errore) per visualizzare il codice di errore specifico nella sezione Error codes (Codici di errore) che contiene la descrizione dettagliata e l'azione consigliata.
10. È possibile esportare i log per visualizzarli. Il file di registro elenca le fasi di avvio della sessione in ordine cronologico e mostra il componente esatto e la fase in cui si è verificato l'errore.
11. Nel caso in cui si sia verificato più di un errore tra i componenti, nella pagina Transaction (Transazione) vengono visualizzati solo gli ultimi dettagli dell'errore noto. I log esportati contengono i dettagli di tutti gli errori relativi alla transazione.

> **Nota:**
>
> I codici di errore lato client e le informazioni diagnostiche sono disponibili solo quando Citrix StoreFront è integrato e invia dati. Per ulteriori informazioni sull'onboarding di StoreFront, vedere Prerequisiti.

## Agente broker

### bka.prepare.session.failure.validation

- Descrizione: Impossibile convalidare la richiesta di preparazione della sessione.
- Azione consigliata: Riprovare l'azione. Se l'errore si ripete, verificare che i connettori siano integri.

### bka.prepare.session.failure.rejected

- Descrizione: il VDA non può accettare la richiesta di avvio.
- Azione consigliata: riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.

### bka.hdx.prepare.failure.general

- Descrizione: errore di preparazione dell'HDX.
- Azione consigliata: riavviare il VDA.

### bka.hdx.validate.failure.ticket_not_found

- Descrizione: ticket o avvio di riferimento non presente nella cache di avvio.
- Azione consigliata: assicurarsi che il VDA sia in grado di comunicare con il connettore.

#### bka.ticketing.validate.failure.unlicensed

- Descrizione: impossibile verificare la licenza per l'avvio.
- Azione consigliata: contattare il supporto Citrix.

#### bka.ticketing.validate.failure.general

- Descrizione: errore generico durante la convalida del ticket.
- Azione consigliata: raccogliere i registri sul VDA e contattare il supporto Citrix.

#### bka.set.configuration.failure.policy

- Descrizione: si è verificato un errore durante l'impostazione dei criteri.
- Azione consigliata: riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.

#### bka.set.configuration.failure

- Descrizione: si è verificato un errore durante la configurazione dell'impostazione.
- Azione consigliata: riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.

### Broker

#### brk.validate.credentials.failure.invalid

- Descrizione: impossibile convalidare le credenziali a causa di un problema. Il motivo può essere espanso nel parametro message.
- Azione consigliata: Riprovare l'azione. Se l'errore si ripete, verificare che i connettori siano integri.

#### brk.resolve.machine.failure.general

- Descrizione: impossibile enumerare o risolvere il lavoratore. Il motivo può essere espanso nel parametro message.
- Azione consigliata: assicurarsi che le macchine in grado di avviare questa applicazione siano registrate presso il Broker. Assicurarsi che tutte le macchine disponibili non abbiano raggiunto la loro capacità.

**brk.license.check.failure.constraints**

- Descrizione: impossibile avviare la sessione a causa dei vincoli di licenza.
- Azione consigliata: assicurarsi che siano disponibili licenze per questo tipo di applicazione o desktop.

**brk.resolve.machine.failure.timeout**

- Descrizione: il tempo del broker è scaduto durante il contatto con il database.
- Azione consigliata: problemi di comunicazione con il database del sito. Contattare il supporto Citrix.

**brk.poweron.forlaunch.queued.failure.general**

- Descrizione: Azione di accensione in coda non riuscita.
- Azione consigliata: problemi di comunicazione con il database del sito. Contattare il supporto Citrix.

**brk.set.configuration.failure.general**

- Descrizione: errore non specificato durante l'impostazione della configurazione sul VDA di destinazione.
- Azione consigliata: riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.

**brk.prepare.session.failure.host_unreachable**

- Descrizione: impossibile comunicare con il VDA.
- Azione consigliata: riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.

**brk.prepare.session.failure.general**

- Descrizione: impossibile preparare la sessione in caso di errori VDA, UnsupportedClientType o ConnectionRefused.
- Azione consigliata: riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.

**brk.validate.ticket.failure.license**

- Descrizione: impossibile recuperare una licenza valida per questa sessione.

- Azione consigliata: verificare lo stato di integrità del sito e assicurarsi che tutti i connettori e Citrix DDC siano operativi.

#### brk.validate.ticket.failure.general

- Descrizione: chiamata ticket non valida.
- Azione consigliata: contattare il supporto Citrix.

#### brk.reverse.prepare.failure.general

- Descrizione: errore generico durante l'avvio della sessione.
- Azione consigliata: verificare lo stato di integrità del sito e assicurarsi che tutti i connettori e Citrix DDC siano operativi.

#### brk.reverse.prepare.failure.lease_revoked

- Descrizione: il contratto di leasing per questa sessione è stato revocato.
- Azione consigliata: riprovare l'azione; se l'errore si ripete, verificare che i connettori siano in uno stato integro.

#### brk.reverse.prepare.failure.resource_unavailable

- Descrizione: la risorsa è già in uso o è temporaneamente non disponibile.
- Azione consigliata: riprovare l'azione; se l'errore si ripete, verificare che i connettori siano in uno stato integro.

#### brk.reverse.prepare.failure.app_protection

- Descrizione: App Protection manca ed è necessario per questa sessione.
- Azione consigliata: assicurarsi che la protezione delle app sia abilitata su questo VDA o rimuovere il requisito di App Protection dall'applicazione.

### HDX VDA Linux

#### VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- Descrizione: non è consentito riconnettersi a una sessione in stato di pre-scollegamento.
- Azione consigliata: riprovare ad avviare più tardi, in modo da dare alla sessione il tempo di scollegarsi.

#### VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Descrizione: riconnettersi a una sessione non in uscita.
- Azione consigliata: riprovare l'avvio più tardi. Se il problema persiste, contattate il supporto Citrix.

#### VDA_LINUX_ERR_SAME_KEY

- Descrizione: durante la preparazione per una connessione è già presente una sessione esistente con la stessa chiave di sessione.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_GET_FQDN

- Descrizione: impossibile ottenere il nome di dominio completo di questo VDA.
- Azione consigliata: verificare che la configurazione DNS sul VDA sia corretta

#### VDA_LINUX_ERR_NO_CGP_LISTENER

- Descrizione: non è in esecuzione un listener CGP.
- Azione consigliata: verificare che il criterio **Session reliability connections** (connessioni di affidabilità della sessione) sia abilitato. Verificare che il listener CGP sia in ascolto sulla porta prevista del VDA (la porta predefinita è 2598, che può essere modificata tramite il criterio **Session reliability port number** [Numero di porta di affidabilità della sessione]).

#### VDA_LINUX_ERR_DTLS_CONNECT

- Descrizione: impossibile stabilire una connessione DTLS al servizio Gateway.
- Azione consigliata: verificare che il nome di dominio completo del servizio Gateway sia raggiungibile dal VDA. Verificare che il percorso `/var/xdl/keystore/cacerts` esista nel VDA. Rimuovere `/var/xdl/keystore` ed eseguire `/var/xdl/split_ca_bundle.sh` per rigenerare i certificati CA. Verificare che l'FQDN del servizio Gateway sia considerato attendibile dal VDA.

#### VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- Descrizione: impossibile accettare l'handshake EDT dal client.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_TCP_CONNECT

- Descrizione: impossibile stabilire una connessione TCP al servizio Gateway.
- Azione consigliata: verificare che il nome di dominio completo del servizio Gateway sia raggiungibile dal VDA.

#### VDA_LINUX_ERR_TLS_CONNECT

- Descrizione: impossibile stabilire un handshake TLS al servizio Gateway.
- Azione consigliata: verificare che il percorso `/var/xdl/keystore/cacerts` esista nel VDA. Rimuovere `/var/xdl/keystore` ed eseguire `/var/xdl/split_ca_bundle.sh` per rigenerare i certificati CA. Verificare che l'FQDN del servizio Gateway sia attendibile.

#### VDA_LINUX_ERR_RDVZ_HANDSHAKE

- Descrizione: impossibile stabilire un handshake di rendezvous al servizio Gateway.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- Descrizione: impossibile accettare una connessione ICA.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED

- Descrizione: non è consentito riconnettersi a una sessione anonima.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_CONN_NOT_ALLOWED

- Descrizione: la connessione non è consentita.
- Azione consigliata: se il codice risultato è 3, verificare che la licenza non sia scaduta, altrimenti riprovare ad avviare più tardi. Se non si riesce a risolvere il problema, contattare il supporto Citrix.

#### VDA_LINUX_ERR_CONN_GENERAL

- Descrizione: impossibile convalidare la connessione.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_USER_CANCELLED_LOGIN

- Descrizione: accesso annullato da parte dell'utente finale.
- Azione consigliata: questo errore è previsto, quando l'SSO è disabilitato e l'utente finale fa clic sul pulsante "Annulla"nella casella di accesso; altrimenti, contattare il supporto Citrix.

#### VDA_LINUX_ERR_GET_TARGET

- Descrizione: impossibile ottenere la sessione di destinazione.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_START_LOGON_TIMERS

- Descrizione: impossibile avviare i timer di accesso.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- Descrizione: impossibile inviare il comando alla sessione di destinazione.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Descrizione: impossibile pubblicare un evento di riconnessione.
- Azione consigliata: contattare il supporto Citrix.

#### VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Descrizione: timeout della riconnessione alla sessione utente.
- Azione consigliata: contattare il supporto Citrix.

### HDX VDA Windows

#### RENDEZVOUS_CONNECT_FAILED_TCP

- Descrizione: un tentativo di connessione al trasporto Rendezvous in uscita su TCP non è riuscito.
- Azione consigliata: possono verificarsi guasti sporadici a causa di condizioni di rete scadenti. Questo è previsto. Controllare la configurazione VDA se ciò si verifica frequentemente, quindi contattare il supporto Citrix.

**RENDEZVOUS_CONNECT_FAILED_EDT**

- Descrizione: un tentativo di connessione al trasporto Rendezvous in uscita su TCP non è riuscito.
- Azione consigliata: possono verificarsi guasti sporadici a causa di condizioni di rete scadenti. Questo è previsto. Controllare la configurazione VDA se ciò si verifica frequentemente, quindi contattare il supporto Citrix.

**RENDEZVOUS_CONNECT_FAILED_PROXY**

- Descrizione: un tentativo di connessione al trasporto Rendezvous in uscita non è riuscito a causa di una configurazione proxy non valida.
- Azione consigliata: controllare la configurazione del proxy Rendezvous, contattare il supporto Citrix.

**RENDEZVOUS_CONNECT_FAILED_DTLS**

- Descrizione: un tentativo di connessione al trasporto Rendezvous in uscita non è riuscito a causa di un errore dell'handshake di trasporto sicuro.
- Azione consigliata: controllare la configurazione del Rendezvous, controllare la configurazione crittografica. Contattare il supporto Citrix.

**RENDEZVOUS_CONNECT_FAILED_TLS**

- Descrizione: un tentativo di connessione al trasporto Rendezvous in uscita non è riuscito a causa di un errore dell'handshake di trasporto sicuro.
- Azione consigliata: controllare la configurazione del Rendezvous, controllare la configurazione crittografica e contattare il supporto Citrix.

**RENDEZVOUS_CONNECT_FAILED_CGP**

- Descrizione: un tentativo di connessione al trasporto Rendezvous in uscita non è riuscito a causa di un problema di configurazione CGP.
- Azione consigliata: verificare che CGP (Session Reliability) sia abilitato e che le porte CGP siano ascoltate, contattare il supporto Citrix.

**CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT**

- Descrizione: l'interruzione della rete non è stata risolta a causa del timeout, l'affidabilità della sessione non è riuscita a riprendere la connessione.

- Azione consigliata: possono verificarsi guasti sporadici a causa di condizioni di rete scadenti. Questo è previsto.

#### CGP_SR_SUSPEND_RESUME_FAILED

- Descrizione: l'interruzione della rete non è stata risolta a causa di un errore imprevisto, l'affidabilità della sessione non è riuscita a riprendere la connessione.
- Azione consigliata: possono verificarsi guasti sporadici a causa di condizioni di rete scadenti. Questo è previsto.

#### PREPARE_RECONNECT_REJECTED

- Descrizione: il VDA ha rifiutato una richiesta di riconnessione da una connessione ICA in entrata a causa di una chiave di sessione non valida.
- Azione consigliata: controllare la configurazione del VDA, contattare il supporto Citrix.

#### Errore: PREPARE_REJECTED

- Descrizione: il VDA ha rifiutato una richiesta di connessione da una connessione ICA in entrata a causa di una chiave di sessione non valida.
- Azione consigliata: controllare la configurazione del VDA, contattare il supporto Citrix.

#### PREPARE_LISTENING_FAILED

- Descrizione: il VDA non è riuscito ad avviare i listener per la connessione ICA in ingresso.
- Azione consigliata: controllare la configurazione di rete, verificare che le porte del listener non siano utilizzate da altre applicazioni, contattare il supporto Citrix.

#### RENDEZVOUSCONNECTIONREQ_FAILED

- Descrizione: il VDA non è riuscito a notificare allo stack ICA di avviare una connessione Rendezvous in uscita.
- Azione consigliata: controllare la configurazione del Rendezvous, controllare la configurazione del proxy di Rendezvous, controllare la configurazione CGP (Session Reliability), contattare il supporto Citrix.

#### RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- Descrizione: il VDA non è riuscito a richiedere allo stack ICA di avviare una connessione Rendezvous in uscita a causa di un errore di configurazione del proxy.
- Azione consigliata: controllare la configurazione del proxy Rendezvous, contattare il supporto Citrix.

#### ESTABLISH_SESSION_FAILED

- Descrizione: VDA non è riuscito a creare una sessione per la connessione ICA in ingresso o non è riuscito a connettersi a una sessione esistente.
- Azione consigliata: contattare il supporto Citrix.

#### ICA_ESTABLISH_FAILED

- Descrizione: le connessioni ICA sono accettate o l'handshake non è riuscito.
- Azione consigliata: contattare il supporto Citrix.

#### VALIDATE_FAILED

- Descrizione: il broker non è riuscito a convalidare una richiesta di connessione ICA in entrata dal VDA.
- Azione consigliata: contattare il supporto Citrix.

#### VALIDATE_TICKETING_FAILED

- Descrizione: il broker non è riuscito a convalidare una richiesta di connessione ICA in entrata dal VDA a causa di un problema di ticketing.
- Azione consigliata: contattare il supporto Citrix.

### MCS

#### brk.poweron.forlaunch.execution.generalfailure

- Descrizione: errori generali.
- Azione consigliata: contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.insufficientresourcefailure**

- Descrizione: un'operazione dell'hypervisor non può essere completata a causa di risorse insufficienti sull'hypervisor.
- Azione consigliata: controllare la quota di risorse dell'hypervisor. Se non si riesce a trovare una soluzione, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.nosuchmanagedmachine**

- Descrizione: un ID macchina non esiste.
- Azione consigliata: controllare l'ID macchina nell'hypervisor. Se non si riesce a trovare una soluzione, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.hypervisorconnectionfailure**

- Descrizione: impossibile stabilire una connessione all'hypervisor. Ad esempio, l'indirizzo dell'infrastruttura di hosting non è stato trovato.
- Azione consigliata: verificare che l'indirizzo dell'infrastruttura di hosting sia corretto. Se non si riesce a trovare una soluzione, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.invalidcredentialsfailure**

- Descrizione: credenziali non valide.
- Azione consigliata: verificare le credenziali per la connessione all'hypervisor. Se non si riesce a trovare una soluzione, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.authorizationfailure**

- Descrizione: privilegi o credenziali insufficienti.
- Azione consigliata: verificare l'autorizzazione assegnata alle credenziali per la connessione all'hypervisor. Se non si riesce a trovare una soluzione, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.sslcertauthfailure**

- Descrizione: non è possibile stabilire una connessione a causa di un problema di autenticazione SSL.
- Azione consigliata: controllare il certificato di connessione dell'hypervisor. Se non si riesce a trovare una soluzione, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.ratelimitedfailure**

- Descrizione: la connessione cloud segnala che la velocità è limitata.
- Azione consigliata: riprovare la connessione in un secondo momento se la richiesta è bloccata dal limite di velocità dell'hypervisor. Se non si riesce a trovare una soluzione, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.connectorconnectionfailure**

- Descrizione: si verificano errori nel connettore cloud. Ad esempio, si verifica un timeout durante l'attesa della connessione. Una volta raggiunto il timeout, il connettore cloud viene disconnesso.
- Azione consigliata: riavviare il connettore cloud. In caso di esito negativo, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.remotehclserverconnectionfailure**

- Descrizione: non sono stati rilevati errori sul plug-in proxy HCL/remoto o sul punto finale durante la configurazione della connessione al plug-in.
- Azione consigliata: riavviare il connettore. In caso di esito negativo, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.expiredcredentialsfailure**

- Descrizione: è stata fornita una credenziale scaduta.
- Azione consigliata: aggiornare le credenziali scadute utilizzate dalla connessione all'hypervisor.

**brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure**

- Descrizione: errori durante la creazione della macchina.
- Azione consigliata: contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.detachdiskfailed**

- Descrizione: il disco di disconnessione utilizzato dalla macchina virtuale ha riportato un errore.
- Azione consigliata: contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.createclonefailed**

- Descrizione: creazione del disco clone non riuscita nell'hypervisor.
- Azione consigliata: contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.provisionedvmnotfound**

- Descrizione: impossibile trovare la macchina virtuale di cui è stato eseguito il provisioning.
- Azione consigliata: rimuovere la macchina virtuale di cui è stato eseguito il provisioning dal catalogo. In caso di esito negativo, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.invalidvmstate**

- Descrizione: l'operazione non può procedere a causa di uno stato non valido della macchina virtuale.
- Azione consigliata: riavviare prima la macchina virtuale, quindi riprovare l'operazione.

**brk.poweron.forlaunch.execution.insufficientresources**

- Descrizione: risorse insufficienti durante il funzionamento.
- Azione consigliata: controllare la quota di risorse utilizzata dall'hypervisor.

**brk.poweron.forlaunch.execution.hypervisorinmaintenancemode**

- Descrizione: l'operazione non può continuare perché l'hypervisor è in modalità di manutenzione.
- Azione consigliata: verificare se l'hypervisor è in modalità di manutenzione.

**brk.poweron.forlaunch.execution.delayed**

- Descrizione: l'operazione è in coda.
- Azione consigliata: attendere il completamento del processo. Se l'operazione non riesce, contattare il supporto Citrix.

**brk.poweron.forlaunch.execution.recreatevmfailed**

- Descrizione: la ricreazione della macchina virtuale non è riuscita.
- Azione consigliata: contattare il supporto Citrix.

#### brk.poweron.forlaunch.execution.unknownvirtualmachine

- Descrizione: macchina virtuale sconosciuta.
- Azione consigliata: contattare il supporto Citrix.

#### brk.poweron.forlaunch.execution.ratelimitexceed

- Descrizione: la connessione cloud limita ha velocità limitata.
- Azione consigliata: riprovare la connessione in un secondo momento se la richiesta è stata bloccata dal limite di velocità dell'hypervisor.

#### brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- Descrizione: il disco virtuale non è memorizzato.
- Azione consigliata: riprovare più tardi. In caso di esito negativo, contattare il supporto Citrix.

### Profile Management

#### xendesktop.upm.userprofile.error.failure

- Descrizione: Citrix Profile Management non è riuscito a elaborare il profilo utente. Utilizzare invece un profilo temporaneo.
- Azione consigliata: questo errore non causa un errore di accesso. Citrix Profile Management utilizza invece un profilo temporaneo. Per risolvere l'errore, controllare i registri eventi di Windows.

#### xendesktop.upm.userprofile.error.timeout

- Descrizione: Citrix Profile Management non è riuscito a elaborare il profilo utente entro il tempo specificato.
- Azione consigliata: questo errore non causa un errore di accesso. Citrix Profile Management continua l'elaborazione del profilo utente. Per risolvere l'errore, controllare i log di Citrix Profile Management.

## WEM Agent

### wem.agent.userpolicy.error.failure

- Descrizione: l'agente WEM (Workspace Environment Management) non è riuscito a elaborare i criteri di gruppo per l'utente. L'accesso dell'utente continua.
- Azione consigliata: l'errore non causa errori di accesso. Per ulteriori dettagli, consultare la documentazione del prodotto WEM e controllare i log di servizio dell'agente WEM.

### wem.agent.userpolicy.error.timeout

- Descrizione: l'agente WEM (Workspace Environment Management) non è riuscito a elaborare i criteri di gruppo per l'utente entro il tempo specificato. L'accesso dell'utente continua.
- Azione consigliata: l'errore non causa errori di accesso. Per ulteriori dettagli, consultare la documentazione del prodotto WEM e controllare i log di servizio dell'agente WEM.

## Android dopo l'avvio

### SessionManager.Launch.EngineLoadFailed

- Descrizione: impossibile caricare o inizializzare ICA Engine.
- Azione consigliata: contattare il supporto Citrix.

### SessionManager.Launch.ConnectionFailed

- Descrizione: motore spento prima del collegamento.
- Azione consigliata: contattare il supporto Citrix.

### SessionManager.Launch.LogonFailed

- Descrizione: sessione disconnessa senza completare l'accesso.
- Azione consigliata: contattare il supporto Citrix.

### SessionManager.LeaseResolution.Failed

- Descrizione: impossibile tentare l'avvio del lease.
- Azione consigliata: contattare il supporto Citrix.

#### SessionManager.clxmtp.SoftDeny

- Descrizione: negoziazione CLXMTP del motore non riuscita (soft deny).
- Azione consigliata: contattare il supporto Citrix.

#### SessionManager.clxmtp.SoftDeny_Implicit

- Descrizione: connessione CLXMTP del motore non riuscita (soft deny implicito).
- Azione consigliata: contattare il supporto Citrix.

#### Transport.Connect.NoCGP_Fail

- Descrizione: connessione non riuscita (CGP disabilitato).
- Azione consigliata: contattare il supporto Citrix.

#### Transport.Connect.FallbackFail

- Descrizione: connessione non riuscita. È stato tentato il fallback dell'ICA.
- Azione consigliata: contattare il supporto Citrix.

#### Transport.Connect.Fail

- Descrizione: la connessione non è disponibile.
- Azione consigliata: contattare il supporto Citrix.

### Android prima dell'avvio

#### CWA-ICADOWNLOAD_ERR_00001

- Descrizione: il tipo di richiesta di invio ICA non è corretto.
- Azione consigliata: contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00002

- Descrizione: la richiesta ICA non è valida.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00003**

- Descrizione: lo store è nullo per la richiesta ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00004**

- Descrizione: l'URL dello store è nullo per la richiesta ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00005**

- Descrizione: il parametro resource è null per la richiesta ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00006**

- Descrizione: il parametro resource fornito per la richiesta ICA non è un tipo di risorsa valido.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00007**

- Descrizione: il parametro resource fornito per la richiesta ICA è null per l'URL di avvio ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00008**

- Descrizione: la richiesta ICA è nulla con i parametri del gestore dell'autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00009**

- Descrizione: il corpo della richiesta ICA è nullo.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000010**

- Descrizione: impossibile creare un'entità HTTP dal corpo della richiesta ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000011**

- Descrizione: impossibile scaricare il file ICA a causa di un'eccezione alla creazione della richiesta di gestione dell'autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000012**

- Descrizione: impossibile scaricare il file ICA a causa di un'eccezione all'esecuzione della richiesta di gestione dell'autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000013**

- Descrizione: impossibile scaricare il file ICA a causa di una risposta imprevista dalla richiesta di gestione dell'autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000014**

- Descrizione: impossibile scaricare il file ICA quando si copia inputStream dalla risposta della gestione dell'autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000015**

- Descrizione: impossibile analizzare il documento ICA utilizzando inputStream dalla risposta della gestione dell'autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000016**

- Descrizione: il documento ICA scaricato è nullo senza alcuna eccezione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000017**

- Descrizione: impossibile scaricare il file ICA a causa di una risposta non riuscita.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000018**

- Descrizione: la risorsa non è disponibile.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000019**

- Descrizione: la risorsa da avviare non esiste, non è abilitata o non è visibile a un utente.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000020**

- Descrizione: non ci sono più sessioni attive.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000021**

- Descrizione: il server non dispone della licenza necessaria per eseguire l'attività richiesta.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000022**

- Descrizione: non sono disponibili workstation.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000023**

- Descrizione: impossibile connettersi alla workstation. Il server ha rifiutato la connessione.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000024**

- Descrizione: la workstation è in manutenzione e non è disponibile per l'uso.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000025**

- Descrizione: impossibile avviare la risorsa a causa di un errore di tipo `resourceerror` nel file ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000026**

- Descrizione: impossibile avviare la risorsa a causa di un errore di tipo `generalapplauncherror` nel file ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000027**

- Descrizione: impossibile avviare la risorsa a causa di un errore sconosciuto nel file ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000028**

- Descrizione: impossibile avviare la risorsa a causa di un errore di riavvio nel file ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000029**

- Descrizione: impossibile avviare la risorsa a causa di un errore di ripresa nel file ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000030**

- Descrizione: impossibile avviare la risorsa a causa di un errore indefinito nel file ICA.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_000031**

- Descrizione: impossibile scaricare il file ICA. Tuttavia, il codice di errore non si trova nella mappa definita.
- Azione consigliata: contattare il supporto Citrix.

## Linux dopo l'avvio

### SessionManager.Launch.EngineLoadFailed

- Descrizione: impossibile caricare il motore ICA.
- Azione consigliata: contattare il supporto Citrix.

### SessionManager.Launch.Failed

- Descrizione: impossibile avviare la sessione.
- Azione consigliata: contattare il supporto Citrix.

### SessionManager.Launch.ConnectionFailed

- Descrizione: motore spento prima del collegamento.
- Azione consigliata: cercare altri errori associati al tentativo di avvio.

### SessionManager.Launch.LogonFailed

- Descrizione: sessione disconnessa senza completare l'accesso.
- Azione consigliata: questo errore indica un problema di accesso, che potrebbe includere un errore da parte dell'utente nell'immettere manualmente le credenziali. Scoprire la modalità con cui l'utente ha tentato di accedere al VDA remoto.

### SessionManager.LeaseResolution.Failed

- Descrizione: impossibile tentare l'avvio del lease.
- Azione consigliata: verificare che i lease siano stati sincronizzati con il computer client e siano ancora validi. L'utente può accedere a Citrix Workspace in modalità online per attivare la (ri)sincronizzazione dei lease. Cercare errori inviati dai componenti Gateway o Cloud Connector. Questi errori potrebbero indicare i motivi dell'errore.

### Transport.Connect.NoCGP_Fail

- Descrizione: connessione non riuscita (CGP disabilitato).
- Azione consigliata: indagare sul motivo per cui il client non è in grado di contattare un VDA tramite TCP o EDT.

#### Transport.Connect.FallbackFail

- Descrizione: connessione non riuscita. È stato tentato il fallback dell'ICA.
- Azione consigliata: indagare sul motivo per cui il client non è in grado di contattare un gateway, un Connector o un VDA tramite TCP o EDT.

#### Transport.Connect.Fail

- Descrizione: l'app Citrix Workspace non è riuscita a connettersi a gateway, un Connector o un VDA tramite TCP, EDT o UDP.
- Azione consigliata: verificare perché il client non è in grado di contattare il gateway, il Connector o il VDA tramite TCP, EDT o UDP. Il firewall tra client e host potrebbe non consentire i protocolli (UDP/TCP) o le porte richieste.

#### SessionManager.clxmtp.SoftDeny

- Descrizione: negoziazione CLXMTP del motore non riuscita (soft deny).
- Azione consigliata: questo errore non indica che l'avvio non debba riuscire. Indica che il motore non può riuscire attraverso un percorso di rete specifico. Cercare errori inviati dai componenti Gateway o Cloud Connector. Questi errori potrebbero indicare i motivi dell'errore.

#### SessionManager.clxmtp.SoftDeny_Implicit

- Descrizione: connessione CLXMTP del motore non riuscita (soft deny implicito).
- Azione consigliata: questo errore non indica che l'avvio non debba riuscire. Indica che il motore non può riuscire attraverso un percorso di rete specifico. Indagare sul motivo per cui il client non può contattare un Connector o un gateway. Potrebbe essere previsto che quell'host sia inaccessibile a causa della topologia di rete o delle restrizioni del firewall.

### Linux prima dell'avvio

#### CWA-ICADOWNLOAD_ERR_00001

- Descrizione: impossibile connettersi allo store a causa della mancata risposta dell'app Citrix Workspace.
- Azione consigliata: verificare se Citrix Workspace o StoreFront sono inattivi. Inoltre, verificare la connettività Internet.

**CWA-ICADOWNLOAD_ERR_00002**

- Descrizione: l'utente ha annullato l'avvio della sessione.
- Azione consigliata: riavviare la sessione dopo qualche tempo.

**CWA-ICADOWNLOAD_ERR_00003**

- Descrizione: impossibile connettersi allo store. Verificare che i certificati del server siano validi.
- Azione consigliata: verificare se i certificati del server sono installati e attivi.

**CWA-ICADOWNLOAD_ERR_00004**

- Descrizione: la risorsa da avviare non esiste, non è abilitata o non è visibile a un utente.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00005**

- Descrizione: non sono disponibili workstation per questa richiesta.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00006**

- Descrizione: il server non dispone della licenza necessaria per eseguire l'attività richiesta.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00007**

- Descrizione: il server ha rifiutato la connessione alla workstation.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00008**

- Descrizione: la workstation richiesta è in manutenzione e non è disponibile per l'uso.
- Azione consigliata: contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00009

- Descrizione: è stato raggiunto il limite massimo di sessioni.
- Azione consigliata: raggiunto il limite massimo di sessioni configurato da un amministratore. Riavviare la sessione.

#### CWA-ICADOWNLOAD_ERR_000010

- Descrizione: errore generale che non può essere ulteriormente specificato.
- Azione consigliata: contattare il supporto Citrix.

### Mac dopo l'avvio

#### Impossibile avviare il desktop

- Descrizione: impossibile avviare il desktop "Nome desktop". ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

#### Impossibile avviare il visualizzatore

- Descrizione: impossibile avviare il visualizzatore. ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

#### Impossibile avviare il desktop

- Descrizione: il desktop "Nome desktop"è in manutenzione pianificata. ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

#### Impossibile avviare l'applicazione

- Descrizione: "nome app"non è stata avviata.
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

#### Impossibile avviare l'applicazione

- Descrizione: "nome app"non è stata avviata. ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

**Impossibile avviare il desktop**

- Descrizione: impossibile avviare il desktop "Nome desktop".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

**Impossibile avviare il desktop**

- Descrizione: impossibile avviare il desktop "Nome desktop". ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

**Impossibile avviare il visualizzatore**

- Descrizione: il visualizzatore non è riuscito ad aprire "Nome applicazione". ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

**Impossibile avviare il visualizzatore**

- Descrizione: il visualizzatore non è riuscito ad aprire il desktop "Nome desktop". ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

**Impossibile avviare il desktop**

- Descrizione: il desktop "Nome desktop"è in manutenzione pianificata.
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

**Impossibile avviare il desktop**

- Descrizione: il desktop "Nome desktop"è in manutenzione pianificata. ID transazione - "ID transazione".
- Azione consigliata: contattare l'amministratore fornendo dettagli dell'errore.

**Impossibile connettersi al desktop**

- Descrizione: impossibile raggiungere il desktop "nome desktop". ID transazione - "ID transazione". Riprovare più tardi.
- Azione consigliata: se il problema persiste, contattare l'amministratore fornendo dettagli dell'errore.

## Mac prima dell'avvio

#### CWA-ICADOWNLOAD_ERR_00001

- Descrizione: il file ICA non è valido.
- Azione consigliata: contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00002

- Descrizione: la richiesta di avvio è scaduta.
- Azione consigliata: verificare la connessione a Internet o contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00003

- Descrizione: il server non ha risposto.
- Azione consigliata: contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00004

- Descrizione: la risorsa da avviare non esiste, non è abilitata o non è visibile all'utente.
- Azione consigliata: contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00005

- Descrizione: Il server non è raggiungibile.
- Azione consigliata: contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00006

- Descrizione: errore durante l'avvio del visualizzatore.
- Azione consigliata: contattare il supporto Citrix.

#### CWA-ICADOWNLOAD_ERR_00007

- Descrizione: impossibile avviare un evento Apple Open.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00008**

- Descrizione: il percorso del visualizzatore non è raggiungibile.
- Azione consigliata: contattare il supporto Citrix.

**CWA-ICADOWNLOAD_ERR_00009**

- Descrizione: l'utente ha annullato l'autenticazione.
- Azione consigliata: chiedere all'utente di riavviare la risorsa.

**CWA-ICADOWNLOAD_ERR_000010**

- Descrizione: l'utente ha annullato la finestra LSI.
- Azione consigliata: chiedere all'utente di riavviare la risorsa.

**CWA-ICADOWNLOAD_ERR_000011**

- Descrizione: la workstation richiesta è in manutenzione e non è disponibile per l'uso.
- Azione consigliata: chiedere all'utente di provare dopo che la manutenzione è stata completata e la workstation è disponibile per l'uso.

**CWA-ICADOWNLOAD_ERR_000012**

- Descrizione: le credenziali di accesso dell'utente devono essere modificate.
- Azione consigliata: chiedere all'utente di modificare le credenziali di accesso.

**CWA-ICADOWNLOAD_ERR_000013**

- Descrizione: la sessione che collega la risorsa non è più attiva.
- Azione consigliata: chiedere all'utente di riprovare o contattare il supporto tecnico Citrix per ulteriore assistenza.

**CWA-ICADOWNLOAD_ERR_000014**

- Descrizione: impossibile scaricare il file ICA.
- Azione consigliata: contattare il supporto Citrix.

## Windows dopo l'avvio

### SessionManager.Launch.EngineLoadFailed

- Descrizione: i componenti principali necessari per stabilire una connessione a un desktop remoto o a un'applicazione non sono stati caricati o inizializzati correttamente. Ulteriori dettagli potrebbero essere forniti nel messaggio di errore.
- Azione consigliata: l'app Citrix Workspace non funziona come previsto. Questo problema potrebbe essere causato da una DLL di canali virtuali di terze parti (non Citrix) o da un altro componente del sistema. Potrebbe essere necessario raccogliere e inviare tracce CDF per determinare la natura dell'errore.

### SessionManager.Launch.ConnectionFailed

- Descrizione: questo errore è un errore generico che indica che un tentativo di avvio è fallito. Altri errori inviati potrebbero indicarne la causa.
- Azione consigliata: cercare altri errori associati al tentativo di avvio.

### SessionManager.Launch.LogonFailed

- Descrizione: questo errore indica che è stata stabilita una connessione a un desktop remoto o a un'applicazione, ma la sessione si è disconnessa senza completare l'accesso a Windows (o altro sistema operativo).
- Azione consigliata: questo errore indica che l'accesso non è riuscito, che potrebbe includere il fatto che l'utente non è riuscito a immettere manualmente le credenziali. Scoprire la modalità con cui l'utente ha tentato di accedere al VDA remoto.

### SessionManager.Launch.Cancelled

- Descrizione: il tentativo di connessione del motore Citrix è stato annullato, molto probabilmente mediante un'azione dell'utente.
- Azione consigliata: questo errore indica il motivo per cui una connessione non è stata stabilita correttamente, ma probabilmente indica un comportamento corretto.

### SessionManager.LeaseResolution.Failed

- Descrizione: indica che un avvio offline (chiamato anche "leasing") non è riuscito. Questo errore è dovuto al fatto che un lease valido e richiesto per la risorsa non è stato trovato sul computer

client. Inoltre, il Gateway o il Cloud Connector hanno rifiutato la richiesta di avvio o questa non era valida per un qualche motivo.
- Azione consigliata: verificare che i lease siano stati sincronizzati con il computer client e siano ancora validi. L'utente può accedere a Citrix Workspace in modalità online per attivare la (ri)sincronizzazione dei lease. Cercare gli errori inviati dai componenti Gateway o Cloud Connector. Questi errori potrebbero indicare i motivi dell'errore.

#### SessionManager.clxmtp.SoftDeny

- Descrizione: è stato tentato l'avvio di un lease e un Connector o Gateway ha informato il client che non può completare l'avvio richiesto. Tuttavia, gli altri connettori o gateway potrebbero essere in grado di aiutare l'avvio.
- Azione consigliata: questo errore non indica che l'avvio non debba riuscire. Indica che il motore non può riuscire attraverso un percorso di rete specifico. Cercare errori inviati dai componenti Gateway o Cloud Connector. Questi errori potrebbero indicare i motivi dell'errore.

#### SessionManager.clxmtp.SoftDeny_Implicit

- Descrizione: è stato tentato l'avvio di un lease e un connettore o gateway non è raggiungibile. Tuttavia, altri connettori o gateway potrebbero essere in grado di aiutare l'avvio.
- Azione consigliata: questo errore non indica che l'avvio non debba riuscire. Indica che il motore non può riuscire attraverso un percorso di rete specifico. Indagare sul motivo per cui il client non può contattare un Connector o un gateway. Potrebbe essere previsto che quell'host sia inaccessibile a causa della topologia di rete o delle restrizioni del firewall.

#### Transport.Connect.NoCGP_Fail

- Descrizione: i componenti core (motore) dell'app Citrix Workspace non sono riusciti a connettersi a un host VDA tramite il protocollo ICA (porta 1494). Non sono stati compiuti tentativi di connessione a un gateway o un VDA tramite il protocollo CGP, se questo evento è stato inviato.
- Azione consigliata: indagare sul motivo per cui il client non è in grado di contattare un VDA tramite TCP o EDT.

#### Transport.Connect.FallbackFail

- Descrizione: i componenti core (motore) dell'app Citrix Workspace non sono riusciti a connettersi a un host VDA tramite il protocollo ICA (porta 1494). Dopo questo errore, l'app Citrix Workspace non riesce a connettersi a un gateway o a un VDA tramite il protocollo CGP (porta 2598).

- Azione consigliata: verificare perché il client non è in grado di contattare un gateway, un connettore o un VDA tramite TCP o EDT.

#### Transport.Connect.Fail

- Descrizione: i componenti core dell'app Citrix Workspace (motore) non sono riusciti a connettersi a un gateway o a un VDA tramite il protocollo CGP (porta 2598). Non sono stati compiuti tentativi di connessione a un VDA tramite il protocollo ICA se è stato emesso questo evento.
- Azione consigliata: verificare perché il client non è in grado di contattare un gateway, un connettore o un VDA tramite TCP o EDT.

### Windows prima dell'avvio

#### CWA-ICADOWNLOAD_ERR_00001

- Descrizione: impossibile connettersi allo store a causa della mancata risposta dell'app Citrix Workspace.
- Azione consigliata: verificare se Citrix Workspace o StoreFront sono inattivi. Inoltre, verificare la connettività Internet.

#### CWA-ICADOWNLOAD_ERR_00002

- Descrizione: l'utente ha annullato l'avvio della sessione.
- Azione consigliata: riavviare la sessione dopo qualche tempo.

#### CWA-ICADOWNLOAD_ERR_00003

- Descrizione: impossibile connettersi allo store. Verificare che i certificati del server siano validi.
- Azione consigliata: contattare l'amministratore IT fornendo dettagli dell'errore.

#### CWA-ICADOWNLOAD_ERR_00004

- Descrizione: la risorsa da avviare non esiste, non è abilitata o non è visibile a un utente.
- Azione consigliata: contattare l'amministratore IT fornendo dettagli dell'errore.

#### CWA-ICADOWNLOAD_ERR_00005

- Descrizione: non sono disponibili workstation per questa richiesta.
- Azione consigliata: contattare l'amministratore IT fornendo dettagli dell'errore.

#### CWA-ICADOWNLOAD_ERR_00006

- Descrizione: il server non dispone della licenza necessaria per eseguire l'attività richiesta.
- Azione consigliata: contattare l'amministratore IT fornendo dettagli dell'errore.

#### CWA-ICADOWNLOAD_ERR_00007

- Descrizione: il server ha rifiutato la connessione alla workstation.
- Azione consigliata: contattare l'amministratore IT fornendo dettagli dell'errore.

#### CWA-ICADOWNLOAD_ERR_00008

- Descrizione: la workstation richiesta è in manutenzione e non è disponibile per l'uso.
- Azione consigliata: contattare l'amministratore IT fornendo dettagli dell'errore.

#### CWA-ICADOWNLOAD_ERR_00009

- Descrizione: è stato raggiunto il limite massimo di sessioni.
- Azione consigliata: raggiunto il limite massimo di sessioni configurato da un amministratore. Riavviare la sessione.

#### CWA-ICADOWNLOAD_ERR_000010

- Descrizione: errore generale che non può essere ulteriormente specificato.
- Azione consigliata: contattare l'amministratore IT fornendo dettagli dell'errore.

### Workspace

#### StoreLaunchIcaEndpoint.LaunchFailed

- Descrizione: si è verificato un errore durante l'avvio.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

#### StoreLaunchSessionEndpoint.BadRequest

- Descrizione: i parametri della richiesta di avvio non sono validi o sono vuoti.
- Azione consigliata: contattare il supporto Citrix.

**StoreLaunchSessionEndpoint.FarmUnavailable**

- Descrizione: non c'erano farm disponibili per l'avvio.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops.

**StoreLaunchSessionEndpoint.Error**

- Descrizione: si è verificato un errore interno durante l'avvio.
- Azione consigliata: contattare il supporto Citrix.

**StoreGetIcaFileEndpoint.BadRequest**

- Descrizione: nella richiesta non è stato fornito alcun ticket di avvio.
- Azione consigliata: contattare il supporto Citrix.

**StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed**

- Descrizione: Workspace non è riuscito a recuperare il file ICA.
- Azione consigliata: contattare il supporto Citrix.

**StoreGetIcaFileEndpoint.Error**

- Descrizione: Workspace non è riuscito a recuperare il file ICA.
- Azione consigliata: contattare il supporto Citrix.

**WebProxyGetLaunchStatusEndPoint.DSAuthFailure**

- Descrizione: si è verificato un problema di autenticazione.
- Azione consigliata: provare a eseguire nuovamente l'autenticazione. Contattare il supporto Citrix.

**WebProxyGetLaunchStatusEndPoint.LaunchFailed**

- Descrizione: si è verificato un errore interno durante l'avvio dell'applicazione.
- Azione consigliata: contattare il supporto Citrix.

**WebProxyGetLaunchStatusEndPoint.ResourceNotFound**

- Descrizione: l'avvio non è riuscito perché l'applicazione non è stata trovata.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops e la configurazione dell'applicazione.

**WebProxyLaunchIcaEndpoint.DSAuthFailure**

- Descrizione: si è verificato un problema di autenticazione.
- Azione consigliata: provare a eseguire nuovamente l'autenticazione. Contattare il supporto Citrix.

**WebProxyLaunchIcaEndpoint.LaunchFailed**

- Descrizione: si è verificato un errore interno durante l'avvio dell'applicazione.
- Azione consigliata: contattare il supporto Citrix.

**WebProxyLaunchIcaEndpoint.ResourceNotFound**

- Descrizione: l'avvio non è riuscito perché l'applicazione non è stata trovata.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops e la configurazione dell'applicazione.

**WebProxySessionsLaunchIcaEndpoint.SessionNotFound**

- Descrizione: Workspace non è riuscito a riconnettersi alla sessione HDX esistente. La sessione potrebbe essere terminata.
- Azione consigliata: riavviare l'applicazione.

**WebProxySessionsLaunchIcaEndpoint.DSAuthFailure**

- Descrizione: si è verificato un problema di autenticazione.
- Azione consigliata: provare a eseguire nuovamente l'autenticazione. Contattare il supporto Citrix.

**WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed**

- Descrizione: Workspace non è riuscito a riconnettersi alla sessione HDX esistente. La sessione potrebbe essere terminata.
- Azione consigliata: contattare il supporto Citrix.

**WebProxySessionsLaunchIcaEndpoint.Error**

- Descrizione: si è verificato un errore interno durante la riconnessione alla sessione.
- Azione consigliata: contattare il supporto Citrix.

**WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure**

- Descrizione: si è verificato un problema di autenticazione.
- Azione consigliata: provare a eseguire nuovamente l'autenticazione. Contattare il supporto Citrix.

**WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed**

- Descrizione: Workspace non è riuscito a riconnettersi alla sessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**WebProxySessionsGetLaunchStatusEndpoint.Error**

- Descrizione: si è verificato un errore interno durante la riconnessione alla sessione.
- Azione consigliata: contattare il supporto Citrix.

**DetermineGateway.Error**

- Descrizione: Workspace non è riuscito a determinare a quale gateway connettersi.
- Azione consigliata: verificare la configurazione del gateway. Contattare il supporto Citrix.

**ConnectionRoutingProviderLaunch.Error**

- Descrizione: Workspace non è riuscito a determinare a quale gateway connettersi.
- Azione consigliata: verificare la configurazione del gateway. Contattare il supporto Citrix.

**BrokerGetAddressCall.AnonymousPrelaunchNotSupported**

- Descrizione: Workspace non può avviare l'applicazione perché la farm non supporta gli avvii anonimi.
- Azione consigliata: contattare il supporto Citrix.

**BrokerGetAddressCall.LeasingError**

- Descrizione: Workspace ha ricevuto un errore dal broker Citrix Virtual Apps and Desktops.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**BrokerGetAddressCall.ServiceConnectionError**

- Descrizione: Workspace non è riuscito a contattare alcun broker Citrix Virtual Apps and Desktops nella farm.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**BrokerGetAddressCall.BrokerError**

- Descrizione: Workspace ha ricevuto un errore da un broker Citrix Virtual Apps and Desktops.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**BrokerGetAddressCall.LicensingError**

- Descrizione: Workspace non è riuscito ad avviare l'applicazione a causa di un errore di licenza.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**BrokerGetAddressCall.Error**

- Descrizione: Workspace non è in grado di recuperare i dettagli VDA dal broker Citrix Virtual Apps and Desktops.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**GetLaunchReference.NoAccessToken**

- Descrizione: Workspace non riesce a connettersi correttamente al VDA.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**GetLaunchReference.BrokerError**

- Descrizione: Workspace non riesce a connettersi correttamente al VDA.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**GetLaunchReference.Error**

- Descrizione: Workspace non riesce a connettersi correttamente al VDA.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**GenerateIcaFile.InvalidIcaSetting**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**StoreIcaFileAndGetTicket.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetFasVdaLogonTicket.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GenerateSTATicket.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetVdaAddress.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetTicket.NoAccessToken**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetTicket.BrokerError**

- Descrizione: il broker Citrix Virtual Apps and Desktops non è riuscito ad avviare la sessione HDX.
- Azione consigliata: verificare l'ID specificato nel messaggio di errore e verificare i log di Citrix Virtual Apps and Desktops.

**GetTicket.ServiceConnectionError**

- Descrizione: Workspace non è in grado di contattare un broker Citrix Virtual Apps and Desktops.
- Azione consigliata: contattare il supporto Citrix.

**GetTicket.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetNetscalerConfigurationByCustomer.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**DiscoverMPSServerCapabilities.Error**

- Descrizione: si è verificato un problema durante la richiesta al broker Citrix Virtual Apps and Desktops.
- Azione consigliata: verificare i log di Citrix Virtual Apps and Desktops. Contattare il supporto Citrix.

**GetResourceLocationNetScalerConfig.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetCustomerResourceLocations.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetResourceLocationFromResourceProvider.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetNetScalerGatewayInfo.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetCustomerEntitlements.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

**GetResourceLocationForServerFeed.Error**

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

#### GetResourceInformation.Error

- Descrizione: si è verificato un errore interno mentre veniva stabilita una connessione HDX.
- Azione consigliata: contattare il supporto Citrix.

### Citrix Gateway come servizio

#### CGS-ICASN_ERR_00001

- Descrizione: avvio dell'applicazione non riuscito a causa di un errore di analisi della richiesta.
- Azione consigliata: contattare il supporto Citrix.

#### CGS-ICASN_ERR_00002

- Descrizione: impossibile convalidare il ticket di autenticazione.
- Azione consigliata: contattare il supporto Citrix.

#### CGS-ICASN_ERR_00003

- Descrizione: impossibile convalidare il ticket di autenticazione.
- Azione consigliata: contattare il supporto Citrix.

#### CGS-ICASN_ERR_00004

- Descrizione: impossibile convalidare il ticket di autenticazione.
- Azione consigliata: contattare il supporto Citrix.

#### CGS-ICASN_ERR_00005

- Descrizione: impossibile stabilire la connessione al connettore.
- Azione consigliata: verificare lo stato del connettore. Se il problema persiste, contattare il supporto Citrix.

#### CGS_ICASN_ERR_00006

- Descrizione: La richiesta di connessione al connettore è scaduta.
- Azione consigliata: verificare lo stato del connettore. Verificare se alcune impostazioni del proxy bloccano il traffico tra connettore/VDA e NGS. Verificare la connettività tra il VDA e il connettore. Se il problema persiste, contattare il supporto Citrix.

**CGS_ICASN_ERR_00007**

- Descrizione: l'app Citrix Workspace ha chiuso la connessione.
- Azione consigliata: verificare che la connettività di rete lato client sia stabile. Se il problema persiste, contattare il supporto Citrix.

**CGS_ICASN_ERR_00008**

- Descrizione: Il back-end ha chiuso la connessione.
- Azione consigliata: verificare lo stato del connettore. Verificare la stabilità della rete dal connettore/VDA alla rete pubblica (NGS). Se il problema persiste, contattare il supporto Citrix.

**CGS_ICASN_ERR_00009**

- Descrizione: errore mentre viene stabilito il collegamento VDA a NGS (Rendezvous).
- Azione consigliata: verificare lo stato del connettore. Il VDA deve essere in grado di raggiungere il servizio NGS. Verificare la connettività tra il VDA e il connettore. Se il problema persiste, contattare il supporto Citrix.

**CGS_ICASN_ERR_00010**

- Descrizione: fallback da EDT a TCP. Verificare i prerequisiti per l'EDT.
- Azione consigliata: Rendezvous deve essere abilitato e il VDA deve essere in grado di raggiungere il servizio NGS tramite UDP. Se il problema persiste, contattare il supporto Citrix.

**CGS_ICASN_ERR_00011**

- Descrizione: errore nel servizio interno di NGS.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00012**

- Descrizione: errore nel servizio interno di NGS.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00013**

- Descrizione: errore nella convalida GCT.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00014**

- Descrizione: errore nella convalida GCT.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00015**

- Descrizione: errore nel servizio interno di NGS.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00016**

- Descrizione: errore nel servizio interno di NGS.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00017**

- Descrizione: errore nel servizio interno di NGS.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00018**

- Descrizione: impossibile convalidare il ticket di autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00019**

- Descrizione: impossibile convalidare il ticket di autenticazione.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00020**

- Descrizione: errore nella licenza interna di CGS.
- Azione consigliata: contattare il supporto Citrix.

**CGS_ICASN_ERR_00021**

- Descrizione: fallback di Rendezvous v2 perché il flag di funzionalità è disabilitato.
- Azione consigliata: contattare il supporto Citrix.

#### CGS_ICASN_ERR_00022

- Descrizione: errore nel servizio interno di NGS.
- Azione consigliata: contattare il supporto Citrix.

#### CGS_ICASN_ERR_00023

- Descrizione: timeout nello scambio CLXMTP.
- Azione consigliata: verificare che i connettori siano integri e raggiungibili dal servizio NGS. Se il problema persiste, contattare il supporto Citrix.

#### CGS_ICASN_ERR_00024

- Descrizione: errore della convalida VSR CLXMTP.
- Azione consigliata: contattare il supporto Citrix.

#### CGS_ICASN_ERR_00025

- Descrizione: errore della convalida VSR CLXMTP.
- Azione consigliata: contattare il supporto Citrix.

#### CGS_ICASN_ERR_00026

- Descrizione: il connettore non è disponibile in CLXMTP.
- Azione consigliata: verificare se il connettore è in stato integro per la posizione della risorsa. Se il problema persiste, contattare il supporto Citrix.

#### CGS_ICASN_ERR_00027

- Descrizione: reindirizzamento CLXMTP al connettore non riuscito dopo il numero massimo di prove.
- Azione consigliata: verificare se il connettore è in stato integro per la posizione della risorsa. Verificare che il servizio `Citrix ClxMtp Service` sia in esecuzione su tutti i connettori. Contattare il supporto Citrix.

#### CGS_ICASN_ERR_00028

- Descrizione: impossibile comunicare con il Controller.
- Azione consigliata: contattare il supporto Citrix.

#### Success: CGS_ICASN_SUCCESS_00001

- Descrizione: richiesta di avvio della sessione ricevuta.
- Azione consigliata: non applicabile

#### Success: CGS_ICASN_SUCCESS_00002

- Descrizione: richiesta di avvio della sessione completata.
- Azione consigliata: non applicabile

### Proxy XAXD

#### XDPXY_INF_00001

- Descrizione: il broker invia una richiesta al VDA per prepararsi alle connessioni in entrata.
- Azione consigliata: non applicabile

#### XDPXY_INF_00002

- Descrizione: il VDA conferma la richiesta di connessione da parte del Broker.
- Azione consigliata: non applicabile

#### XDPXY_ERR_00001

- Descrizione: impossibile comunicare con il VDA.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_ERR_00002

- Descrizione: timeout di XaxdProxy durante l'attesa di una risposta dal VDA.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.

  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_ERR_00003

- Descrizione: si è verificato un errore o un'eccezione WCF durante il tentativo di effettuare la richiesta.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_INF_00003

- Descrizione: la richiesta di convalida per la connessione ICA o RDP in entrata viene richiamata dallo stack.
- Azione consigliata: non applicabile

#### XDPXY_INF_00004

- Descrizione: viene stabilita la convalida della connessione ICA o RDP in ingresso.
- Azione consigliata: non applicabile

#### XDPXY_ERR_00001

- Descrizione: impossibile comunicare con il proxy VDA.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_ERR_00002

- Descrizione: timeout di XaxdProxy durante l'attesa di una risposta dal Proxy VDA.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_ERR_00003

- Descrizione: si è verificata un'eccezione durante il tentativo di effettuare la richiesta.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Riavviare il servizio Citrix Delivery Agent sul VDA o riavviare il VDA.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_INF_00005

- Descrizione: viene effettuata una richiesta di traffico di sessione HDX diretto a VDA.
- Azione consigliata: non applicabile

#### XDPXY_INF_00006

- Descrizione: il VDA stabilisce una connessione diretta con il piano di controllo di Citrix Cloud per il traffico di sessione HDX.
- Azione consigliata: non applicabile

#### XDPXY_INF_00007

- Descrizione: il client invia una richiesta di connessione a StoreFront locale per una risorsa.
- Azione consigliata: non applicabile

#### XDPXY_INF_00008

- Descrizione: StoreFront locale accetta la richiesta di connessione inviata dal client per la risorsa.
- Azione consigliata: non applicabile

#### XDPXY_ERR_00004

- Descrizione: XaxdProxy ha ricevuto una risposta di errore HTTP durante il tentativo di connessione.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Verificare la stabilità della rete dal connettore alla rete pubblica.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_ERR_00006

- Descrizione: la richiesta XML è in formato non valido.
- Azione consigliata: contattare il supporto Citrix

#### XDPXY_ERR_00007

- Descrizione: la richiesta XML ha intestazioni e/o formato delle credenziali non validi.
- Azione consigliata: scollegarsi, effettuare nuovamente l'accesso e riprovare. Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_INF_00011

- Descrizione: l'avvio della continuità del servizio è richiesto dall'utente tramite WSA.
- Azione consigliata: non applicabile

#### XDPXY_INF_00012

- Descrizione: l'avvio della continuità del servizio è richiesto dall'utente tramite WSA.
- Azione consigliata: non applicabile

#### XDPXY_ERR_00004

- Descrizione: XaxdProxy ha riportato un errore HTTP durante il tentativo di connessione.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_ERR_00008

- Descrizione: avvio della continuità del servizio non riuscito per timeout di XaxdProxy durante l'attesa di una risposta.
- Azione consigliata: controllare l'integrità del connettore. Per ulteriori informazioni, vedere Citrix Cloud Connector e CTX224133.
  - Se si dispone di un proxy Web tra Connector e Broker, assicurarsi che sia configurato correttamente.
  - Se il problema persiste, contattare il supporto Citrix.

#### XDPXY_ERR_00009

- Descrizione: avvio della continuità del servizio non riuscito a causa del blocco e/o della revoca del lease.
- Azione consigliata: contattare l'amministratore di Citrix Cloud fornendo dettagli dell'errore. Per ulteriori informazioni, vedere la documentazione di Continuità del servizio.
  - Se il problema persiste, contattare il supporto Citrix.

## Citrix DaaS per Citrix Service Provider

October 6, 2022

Questo articolo descrive come i **Citrix Service Provider (CSP)** possono configurare Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) per i clienti tenant in Citrix Cloud. Per una panoramica delle funzionalità disponibili per i partner Citrix, vedere Citrix Cloud for Partners.

## Requisiti

- Essere partner Citrix Service Provider.
- Avere un account Citrix Cloud.
- Disporre di una sottoscrizione a Citrix DaaS.

## Limitazioni e problemi noti

### Limitazioni

- Le modifiche al nome del tenant richiedono fino a 24 ore per essere applicate a tutte le interfacce.
- Quando si crea un tenant, l'indirizzo e-mail deve essere univoco.
- Il filtro in **Manage > Full Configuration** per ambito (simile a Monitor) non è disponibile. Per visualizzare le risorse associate a un ambito, selezionare **Administrators** nel riquadro di sinistra. Nella scheda **Scopes** (Ambiti), selezionare l'ambito, quindi selezionare **Edit Scope** (Modifica ambito) nel riquadro Action.

### Problemi noti

- Dopo l'assegnazione degli ambiti a una risorsa, non è possibile utilizzare la console di gestione per rimuoverli o annullarne l'assegnazione. Tali attività sono supportate solo tramite PowerShell.
- **Manage > Full Configuration** non applica gli ambiti. L'utente è responsabile della selezione dell'ambito appropriato durante la creazione di cataloghi di macchine, gruppi di consegna e gruppi di applicazioni.
- Quando vengono creati più di 15 ambiti (creati automaticamente e personalizzati), le informazioni di accesso personalizzate di Citrix Cloud per un amministratore (**Identity and Access Management > Administrators**) non vengono visualizzate correttamente. Soluzione alternativa: limitare gli ambiti a 15 o meno.

## Aggiungere un cliente

1. Accedere a Citrix Cloud con le credenziali del CSP. Selezionare **Customers** nel menu in alto a sinistra.
2. Dalla dashboard del cliente, selezionare **Invite or Add**. Fornire le informazioni richieste.
3. Se il cliente non dispone di un account Citrix Cloud, l'aggiunta del cliente crea un account cliente. L'aggiunta del cliente, inoltre, aggiunge automaticamente l'utente come amministratore ad accesso completo dell'account di quel cliente.

4. Se il cliente ha un account Citrix Cloud:
    a) Viene visualizzato un URL di Citrix Cloud, che si copia e si invia al cliente. Per informazioni dettagliate su questo processo, vedere Inviting a customer to connect.
    b) Il cliente deve aggiungere l'utente come amministratore ad accesso completo al proprio account. Vedere Add administrators to a Citrix Cloud account.

È possibile aggiungere altri amministratori in un secondo momento e controllare quali clienti possono vedere nelle console **Manage** e **Monitor**.

### Aggiungere Citrix DaaS a un cliente

1. Accedere a Citrix Cloud con le credenziali del CSP. Selezionare **Customers** nel menu in alto a sinistra.
2. Dalla dashboard del cliente, nel menu con i puntini di sospensione per il cliente, selezionare **Add Service**.
3. In **Select a service to add** (Seleziona servizio da aggiungere), selezionare **Virtual Apps and Desktops**.
4. Selezionare **Continue** (Continua).

Dopo aver completato questa procedura, il cliente viene aggiunto alla sottoscrizione Citrix DaaS.

Al termine dell'onboarding, viene creato automaticamente un nuovo ambito cliente in Citrix DaaS. L'ambito è visibile nella schermata **Manage > Full Configuration**. Questo ambito è unico per quel cliente. È possibile rinominare l'ambito, ma non è possibile eliminarlo.

Utilizzare questo ambito per personalizzare l'accesso per altri amministratori. Ad esempio, supponiamo che si disponga di 10 clienti e due amministratori. Utilizzando l'ambito univoco, è possibile limitare l'accesso di un amministratore a soli tre clienti. L'altro amministratore può accedere a uno di questi tre clienti, più altri due clienti. Per ulteriori informazioni, vedere Controllare l'accesso degli amministratori ai clienti.

### Impostare un'ubicazione per le risorse

Una posizione delle risorse contiene le macchine che distribuiscono app e desktop per i clienti e componenti dell'infrastruttura come Citrix Cloud Connectors. Per ulteriori informazioni, vedere Connect to Citrix Cloud.

### Configurare cataloghi e gruppi per distribuire app e desktop

Un catalogo è un gruppo di macchine virtuali identiche. Quando si crea un catalogo, viene utilizzata un'immagine (con altre impostazioni) come modello per la creazione delle macchine. Per ulteriori

informazioni, vedere Creare cataloghi di macchine.

Un gruppo di consegna è una raccolta di macchine selezionate da uno o più cataloghi di macchine. Nel gruppo di consegna è specificato quali utenti possono utilizzare tali macchine, oltre alle applicazioni e ai desktop disponibili per tali utenti. Per ulteriori informazioni, vedere Creare gruppi di consegna.

I gruppi di applicazioni consentono di gestire raccolte di applicazioni. È possibile creare gruppi di applicazioni per applicazioni condivise tra gruppi di consegna diversi o utilizzate da un sottoinsieme di utenti all'interno di gruppi di consegna. Per ulteriori informazioni, vedere Creare gruppi di applicazioni.

Durante la configurazione dei gruppi, accertarsi che:

- L'ambito del gruppo di consegna sia un sottoinsieme dell'ambito del catalogo macchine. Ad esempio, si supponga che l'ambito del catalogo sia A e B. L'ambito del gruppo di consegna può essere A o B oppure A e B.
- L'ambito del gruppo di applicazioni sia un sottoinsieme dell'ambito del gruppo di consegna. Si supponga, ad esempio, che i gruppi di consegna associati a un gruppo di applicazioni abbiano gli ambiti A e B. L'ambito del gruppo di applicazioni può essere A o B oppure A e B.

## Domini federati

I domini federati consentono agli utenti clienti di utilizzare le credenziali di un dominio collegato alla posizione della risorsa per accedere alla propria area di lavoro. Ciò consente di fornire aree di lavoro dedicate ai clienti a cui gli utenti clienti possono accedere utilizzando un URL dell'area di lavoro personalizzato (ad esempio, customer.cloud.com), mentre la posizione della risorsa è ancora sul proprio account Citrix Cloud. Insieme all'area di lavoro condivisa, è possibile fornire aree di lavoro dedicate a cui i clienti possono accedere utilizzando l'URL dell'area di lavoro CSP (ad esempio, csppartner.cloud.com).

Per consentire ai clienti di accedere alla loro area di lavoro dedicata, aggiungerli ai domini appropriati che si gestiscono. Dopo aver configurato l'area di lavoro tramite Workspace Configuration, gli utenti clienti possono accedere alla propria area di lavoro e accedere alle app e ai desktop resi disponibili.

### Aggiungere un cliente a un dominio

1. Accedere a Citrix Cloud con le credenziali del CSP. Selezionare **Customers** nel menu in alto a sinistra.
2. Dalla dashboard del cliente, selezionare **Identity and Access Management** (Gestione identità e accesso) nel menu in alto a sinistra.
3. Nella scheda **Domains**, selezionare **Manage Federated Domain** (Gestisci dominio federato) nel menu con i puntini di sospensione del dominio.

4. Nella scheda **Manage Federated Domain**, nella colonna **Available customers**, selezionare un cliente da aggiungere al dominio. Selezionare il segno più accanto al nome del cliente. Il cliente selezionato viene ora visualizzato nella colonna **Federated customers** (Clienti federati). Ripetere l'operazione per aggiungere altri clienti. Al termine, selezionare **Apply**.

#### Rimuovere un cliente da un dominio

Quando si rimuove un cliente da un dominio che si gestisce, gli utenti del cliente non possono più accedere alle loro aree di lavoro utilizzando le credenziali di quel dominio.

1. Dal menu Citrix Cloud, selezionare **Identity and Access Management**, quindi selezionare **Domains**.
2. Individuare il dominio che si desidera gestire e selezionare il pulsante con i puntini di sospensione. Selezionare **Manage Federated Domain**.
3. Dall'elenco dei clienti federati, individuare o cercare i clienti che si desidera rimuovere e selezionare il pulsante X. Selezionare **Remove all** per rimuovere dal dominio tutti i clienti dell'elenco. I clienti selezionati passano all'elenco dei clienti disponibili.
4. Selezionare **Apply**.
5. Esaminare i clienti selezionati e selezionare **Remove Customers**.

### Controllare l'accesso degli amministratori ai clienti

È possibile controllare l'accesso amministratore ai clienti utilizzando l'ambito unico creato quando è stato aggiunto Citrix DaaS al cliente. È possibile configurare l'accesso quando si aggiunge un amministratore oppure in seguito.

Per informazioni su come limitare l'accesso utilizzando ruoli e ambiti in Citrix DaaS, vedere Amministrazione delegata.

#### Aggiungere un amministratore con accesso limitato

1. Accedere a Citrix Cloud con le credenziali del CSP. Selezionare **Customers** nel menu in alto a sinistra.
2. Dalla dashboard del cliente, selezionare **Identity and Access Management** (Gestione identità e accesso) nel menu in alto a sinistra.
3. Nella scheda **Administrators**, selezionare **Add Administrators From** (Aggiungi amministratori da), quindi selezionare **Citrix Identity**.
4. Digitare l'indirizzo e-mail della persona che si sta aggiungendo come amministratore, quindi selezionare **Invite**.

5. Configurare le autorizzazioni di accesso appropriate per l'amministratore. Citrix consiglia di selezionare **Custom access** (Accesso personalizzato), a meno che non si desideri che l'amministratore abbia il controllo di gestione di Citrix Cloud e di tutti i servizi sottoscritti.
6. Dopo aver selezionato **Custom access** (Accesso personalizzato), selezionare una o più coppie di ruoli e ambiti per Citrix DaaS, in base alle esigenze. Assicurarsi di abilitare solo le voci che contengono l'ambito univoco creato per il cliente.
7. Quando si è finito di selezionare coppie di ruoli e ambiti, selezionare **Send Invite** (Invia invito).

Quando l'amministratore accetta l'invito, ha l'accesso che gli è stato assegnato.

#### Modificare le autorizzazioni di amministrazione delegata per gli amministratori

1. Accedere a Citrix Cloud con le credenziali del CSP. Selezionare **Customers** nel menu in alto a sinistra.
2. Dalla dashboard del cliente, selezionare **Identity and Access Management** (Gestione identità e accessi) nel menu in alto a sinistra.
3. Nella scheda **Administrators**, selezionare **Edit Access** (Modifica accesso) dal menu con i puntini di sospensione dell'amministratore.
4. Selezionare ed eliminare le coppie di ruoli e ambiti per Citrix DaaS secondo necessità. Assicurarsi di abilitare solo le voci che contengono l'ambito univoco creato per il cliente.
5. Selezionare **Save** (Salva).

#### Visualizzare gli amministratori dei clienti e i corrispondenti ruoli e ambiti assegnati

1. Accedere a Citrix Cloud con le credenziali del CSP. Selezionare **Customers** nel menu in alto a sinistra.
2. Dal Customer Dashboard, selezionare **I miei servizi > DaaS** nel menu in alto a sinistra.
3. In Citrix DaaS, selezionare **Manage > Full Configuration** (Gestisci > Configurazione completa).
4. Selezionare **Administrators** nel riquadro di sinistra.

Le informazioni sono disponibili in tre schede:

- La scheda **Administrators** elenca gli amministratori che sono stati creati, insieme ai loro ruoli e ambiti.
- La scheda **Roles** elenca tutti i ruoli. Per visualizzare i dettagli del ruolo, selezionare il ruolo nel riquadro centrale. Nella parte inferiore di quel riquadro sono elencati i tipi di oggetto e le autorizzazioni associate al ruolo. Selezionare la scheda **Administrators** nel riquadro inferiore per visualizzare un elenco degli amministratori che attualmente dispongono di questo ruolo.
- La scheda **Scopes** (Ambiti) elenca tutti gli ambiti, compresi quelli generati per i clienti dei partner Citrix.

### Configurare le aree di lavoro

Il cliente dispone di una propria area di lavoro con un URL `customer.cloud.com` univoco. Questa area di lavoro è dove gli utenti del cliente accedono alle app e ai desktop pubblicati.

L'URL dell'area di lavoro viene visualizzato in due punti:

- Dalla dashboard Customer, selezionare **Workspace Configuration** dal menu nel menu in alto a sinistra.
- Dalla pagina di **benvenuto** di Citrix DaaS (scheda **Overview** [Panoramica]), l'URL dell'area di lavoro viene visualizzato nella parte inferiore della pagina.

È possibile modificare l'accesso e l'autenticazione in un'area di lavoro. È inoltre possibile personalizzare l'aspetto e le preferenze dell'area di lavoro. Per maggiori informazioni, vedere i seguenti articoli:

- Configurare le aree di lavoro
- Rendere sicure le aree di lavoro

### Monitorare il servizio di un cliente

Il dashboard **Monitor** in un ambiente CSP è essenzialmente lo stesso di un ambiente non CSP. Per ulteriori informazioni, vedere Monitor.

Per impostazione predefinita, il dashboard **Monitor** visualizza informazioni su tutti i clienti. Per visualizzare informazioni su un cliente, utilizzare **Select Customer**.

Tenere presente che la possibilità di visualizzare i monitor per un cliente è controllata dall'accesso configurato dall'amministratore. L'accesso deve includere una coppia di ruoli e ambiti che includa l'ambito univoco del cliente.

Se sono stati utilizzati ruoli incorporati per configurare l'accesso: i ruoli incorporati controllano se l'amministratore può vedere le visualizzazioni **Manage** e **Monitor**. Se sono state selezionate solo coppie di ruolo e ambito cliente che non includono la visibilità della scheda **Monitor**, l'amministratore non vedrà la scheda **Monitor** per alcuno dei clienti selezionati. Ad esempio, se si concede a un amministratore l'accesso **Read Only Administrator,customerABC** (Amministratore di sola lettura, cliente ABC), tale amministratore non vedrà la scheda **Monitor** per il cliente ABC, perché gli amministratori di sola lettura non hanno accesso alle visualizzazioni Monitor.

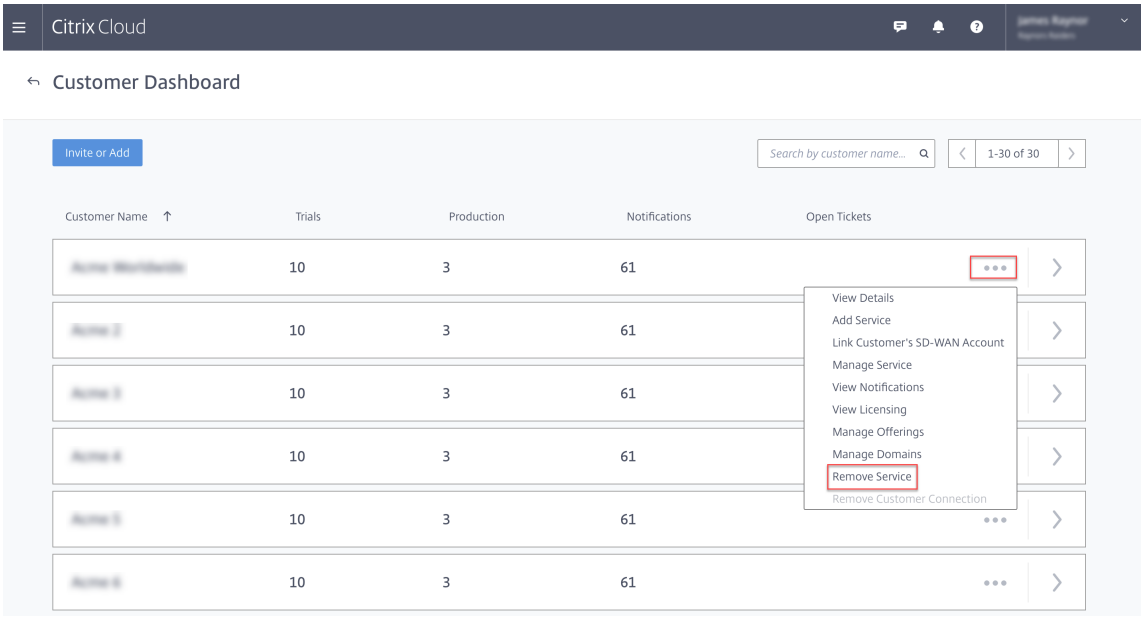
 

## Rimuovere un servizio

### Prerequisiti

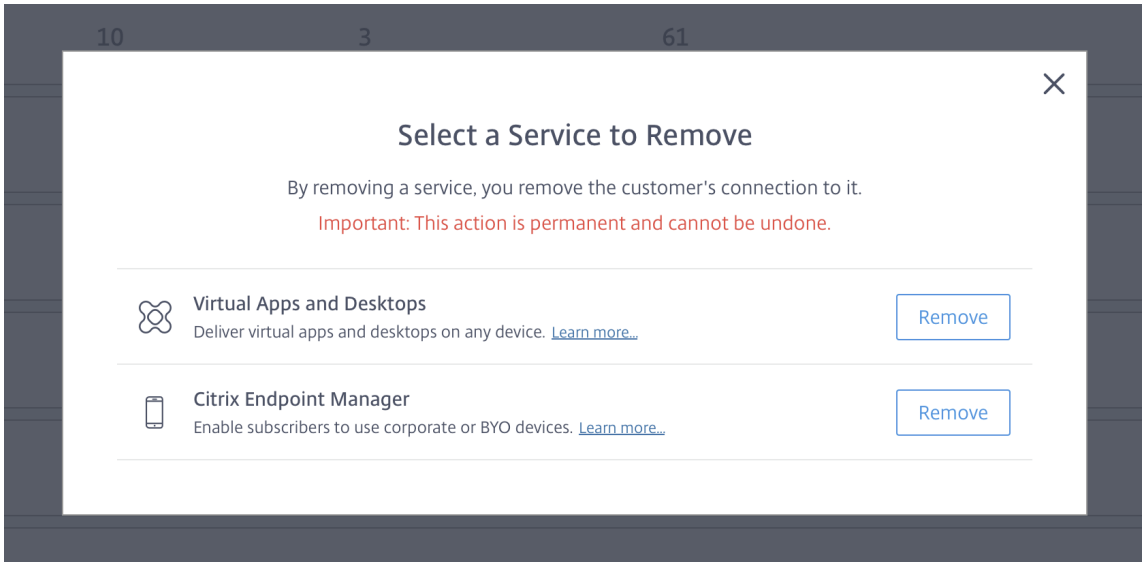
- Assicurarsi che l'ambito del cliente non sia collegato ad alcun oggetto Citrix DaaS. Se sono collegati, non è possibile rimuovere il servizio. Per scollegare gli ambiti, andare a **Citrix Studio > Administrators > Scopes** (Citrix Studio > Amministratori > Ambiti) e modificare l'ambito.
- Per conoscere l'ambito del cliente e gestirlo, vedere Creare e gestire l'ambito.

1. Accedere a Citrix Cloud con le credenziali Citrix Service Provider.
2. Nella **dashboard Customer** (Cliente), fare clic sul menu con i **puntini di sospensione** (...) del cliente da cui si desidera rimuovere un servizio e selezionare **Remove Service** (Rimuovi servizio).

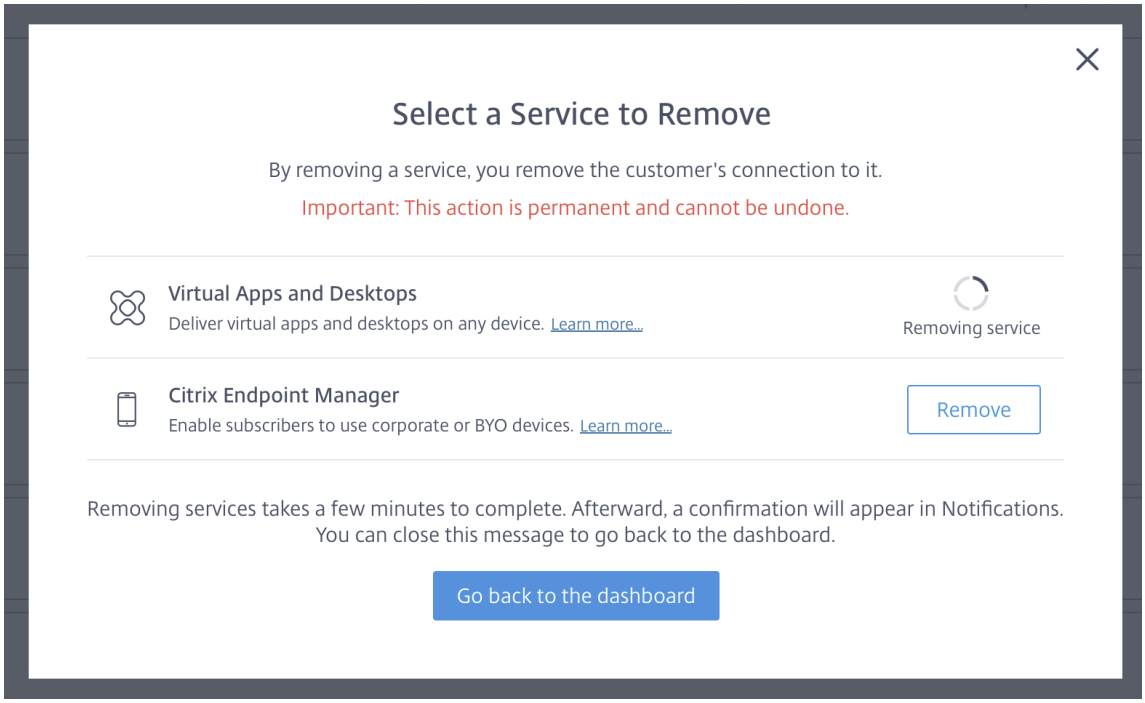



Viene visualizzata la pagina **Service to Remove** (Servizio da rimuovere).




3. Fare clic su **Remove** (Rimuovi) per rimuovere il servizio.




## Servizio Citrix Gateway

October 5, 2022

Citrix Gateway offre agli utenti un accesso sicuro alle applicazioni di Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops).

Il servizio Citrix Gateway consente l'accesso remoto sicuro a tali applicazioni, senza dover distribuire Citrix Gateway nella DMZ o riconfigurare il firewall. Il sovraccarico dell'infrastruttura dovuto all'utilizzo di Citrix Gateway passa a Citrix Cloud.

Per ulteriori informazioni sul servizio Citrix Gateway, vedere la documentazione del prodotto, che include argomenti come abilitare il servizio Citrix Gateway e i problemi noti per la versione in uso.

Citrix ADC è un controller di distribuzione delle applicazioni che analizza il traffico specifico dell'applicazione per distribuire, ottimizzare e proteggere il traffico di rete Layer 4-Layer 7 (L4-L7) in modo intelligente per le applicazioni Web. L'appliance virtuale Citrix ADC VPX può essere ospitata su varie piattaforme di virtualizzazione e cloud. Per ulteriori informazioni, vedere Deploy a Citrix ADC VPX instance.

## SDK e API

December 18, 2023

### SDK Remote PowerShell per Citrix DaaS

L'SDK Remote PowerShell automatizza le attività complesse e ripetitive. Fornisce il meccanismo per configurare e gestire l'ambiente Citrix DaaS (in precedenza chiamato servizio Citrix Virtual Apps and Desktops) senza utilizzare le interfacce utente **Manage** (Gestisci).

- I dettagli sui cmdlet sono forniti nell'SDK Citrix DaaS.
- I moduli supportati sono elencati in Support and limitations. In questa sezione vengono inoltre elencati i cmdlet disabilitati in questo SDK.
- L'SDK Remote PowerShell è disponibile per il download nel sito Web di Citrix.

Questo prodotto supporta le versioni di PowerShell dalla 3 alla 5.

#### In che modo questo SDK si differenzia dall'SDK per le distribuzioni gestite dal cliente

In una distribuzione Citrix Virtual Apps and Desktops installata e gestita dagli amministratori dei clienti, tali amministratori eseguono cmdlet e script in un sito contenente VDA e controller di distribuzione all'interno di una struttura di dominio comune. Al contrario, Citrix DaaS suddivide rispettivamente i VDA e i controller in una posizione risorsa e nel piano di controllo. Questa divisione significa che l'SDK PowerShell di Citrix Virtual Apps and Desktops originale non funziona in un ambiente Citrix DaaS. Non può attraversare il limite di sicurezza dalla posizione della risorsa al piano di controllo.

La soluzione è l'SDK Remote PowerShell Citrix DaaS. Quando viene eseguito nella posizione della risorsa, l'SDK Remote PowerShell accede al piano di controllo come se fosse locale. In questo modo fornisce le stesse funzionalità di un singolo sito Citrix Virtual Apps and Desktops. Esiste solo il livello di comunicazione non visibile più basso, migliorato per funzionare in un singolo sito locale o nell' ambiente cloud. I cmdlet sono gli stessi e la maggior parte degli script esistenti rimane invariata.

Il cmdlet `Get-XdAuthentication` fornisce l'autorizzazione ad attraversare la posizione sicura delle risorse per controllare il limite del piano. Per impostazione predefinita, `Get-XdAuthentication` chiede agli utenti le credenziali CAS e si deve eseguire una volta per sessione di PowerShell. In alternativa, l'utente può definire un profilo di autenticazione utilizzando un Secure Client di accesso API, creato nella console Citrix Cloud. In entrambi i casi, le informazioni di sicurezza persistono per l'utilizzo nelle successive chiamate di PowerShell SDK. Se questo cmdlet non viene eseguito in modo esplicito, viene invocato dal primo cmdlet di PowerShell SDK.

#### Prerequisiti

Per utilizzare l'SDK Remote PowerShell di Citrix DaaS, inserire nella whitelist i seguenti URL:

#### Commerciale

- `https://accounts.cloud.com`
- `https://[service].citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

#### Giappone

- `https://accounts.citrixcloud.jp`
- `https://[service].citrixworkspacesapi.jp/[customerid]`
- `https://[customerid].apps.citrixworkspacesapi.jp:443`

#### Governo

- `https://accounts.cloud.us`
- `https://[service].citrixworkspacesapi.us/[customerid]`
- `https://[customerid].xendesktop.us:443`

#### Installare e utilizzare l'SDK Remote PowerShell

Requisiti e considerazioni:

> **Nota:**
>
> Non installare l'SDK Remote PowerShell su un computer Citrix Cloud Connector. Può essere installato su qualsiasi computer collegato al dominio all'interno della stessa posizione delle risorse.
>
> Citrix non supporta l'esecuzione dei cmdlet di questo SDK sui Cloud Connector. Il funzionamento dell'SDK non coinvolge i connettori cloud.
>
> Se si dispone anche di una distribuzione Citrix Virtual Apps and Desktops (oltre alla distribuzione Citrix DaaS), non installare l'SDK Remote PowerShell su una macchina on-premise del Delivery Controller.

- Installare **Microsoft Edge WebView2**.
- Verificare che sulla macchina sia disponibile PowerShell 3.0, 4.0 o 5.0.
- Il programma di installazione SDK scarica e installa .NET Framework 4.8 (o una versione successiva supportata) se non è già installato.
- Se sulla macchina è già installato l'SDK Citrix Virtual Apps and Desktops, rimuovere tale SDK (da Programmi e funzionalità di Windows) prima di installare l'SDK Remote PowerShell.
- Per un ambiente automatizzato, utilizzare il parametro `-quiet` per installare l'SDK senza l'input dell'utente.

Per installare l'SDK Remote PowerShell:

1. Dalla pagina di download scaricare l'SDK Remote PowerShell per Virtual Apps and Desktops.
2. Installare ed eseguire l'SDK.

Vengono creati registri di installazione in `%TEMP%\CitrixLogs\CitrixPoshSdk`. I registri possono aiutare a risolvere i problemi di installazione.

Eseguire l'SDK su un computer collegato a un dominio all'interno della posizione di quella risorsa:

- Aprire un prompt dei comandi di PowerShell. Non è necessario eseguirlo come amministratore.
- Se si desidera utilizzare lo snap-in (anziché il modulo), aggiungere lo snap-in utilizzando il cmdlet `Add-PSSnapin` (o `asnp`).
- È possibile eseguire l'autenticazione esplicita utilizzando il cmdlet `Get-XdAuthentication`. In alternativa, eseguire il primo comando dell'SDK Remote PowerShell, che richiede la stessa autenticazione di `Get-XdAuthentication`. Se si utilizza un proxy, è necessario autenticarsi nel proxy per poter utilizzare il cmdlet `Get-XdAuthentication`. Per ulteriori informazioni, vedere Utilizzare Remote PowerShell SDK con unproxy.
- Per ignorare il prompt di autenticazione, è possibile utilizzare il cmdlet `Set-XdCredentials` per creare un profilo di autenticazione predefinito, utilizzando un Secure Client creato nella console di Citrix Cloud.
- Continuare a eseguire i cmdlet di PowerShell SDK o gli script di automazione di PowerShell SDK. Vedere un esempio.

Per disinstallare l'SDK Remote PowerShell, dalla funzionalità Windows per la rimozione o la modifica dei programmi selezionare **Citrix Virtual Apps and Desktops Remote PowerShell SDK** (SDK Remote PowerShell Citrix Virtual Apps and Desktops). Fare clic con il pulsante destro del mouse e selezionare **Uninstall**. Seguire le istruzioni della finestra di dialogo.

**Utilizzare Remote PowerShell SDK con unproxy** Se si utilizza un proxy, potrebbe non essere possibile utilizzare il cmdlet `Get-xdAuthentication` perché il proxy blocca le richieste HTTP effettuate dal cmdlet.

Esistono due modi per autenticarsi sul proxy. È possibile utilizzare il parametro `ProxyUseDefault` o i parametri `ProxyPassword` e `ProxyUsername`:

- Il parametro `ProxyUseDefault` abilita l'autenticazione al proxy utilizzando le credenziali proxy predefinite. Ad esempio:

```
Get-XdAuthentication -ProxyUseDefault
<!--NeedCopy-->
```

- I parametri `ProxyUsername` e `ProxyPassword` abilitano l'autenticazione al proxy all'interno della sessione di PowerShell. Ad esempio:

```
$secureString = ConvertTo-SecureString -String "password" -
    AsPlainText -Force

Get-XdAuthentication -ProxyUsername user1 -ProxyPassword
    $secureString
<!--NeedCopy-->
```

### Attività di esempio

Fra le attività comuni è inclusa l'impostazione di cataloghi di macchine, applicazioni e utenti. Di seguito è riportato uno script di esempio.

```
    $users = "xd.local\Domain Users"

    $TSVDACatalogName = "TSVDA"

    $TSVDADGName = "TSVDA"

    $TSVDAMachineName = "xd\ds-tsvda2"

    #Create TSVDA Catalog

    $brokerUsers = New-BrokerUser -Name $users

    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
        AllocationType "Random" -Description $TSVDACatalogName -
```

```
        PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
        SessionSupport "MultiSession" -MachinesArePhysical $true
14
15      #Add TSVDA Machine to Catalog
16
17      $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
            -CatalogUid $catalog.uid
18
19      #Create new desktops & applications delivery group
20
21      $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
            $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession
            " -DeliveryType DesktopsAndApps -Description $TSVDADGName
22
23      #Create notepad application
24
25      New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
            Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
26
27      #Assign users to desktops and applications
28
29      New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
            $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31      New-BrokerAccessPolicyRule -Name $TSVDADGName -
            IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
            DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33      New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
            DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
            $TSVDADGName
34
35      #Add machine to delivery group
36
37      Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
38  <!--NeedCopy-->
```

### Supporto e limitazioni

I seguenti sistemi operativi sono supportati dall'SDK Remote PowerShell:

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

In questa versione sono supportati i seguenti moduli Citrix Virtual Apps and Desktops PowerShell:

- Broker
- Identità di Active Directory (AD)
- Creazione di macchine
- Configurazione
- Registrazione della configurazione
- Host
- Amministrazione delegata
- Analisi

Per informazioni dettagliate sui cmdlet, vedere Citrix Virtual Apps and Desktops SDK.

Dopo l'autenticazione, l'accesso remoto rimane valido nella sessione di PowerShell corrente per 24 ore. Una volta trascorse, è necessario inserire le credenziali.

L'SDK Remote PowerShell deve essere eseguito su un computer all'interno della posizione della risorsa.

I seguenti cmdlet sono disabilitati nelle operazioni remote per mantenere l'integrità e la sicurezza del piano di controllo Citrix Cloud.

**Citrix.ADIdentity.Admin.V2:**

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

**Citrix.Analytics.Admin.V1:**

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership

- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

**Citrix.DelegatedAdmin.Admin.V1:**

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

**Citrix.Broker.Admin.V2:**

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection

- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

**Citrix.Configuration.Admin.V2:**

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

**Citrix.Host.Admin.V2:**

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript

- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

**Citrix.ConfigurationLogging.Admin.V1:**

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

**Citrix.MachineCreation.Admin.V2:**

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

**Citrix.EnvTest.Admin.V1:**

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript

- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

**Citrix.Monitor.Admin.V1:**

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

**Citrix.Storefront.Admin.V1:**

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

### Modulo di rilevamento Citrix DaaS per pacchetti e server App-V

Citrix DaaS è in grado di fornire le applicazioni contenute nei pacchetti App-V agli endpoint utilizzando uno dei seguenti metodi:

- Metodo di gestione single admin (accesso ai pacchetti da una condivisione di rete)
- Metodo di gestione dual admin (accesso ai pacchetti da un server di gestione Microsoft App-V)

Il processo di registrazione dei pacchetti App-V, della gestione di Microsoft App-V e dei server di pubblicazione con la libreria applicazioni mediante Citrix DaaS differisce leggermente dalla registrazione

dei pacchetti utilizzando una distribuzione on-premise. Tuttavia, il processo di assegnazione delle applicazioni agli utenti e del loro avvio sull'endpoint di un utente è identico.

La console di gestione di Citrix DaaS in Citrix Cloud non è in grado di visualizzare i file in una posizione risorsa. Inoltre, non è in grado di rilevare direttamente i pacchetti App-V o i server Microsoft App-V presenti nell'infrastruttura. Il modulo di rilevamento fornisce funzioni che rilevano le informazioni sui pacchetti App-V nell'infrastruttura on-premise e caricano le informazioni sul pacchetto in Citrix DaaS. Le informazioni sui pacchetti includono i pacchetti App-V, i server Microsoft App-V e le app contenute nei pacchetti.

Il modulo di individuazione utilizza l'SDK Remote PowerShell per Virtual Apps and Desktops. È in grado di rilevare le informazioni sui pacchetti da una condivisione di rete o da un server di gestione Microsoft App-V. È possibile utilizzare il modulo di rilevamento su una macchina nella posizione delle risorse.

Prerequisiti per l'utilizzo del modulo di rilevamento:

- Verificare che PowerShell 3.0 o versione successiva sia disponibile sul computer.
- Verificare che l'SDK Remote PowerShell di Citrix Virtual Apps and Desktops sia installato sul computer.
- Verificare di avere accesso alla condivisione di rete contenente i pacchetti App-V.
- Verificare di avere accesso al server in cui sono installati i Citrix Cloud Connector e su cui è ospitato il server di gestione Microsoft App-V.

#### Aggiungere pacchetti App-V alla libreria delle applicazioni in Citrix Cloud

La procedura seguente è valida per aggiungere pacchetti App-V da condivisioni di rete (gestione single admin) e aggiungere tutti i pacchetti App-V pubblicati da Microsoft App-V Management Server (gestione dual admin). Con il metodo di gestione dual admin, è necessario gestire i pacchetti App-V aggiunti proprio come si fa quando si utilizza il metodo di gestione single admin.

1. Scaricare il modulo di individuazione dalla pagina dei download di Citrix DaaS https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html. Estrarre il file zip `Citrix.Cloud.AppLibrary.Admin.v1.psm1` in una cartella a portata di mano.

   > **Nota:**
   >
   > Questo file è disponibile anche nell'ISO di Citrix Virtual Apps and Desktops contenuto in `Support\Tools\Scripts`. È possibile copiarlo localmente o inserire un collegamento diretto all'unità CD.

2. Verificare che l'SDK Remote PowerShell di Virtual Apps and Desktops sia installato sul computer.

3. Passare alla cartella contenente il modulo di individuazione. Nella finestra di PowerShell digitare il percorso completo della cartella contenente il modulo di individuazione e quindi premere **Invio**.
4. Importare il modulo di rilevamento con il comando `Import-Module .\Citrix.Cloud.AppLibrary.Admin.v1.psm1`.
5. Aggiungere i pacchetti App-V alla libreria applicazioni in Citrix Cloud utilizzando uno dei seguenti metodi.

   - Per aggiungere pacchetti App-V da una condivisione di rete, eseguire il cmdlet PowerShell: `Import-AppVPackageToCloud`.

     Ad esempio: `Import-AppVPackageToCloud –PackagePath \\AppVSrv\share\Notepad++.appv`

     Per la guida dei cmdlet, digitare `Get-Help Import-AppVPackageToCloud`.

   - Per aggiungere pacchetti App-V da un server di gestione Microsoft App-V, eseguire il cmdlet PowerShell: `Import-AppVPackagesFromManagementServerToCloud`

     Ad esempio: `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

     Per la guida del cmdlet, digitare `Get-Help Import-AppVPackagesFromManagementServerT`

     Questo comando importa tutti i pacchetti App-V pubblicati dal server di gestione Microsoft App-V a Citrix Cloud.

     Dopo aver aggiunto i pacchetti App-V a Citrix Cloud, è necessario gestirli come si fa utilizzando il metodo di gestione single admin.

6. Accedere a Citrix Cloud. Selezionare il cliente di destinazione. Una volta eseguito correttamente lo script, i pacchetti App-V vengono aggiunti alla libreria delle applicazioni in Citrix Cloud.

#### Funzioni PowerShell di alto livello

Il modulo contiene le seguenti funzioni di alto livello che è possibile richiamare dal proprio script PowerShell:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Rileva e carica su Citrix DaaS tutte le informazioni necessarie per pubblicare le applicazioni da un singolo pacchetto App-V.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  Individua i percorsi UNC dei pacchetti pubblicati dal server di gestione e richiama **Import-AppVPackageToCloud** per ciascuno di essi a turno.

  I pacchetti rilevati in questo modo vengono caricati in Citrix DaaS utilizzando il metodo di gestione a singolo amministratore. Citrix DaaS non è in grado di fornire pacchetti utilizzando il metodo di gestione a doppio amministratore.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Rileva il server di gestione e pubblicazione di Microsoft App-V e ne importa il contenuto nella libreria applicazioni. Questo cmdlet importa tutti i pacchetti gestiti utilizzando il server di gestione Microsoft App-V e le informazioni correlate. È possibile aggiungere e rimuovere server tramite PowerShell.

  Questo cmdlet aggiunge pacchetti App-V in modalità dual admin. Vengono importati solo i pacchetti App-V pubblicati sul server di gestione Microsoft App-V a cui sono stati aggiunti gruppi AD. Se si apportano modifiche al server di gestione Microsoft App-V, eseguire nuovamente questo cmdlet per sincronizzare la libreria applicazioni con il server di gestione Microsoft App-V.

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Rimuove i server di gestione e pubblicazione di Microsoft App-V aggiunti alla libreria applicazioni.

  Questo cmdlet rimuove i server di gestione e pubblicazione Microsoft App-V specificati, oltre a tutti i pacchetti App-V associati.

Eseguire il modulo di rilevamento per i pacchetti e i server App-V su un computer collegato al dominio all'interno della posizione di quella risorsa. Seguire i consigli contenuti in Installare e utilizzare l'SDK Remote PowerShell per iniziare. Continuare a eseguire cmdlet o script PowerShell. Vedere gli esempi seguenti.

#### Attività di esempio

Importare il modulo di rilevamento dei pacchetti App-V di Citrix DaaS.

```
1 import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.
     v1.psm1"
2 <!--NeedCopy-->
```

Passare attraverso la directory dell'archivio dei pacchetti App-V e caricare ciascun pacchetto.

```
Get-ChildItem -Path "\FileServer.domain.net\App-V Packages" -Filter *.appv |
Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName
 }

<!--NeedCopy-->
```

Scoprire e caricare i pacchetti registrati con un server di gestione Microsoft App-V.

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVManagementServer.domain.net
<!--NeedCopy-->
```

Rilevare il server di gestione e pubblicazione di Microsoft App-V e aggiungere la configurazione alla libreria applicazioni. In questo modo vengono importati anche tutti i pacchetti gestiti dal server di gestione di Microsoft App-V in modalità dual admin.

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer.domain.net  – PublishingServerUrl http://AppVManagementServer.domain.net:8001
<!--NeedCopy-->
```

Leggere la documentazione della guida di PowerShell inclusa nel modulo.

```
Get-Help Import-AppVPackageToCloud
<!--NeedCopy-->
```

#### Limiti

- Non è possibile rilevare i pacchetti App-V sull'infrastruttura della posizione risorsa direttamente dalla console di gestione Citrix DaaS in Citrix Cloud. Per ulteriori informazioni su Citrix Cloud, vedere la documentazione di Citrix Cloud.
- La console di gestione Citrix DaaS in Citrix Cloud non dispone di una connessione live al server di gestione Microsoft App-V. Le modifiche apportate ai pacchetti e ad altre configurazioni nel server di gestione di Microsoft App-V non vengono riportate nella console di gestione di Citrix DaaS fino a quando non viene rieseguito `Import-AppVDualAdminCloud`.

### API Monitor Service OData

Oltre a utilizzare le funzioni di Monitor per visualizzare i dati storici, è possibile eseguire query sui dati utilizzando l'API del servizio di monitoraggio. Utilizzare l'API per:

- Analizzare le tendenze storiche per la pianificazione
- Eseguire una risoluzione dettagliata dei problemi di connessione e guasti della macchina
- Estrarre informazioni da inserire in altri strumenti e processi; ad esempio, utilizzando le tabelle PowerPivot di Microsoft Excel per visualizzare i dati in modi diversi
- Creare un'interfaccia utente personalizzata oltre ai dati forniti dall'API

Per ulteriori informazioni, vedere API Monitor Service OData. Per accedere all'API Monitor Service, vedere Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

### API Citrix DaaS

Le API Citrix DaaS sono disponibili all'indirizzo https://developer.cloud.com/citrixworkspace/citrix-daas.

### Dichiarazione di non responsabilità

Questo software/codice di esempio viene fornito "COSÌ COM'È"senza dichiarazioni, garanzie o condizioni di alcun tipo. È possibile utilizzarlo, modificarlo e distribuirlo a proprio rischio. CITRIX NON RICONOSCE ALCUNA GARANZIA ESPRESSA, IMPLICITA, SCRITTA, ORALE O DI LEGGE, INCLUSE, A TITOLO ESEMPLIFICATIVO, LE GARANZIE DI COMMERCIABILITÀ, ADEGUATEZZA PER UNO SCOPO SPECIFICO E NON VIOLAZIONE DEI DIRITTI DI TERZI. Senza che ciò comporti una limitazione a quanto sopra, l'utente riconosce e accetta che (a) il software/codice di esempio potrebbe presentare errori, difetti di progettazione o altri problemi, con conseguente perdita di dati o danni alla proprietà; (b) potrebbe non essere possibile rendere il software/codice di esempio completamente funzionante; e (c) Citrix può, senza preavviso o responsabilità nei confronti dell'utente, cessare di rendere disponibile la versione corrente e/o qualsiasi versione futura del software/codice di esempio. In nessun caso il software/codice deve essere utilizzato per supportare attività estremamente pericolose, incluse, a titolo esemplificativo ma non esaustivo, attività di supporto vitale o di sabbiatura. NÉ CITRIX NÉ NESSUNA DELLE SUE CONSOCIATE O DEI SUOI AGENTI SARÀ RESPONSABILE IN RECLAMI RELATIVI A INADEMPIMENTO CONTRATTUALE O E PER QUANTO LEGALMENTE IMPUTABILE, DI ALCUN TIPO DI DANNI DERIVANTI DALLA SUA DECISIONE DI UTILIZZARE IL SOFTWARE/CODICE DI ESEMPIO, INCLUSI, A TITOLO ESEMPLIFICATIVO, I DANNI DIRETTI, SPECIALI, ACCIDENTALI, MORALI, CONSEQUENZIALI O DI ALTRO TIPO, ANCHE NEL CASO IN CUI LA POSSIBILITÀ DEL VERIFICARSI DI TALI DANNI FOSSE STATA COMUNICATA. L'utente accetta di indennizzare e difendere Citrix da qualsiasi reclamo derivante dall'uso, dalla modifica o dalla distribuzione del codice.