



Citrix DaaS per Azure

Machine translated content

Disclaimer

La versione ufficiale di questo contenuto è in inglese. Per alcuni dei contenuti della documentazione Cloud Software Group è stata impiegata la traduzione automatica solo per comodità. Cloud Software Group non ha alcun controllo sui contenuti tradotti in modo automatico, che possono contenere errori, imprecisioni o linguaggio inadatto. Non viene offerta alcuna garanzia di alcun tipo, espressa o implicita, circa l'accuratezza, l'affidabilità, l'idoneità o la correttezza di qualsiasi traduzione dall'originale inglese in qualsiasi altra lingua, o che il prodotto o servizio Cloud Software Group sia conforme a qualsiasi contenuto in traduzione automatica, e qualsiasi garanzia fornita ai sensi del contratto di licenza per l'utente finale applicabile o i termini di servizio, o qualsiasi altro accordo con Cloud Software Group che il prodotto o il servizio sia conforme a qualsiasi documentazione non si applicheranno nella misura in cui tale documentazione sia in traduzione automatica. Cloud Software Group non sarà ritenuta responsabile per eventuali danni o problemi che potrebbero derivare dall'utilizzo di contenuti per cui si è impiegata la traduzione automatica.

Contents

Citrix DaaS Standard per Azure	2
Novità	15
Panoramica tecnica sulla sicurezza	20
Abbonati a Citrix DaaS per Azure	33
Per iniziare	42
Create catalogs (Crea cataloghi)	46
Accesso remoto al PC	58
Sottoscrizioni di Azure	68
Connessioni di rete	74
Immagini	100
Utenti e autenticazione	111
Gestisci cataloghi	118
Monitoraggio	134
Citrix DaaS per Azure per i provider di servizi Citrix	141
Risoluzione dei problemi	147
Limiti	151
Riferimenti	153

Citrix DaaS Standard per Azure

October 7, 2022

Introduzione

Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure) è il modo più semplice e veloce per distribuire app e desktop Windows da Microsoft Azure. Citrix DaaS for Azure offre funzionalità di gestione, provisioning e gestione basate su cloud per la distribuzione di app e desktop virtuali su qualsiasi dispositivo.

Questa soluzione include:

- Gestione e provisioning basati su cloud per la distribuzione di desktop virtuali di Azure ospitati da Citrix e app da macchine multisesione.
- Un'esperienza utente ad alta definizione da un'ampia gamma di dispositivi, utilizzando l'app Citrix Workspace.
- Flussi di lavoro semplificati per la creazione e la gestione delle immagini, insieme alle immagini a sessione singola e multisesione per Windows e Linux preparate da Citrix che hanno installato l'ultimo Citrix Virtual Delivery Agent (VDA).
- Proteggi l'accesso remoto da qualsiasi dispositivo utilizzando i punti di presenza globali del servizio Citrix Gateway.
- Funzionalità avanzate di monitoraggio e gestione dell'help desk.
- Azure IaaS gestito, tra cui elaborazione, archiviazione e rete di Azure per la distribuzione di desktop virtuali.

La funzione Citrix Remote PC Access consente agli utenti di utilizzare in remoto le macchine fisiche esistenti situate in ufficio. Gli utenti ricevono la migliore esperienza utente utilizzando Citrix HDX per offrire la propria sessione PC da ufficio.

Se avete familiarità con altri prodotti Citrix DaaS, Citrix DaaS for Azure semplifica la distribuzione di app e desktop virtuali. Citrix è in grado di gestire l'infrastruttura per l'hosting di tali carichi di lavoro.

Citrix DaaS for Azure è un servizio Citrix Cloud. Citrix Cloud è la piattaforma che ospita e gestisce i servizi Citrix Cloud. [Scoprite di più su Citrix Cloud.](#)

Per informazioni su componenti, flusso di dati e considerazioni sulla sicurezza, vedere [Panoramica sulla sicurezza tecnica](#). In questo articolo vengono inoltre delineate le responsabilità dei clienti e di Citrix.

Come gli utenti accedono a desktop e app

Gli utenti (a volte chiamati abbonati) accedono ai loro desktop e alle loro app direttamente tramite il browser, utilizzando il client Citrix HTML5. Gli utenti visitano un URL di Citrix Workspace fornito dall'utente, il loro amministratore. La piattaforma Citrix Workspace enumera e fornisce le risorse digitali agli utenti. Gli utenti avviano un desktop o un'applicazione dal proprio spazio di lavoro.

Dopo aver configurato un catalogo di macchine che distribuiscono desktop e app (o un catalogo contenente macchine fisiche per l'accesso remoto ai PC), Citrix DaaS per Azure visualizza l'URL dell'area di lavoro. Notifichi quindi agli utenti di accedere a tale URL per avviare il desktop e le app.

In alternativa alla navigazione su Citrix Workspace per accedere ai desktop e alle app, gli utenti possono installare un'app Citrix Workspace sul proprio dispositivo. Scarica l'app giusta per il sistema operativo del dispositivo endpoint: <https://www.citrix.com/downloads/workspace-app/>.

Concetti e terminologia

Questa sezione introduce alcuni degli elementi e dei termini utilizzati dagli amministratori in Citrix DaaS per Azure:

- [Cataloghi](#)
- [Posizioni delle risorse](#)
- [Immagini](#)
- [Sottoscrizioni di Azure](#)
- [Connessioni di rete](#)
- [Unito al dominio e non unito al dominio](#)

Cataloghi

Un catalogo è un gruppo di macchine.

- I desktop e le app che Citrix DaaS for Azure offre agli utenti risiedono su macchine virtuali (VM). Tali macchine virtuali vengono create (sottoposte a provisioning) nel catalogo.

Quando si distribuiscono i desktop, le macchine del catalogo vengono condivise con utenti selezionati. Quando si pubblicano applicazioni, le macchine con più sessioni ospitano applicazioni condivise con utenti selezionati.

- Per l'accesso remoto al PC, un catalogo contiene macchine fisiche esistenti a sessione singola. Una distribuzione comune include le macchine situate nell'ufficio. È possibile controllare l'accesso degli utenti a tali computer tramite il metodo di assegnazione utente configurato e gli utenti selezionati.

Se avete familiarità con altri prodotti Citrix DaaS, un catalogo in Citrix DaaS è simile alla combinazione di un catalogo macchine e un gruppo di distribuzione.

Per ulteriori informazioni, vedere:

- [Crea cataloghi per desktop e app pubblicati.](#)
- [Crea cataloghi per l'accesso remoto al PC.](#)
- [Gestisci i cataloghi.](#)
- [Utenti e autenticazione.](#)

Posizioni delle risorse

Le macchine di un catalogo risiedono in una [posizione delle risorse](#). Una posizione di risorsa contiene anche due o più [connettori cloud](#).

- Quando pubblicate desktop o app, Citrix crea automaticamente la posizione delle risorse e i Connettori Cloud quando create il primo catalogo.
- Per l'accesso remoto al PC, l'amministratore crea la posizione della risorsa e i connettori cloud prima di creare un catalogo.

Quando crei altri cataloghi per desktop e app pubblicati, la sottoscrizione, l'area e il dominio di Azure determinano se Citrix crea un'altra posizione per le risorse. Se questi criteri corrispondono a un catalogo esistente, Citrix tenta di riutilizzare la posizione della risorsa.

Per ulteriori informazioni, vedere:

- [Specificare le informazioni sulla posizione delle risorse quando si crea un catalogo.](#)
- [Azioni sulla posizione delle risorse.](#)

Immagini

Quando si crea un catalogo per desktop e app pubblicati, viene utilizzata un'immagine macchina (con altre impostazioni) come modello per la creazione delle macchine.

- Citrix DaaS for Azure 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

Ogni immagine preparata da Citrix ha un Citrix VDA e 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 per Azure.

Citrix aggiorna le immagini preparate disponibili quando viene rilasciata una nuova versione di VDA.

- Puoi anche importare e utilizzare immagini personalizzate da Azure. È necessario installare un VDA (e altro software) sull'immagine prima di poter essere utilizzato per creare un catalogo.

Il termine **VDA** spesso si riferisce alla macchina che fornisce app o desktop e al componente software installato su tale macchina.

Per ulteriori informazioni, vedere [Immagini](#).

Sottoscrizioni di Azure

È possibile creare cataloghi per la distribuzione di desktop e app e creare/importare immagini in una sottoscrizione di Citrix Managed Azure o in una sottoscrizione Azure personalizzata (gestita dal cliente).

Se ordinate solo Citrix DaaS per Azure, dovete importare (aggiungere) e utilizzare le vostre sottoscrizioni di Azure. Se ordinate anche un fondo di consumo di Citrix Azure, riceverete una sottoscrizione a Citrix Managed Azure. È quindi possibile utilizzare una sottoscrizione di Citrix Managed Azure o una delle sottoscrizioni Azure importate durante la creazione di un catalogo o la creazione di una nuova immagine.

Per ulteriori informazioni, vedere:

- [Gli scenari di distribuzione](#) illustrano come utilizzare le sottoscrizioni di Azure con Citrix DaaS per Azure.
- [Le sottoscrizioni di Azure](#) spiegano le differenze tra le sottoscrizioni gestite da Citrix Azure e quelle di Azure gestite dal cliente. In questo articolo viene inoltre descritto come visualizzare, aggiungere e rimuovere le sottoscrizioni.
- [L'analisi tecnica sulla sicurezza](#) descrive le differenze di responsabilità tra Citrix Managed Azure e le sottoscrizioni di Azure gestite dal cliente.

Connessioni di rete

Quando crei un catalogo utilizzando una sottoscrizione di Citrix Managed Azure, indichi se e come gli utenti possono accedere a posizioni e risorse sulla loro rete locale aziendale dai desktop e dalle app pubblicati. Le scelte sono: nessuna connettività, peering di Azure VNet e Citrix SD-WAN.

Quando usi la tua sottoscrizione di Azure, non è necessario creare una connessione. Devi solo importare (aggiungere) la sottoscrizione di Azure al servizio.

Per ulteriori informazioni, vedere [Connessioni di rete](#).

Unito al dominio e non unito al dominio

Diverse funzioni e operazioni di servizio differiscono a seconda che le macchine (VDA) siano collegate al dominio o non appartenenti al dominio. L'appartenenza al dominio influisce anche sugli scenari di distribuzione disponibili.

- Sia le macchine unite al dominio che quelle non appartenenti al dominio supportano uno qualsiasi dei metodi di autenticazione utente disponibili nell'area di lavoro dell'utente.
- È possibile pubblicare desktop, app o entrambi da computer appartenenti al dominio e non appartenenti al dominio. I computer nei cataloghi di Accesso remoto a PC devono essere collegati al dominio.

Nella tabella seguente sono elencate diverse differenze tra i computer non appartenenti al dominio e quelli appartenenti al dominio durante la distribuzione di desktop e app.

Non unito a un dominio	Aderente al dominio
Active Directory non viene utilizzato per le macchine. I computer non fanno parte di un dominio AD. I criteri di gruppo di Active Directory non possono essere applicati alle macchine (VDA). È possibile applicare un oggetto Criteri di gruppo locale all'immagine utilizzata per creare un catalogo. Gli utenti accedono utilizzando il servizio Single Sign-On.	Active Directory viene utilizzato per le macchine. I computer sono uniti a un dominio AD. I VDA ereditano i criteri di gruppo per l'unità organizzativa AD specificata durante la creazione del catalogo. Quando gli utenti accedono al proprio workspace utilizzando un metodo di autenticazione diverso da Active Directory, viene richiesto l'accesso anche all'avvio di un desktop o di un'app.
Non è necessaria una connessione a una rete locale.	(Quando si utilizza un abbonamento a Citrix Managed Azure) È necessario disporre di una connessione per accedere a una rete locale, utilizzando Microsoft Azure VNet o Citrix SD-WAN.

Non unito a un dominio

Aderente al dominio

È necessario utilizzare una sottoscrizione di Citrix Managed Azure per il provisioning dei VDA. (Non è possibile utilizzare le sottoscrizioni di Azure personalizzate per il provisioning di VDA. Tuttavia, gli utenti possono essere connessi dal tuo Azure AD.)

Puoi usare una sottoscrizione di Citrix Managed Azure e le tue sottoscrizioni di Azure.

Impossibile risolvere i problemi utilizzando una macchina bastion o un RDP diretto.

Può risolvere i problemi utilizzando una macchina bastion o un RDP diretto.

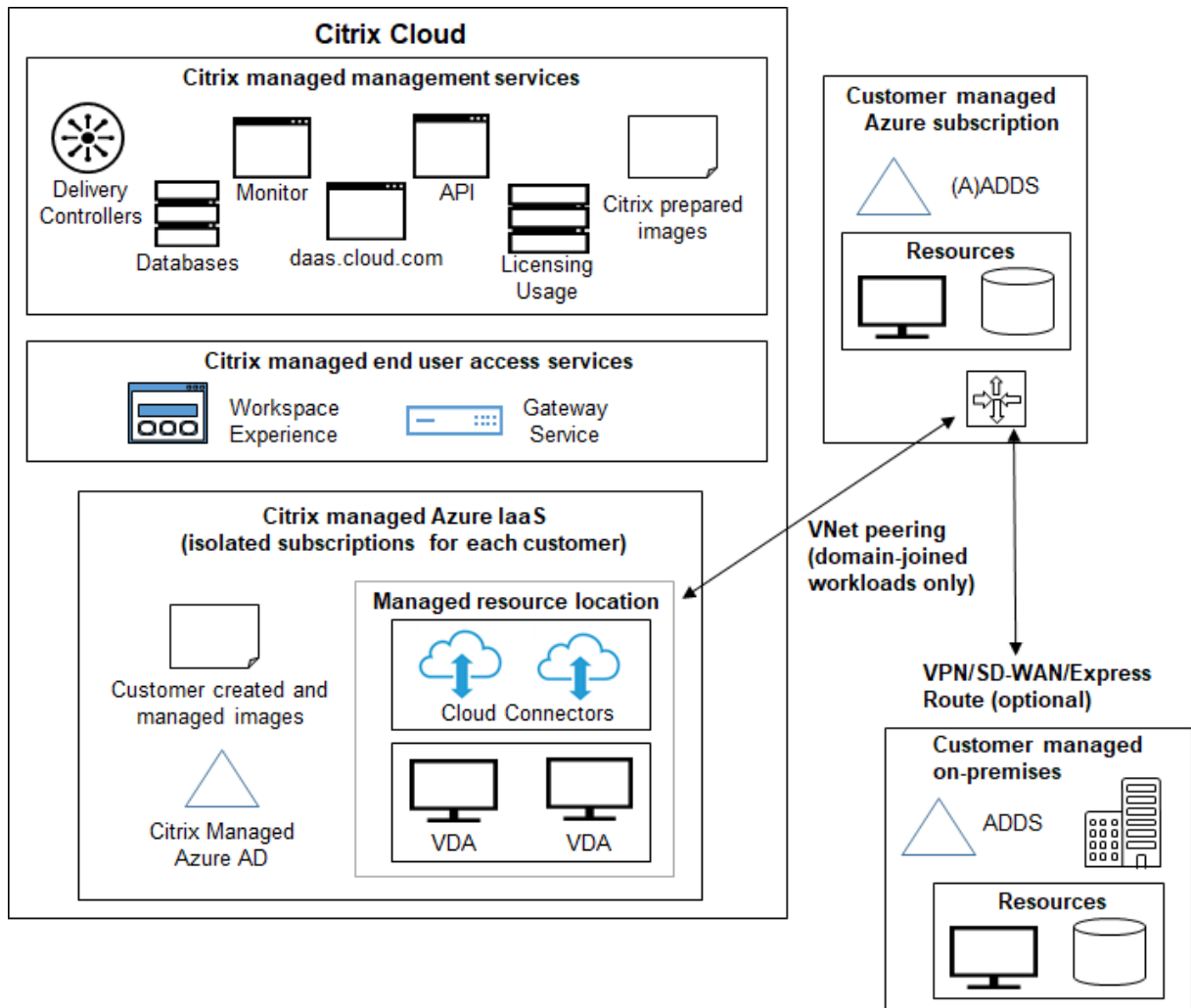
Non è possibile utilizzare Citrix Profile Management. (Consigliato: utilizzare cataloghi persistenti.)

È possibile utilizzare Citrix Profile Management o FSLogix.

Scenari di implementazione

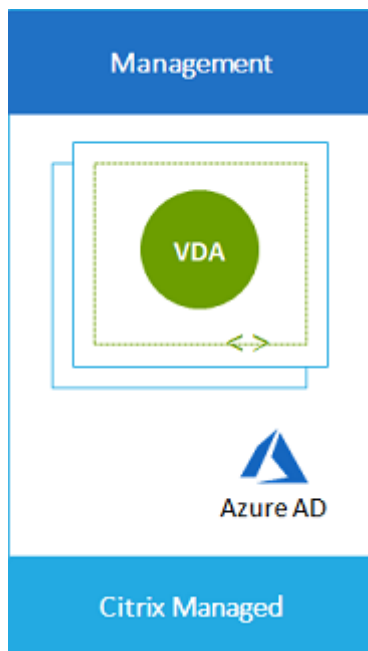
Gli scenari di distribuzione per desktop e app pubblicati variano a seconda che si utilizzi una sottoscrizione di Citrix Managed Azure o una sottoscrizione di Azure gestita dal cliente.

Distribuzione in una sottoscrizione di Citrix Managed Azure

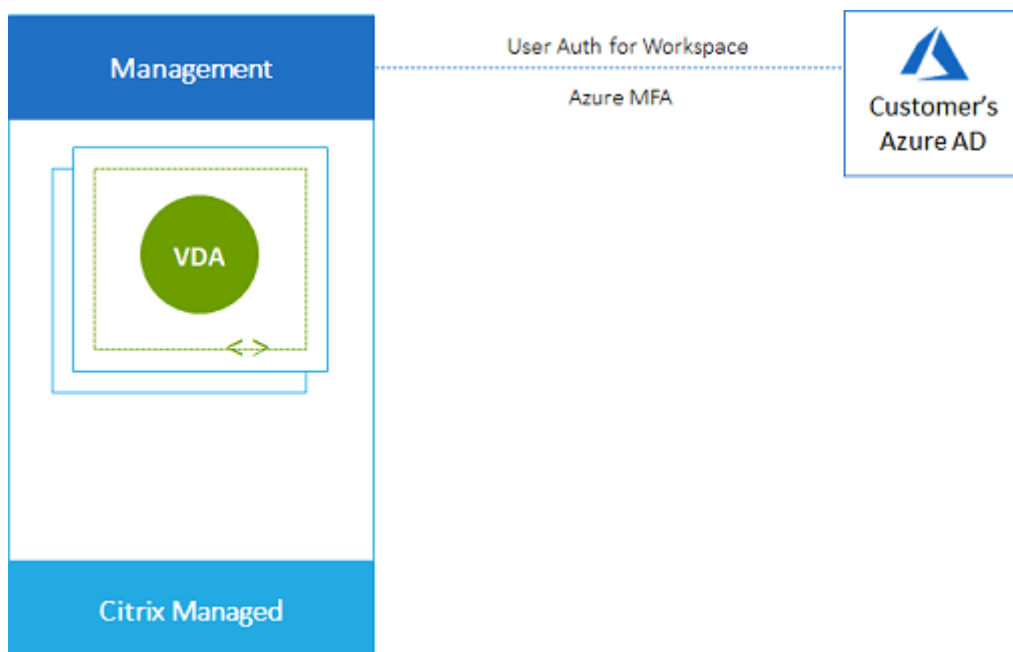


Citrix DaaS for Azure supporta diversi scenari di distribuzione per la connessione e l'autenticazione degli utenti.

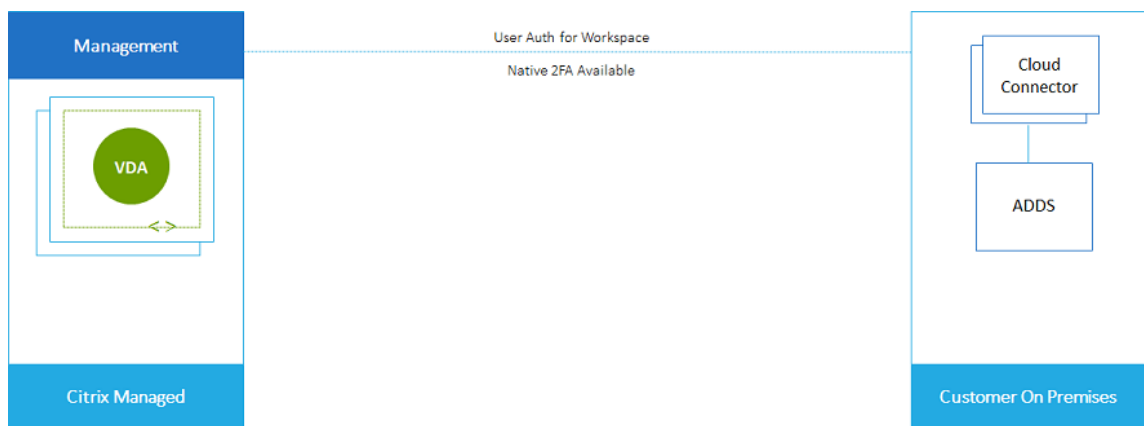
- **Azure AD gestito:** questa è la distribuzione più semplice, con VDA non appartenenti al dominio. È consigliato per le prove di concetto. È possibile utilizzare Managed Azure AD (gestito da Citrix) per gestire gli utenti. Gli utenti non hanno bisogno di accedere alle risorse della rete locale.



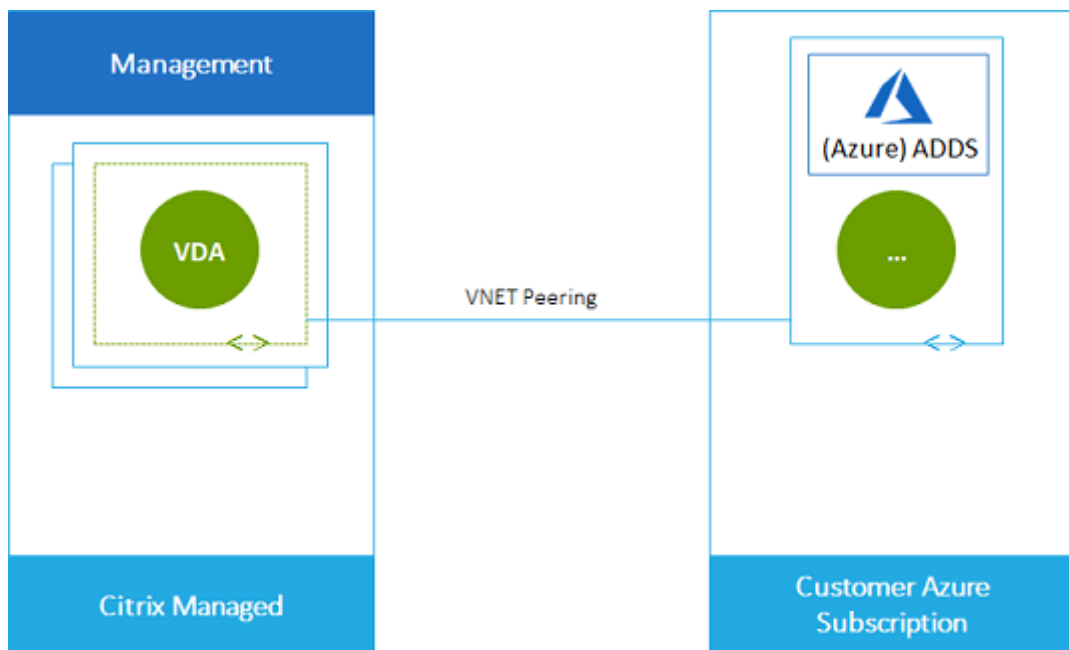
- **Azure Active Directory del cliente:** questa distribuzione contiene VDA non appartenenti al dominio. È possibile utilizzare Active Directory o Azure Active Directory (AAD) per l'autenticazione dell'utente finale. In questo scenario, gli utenti non hanno bisogno di accedere alle risorse della rete locale.



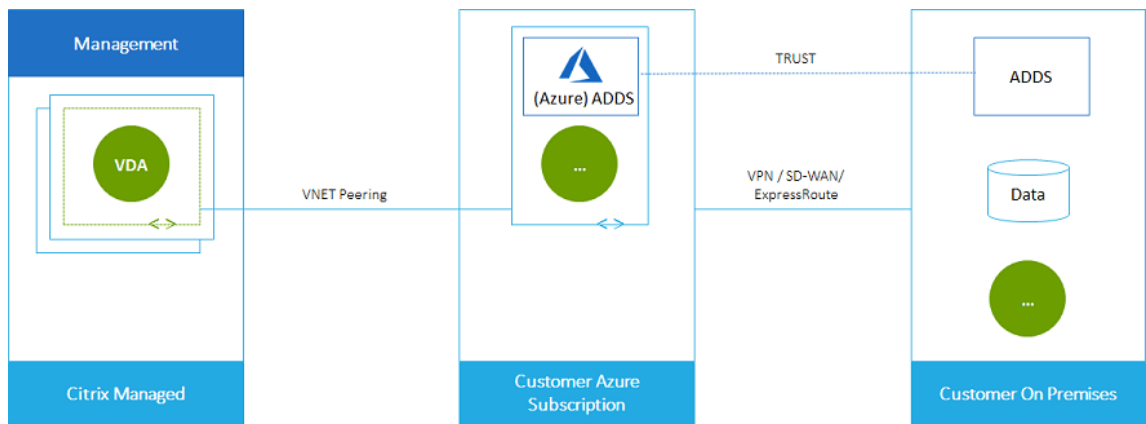
- **Azure Active Directory del cliente con accesso locale:** questa distribuzione contiene VDA non appartenenti al dominio. È possibile utilizzare il proprio AD o AAD per l'autenticazione dell'utente finale. In questo scenario, l'installazione di Citrix Cloud Connectors nella rete locale consente l'accesso alle risorse della rete.



- Servizi di dominio Azure Active Directory e peering VNet del cliente:** se il tuo AD o AAD risiede nella tua sottoscrizione di Azure VNet e Azure, puoi utilizzare la funzionalità peering di Microsoft Azure VNet per una connessione di rete e Azure Active Directory Domain Services (AADDs) per l'autenticazione dell'utente finale. I VDA sono uniti al tuo dominio.

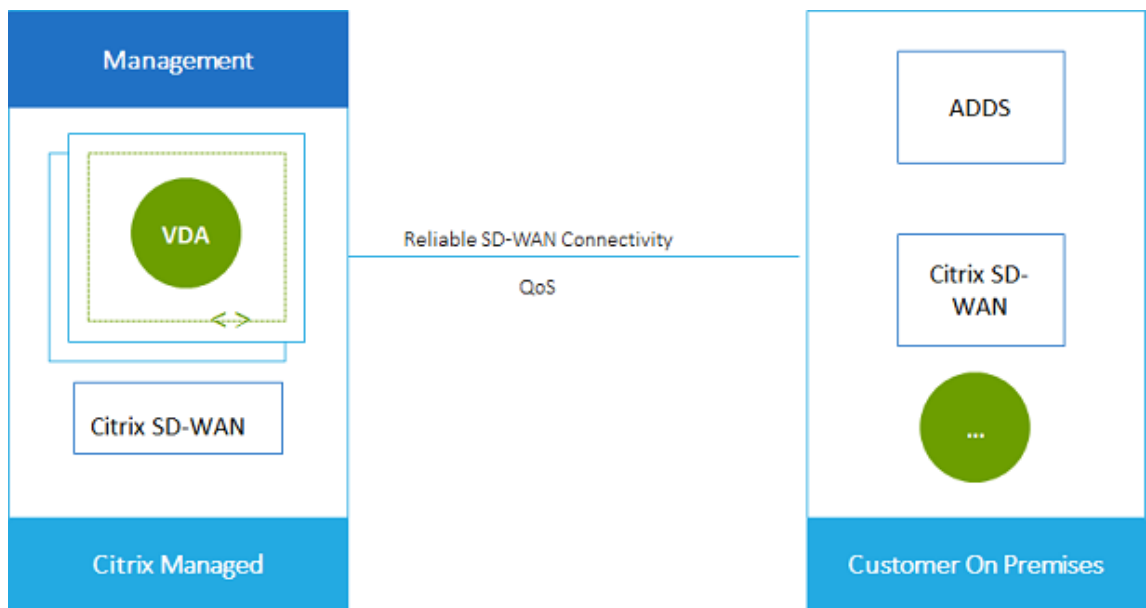


Per consentire agli utenti di accedere ai dati archiviati nella rete locale, puoi utilizzare la connessione VPN dalla sottoscrizione di Azure alla posizione locale. Il peering Azure VNet viene utilizzato per la connettività di rete. Servizi di dominio Active Directory nella posizione locale viene utilizzato per l'autenticazione dell'utente finale.

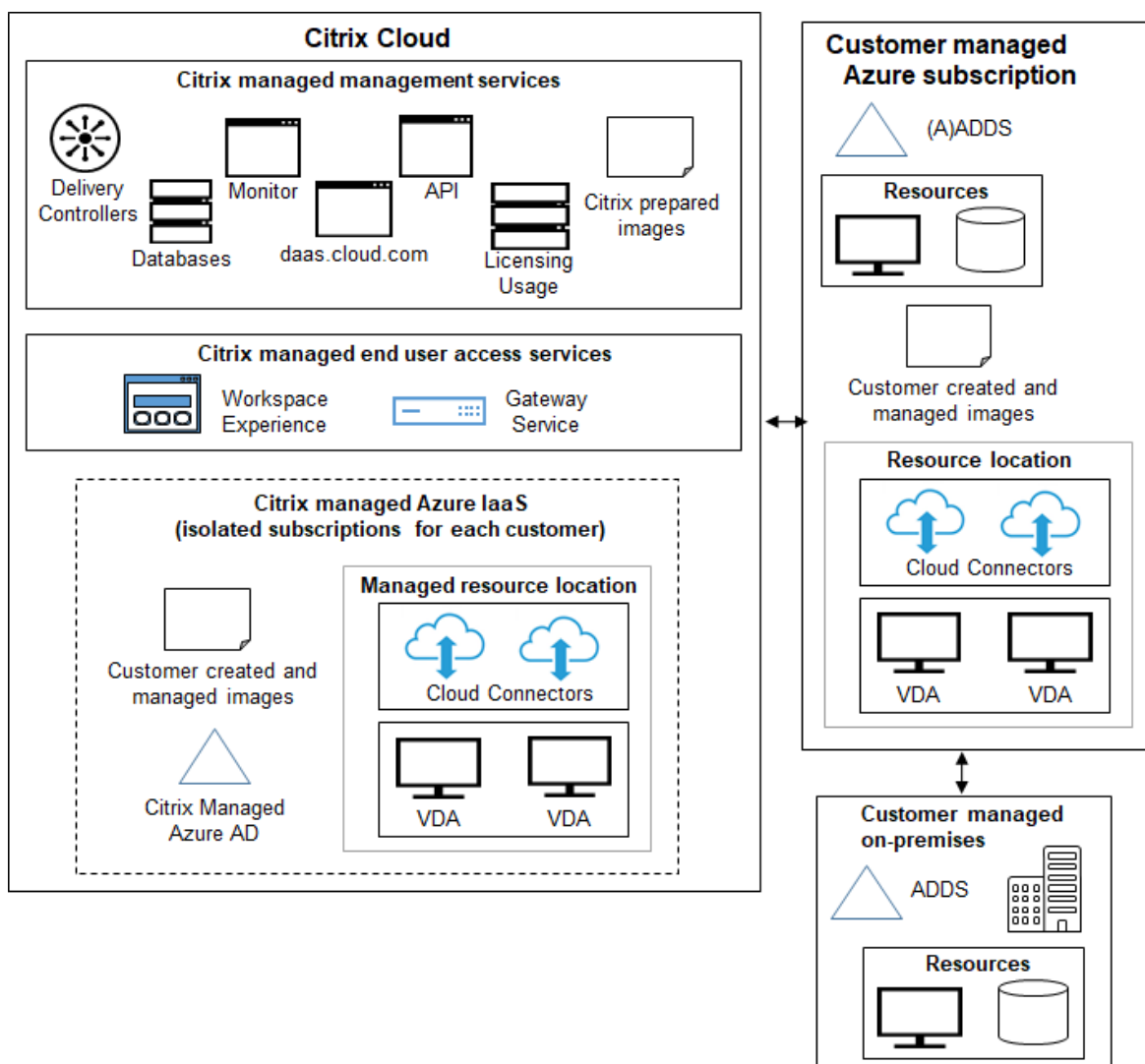


- **Active Directory e SD-WAN del cliente:** è possibile fornire agli utenti l'accesso a file e altri elementi dalle reti SD-WAN locali o cloud.

Citrix SD-WAN ottimizza tutte le connessioni di rete necessarie a Citrix DaaS per Azure. Lavorando di concerto con le tecnologie HDX, Citrix SD-WAN fornisce qualità del servizio e affidabilità di connessione per ICA e Citrix DaaS out-of-band per il traffico Azure.



Distribuzione in una sottoscrizione di Azure gestita dal cliente



La distribuzione nell'immagine precedente utilizza una sottoscrizione di Azure gestita dal cliente. Tuttavia, la sottoscrizione di Citrix Managed Azure rimane un'opzione per altri cataloghi e immagini, come indicato dalla struttura tratteggiata.

Interfacce di gestione

Citrix DaaS for Azure dispone di due interfacce grafiche di gestione: Quick Deploy e Full Configuration.

- **Quick Deploy** ti consente di creare rapidamente cataloghi e iniziare a distribuire desktop e app ai tuoi utenti. (Da qui il nome, Quick Deploy). È l'interfaccia predefinita all'avvio di Citrix DaaS for Azure. Puoi accedere a questa interfaccia anche selezionando **Gestisci > Distribuzione rap-**

ida di Azure. Le istruzioni contenute in questo set di documentazione del prodotto presuppongono l'utilizzo di Quick Deploy.

Se si prevede di utilizzare una sottoscrizione di Citrix Managed Azure durante la creazione di un catalogo o di un'immagine, è necessario utilizzare Quick Deploy.

- **La configurazione completa** offre funzionalità avanzate e opzioni di configurazione per personalizzare e gestire la distribuzione. I cataloghi creati in Quick Deploy vengono visualizzati automaticamente in Configurazione completa. Per passare da Distribuzione rapida a Configurazione completa, selezionare **Gestisci > Configurazione completa**.

Quando si crea un catalogo in Quick Deploy, un gruppo di consegna associato e una connessione host vengono creati automaticamente in Configurazione completa.

La configurazione completa offre inoltre un proprio processo di creazione del catalogo che include la creazione di una connessione all'host di Azure, quindi la creazione di un catalogo e di un gruppo di consegna. Tale processo è supportato solo se utilizzi la tua sottoscrizione di Azure. È molto più semplice creare il catalogo in Quick Deploy.

La configurazione completa supporta i processi correlati all'hypervisor e agli host di servizi cloud diversi da Azure. Questi non sono disponibili per i clienti Citrix DaaS for Azure.

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, vedere [Gestire i cataloghi](#). 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 **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, fai 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.

Per informazioni su come gestire i cataloghi convertiti nella configurazione completa, vedere:

- [Gestione dei cataloghi delle macchine](#) (la configurazione completa si riferisce ai cataloghi come cataloghi di macchine)
- [Gestire i gruppi di consegna](#)

Ulteriori informazioni

Per i dettagli tecnici, vedere:

- [Architettura di riferimento](#) Citrix Tech Zone
- [Tech brief](#) Citrix Tech Zone

Per informazioni sull'automazione delle distribuzioni, vedere l'[anteprima dell'API pubblica dei desktop gestiti](#).

Quando si è pronti, [iniziare](#).

Novità

December 28, 2023

Uno degli obiettivi di Citrix è fornire nuove funzionalità e aggiornamenti di prodotto a Citrix DaaS per i clienti di Azure quando sono disponibili. Le nuove versioni offrono più valore, quindi non c'è motivo di ritardare gli aggiornamenti. Per te, l'amministratore del cliente, questo processo è trasparente.

Aggiornamenti delle immagini preparati da Citrix

Le [immagini preparate da Citrix](#) hanno installato un Citrix Virtual Delivery Agent (VDA) attualmente installato. Generalmente, le nuove versioni di VDA vengono rilasciate più volte all'anno e le immagini preparate da Citrix disponibili vengono aggiornate automaticamente con l'ultimo VDA. Per informazioni sulle funzionalità nuove e migliorate della versione attuale di VDA, vedere:

- [Windows VDA](#)
- [VDA Linux](#)

agosto 2022

- Questa funzionalità è disponibile a livello generale: ora puoi creare cataloghi di macchine aggiunte ad Azure Active Directory. Vedere [Creare cataloghi](#).

maggio 2022

- Ora puoi creare cataloghi di macchine unite al tuo Azure Active Directory. Questa funzionalità è disponibile in anteprima. Vedere [Creare cataloghi](#).
- I fornitori di servizi Citrix possono ora rimuovere il servizio Citrix DaaS per Azure dai clienti. Vedere [Rimuovere un servizio](#).

aprile 2022

- È ora disponibile la creazione di connessioni host per Citrix Hypervisor, Microsoft SCVMM, VMware vSphere, Prism Central e Nutanix AHV. Pertanto, è ora possibile utilizzare hypervisor locali oltre ad Azure.
- Il nome del prodotto è cambiato da Citrix Virtual Apps and Desktops Standard for Azure a Citrix DaaS Standard for Azure. Per ulteriori informazioni sul rebranding di tutte le offerte Citrix DaaS (precedentemente Citrix Virtual Apps and Desktops service), consultate [Novità di Citrix DaaS](#). Scopri di più sulle modifiche al nome nel [nostro annuncio sul nostro blog](#).

gennaio 2022

- Quando crei cataloghi, ora puoi archiviare le tue macchine su uno storage SSD standard. In precedenza, erano supportati solo dischi standard (HDD) e SSD premium.
- Supporto per queste nuove regioni per l'hosting di carichi di lavoro VDA: Brasile meridionale, India centrale, Giappone orientale, Stati Uniti centro-meridionali e Regno Unito meridionale.
- Le istantanee e il ripristino sono ora disponibili per i desktop persistenti ospitati su Citrix Managed Azure e BYO Azure. Vedi [istantanea e ripristino VDA](#).
- Sono ora disponibili indirizzi IP pubblici statici per tutto il traffico in uscita dai VDA ospitati. È possibile configurare un gateway NAT di Azure per ottenere l'indirizzo IP. Vedere [Creare un indirizzo IP statico pubblico](#).
- La VPN di Azure è disponibile per l'anteprima tecnica. La VPN di Azure consente di connettere Citrix Managed Azure direttamente con i data center locali. Vedi [Anteprima tecnica di Azure VPN](#).
- Sono disponibili nuove immagini Linux per le immagini preparate da Citrix.

novembre 2021

- Sono ora disponibili [prove](#) di 7 giorni approvate automaticamente (oltre alle prove approvate dalle vendite).
- I provider di servizi Citrix possono ora gestire gli utenti dalla dashboard **Gestisci > Azure Quick Deploy** del servizio o dalla console Citrix Cloud. Per i dettagli, consulta [Accesso dei partner al fornitore di identità del cliente](#).

ottobre 2021

- Nuove informazioni sulla [gestione dei cataloghi creati in Quick Deploy](#).

settembre 2021

- Il [contenuto dell'API di anteprima](#) è disponibile.
- Supporto per Windows Server 2022 (richiede un VDA 2106 minimo).

luglio 2021

- Interfaccia di gestione di Web Studio rinominata Configurazione completa.

giugno 2021

- Supporto per due [interfacce di gestione](#): Quick Deploy e Web Studio.

maggio 2021

- Questo servizio supporta l'[anteprima di Service Continuity](#).
- [Le immagini preparate da Citrix](#) ora includono le versioni a sessione singola e multisezione di Ubuntu.
- Quando si [aggiunge un Cloud Connector a una posizione di risorsa](#), utilizzando una sottoscrizione di Citrix Managed Azure, è possibile specificare il tipo di prestazioni del computer Cloud Connector.
- Quando si [crea un catalogo](#), le opzioni relative alle prestazioni della macchina includono opzioni che corrispondono al tipo di generazione (gen1 o gen2) dell'immagine selezionata. È possibile [aggiornare un catalogo](#) con un'immagine di tipo di generazione diverso, se i computer del catalogo supportano tale tipo di generazione.

aprile 2022

- Il nome del prodotto è cambiato da Citrix Virtual Apps and Desktops Standard for Azure a Citrix DaaS Standard for Azure.

gennaio 2021

- Supporto in anteprima per visualizzare l'[utilizzo degli impegni di consumo](#).

ottobre 2020

- È possibile utilizzare la funzione [Shadow Monitor](#) per visualizzare o lavorare sulla VM o sulla sessione di un utente.
- Supporto di produzione per [Remote PC Access](#).
- Opzione di creazione del catalogo avanzata per [utilizzare la licenza idonea per Azure Virtual Desktop o il Vantaggio Azure](#)
- Se un'azione di riavvio su un computer non ha esito positivo, è possibile utilizzare un'[azione di riavvio forzato](#).

settembre 2020

- I [dettagli sulle immagini](#) vengono riorganizzati e ampliati. Ad esempio, ora è possibile aggiungere e modificare note sulle immagini preparate o importate. È inoltre possibile limitare l'accesso solo agli indirizzi IP specificati.
- Quando [crei una connessione peering di Azure VNet](#) che utilizzerà un gateway di rete virtuale di Azure, ora puoi anche abilitare la propagazione della rotta del gateway di rete virtuale.
- Modifica del nome del prodotto da Citrix Managed Desktops a Citrix Virtual Apps and Desktops Standard for Azure.

agosto 2020

- Supporto in anteprima per [Remote PC Access](#).
- È ora disponibile un'immagine di Windows Server 2019 preparata da Citrix.

luglio 2020

- Quando aggiungi un Cloud Connector a una posizione risorsa, utilizzando una sottoscrizione di Azure gestita dal cliente, puoi specificare il tipo di prestazioni del computer Cloud Connector e il gruppo di risorse di Azure. Per ulteriori informazioni, vedere Azioni relative all'[ubicazione delle risorse](#)
- Durante la creazione di un catalogo, è possibile specificare uno schema di denominazione delle macchine. Vedere [Creare un catalogo utilizzando la creazione personalizzata](#).

giugno 2020

- In un ambiente CSP, le connessioni SD-WAN vengono create in base al tenant. Perché l'opzione di connessione SD-WAN sia disponibile per l'amministratore del CSP, il tenant deve disporre di un'autorizzazione al servizio SD-WAN Orchestrator. Per ulteriori informazioni, vedere [Filtrare le risorse per cliente \(distribuzioni multitenant\)](#).
- Supporto di produzione per [VDA Linux](#) quando si utilizza una sottoscrizione di Azure gestita dal cliente.
- Il [limite](#) di VDA per abbonamento è ora di 1.200.

maggio 2020

- È possibile [aggiungere un'altra sottoscrizione di Citrix Managed Azure](#) quando sono necessarie più macchine rispetto al limite per sottoscrizione di Citrix Managed Azure.
- Ulteriori informazioni sui [server DNS](#).

marzo 2020

- Supporto di produzione per [connessioni SD-WAN](#).

febbraio 2020

- Per visualizzare le informazioni sull'utilizzo delle licenze Citrix, segui le linee guida in [Monitorare il monitoraggio delle licenze e dell'utilizzo per Citrix DaaS Standard for Azure](#).
- Supporto in anteprima per cataloghi contenenti macchine Red Hat Enterprise Linux o Ubuntu. Questa funzionalità è valida solo quando si utilizza una sottoscrizione di Azure gestita dal cliente e richiede un'immagine importata contenente un Citrix Linux VDA.
- Ora è possibile configurare il bilanciamento del carico verticale o orizzontale per tutte le macchine multiseSSIONE. (In precedenza, tutte le macchine utilizzavano il bilanciamento del carico orizzontale.) Questa selezione globale si applica a tutti i cataloghi della distribuzione. Vedere [Bilanciamento del carico](#).
- Ora puoi aggiungere una sottoscrizione di Azure se non sei un amministratore globale.
- Un'immagine preparata da Citrix è ora disponibile per Windows 10 Enterprise Virtual Desktop (multi-sessione) con Office 365 ProPlus.

gennaio 2020

- Aggiunge il supporto per percorsi personalizzati nelle connessioni peering VNet.
- Aggiornamenti all'articolo sulla sicurezza per migliorare le informazioni su porte e regole.

novembre 2019

- Supporto in anteprima per le connessioni SD-WAN.

ottobre 2019

- In [Sistemi operativi supportati](#), sono state aggiunte voci per:
 - Windows 7 (supporta solo VDA 7.15 con l'ultimo aggiornamento cumulativo).
 - Windows Server 2019.
- È ora disponibile un'[immagine preparata per Citrix](#) per Windows Server 2012 R2.
- Aggiunte informazioni sulle impostazioni della posizione delle risorse. Per ulteriori informazioni, vedere [Azioni ubicazione risorse](#) e [Impostazioni ubicazione risorse durante la creazione di un catalogo](#).

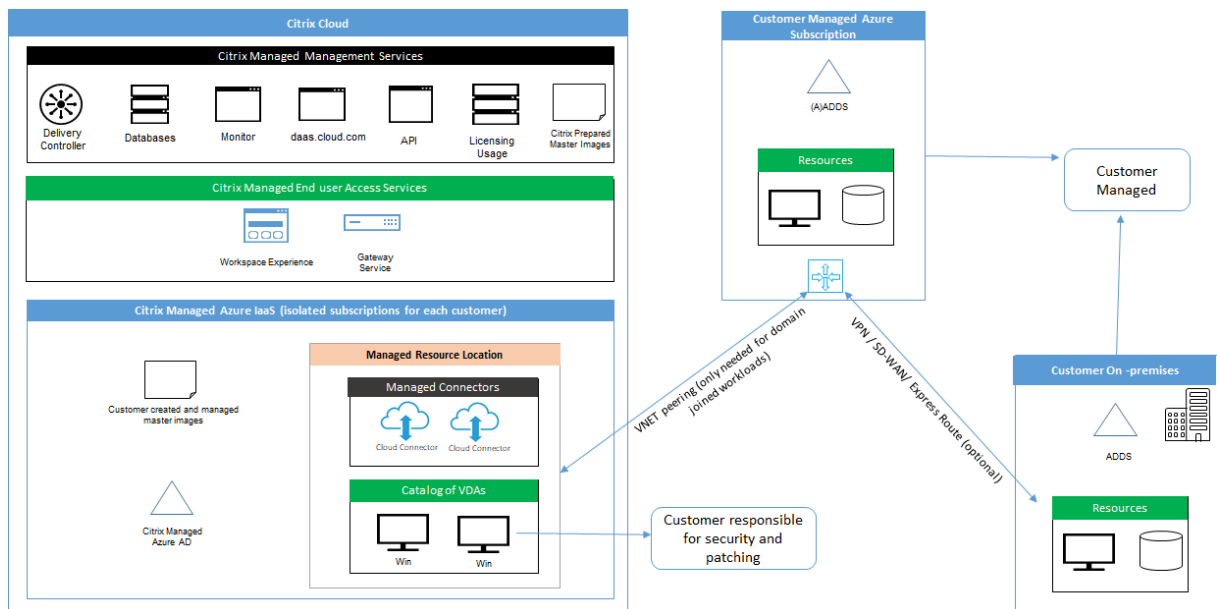
settembre 2019

- Per impostazione predefinita, le macchine vengono create in una sottoscrizione di Citrix Managed Azure. Ora puoi anche creare cataloghi e immagini nella tua sottoscrizione di Azure gestita dal cliente.

Panoramica tecnica sulla sicurezza

October 7, 2022

Il diagramma seguente mostra i componenti di una distribuzione Citrix DaaS Standard per Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure). In questo esempio viene utilizzata una connessione di peering VNet.



Con Citrix DaaS for Azure, i Virtual Delivery Agent (VDA) del cliente che distribuiscono desktop e app, oltre a Citrix Cloud Connectors, vengono distribuiti in una sottoscrizione di Azure e in un tenant gestiti da Citrix.

NOTA:

Questo articolo fornisce una panoramica dei requisiti di sicurezza per i clienti che distribuiscono Citrix DaaS per Azure utilizzando una sottoscrizione Citrix Managed Azure. Per una panoramica dell'architettura di una distribuzione di Citrix DaaS per Azure che utilizza una sottoscrizione di Azure gestita dal cliente, incluse le informazioni sulla sicurezza, consulta [Architettura di riferimento: servizio Virtual Apps and Desktops - Azure](#).

Conformità basata su cloud Citrix

A gennaio 2021, l'utilizzo di Citrix Managed Azure Capacity con varie edizioni 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

Citrix DaaS for Azure distribuisce almeno due connettori cloud in ogni posizione delle 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 Connector. 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 al Citrix DaaS solo per il personale operativo di Azure 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 for Azure per creare e personalizzare una nuova immagine macchina, le porte 3389-3390 vengono aperte temporaneamente nella VNet gestita da Citrix, in modo che il cliente possa RDP sulla macchina contenente la nuova immagine macchina, per personalizzarla.

Responsabilità di Citrix nell'utilizzo delle connessioni di peering di Azure VNet

Affinché VDA in Citrix DaaS for Azure possano contattare controller di dominio locali, condivisioni di file o altre risorse intranet, Citrix DaaS for Azure 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 da cloud a locale scelta dal cliente, ad esempio Azure ExpressRoute o 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

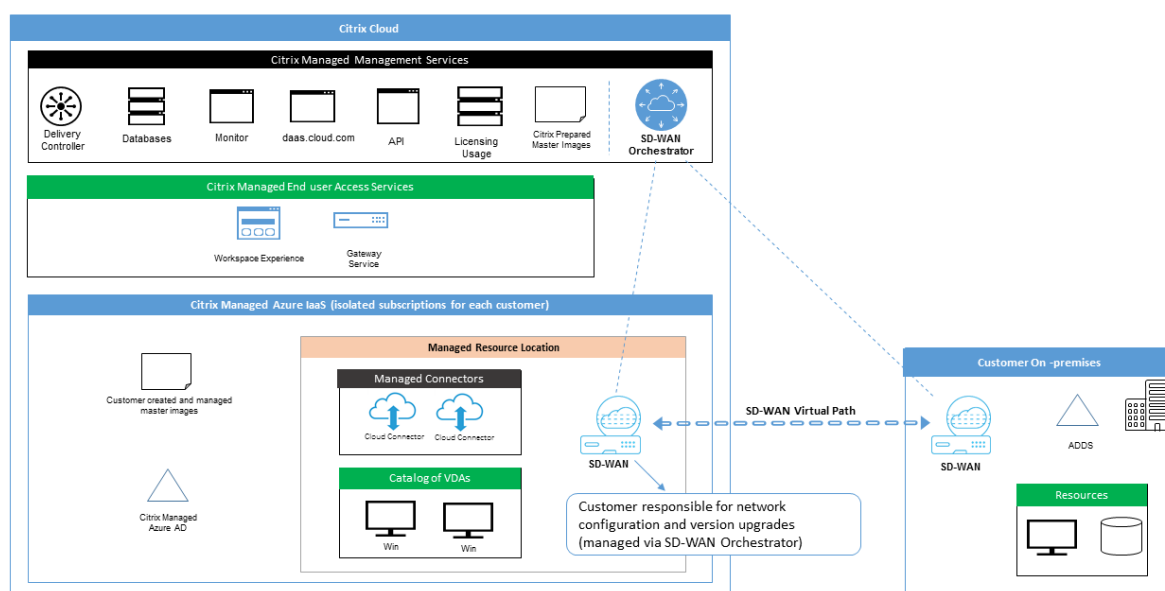
Citrix supporta un modo completamente automatizzato di distribuire istanze Citrix SD-WAN virtuali per abilitare la connettività tra Citrix DaaS for Azure e le risorse locali. La connettività Citrix SD-WAN presenta numerosi vantaggi rispetto al peering VNet, tra cui:

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 for Azure di utilizzare SD-WAN Orchestrator per la gestione delle loro reti Citrix SD-WAN.

Il diagramma seguente mostra i componenti aggiunti in una distribuzione Citrix DaaS per Azure utilizzando la connettività SD-WAN.



La distribuzione di Citrix SD-WAN per Citrix DaaS for Azure è simile alla configurazione di distribuzione di Azure standard 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 rete virtuale, 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 for Azure, 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 di macchine caricate su Citrix DaaS per Azure, 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.

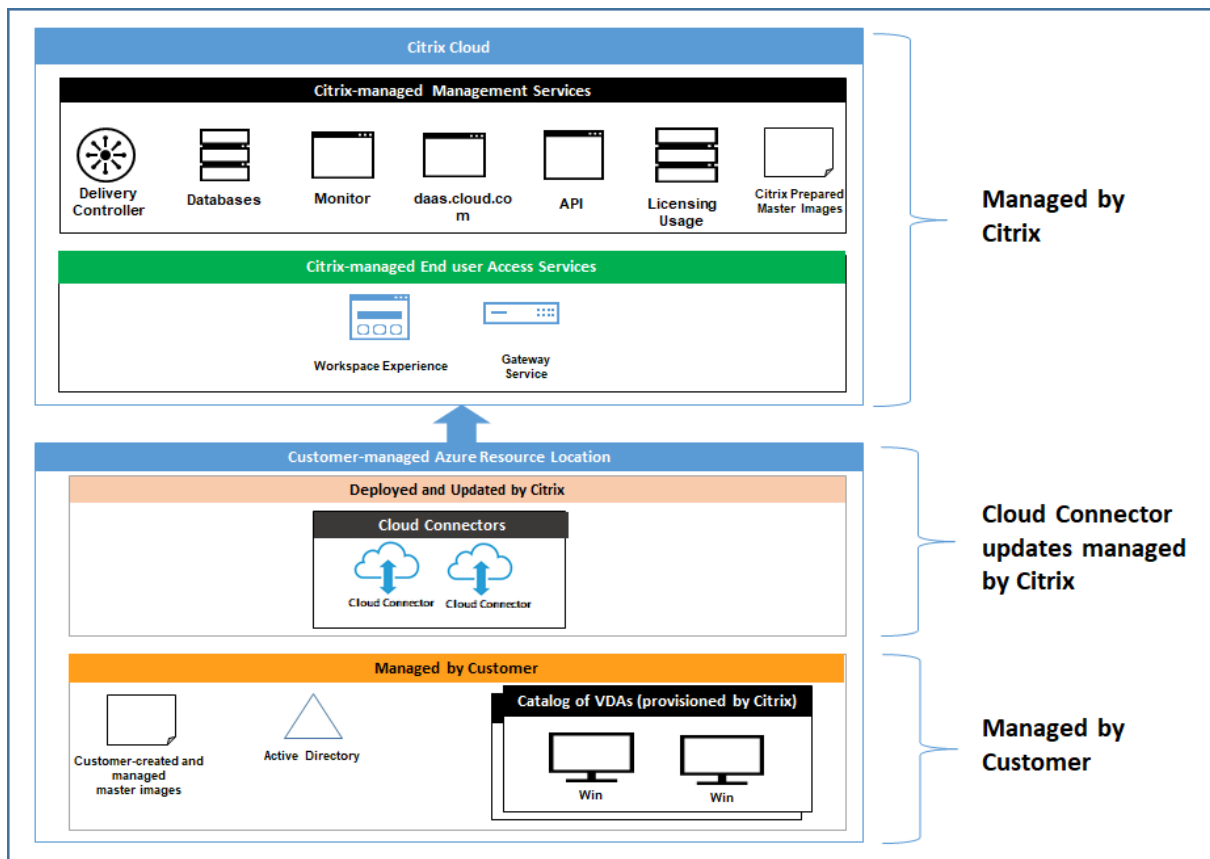
- Viene consentita temporaneamente la porta 3389 in entrata dall'indirizzo IP del bastione a qualsiasi indirizzo nella VNet (VDA e Cloud Connector).
- Si continua a bloccare l'accesso RDP tra i Cloud Connector, i VDA e altri VDA.

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 piena flessibilità per configurare le istanze SD-WAN virtuali utilizzate con Citrix DaaS for Azure in base ai loro requisiti di rete, ad eccezione

di alcuni elementi necessari per garantire il corretto funzionamento di SD-WAN nella VNet gestita da Citrix. 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 su Citrix DaaS per le istanze SD-WAN di Azure devono essere gestite dai clienti in base alle pianificazioni 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 della SD-WAN possono comportare rischi per la sicurezza sia per le risorse virtuali in Citrix DaaS per Azure, sia per le risorse locali raggiungibili tramite 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 del lancio. 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 di Azure, il cliente è responsabile della ricostruzione della propria rete virtuale gestita dal cliente in una nuova regione e della creazione di un nuovo peering VNet o di una nuova istanza SD-WAN all'interno di Citrix DaaS for Azure.

Citrix e le responsabilità condivise con i clienti

Citrix Cloud Connector per cataloghi aggiunti a un dominio

Citrix DaaS for Azure distribuisce almeno due connettori cloud in ogni posizione delle 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 riscontrasse problemi con il catalogo in Citrix DaaS per Azure, ci sono due opzioni per la risoluzione dei problemi: utilizzare 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 for Azure.

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, è responsabile di fornire a Citrix DaaS per Azure un account di dominio (nome utente e password) con le autorizzazioni per unire le

macchine al dominio. Quando fornisce le credenziali di dominio, il cliente è responsabile del rispetto dei seguenti principi di sicurezza:

- **Verificabile:** l'account deve essere creato appositamente per Citrix DaaS per l'utilizzo di Azure in modo che sia facile controllare a cosa serve l'account.
- **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](#)

Abbonati a Citrix DaaS per Azure

December 21, 2022

Introduzione

Potete sottoscrivere Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure service) e ordinare il Citrix Azure Consumption Fund, tramite Citrix o tramite Azure Marketplace. È possibile valutare Citrix DaaS per Azure tramite Citrix.

Se attualmente siete abbonati a Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials, potete eseguire l'aggiornamento a Citrix DaaS Standard per Azure.

Un ordine completo è composto da due parti:

- **Citrix DaaS Standard for Azure:** consente di utilizzare le proprie sottoscrizioni Azure (gestite dal cliente).

- **Citrix Azure Consumption Fund:** consente inoltre di utilizzare una sottoscrizione di Citrix Managed Azure, oltre alle proprie sottoscrizioni di Azure. L'utilizzo di una sottoscrizione a Citrix Managed Azure offre i seguenti vantaggi:
 - Fatturazione singola da Citrix, piuttosto che fatturazioni da più aziende.
 - [Differenze tra le funzionalità della sottoscrizione ad Azure.](#)
 - Supporto Microsoft di livello premium tramite Citrix.

Il fondo di consumo di Citrix Azure non è richiesto. Tuttavia, se non ne hai, sei limitato a utilizzare solo le tue sottoscrizioni di Azure e non ricevi gli altri vantaggi delle funzionalità.

Il processo di ordinazione varia leggermente, a seconda che si effettui un ordine tramite Citrix o Azure Marketplace:

- Quando ordinate tramite Citrix, potete ordinare contemporaneamente Citrix DaaS Standard for Azure e Citrix Azure Consumption Fund.
- Quando ordinate tramite Azure Marketplace, ordinate innanzitutto Citrix DaaS Standard per Azure. Quindi, ordinate il fondo di consumo di Citrix Azure.

Se decidi di ordinare solo Citrix DaaS per Azure, puoi ordinare il Citrix Azure Consumption Fund in un secondo momento, tramite Azure Marketplace o tramite il rappresentante del tuo account Citrix.

Indipendentemente da dove ordini Citrix DaaS Standard for Azure e dal fondo di consumo, Citrix fornisce assistenza per l'onboarding. Verificheremo inoltre che Citrix DaaS Standard for Azure sia in esecuzione e configurato correttamente.

Riepilogo ordini

Riepilogo delle fasi dell'ordine:

1. Ottieni un account Citrix Cloud.

Se disponete già di un account Citrix Cloud e attualmente vi iscrivete a Citrix DaaS, consultate [Se siete attualmente abbonati a Citrix DaaS.](#)

2. Ordinate Citrix DaaS Standard per Azure e il fondo di consumo tramite Azure Marketplace oppure ordinate tramite Citrix.

Prove

Citrix DaaS Standard for Azure offre due tipi di versioni di prova:

- **Approvato dalle vendite:** in una versione di valutazione approvata dalle vendite, potete utilizzare una sottoscrizione Citrix Managed Azure per creare cataloghi, immagini e altre attività. Dalla versione di valutazione, potete convertire in una sottoscrizione al servizio a pagamento e ordinare il Citrix Managed Azure Consumption Fund. Se non acquistate consumi, tutte le risorse create utilizzando la sottoscrizione Citrix Managed Azure vengono eliminate automaticamente, il che potrebbe influire sugli utenti.
- **Approvazione automatica:** in una versione di valutazione approvata automaticamente, puoi utilizzare la tua sottoscrizione di Azure (gestita dal cliente) per creare cataloghi, immagini e altre attività. Dalla versione di prova, puoi convertire in un abbonamento a pagamento. Per ulteriori informazioni, consulta Prove di assistenza approvate automaticamente.

Per ulteriori informazioni sulle prove, consultate le versioni di [prova del servizio Citrix Cloud](#).

Prove di assistenza approvate

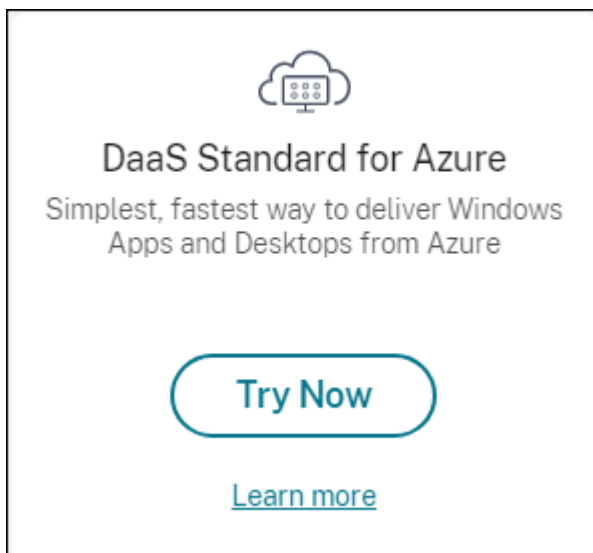
- Una versione di valutazione automatica di Citrix DaaS Standard for Azure dura 7 giorni di calendario.
- Durante una versione di valutazione approvata automaticamente, puoi creare cataloghi utilizzando la sottoscrizione di Azure. I cataloghi contengono le macchine che forniscono desktop o applicazioni.
- Potete creare cataloghi utilizzando un'immagine preparata per Citrix, un'immagine importata da Azure o un'immagine creata in Citrix DaaS Standard for Azure.
- Gli utenti devono essere configurati in un provider di identità [supportato](#) da Citrix Workspace.
- Puoi assegnare fino a 25 utenti ai cataloghi nella distribuzione di prova. Sebbene sia possibile assegnare un utente a più di un catalogo, in una distribuzione di prova è consentito un totale di 25 utenti denominati univoci.
- Devi avere un account utente Microsoft Azure e almeno una sottoscrizione di Azure in tale account. (Le versioni di prova supportano solo casi d'uso della sottoscrizione di Azure di proprietà del cliente (bring your own).)

Richiedere e utilizzare una versione di prova del servizio approvata automaticamente

1. Create un account Citrix Cloud (se non ne avete già uno).
 - a) Passate a [Citrix Cloud](#).
 - b) Seleziona **Registrati e provalo gratuitamente**.
 - c) Seguire la guida sullo schermo.

In pochi istanti, riceverete un'e-mail sul vostro account Citrix Cloud. Seleziona il link di accesso nell'e-mail.

2. Richiedi una versione di prova. Nella console di Citrix Cloud, selezionate **Prova ora** nel riquadro **DaaS Standard for Azure**.



Riceverai un'e-mail quando la versione di prova del servizio sarà attivata e pronta (di solito circa due ore dopo la richiesta della versione di prova).

3. Accedere a [Citrix Cloud](#).
4. Fai clic su **Gestisci** nel riquadro **DaaS Standard for Azure**.
5. Configura e configura il tuo ambiente di prova. Durante la configurazione, potrai:
 - a) [Aggiungi la tua sottoscrizione di Azure al servizio](#).
 - b) [Connetti il tuo provider di identità tramite la console Citrix Cloud](#).
 - c) [Crea un catalogo](#).
 - d) [Aggiungi utenti dal tuo provider di identità al catalogo](#).
 - e) [Notificate agli utenti l'URL di Citrix Workspace](#).

L'interfaccia grafica ti guida attraverso il processo di configurazione. Per ulteriori informazioni, consultate la documentazione del prodotto:

- [Acquisisci familiarità con il prodotto e la sua terminologia](#).
- [Rivedi i riassunti e i dettagli della configurazione](#)

Ottieni un account Citrix Cloud

Per creare un account Citrix Cloud e richiedere una versione di prova, visitare il <https://onboarding.cloud.com>. Per ulteriori informazioni su questo processo, consultate [Registrazione a Citrix Cloud](#). Il tuo

account ha un Organization ID (OrgID) che appare sempre nell'angolo in alto a destra della console di Citrix Cloud.

Passaggi successivi: ordina Citrix DaaS Standard per Azure tramite Citrix o tramite Azure Marketplace.

Se attualmente siete abbonati a Citrix DaaS

Un account Citrix Cloud (OrgID) consente di abbonarsi a una sola edizione di Citrix DaaS alla volta.

È possibile eseguire l'aggiornamento da Citrix DaaS Standard for Azure a una delle seguenti edizioni:

- Edizione Citrix DaaS Advanced
- Edizione Citrix DaaS Premium.

Contattate il vostro rappresentante Citrix per i dettagli.

Se attualmente siete abbonati a un'edizione Citrix DaaS diversa da Advanced o Premium (ad esempio, Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials) e desiderate abbonarvi a Citrix DaaS Standard for Azure, dovete:

- Abbonatevi a Citrix DaaS Standard for Azure utilizzando un altro account Citrix Cloud (OrgID). Per informazioni dettagliate, consultate [Aggiornamento a Citrix DaaS Standard for Azure](#).
- Smantellate il servizio di cui disponete e ordinate Citrix DaaS Standard for Azure. Per istruzioni sul ritiro, vedere [CTX239027](#).

Potete utilizzare una sottoscrizione Citrix Managed Azure acquistando il Citrix Azure Consumption Fund con una delle seguenti edizioni di servizio:

- Citrix DaaS Standard per Azure
- Citrix DaaS Advanced
- Citrix DaaS Advanced Plus
- Citrix DaaS Premium

Ordinare tramite Citrix

Potete ordinare Citrix DaaS Standard for Azure (incluso il fondo di consumo) tramite Citrix Cloud o tramite il vostro rappresentante commerciale Citrix.

Tramite Citrix Cloud:

1. Accedere a [Citrix Cloud](#). Fai clic su **Prova ora** nel riquadro **DaaS Standard for Azure**. Completa le informazioni richieste. Il testo sul riquadro cambia in **Prova richiesta**.

2. Citrix vi contatta. Quando Citrix DaaS Standard for Azure è disponibile per l'uso, il testo nel riquadro cambia in **Gestisci**.
3. Accedere a [Citrix Cloud](#). Nel riquadro **DaaS Standard for Azure**, fai clic su **Gestisci**. La prima volta che accedete a Citrix DaaS Standard for Azure, verrete indirizzati alla pagina di **benvenuto** di Quick Deploy.

Annulare un abbonamento mensile tramite Citrix

Gli abbonamenti mensili si rinnovano automaticamente all'inizio di ogni mese. È possibile utilizzare il dashboard di Citrix DaaS Standard for Azure per annullare una sottoscrizione mensile ordinata tramite Citrix.

(Non è possibile utilizzare il dashboard di Citrix DaaS Standard per Azure per annullare altri tipi di sottoscrizione ordinati tramite Citrix o ordini effettuati tramite Azure Marketplace).

Per annullare un abbonamento mensile:

1. Accedere a [Citrix Cloud](#).
2. Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**.
3. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Generale** a destra.
4. Fai clic su **Annulla abbonamento**.
5. Sono elencate le risorse attive, ad esempio cataloghi, immagini e connessioni. La pagina illustra le azioni intraprese da Citrix durante l'annullamento. Ti informa inoltre delle eventuali azioni che devi intraprendere. Indica il motivo per cui stai annullando il servizio. Se lo si desidera, è possibile fornire ulteriori feedback. Al termine, fai clic su **Annulla abbonamento**.
6. Conferma di aver compreso i termini della cancellazione.

Un banner sulla dashboard di Citrix DaaS Standard for Azure indica la ricezione della richiesta di annullamento.

Se annullate l'abbonamento accidentalmente, contattate il vostro rappresentante commerciale Citrix o il partner Citrix prima della fine del mese per riattivare Citrix DaaS Standard for Azure.

Ordinare tramite Azure Marketplace

Ordinate prima Citrix DaaS Standard per Azure, quindi ordinate il Citrix Azure Consumption Fund.

Non è possibile ordinare il fondo di consumo a meno che non sia stato acquistato in precedenza Citrix DaaS Standard for Azure. Non è possibile combinare Citrix DaaS Standard for Azure e il fondo di consumo in un unico ordine.

Citrix DaaS Standard for Azure non è disponibile tramite il portale dei provider di soluzioni cloud di Azure. Se siete clienti dell'assistenza prioritaria o siete interessati all'assistenza prioritaria, contattate il vostro rappresentante dell'account Citrix.

Requisiti:

- L'OrgID del tuo account Citrix Cloud.
 - Se avete un account Citrix Cloud, ma non conoscete l'OrgID, guardate nell'angolo in alto a destra della console Citrix Cloud. Oppure, guarda l'email che hai ricevuto quando hai creato l'account.
 - Se non disponi di un account Citrix Cloud, segui le indicazioni riportate in Ottenere un account Citrix Cloud.
- Un account di Azure e almeno una sottoscrizione di Azure in tale account.

Ordina Citrix DaaS Standard per Azure tramite Azure Marketplace

1. Accedere ad [Azure Marketplace](#) utilizzando le credenziali dell'account Azure.
2. Cercate e quindi accedete a **Citrix DaaS Standard for Azure**.
3. Fare clic su **OTTIENI SUBITO**.
4. Nel messaggio **Ancora una cosa**, selezionare la casella di controllo e quindi fare clic su **Continua**.
5. Le schede contengono informazioni su prodotto, piani, prezzi e utilizzo. Quando sei pronto, seleziona un piano (se ne sono disponibili più di uno), quindi fai clic su **Configura + iscriviti**.
6. Nella scheda **Basics** (Elementi di base):
 - **Abbonamento**: indica il piano selezionato.
 - **Nome**: inserisci un nome per il tuo ordine di abbonamento.
 - La sezione **Piano** mostra il prezzo per il piano selezionato, in base ai termini mensili e pluriennali (annuali).

Per modificare la durata del piano (mensile o annuale), seleziona **Modifica piano**. Seleziona il termine desiderato e fai clic su **Cambia piano**.
7. Nella scheda **Rivedi + iscriviti** :
 - Controlla i dettagli di contatto forniti in precedenza per il profilo di base di Azure. È possibile modificare l'indirizzo, il numero di telefono o entrambi.
 - Fai clic su **Iscriviti**.
8. Nella pagina **Abbonamento in corso**, fai clic su **Configura account ora**. (Se il pulsante è disabilitato, attendi qualche istante.) Si viene reindirizzato a una pagina di attivazione di Citrix.
9. Nella pagina di attivazione:

- Utilizzate il **link Accedi** per accedere a Citrix Cloud. Un accesso riuscito compila automaticamente il campo **ID organizzazione**.
- **Quantity** (Quantità): immettere il numero di utenti (Un ordine iniziale deve essere di almeno 25.) Viene visualizzato un prezzo stimato.
- Accetta i termini e le condizioni, quindi fai clic su **Attiva ordine**.

Citrix vi 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 Standard for Azure. Ricorda: con solo Citrix DaaS Standard for Azure, puoi usare solo le tue sottoscrizioni di Azure.

Non eliminare la risorsa Citrix DaaS Standard for Azure in Azure. L'eliminazione di tale risorsa annulla l'abbonamento.

Ordina il fondo di consumo tramite Azure Marketplace

1. Accedere ad [Azure Marketplace](#) utilizzando le credenziali dell'account Azure.
2. Cercare e quindi accedere a **Citrix Azure Consumption Fund**.
3. Fare clic su **OTTIENI SUBITO**.
4. Fai clic su **Configura + iscriviti**.
5. Nella pagina **Iscriviti** :
 - In **Nome**, immettere un nome facilmente riconoscibile, ad esempio "Desktop gestiti". È possibile utilizzare questo nome in un secondo momento, se si desidera modificare l'abbonamento al servizio.
 - Indicare il numero di utenti che si desidera supportare, nell'intervallo 25—100000.
 - Inserisci il tuo indirizzo e-mail e il numero di telefono.

Quando hai finito, fai clic su **Iscriviti**.

6. Nella pagina di **avanzamento della sottoscrizione**, quando il pulsante **Configura account SaaS sul sito dell'editore** diventa attivo (blu), fare clic su di esso. Verrete automaticamente indirizzati a una pagina di attivazione dell'ordine Citrix.
7. Nella pagina di attivazione dell'ordine Citrix, immettete Citrix Cloud OrgID. Viene visualizzato l'indirizzo e-mail inserito in precedenza. È possibile modificarlo, se necessario. Quando hai finito, fai clic su **Attiva ordine**.
8. L'evasione dell'ordine del fondo di consumo non richiede molto tempo. Quando Citrix riceve una notifica dell'ordine, nella console di Citrix DaaS for Azure viene visualizzato un banner che indica che è in preparazione una sottoscrizione Citrix Managed Azure.

Il pannello **Sottoscrizioni cloud** a destra della dashboard **Gestisci > Distribuzione rapida di Azure** indica quando la sottoscrizione è pronta per l'uso.

Aumentare o diminuire le postazioni utente tramite Azure Marketplace

Se devi aumentare le postazioni utente, crea un nuovo ordine di Azure Marketplace per il numero aggiuntivo di postazioni che desideri.

Per ridurre il numero di postazioni disponibili, annullare Citrix DaaS Standard for Azure in Azure Marketplace, quindi effettuare un ordine per il numero di postazioni desiderato.

Annullare Citrix DaaS Standard per Azure o il fondo di consumo tramite Azure Market

Per annullare Citrix DaaS Standard for Azure o il fondo di consumo tramite Azure Marketplace:

1. Accedi ad [Azure Marketplace](#).
2. Cerca **DaaS**.
3. Seleziona **Nuovo > Visualizza**.
4. Seleziona la risorsa che desideri annullare.
5. Nel menu con i puntini di sospensione della risorsa, seleziona **Elimina**.
6. Fai clic su **Sì** nella casella di conferma per confermare di conoscere la politica di rimborso e di voler annullare la risorsa.

Importante:

Non annullare il Fondo di consumo di Citrix Azure se si utilizzano risorse gestite da Citrix, come cataloghi o immagini create nella sottoscrizione di Citrix Managed Azure.

Quando il tuo ordine viene approvato ed elaborato

Dopo l'approvazione della versione di prova o del servizio, nella home page di Citrix Cloud vengono visualizzati diversi riquadri:

- Citrix DaaS per Azure
- Citrix DaaS
- portale

Citrix DaaS for Azure è l'unico servizio attivato per il vostro utilizzo.

Per iniziare a usare Citrix DaaS Standard for Azure, accedete a [Citrix Cloud](#). Accedere a Citrix DaaS Standard for Azure utilizzando uno dei seguenti metodi:

- Nel riquadro **DaaS Standard for Azure**, fai clic su **Gestisci**.

- Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**.

Per istruzioni sulla configurazione, vedere Guida [introduttiva](#).

Aggiornamento a Citrix DaaS Standard per Azure

Se al momento avete sottoscritto il servizio Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials, aggiornate a Citrix DaaS Standard per Azure completando le seguenti attività.

1. Creare un nuovo ID organizzativo (OrgID) da utilizzare con Citrix DaaS Standard for Azure all'indirizzo <https://onboarding.cloud.com/>. (Come descritto in precedenza in questo articolo, non è possibile utilizzare lo stesso OrgID per abbonarsi a più di un'edizione Citrix DaaS).
2. Contattate il reparto vendite Citrix per acquistare Citrix DaaS Standard for Azure e il Citrix Azure Consumption Fund, utilizzando il nuovo OrgID. (Non è necessario ordinare il fondo di consumo, ma senza di esso non è possibile accedere a tutte le funzionalità di Citrix DaaS Standard for Azure).
3. Accedere a [Citrix Cloud](#). Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**.
4. [Aggiungete almeno una delle vostre sottoscrizioni Azure](#) a Citrix DaaS Standard for Azure.
5. [Importa una o più immagini dalle tue sottoscrizioni di Azure](#) in Citrix DaaS Standard for Azure.
6. [Crea cataloghi](#) utilizzando le immagini importate dalle sottoscrizioni di Azure.
7. [Aggiungi utenti](#) ai cataloghi che hai creato.
8. Se si desidera mantenere lo stesso URL dell'area di lavoro utilizzato con Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials:
 - a) Accedere a Citrix Cloud utilizzando l'OrgID utilizzato con il servizio Essentials. Selezionare **Configurazione workspace** nel menu in alto a sinistra. [Cambia l'URL dell'area di lavoro](#) in qualcosa di diverso.
 - b) Accedete a Citrix Cloud utilizzando l'OrgID che utilizzate con Citrix DaaS Standard for Azure. Selezionare **Configurazione workspace** nel menu in alto a sinistra. [Modificare l'URL dell'area di lavoro](#) con quello utilizzato in precedenza per il servizio Essentials.
9. Accedi ad Azure ed elimina tutte le risorse utilizzate con il servizio Essentials. Per ulteriori informazioni, vedere [Annullare Virtual Apps Essentials](#). (La procedura è equivalente per Citrix Virtual Desktops Essentials.)
10. Interrompi il servizio Essentials eliminando la risorsa di Azure Marketplace in Azure.

Per iniziare

September 7, 2022

In questo articolo vengono riepilogate le attività di configurazione per la distribuzione di desktop e app utilizzando Citrix Daas Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure service). Ti consigliamo di rivedere ogni procedura prima di eseguirla effettivamente, in modo da sapere cosa aspettarti.

Per le attività di configurazione di Accesso remoto al PC, vedere [Accesso remoto al PC](#).

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 e-mail**.

Riepilogo attività di configurazione

Le seguenti sezioni di questo articolo guidano l'utente attraverso le attività di configurazione:

1. Preparati per l'installazione.
2. Impostare una distribuzione seguendo le indicazioni riportate in uno dei seguenti elementi:
 - Implementazione rapida del proof of concept
 - Implementazione in
3. Fornisci l'URL dell'area di lavoro ai tuoi utenti.

Preparazione

- Se non hai familiarità con cataloghi, immagini, connessioni di rete o sottoscrizioni di Azure, vedere i [concetti introduttivi e le informazioni terminologiche](#).
- Leggete la [panoramica sulla sicurezza](#) per scoprire e capire di cosa siete responsabili voi (il cliente) e Citrix.
- Se non disponi già di un account Citrix Cloud che può essere utilizzato per questo servizio, [procurenene uno e quindi registratevi al servizio](#).
- Esaminare i requisiti di sistema.
- Rivedi le fasi di configurazione: prova di concetto o produzione.

Imposta una rapida implementazione di un proof of concept

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 computer collegati a un dominio, [verificare di disporre di voci valide per il server DNS](#).
3. Se utilizzi la tua sottoscrizione di Azure (invece di una sottoscrizione di Azure gestita da Citrix), [importa la tua sottoscrizione di Azure](#).
4. [Crea o importa 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 multisezione, [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. Notifica agli utenti l'URL dell'area di lavoro.

Dopo aver configurato la distribuzione, utilizzate la dashboard **Monitor** in Citrix DaaS for Azure per vedere l'[utilizzo del desktop](#), [le sessioni](#) e le [macchine](#).

Requisiti di sistema

Per tutte le implementazioni:

- **Citrix Cloud:** questo servizio viene fornito tramite Citrix Cloud e richiede un account Citrix Cloud per completare il processo di onboarding. Per ulteriori informazioni, consultate [Ottenere un account Citrix Cloud](#).
- **Licenze di Windows:** assicurati di avere una licenza appropriata per Servizi Desktop remoto per eseguire carichi di lavoro di Windows Server o Licenze di Desktop virtuale di Azure per Windows 10.

Se utilizzi un abbonamento a Citrix Managed Azure:

- **Sottoscrizioni di Azure quando si utilizza il peering di Azure VNet (facoltativo):** se si prevede di accedere alle risorse (ad esempio AD e altre condivisioni di file) nella propria rete di Azure utilizzando connessioni peer di Azure VNet, è necessario disporre di una sottoscrizione di Azure.
- **Partecipazione di VDA ad Azure Active Directory (facoltativo):** per unire i 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 ulteriori informazioni, vedere [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 desiderate utilizzare le vostre immagini di Azure durante la creazione di un catalogo, tali [immagini devono soddisfare determinati requisiti](#) prima di importarle in Citrix DaaS per Azure.

Informazioni aggiuntive:

- Requisiti di connettività Internet: requisiti di [sistema e connettività](#)
- Limiti di risorse nella distribuzione di un servizio: [limiti](#).

Sistemi operativi supportati

Quando si utilizza un abbonamento a Citrix Managed Azure:

- Windows 7 (VDA deve essere 7.15 LTSR con l'ultimo aggiornamento cumulativo)
- Windows 10 a sessione singola
- Windows 10 multisessione
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (versione minima: VDA 2106)
- Red Hat Enterprise Linux e Ubuntu

Quando si utilizza una sottoscrizione di Azure gestita dal cliente:

- Windows 7 (VDA deve essere 7.15 LTSR con l'ultimo aggiornamento cumulativo)
- 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
- Windows Server 2022 (versione minima: VDA 2106)
- Red Hat Enterprise Linux e Ubuntu

URL dell'area di lavoro

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.

Dalla dashboard **Gestione > Distribuzione rapida di Azure**, visualizza l'URL espandendo **Accesso utente e autenticazione** sulla destra.

È possibile modificare la prima parte dell'URL del workspace in Citrix Cloud. Per istruzioni, vedere [Personalizzare l'URL dell'area di lavoro](#).

Ottieni aiuto

Consulta l'articolo [Risoluzione dei problemi](#).

Se hai ancora problemi con il servizio, apri un ticket seguendo le istruzioni in [Come ottenere assistenza e supporto](#).

Create catalogs (Crea cataloghi)

October 7, 2022

Se utilizzato per desktop e app pubblicati, un catalogo è un gruppo di macchine virtuali identiche. Quando si distribuiscono i desktop, le macchine del catalogo vengono condivise con utenti selezionati. Quando si pubblicano applicazioni, le macchine con più sessioni ospitano applicazioni condivise con utenti selezionati.

Nota:

Per informazioni sulla creazione di cataloghi Remote PC Access, vedere [Accesso remoto al PC](#).

Tipi di macchine

Un catalogo 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 computer, che restituisce il numero totale di sessioni supportate dal catalogo.

Quando si distribuiscono i desktop, i tipi di computer statici e casuali vengono talvolta chiamati “tipi di desktop”.

Modi per creare un catalogo

Esistono diversi modi per creare e configurare un catalogo:

- **Lacreazione rapida** è il modo più veloce per iniziare. Fornite informazioni minime e Citrix DaaS for Azure si occuperà del resto. Un catalogo di creazione rapida è ideale per un ambiente di test o un proof of concept.
- **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 di: immagini preparate da Citrix, immagini importate da Azure o immagini create in Citrix DaaS for Azure 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).	Durante la creazione è possibile configurare un programma di gestione dell'alimentazione.
È necessario utilizzare un abbonamento a Citrix Managed Azure.	Puoi usare Citrix Managed Azure o la tua sottoscrizione di Azure.

Per ulteriori informazioni, vedere:

- Creare un catalogo utilizzando la creazione rapida
- Creare un catalogo utilizzando la creazione personalizzata

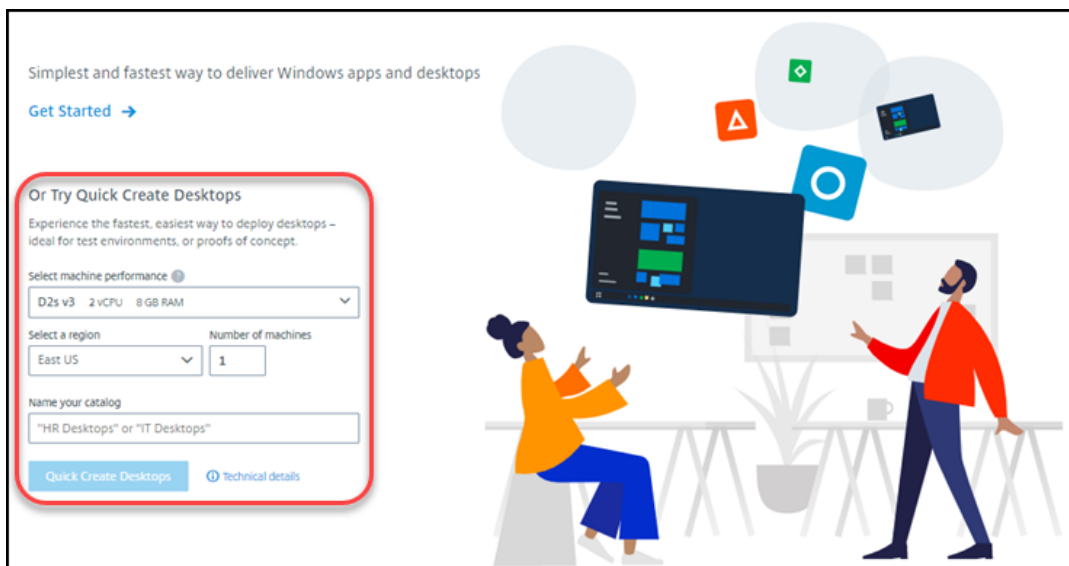
Creare un catalogo utilizzando la creazione rapida

Questo metodo di creazione del catalogo utilizza sempre una sottoscrizione di Citrix Managed Azure.

1. Accedere a [Citrix Cloud](#).
2. Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**.

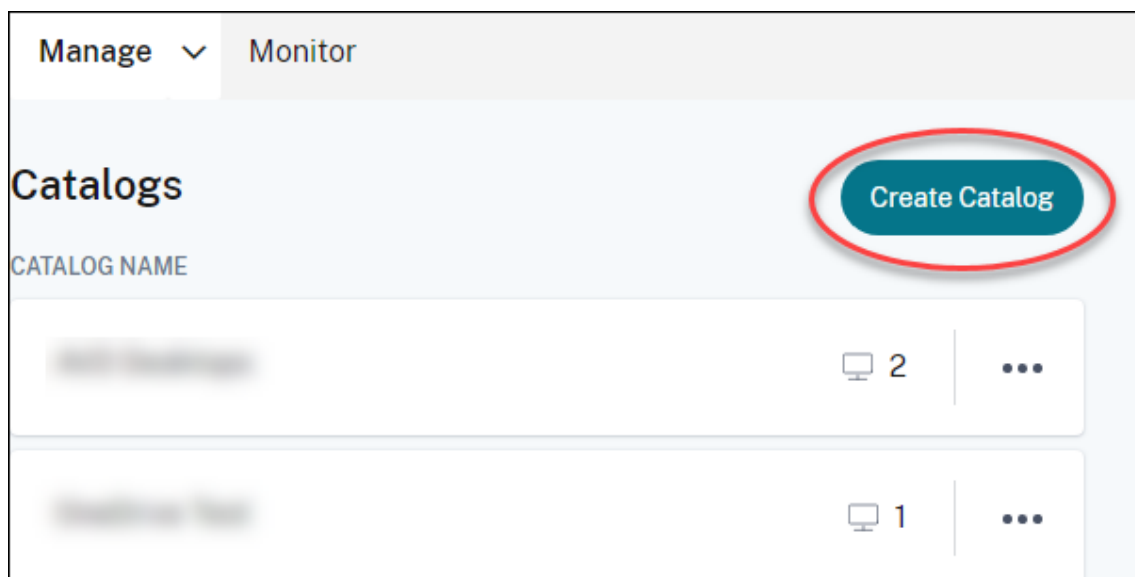
3. Se un catalogo non è ancora stato creato, si sarà reindirizzati alla pagina di **benvenuto** di Quick Deploy. Scegli una delle seguenti opzioni:

- Configurare il catalogo in questa pagina. Continuare con i passaggi da 6 a 10.



- Fare clic su **Inizia**. Verrai indirizzato alla dashboard **Gestisci > Distribuzione rapida di Azure**. Fare clic su **Create Catalog** (Crea catalogo).

4. Se un catalogo è già stato creato (e ne stai creando un altro), verrai indirizzato alla dashboard **Gestisci > Distribuzione rapida di Azure**. Fare clic su **Create Catalog** (Crea catalogo).



5. Fare clic su **Creazione rapida** nella parte superiore della pagina, se non è già selezionata.

Create Catalog

Custom Create **Quick Create**

Select machine performance

D2s v3 2 vCPU 8 GB RAM

Select a region

East US

Name your catalog

Enter a friendly name to identify this group of desktops like "Marketing" or "HR"

"HR Desktops" or "IT Desktops"

Number of machines

1

Quick Create Catalogs Use

- Static machines
- Managed Azure AD
- No connectivity to your corporate network
- Citrix-managed Windows 10 master image
- Cost Saver preset power settings

Create Catalog Cancel Users will be assigned after the machines

- **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.
- **Numero di macchine**: digitare il numero di macchine desiderato.

6. Al termine, fai clic su **Crea catalogo**. (Se si sta creando il primo catalogo dalla pagina **iniziale** di Distribuzione rapida, fare clic su **Desktop di creazione rapida**.)

Verrai indirizzato automaticamente alla dashboard **Gestisci > Distribuzione rapida di Azure**. Durante la creazione del catalogo, il nome del catalogo viene aggiunto all'elenco dei cataloghi, indicando lo stato di avanzamento durante la creazione.

Citrix DaaS for Azure crea anche automaticamente una posizione delle risorse e aggiunge due connettori cloud.

Cosa fare dopo:

- Se si utilizza Citrix Managed Azure AD per l'autenticazione utente, è possibile [aggiungere utenti alla directory](#) durante la creazione del catalogo.

- Indipendentemente dal metodo di autenticazione utente utilizzato, dopo la creazione del catalogo, [aggiungere utenti al catalogo](#).

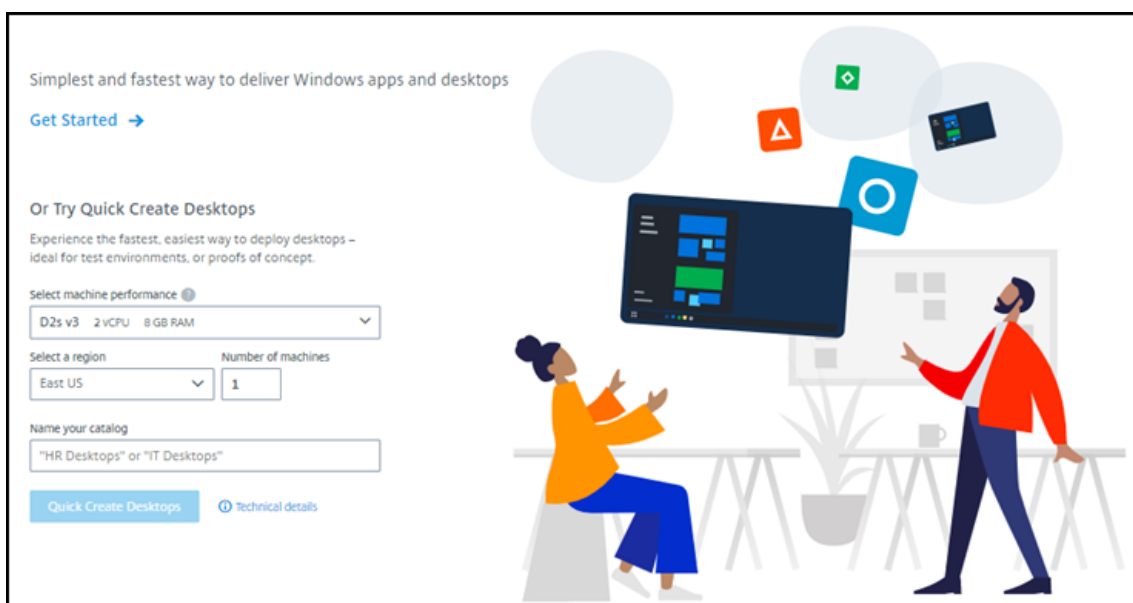
Creare un catalogo utilizzando la creazione personalizzata

Se si utilizza una sottoscrizione di Citrix Managed Azure e si prevede di utilizzare una connessione alle risorse di rete locali, [creare tale connessione di rete](#) prima di creare il catalogo. Per consentire agli utenti di accedere alle risorse locali o ad altre risorse di rete, sono necessarie anche le informazioni di Active Directory per tale posizione.

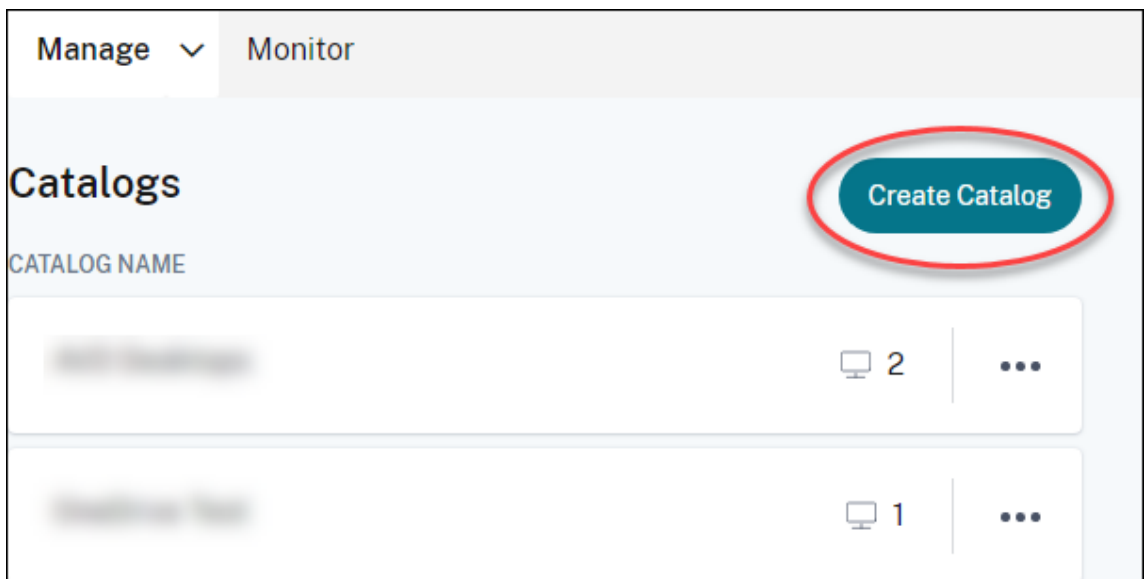
Se non disponete di una sottoscrizione Citrix Managed Azure, dovete [importare \(aggiungere\) almeno una delle vostre sottoscrizioni Azure](#) a Citrix DaaS for Azure prima di creare un catalogo.

Per creare un catalogo:

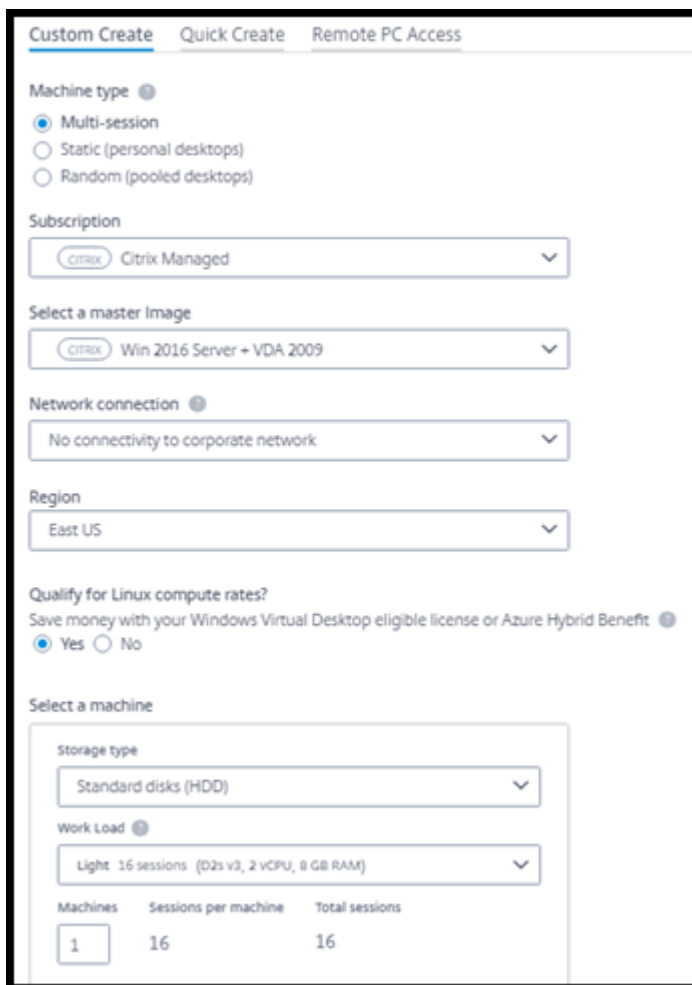
1. Accedere a [Citrix Cloud](#).
2. Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**.
3. Se un catalogo non è ancora stato creato, si sarà reindirizzati alla pagina di **benvenuto** di Quick Deploy. Fare clic su **Inizia**. Alla fine della pagina introduttiva, **accedi alla dashboard Gestisci > Azure Quick Deploy** . Fare clic su **Create Catalog** (Crea catalogo).



Se un catalogo è già stato creato, si passa alla dashboard **Gestisci > Distribuzione rapida di Azure** . Fare clic su **Create Catalog** (Crea catalogo).



4. Seleziona **Crea personalizzata** nella parte superiore della pagina, se non è già selezionata.



5. 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). Seleziona una sottoscrizione di Azure. Per ulteriori informazioni, vedere [Sottoscrizioni di Azure](#).
- **Immagine principale:** selezionare un'immagine del sistema operativo. Per ulteriori informazioni, vedere [Immagini](#).
- **Connessione di rete:** selezionare la connessione da utilizzare per accedere alle risorse della rete. Per ulteriori informazioni, consultate [Connessioni di rete](#).
 - Per una sottoscrizione a Citrix Managed Azure, le opzioni disponibili sono:
 - * **Nessuna connettività:** gli utenti non possono accedere a posizioni e risorse sulla rete aziendale locale.
 - * *Connessioni:* selezionare una connessione, ad esempio un peering VNet o una connessione SD-WAN.
 - Per una sottoscrizione di Azure gestita dal cliente, seleziona il gruppo di risorse, la rete virtuale e la subnet appropriati.
- **Regione:** (disponibile solo se è stata selezionata l'opzione **Nessuna connettività** nella **connessione di rete**) Selezionare un'area in cui si desidera creare i desktop. È possibile selezionare una regione vicina agli utenti.

Se è stato selezionato un nome di connessione in **Connessione di rete**, il catalogo utilizza la regione di tale rete.

- **Qualificati per le tariffe di calcolo Linux?** (Disponibile solo se è stata selezionata un'immagine Windows). Puoi risparmiare denaro utilizzando la licenza idonea o il Vantaggio Azure Hybrid.

Vantaggio Desktop virtuale di Azure: licenze per utente di Windows 10 o Windows 7 idonee 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):
 - **Tipo di archiviazione.** Disco standard (HDD), SSD standard o SSD premium.
 - **Prestazioni della macchina** (per tipo di macchina **statica** o **casuale**) o **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 vuoi in questo catalogo.
- **Schema di denominazione macchina:** vedere Schema di denominazione macchina.
- **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 **Il configure this later** (Da configurare in seguito) è selezionata. Per ulteriori informazioni, vedere [Programmi di gestione dell'alimentazione](#).

6. Al termine, fai clic su **Crea catalogo**.

Il dashboard **Gestisci > Distribuzione rapida di Azure** indica quando viene creato il catalogo. Citrix DaaS for Azure crea anche automaticamente una posizione delle risorse e aggiunge due connettori cloud.

Cosa fare dopo:

- 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).

Creazione di cataloghi di macchine aggiunte a un dominio di Azure AD

Puoi utilizzare la creazione personalizzata per creare cataloghi di macchine unite alla tua Azure Active Directory.

Requisiti

La distribuzione deve includere Citrix Cloud Connectors. Machine Creation Services distribuisce i tuoi connettori cloud in base alle informazioni fornite sul tuo dominio Azure AD quando crei un catalogo.

Questo tipo di catalogo può essere utilizzato solo per il provisioning di macchine statiche o casuali. Al momento il provisioning di macchine multisessione non è supportato.

Non aggiungere l'immagine master ad Azure AD prima di aver creato un catalogo. Citrix MCS unisce l'immagine master ad Azure AD quando il catalogo viene creato.

Utilizzare la versione VDA 2203 o superiore.

Nel portale di Azure, assegnare il ruolo IAM Virtual Machine User Login alle macchine virtuali nel catalogo. Puoi farlo in diversi modi:

- Più sicuro: se si stanno creando macchine statiche, assegnare il ruolo all'utente assegnato alla macchina.
- Metodo alternativo: Assegnare il ruolo sui gruppi di risorse contenenti le macchine virtuali a tutti gli utenti con accesso al catalogo.
- Meno sicuro: Assegnare il ruolo sulle sottoscrizioni, a tutti gli utenti con accesso al catalogo.

Imposta l'autenticazione Workspace per utilizzare Azure AD che stai unendo alle macchine nel catalogo. Per istruzioni, consultate [Configurare l'autenticazione utente in Citrix Cloud](#).

Per ulteriori informazioni sui requisiti, i problemi noti e le considerazioni, vedi le informazioni sulle configurazioni VDA aggiunte ad [Azure AD pure nella configurazione VDA aggiunta ad Azure Active Directory e non dominio](#).

Per creare un catalogo

1. Accedere a [Citrix Cloud](#).
2. Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**.
3. Seleziona **Gestisci > Distribuzione rapida di Azure**.
4. Se un catalogo non è stato ancora creato, si accede alla pagina di **benvenuto**. Seleziona **Inizia**. Alla fine della pagina di introduzione, viene visualizzata la dashboard **Gestione > Azure Quick Deploy**. Seleziona **Crea catalogo**. Se un catalogo è già stato creato, si passa alla dashboard **Gestisci > Distribuzione rapida di Azure**. Seleziona **Crea catalogo**.
5. Seleziona **Crea personalizzata** nella parte superiore della pagina, se non è già selezionata.
6. Completa i seguenti campi.
 - **Tipo di macchina**. Selezionare **Statico (desktop personali)** o **Casuale (desktop in pool)**.
 - **Abbonamento**. Seleziona il tuo abbonamento Azure.
 - **Immagine master**. Selezionare un'immagine del sistema operativo da utilizzare per le macchine nei cataloghi.

- **Connessione di rete.** Selezionare il gruppo di risorse, la rete virtuale e la subnet appropriati.
- **Configurazione del dominio.** Seleziona **Azure Active Directory** come tipo di dominio. Potrebbe apparire un avviso che ti ricorda di impostare l'autenticazione dell'area di lavoro per utilizzare questo Azure AD.

7. Completa il resto della procedura guidata per creare il catalogo.

Impostazioni della posizione delle risorse durante la creazione di un catalogo

Quando si crea un catalogo, è possibile configurare facoltativamente diverse impostazioni di posizione delle risorse.

Quando fate clic su **Impostazioni avanzate** nella finestra di dialogo di creazione del catalogo Quick Deploy, Citrix DaaS for Azure recupera le informazioni sulla posizione delle risorse.

- Se si dispone già di una posizione di risorsa per il dominio e la connessione di rete selezionati per il catalogo, è possibile salvarlo per utilizzarlo 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 della risorsa (se applicabile).

Una volta terminate le impostazioni avanzate, fate clic su **Salva** per tornare alla finestra di dialogo per la creazione del catalogo Distribuzione rapida.

Dopo aver creato un catalogo, sono disponibili diverse azioni relative all'ubicazione delle risorse. 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 mediante Distribuzione rapida, selezionare **Specifica schema di denominazione macchina**. Utilizzare caratteri jolly da 1 a 4 (cancelletto) per indicare la posizione in cui vengono visualizzati 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).
- Una volta che il catalogo contiene 99 macchine, la creazione successiva della macchina non riesce. Il servizio 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 scalare oltre 99 macchine.

Se non specificate uno schema di denominazione delle macchine, Citrix DaaS for Azure utilizza lo schema di denominazione predefinito **DAS%%%%-**-###**.

- **%%%%** = cinque caratteri alfanumerici casuali corrispondenti al prefisso della posizione della risorsa
- ****** = due caratteri alfanumerici casuali per il catalogo
- **###** = tre cifre

Informazioni correlate

- [Macchine unite al dominio e non appartenenti al dominio.](#)
- [Cataloghi Remote PC Access.](#)
- [Crea un catalogo in una rete che utilizza un server proxy.](#)
- [Visualizza le informazioni sul catalogo.](#)

Accesso remoto al PC

October 7, 2022

Introduzione

Nota:

In questo articolo viene descritto come configurare Remote PC Access quando si utilizza l'interfaccia di gestione Quick Deploy in Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure service). Per informazioni sulla configurazione di Accesso remoto al PC quando si utilizza l'interfaccia di gestione della configurazione completa, vedere [Accesso remoto al PC](#).

Citrix Remote PC Access 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 supporta le macchine collegate al dominio.

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) [Configurate un account Citrix Cloud e sottoscrivete il servizio Citrix DaaS Standard for Azure.](#)
 - b) Impostare una posizione delle risorse 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 connettori cloud nella posizione delle risorse.
4. Dall'interfaccia di gestione di Citrix DaaS per Azure Quick Deploy:
 - a) Crea un catalogo Remote PC Access. 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 pre-assegnato.
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.

Generale:

- Le macchine devono eseguire un sistema operativo Windows 10 o Linux (Red Hat Enterprise Linux e Ubuntu) a sessione singola.
- Il computer deve essere unito a un dominio di Servizi di dominio Active Directory.
- Se si ha familiarità con l'utilizzo di Accesso remoto al PC con Citrix Virtual Apps and Desktops, la funzionalità Wake-on-LAN non è disponibile in Citrix DaaS per Azure.

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.
 - Assicurati che i connettori cloud siano raggiungibili 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.
 - Macchine a doppio avvio.
- 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 **Spegni**.
- 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 sganci il laptop, il VDA si registra nuovamente con i connettori cloud tramite Wi-Fi. Tuttavia, quando si riancora il laptop, il VDA non passa all'utilizzo della connessione cablata fino a quando non si scollega l'adattatore wireless. Alcuni dispositivi offrono una funzionalità integrata di disconnessione dell'adattatore 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.

Linux VDA:

- Usare Linux VDA su macchine fisiche solo in modalità non 3D. A causa delle limitazioni del driver NVIDIA, lo schermo locale del PC non può essere oscurato e visualizza le attività della sessione quando la modalità HDX 3D è abilitata. 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 i metodi di assegnazione automatica statici o assegnati 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 Directory), 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 **Diagnostica**, fare clic su **Connetti**. Accertarsi 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 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 opzionali. L'opzione `/includeadditional` specifica esattamente quali componenti si desidera installare.

Ad esempio, il comando seguente impedisce l'installazione di tutti i componenti aggiuntivi facoltativi ad eccezione 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, seleziona **I miei servizi > DaaS Standard for Azure**.
3. Se non hai ancora creato cataloghi, fai clic su **Inizia** nella pagina di **benvenuto** di Quick Deploy. Se hai creato un catalogo, fai clic su **Crea catalogo** nella dashboard **Gestisci > Azure Quick Deploy**.
4. Nella scheda **Remote PC Access** (Accesso remoto PC), selezionare un metodo per assegnare gli utenti alle macchine.
5. Immettere un nome per il catalogo e selezionare la posizione risorsa creata.
6. Aggiungere le macchine.
7. Fare clic su **Create Catalog** (Crea catalogo).
8. Nella pagina **Creazione del catalogo Accesso remoto PC**, fare clic su **Fine**.
9. Una voce per il nuovo catalogo viene visualizzata nella dashboard **Gestisci**.

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**.
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 di Accesso remoto a PC, seleziona il catalogo dalla dashboard **Gestisci > Distribuzione rapida di Azure** (fai clic in un punto qualsiasi della voce).

- 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.

Sottoscrizioni di Azure

December 28, 2023

Introduzione

Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure service) supporta sia le sottoscrizioni Citrix Managed Azure che le vostre sottoscrizioni Azure gestite dal cliente.

- Per utilizzare le proprie sottoscrizioni di Azure, è innanzitutto necessario importare (aggiungere) una o più sottoscrizioni in Citrix DaaS for Azure. Tale azione consente a Citrix DaaS for Azure di accedere alle sottoscrizioni di Azure.

- L'utilizzo di un abbonamento a Citrix Managed Azure non richiede alcuna configurazione di sottoscrizione. Tuttavia, per avere a disposizione una sottoscrizione Citrix Managed Azure, è necessario aver ordinato il Citrix Azure Consumption Fund (in aggiunta a Citrix DaaS Standard for Azure).

Quando crei un catalogo o crei un'immagine, scegli tra le sottoscrizioni di Azure disponibili.

Alcune funzionalità del servizio differiscono a seconda che le macchine siano in una sottoscrizione di Citrix Managed Azure o nella 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 di creazione personalizzati.
Sempre disponibile (ed è la selezione predefinita dell'abbonamento) durante la creazione di cataloghi e immagini.	È necessario aggiungere la sottoscrizione di Azure a Citrix DaaS per Azure prima di creare un catalogo.
Per l'autenticazione utente, supporta Citrix Managed Azure Active Directory o la propria Active Directory.	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 tue reti virtuali.
Quando si utilizza il peering VNet di Azure per connettersi alle risorse, è necessario creare una connessione peer VNet in Citrix DaaS for Azure.	Seleziona 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 nell'abbonamento.

Visualizza gli abbonamenti

Per visualizzare i dettagli della sottoscrizione, dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Sottoscrizioni cloud** a destra. Quindi fai clic su una voce di abbonamento.

- La pagina **Dettagli** include il numero di macchine, più i numeri e i nomi dei cataloghi e delle immagini nell'abbonamento.
- La pagina **Posizioni risorse** elenca le posizioni delle risorse 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 Standard for Azure prima di creare un catalogo o un'immagine che utilizzi 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 privilegi 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 privilegi di proprietario per la sottoscrizione:** prima di aggiungere la sottoscrizione a Citrix DaaS per Azure, creare un'app Azure in Azure AD e aggiungere l'app come collaboratore della sottoscrizione. Quando aggiungete tale sottoscrizione a Citrix DaaS for Azure, fornite informazioni pertinenti sull'app.

Aggiungere sottoscrizioni di Azure gestite dal cliente se si ha il ruolo di amministratore globale

Questa attività richiede privilegi di amministratore globale per la directory e i privilegi di proprietario per la sottoscrizione.

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Sottoscrizioni cloud** sulla destra.
2. Fare clic su **Aggiungi abbonamento di Azure**.
3. Nella pagina **Aggiungi sottoscrizioni**, fai clic su **Aggiungi la sottoscrizione di Azure**.
4. Seleziona il pulsante che consente a Citrix DaaS for Azure di accedere alle tue sottoscrizioni Azure per tuo conto.
5. Fare clic su **Autentica account Azure**. Sei reindirizzato alla pagina di accesso di Azure.
6. Inserisci le credenziali di Azure.
7. Si ritorna automaticamente a Citrix DaaS per Azure. La pagina **Aggiungi sottoscrizione** elenca le sottoscrizioni di Azure rilevate. Utilizzare la casella di ricerca per filtrare l'elenco, se necessario. Seleziona uno o più abbonamenti. Al termine, fai clic su **Aggiungi abbonamenti**.
8. Conferma di voler aggiungere gli abbonamenti selezionati.

Le sottoscrizioni di Azure selezionate vengono elencate quando espandi **Sottoscrizioni**. Le sottoscrizioni aggiunte sono disponibili per la selezione durante la creazione di un catalogo o di un'immagine.

Aggiungi sottoscrizioni di Azure gestite dai clienti se non sei un amministratore globale

L'aggiunta di una sottoscrizione di Azure quando non sei un amministratore globale è un processo in due parti:

- Prima di aggiungere una sottoscrizione a Citrix DaaS for Azure, create un'app in Azure AD e quindi aggiungetela come collaboratore della sottoscrizione.
- Aggiungete la sottoscrizione a Citrix DaaS for Azure, utilizzando le informazioni sull'app creata in Azure.

Crea un'app in Azure AD e aggiungila 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, seleziona **Azure Active Directory**.
 - c) Nell'elenco **Gestisci**, fai clic su **Registrazioni app**.
 - d) Fai clic su **+ Nuova registrazione**.
 - e) Nella pagina **Registrazione di un'applicazione**, fornire le seguenti informazioni:
 - **Nome:** immettere il nome della connessione
 - **Tipo di applicazione:** selezionare **Web app / API** (App web/API)
 - **URI di reindirizzamento:** lascia vuoto
 - f) Fare clic su **Create** (Crea).
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) Annotare l'**ID applicazione** e l'**ID directory**. Lo utilizzerai in seguito quando aggiungerai la tua sottoscrizione a Citrix DaaS per Azure.
 - c) In **Gestisci**, seleziona **Certificati e segreti**.
 - d) Nella pagina **Client secrets** (Segreti del client), selezionare **+ New client secret** (+ Nuovo segreto del client).
 - e) Nella pagina **Aggiungi segreto client**, fornire una descrizione e selezionare un intervallo di scadenza. Quindi fare clic su **Add**.
 - f) Prendi nota del valore segreto del cliente. Lo utilizzerai in seguito quando aggiungerai la tua sottoscrizione a Citrix DaaS per Azure.

- g) Selezionare la sottoscrizione di Azure che si desidera collegare (aggiungere) a Citrix DaaS per Azure, quindi fare clic su **Controllo di accesso (IAM)**.
- h) Nella casella **Aggiungi un'assegnazione di ruolo** fare clic su **Aggiungi**.
- i) Nella scheda **Aggiungi assegnazione ruolo**, selezionare quanto segue:
 - **Role** (Ruolo): collaboratore
 - **Assign access to** (Assegna l'accesso a:) utente, gruppo o entità servizio di Azure AD
 - **Seleziona:** il nome dell'app di Azure creata in precedenza.
- j) Fare clic su **Save** (Salva).

Aggiungete la vostra sottoscrizione a Citrix DaaS per Azure Avrai bisogno dell'ID applicazione, dell'ID della directory e del valore segreto client dell'app creata in Azure AD.

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Sottoscrizioni cloud** sulla destra.
2. Fare clic su **Aggiungi abbonamento di Azure**.
3. Nella pagina **Aggiungi sottoscrizioni**, fai clic su **Aggiungi le sottoscrizioni di Azure**.
4. Seleziona **Ho un'app di Azure con ruolo di collaboratore per la sottoscrizione**.
5. Immettere l'ID tenant (ID directory), l'ID client (ID applicazione) e il segreto client per l'app creata in Azure.
6. Fai clic su **Seleziona l'abbonamento** e quindi seleziona l'abbonamento desiderato.

Successivamente, dalla pagina **Dettagli** della sottoscrizione nella dashboard di Citrix DaaS for Azure, è possibile aggiornare il segreto client o sostituire l'app di Azure dal menu con i puntini di sospensione.

Se Citrix DaaS for Azure non è in grado di accedere a una sottoscrizione di Azure dopo l'aggiunta, non sono consentite diverse operazioni di gestione dell'alimentazione del catalogo e singole macchine. Un messaggio offre la possibilità di aggiungere nuovamente l'abbonamento. Se la sottoscrizione è stata originariamente aggiunta utilizzando un'app Azure, è possibile sostituire l'app Azure.

Aggiungere le sottoscrizioni di Citrix Managed Azure

Una sottoscrizione a Citrix Managed Azure supporta il numero di macchine indicato in [Limiti](#). (In questo contesto, *le macchine* si riferiscono a macchine virtuali su cui è installato Citrix VDA. 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 sei vicino 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 di Citrix Managed Azure supera il valore indicato in [Limiti](#).

Ad esempio, si supponga un limite ipotetico di 1.000 macchine per sottoscrizione di 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. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Sottoscrizioni cloud** sulla destra.
3. Fare clic su **Aggiungi abbonamento di Azure**.

4. Nella pagina **Aggiungi sottoscrizioni**, fare clic su **Aggiungi una sottoscrizione a Citrix Managed Azure**.
5. Nella pagina **Aggiungi un abbonamento gestito Citrix**, fare clic su **Aggiungi abbonamento** nella parte inferiore della pagina.

Se ricevete una notifica che si è verificato un errore durante la creazione di una sottoscrizione a Citrix Managed Azure, contattate il supporto Citrix.

Rimuovi le sottoscrizioni di Azure

Per rimuovere una sottoscrizione di Azure, devi prima eliminare tutti i cataloghi e le immagini che la utilizzano.

Se si dispone di una o più sottoscrizioni di Citrix Managed Azure, non è possibile rimuoverle tutte. Deve rimanerne almeno una.

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Sottoscrizioni cloud** sulla destra.
2. Fai clic sulla voce di abbonamento.
3. Nella scheda **Dettagli**, fai clic su **Rimuovi abbonamento**.
4. Fare clic su **Autentica account Azure**. Sei reindirizzato alla pagina di accesso di Azure.
5. Inserisci le credenziali di Azure.
6. Si ritorna automaticamente a Citrix DaaS per Azure. Confermare l'eliminazione nelle caselle di controllo e quindi fare clic su **Sì, Elimina abbonamento**.

Connessioni di rete

May 9, 2023

Introduzione

In questo articolo vengono fornite informazioni dettagliate su diversi [scenari di distribuzione](#) quando si utilizza una sottoscrizione di Citrix Managed Azure.

Quando si crea un catalogo, si indica se e in che modo gli utenti accedono alle posizioni e alle risorse nella propria rete locale aziendale dai desktop e dalle app Citrix DaaS Standard for Azure (precedentemente Citrix Virtual Apps and Desktops Standard for Azure).

Quando si utilizza una sottoscrizione a Citrix Managed Azure, le opzioni disponibili sono le seguenti:

- No connectivity (Nessuna connettività)
- Azure VNet peering (Peering di Azure VNet)
- SD-WAN

Quando si utilizza una delle proprie sottoscrizioni Azure gestite dal cliente, non è necessario creare una connessione a Citrix DaaS for Azure. È sufficiente [aggiungere la sottoscrizione di Azure a Citrix DaaS for Azure](#).

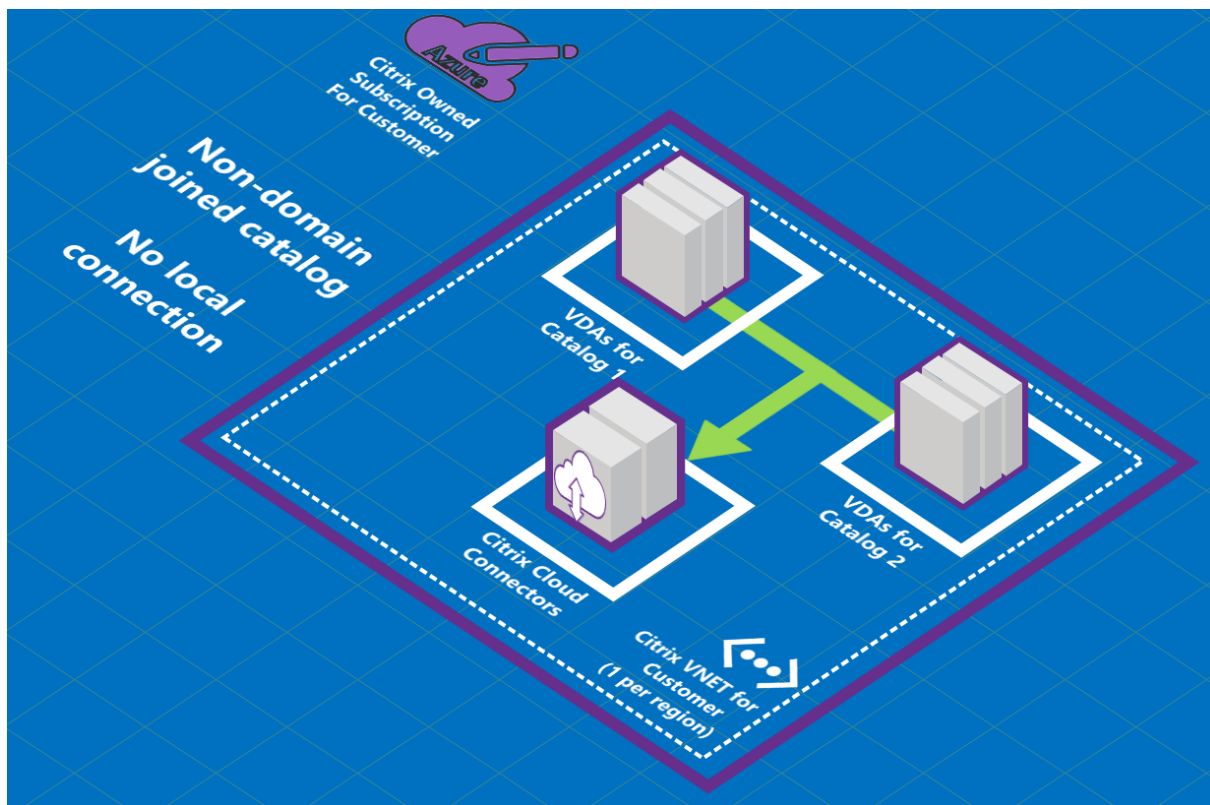
Non è possibile modificare il tipo di connessione di un catalogo dopo la creazione del catalogo.

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 Citrix DaaS per Azure agli indirizzi IP del provider DNS nell'elenco di indirizzi consentiti. L'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)

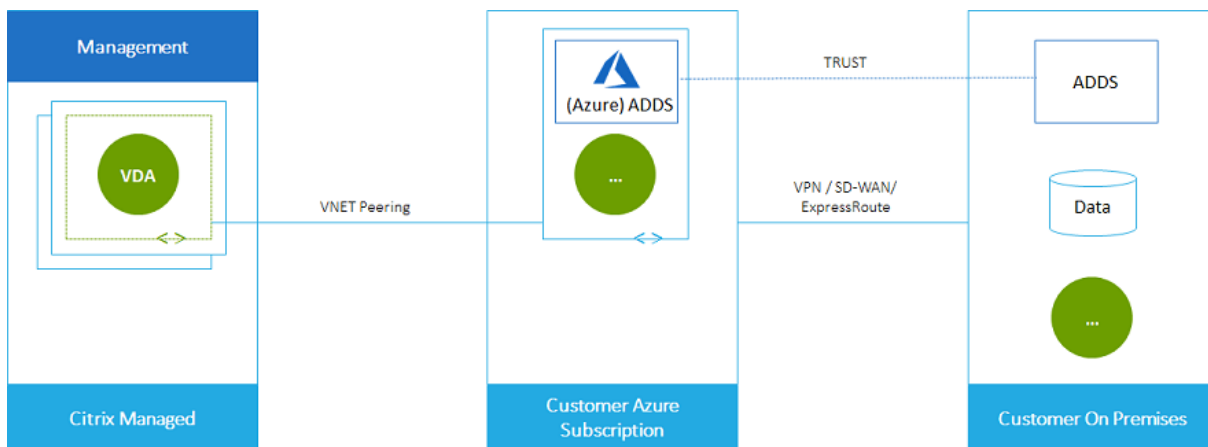
Quando un catalogo è configurato con **No connectivity** (Nessuna connettività), gli utenti non possono accedere alle risorse sulla propria rete on-premise o su altre reti. Questa è l'unica scelta quando si crea un catalogo utilizzando la creazione rapida.



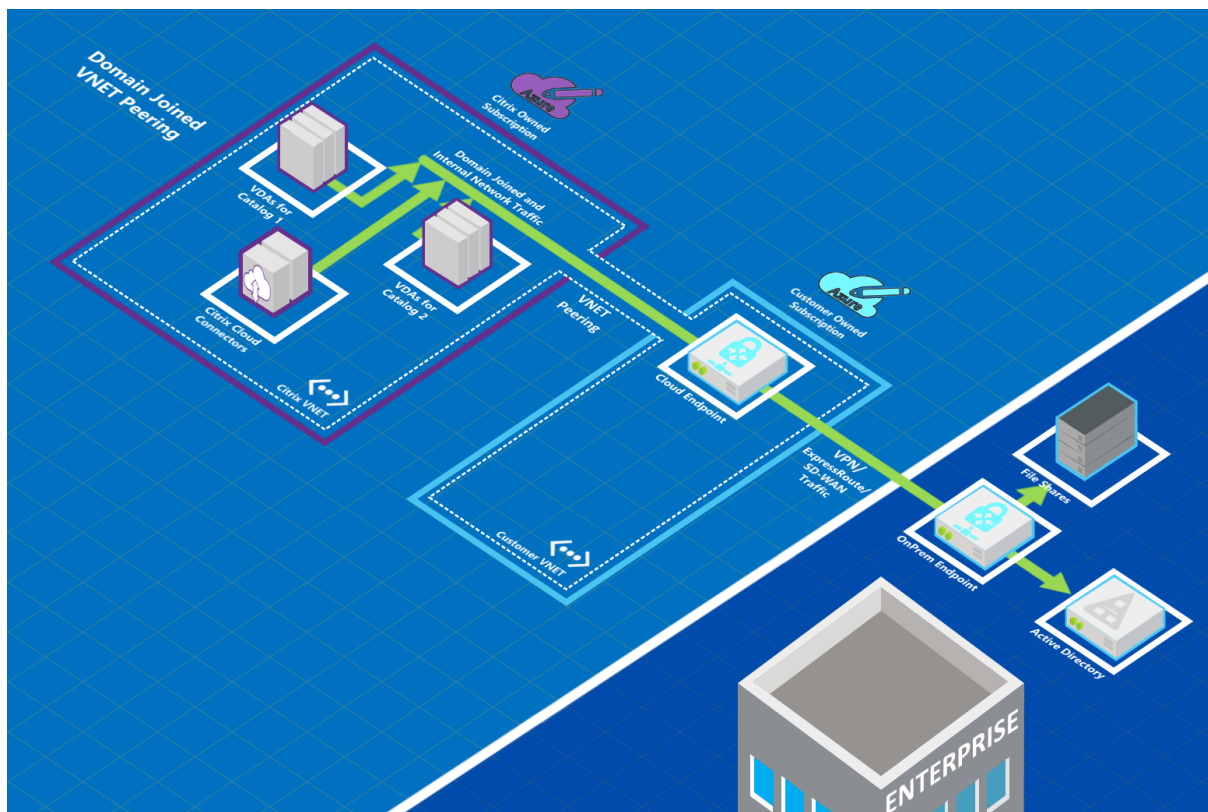
Informazioni sulle connessioni peering di Azure VNet

Il peering della rete virtuale connette senza problemi due reti virtuali (VNET) di Azure: la tua e Citrix DaaS per Azure VNet. Il peering consente inoltre agli utenti di accedere a file e altri elementi dalle reti locali.

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 risorse di rete locali (ad esempio i file server) aggiungendo il dominio locale quando si crea un catalogo. (ovvero, ti unisci al dominio AD in cui risiedono le condivisioni di file e altre risorse necessarie). La sottoscrizione di Azure si connette a tali risorse (nella grafica, utilizzando una VPN o Azure ExpressRoute). Quando si crea il catalogo, si forniscono le credenziali del dominio, dell'unità organizzativa e dell'account.

Importante:

- Scoprite di più sul peering VNet prima di utilizzarlo in Citrix DaaS per Azure.
- Creare una connessione peering VNet prima di creare un catalogo che la utilizzi.

Route personalizzate per il peering della rete virtuale di Azure

I percorsi personalizzati o definiti dall'utente sostituiscono i percorsi di sistema predefiniti di Azure per indirizzare il traffico tra macchine virtuali in un peering VNet, reti locali e Internet. È possibile utilizzare route personalizzate se ci sono reti a cui le risorse di Citrix DaaS for Azure dovrebbero accedere ma non sono collegate direttamente tramite peering VNet. Ad esempio, è possibile creare un percorso personalizzato che impone il traffico attraverso un'appliance di rete verso Internet o verso una subnet di rete locale.

Per utilizzare percorsi personalizzati:

- 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 per Azure.
- Quando si aggiungono route personalizzate, è necessario aggiornare le tabelle di instradamento della propria azienda con le informazioni VNet di destinazione Citrix DaaS for Azure per garantire la connettività end-to-end.
- Le route personalizzate vengono visualizzate in Citrix DaaS for Azure nell'ordine in cui sono state immesse. Questo ordine di visualizzazione non influisce sull'ordine in cui Azure seleziona le rotte.

Prima di utilizzare percorsi personalizzati, vedere l'articolo di Microsoft [Routing del traffico di rete virtuale](#) per informazioni sull'utilizzo di instradamenti personalizzati, tipi di hop successivo e su come Azure seleziona gli instradamenti per il traffico in uscita.

È possibile aggiungere route personalizzate quando si crea una connessione peering VNet di Azure o a percorsi esistenti nel proprio ambiente Citrix DaaS per Azure. Quando si è pronti a utilizzare percorsi personalizzati con il peering VNet, 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 del peering di Azure VNet

- Credenziali per il proprietario di una sottoscrizione di Azure Resource Manager. Deve essere un account di Azure Active Directory. Citrix DaaS for Azure 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:** durante la creazione della connessione, è necessario fornire uno spazio di indirizzi CIDR disponibile (indirizzo IP e prefisso di rete) univoco tra le risorse di rete e le reti virtuali di Azure connesse. Questo è l'intervallo IP assegnato alle VM all'interno della VNet peered di Citrix DaaS per Azure.

Assicurati di specificare un intervallo IP che non si sovrapponga agli indirizzi utilizzati nelle reti di Azure e locali.

- Ad esempio, se la rete virtuale di Azure ha uno spazio di indirizzi di 10.0.0.0 /16, creare la connessione peering VNet in Citrix DaaS per Azure come qualcosa del tipo 192.168.0.0 /24.
- In questo esempio, la creazione di una connessione peering con un intervallo IP 10.0.0.0 /24 sarebbe considerata un intervallo di indirizzi sovrapposto.

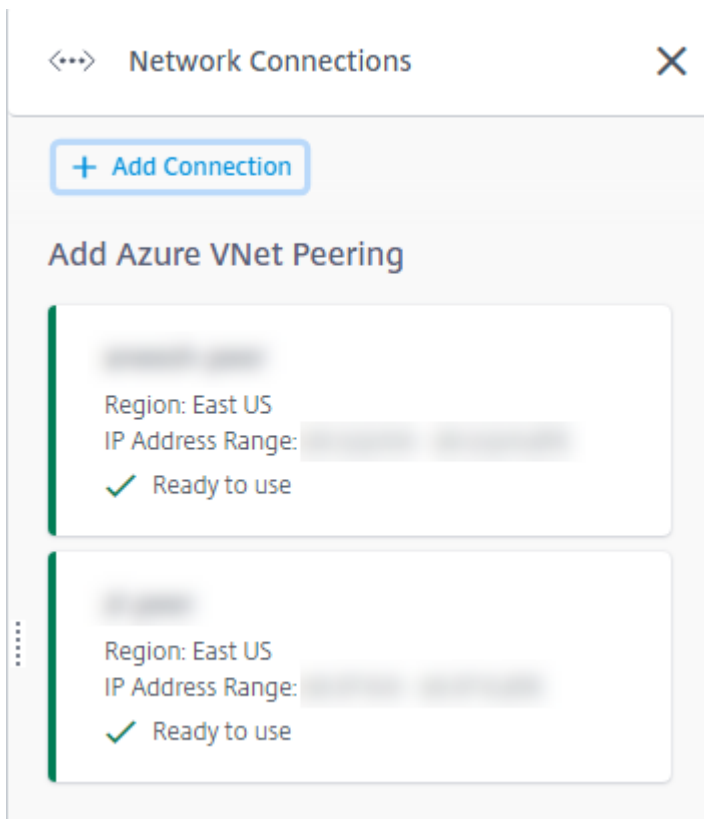
Se gli indirizzi si sovrappongono, la connessione di peering della rete virtuale potrebbe non essere creata correttamente. Inoltre, non funziona correttamente per le attività di amministrazione del sito.

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. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Connessioni di rete** sulla destra. Se sono già impostate delle connessioni, vengono elencate.



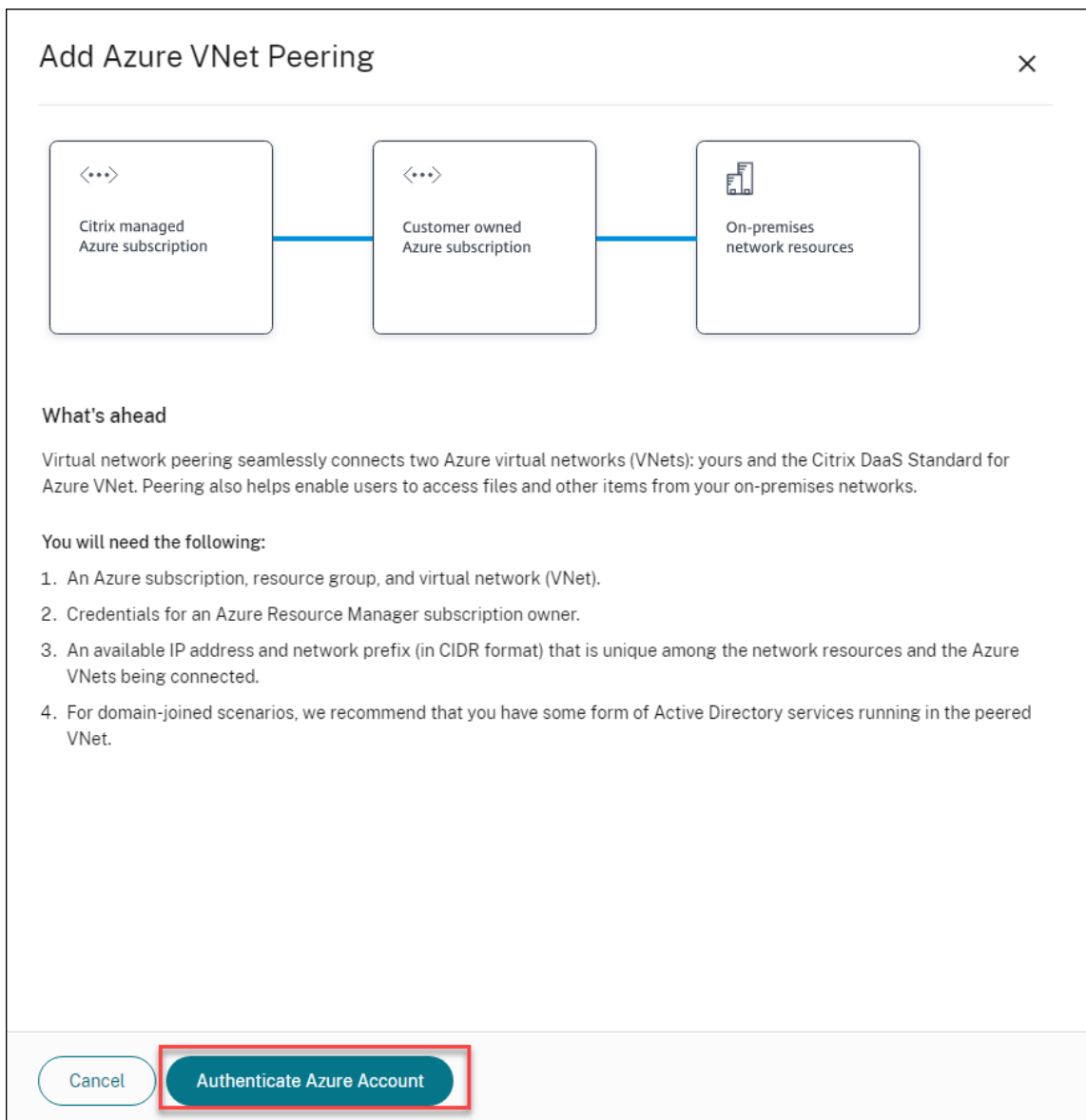
2. Fare clic su **Aggiungi connessione**.
3. Fare clic in un punto qualsiasi della casella **Aggiungi peering di Azure VNet**.

Add a network connection

Choose how you want to connect to your local network:

Add Azure VNet Peering
Easy setup for Azure customers – Seamlessly connect your Azure virtual network.

4. Fare clic su **Autentica account Azure**.



5. Citrix DaaS for Azure ti porta automaticamente alla pagina di accesso di Azure per autenticare le tue sottoscrizioni di Azure. Dopo aver effettuato l'accesso ad Azure (con le credenziali dell'account amministratore globale) e aver accettato i termini, si torna alla finestra di dialogo dei dettagli per la creazione della connessione.

Add Azure VNet Peering

Azure VNet peering name

VNet details to peer

Select Azure Subscription

Select Resource Group

Select VNet to Peer

✓ This VNet is in the West US region, which is supported

Is this VNet using an Azure Virtual Network Gateway?

No Yes

IP address and network prefix to be used by VNet peering ?

⚠ The IP addresses cannot conflict with any existing IP addresses in your network.

/

✓ 10.2.0.0 - 10.2.0.255 (251 addresses available for machines)

Do you want to add routes? ?

No Yes

Cancel

Add VNet Peering

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 di Microsoft [Azure VPN Gateway](#).
9. Se hai risposto **Sì** nel passaggio precedente (la rete virtuale selezionata utilizza un gateway di rete virtuale di Azure), indica se desideri abilitare la propagazione della rotta del gateway di rete virtuale. Se abilitato, Azure apprende automaticamente (aggiunge) tutti i percorsi attraverso il gateway.

È possibile modificare questa impostazione in un secondo momento nella pagina **Details** (Dettagli) della connessione. Tuttavia, la modifica può causare modifiche al modello di percorso e interruzioni del traffico VDA. Inoltre, se lo si disabilita in un secondo momento, è necessario aggiungere manualmente instradamenti alle reti che verranno utilizzate dai VDA.

10. Digitare un indirizzo IP e selezionare una maschera di rete. Viene visualizzato l'intervallo di indirizzi da utilizzare, oltre al numero di indirizzi supportati dall'intervallo. Assicurati che l'intervallo IP non si sovrapponga agli indirizzi utilizzati nelle reti di Azure e locali.
 - Ad esempio, se Azure VNet dispone di uno spazio di indirizzi 10.0.0.0 /16, creare la connessione peering VNet in Citrix Virtual Apps and Desktops Standard come qualcosa come 192.168.0.0 /24.
 - In questo esempio, la creazione di una connessione peering VNet con un intervallo IP 10.0.0.0 /24 sarebbe considerata un intervallo di indirizzi sovrapposto.

Se gli indirizzi si sovrappongono, la connessione di peering VNet 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.

Do you want to add routes? ?

No Yes

i Make sure your company's route tables are updated with the Citrix Managed Desktops VNet information to ensure end-to-end connectivity: 10.2.0.0/24 (provided above).
Added routes override Azure default routing. Routes apply to all connections from machines using this VNet peering.

Route name

USA-traffic

Destination IP address and network prefix ?

10.2.0.0

/ 24 ?

✓ 10.2.0.0 - 10.2.0.255

Next hop type ?

Virtual appliance

Next hop address ?

10.2.0.124

[+ Add route](#)

Per ulteriori informazioni sui tipi di hop successivo, vedere [Instradamenti personalizzati](#) nell'articolo Microsoft [Routing del traffico di rete virtuale](#).

- d) Fare clic su **Aggiungi percorso** per creare un altro percorso personalizzato per la connessione.

12. Fare clic su **Aggiungi peering VNet**.

Una volta creata, la connessione viene elencata in **Connessioni di rete > Peer vNet di Azure** sul lato destro del dashboard **Gestisci > Distribuzione rapida di Azure**. 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

[Blurred text]

Details Routes

Not in use



Catalogs

0

Machines

0

Images

0

Bastions

0

Region

VNet 1 [Blurred]
East US

VNet 2 - CITRIX MANAGED
East US

Allocated Network Space

IP ADDRESS RANGE
[Blurred]

IP ADDRESS AVAILABLE FOR MACHINES
[Blurred]

DNS SERVERS
[Blurred]

Peered Virtual Network Details

VIRTUAL NETWORK
[Blurred]

SUBSCRIPTION ID
[Blurred]

RESOURCE GROUP
[Blurred]

AZURE VIRTUAL NETWORK GATEWAY
Disabled

Delete Connection

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **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 un percorso personalizzato:

1. Dai dettagli della connessione di peering VNet, selezionare **Instradamenti** e quindi fare clic su **Aggiungi percorso**.
2. 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.
3. Indicare se si desidera abilitare la route personalizzata. Per impostazione predefinita, il percorso personalizzato è abilitato.
4. Fai clic su **Aggiungi percorso**.

Per modificare o disabilitare un percorso personalizzato:

1. Dai dettagli della connessione di peering VNet, selezionare **Instradamenti** e quindi individuare il percorso personalizzato che si desidera gestire.
2. Dal menu con i puntini di sospensione, selezionate **Modifica**.

Details **Routes**

Make sure your company's route tables are updated with the Citrix Managed Desktops VNet information to ensure end-to-end connectivity: [redacted] (allocated IP address and network prefix).

Added custom (user-defined) routes override the Azure default routing. Routes apply to connections from all machines using this VNet peering. Custom routes are listed in the order they were created. See the [Microsoft Azure documentation](#) for details about how routes are selected.

Name	Enabled	IP Address/Network Prefix	Next Hop
USA-Traffic	Yes	[redacted]	VnetLocal

3. Apportare le modifiche necessarie all'indirizzo IP e al prefisso di destinazione o al tipo di hop successivo, in base alle esigenze.
4. Per abilitare o disabilitare un percorso personalizzato, in **Abilita questo percorso?**, seleziona **Sì** o **No**.
5. Fare clic su **Save** (Salva).

Per eliminare un percorso personalizzato:

1. Dai dettagli della connessione di peering VNet, selezionare **Instradamenti** e quindi individuare il percorso personalizzato che si desidera gestire.
2. Dal menu con i puntini di sospensione, selezionare **Elimina**.
3. Selezionare **L'eliminazione di un percorso può interrompere le sessioni attive** per riconoscere l'impatto dell'eliminazione del percorso personalizzato.
4. Clicca su **Elimina percorso**.

Eliminare una connessione peering di Azure VNet

Prima di poter eliminare un peer di Azure VNet, rimuovi tutti i cataloghi ad esso associati. Vedere [Eliminare un catalogo](#).

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Connessioni di rete** sulla destra.
2. Selezionare la connessione che si desidera eliminare.
3. Dai dettagli della connessione, fai clic su **Elimina connessione**.

Informazioni sulle connessioni SD-WAN

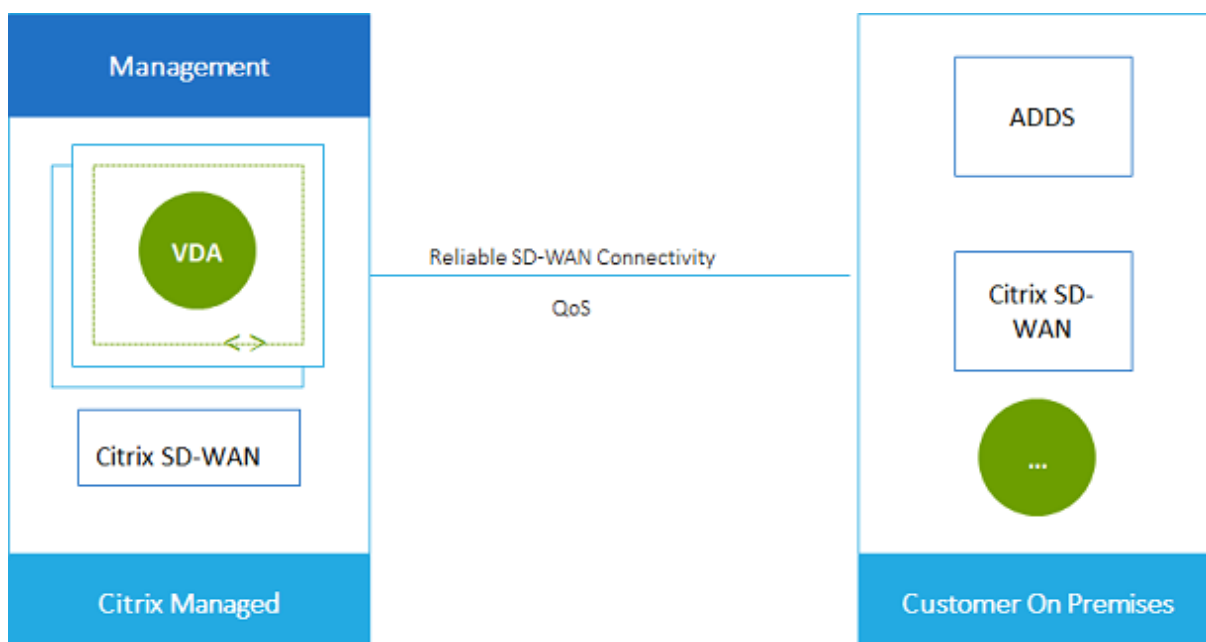
Importante:

Citrix SD-WAN è stato deprecato e tutti i contenuti correlati verranno rimossi dalla documentazione in una versione futura. Si consiglia di passare a soluzioni di rete alternative per garantire l'accesso ininterrotto ai servizi Citrix.

Citrix SD-WAN ottimizza tutte le connessioni di rete necessarie a Citrix Virtual Apps and Desktops Standard for Azure. Lavorando di concerto con le tecnologie HDX, Citrix SD-WAN offre qualità del servizio e affidabilità della connessione per il traffico ICA e Citrix Virtual Apps and Desktops Standard 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 non vengono soddisfatti i seguenti requisiti, l'opzione di connessione di rete SD-WAN non è disponibile.
 - Diritti Citrix Cloud: Citrix Virtual Apps and Desktops Standard per Azure 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 IP VNet: fornisce uno spazio di indirizzi CIDR disponibile (indirizzo IP e prefisso di rete) univoco tra le risorse di rete connesse. Questo è l'intervallo IP assegnato alle VM all'interno di Citrix Virtual Apps and Desktops Standard VNet.

Assicurati di specificare un intervallo IP che non si sovrapponga agli indirizzi utilizzati nelle reti cloud e locali.

- Ad esempio, se la rete dispone di uno spazio di indirizzi di 10.0.0.0 /16, creare la connessione in Citrix Virtual Apps and Desktops Standard come qualcosa come 192.168.0.0 /24.
- In questo esempio, la creazione di una connessione con un intervallo IP 10.0.0.0 /24 sarebbe 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'amministratore di Citrix DaaS for Azure 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 informazioni dettagliate sulla configurazione SD-WAN, vedere [Configurazione SD-WAN per l'integrazione Citrix Virtual Apps and Desktops Standard per Azure](#).

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Connessioni di rete** sulla destra.
2. Fare clic su **Aggiungi connessione**.

3. Nella pagina **Aggiungi una connessione di rete**, fare clic in un punto qualsiasi della casella SD-WAN.
4. La pagina successiva riassume ciò che ci aspetta. Quando hai finito di leggere, fai clic su **Avvia configurazione SD-WAN**.
5. Nella pagina **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. Consulta i requisiti di connessione SD-WAN e la preparazione per informazioni su come evitare conflitti.
6. Quando hai finito, fai clic su **Crea ramo**.
7. Nella pagina successiva vengono riepilogati gli elementi da cercare nel dashboard **Gestisci > Azure Quick Deploy**. Quando hai finito di leggere, fai clic su **Ottenuto**.
8. Nella dashboard **Gestisci > Distribuzione rapida di Azure**, la nuova voce SD-WAN in **Connessioni di rete** mostra l'avanzamento del processo di configurazione. Quando la voce diventa arancione con il messaggio **In attesa di attivazione da parte dell'amministratore SD-WAN**, avvisare l'amministratore di SD-WAN Orchestrator.
9. Per le attività di amministratore di SD-WAN Orchestrator, consultare la [documentazione del prodotto](#) SD-WAN Orchestrator.
10. Al termine dell'amministratore di SD-WAN Orchestrator, la voce SD-WAN in **Connessioni di rete** diventa verde, con il messaggio **È possibile creare cataloghi utilizzando questa connessione**.

Visualizzare i dettagli della connessione SD-WAN

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Connessioni di rete** sulla destra.
2. Seleziona **SD-WAN** se non è l'unica selezione.
3. Fare clic sulla connessione che si desidera visualizzare.

Il display 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. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Connessioni di rete** sulla destra.
2. Seleziona SD-WAN se non è l'unica selezione.
3. Fare clic sulla connessione che si desidera eliminare per espandere i dettagli.
4. Nella scheda **Dettagli**, fare clic su **Elimina connessione**.
5. Confermare l'eliminazione.

Anteprima tecnica di Azure VPN

La funzionalità VPN di Azure è disponibile per l'anteprima tecnica.

Informazioni sulle connessioni gateway VPN di Azure

Una connessione gateway VPN di Azure fornisce un collegamento di comunicazione tra i VDA di Azure gestiti da Citrix (desktop e app) e le risorse della tua azienda, come reti locali o risorse in altre posizioni cloud. È simile alla configurazione e alla connessione a una filiale remota.

La connettività sicura utilizza i protocolli standard del settore Internet Protocol Security (IPSec) e Internet Key Exchange (IKE).

Durante il processo di creazione della connessione:

- Fornite le informazioni che Citrix utilizza per creare il gateway e la connessione.
- Citrix crea un gateway VPN di Azure basato su route da sito a sito. Il gateway VPN forma un tunnel IPSec (Internet Protocol Security) diretto tra la sottoscrizione Azure gestita da Citrix e il dispositivo host della VPN.
- Dopo che Citrix ha creato il gateway e la connessione VPN di Azure, aggiornate la configurazione della VPN, le regole del firewall e le tabelle di instradamento. Per questo processo, utilizzate

un indirizzo IP pubblico fornito da Citrix e una chiave precondivisa (PSK) fornita per creare la connessione.

Un esempio di connessione è illustrato in [Creare una connessione gateway VPN di Azure](#).

Non è necessaria una sottoscrizione di Azure per creare questo tipo di connessione.

È inoltre possibile utilizzare percorsi personalizzati con questo tipo di connessione.

Percorsi personalizzati gateway VPN di Azure

I percorsi personalizzati o definiti dall'utente sostituiscono i percorsi di sistema predefiniti per indirizzare il traffico tra le macchine virtuali nelle reti e Internet. È possibile utilizzare percorsi personalizzati se vi sono reti a cui le risorse Citrix Virtual Apps and Desktops Standard devono accedere ma che non sono direttamente connesse tramite un gateway VPN di Azure. Ad esempio, è possibile creare un percorso personalizzato che impone il traffico attraverso un'appliance di rete verso Internet o verso una subnet di rete locale.

Quando si aggiungono percorsi personalizzati a una connessione, tali percorsi si applicano a tutte le macchine che utilizzano tale connessione.

Per utilizzare percorsi personalizzati:

- È necessario disporre di un gateway di rete virtuale esistente o di un'appliance di rete come Citrix SD-WAN nell'ambiente Citrix Virtual Apps and Desktops Standard.
- Quando aggiungi percorsi personalizzati, devi aggiornare le tabelle dei percorsi della tua azienda con le informazioni sulla VPN di destinazione per garantire la connettività end-to-end.
- I percorsi personalizzati vengono visualizzati nella scheda **Collegamento > Percorsi** nell'ordine in cui sono stati inseriti. Questo ordine di visualizzazione non influisce sull'ordine in cui vengono selezionati i percorsi.

Prima di utilizzare percorsi personalizzati, vedere l'articolo di Microsoft [Routing del traffico di rete virtuale](#) per informazioni sull'utilizzo di instradamenti personalizzati, tipi di hop successivo e su come Azure seleziona gli instradamenti per il traffico in uscita.

Puoi aggiungere route personalizzate quando crei una connessione gateway VPN di Azure o a connessioni esistenti nel tuo ambiente di servizio.

Requisiti e preparazione della connessione al gateway VPN di Azure

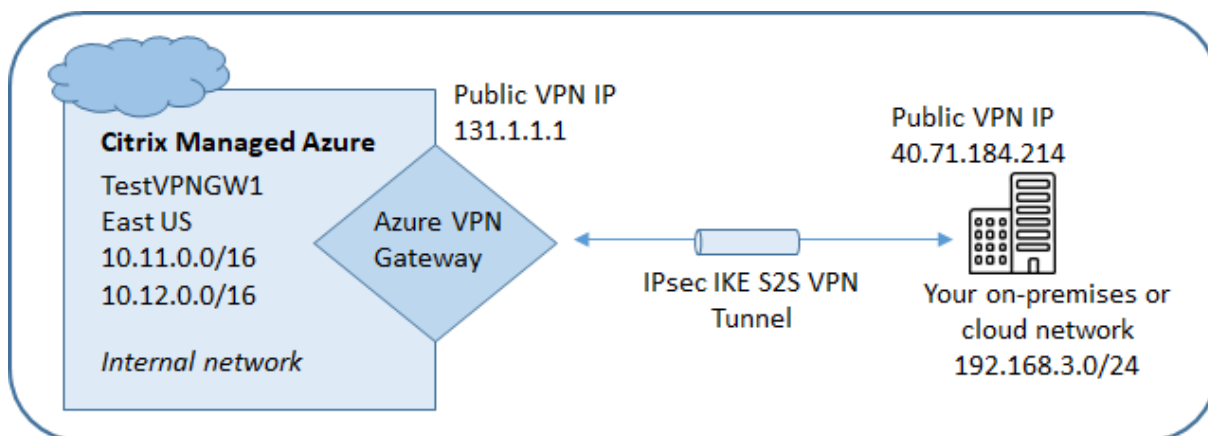
- Per ulteriori informazioni sul gateway VPN di Azure, vedi l'articolo Microsoft [Cos'è il gateway VPN?](#)
- Esamina i requisiti per tutte le connessioni di rete.

- Devi avere una VPN configurata. La rete virtuale deve essere in grado di inviare e ricevere traffico attraverso il gateway VPN. Una rete virtuale non può essere associata a più di un gateway di rete virtuale.
- È necessario disporre di un dispositivo IPsec con un indirizzo IP pubblico. Per informazioni sui dispositivi VPN convalidati, consulta l'articolo di Microsoft [Informazioni sui dispositivi VPN](#).
- Esamina la procedura Crea una connessione al gateway VPN di Azure prima di avviarla effettivamente, in modo da poter raccogliere le informazioni necessarie. Ad esempio, avrai bisogno di indirizzi consentiti nella tua rete, intervalli IP per i VDA e il gateway, il throughput e il livello di prestazioni desiderati e gli indirizzi dei server DNS.

Crea una connessione gateway VPN di Azure

Assicurati di rivedere questa procedura prima di avviarla effettivamente.

Il diagramma seguente mostra un esempio di configurazione di una connessione gateway VPN di Azure. In genere, Citrix gestisce le risorse sul lato sinistro del diagramma e voi gestite le risorse sul lato destro. Alcune descrizioni nella procedura seguente includono riferimenti agli esempi del diagramma.



1. Dalla dashboard **Gestisci** in Citrix DaaS for Azure, espandete **Connessioni di rete** sulla destra.
2. Fare clic su **Aggiungi connessione**.
3. Fai clic in un punto qualsiasi della casella **Gateway VPN di Azure**.
4. Esamina le informazioni nella pagina **Aggiungi connessione VPN**, quindi fai clic su **Avvia configurazione VPN**.
5. Nella pagina **Aggiungi una connessione**, fornire le seguenti informazioni.
 - **Nome:** un nome per la connessione. (Nel diagramma, il nome è TestVpnGW1.)

- **Indirizzo IP VPN:** il tuo indirizzo IP pubblico.

Nel diagramma, l'indirizzo è 40.71.184.214.

- **Reti consentite:** uno o più intervalli di indirizzi a cui il servizio Citrix è autorizzato ad accedere sulla rete. In genere, questo intervallo di indirizzi contiene le risorse a cui gli utenti devono accedere, ad esempio i file server.

Per aggiungere più di un intervallo, fare clic su **Aggiungi altri indirizzi IP** e immettere un valore. Ripetere se necessario.

Nel diagramma, l'intervallo di indirizzi è 192.168.3.0/24.

- **Chiave pre-condivisa:** un valore utilizzato da entrambe le estremità della VPN per l'autenticazione (simile a una password). Decidi tu qual è questo valore. Assicurati di annotare il valore. Ne avrai bisogno in seguito quando configurerai la tua VPN con le informazioni sulla connessione.
- **Prestazioni e velocità effettiva:** il livello di larghezza di banda da utilizzare quando gli utenti accedono alle risorse della rete.

Tutte le scelte non supportano necessariamente il Border Gateway Protocol (BGP). In questi casi, i campi **delle impostazioni BCP** non sono disponibili.

- **Area:** area di Azure in cui Citrix distribuisce macchine che distribuiscono desktop e app (VDA), quando create cataloghi che utilizzano questa connessione. Non è possibile modificare questa selezione dopo aver creato la connessione. Se in seguito si decide di utilizzare una regione diversa, è necessario creare o utilizzare un'altra connessione che specifichi la regione desiderata.

Nel diagramma, la regione è EastUS.

- **Modalità active-active (alta disponibilità):** indica se vengono creati due gateway VPN per un'elevata disponibilità. Quando questa modalità è abilitata, è attivo un solo gateway alla volta. Scopri il gateway VPN di Azure attivo-attivo nel documento Microsoft [Highly Available Cross-Premises Connectivity](#).
- **Impostazioni BGP:** (Disponibile solo se le **prestazioni e il throughput** selezionati supportano BGP). Indica se utilizzare il Border Gateway Protocol (BGP). Scopri di più su BGP nel documento Microsoft: [Informazioni su BGP with Azure VPN Gateway](#). Se abiliti BGP, fornisci le seguenti informazioni:
 - **Numero di sistema autonomo (ASN):** ai gateway di rete virtuale di Azure viene assegnato un ASN predefinito di 65515. Una connessione abilitata per BGP tra due gateway di rete richiede che i relativi ASN siano diversi. Se necessario, è possibile modificare l'ASN ora o dopo la creazione del gateway.

- **Indirizzo IP peering IP BGP:** Azure supporta IP BGP nell'intervallo 169.254.21.x a 169.254.22.x.
- **Subnet VDA:** l'intervallo di indirizzi in cui risiedono Citrix VDA (macchine che forniscono desktop e app) e Cloud Connectors quando si crea un catalogo che utilizza questa connessione. Dopo aver inserito un indirizzo IP e selezionato una maschera di rete, viene visualizzato l'intervallo di indirizzi e il numero di indirizzi supportati dall'intervallo.

Sebbene questo intervallo di indirizzi sia mantenuto nella sottoscrizione di Azure gestita da Citrix, funziona come se fosse un'estensione della rete.

- L'intervallo IP non deve sovrapporsi agli indirizzi utilizzati nelle reti locali o in altre reti cloud. Se gli indirizzi si sovrappongono, la connessione potrebbe non essere stata creata correttamente. Inoltre, un indirizzo sovrapposto non funzionerà correttamente per le attività di amministrazione del sito.
- L'intervallo di subnet VDA deve essere diverso dall'indirizzo della subnet del gateway.
- Non è possibile modificare questo valore dopo aver creato la connessione. Per utilizzare un valore diverso, create un'altra connessione.

Nel diagramma, la sottorete VDA è 10.11.0.0/16.

- **Subnet gateway:** l'intervallo di indirizzi in cui risiederà il gateway VPN di Azure quando crei un catalogo che utilizza questa connessione.
 - L'intervallo IP non deve sovrapporsi agli indirizzi utilizzati nelle reti locali o in altre reti cloud. Se gli indirizzi si sovrappongono, la connessione potrebbe non essere stata creata correttamente. Inoltre, un indirizzo sovrapposto non funzionerà correttamente per le attività di amministrazione del sito.
 - L'intervallo di subnet del gateway deve essere diverso dall'indirizzo della subnet VDA.
 - Non è possibile modificare questo valore dopo aver creato la connessione. Per utilizzare un valore diverso, create un'altra connessione.

Nel diagramma, la sottorete gateway è 10.12.0.9/16.

- **Percorsi:** indica se si desidera aggiungere percorsi personalizzati alla connessione. Se desideri aggiungere percorsi personalizzati, fornisci le seguenti informazioni:
 - Digitare un nome descrittivo per il percorso personalizzato.
 - Immettere l'indirizzo IP di destinazione e il prefisso di rete. Il prefisso di rete deve essere compreso tra 16 e 24.
 - Selezionare un tipo di hop successivo per il punto in cui si desidera che il traffico venga instradato. Se si seleziona **Virtual appliance**, immettere l'indirizzo IP interno dell'appliance. Per ulteriori informazioni sui tipi di hop successivo, vedere [Instradamenti personalizzati](#) nell'articolo Microsoft [Routing del traffico di rete virtuale](#).

Per aggiungere più di un percorso, fai clic su **Aggiungi percorso** e inserisci le informazioni richieste.

- **Server DNS:** inserisci gli indirizzi dei tuoi server DNS e indica il server preferito. Sebbene sia possibile modificare le voci del server DNS in un secondo momento, tenere presente che la loro modifica può potenzialmente causare problemi di connettività per le macchine nei cataloghi che utilizzano questa connessione.

Per aggiungere più di due indirizzi server DNS, fare clic su **Aggiungi DNS alternativo** e quindi immettere le informazioni richieste.

6. Fai clic su **Crea connessione VPN**.

Dopo che Citrix ha creato la connessione, questa viene elencata in **Connessioni di rete > Gateway VPN di Azure** nella dashboard **Gestisci** in Citrix DaaS for Azure. La scheda di connessione contiene un indirizzo IP pubblico. (Nel diagramma, l'indirizzo è 131.1.1.1.)

- Utilizza questo indirizzo (e la chiave pre-condivisa specificata durante la creazione della connessione) per configurare la VPN e i firewall. Se hai dimenticato la chiave già condivisa, puoi modificarla nella pagina **Dettagli** della connessione. Avrai bisogno della nuova chiave per configurare la tua estremità del gateway VPN.

Ad esempio, consentire eccezioni nel firewall per gli intervalli di indirizzi IP della subnet VDA e del gateway configurati.

- Aggiorna le tabelle di route della tua azienda con le informazioni sulla connessione al gateway VPN di Azure per garantire la connettività end-to-end.

Nel diagramma, sono necessarie nuove rotte per il traffico che va da 192.168.3.0/24 a 10.11.0.0/16 e 10.12.0.9/16 (le sottoreti VDA e gateway).

- Se hai configurato percorsi personalizzati, apporta anche gli aggiornamenti appropriati per loro.

Quando entrambe le estremità della connessione sono state configurate correttamente, la voce della connessione in **Connessioni di rete > Gateway VPN di Azure** indica **Pronto all'uso**.

Visualizza una connessione gateway VPN di Azure

1. Dalla dashboard **Gestisci** in Citrix DaaS for Azure, espandete **Connessioni di rete** sulla destra.
2. Seleziona la connessione che desideri visualizzare.

Display:

- La scheda **Dettagli** mostra il numero di cataloghi, macchine, immagini e bastioni che utilizzano questa connessione. Contiene anche la maggior parte delle informazioni configurate per questa connessione.

- La scheda **Percorsi** elenca le informazioni sul percorso personalizzato per la connessione.

Gestisci percorsi personalizzati per una connessione gateway VPN di Azure

In una connessione gateway VPN di Azure esistente, puoi aggiungere, modificare, disabilitare ed eliminare route personalizzate.

Per informazioni sull'aggiunta di route personalizzate quando crei una connessione, vedi Creare una connessione gateway VPN di Azure.

Importante:

la modifica, la disabilitazione o l'eliminazione di percorsi personalizzati modifica il flusso di traffico della connessione e potrebbe interrompere le sessioni utente attive.

1. Dalla dashboard **Gestisci** in Citrix DaaS for Azure, espandete **Connessioni di rete** sulla destra.
2. Seleziona la connessione che desideri visualizzare.
 - Per aggiungere un percorso personalizzato:
 - a) Dalla scheda **Percorsi** della connessione, fai clic su **Aggiungi percorso**.
 - b) 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.
 - c) Indicare se si desidera abilitare la route personalizzata. Per impostazione predefinita, il percorso personalizzato è abilitato.
 - d) Fai clic su **Aggiungi percorso**.
 - Per modificare o abilitare/disabilitare un percorso personalizzato:
 - a) Dalla scheda **Percorsi** della connessione, individua il percorso personalizzato che desideri gestire.
 - b) Dal menu con i puntini di sospensione, selezionate **Modifica**.
 - c) Modificare l'indirizzo IP e il prefisso di destinazione, o il tipo di hop successivo, in base alle esigenze.
 - d) Indicare se si desidera abilitare il percorso.
 - e) Fare clic su **Save** (Salva).
 - Per eliminare un percorso personalizzato:
 - a) Dalla scheda **Percorsi** della connessione, individua il percorso personalizzato che desideri gestire.

- b) Dal menu con i puntini di sospensione, selezionare **Elimina**.
- c) Selezionare **L'eliminazione di un percorso può interrompere le sessioni attive** per riconoscere l'impatto dell'eliminazione del percorso personalizzato.
- d) Clicca su **Elimina percorso**.

Reimposta o elimina una connessione gateway VPN di Azure

Importante:

- Il ripristino di una connessione causa la perdita della connessione corrente ed entrambe le estremità devono ristabilirla. Un reset interrompe le sessioni utente attive.
- Prima di poter eliminare una connessione, eliminate tutti i cataloghi che la utilizzano. Vedere [Eliminare un catalogo](#).

Per ripristinare o eliminare una connessione:

1. Dalla dashboard **Gestisci** in Citrix DaaS for Azure, espandete **Connessioni di rete** sulla destra.
2. Seleziona la connessione che desideri ripristinare o eliminare.
3. Dalla scheda **Dettagli** della connessione:
 - Per ripristinare la connessione, fare clic su **Ripristina connessione**.
 - Per eliminare la connessione, fare clic su **Elimina connessione**.
4. Se richiesto, conferma l'azione.

Creare un indirizzo IP statico pubblico

Se si desidera che tutte le macchine VDA su una connessione utilizzino un singolo indirizzo IP statico pubblico (gateway) in uscita su Internet, abilitare un gateway NAT. È possibile abilitare un gateway NAT per le connessioni a cataloghi che sono aggiunti a domini o non a dominio.

Per abilitare un gateway NAT per una connessione:

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Connessioni di rete** sulla destra.
2. In **Connessioni di rete**, selezionare una connessione in **CITRIX MANAGED** o **AZURE VNET PEERINGS**.
3. Nella scheda dei dettagli della connessione, fare clic su **Abilita gateway NAT**.
4. Nella pagina Abilita gateway NAT, spostare il dispositivo di scorrimento su **Sì** e configurare un tempo di inattività.

5. Clicca su **Conferma modifiche**.

Quando abiliti un gateway NAT:

- Azure assegna automaticamente un indirizzo IP statico pubblico al gateway. (Non è possibile specificare questo indirizzo.) Tutti i VDA in tutti i cataloghi che utilizzano questa connessione utilizzeranno tale indirizzo per la connettività in uscita.
- È possibile specificare un valore di timeout di inattività. Tale valore indica il numero di minuti in cui una connessione in uscita aperta tramite il gateway NAT può rimanere inattiva prima che la connessione venga chiusa.
- È necessario consentire l'indirizzo IP statico pubblico nel firewall.

È possibile tornare alla scheda dei dettagli della connessione per abilitare o disabilitare il gateway NAT e modificare il valore di timeout.

Immagini

October 7, 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.

Immagini preparate da Citrix

Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure) 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
- Windows Server 2022
- Linux Ubuntu (sessione singola e multisessione)

Le immagini preparate da Citrix dispongono di un Citrix Virtual Delivery Agent (VDA) e di strumenti di 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 per Azure. Le immagini fornite da Citrix sono annotate come **CITRIX**.

Puoi anche importare e utilizzare la tua immagine da Azure.

Modalità di utilizzo delle immagini

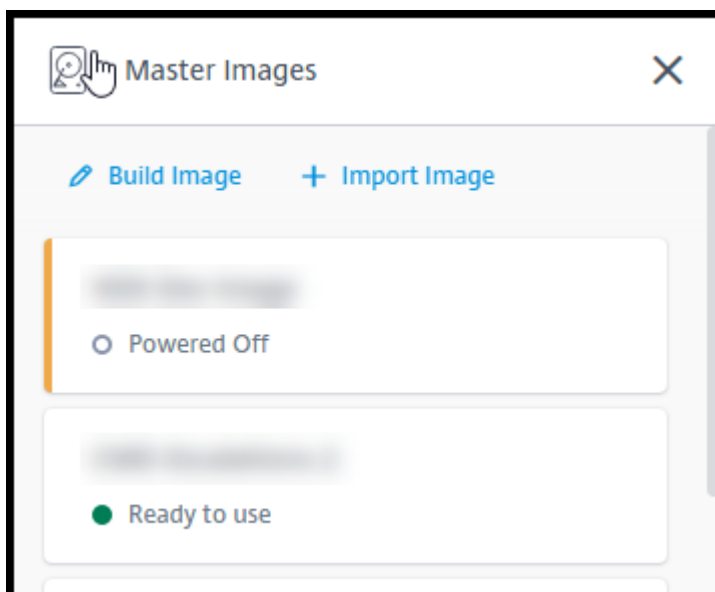
Le opzioni disponibili sono:

- **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 utilizzare l'immagine personalizzata durante la creazione di un catalogo.

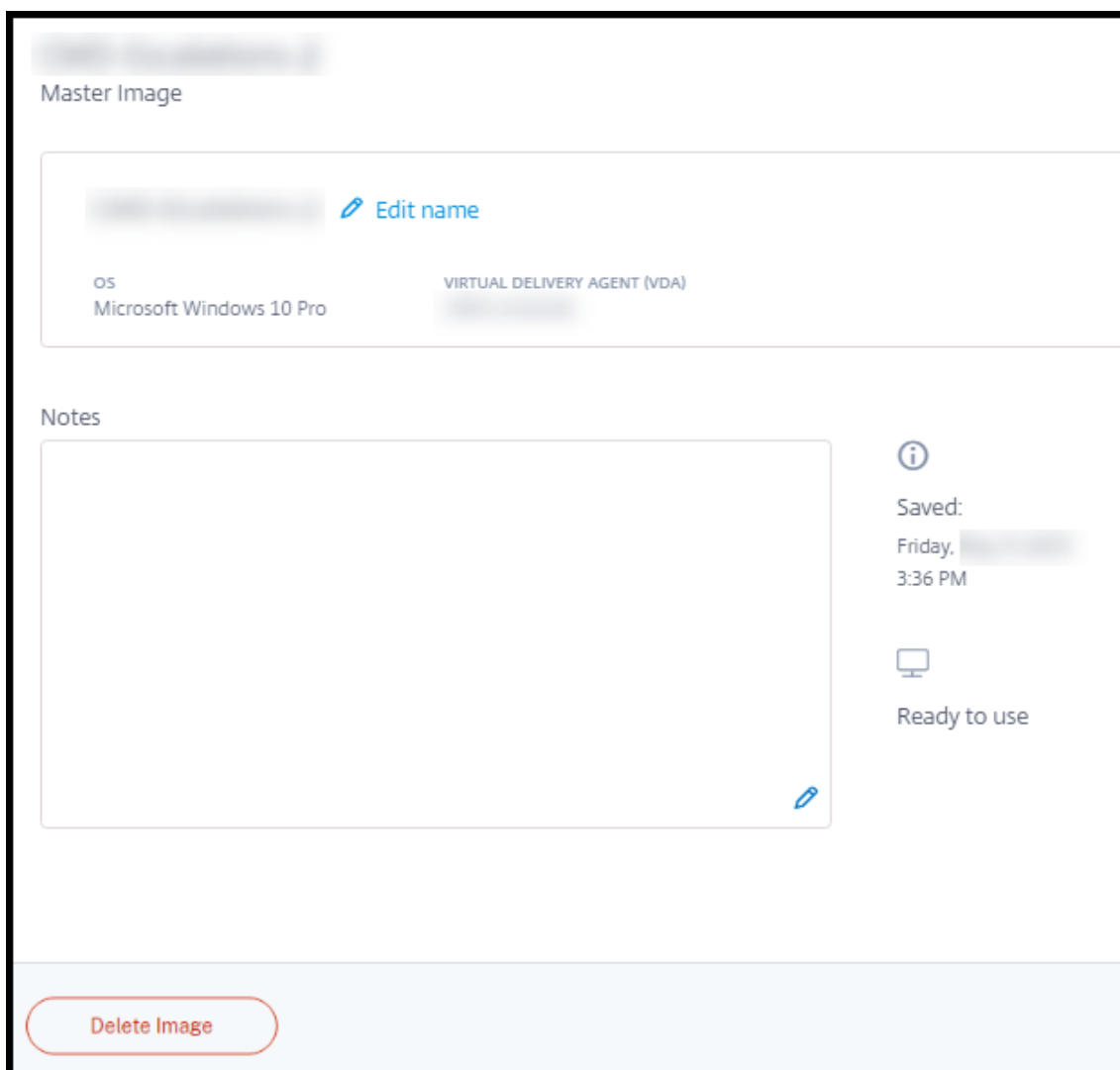
Quando create un catalogo, Citrix DaaS for Azure verifica che l'immagine utilizzi un sistema operativo valido e che disponga di Citrix VDA e di strumenti di risoluzione dei problemi installati (insieme ad altri controlli).

Visualizzare le informazioni sull'immagine

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Immagini master** a destra. Il display elenca le immagini fornite da Citrix e le immagini create e importate.



2. Fare clic su un'immagine per visualizzarne i dettagli.



Dalla scheda dei dettagli è possibile:

- Cambia (modifica) il nome dell'immagine.
- Aggiungere e modificare note (disponibile solo per le immagini preparate o importate, non per le immagini fornite da Citrix).
- Elimina 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. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Immagini master** a destra.
2. Fai clic su **Crea immagine**.

The screenshot shows a web form titled "Name the new master image". The form contains several sections: "Name the new master image" with an empty text input; "Select a master image as base" with a dropdown menu showing "Win 10 EVD (Multi-session) 1909 + Office 365 ProPlus + VC"; "Subscription" with a dropdown menu showing "Citrix Managed"; "Network connection" with a dropdown menu showing "No connectivity to corporate network"; "Region" with a dropdown menu showing "East US"; "Set log-on credentials for the image machine" section containing "Login details for image building machine" with three input fields for "Username", "Password", and "Confirm password"; "Performance (the machine that runs the image)" with a dropdown menu showing "D2s v3 2 vCPU 8 GB RAM"; "Restricted IP access" with a blue link "+ Add IP addresses"; and "Add Notes" with an empty text area.

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.
- **Sottoscrizione**: seleziona una sottoscrizione di Azure. Per ulteriori informazioni, vedere [Sottoscrizioni di Azure](#).
- **Connessione di rete**:
 - Se si utilizza una sottoscrizione Citrix Managed Azure, selezionare **No connectivity** (Nessuna connettività) o una connessione creata in precedenza.
 - Se utilizzi la tua sottoscrizione di Azure gestita dal cliente, seleziona il gruppo di risorse, la rete virtuale e la subnet. Quindi aggiungi i dettagli del dominio: FQDN, OU, nome account di servizio e credenziali.
- **Configurazione del dominio**: Selezionare il tipo di dominio: Active Directory o non appartenente al dominio.

- Se si seleziona Active Directory, selezionare o aggiungere un dominio. Specificare un'unità organizzativa (opzionale), un nome account di servizio e una password.
- Se selezioni non aderito al dominio, non sono necessarie informazioni aggiuntive.
- **Regione:** (disponibile solo per **Nessuna connettività**). Selezionare una 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.
- **Accesso IP limitato:** se si desidera limitare l'accesso a indirizzi specifici, selezionare **Aggiungi indirizzi IP** e quindi immettere uno o più indirizzi. Dopo aver aggiunto gli indirizzi, **fare clic su Fine** per tornare alla scheda **Crea immagine**.
- **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.
- **Join al dominio locale:** indicare se si desidera unirsi al dominio Active Directory locale.
 - Se si seleziona **Sì**, inserire le informazioni di Azure: nome di dominio completo, unità organizzativa, nome account di servizio e credenziali.
 - Se si seleziona **No**, immettere le credenziali per il computer host.

4. Quando hai finito, fai clic su **Crea immagine**.

La creazione di un'immagine può richiedere fino a 30 minuti. Nella dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Immagini master** sulla destra per visualizzare lo stato corrente (ad esempio **Immagine creazione** o **Pronto per la personalizzazione**).

Azione successiva: connettersi a una nuova immagine e personalizzarla.

Connettiti a una nuova immagine e personalizzala

Dopo la creazione di una nuova immagine, il suo nome viene aggiunto all'elenco delle immagini, con lo stato **Pronto per la personalizzazione** (o una formulazione simile). Per personalizzare l'immagine, devi prima scaricare un file RDP. Quando si utilizza quel file per connettersi all'immagine, è possibile aggiungere applicazioni e altro software all'immagine.

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Immagini master** a destra. Fai clic sull'immagine a cui vuoi connetterti.

2. Fai clic su **Scarica file RDP**. Download di 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 ciò accade, fai clic su **Accensione**.

3. Fare doppio clic sul client RDP scaricato. Tenta automaticamente di connettersi all'indirizzo della macchina che contiene 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. Al termine della personalizzazione della nuova immagine, torna alla casella **Immagini master** e fai clic su **Fine build**. La nuova immagine viene sottoposta automaticamente a test di convalida.

Successivamente, quando si crea un catalogo, la nuova immagine viene inclusa nell'elenco delle immagini che è possibile selezionare.

Nella dashboard **Gestisci > Distribuzione rapida**, le immagini visualizzate a destra indicano il numero di cataloghi e macchine che utilizzano ciascuna immagine.

Nota:

Dopo aver finalizzato un'immagine, non è possibile modificarla. È necessario creare una nuova immagine (utilizzando l'immagine precedente come punto di partenza) e quindi aggiornare la nuova immagine.

Importa 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:

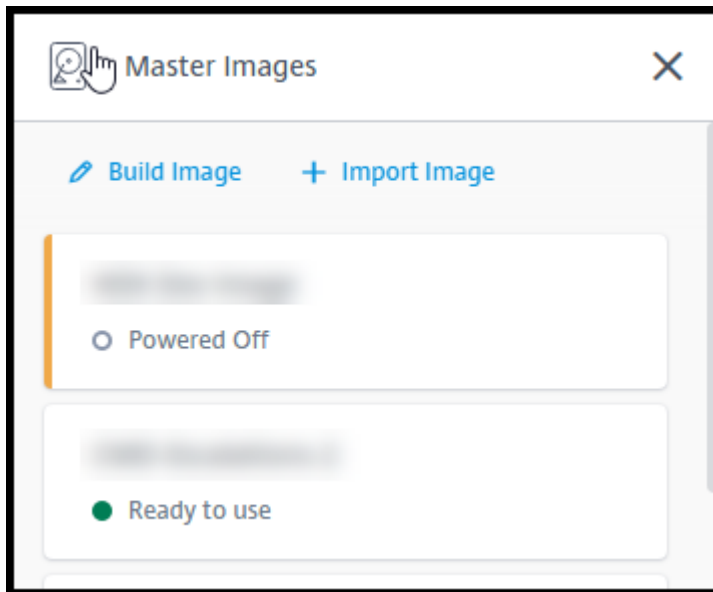
Citrix DaaS for Azure non supporta l'importazione di dischi associati alle macchine virtuali di seconda generazione di Azure.

Citrix esegue test di convalida sull'immagine importata. Assicuratevi che i seguenti requisiti siano soddisfatti quando preparate l'immagine da importare in Citrix DaaS per Azure.

- **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 di Microsoft [Panoramica di Azure Virtual Machine Agent](#).

Importa l'immagine

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Immagini master** a destra.



2. Fai clic su **Importa immagine**.

Choose how to import your image

Browse storage account
 Use Azure public URL

Subscription
[Dropdown menu]

Choose resource group
[Dropdown menu]

Storage account
[Dropdown menu]

Choose master image
[Dropdown menu]

Master image type
 Windows
 Linux

Name the new master image
[Text input field: Eg. "Windows 10 + My Apps"]

Add Notes
[Text area: Enter notes here (up to 1024 characters). You can see and change them in the image's details.]

3. Scegliere come importare l'immagine.

- Per i dischi gestiti, utilizzare la funzionalità di esportazione per generare un URL SAS. Im-

postare 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** (Sfoggia 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) Immettete l'URL generato da Azure per il disco rigido virtuale. Per informazioni, fai clic sul collegamento al documento Microsoft [Scarica un disco rigido virtuale Windows da Azure](#).
- b) Seleziona un abbonamento. (un'immagine Linux può essere importata solo se si seleziona una sottoscrizione gestita dal cliente).
- c) Assegna un nome all'immagine.

6. Quando hai finito, fai clic su **Importa immagine**.

Aggiorna un catalogo con una nuova immagine

Il tipo di catalogo determina quali macchine vengono aggiornate quando si aggiorna il catalogo.

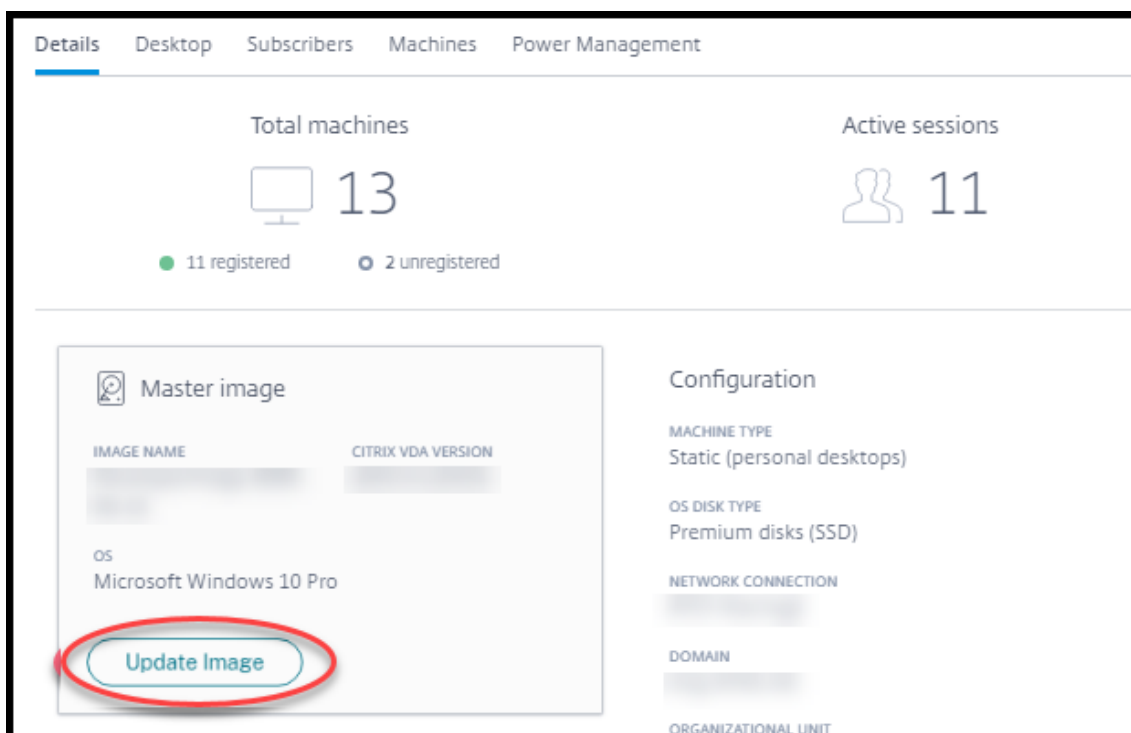
- Per un catalogo casuale, tutte le macchine attualmente presenti nel catalogo vengono aggiornate con l'immagine più recente. Se si aggiungono altri desktop a tale catalogo, si basano sull'immagine più recente.
- Per un catalogo statico, le macchine attualmente presenti nel catalogo non vengono aggiornate 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 **Gestisci > Distribuzione rapida di Azure**, fai clic in un punto qualsiasi della voce del catalogo.

2. Nella scheda **Dettagli**, fai clic su **Aggiorna immagine**.



3. Selezionare un'immagine.
4. Per cataloghi casuali o multisessione: selezionare un intervallo di disconnessione. Dopo che Citrix DaaS for Azure ha completato l'elaborazione iniziale delle immagini, i sottoscrittori ricevono un avviso per salvare il lavoro e disconnettersi dai desktop. L'intervallo di disconnessione indica il tempo trascorso dagli abbonati dopo aver ricevuto il messaggio fino al termine automatico della sessione.
5. Fai clic su **Aggiorna immagine**.

Eliminazione di un'immagine

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Immagini master** a destra.
2. Fare clic sull'immagine che si desidera eliminare.
3. Fai clic su **Elimina immagine** nella parte inferiore della scheda. Confermare l'eliminazione.

Installare un Windows VDA su un'immagine

Utilizzate la procedura seguente per preparare un'immagine Windows che intendete importare in Citrix DaaS per Azure. 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 collegamento **Download** nella barra di navigazione di Citrix Cloud. Oppure, utilizzate un browser per accedere alla pagina di [download](#) di Citrix DaaS per Azure.

Scarica un VDA sulla VM. 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 **Ambiente**, selezionare l'opzione per creare un'immagine utilizzando MCS, quindi fare clic su **Avanti**.
5. Nella pagina **Componenti principali**, fare clic su **Avanti**.
6. Nella pagina **Delivery Controller**, selezionare **Consenti a Machine Creation Services di farlo automaticamente**, quindi fare clic su **Avanti**.
7. Lasciate le impostazioni predefinite nelle pagine **Componenti aggiuntivi**, **Funzionalità Firewall**, a meno che Citrix non vi indichi diversamente. Fare clic su **Avanti** in ogni pagina.
8. Nella pagina **Riepilogo**, fai clic su **Installa**. I prerequisiti iniziano l'installazione. Quando viene richiesto il riavvio, procedere.
9. L'installazione del VDA riprende automaticamente. L'installazione dei prerequisiti viene completata e successivamente vengono installati i componenti e le funzionalità. Nella pagina **Call Home**, lasciare l'impostazione predefinita (a meno che Citrix non indichi diversamente). Dopo aver effettuato la connessione, fare clic su **Avanti**.
10. Fare clic su **Finish**. Il computer si riavvia automaticamente.
11. Per assicurarsi che la configurazione sia corretta, avviare una o più applicazioni installate sulla macchina virtuale.
12. Spegnerne la macchina virtuale. Non eseguire il Sysprep dell'immagine.

Per ulteriori informazioni sull'installazione dei VDA, vedere [Installare i VDA](#).

Utenti e autenticazione

December 28, 2023

Metodi di autenticazione utente

Gli utenti devono autenticarsi quando accedono a Citrix Workspace per avviare il desktop o le app.

Citrix DaaS for Azure supporta i seguenti metodi di autenticazione utente:

- **Managed Azure AD:** Managed Azure AD è un Azure Active Directory (AAD) fornito e gestito 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.

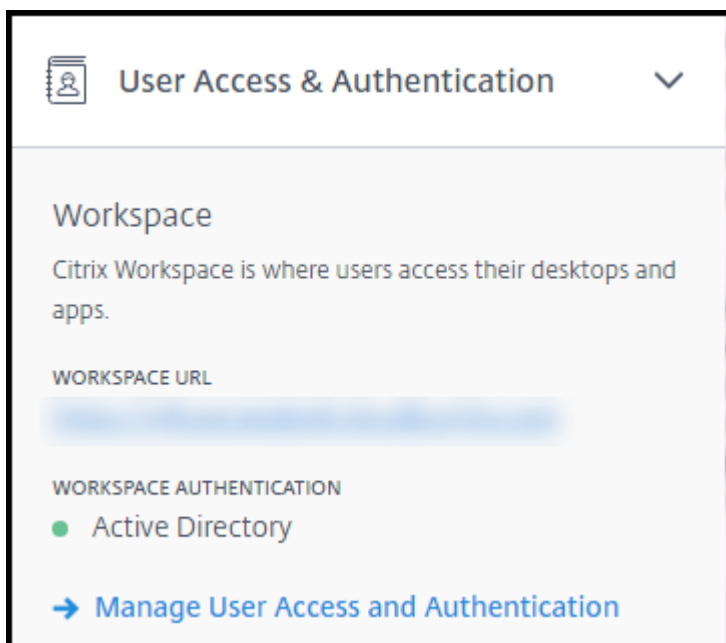
Nota:

Il metodo di autenticazione Managed Azure AD è configurato per impostazione predefinita. Cioè, è connesso automaticamente in Citrix Cloud e l'autenticazione Workspace è impostata automaticamente per l'utilizzo di Managed Azure AD for Citrix DaaS for Azure. 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.

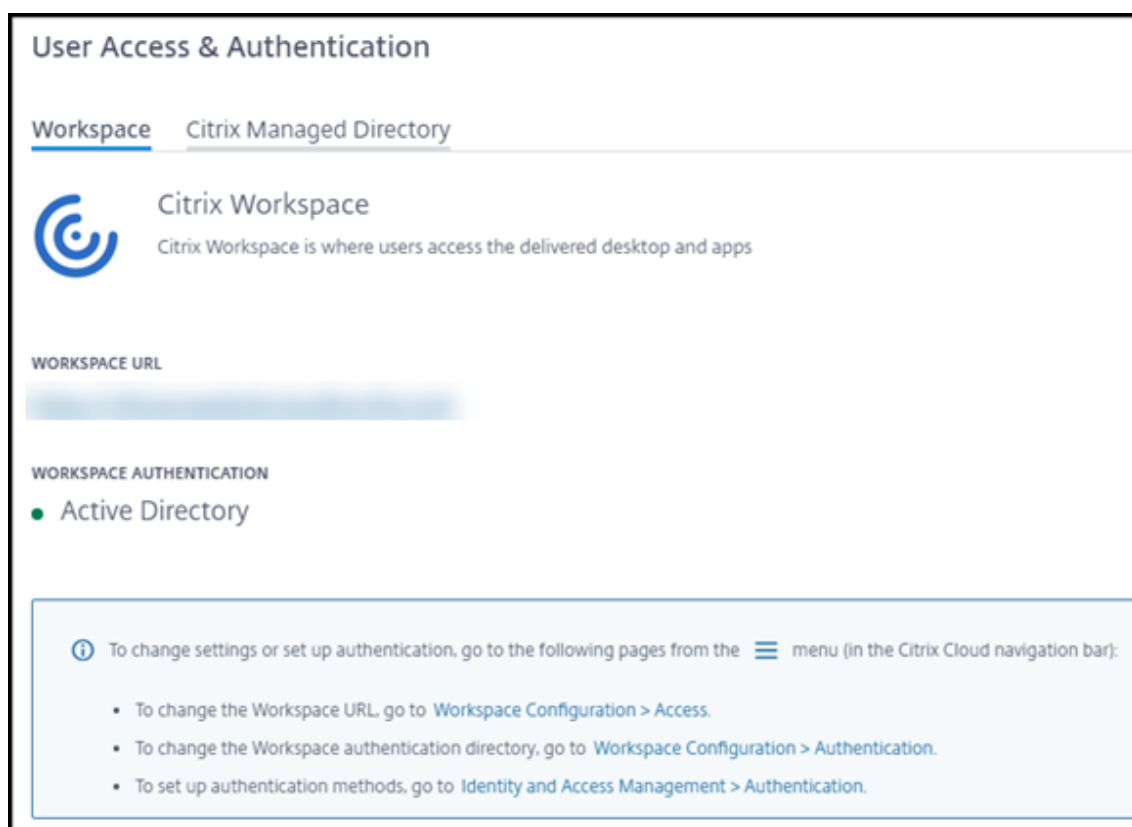
Se Managed Azure AD è disconnesso, l'autenticazione di Workspace passerà ad Active Directory. Se si desidera utilizzare un metodo di autenticazione diverso, procedere nel modo seguente.

Per modificare il metodo di autenticazione:

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, fai clic su **Accesso e autenticazione utente** a destra.



2. Fare clic su **Gestisci accesso e autenticazione degli utenti**. Selezionare la scheda **Area di lavoro**, 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.

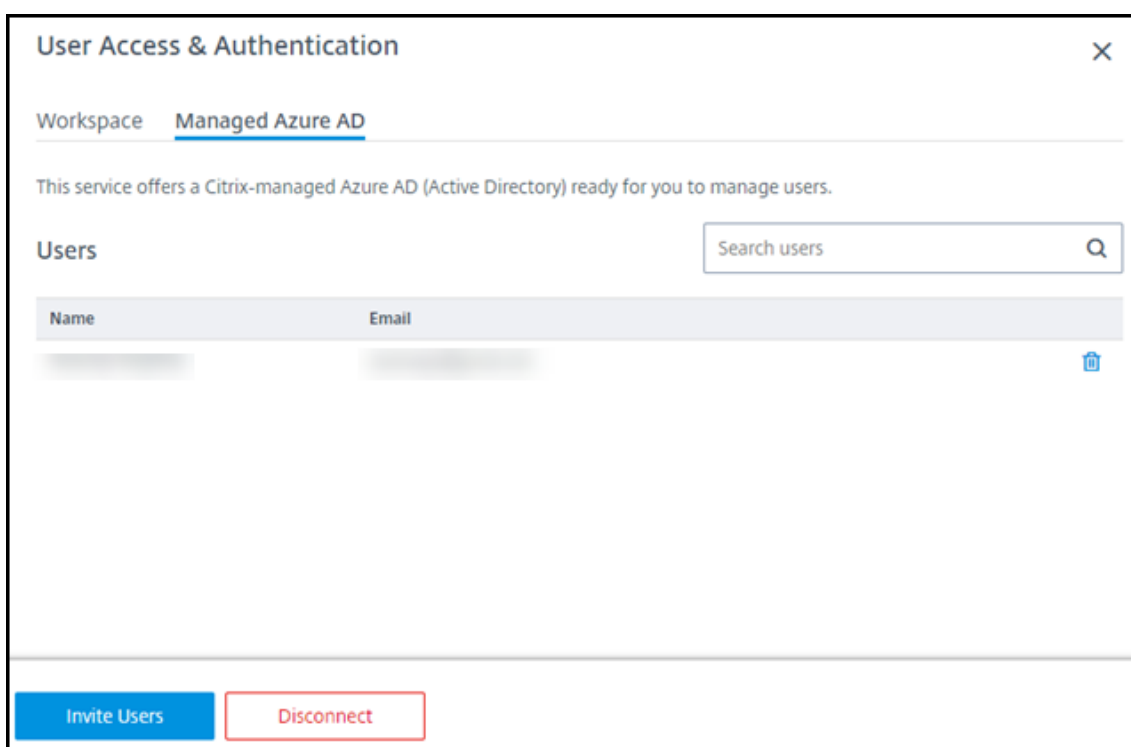
Fornire il nome e gli indirizzi e-mail dei propri utenti. Citrix invia quindi un invito via e-mail a ciascuno di essi. L'e-mail indica agli utenti di fare clic su un collegamento che li unisce a Citrix Managed Azure AD.

- Se l'utente dispone già di un account Microsoft con l'indirizzo e-mail fornito, viene utilizzato tale account.

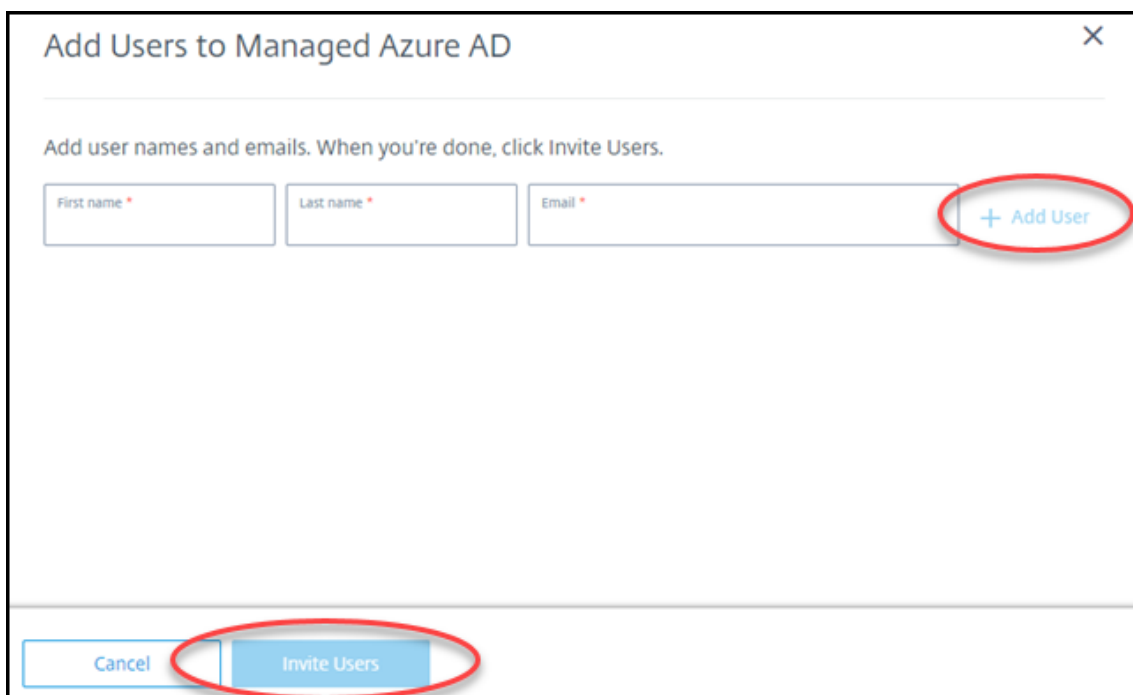
- Se l'utente non dispone di un account Microsoft con l'indirizzo e-mail, Microsoft crea un account.

Per aggiungere e invitare utenti a Managed Azure AD:

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Accesso utente e autenticazione** a destra. Fare clic su **Gestisci accesso e autenticazione degli utenti**.
2. Fai clic sulla scheda **Managed Azure AD**.
3. Fai clic su **Invita utenti**.



4. Digitare il nome e l'indirizzo e-mail di un utente, quindi fare clic su **Aggiungi utente**.



5. Ripetere il passaggio precedente per aggiungere altri utenti.
6. Quando hai finito di aggiungere le informazioni utente, fai clic su **Invita utenti** nella parte inferiore della scheda.

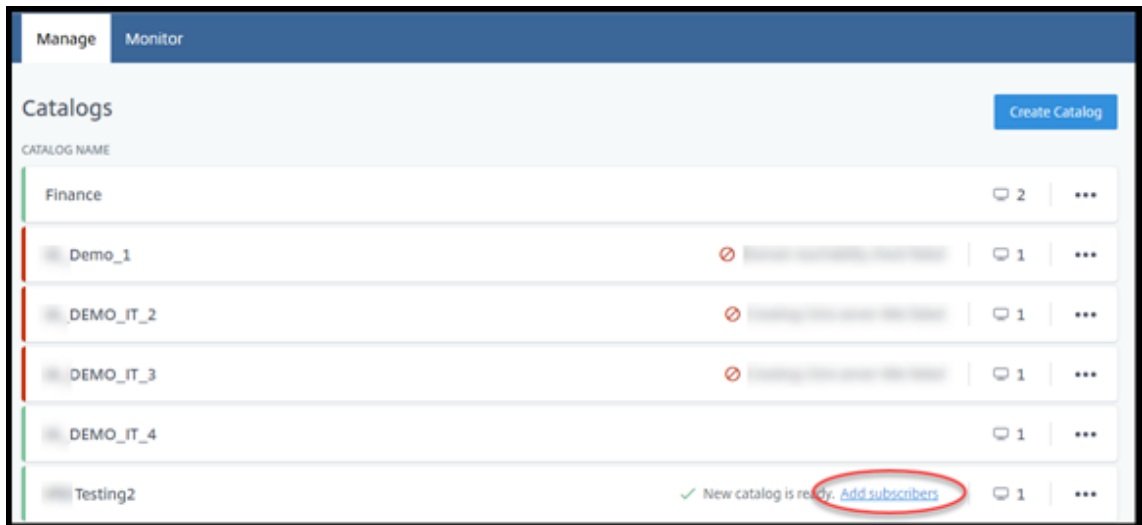
Per eliminare un utente da Managed Azure AD, fai clic sull'icona del cestino accanto al nome dell'utente che desideri eliminare dalla directory. Confermare l'eliminazione.

Passaggio successivo: aggiungere utenti al catalogo

Aggiungere o rimuovere utenti in un catalogo

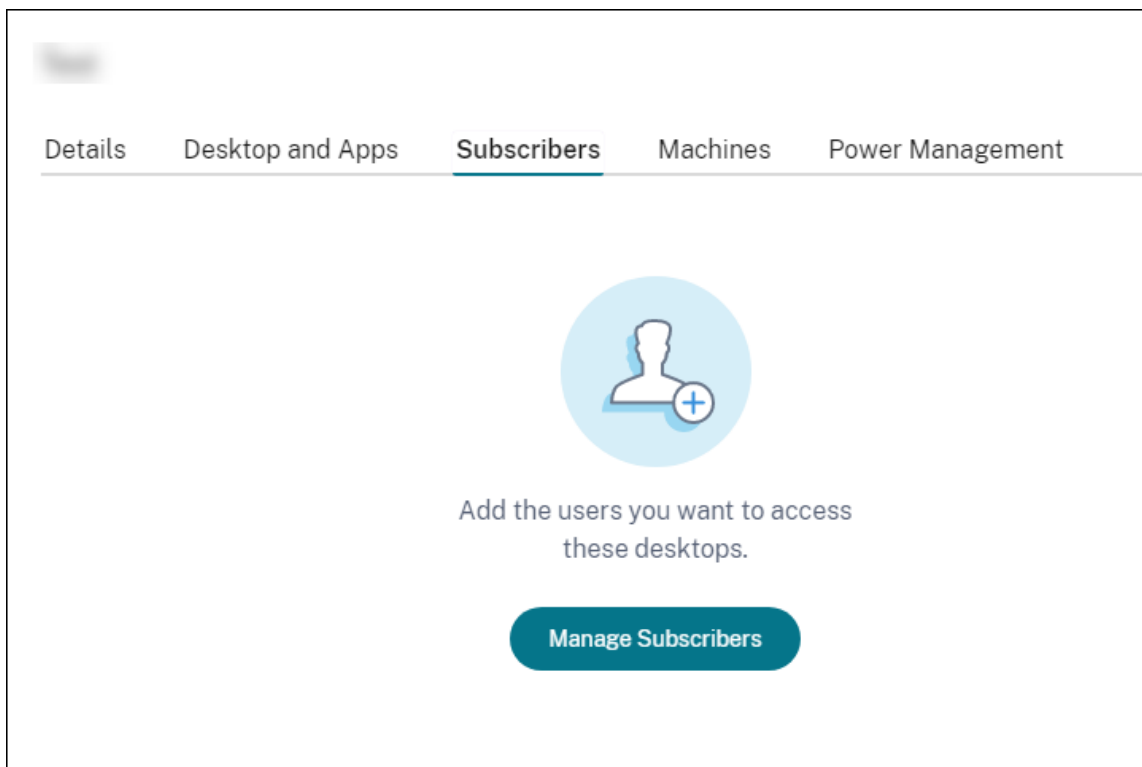
Completare questa procedura indipendentemente dal metodo di autenticazione utilizzato.

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, se non avete aggiunto alcun utente a un catalogo, fate clic su **Aggiungi sottoscrittori**.

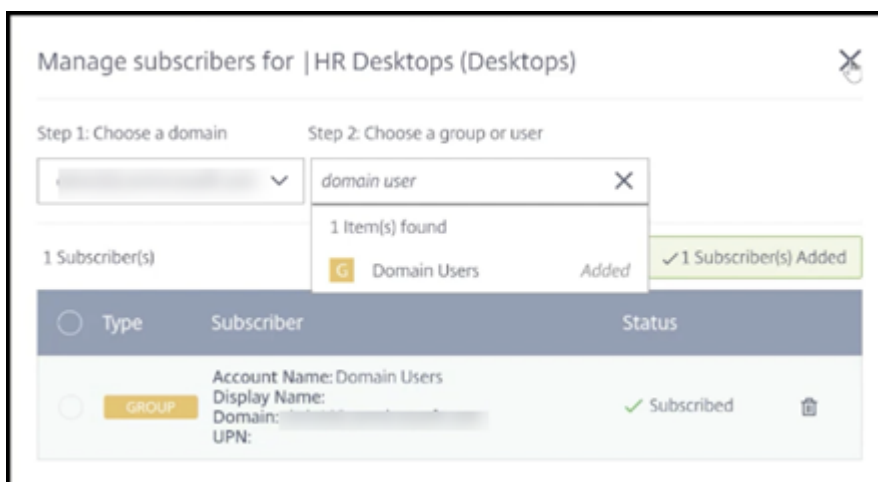


Per aggiungere utenti a un catalogo che ha già utenti, fare clic in un punto qualsiasi della voce del catalogo.

2. Nella scheda **Abbonati**, fai clic su **Gestisci abbonati**.



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. Seleziona altri utenti, secondo necessità. Quando hai finito, fai clic sulla **X** nell'angolo in alto a destra.

Per rimuovere utenti da un catalogo, attenersi ai passaggi 1 e 2. Nel passaggio 3, fai clic sull'icona del cestino accanto al nome che desideri eliminare (invece di selezionare un dominio e un gruppo/utente). Questa azione rimuove l'utente dal catalogo, non dall'origine (ad esempio Managed Azure AD o il proprio AD o AAD).

Passi successivi:

- Per un catalogo con macchine multisesione, [aggiungere le applicazioni](#), se non lo si è già fatto.
- Per tutti i cataloghi, [inviare l'URL di Citrix Workspace](#) ai vostri utenti.

Ulteriori informazioni

Per ulteriori informazioni sull'autenticazione in Citrix Cloud, consultare [Gestione delle identità e degli accessi](#).

Gestisci cataloghi

October 7, 2022

Nota:

In questo articolo vengono descritte le attività che è possibile utilizzare per gestire i cataloghi creati nell'interfaccia Quick Deploy. Per informazioni sulla gestione del catalogo tramite l'interfaccia di gestione della configurazione completa, vedere [Gestire i cataloghi delle macchine](#).

Aggiungere macchine a un catalogo

Mentre le macchine vengono aggiunte a un catalogo, non è possibile apportare altre modifiche a tale catalogo.

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, fai clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Macchine**, fare clic su **Aggiungi macchine al catalogo**.

The screenshot shows the 'Machines' tab in the Citrix DaaS console. At the top, there are navigation tabs: Details, Desktop, Subscribers, Machines (selected), and Power Management. Below the tabs is a notification box: 'Monitor shows all machine details and actions. Some actions are available here, but we recommend using Monitor for all machine features and information.' with a 'Go to Monitor' link. The main content area displays 'Total Machines' as 12, with a breakdown: 11 powered on (green dot), 1 powered off (grey dot), 11 active sessions (person icon), and 1 unregistered (yellow triangle). Below this is a search bar labeled 'Search machines' and a 'Refresh' button. A table lists machine details with columns: Name, Power, Registration, Assigned Users, Sessions, and IP Address. The table shows three rows of machines, all with 'On' power status and 'Registered' status. At the bottom, there is a large teal button labeled 'Add Machines to Catalog'.

3. Immettere il numero di macchine che si desidera aggiungere al catalogo.

The screenshot shows a dialog box titled 'How many machines do you want to add?'. It features a text input field containing the number '1'. Below the input field is a large teal button labeled 'Add Machines to Catalog'. To the right of the button is an information icon and a warning message: 'This action takes time. You won't be able to see the image until this is done.'

4. (Valido solo se il catalogo è collegato a un dominio.) Digitare il nome utente e la password per l'account del servizio.
5. Fare clic su **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. Dal dashboard **Gestisci > Distribuzione rapida di Azure**, seleziona un catalogo contenente macchine con più sessioni.
2. Nella scheda **Dettagli**, fai clic su **Modifica** accanto a **Sessioni per computer**.
3. Immettere un nuovo numero di sessioni per computer.
4. Fai clic su **Aggiorna numero di sessioni**.
5. Conferma la tua 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 nel dashboard **Gestisci > Azure Quick Deploy** sono disponibili anche nel dashboard **Monitor** in Citrix DaaS Standard per Azure (in precedenza servizio Citrix Virtual Apps and Desktops Standard for Azure).

Per selezionare le azioni dal dashboard **Gestisci > Azure Quick Deploy** :

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, fai clic in un punto qualsiasi della voce di un 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:

- **Riavvia:** riavvia il computer selezionato.
- **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.
- **Attiva/disattiva la modalità di manutenzione:** attiva la modalità di manutenzione (se è disattivata) o disattiva (se è attiva) per la macchina selezionata.

Per impostazione predefinita, la modalità di manutenzione è disattivata per una macchina. L'attivazione della modalità di manutenzione per una macchina impedisce la creazione di nuovi collegamenti a quella macchina. Gli utenti possono connettersi alle sessioni esistenti su quel computer, ma non possono avviare nuove sessioni su quel computer. È possibile mettere un computer in modalità di manutenzione prima di applicare le patch o per la risoluzione dei problemi.

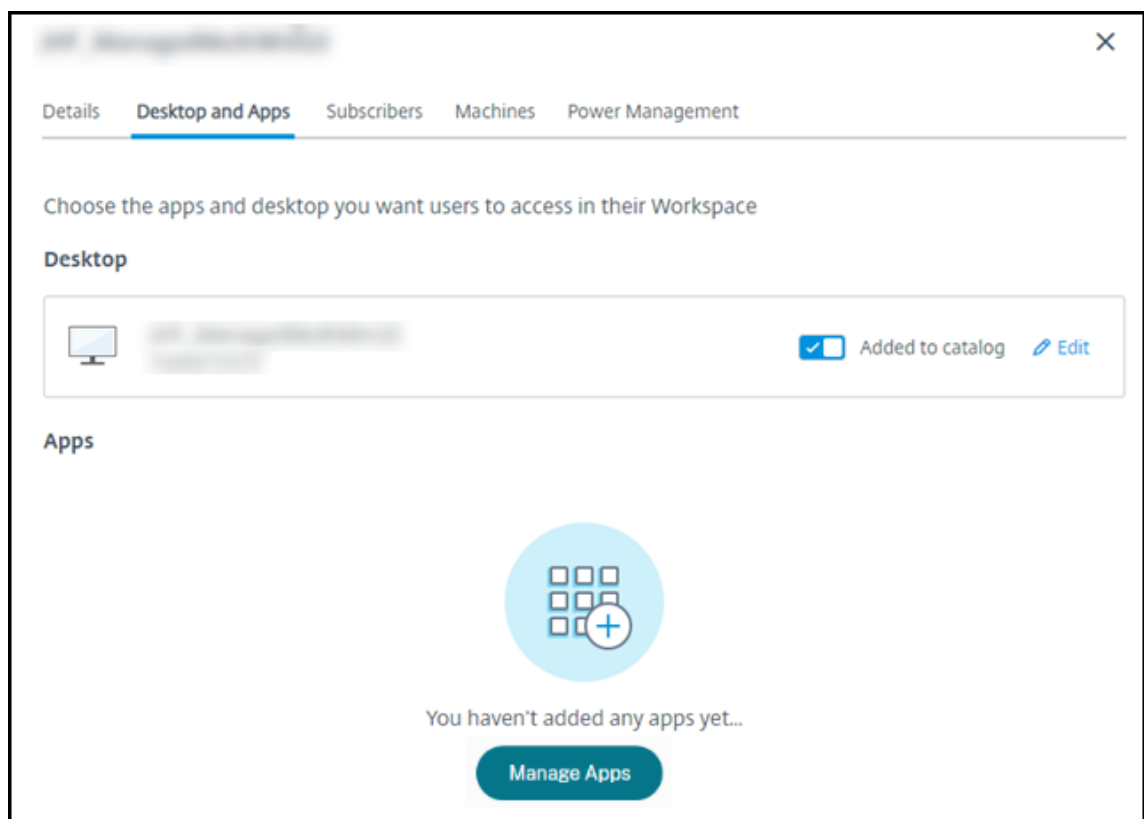
- **Elimina:** elimina la macchina selezionata. Questa azione è disponibile solo quando il numero di sessioni del computer è pari a zero. Confermare l'eliminazione.

Quando un computer viene eliminato, tutti i dati sul computer vengono rimossi.

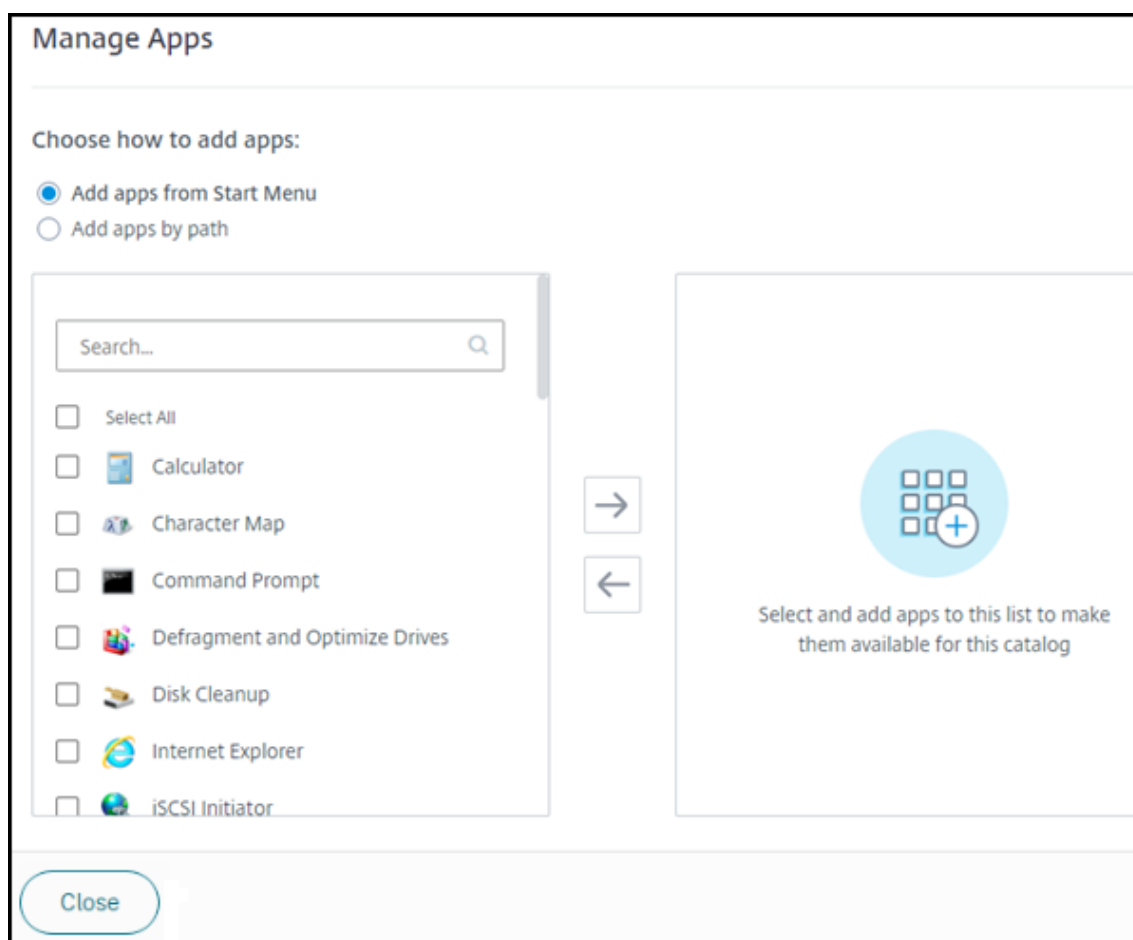
- **Forza riavvio:** forza il riavvio del computer selezionato. Selezionare questa azione solo se un'azione di **riavvio** per il computer non è riuscita.

Aggiungere app a un catalogo

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, fai clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Desktop e app**, fai clic su **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**:



- Seleziona le app disponibili nella colonna di sinistra. (Utilizzare la **funzione Cerca** per personalizzare l'elenco delle app.) Fare clic sulla freccia destra tra le colonne. Le app selezionate vengono spostate nella colonna di destra.
 - Allo stesso modo, per rimuovere le app, selezionala nella colonna di destra. Fai clic sulla freccia sinistra tra le colonne.
 - Se il menu **Start** ha 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:

Manage Apps


Choose how to add apps:

Add apps from Start Menu

Add apps by path

Enter the App Details Displayed to Users

App Name *

 [Change Icon](#) ⓘ

Description

Enter the App Parameters

Path *

Command Line Parameters:

Working Directory:

Select and add apps to this list to make them available for this catalog

Close

- Immettere il nome dell'app. Questo è il nome che gli utenti vedono in Citrix Workspace.
- L'icona mostrata è l'icona che gli utenti vedono in Citrix Workspace. Per selezionare un'altra icona, fare clic su **Cambia icona** e passare all'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, consultate [Passare i parametri alle applicazioni pubblicate](#).

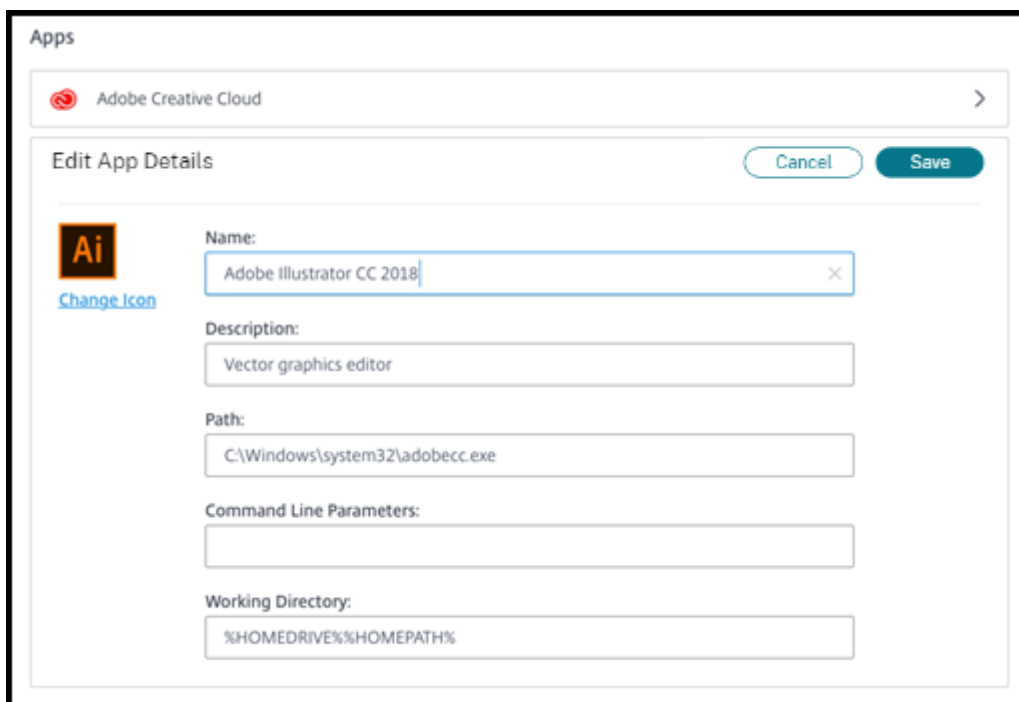
6. Al termine, fai clic su **Chiudi**.

Cosa fare dopo (se state completando il flusso di creazione e distribuzione del catalogo): [inviare l'URL di Citrix Workspace ai vostri utenti](#), se non l'avete già fatto.

Nei VDA di 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 **Gestisci > Distribuzione rapida di Azure**, fai 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. Fai clic sull'icona della matita.



The screenshot shows the 'Edit App Details' dialog box for an application named 'Adobe Creative Cloud'. The dialog has a 'Cancel' button and a 'Save' button. The application icon is 'Ai' (Adobe Illustrator) with a 'Change Icon' link below it. The fields are as follows:

- Name:** Adobe Illustrator CC 2018
- Description:** Vector graphics editor
- Path:** C:\Windows\system32\adobecc.exe
- Command Line Parameters:** (empty)
- Working Directory:** %HOMEDRIVE%\%HOMEPATH%

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 che gli utenti vedono nel loro Citrix Workspace, fate clic su **Cambia icona** e individuate l'icona che desiderate visualizzare.
6. Quando hai finito, fai clic su **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 doppie per indicare che lo spazio appartiene alla riga di comando. Aggiungere virgolette doppie attorno al percorso e un altro insieme di virgolette doppie attorno ai simboli percentuale e stella. 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 **Gestisci > Distribuzione rapida di Azure**, fai clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Desktop e app**, fai clic sull'icona del cestino accanto alle app che desideri 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 **Gestisci > Distribuzione rapida di Azure**, fai clic in un punto qualsiasi della voce del catalogo.

2. Nella scheda **Dettagli**, fare clic su **Elimina catalogo** nella parte inferiore della finestra.
3. Confermare l'eliminazione selezionando le caselle di controllo di conferma e quindi facendo clic sul pulsante di conferma.

Per aiutare a identificare gli account computer di Active Directory residui che è necessario eliminare, è possibile scaricare un elenco di nomi di computer 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.

Details Desktop and Apps Subscribers Machines **Power Management**

Presets
Cost Saver ▾

General

Disconnect desktop sessions when idle
After 15 Minutes ▾

Log Off Disconnected Sessions
After 15 Minutes ▾

Power Off Delay
After 30 Minutes ▾

Work hours ⓘ

Time Zone
(UTC-05:00) Eastern Time (US & Canada) ▾

Power on machines
SUN MON TUE WED THU FRI SAT

Start End
▾ ▾ ▾ ▾

Capacity buffer
10 %

Minimum running machines
1

After-hours ⓘ

Capacity buffer
10 %

Minimum running machines
1

Save Changes

Una pianificazione di gestione dell'alimentazione contiene le seguenti informazioni.

Pianificazioni preimpostate Citrix DaaS for Azure 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 multisezione. 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 multisezione 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 multisezione. 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 della sessione corrente. Ad esempio, se ci sono 100 sessioni attive e il buffer di capacità è del 10%, Citrix DaaS for Azure 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 **Gestisci > Distribuzione rapida di Azure**, fai 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. Imposta i valori desiderati per la pianificazione personalizzata.
5. Fai clic su **Personalizza** in alto e salva le impostazioni correnti come nuovo predefinito. Immettete un nome per il nuovo predefinito e fate clic sul segno di spunta.
6. Quando hai finito, fai clic su **Salva modifiche**.

Successivamente, è possibile modificare o eliminare un predefinito personalizzato utilizzando le icone della matita o del cestino nel menu **Predefiniti**. Non è possibile modificare o eliminare i preset comuni.

Istantanee e ripristino VDA

Le funzionalità di snapshot e ripristino di Citrix DaaS per Azure forniscono un modo per il ripristino da perdite di dati non pianificate o altri errori nei VDA che distribuiscono desktop e app. L'operazione di istantanea acquisisce e memorizza un'istantanea della macchina. Successivamente, un'operazione di ripristino utilizza un'istantanea selezionata.

- È possibile configurare programmi di snapshot giornalieri e settimanali per tutte le macchine in un catalogo. Queste istantanee sono chiamate *istantanee automatiche*. Viene scattata un'istantanea di ogni macchina presente nel catalogo. Non ci sono pianificazioni di istantanee predefinite.
- È possibile eseguire il backup di una singola V in un catalogo su richiesta. Questa è chiamata istantanea manuale. È possibile creare un'*istantanea manuale* di una macchina anche se il catalogo a cui appartiene dispone di istantanee pianificate. (Tuttavia, non è possibile pianificare istantanee su un solo computer.)

Importante:

Le funzionalità di snapshot e ripristino di Citrix DaaS for Azure sono supportate solo per le macchine nei cataloghi statici e assegnate agli utenti.

Pianificazioni istantanee

Ricorda: le pianificazioni istantanee si applicano a tutte le macchine in un catalogo.

Per impostazione predefinita, non ci sono pianificazioni di istantanee.

Per gestire le pianificazioni degli snapshot:

1. Dalla dashboard **Gestisci**, fai clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Dettagli**, fare clic su **Pianifica istantanee**.
3. Nella pagina **Pianifica istantanee**, configurare le pianificazioni per le istantanee automatiche settimanali o giornaliere o entrambe:
 - Per aggiungere o modificare istantanee settimanali, spostare il dispositivo di scorrimento per le **istantanee automatiche settimanali** finché non viene visualizzato un segno di spunta. Seleziona il giorno della settimana e l'ora di inizio.
 - Per aggiungere o modificare istantanee giornaliere, spostare il dispositivo di scorrimento per le **istantanee automatiche giornaliere** finché non viene visualizzato un segno di spunta. Seleziona l'ora di inizio.
 - Per rimuovere le istantanee settimanali, sposta il dispositivo di scorrimento per le **istantanee automatiche settimanali** finché non viene visualizzata una **X**.
 - Per rimuovere le istantanee giornaliere, spostare il dispositivo di scorrimento per le **istantanee automatiche giornaliere** finché non viene visualizzata una **X**.
4. Quando hai finito, fai clic su **Salva** nella parte inferiore della pagina.

Istantanee manuali

Un'istananea manuale è per una singola macchina in un catalogo. (Non è possibile creare una pianificazione per scattare un'istananea di singole macchine.)

1. Dalla dashboard **Gestisci**, fai clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Macchine**, trova la macchina di cui vuoi scattare un'istananea. Seleziona **Istantanee** nel menu puntini di sospensione per quel computer.
3. Nella pagina **Istantanee per VDA-Name**, fare clic su **Crea istantanea manuale**.
4. Fornisci un nome per l'istananea. Consigliato: scegli un nome che puoi identificare facilmente in seguito.
5. Conferma la tua richiesta.

Visualizza e gestisci le istantanee

1. Dalla dashboard **Gestisci**, fai clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Macchine**, trova la macchina di cui vuoi scattare un'istananea. Seleziona **Istantanee** nel menu puntini di sospensione per quel computer.
3. Nella pagina **Backup per VDA-name**:
 - Se non ci sono istantanee per la macchina, un messaggio guida l'utente a creare un'istananea manuale per questo computer o a creare istantanee pianificate per tutte le macchine nel catalogo che contiene questa macchina.
 - È possibile selezionare una delle istantanee e ripristinare il computer. Vedi Ripristina.
 - È possibile eliminare le istantanee. Selezionare le caselle di controllo per una o più istantanee e quindi fare clic su **Elimina** nell'intestazione della tabella. Conferma la tua richiesta.

Suggerimento: quando elimini un catalogo, tutte le istantanee vengono distrutte.

Restore (Ripristina)

È possibile ripristinare una macchina da qualsiasi istantanea disponibile per quella macchina.

Durante un ripristino, la macchina è spenta. Nessuna delle azioni nel menu con i puntini di sospensione di una macchina è disponibile durante il ripristino di un'istananea.

1. Dalla dashboard **Gestisci**, fai clic in un punto qualsiasi della voce del catalogo.
2. Nella scheda **Macchine**, trova la macchina di cui vuoi scattare un'istananea. Seleziona **Istantanee** nel menu puntini di sospensione per quel computer.
3. Nella pagina ****Istantanee per VDA-name** pagina**, selezionare la casella di controllo dell'istananea che si desidera utilizzare.
4. Fai clic su **Ripristina** nell'intestazione della tabella.
5. Conferma la richiesta.

La colonna **Stato** nella scheda **Macchine** indica l'avanzamento e l'esito dell'operazione di ripristino.

Se una macchina non riesce a ripristinare un'istananea, riprovare.

Informazioni correlate

- [Aggiornare un catalogo con una nuova immagine](#)
- [Aggiunta e rimozione di utenti in un catalogo](#)
- [Unito al dominio e non unito al dominio](#)

Monitoraggio

May 9, 2023

Dalla dashboard **Monitor**, è possibile visualizzare l'utilizzo del desktop, le sessioni e le macchine nella distribuzione di Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure). È inoltre possibile controllare le sessioni, gestire le macchine, terminare le applicazioni in esecuzione e terminare i processi in esecuzione.

Per accedere alla dashboard **Monitor** (Monitoraggio):

1. Accedi a [Citrix Cloud](#), se non l'hai già fatto. Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**.
2. Dalla dashboard **Gestisci**, fai clic sulla scheda **Monitor**.

Monitoraggio dell'utilizzo 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 o ultimo mese.

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.

Report sull'utilizzo del desktop

Per scaricare un report contenente informazioni sugli avviamenti dei computer durante l'ultimo mese, fare clic su **Avvia attività**. 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. Le opzioni disponibili sono:

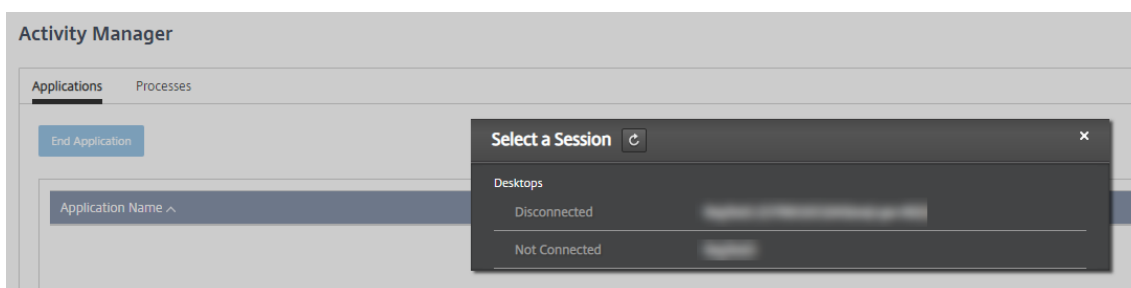
- Filtrare la visualizzazione per macchine, sessioni, connessioni o applicazioni.
- Affinare la visualizzazione di sessioni o macchine scegliendo i criteri desiderati, creando un filtro usando le espressioni.

- Salvare i filtri creati per riutilizzarli.

Controllare le applicazioni di un utente

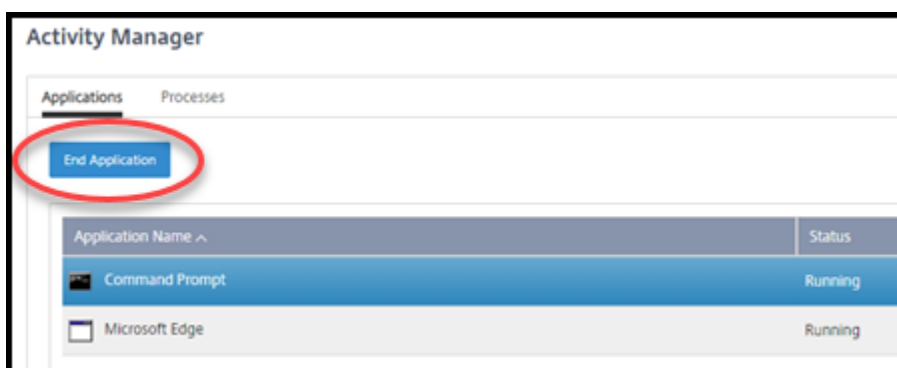
È possibile visualizzare e gestire applicazioni e processi per un utente che ha una sessione in esecuzione o un desktop assegnato.

1. Dalla dashboard **Monitor**, fare clic su **Cerca** e immettere il nome utente (o i caratteri iniziali del nome utente), il computer o l'endpoint. Dai risultati della ricerca, seleziona l'elemento che stai cercando. (Per comprimere la casella di ricerca senza eseguire la ricerca, fare nuovamente clic su **Cerca**.)
2. Seleziona una sessione.



L'Activity Manager elenca le applicazioni e i processi per la sessione dell'utente.

3. Per terminare un'applicazione, nella scheda **Applicazioni** in Gestione attività fare clic nella riga dell'applicazione per selezionare l'applicazione e quindi fare clic su **Termina applicazione**.



4. Per terminare un processo, nella scheda **Processi** in Gestione attività fare clic nella riga del processo per selezionare tale processo, quindi fare clic su **Termina processo**.
5. Per visualizzare i dettagli della sessione, fai clic su **Dettagli** in alto a destra. Per tornare alla visualizzazione delle applicazioni e dei processi, fare clic su Gestione attività in alto a destra.
6. Per controllare la sessione, fare clic su **Controllo sessione > Disconnetti** o **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. Verificarlo controllando il nome della macchina elencato nella barra del titolo di **User**.

Shadowing viene avviato in una nuova scheda del browser. Assicurarsi che il browser consenta i popup dall'URL di Citrix Cloud.

In un abbonamento a Citrix Managed Azure, lo shadowing è supportato solo per gli utenti su macchine aggiunte a un dominio. Per eseguire lo shadowing di una macchina non unita al dominio in un abbonamento Citrix Managed Azure, 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.

Abilita shadowing

1. Dalla dashboard **Monitor**, vai alla vista **Dettagli utente**.
2. Selezionare la sessione utente, quindi fare clic su **Shadow** nella visualizzazione **Gestione attività** o nel pannello **Dettagli sessione**.

VDA Shadow 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-websocketify` 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 shadowing viene inizializzata e viene visualizzata una richiesta di conferma sul dispositivo dell'utente.

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 ombreggiata.

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. Dalla dashboard **Monitor**, fai clic su **Filtri**.

Filters - All Machines Data is updated every minute

View Machines Sessions

Type Of Machine All Machines

Refine By + x

Save Save As Delete Clear

Desktop OS Machines 10

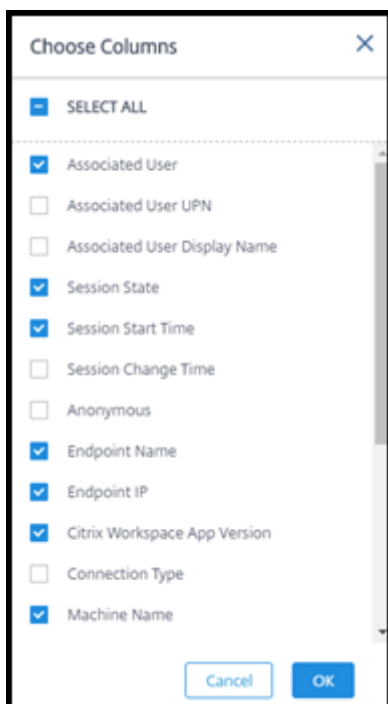
Power Control Maintenance Mode Export Choose Columns

Machine Name	Machine Catalog	Is Assigned	IP Address	Power State	Sessions	Maintenance Mode
--------------	-----------------	-------------	------------	-------------	----------	------------------

2. Selezionare la vista **Sessions** (Sessioni).

<input type="checkbox"/>	Associated User ↑	Session State	Session Start Time	Endpoint Name	Endpoint IP	Citrix Workspace App Version	Machine Name	IP Address	Idle Time
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	n/a

- Per personalizzare la visualizzazione, fare clic su **Scegli colonne** e selezionare le caselle di controllo degli elementi che si desidera visualizzare. Quando hai finito, fai clic su **OK**. Il display delle sessioni si aggiorna automaticamente.



- Fare clic sulla casella di controllo a sinistra di ogni sessione che si desidera controllare.
- Per disconnettersi o disconnettere la sessione, selezionare **Controllo sessione > Disconnetti** o **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.

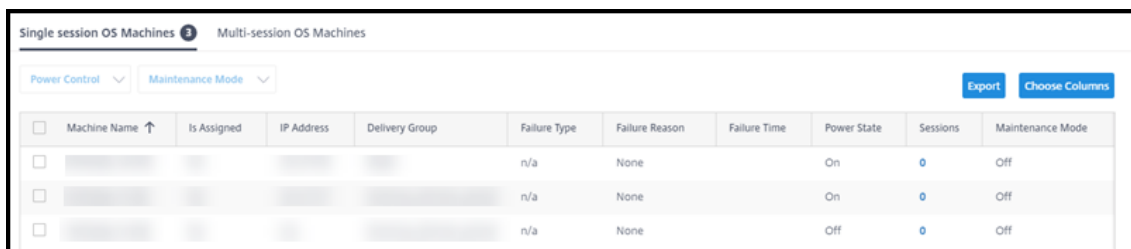
Report informativo sulla sessione

Per scaricare le informazioni sulla sessione, fare clic su **Esporta** sul display 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

I display della macchina vengono aggiornati ogni minuto.

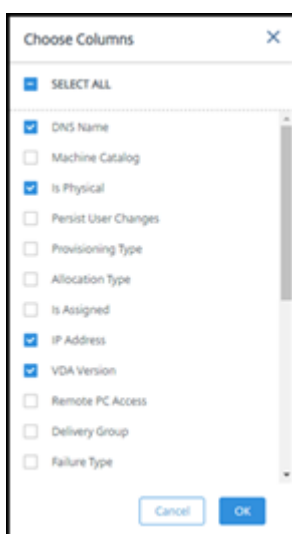
1. Dalla dashboard **Monitor**, fai clic su **Filtri**.
2. Seleziona la vista **Macchine**.



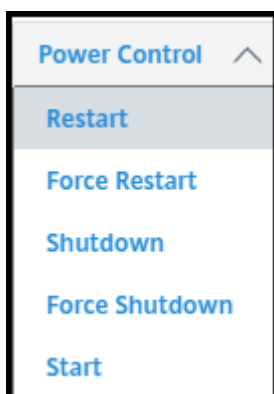
<input type="checkbox"/>	Machine Name ↑	Is Assigned	IP Address	Delivery Group	Failure Type	Failure Reason	Failure Time	Power State	Sessions	Maintenance Mode
<input type="checkbox"/>					n/a	None		On	0	Off
<input type="checkbox"/>					n/a	None		On	0	Off
<input type="checkbox"/>					n/a	None		Off	0	Off

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, fare clic su **Scegli colonne** e selezionare le caselle di controllo degli elementi che si desidera visualizzare. Quando hai finito, fai clic su **OK**. Il display della macchina si aggiorna automaticamente.



4. Per controllare l'alimentazione delle macchine o posizionarle in modalità di manutenzione o fuori dalla modalità di manutenzione, fare clic sulla casella di controllo a sinistra di ogni macchina che si desidera controllare.
5. Per controllare l'alimentazione delle macchine selezionate, fare clic su **Controllo alimentazione** e selezionare un'azione.



6. Per posizionare le macchine selezionate in modalità di manutenzione o fuori dalla modalità di manutenzione, fare clic su **Modalità manutenzione > ON** o **Modalità manutenzione > OFF**.

Quando si utilizza la funzione di ricerca per trovare e selezionare un computer, vengono visualizzati i dettagli della macchina, l'utilizzo, l'utilizzo cronologico (degli ultimi sette giorni) e gli IOPS medi.

Report informativo sulla macchina

Per scaricare le informazioni sulla sessione, fare clic su **Esporta** sul display del computer. 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](#)

Citrix DaaS per Azure per i provider di servizi Citrix

October 7, 2022

In questo articolo viene descritto come Citrix Service Provider (CSP) possono configurare Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure service) 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.
- Avete un abbonamento a Citrix DaaS per Azure.

Limitazioni

- Le modifiche al nome del cliente possono richiedere fino a 24 ore per essere applicate su tutte le interfacce.
- Quando si crea un cliente, l'indirizzo e-mail deve essere univoco.

Problemi noti

- Dopo che l'utente di un cliente è stato assegnato a una risorsa, non è possibile rimuoverlo o annullarlo.
- La console di gestione non impone la separazione tra utenti del cliente. L'utente è responsabile dell'aggiunta di utenti ai cataloghi e alle risorse appropriati.

Aggiungere un cliente

1. Accedere a Citrix Cloud con le credenziali del CSP. Fare clic su **Clienti** nel menu in alto a sinistra.
2. Dalla dashboard del **cliente**, fai clic su **Invita o Aggiungi**. Fornisci le informazioni richieste.

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.

3. 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](#).

Puoi aggiungere altri amministratori in un secondo momento e controllare quali clienti possono vedere nei dashboard di Citrix DaaS for Azure **Manage** and **Monitor** .

Aggiungere Citrix DaaS per Azure a un cliente

1. Accedere a Citrix Cloud con le credenziali del CSP. Fare clic su **Clienti** nel menu in alto a sinistra.
2. Dalla dashboard **Cliente**, seleziona **Aggiungi servizio** nel menu con i puntini di sospensione per il cliente.
3. In **Selezionare un servizio da aggiungere**, fate clic su **Citrix DaaS Standard for Azure**.
4. Fare clic su **Continue** (Continua).

Dopo aver completato questa procedura, il cliente viene iscritto alla sottoscrizione Citrix DaaS per Azure.

Al termine dell'onboarding, viene creato automaticamente un nuovo cliente in Citrix DaaS per Azure. Il cliente è visibile in **Gestisci > Distribuzione rapida**.

Filtra le risorse per cliente

Puoi filtrare le risorse per cliente nel dashboard di Citrix DaaS per Azure **Manage > Azure Quick Deploy**. (Per impostazione predefinita, vengono visualizzate tutte le risorse.) Quando lavori con risorse come cataloghi, immagini di macchine e sottoscrizioni di Azure, puoi selezionare display cliente specifici per organizzare le risorse dei tuoi tenant.

Le connessioni SD-WAN vengono create in base al cliente. Il cliente deve disporre di un diritto al servizio SD-WAN Orchestrator.

- Per creare una connessione SD-WAN per un cliente, segui le indicazioni in [Creare una connessione SD-WAN](#). Nella pagina **Aggiungi una connessione di rete**, selezionare il cliente. È possibile selezionare la casella del tipo di connessione SD-WAN solo se il cliente dispone di un'autorizzazione al servizio SD-WAN Orchestrator.
- Affinché la creazione della connessione abbia esito positivo, il cliente deve disporre anche di un Master Control Node (MCN) installato. Tuttavia, solo il servizio SD-WAN Orchestrator determina se è possibile selezionare il tipo di connessione SD-WAN.

Crea cataloghi per distribuire app e desktop

Un catalogo è un gruppo di utenti e la raccolta di macchine virtuali a cui hanno accesso. 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](#).

Domini federati

I domini federati consentono agli utenti dei clienti di utilizzare le credenziali di un dominio collegato alla posizione della risorsa per accedere al proprio workspace. Potete fornire aree di lavoro dedicate

ai vostri clienti a cui i loro utenti possono accedere tramite un URL dell'area di lavoro personalizzato (ad esempio, `customer.cloud.com`), mentre la posizione delle risorse rimane sul vostro account Citrix Cloud.

Puoi fornire aree di lavoro dedicate insieme all'area di lavoro condivisa 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 al loro spazio di lavoro dedicato, aggiungili ai domini appropriati che gestisci.

Dopo aver configurato l'area di lavoro tramite [Configurazione del workspace](#), gli utenti dei clienti possono accedere al proprio spazio 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. Fare clic su **Clienti** nel menu in alto a sinistra.
2. Dalla dashboard del **cliente**, seleziona **Gestione identità e accessi** nel menu in alto a sinistra.
3. Nella scheda **Domini**, seleziona **Gestisci dominio federato** nel menu con i puntini di sospensione del dominio.
4. Nella scheda **Gestisci dominio federato**, nella colonna **Clienti disponibili**, seleziona un cliente che desideri aggiungere al dominio. Fai clic sul segno più accanto al nome del cliente. Il cliente selezionato viene ora visualizzato nella colonna **Clienti federati**. Ripetere l'operazione per aggiungere altri clienti.
5. Al termine, fai clic su **Applica**.

Rimuovere un cliente da un dominio

Quando rimuovi un cliente da un dominio che gestisci, gli utenti del cliente non possono più accedere alle loro aree di lavoro utilizzando le credenziali del tuo dominio.

1. Da Citrix Cloud, selezionate **Gestione identità e accessi** nel menu in alto a sinistra.
2. Nella scheda **Domini**, seleziona **Gestisci dominio federato** dal menu con i puntini di sospensione del dominio che desideri gestire.
3. Dall'elenco dei clienti federati, individuare o cercare i clienti che si desidera rimuovere.
 - Fare clic su **X** per rimuovere un cliente.
 - Per rimuovere tutti i clienti elencati dal dominio, fai clic su **Rimuovi tutto**.

I clienti selezionati passano all'elenco dei **clienti disponibili**.

4. Fare clic su **Applica**.
5. Rivedi i clienti selezionati, quindi fai clic su **Rimuovi clienti**.

Aggiunta di un amministratore con accesso limitato

1. Accedere a Citrix Cloud con le credenziali del CSP. Fare clic su **Clienti** nel menu in alto a sinistra.
2. Dalla dashboard del **cliente**, seleziona **Gestione identità e accessi** nel menu in alto a sinistra.
3. Nella scheda **Amministratori**, fare clic su **Aggiungi amministratori da**, quindi selezionare **Citrix Identity**.
4. Digita l'indirizzo e-mail della persona che stai aggiungendo come amministratore, quindi fai clic su **Invita**.
5. Configurare le autorizzazioni di accesso appropriate per l'amministratore. Citrix consiglia di selezionare **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. Selezionate una o più coppie di ruoli e ambiti per Citrix DaaS for Azure, in base alle esigenze.
7. Quando hai finito, fai clic su **Invia invito**.

Quando l'amministratore accetta l'invito, ha l'accesso che gli è stato assegnato.

Accesso dei partner al provider di identità del cliente

È possibile gestire gli utenti dalla dashboard di Citrix DaaS per Azure **Manage > Azure Quick Deploy** o dalla console Citrix Cloud.

Quando si utilizza un provider di identità non AD per gli utenti (ad esempio Citrix Managed Azure AD), è necessario essere un amministratore di Citrix Cloud Identity and Workspace per il cliente prima di poter gestire gli utenti per quel cliente. Se non sei l'amministratore di un cliente, non puoi aggiungere o eliminare utenti per quel cliente.

Per gestire gli utenti di un cliente da **Gestisci > Dashboard di Azure Quick Deploy**, seleziona il partner o il cliente in **Mostra elementi per**.

- **Esempio 1:** Seleziona il cliente A da **Mostra articoli per**. La dashboard ora mostra solo gli articoli per il cliente A. Quando selezioni un catalogo, nella scheda **Iscritti** vengono visualizzati solo gli utenti del cliente A. Puoi aggiungere o rimuovere utenti per il cliente A (supponendo che tu sia un amministratore per quel cliente).
- **Esempio 2:** Seleziona la voce partner in **Mostra articoli per**. La dashboard ora mostra solo gli articoli dei partner. Nella scheda **Iscritti**, vengono visualizzati solo gli utenti creati per il partner. Non vengono visualizzate le voci dei clienti. Puoi aggiungere o rimuovere utenti per quel partner (supponendo che tu sia un amministratore di quel partner), ma non puoi gestire nessun utente cliente da questa posizione.

Per gestire gli utenti di un cliente dalla console Citrix Cloud, selezionate il cliente quando richiesto dopo l'accesso (o in seguito, utilizzando **Change Customer** nell'area in alto a destra della console Citrix Cloud). Quando si utilizza la **Libreria** per gestire gli utenti, il contesto di visualizzazione riflette

il cliente selezionato. Ad esempio, se hai selezionato il cliente A, la Libreria mostra solo le offerte del cliente A.

Modifica delle autorizzazioni di amministrazione delegata per gli amministratori

1. Accedere a Citrix Cloud con le credenziali del CSP. Fare clic su **Clienti** nel menu in alto a sinistra.
2. Dalla dashboard del **cliente**, seleziona **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 o deselezionare le coppie di ruoli e ambiti per Citrix DaaS for Azure, in base alle esigenze. Assicurarsi di abilitare solo le voci che contengono l'ambito univoco creato per il cliente.
5. Fare clic su **Save** (Salva).

Accedi e configura le aree di lavoro

Ogni cliente ottiene il proprio spazio di lavoro con un `customer.cloud.com` URL univoco. Questo URL è il punto in cui gli utenti del cliente accedono alle app e ai desktop pubblicati.

- **Da Citrix DaaS Standard per Azure:** nella dashboard **Gestisci > Azure Quick Deploy**, visualizza l'URL espandendo **User Access & Authentication** sulla destra.
- **Da Citrix Cloud:** dalla dashboard del **cliente**, selezionare **Configurazione workspace** dal menu in alto a sinistra. Visualizza l'URL nella scheda **Accesso**.

È possibile modificare l'accesso e l'autenticazione in un workspace. È inoltre possibile personalizzare l'aspetto e le preferenze dell'area di lavoro. Per maggiori informazioni, vedere i seguenti articoli:

- [Configurazione delle aree di lavoro](#)
- [Spazi di lavoro sicuri](#)

Monitorare il servizio di un cliente

Il dashboard di Citrix DaaS for Azure **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**.

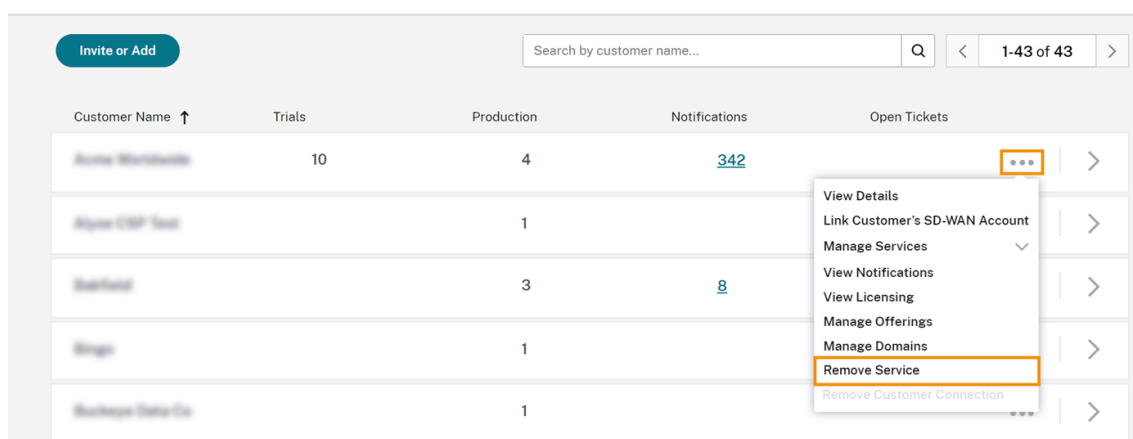
Tieni presente che la possibilità di visualizzare i **monitor** per un cliente è controllata dall'accesso configurato dall'amministratore.

Rimuovi un servizio

Prima di iniziare, assicuratevi che l'ambito del cliente non sia collegato ad alcun oggetto Citrix DaaS Standard for Azure. Se sono collegati, non è possibile rimuovere il servizio. Per scollegare gli ambiti, andate a **Citrix Studio > Amministratori > Ambiti** e modificate l'ambito. Per ulteriori informazioni sullo scollegamento degli ambiti, consulta [Creare e gestire l'ambito](#).

1. Accedete a Citrix Cloud con le vostre credenziali Citrix Service Provider.
2. Nella dashboard del **cliente**, fai clic sul menu con i puntini di sospensione (...) del cliente da cui desideri rimuovere un servizio e seleziona **Rimuovi servizio**.

← Customer Dashboard



Viene visualizzata la pagina **Servizio da rimuovere**.

3. Fare clic su **Rimuovi** per rimuovere il servizio.

Risoluzione dei problemi

September 7, 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. Cloud Connectors consente a Citrix Cloud di comunicare con la posizione della risorsa. Citrix installa e aggiorna i connettori cloud.

Facoltativamente, è possibile avviare diverse azioni di Cloud Connector e posizione delle risorse. Vedere:

- [Azioni della posizione risorsa](#)
- [Impostazioni della posizione delle risorse durante la creazione di un catalogo](#)

Citrix DaaS for Azure dispone di strumenti di risoluzione dei problemi e di supportabilità che possono aiutare a risolvere i problemi di configurazione e comunicazione con le macchine che distribuiscono 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. Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Risoluzione dei problemi e supporto** a 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.

- 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.
- 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.
- 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).
- Fare clic su **Download RDP File** (Scarica file RDP).
- 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).
- 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

- Dalla dashboard **Gestisci > Distribuzione rapida di Azure** in Citrix DaaS per Azure, espandi **Risoluzione dei problemi e supporto** a destra.
- 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](#).

Limiti

May 9, 2023

In questo articolo vengono elencati i limiti per le risorse in una distribuzione di Citrix DaaS Standard per Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure service).

Nota:

I limiti sono consigliati da Citrix.

Limiti di configurazione

Risorsa	Limite
Domini di Active Directory	25
Cataloghi	100
Posizioni delle risorse	25
VDA per abbonamento	2,500

Limiti di posizione delle risorse

Nella tabella seguente sono elencati i limiti per ogni posizione di risorsa. Se le vostre esigenze superano questi limiti, Citrix consiglia di utilizzare più posizioni di risorse.

Risorsa	Limite
Domini di Active Directory	1
VDA a sessione singola	10,000
VDA multisessione	1,000

I Citrix Cloud Connectors sono assegnati alle sedi delle risorse e collegano i carichi di lavoro a Citrix DaaS per Azure. Per informazioni sui limiti di Cloud Connector e per consigli su dimensioni e scalabilità, vedere [Considerazioni su scalabilità e dimensioni per i connettori cloud](#).

Limiti di provisioning

Nella tabella seguente sono elencati i massimi consigliati per un singolo account Citrix Cloud.

Per implementazioni su larga scala, Citrix consiglia un modello hub-and-spoke, in cui i VDA sono distribuiti su più abbonamenti e connessioni di rete.

Risorsa	Limite
VDA multisessione per catalogo	500
VDA a sessione singola per catalogo	1,200
VDA per abbonamento Microsoft Azure	2,500

Limiti di utilizzo

Risorsa	Limite
Amministratori completi di Monitoraggio simultaneo	5
Utenti finali simultanei	100,000
Risorse pubblicate per un singolo utente	250
Lancio di sessioni al minuto	3,000

Limiti di prova

Nella tabella seguente sono elencati i limiti durante una prova di Citrix DaaS per Azure.

Abbonamento Azure	Risorsa	Limite
Sottoscrizione Citrix Managed Azure	Numero massimo di cataloghi	3
	Numero massimo di utenti	25
	Numero massimo di VDA per catalogo	3
Abbonamento Azure gestito dal cliente	Numero massimo di cataloghi	10
	Numero massimo di utenti	25
	Numero massimo di VDA per catalogo	10

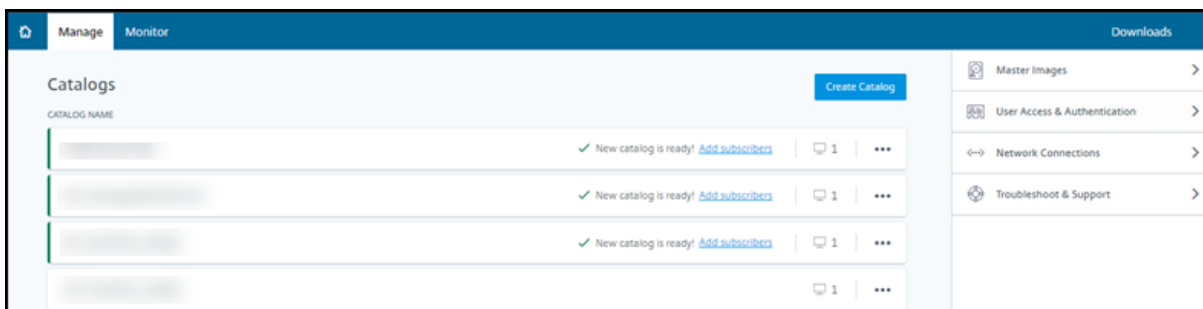
Riferimenti

September 7, 2022

Dashboard

La maggior parte delle attività di amministratore per Citrix DaaS Standard for Azure (in precedenza Citrix Virtual Apps and Desktops Standard for Azure service) possono essere inserite tramite i dash-

board **Gestisci e monitora**. Dopo aver creato il primo catalogo, la dashboard **Gestisci** viene avviata automaticamente quando si accede a Citrix Cloud e si seleziona Citrix DaaS for Azure.



Puoi accedere alle dashboard dopo che la tua richiesta di prova o acquisto è stata approvata e completata.

Per accedere alle dashboard:

1. Accedere a [Citrix Cloud](#).
2. Nel menu in alto a sinistra, seleziona **I miei servizi > DaaS Standard for Azure**. (In alternativa, puoi fare clic su **Gestisci** nel riquadro **DaaS Standard for Azure** nell'area principale del display).
3. Se un catalogo non è ancora stato creato, fai clic su **Inizia** nella pagina di **benvenuto**. Verrai indirizzato alla dashboard **Gestisci > Distribuzione rapida di Azure**.
4. Se un catalogo è già stato creato, verrai indirizzato automaticamente alla dashboard **Gestisci > Distribuzione rapida di Azure**.
5. Per accedere alla dashboard **Monitor**, fare clic sulla scheda **Monitor**.

Per una guida all'interno del prodotto dalla dashboard, fai clic sull'icona nell'angolo in basso a destra.



Schede catalogo nella dashboard Gestisci

Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, fai 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](#), [modificare](#) o [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 ulteriori informazioni, vedere [Gestire i cataloghi](#). Molte delle azioni della macchina sono disponibili anche dal dashboard **Monitor**. Vedere [Macchine per il monitoraggio e il controllo dell'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

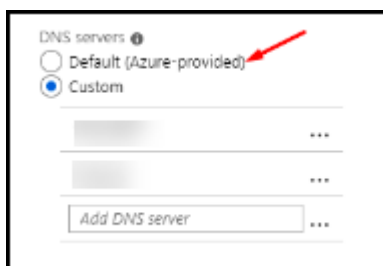
Questa sezione si applica a tutte le distribuzioni che contengono [computer collegati al dominio](#). È possibile ignorare questa sezione se si utilizzano solo macchine non aggiunte a un dominio.

1. Prima di creare un catalogo unito a un dominio (o una connessione, se si utilizza una sottoscrizione di Citrix Managed Azure), verificare se sono presenti voci del server DNS in grado di risolvere nomi di dominio pubblici e privati.

Quando Citrix DaaS for Azure crea un catalogo o una connessione, cerca almeno una voce valida del server DNS. Se non vengono trovate voci valide, l'operazione di creazione ha esito negativo.

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 avere almeno una voce valida. Citrix DaaS for Azure non può essere utilizzato con l'**impostazione predefinita (fornita da Azure)**.



- Se **Predefinito (fornito da Azure)** è abilitato, modificare l'impostazione **su Personalizzata** e aggiungere almeno una voce del server DNS.
- Se disponete già di voci server DNS in **Personalizzate**, verificate che le voci che desiderate utilizzare con Citrix DaaS for Azure possano risolvere nomi IP di dominio pubblico e privato.
- 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 utilizzi la tua sottoscrizione di Azure, puoi modificarli in Azure (come descritto nei passaggi precedenti). In alternativa, potete modificarli in Citrix DaaS for Azure.
- Quando si utilizza una sottoscrizione Citrix Managed Azure, Citrix DaaS for Azure non sincronizza le modifiche all'indirizzo DNS apportate in Azure. Tuttavia, potete modificare le impostazioni DNS per la connessione in Citrix DaaS for Azure.

Tieni 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 Citrix DaaS per Azure

Prima di aggiungere un indirizzo server DNS a una connessione, assicurarsi che il server DNS sia in grado di risolvere 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 l'indirizzo di un server DNS durante la creazione di una connessione, fare clic su **Modifica server DNS** nella pagina **Aggiungi tipo di connessione**. In alternativa, se un messaggio indica che non sono stati trovati indirizzi server DNS, fare clic su **Aggiungi server DNS**. Continuare con il passaggio 3.
2. Per aggiungere, modificare o rimuovere un indirizzo del server DNS per una connessione esistente:
 - a) Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Connessioni di rete** sulla destra.
 - b) Selezionare la connessione che si desidera modificare.
 - c) Fai clic su **Modifica server DNS**.
3. Aggiungi, modifica o rimuovi indirizzi.
 - a) Per aggiungere un indirizzo, fare clic su **Aggiungi server DNS** e quindi immettere 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, fai clic sull'icona del cestino accanto alla voce dell'indirizzo. Non è possibile rimuovere tutti gli indirizzi dei server DNS. La connessione deve avere almeno una.

4. Al termine, fai clic su **Conferma modifiche** nella parte inferiore della pagina.
5. Riavvia tutti i computer 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. Utilizzare il comando **Esegui** per avviare `gpedit.msc`, che apre l'Editor criteri di gruppo.
4. In `User Configuration Citrix Policies > Unfiltered`, fai clic su **Modifica criterio**.

Se la console di gestione Criteri di gruppo non riesce (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 appartenenti al dominio, dal passaggio 2 fino alla fine.

Nota:

Sebbene la console di Citrix Studio non sia disponibile in Citrix DaaS per Azure, consultate gli articoli di [riferimento sulle impostazioni dei criteri](#) per informazioni su ciò che è disponibile.

Azioni sulla posizione delle risorse

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. Vedere [Impostazioni ubicazione risorse durante la creazione di un catalogo](#).

(Per l'accesso remoto al PC, è possibile creare la posizione delle risorse e i connettori cloud.)

Questa sezione descrive le azioni disponibili dopo la creazione di una posizione risorsa.

1. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Sottoscrizioni cloud** a destra.
2. Fai clic sull'abbonamento.
 - La scheda **Dettagli** mostra il numero e i nomi dei cataloghi e delle immagini nell'abbonamento. Indica inoltre il numero di macchine in grado di distribuire desktop o app. Tale conteggio non include le macchine utilizzate per altri scopi, ad esempio immagini, Connettori cloud o server licenze RDS
 - Nella scheda **Posizioni risorse** sono elencate le ubicazioni di ogni 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 per il Cloud Connector che si desidera riavviare. Clicca su **Riavvia**.

Aggiungi connettori

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 **Sì**, specificare il nome di dominio completo del server proxy o l'indirizzo IP e il numero di porta.

Al termine, fai clic su **Aggiungi connettori**.

Elimina connettori

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 per il Cloud Connector che si desidera eliminare. Quindi clicca su **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 è disponibile un aggiornamento. Quando hai finito, fai clic su **Salva**.

Rinomina

Immettere il nuovo nome per l'ubicazione della risorsa. Fare clic su **Save** (Salva).

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 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

1. Installare un server licenze di Servizi Desktop remoto in una delle macchine virtuali disponibili. La VM 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 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.

Nella scheda **Generale** del dashboard **Gestisci > Distribuzione rapida di Azure**, il valore **Consumo** indica la quantità di consumo utilizzata nel mese di calendario corrente. Tale valore include gli impegni mensili e a termine.

Quando fai clic su **Generale**, la scheda **Notifiche** include:

- Consumo totale utilizzato per il mese (mensile e per periodo).
- 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, consulta [Monitorare le licenze e l'utilizzo di Citrix DaaS Standard for Azure](#).

Facoltativamente, puoi richiedere che le notifiche vengano visualizzate nella dashboard **Gestisci** quando l'utilizzo del consumo (per impegni mensili, a termine o entrambi) raggiunge un livello specificato. Per impostazione predefinita, le notifiche sono disattivate.

1. Nella scheda **Notifiche**, fai clic su **Modifica preferenze di notifica**.
2. Per abilitare le notifiche, fare clic sul dispositivo di scorrimento in modo che venga visualizzato il segno di spunta.
3. Immettere un valore. Ripetere l'operazione per l'altro tipo di consumo, se necessario.
4. Fare clic su **Save** (Salva).

Per disattivare le notifiche, fare clic sul dispositivo di scorrimento in modo che il segno di spunta non venga più visualizzato, quindi fare clic su **Salva**.

Monitorare l'utilizzo delle licenze Citrix

Per visualizzare le informazioni sull'utilizzo delle licenze Citrix, segui le linee guida in [Monitoraggio delle licenze e dell'utilizzo di Citrix DaaS Standard for Azure](#). 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 (come Studio o Quick Deploy).

Assicurati di aver configurato i limiti massimi di sessione per tutti i cataloghi prima di procedere.

- Nell'interfaccia di gestione Quick Deploy per Citrix DaaS for Azure, tale impostazione si trova nella scheda **Dettagli** di ciascun catalogo.
- In altri servizi ed edizioni Citrix DaaS, utilizzate le impostazioni dei criteri di gestione del carico.

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.

È possibile configurare uno dei due metodi di bilanciamento del carico: orizzontale o verticale. Il metodo si applica a tutti i cataloghi multiseSSIONE (e quindi a tutti i computer multiseSSIONE) nella distribuzione del servizio.

- **Bilanciamento del carico orizzontale:** una sessione utente in entrata viene assegnata alla macchina meno caricata disponibile.

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 al computer acceso con l'indice di carico più alto. (Citrix DaaS for Azure calcola e quindi assegna un indice di carico per ogni macchina multiseSSIONE. Il calcolo prende in considerazione 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. Dalla dashboard **Gestisci > Distribuzione rapida di Azure**, espandi **Generale** a destra.
2. In **Impostazioni globali**, fai clic su **Visualizza tutto**.
3. Nella pagina **Impostazioni globali**, in **Bilanciamento del carico del catalogo multiseSSIONE**, scegliere il metodo di bilanciamento del carico.
4. Fai clic su **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 **Gestisci > Dashboard di distribuzione rapida di Azure**, avvia il [processo di creazione del catalogo](#) fornendo le informazioni richieste e quindi facendo clic su **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 della risorsa inizia con "DAS", a meno che non sia stato fornito un nome di posizione della risorsa durante la creazione del catalogo. Nella console di Citrix DaaS for Azure, espandere le **sottoscrizioni cloud**. Nella scheda **Posizioni risorse**, controlla se la posizione della risorsa appena creata contiene connettori cloud. 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, [installa un Cloud Connector](#) su ogni VM. Assicurati che i Connettori Cloud si trovino nella stessa posizione delle risorse create in precedenza. Segui le indicazioni riportate in:
 - [Configurazione proxy e firewall di Cloud Connector](#)
 - [Requisiti di sistema e connettività](#)
5. Dal dashboard **Gestisci > Distribuzione rapida di Azure**, ripeti 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

- Rivedi [la risoluzione dei problemi](#).
- Se hai bisogno di ulteriore assistenza con Citrix DaaS for Azure, apri un ticket di supporto seguendo le indicazioni in [Come ottenere assistenza e supporto](#).



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).