Citrix Virtual Apps and Desktops 7 2402 LTSR

Contents

Citrix Virtual Apps and Desktops 7 2402 LTSR

August 22, 2024

Informazioni sulla versione

Il programma Long Term Service Release (LTSR) per Citrix Virtual Apps and Desktops fornisce stabilità e supporto a lungo termine per le release di Citrix Virtual Apps and Desktops.

Gli LTSR sono disponibili anche per Citrix Virtual Apps and Desktops 2203 e 1912.

Questa versione di Citrix Virtual Apps and Desktops include nuove versioni di Windows Virtual Delivery Agent (VDA) e nuove versioni di diversi componenti principali. È possibile effettuare le seguenti operazioni:

- **Installare o aggiornare un sito**: utilizzare l'ISO di questa versione per installare o aggiornare i componenti principali e i VDA. L'installazione o l'aggiornamento alla versione più recente consente di utilizzare le funzionalità più recenti.
- **Installare o aggiornare i VDA in un sito esistente**: se si dispone già di una distribuzione e non si è pronti per l'aggiornamento dei componenti principali, è comunque possibile utilizzare alcune delle più recenti funzionalità HDX installando (o eseguendo l'aggiornamento a) un nuovo VDA. L'aggiornamento dei soli VDA può essere utile quando si desidera testare i miglioramenti in un ambiente non di produzione.

  Dopo aver aggiornato i VDA a questa versione, non è necessario aggiornare il livello funzionale del catalogo macchine. Per ulteriori informazioni, vedere Versioni VDA e livelli funzionali.

Per istruzioni di installazione e aggiornamento:

- Se si sta creando un nuovo sito, seguire la sequenza in Installazione e configurazione.
- Se si sta aggiornando un sito, vedere Aggiornare una distribuzione.

Citrix Virtual Apps and Desktops 7 2402 LTSR

Secure HDX (anteprima)

È ora possibile utilizzare Secure HDX, una soluzione ALE (Application Level Encryption) che impedisce a qualsiasi elemento di rete nel percorso di traffico di ispezionare il traffico HDX. Per ulteriori informazioni, vedere HDX sicuro.

Nuovo criterio HDX Graphics: consente il blocco dello schermo di Windows

Con il nuovo criterio **Allow Windows screen lock** (Consenti il blocco dello schermo di Windows) in HDX Graphics, ora si ha la possibilità di modificare i timeout di visualizzazione di Windows in una sessione di Citrix Virtual Desktop sul sistema operativo Workstation in base alle proprie esigenze.
Per ulteriori informazioni, vedere Consentire il blocco dello schermo di Windows.

Nuova modalità di tolleranza alle perdite per i criteri audio

La modalità di tolleranza alle perdite per l'audio è ora disponibile per consentire la trasmissione dell'audio tramite il criterio della modalità di tolleranza alle perdite.
Per ulteriori informazioni, vedere Modalità di tolleranza alle perdite.

File binari di terze parti con firma

I file binari distribuiti da Citrix sono ora firmati. I file binari firmati sono convalidati da certificati generati da Citrix o da certificati autentici di terze parti. Per ulteriori informazioni, vedere Installare i VDA.

Log di sistema migliorati per il reindirizzamento dei contenuti del browser

Con i miglioramenti apportati ai log di sistema, il reindirizzamento dei contenuti del browser ora consente agli amministratori di monitorare lo stato della funzionalità. Per ulteriori informazioni, vedere How to troubleshoot browser content redirection.

Configurazione avanzata del reindirizzamento bidirezionale dei contenuti

In precedenza, la configurazione del reindirizzamento bidirezionale dei contenuti comportava la gestione di tre criteri distinti: Allow bidirectional content redirection (Consenti il reindirizzamento bidirezionale dei contenuti), Allow redirection of URLs to VDA (Consenti il reindirizzamento degli URL al VDA) e Allow redirection of URLs to the Client (Consenti il reindirizzamento degli URL al client). Questi criteri richiedono configurazioni sia sul lato server che sul lato client (tramite Criteri di gruppo). A partire da questa versione, abbiamo consolidato tutti e tre i criteri in un unico criterio unificato. Non solo semplifica e migliora il processo di configurazione, ma elimina anche la necessità di configurazioni lato client.
Per ulteriori informazioni, vedere Configurazione del reindirizzamento bidirezionale dei contenuti.

HDX Reducer

È ora possibile configurare la versione dell'algoritmo di compressione HDX, o Reducer, che si desidera utilizzare nell'host della sessione.
Per ulteriori informazioni, vedere HDX Reducer.

Nuova impostazione del registro HDX per la configurazione del timeout EDT

Ora è possibile configurare il timeout EDT impostando il registro. Per ulteriori informazioni, vedere Configurare il timeout EDT.

Ottimizzazione di Microsoft Teams: voce di registro inserita nell'elenco degli elementi consentiti

A partire da Citrix Virtual Apps and Desktops 2402, non è più necessario configurare manualmente la voce di registro `msedgewebview2.exe` poiché è consentita per impostazione predefinita.

Per ulteriori informazioni, vedere la documentazione Microsoft.

Supporto dell'elenco di elementi consentiti nel canale virtuale per le variabili di ambiente

È ora possibile utilizzare le variabili di ambiente di sistema nel percorso dei processi attendibili. Per ulteriori informazioni, vedere Using system environment variables.

Citrix Secure Private Access per ambienti locali

Accesso privato sicuro per ambienti locali e supporto per ZTNA e altri miglioramenti

La soluzione locale Citrix Secure Private Access migliora il livello generale di sicurezza e conformità di un'organizzazione grazie alla capacità di fornire facilmente un accesso zero-trust alle app basate su browser (app Web interne e SaaS) utilizzando il portale StoreFront locale come portale di accesso unificato alle app Web e SaaS, insieme alle app e ai desktop virtuali come parte integrata di Citrix Workspace. Citrix Secure Private Access locale è una soluzione Zero Trust Network Access (ZTNA) gestita dal cliente che fornisce alla VPN meno accesso alle applicazioni Web e SaaS interne con quanto segue insieme a un'esperienza utente finale senza interruzioni:

- Principio del minimo privilegio
- Single Sign-On (SSO)
- Autenticazione a più fattori
- Valutazione della postura del dispositivo

- Controlli di sicurezza a livello di applicazione
- Funzionalità di protezione delle app

Per ulteriori informazioni, vedere Citrix Secure Private Access for on-premises –General Availability.

Virtual Delivery Agent (VDA) 2402 LTSR

Opzione per installare, aggiornare o disinstallare Citrix Workspace App durante l'installazione, l'aggiornamento o la disinstallazione dei VDA

Questa funzionalità consente di scegliere di installare, aggiornare o disinstallare l'app Citrix Workspace durante l'installazione, l'aggiornamento o la disinstallazione di un VDA nei seguenti scenari:

- Durante l'installazione di un VDA, è possibile scegliere di installare l'app Citrix Workspace. Per impostazione predefinita, l'app Citrix Workspace non viene installata durante l'installazione del VDA.
- Durante un aggiornamento del VDA, se l'app Citrix Workspace non è già installata nel VDA, è possibile scegliere di installare l'app Citrix Workspace.
- Durante un aggiornamento del VDA, se la versione dell'app Citrix Workspace può essere aggiornata, viene visualizzata l'opzione per aggiornarla.
- Durante la disinstallazione di un VDA, è possibile scegliere di non disinstallare l'app Citrix Workspace. Per impostazione predefinita, l'app Citrix Workspace viene disinstallata durante la disinstallazione del VDA. Per ulteriori informazioni, vedere Selezionare i componenti da installare e il percorso di installazione e Opzioni della riga di comando per installare un VDA.

Supporto WebSocket per VDA

Citrix Virtual Apps and Desktops ora consente di utilizzare la tecnologia WebSocket tramite il Citrix Brokering Protocol (CBP) per facilitare la comunicazione tra VDA e Delivery Controller. Questa funzionalità richiede solo la porta TLS 443 per la comunicazione dal VDA al Delivery Controller.

Per ulteriori informazioni, vedere Comunicazione WebSocket tra VDA e Delivery Controller.

Supporto degli aggiornamenti VDA da una condivisione di file locale a cui i VDA hanno accesso (anteprima)

È ora possibile supportare gli aggiornamenti VDA da una condivisione di file locale e specificare la posizione del programma di installazione del VDA tramite i comandi PowerShell. Per ulteriori informazioni, vedere Supportare gli aggiornamenti VDA da una condivisione file locale.

Web Studio

Supporto del provisioning di VM VMware utilizzando i profili macchina

Quando si esegue il provisioning di macchine virtuali VMware utilizzando Machine Creation Service (MCS), è ora possibile selezionare un modello esistente come profilo macchina, lasciando che le macchine virtuali all'interno del catalogo ereditino le impostazioni dalla macchina virtuale selezionata.

Le impostazioni ereditate includono:

- Tag inseriti nel modello
- Attributi personalizzati
- Criteri di archiviazione vSAN
- Versione hardware virtuale
- vSphere Virtual TPM (vTPM)
- Numero di CPU e core per socket
- Numero NIC

Per ulteriori informazioni, vedere Creare cataloghi di macchine.

Gestire le immagini preparate con il nodo Images

In Web Studio è ora disponibile un nodo **Immagini**, che consente di preparare un'immagine MCS (immagine preparata) da un'unica immagine di origine e di distribuirla su vari cataloghi di macchine MCS. Questo nodo facilita la gestione completa del ciclo di vita delle immagini, consentendo di creare definizioni, versioni e cataloghi di immagini.

Le immagini preparate utilizzando questo nodo possono essere utilizzate solo in ambienti Azure e VMware. Per informazioni dettagliate sulla gestione delle immagini, vedere Gestione delle immagini (anteprima).

In alternativa, è anche possibile creare cataloghi con immagini preparate utilizzando il nodo **Machine Catalogs**. Per ulteriori informazioni, vedere Creare cataloghi di macchine.

Criteri correlati

Nuove convalide dei criteri. Sono state aggiunte ulteriori convalide dei criteri. Di conseguenza, l'abilitazione dei criteri o l'esecuzione di un aggiornamento sul posto potrebbe comportare la perdita dei dati dei criteri se sono presenti impostazioni dei criteri non valide. Se si creano o si modificano i criteri utilizzando un metodo diverso da Web Studio, Citrix consiglia di utilizzare la versione più recente dell'SDK e dello snap-in. Per ulteriori informazioni, vedere CTX676686.

Funzionalità deprecate

Le seguenti funzionalità e impostazioni sono state deprecate in Web Studio:

- Ambienti Azure:

  Il provisioning delle VM utilizzando un'immagine master di una regione diversa è stato deprecato. Si consiglia di utilizzare Azure Compute Gallery per replicare l'immagine master nella regione in cui verranno create le macchine virtuali.

- Ambienti AWS:

  L'opzione **Apply machine template properties to virtual machines**, nella pagina **Machine Catalog Setup > Machine Template** è stata deprecata. Consigliamo invece di utilizzare i profili macchina per specificare le proprietà della macchina per le VM.

- Tutti gli ambienti di hypervisor e servizi cloud:

  La configurazione della cache di write-back con solo una cache su disco e nessuna cache di memoria è stata deprecata. Si consiglia di impostare la dimensione della cache di memoria su un valore superiore a zero.

Citrix Director

Integrazione di Secure Private Access con Director (anteprima)

L'integrazione di Secure Private Access con Director consente all'amministratore dell'help desk o all'amministratore completo di monitorare e risolvere tutte le sessioni di Secure Private Access in Director. Per supportare questa funzionalità, è necessario utilizzare la versione 2402 o le versioni successive di Director, Secure Private Access, app Citrix Workspace e VDA.

Le azioni disponibili includono la visualizzazione dei dettagli di quanto segue:

- Sessioni attive di Secure Private Access per un utente nel popup **Select a Session (Seleziona una sessione)** > scheda **Sessions** > **Web Apps and SaaS Apps**
- Enumerazioni non riuscite o bloccate di Secure Private Access e avvii non riusciti dell'app nel popup **Select a Session** (Seleziona una sessione) > scheda **Denied Access** (Accesso negato)
- Visualizzazione dei dettagli della sessione e dell'applicazione per gli avvii delle app attivi e non riusciti
- Visualizzazione dei dettagli della sessione e dell'applicazione per le enumerazioni non riuscite e bloccate

Per ulteriori informazioni, vedere la pagina Integrazione di Secure Private Access con Director (anteprima).

Pannello delle metriche delle prestazioni migliorato

Il pannello **Performance Metrics** (Metriche delle prestazioni) ha una visualizzazione migliorata delle metriche in tempo reale. Quando si fa clic sulla scheda **Session Performance** (Prestazioni della sessione), insieme ai dati in tempo reale, è possibile visualizzare i dati degli ultimi 15 minuti senza attendere il tempo di caricamento della pagina. Questo miglioramento aiuta a ridurre il tempo medio di risoluzione consentendo agli amministratori di correlare le metriche delle prestazioni di più componenti in un'unica visualizzazione. Per ulteriori informazioni, vedere la sezione Metriche delle prestazioni.

Supporto della versione più recente di Microsoft Teams

Citrix Director ora supporta Microsoft Teams versione 2.1 o precedente.

Machine Creation Services (MCS)

Gestione delle immagini (anteprima)

Con la funzionalità di gestione delle immagini, MCS separa la fase di masterizzazione dal generale flusso di lavoro di provisioning.

È possibile preparare un'immagine MCS (immagine preparata) da un'unica immagine di origine e utilizzarla su più cataloghi di macchine MCS diversi. Questa implementazione riduce significativamente i costi di archiviazione e legati ai tempi; inoltre semplifica il processo di distribuzione delle VM e di aggiornamento delle immagini.

I vantaggi dell'utilizzo di questa funzionalità di gestione delle immagini sono:

- Generazione di immagini preparate in anticipo senza creare un catalogo.
- Riutilizzo delle immagini preparate in più scenari, come la creazione e l'aggiornamento di un catalogo.
- Significativa riduzione dei tempi di creazione o aggiornamento del catalogo.

Per informazioni dettagliate sulla gestione delle immagini, vedere Gestione delle immagini (anteprima).

Configurare le autorizzazioni di connessione host di Azure richieste

In precedenza, il test della connessione host verificava se la credenziale fosse valida per connettersi all'hypervisor. Il test non eseguiva la convalida delle autorizzazioni effettive di cui si potrebbe aver bisogno per eseguire operazioni MCS pertinenti come la gestione dell'alimentazione, la creazione di VM e molte altre.

Con questa funzionalità, è ora possibile configurare facilmente tutte le autorizzazioni minime richieste perché un responsabile del servizio o un account utente in Azure collegato a una connessione host esegua tutte le operazioni MCS utilizzando un modello ARM. Questo modello ARM automatizza quanto segue:

- Creazione di un ruolo di Azure con le autorizzazioni minime necessarie per le operazioni.
- Assegnazione di questo ruolo a un'entità di servizio di Azure esistente a livello di sottoscrizione.

È possibile distribuire questo modello ARM utilizzando il portale di Azure o i comandi PowerShell. Per ulteriori informazioni, vedere Modello ARM per le operazioni CVAD.

Verificare la presenza di più NIC in VMware

Negli ambienti VMware, abbiamo introdotto vari controlli preliminari quando l'unità di hosting e il modello di profilo macchina hanno più reti e il parametro `-NetworkMapping` viene utilizzato nei comandi `New-ProvScheme` e `Set-ProvScheme`. Per ulteriori informazioni sull'elenco di controllo preliminare per più NIC, vedere Verificare la presenza di più NIC.

Supporto della creazione di VM Windows 11 in GCP

È ora possibile creare VM Windows 11 in GCP. Se si installa Windows 11 sull'immagine master, è necessario abilitare vTPM durante il processo di creazione dell'immagine master. Inoltre, è necessario abilitare vTPM sull'origine del profilo della macchina (VM o modello di istanza).

Questa funzionalità è applicabile a:

- Cataloghi di macchine MCS persistenti e non persistenti
- Solo il gruppo di nodi con unico tenant

Per informazioni sulla creazione di macchine virtuali Windows 11 sul nodo con unico tenant, vedere Creare macchine virtuali Windows 11 sul nodo con unico tenant.

Supporto della creazione di cataloghi Citrix Provisioning utilizzando i comandi MCS PowerShell in VMware

È ora possibile creare cataloghi Citrix Provisioning utilizzando i comandi MCS PowerShell in VMware.

Questa implementazione offre i seguenti vantaggi:

- Un'unica API unificata per gestire i cataloghi MCS e Citrix Provisioning.
- Vi sono nuove funzionalità per i cataloghi Citrix Provisioning, quali la soluzione di gestione delle identità, il provisioning su richiesta e così via.

Per ulteriori informazioni, vedere Creare cataloghi Citrix Provisioning in Citrix Studio.

Profile Management

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

VDA Linux

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Registrazione della sessione

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Workspace Environment Management

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Citrix Provisioning

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Federated Authentication Service

Per informazioni sulle nuove funzionalità, vedere l'articolo Novità nel relativo documento.

Componenti di base della versione iniziale 2402 LTSR

Componente di base 2402	Versione come indicato in Programmi e funzionalità	Documentazione
VDA a sessione singola	2402.0.4000.4310	VDA a sessione singola
VDA multisessione	2402.0.4000.4310	VDA multisessione
Delivery Controller	7.41.100.229	Delivery Controller
Citrix Studio	7.41.100.251	Citrix Studio
Citrix Director	7.33.4000.26	Citrix Director

Componente di base 2402	Versione come indicato in Programmi e funzionalità	Documentazione
Gestione dei criteri di gruppo Citrix	7.41.100.115	Gestione dei criteri di gruppo Citrix
Estensione lato client dei Criteri di gruppo Citrix	7.41.100.115	
Citrix StoreFront	2402.0.100.64	Citrix StoreFront
Citrix Provisioning	7.41.100	Citrix Provisioning
Universal Print Server	7.33.4000.11	Universal Print Server
Registrazione della sessione	24.2.100.35	Registrazione della sessione
VDA Linux	24.02.0.93	Virtual Delivery Agent per Linux
Profile Management	24.2.100.52	Profile Management
Federated Authentication Service Citrix	10.17.100.90	Citrix Federated Authentication Service (FAS)
Reindirizzamento del contenuto del browser	15.32.4000.12	Reindirizzamento del contenuto del browser
Citrix Probe Agent 2402	7.41.100.78	Download

Componenti compatibili con la versione iniziale 2402 LTSR

I seguenti componenti, nelle versioni indicate di seguito, sono compatibili con gli ambienti LTSR. Non sono idonei per i vantaggi LTSR (ciclo di vita esteso e aggiornamenti cumulativi di sola correzione). Citrix potrebbe richiedere l'aggiornamento a una versione più recente di questi componenti all'interno degli ambienti 2402.

Componenti e caratteristiche compatibili	Versione come indicato in Programmi e funzionalità	Documentazione
HDX RealTime Optimization Pack	2.9.600	HDX RealTime Optimization Pack
Server di licenza	11.17.2.0_BUILD_47000	Server di licenza
Livello di personalizzazione utente	23.9.1	Livello di personalizzazione utente
Lettore Web di registrazione della sessione	22.3.4000.4	Lettore Web di registrazione della sessione

Componenti e caratteristiche compatibili	Versione come indicato in Programmi e funzionalità	Documentazione
Ottimizzazione di Microsoft Teams	15.32.3000.9	Ottimizzazione di Microsoft Teams
Workspace Environment Management	2402.1.100.1	Workspace Environment Management

Esclusioni notevoli dalla versione iniziale 2402 LTSR

Le seguenti funzionalità, componenti e piattaforme non sono idonei per le tappe e i vantaggi del ciclo di vita della versione 2402. In particolare, sono esclusi gli aggiornamenti cumulativi e i vantaggi per il ciclo di vita. Gli aggiornamenti delle funzioni e dei componenti esclusi sono disponibili tramite le normali versioni correnti.

Componenti e funzionalità esclusi
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
Integrazione StoreFront Citrix Online

Piattaforme Windows escluse*
Windows 2008 a 32 bit (per Universal Print Server)

* Citrix si riserva il diritto di aggiornare il supporto della piattaforma in base alle tappe del ciclo di vita dei fornitori terzi.

Problemi risolti

August 22, 2024

Citrix Virtual Apps and Desktops 7 2402 LTSR include i seguenti problemi risolti:

Aspetti generali

- Quando il nome del dispositivo audio è composto da più di 200 caratteri, il dispositivo potrebbe non riuscire a reindirizzarsi alla sessione virtuale. [HDX-58341]
- Per il reindirizzamento della webcam, il client RDP fino al secondo hop non è supportato. [HDX-55630]
- Quando si esegue la scansione di un'immagine in una sessione desktop con l'ambiente configurato come descritto di seguito, l'immagine potrebbe non essere scansionata. Questo problema è intermittente.

  - Installazione del driver dello scanner e dell'applicazione di imaging.
  - Politica di direzione USB abilitata su DDC.
  - Configurazione dell'ambiente:
    * DDC: Win2K19 + 7.33CU4
    * VDA: Win2k19/Win2k16+ 7.40.0.191
    * Client: Win10x64 22H2 + CWA 24.1.0.597

  [HDX-58888]
- L'avvio di una seconda app senza interruzioni non riesce se SSL è abilitato e l'affidabilità sessione è disattivata. Se viene avviata un'app senza interruzioni, il successivo avvio di un'altra app senza interruzioni sullo stesso server deve essere effettuato nella sessione esistente (condivisione della sessione), mentre il client tende ad avviare l'app in una nuova sessione causando l'invio di una richiesta di convalida inaspettata al broker. [HDX-52439].
- Se si utilizza l'audio mono per i flussi audio stereo, potrebbe sentirsi solo un canale audio su uno solo dei due auricolari invece di ricevere entrambi i canali su entrambe le orecchie. [HDX-56344]

Delivery Controller

- Gli aggiornamenti sulla tabella `MonitorData.ResourceUtilization` nel database di monitoraggio sono ritardati. [CVADHELP-22724]
- Quando si utilizza una versione VDA 2203 CU3 con Windows 10, il programma di installazione del VDA non ospita la porta WCF personalizzata se è configurato Rendezvous Proxy. [CVADHELP-24199]

Director

- Quando si utilizza un VDA desktop multisessione o a sessione singola in un **Multi Forest Site**, la funzionalità di ricerca incentrata sull'utente non funziona. [CVADHELP-23174]

Grafica

- Per Windows 11 versione 22H2, quando si sposta una finestra di Windows Media Player all'interno di una sessione, viene visualizzata solo la metà inferiore del video. Per ovviare al problema, selezionare: Impostazioni > Sistema > Multitasking > Snap windows (Accosta finestre) > Show snap layouts when I drag a window to the top of my screen (Mostra layout istantanei quando trascino una finestra nella parte superiore dello schermo) [HDX-42092]
- Quando si utilizza Citrix Virtual Apps and Desktops 2203, è possibile osservare una schermata nera durante la riconnessione alle sessioni disconnesse. [CVADHELP-23615]

Criterio

- Dopo l'aggiornamento di Citrix Virtual Apps and Desktops dalla versione 1912 LTSR CU3 alla versione CU4 o CU5, i VDA potrebbero non registrarsi presso il Delivery Controller e rimanere non registrati. [CVADHELP-19834]
- `CSEngine.exe` sta consumando più memoria del previsto sul VDA. [CVADHELP-20908, CVADHELP-19916]

Studio

- Gli amministratori personalizzati che non dispongono dell'ambito "Tutti"non possono modificare o eliminare i criteri dal set di criteri predefinito. Come soluzione alternativa, aggiungere un ambito al criterio predefinito a cui l'amministratore personalizzato può accedere. [GP-1569]
- Quando si utilizzano sia *Citrix Studio* che *Web Studio* nella distribuzione, è possibile che si verifichi questo: se si crea una cartella delle applicazioni in *Citrix Studio*, ma non vi si aggiunge alcuna applicazione, quella cartella vuota non viene visualizzata in *Web Studio*. [STUD-27526]
- Durante la creazione di una connessione di hosting ad Azure tramite Web Studio, se si fa clic su **Create service principal** (Creare entità di servizio) nella pagina **Connection Details** (Dettagli di connessione) e si fa clic su **Next**, si potrebbe ricevere un messaggio di errore. Per risolvere il problema, consentire i cookie di terze parti nel browser. [STUD-24463]
- Quando si aggiunge l'indirizzo del server StoreFront tramite Citrix Studio e lo si assegna a un gruppo di consegna, lo store è disattivato per impostazione predefinita. [CVADHELP-24862]

Universal Print Server

Stampa

- Quando si utilizza il VDA versione 1912 CU5 e la versione del sistema operativo 2012 R2, diversi lavori di stampa non riescono dal server di stampa Citrix UPS di produzione con il seguente messaggio di errore:
  `CCgpStream::Open: WaitForMultipleObjects time out. InternalUpcRemoteOpenSt : Failed to Open Stream. Abort Job.`
  [CVADHELP-22354]
- Quando si utilizza UPS versione 2212 o 2305 in Citrix Virtual Apps and Desktops versione 2212 o 2305 con VDA Windows 10, nelle stampanti che utilizzano CUPS viene visualizzato il seguente messaggio:
  `Access Denied, cannot connect message`
  [CVADHELP-23644]

VDA per sistema operativo a sessione singola

- Durante l'utilizzo del VDA Windows, è possibile che si verifichi un errore di mappatura della tastiera quando si passa dalla tastiera giapponese a quella coreana. [HDX-59307]
- I valori `SaveRsopToFile`, `SaveRsopToMemory` e `SaveRsopToRegistry` contenuti nella chiave di registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy` potrebbero non essere ripristinati. [CVADHELP-23184]
- Dopo aver aggiornato un VDA alla versione 2203, l'app Skype for Business potrebbe non rispondere nella schermata iniziale. [CVADHELP-21021]
- `CSEngine.exe` sta consumando più memoria del previsto sul VDA. [CVADHELP-19916]
- Un deadlock in Broker Agent impedisce alle macchine di registrarsi nuovamente in caso di modifica dell'IP DNS. [CVADHELP-18952]
- Questa correzione introduce l'opzione della riga di comando `/no_pending_reboot_check` che impedisce di verificare la presenza di un riavvio in sospeso da una precedente installazione di Windows sul computer, quando si installano o si aggiornano componenti principali. [CVADHELP-21686]
- Il processo `WebSocketService.exe` non viene avviato dopo il riavvio del VDA. [CVADHELP-24771]
- Quando si utilizza un VDA versione LTSR 2203 CU 4.1, il VDA potrebbe eseguire un controllo degli errori con il seguente messaggio in qualsiasi momento all'inizio di una sessione o nel corso della stessa.


```
Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys
```

[CVADHELP-24891]

- Quando si utilizza un computer, l'avvio della sessione utente non riesce a intermittenza. [CVADHELP-23922]
- Durante una riconnessione di una sessione ICA, la finestra di chat di un'applicazione di messaggistica di terze parti potrebbe apparire automaticamente in primo piano. [CVADHELP-24000]
- Il processo `Wfshell.exe` potrebbe bloccarsi quando si copiano e incollano file da una workstation locale nella sessione Citrix per VDA LTSR 2203. [CVADHELP-24146]
- Quando si utilizza un VDA per Windows 10 versione 2308, il processo `ctxappvservice.exe` potrebbe bloccarsi. [CVADHELP-24575]
- La copia di contenuti da Microsoft Visio o dall'app Visio pubblicata su un desktop in un'app sul dispositivo utente potrebbe non riuscire. [CVADHELP-23647]
- WebSocketService (servizio WebSocket di reindirizzamento video HTML5) potrebbe bloccarsi. [CVADHELP-23917]
- Un'applicazione impostata nella metà sinistra del monitor sinistro appare erroneamente al centro di questo schermo dopo la riconnessione quando si utilizzano Virtual Apps and Desktops 2203 LTSR, l'app Citrix Workspace 2203 LTSR CU3 (2303 o 2205) e il VDA 2203 LTSR con Windows 11 22h2. [CVADHELP-23878]

VDA per sistema operativo multisessione

- Il processo `WebSocketService.exe` potrebbe consumare più memoria del previsto sui VDA. [CVADHELP-23870]
- `CSEngine.exe` sta consumando più memoria del previsto sul VDA. [CVADHELP-19916]
- Un deadlock in Broker Agent impedisce alle macchine di registrarsi nuovamente in caso di modifica dell'IP DNS. [CVADHELP-18952]
- Il processo `WebSocketService.exe` non viene avviato dopo il riavvio del VDA. [CVADHELP-24771]
- Quando si utilizza un VDA versione LTSR 2203 CU 4.1, il VDA potrebbe eseguire un controllo degli errori con il seguente messaggio in qualsiasi momento all'inizio di una sessione o nel corso della stessa.
  `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys`
  [CVADHELP-24891]
- Alcuni processi dell'app Citrix Workspace potrebbero non chiudersi come previsto quando vengono eseguiti in una sessione di un'applicazione pubblicata. [CVADHELP-24225]

- Nel versione LTSR 2203 CU3, del VDA Server 2019 `WmiPrvSE.exe` si blocca. [CVADHELP-24436]
- Il processo `Wfshell.exe` potrebbe bloccarsi quando si copiano e incollano file da una workstation locale nella sessione Citrix per VDA LTSR 2203. [CVADHELP-24146]
- Il processo Terminal Services potrebbe bloccarsi dopo una riconnessione ACR. [CVADHELP-24364]
- In Windows Server 2022, se un mouse viene spostato in una posizione dedicata dall'app o dal sistema operativo, non è possibile spostare nuovamente il mouse in quella posizione finché non viene spostato in un'altra posizione dall'app o dal sistema operativo. [CVADHELP-24444]
- La finestra di dialogo **Warning Idle Time Expired Message** (Messaggio tempo di avviso di inattività scaduto) non viene visualizzata nella sessione ICA sul VDA del sistema operativo 2022 sebbene il limite di tempo di **inattività della sessione** abbia effetto. [CVADHELP-24646]
- La copia di contenuti da Microsoft Visio o dall'app Visio pubblicata su un desktop in un'app sul dispositivo utente potrebbe non riuscire. [CVADHELP-23647]

Profile Management

- La documentazione di Profile Management 2402 LTSR fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

VDA Linux

- La documentazione di Linux VDA 2402 LTSR fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Registrazione della sessione

- La documentazione di Session Recording 2402 LTSR fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Workspace Environment Management

- La documentazionedi Workspace Environment Management 2402 LTSR fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Citrix Provisioning

- La documentazione di Citrix Provisioning 2402 LTSR fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Federated Authentication Service

- La documentazione del Federated Authentication Service 2402 LTSR fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Requisiti di sistema

August 22, 2024

Introduzione

I requisiti di sistema contenuti in questo documento erano validi al momento del rilascio della versione del prodotto. Periodicamente vengono effettuati aggiornamenti. I requisiti di sistema per i componenti non descritti in questa sezione (ad esempio sistemi host, app Citrix Workspace e Citrix Provisioning) sono descritti nella rispettiva documentazione.

Vedere Prepararsi all'installazione prima di iniziare un'installazione.

A eccezione dei casi in cui è specificato, il programma di installazione dei componenti distribuisce automaticamente i prerequisiti software (ad esempio i pacchetti .NET e C++) se le versioni richieste non vengono rilevate sul computer. Il supporto di installazione Citrix contiene anche alcuni di questi prerequisiti software.

Il supporto di installazione contiene svariati componenti di terze parti. Prima di utilizzare il software Citrix, verificare la disponibilità di aggiornamenti di sicurezza forniti dalle corrispondenti terze parti e installarli.

Per informazioni sulla globalizzazione, vedere l'articolo CTX119253 del Knowledge Center.

Per i componenti e le funzionalità che possono essere installati sui server Windows, le installazioni di Nano Server non sono supportate, a meno che non sia specificato. Server Core è supportato solo per i Delivery Controller e Director.

Requisiti hardware

I valori di RAM e spazio su disco si aggiungono ai requisiti per l'immagine del prodotto, il sistema operativo e altri software presenti sul computer. Le prestazioni varieranno a seconda della configurazione. La configurazione include le funzionalità che sono in uso, più il numero di utenti e altri fattori. L'utilizzo solo del minimo può comportare prestazioni lente.

Nella tabella seguente sono elencati i requisiti minimi per i componenti principali.

Componente	Minimo
Tutti i componenti principali e StoreFront su un unico server, solo per una valutazione, non una distribuzione di produzione	5 GB RAM
Tutti i componenti principali e StoreFront su un unico server, per una distribuzione di prova o un piccolo ambiente di produzione	12 GB di RAM
Delivery Controller (maggiore spazio su disco necessario per la cache host locale)	5 GB di RAM, disco rigido da 800 MB, database: vedere Guida al dimensionamento
Studio	1 GB di RAM, disco rigido da 100 MB
Director	2 GB di RAM, disco rigido da 200 MB
StoreFront	2 GB di RAM, vedere la documentazione di StoreFront per consigli sui dischi
Server di licenza	8 GB di RAM, vedere la documentazione sulle licenze per consigli sui dischi

Dimensionamento delle macchine virtuali che forniscono desktop e applicazioni

Non è possibile fornire raccomandazioni specifiche a causa della natura complessa e dinamica delle offerte hardware e ogni implementazione presenta esigenze specifiche. In genere, il dimensionamento di una macchina virtuale Citrix Virtual Apps si basa sull'hardware e non sui carichi di lavoro degli utenti. L'eccezione è la RAM. È necessaria una quantità maggiore di RAM per le applicazioni che ne fanno maggior uso.

Per ulteriori informazioni:

- Citrix Tech Zone contiene linee guida sul dimensionamento.
- L'articolo Scalabilità di un singolo server di Citrix Virtual Apps and Desktops illustra quanti utenti o VM possono essere supportati su un singolo host fisico.

Microsoft Visual C++

Quando si installa un Delivery Controller, un Virtual Delivery Agent (VDA) o un Universal Print Server, il programma di installazione di Citrix installa automaticamente Microsoft Visual C++ 2015–2022 Redistributable.

- Se la macchina contiene una versione precedente di quel runtime (ad esempio 2015-2019), il programma di installazione di Citrix la aggiorna.
- Se la macchina contiene una versione precedente al 2015, Citrix installa la versione più recente in parallelo.

Delivery Controller

Sistemi operativi supportati:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core

Requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Windows PowerShell 3.0, 4.0 o 5.0.
- Microsoft Visual C++ 2015–2019 Redistributable.

Database

Versioni di Microsoft SQL Server supportate per la configurazione del sito, la registrazione della configurazione e il monitoraggio dei database:

- SQL Server 2022 edizioni Express, Standard ed Enterprise.
- SQL Server 2019 edizioni Express, Standard ed Enterprise.
- SQL Server 2017 edizioni Express, Standard ed Enterprise.
  - Per le nuove installazioni: per impostazione predefinita, SQL Server Express 2017 con aggiornamento cumulativo 16 viene installato durante l'installazione del controller, se non viene rilevata un'esistente installazione di SQL Server supportata.
  - Per gli aggiornamenti, qualsiasi versione esistente di SQL Server Express non viene aggiornata.
- SQL Server 2016 SP2 edizioni Express, Standard ed Enterprise.

Sono supportate le seguenti soluzioni di database ad alta disponibilità (ad eccezione di SQL Server Express, che supporta solo la modalità standalone):

- Istanze del cluster di failover AlwaysOn di SQL Server
- Gruppi di disponibilità AlwaysOn di SQL Server (inclusi i gruppi di disponibilità di base)
- Mirroring del database di SQL Server

L'autenticazione di Windows è necessaria per le connessioni tra il Controller e il database del sito di SQL Server.

Considerazioni sulla cache host locale: Microsoft SQL Server Express LocalDB è una funzionalità di SQL Server Express utilizzata dalla cache host locale in modo autonomo. La cache host locale non richiede componenti di SQL Server Express diversi da SQL Server Express LocalDB.

- Quando si installa un Controller, viene installato Microsoft SQL Server Express LocalDB 2019 con aggiornamento cumulativo 15 per l'utilizzo con la funzionalità Cache host locale. Questa installazione è separata dall'installazione predefinita di SQL Server Express per il database del sito.
- Quando si aggiorna un Controller, la versione esistente di Microsoft SQL Server Express LocalDB non viene aggiornata automaticamente. Per i requisiti e le procedure di sostituzione, vedere Sostituire SQL Server Express LocalDB.

Ulteriori informazioni sui database:

- Database
- CTX114501 elenca i database più supportati attualmente
- Guida al dimensionamento del database
- Cache host locale

Web Studio

> **Nota:**
>
> - È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.
> - Web Studio è una console di gestione basata sul Web che consente di configurare e gestire l'implementazione locale di Citrix Virtual Apps and Desktops. È progettata per una migliore esperienza utente e generalmente risponde più velocemente di Citrix Studio, la console di gestione basata su Windows. Vedere Installare Web Studio.

Sistemi operativi supportati:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core

Citrix Director

Sistemi operativi supportati:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core

Requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Microsoft Internet Information Services (IIS) 7.0 e ASP.NET 2.0. Verificare che nel ruolo del server IIS sia installato il servizio ruolo Contenuto statico. Se il software non è già installato, viene richiesto il supporto di installazione di Windows Server. Quindi, quel software viene installato.
- Per visualizzare i registri eventi sui computer in cui è installato Citrix Director, è necessario installare Microsoft.NET Framework 2.0.

Citrix Profile Management:

- Verificare che i plug-in WMI Citrix Profile Management e Citrix Profile Management siano installati nel VDA (pagina **Componenti aggiuntivi** della procedura guidata di installazione) e che Citrix Profile Management Service sia in esecuzione per visualizzare i dettagli del profilo utente in Director.

Requisiti di integrazione di System Center Operations Manager (SCOM):

- System Center 2012 R2 Operations Manager

Browser supportati per visualizzare Director:

- Internet Explorer 11. La modalità di compatibilità non è supportata per Internet Explorer. Utilizzare le impostazioni del browser consigliate per accedere a Director. Quando si installa Internet Explorer, accettare l'impostazione predefinita per utilizzare le impostazioni di protezione e compatibilità consigliate. Se si è già installato il browser e si è scelto di non utilizzare le impostazioni consigliate, andare a **Strumenti > Opzioni Internet > Avanzate > Reimposta** e seguire le istruzioni.

- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

La risoluzione ottimale dello schermo consigliata per la visualizzazione Director è 1440 x 1024.

Virtual Delivery Agent (VDA) per sistema operativo a sessione singola

Sistemi operativi supportati:

- Windows 11
- Windows 10 (solo x64), qualsiasi versione attualmente supportata dal supporto Mainstream.
  - Per informazioni sul supporto delle versioni, vedere l'articolo CTX224843 del Knowledge Center.

Requisiti:

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Microsoft Visual C++ 2015–2019 Redistributable.

Accesso remoto PC utilizza questo VDA, che viene installato sui PC fisici dell'ufficio. Questo VDA supporta Secure Boot per Accesso remoto PC di Citrix Virtual Desktops su Windows 11 e Windows 10.

Diverse funzionalità di accelerazione multimediale (ad esempio HDX MediaStream Windows Media Redirection) richiedono l'installazione di Microsoft Media Foundation nel computer in cui si installa il VDA. Se nel computer non è installato Media Foundation, le funzionalità di accelerazione multimediale non vengono installate e non funzionano. Non rimuovere Media Foundation dal computer dopo l'installazione del software Citrix. In caso contrario, gli utenti non possono accedere al computer. Nella maggior parte delle edizioni del sistema operativo Windows a sessione singola supportate, il supporto di Media Foundation è già installato e non può essere rimosso. Tuttavia, le edizioni N non includono determinate tecnologie relative ai supporti multimediali; è possibile ottenere tale software da Microsoft o da terze parti. Per ulteriori informazioni, vedere Prepararsi all'installazione.

Per informazioni sui VDA Linux, vedere gli articoli su Linux Virtual Delivery Agent.

Per utilizzare la funzionalità Server VDI, è possibile utilizzare l'interfaccia della riga di comando per installare un VDA per sistema operativo Windows a sessione singola in un computer Windows Server supportato. Per ulteriori informazioni, vedere VDI del server.

Per informazioni sull'installazione di un VDA su una macchina Windows 7, vedere Sistemi operativi precedenti.

Virtual Delivery Agent (VDA) per sistema operativo multisessione

Sistemi operativi supportati:

- Windows 11 (supportato solo con Citrix DaaS)
- Windows 10 (solo x64; supportato solo con Citrix DaaS), qualsiasi versione attualmente supportata dal supporto Mainstream.
- Windows Server 2022
- Windows Server 2019 edizioni Standard e Datacenter
- Windows Server 2016 edizioni Standard e Datacenter

Il programma di installazione implementa automaticamente i seguenti requisiti, che sono disponibili anche sul supporto di installazione Citrix nelle cartelle **Support** :

- Microsoft .NET Framework 4.8 viene installato automaticamente se non è già installato (o se ne è installata una versione successiva).
- Microsoft Visual C++ 2015–2019 Redistributable.

Il programma di installazione installa automaticamente e abilita i servizi ruolo Servizi Desktop remoto, se non sono già installati e abilitati.

Diverse funzionalità di accelerazione multimediale (ad esempio HDX MediaStream Windows Media Redirection) richiedono l'installazione di Microsoft Media Foundation nel computer in cui si installa il VDA. Se nel computer non è installato Media Foundation, le funzionalità di accelerazione multimediale non vengono installate e non funzionano. Non rimuovere Media Foundation dal computer dopo aver installato il software Citrix, altrimenti gli utenti non saranno in grado di accedere al computer. Nella maggior parte delle versioni di Windows Server, la funzionalità Media Foundation viene installata tramite Server Manager. Per ulteriori informazioni, vedere Prepararsi all'installazione.

Se Media Foundation non è presente sul VDA, queste funzionalità multimediali non funzionano:

- Reindirizzamento di Windows Media
- Reindirizzamento video HTML5
- Reindirizzamento webcam HDX RealTime

Per informazioni sui VDA Linux, vedere gli articoli su Linux Virtual Delivery Agent.

Per informazioni sull'installazione di un VDA su una macchina Windows Server 2008 R2, vedere Sistemi operativi precedenti.

Host/risorse di virtualizzazione

Sono supportati gli host/le risorse di virtualizzazione seguenti (in ordine alfabetico). Ove applicabile, sono supportate le versioni *major.minor*, inclusi gli aggiornamenti di tali versioni. L'articolo

CTX131239 del Knowledge Center contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

Alcune funzionalità potrebbero non essere supportate su tutte le piattaforme host o su tutte le versioni della piattaforma. Per ulteriori informazioni, vedere la documentazione della relativa funzionalità.

La funzionalità Riattivazione accesso remoto PC su LAN richiede Microsoft System Center Configuration Manager almeno 2012.

Hypervisor supportati:

- **XenServer (in precedenza Citrix Hypervisor)**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione XenServer.

- **Microsoft System Center Virtual Machine Manager**

  Include qualsiasi versione di Hyper-V registrabile con le versioni supportate di System Center Virtual Machine Manager.

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager.

- **Nutanix Acropolis**

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione Nutanix.

- **VMware vSphere (vCenter + ESXi)**

  Non viene fornito alcun supporto del funzionamento della modalità collegata vSphere vCenter.

  CTX131239 contiene informazioni sulla versione corrente, oltre a collegamenti a problemi noti.

  Per ulteriori informazioni, vedere Ambienti di virtualizzazione VMware.

Host cloud pubblici supportati:

- **Amazon Web Services (AWS)**

  Per informazioni sull'utilizzo di AWS per il provisioning di macchine virtuali, vedere la sezione Ambienti di virtualizzazione Amazon Web Services.

- **Google Cloud Platform**
  Per ulteriori informazioni, vedere Ambienti di virtualizzazione di Google Cloud Platform e Getting Started with Citrix DaaS on Google Cloud.

- **Microsoft Azure Resource Manager**

  Per informazioni sull'utilizzo di Microsoft Azure Resource Manager per il provisioning di macchine virtuali, vedere Ambienti di virtualizzazione Microsoft Azure Resource Manager.

- **Soluzioni Nutanix Cloud e dei partner**

  Per informazioni sull'utilizzo delle soluzioni Nutanix Cloud e dei partner, vedere Soluzioni Nutanix Cloud e dei partner.

- **Soluzioni cloud VMware e dei partner**

  Per informazioni sull'utilizzo delle soluzioni VMware Cloud e dei partner, vedere Soluzioni VMware Cloud e dei partner.

Quando si aggiungono connessioni a host cloud pubblici alla propria distribuzione, tenere presente quanto segue:

- È necessaria la licenza Hybrid Rights. Per informazioni sulla licenza Hybrid Rights, vedere Transition and Trade-Up (TTU) with Hybrid Rights. Per informazioni sull'aggiunta di una licenza, vedere Creare un sito.
- Le fonti di informazioni indirizzano alla documentazione di Citrix DaaS. Se si ha familiarità con gli host cloud pubblici del prodotto Citrix DaaS, la versione locale presenta diverse differenze.
  - In Citrix DaaS, l'interfaccia di gestione è nota come Full Configuration (configurazione completa). Nella versione locale di Citrix Virtual Apps and Desktops, l'interfaccia di gestione è nota come Web Studio.
  - Gli aggiornamenti vengono implementati in Citrix DaaS circa ogni quattro settimane. Pertanto, è possibile che alcune funzionalità disponibili con Citrix DaaS non siano disponibili con la versione locale.

Livelli funzionali di Active Directory

Sono supportati i seguenti livelli di funzionalità per la foresta e il dominio di Active Directory:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

HDX

Audio

L'audio UDP per Multi-Stream ICA è supportato dall'app Citrix Workspace per Windows e dall'app Citrix Workspace per Linux 13.

L'annullamento dell'eco è supportato nell'app Citrix Workspace per Windows.

Vedere il supporto e i requisiti specifici delle funzionalità HDX. Per ulteriori informazioni sulle funzionalità HDX e sulle app Citrix Workspace, vedere la Matrice delle funzionalità.

Distribuzione HDX Windows Media

I seguenti client sono supportati per il recupero dei contenuti sul lato client Windows Media, il reindirizzamento di Windows Media e la transcodificazione multimediale Windows Media in tempo reale: app Citrix Workspace per Windows, app Citrix Workspace per iOS e app Citrix Workspace per Linux.

Per utilizzare il recupero del contenuto sul lato client di Windows Media sui dispositivi Windows 8, impostare Citrix Multimedia Redirector come programma predefinito: in **Pannello di controllo > Programmi > Programmi predefiniti > Impostare i programmi predefiniti**, selezionare **Citrix Multimedia Redirector** e fare clic su **Imposta questo programma come predefinito** o **Scegli i valori predefiniti per questo programma**. La transcodificazione della GPU richiede una GPU NVIDIA abilitata CUDA con capacità di calcolo 1.1 o superiore; vedere https://developer.nvidia.com/cuda/cuda-gpus.

HDX 3D Pro

Il VDA per sistema operativo Windows a sessione singola rileva la presenza di hardware GPU in fase di esecuzione.

La macchina fisica o virtuale che ospita l'applicazione può utilizzare GPU Passthrough o Virtual GPU (vGPU):

- GPU Passthrough è disponibile con:
  - XenServer
  - Nutanix AHV
  - VMware vSphere e VMware ESX, in cui è denominato vDGA (Virtual Direct Graphics Acceleration)
  - Microsoft Hyper-V in Windows Server 2016 in cui è denominato DDA (Discrete Device Assignment).
- vGPU è disponibile con:

  - XenServer
  - Nutanix AHV
  - VMware vSphere

Vedere https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/2402-ltsr/graphics/hdx-3d-pro.

Citrix consiglia che il computer host abbia almeno 4 GB di RAM e quattro CPU virtuali con una velocità di clock di 2,3 GHz o superiore.

Unità di elaborazione grafica (GPU):

- Per l'accelerazione grafica virtualizzata utilizzando l'API NVIDIA GRID, è possibile utilizzare HDX 3D Pro con tutte le GPU NVIDIA GRID supportate dal software NVIDIA Virtual GPU (vGPU) versione 13 e successive; vedere https://docs.nvidia.com/grid/index.html.
  Per un elenco dettagliato degli Hypervisor supportati e dell'hardware supportato, vedere la documentazione del software NVIDIA vGPU.
- L'accelerazione grafica virtualizzata è supportata sulla famiglia di processori Intel Xeon E3 di piattaforme grafiche per data center e sulla serie Intel Data Center GPU Flex. Per ulteriori informazioni, vedere la serie GPU Flex.
- Le GPU AMD sono supportate dalla virtualizzazione MxGPU di AMD. Per ulteriori informazioni sull'hardware supportato, consulta la documentazione AMD.

Dispositivo utente:

- Citrix supporta fino a 8 monitor da 4 k, a seconda delle risorse hardware. A seconda della GPU utilizzata, possono esserci altre restrizioni hardware su questo valore massimo.
- Per i dispositivi utente, Citrix consiglia almeno 4 GB di RAM e una CPU con una velocità di clock di 1,6 GHz o superiore. Per prestazioni ottimali dei dispositivi utente, consigliamo almeno 8 GB di RAM e una CPU dual-core con una velocità di clock di 3 GHz o superiore.
- Per l'accesso a più monitor, Citrix consiglia dispositivi utente con CPU quad-core.
- L'app Citrix Workspace deve essere installata.

Per ulteriori informazioni, vedere gli articoli su HDX 3D Pro e www.citrix.com/xenapp/3d.

Universal Print Server

Universal Print Server comprende componenti client e server. Il componente UpsClient è incluso nell'installazione VDA. Installare il componente UpsServer su ogni server di stampa in cui risiedono stampanti condivise di cui si desidera eseguire il provisioning con Citrix Universal Print Driver nelle sessioni utente.

Il componente UpsServer è supportato in:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Requisiti:

- Microsoft Visual C++ 2015–2019 Redistributable
- Microsoft .NET Framework 4.8 (minimo)

Per i VDA per sistema operativo multisessione, l'autenticazione utente durante le operazioni di stampa richiede che Universal Print Server venga aggiunto allo stesso dominio del VDA.

I pacchetti di componenti client e server autonomi sono disponibili anche per il download.

Per ulteriori informazioni, vedere Eseguire il provisioning delle stampanti.

Altro

Sono supportati solo Citrix License Server 11.17.2 e versioni successive. Per ulteriori informazioni, vedere Licenze.

Per ulteriori informazioni sulla compatibilità delle versioni, vedere la matrice dei prodotti.

Per le versioni StoreFront supportate, vedere i requisiti di sistema di StoreFront.

La Console Gestione Criteri di gruppo Microsoft (GPMC) è necessaria se si memorizzano le informazioni sui criteri Citrix in Active Directory anziché nel database di configurazione del sito. Se si installa `CitrixGroupPolicyManagement_x64.msi` separatamente (ad esempio, su una macchina in cui non è installato un componente principale di Citrix Virtual Apps and Desktops), tale macchina deve avere installato Visual Studio 2015 runtime. Per ulteriori informazioni, vedere la documentazione Microsoft.

Se si desidera modificare gli oggetti Criteri di gruppo di dominio utilizzando GPMC, attivare la funzionalità Gestione Criteri di gruppo (in Windows Server Manager) in tutti i computer contenenti Delivery Controller.

Sono supportate più NIC.

Per impostazione predefinita, l'app Citrix Workspace per Windows non viene installata quando si installa un VDA corrente. Per ulteriori informazioni, vedere la documentazione dell'app Citrix Workspace per Windows.

Per informazioni sul browser supportato per tale funzionalità, vedere Accesso alle app locali.

Questa versione di Citrix Virtual Apps and Desktops richiede almeno HDX RealTime Connector 2.9 LTSR. Per ulteriori informazioni, vedere la documentazione di HDX RealTime Optimization Pack.

Questo prodotto supporta le versioni di PowerShell dalla 3 alla 5.

Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager

August 22, 2024

Seguire queste indicazioni se si utilizza Hyper-V con Microsoft System Center Virtual Machine Manager (VMM) per fornire macchine virtuali.

Questa versione supporta le versioni di VMM elencate in Requisiti di sistema.

> **Nota:**
>
> I cluster Hyper-V misti (contenenti server che eseguono versioni di Hyper-V diverse) non sono supportati.

È possibile utilizzare Citrix Provisioning (in precedenza Provisioning Services) e Machine Creation Services per eseguire il provisioning di quanto segue:

- Macchine virtuali con sistema operativo desktop o server supportate di generazione 1.
- Macchine virtuali con sistema operativo desktop o server supportate di seconda generazione, incluso il supporto dell'avvio sicuro.

Installare e configurare un hypervisor

> **Importante:**
>
> Tutti i Delivery Controller devono trovarsi nella stessa foresta dei server VMM.

1. Installare il server Microsoft Hyper-V e VMM sui server.
2. Installare la console di System Center Virtual Machine Manager in tutti i controller. La versione della console deve corrispondere alla versione del server di gestione. Sebbene una console precedente possa connettersi al server di gestione, il provisioning dei VDA non riesce se le versioni sono diverse.
3. Verificare le seguenti informazioni sull'account:

   L'account utilizzato per specificare gli host in Studio è un amministratore VMM o un amministratore delegato VMM per i computer Hyper-V pertinenti. Se questo account ha solo il ruolo di amministratore delegato in VMM, i dati di archiviazione non vengono elencati in Studio durante il processo di creazione dell'host.

   L'account utente utilizzato per l'integrazione in Studio deve anche essere membro del gruppo di protezione locale degli amministratori in ogni server Hyper-V. Questa configurazione supporta la gestione del ciclo di vita delle macchine virtuali, ad esempio la creazione, l'aggiornamento e l'eliminazione di macchine virtuali.

L'installazione di un controller in un server che esegue Hyper-V non è supportata.

Nelle implementazioni di grandi dimensioni in cui un singolo SCVMM gestisce più cluster in diversi data center, è possibile limitare l'ambito degli amministratori delegati dei gruppi host.

Per limitare l'ambito dei gruppi di host, utilizzare il ruolo di amministratore delegato nella console di Microsoft System Center Virtual Machine Manager (VMM):

1. In **Create User Roles Wizard** (Creazione guidata di creazione ruoli utente), selezionare Fabric Administrator (Delegated Administrator) come ruolo utente.
2. In **Members**, aggiungere l'account utente in Active Directory che si desidera utilizzare come amministratore delegato.
3. In **Scope**, selezionare i gruppi host a cui si desidera che l'amministratore delegato abbia accesso.
4. Creare un nuovo **account Esegui come** utilizzando le credenziali utente dell'amministratore delegato. Utilizzare queste credenziali per creare una connessione hypervisor in un secondo momento. Non utilizzare gli account con ruolo di amministratore principale.

Effettuare il provisioning di Azure Stack HCI tramite SCVMM

Azure Stack HCI è una soluzione cluster di infrastruttura iperconvergente (HCI) che ospita i carichi di lavoro Windows e Linux virtualizzati e la relativa archiviazione in un ambiente ibrido locale.

I servizi ibridi di Azure migliorano il cluster dotandolo di funzionalità come il monitoraggio basato su cloud, il ripristino del sito e i backup delle macchine virtuali. È anche possibile ottenere una visione centrale di tutte le distribuzioni di Azure Stack HCI nel portale di Azure.

Considerazioni

Considerare quanto segue:

- I carichi di lavoro multisessione di Windows 10 Enterprise e Windows 11 Enterprise multisessione non sono supportati.
- Il supporto per la gestione del cluster Azure Stack HCI 23H2 sarà disponibile nella versione SCVMM 2025.

Integrazione di Azure Stack HCI con SCVMM

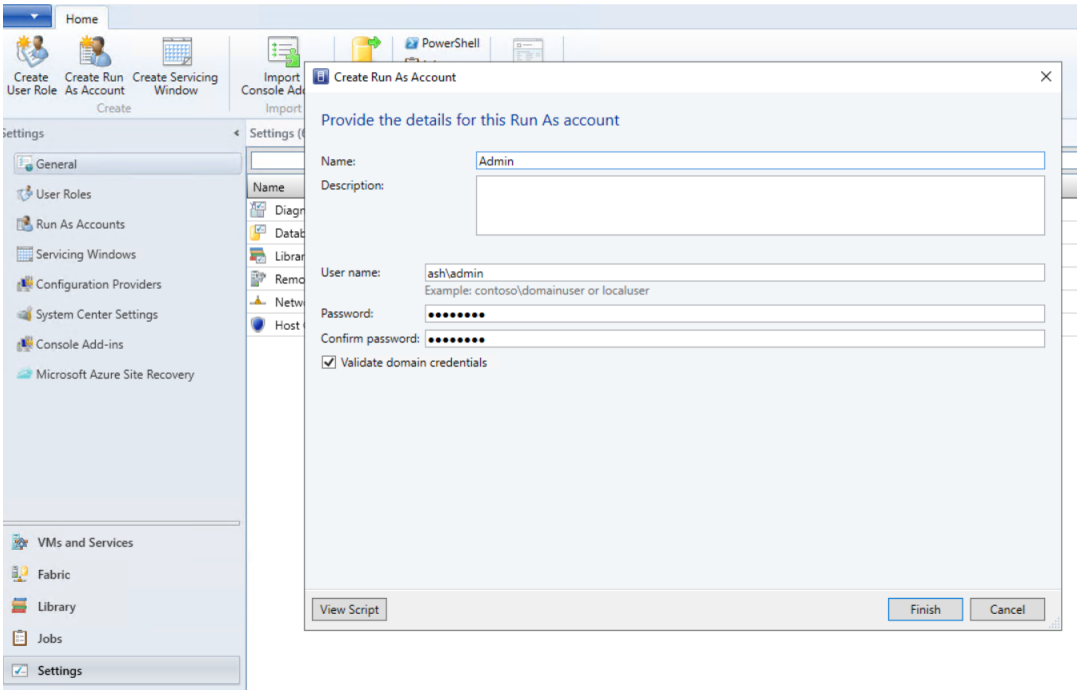
Per integrare Azure Stack HCI con SCVMM, è prima necessario creare un cluster HCI di Azure Stack e quindi integrare quel cluster con SCVMM.

1. Per creare il cluster HCI di Azure Stack, vedere il documento Microsoft Connettersi e gestire la registrazione di Azure Stack HCI.
2. Per integrare il cluster HCI di Azure Stack con SCVMM, effettuare le seguenti operazioni:

   a) Accedere alla macchina preparata per ospitare il server SCVMM e installare SCVMM 2019 UR3 o versione successiva.

   > **Nota:**
   >
   > Installare la Console di amministrazione SCVMM 2019 UR3 o versione successiva su tutti i controller.

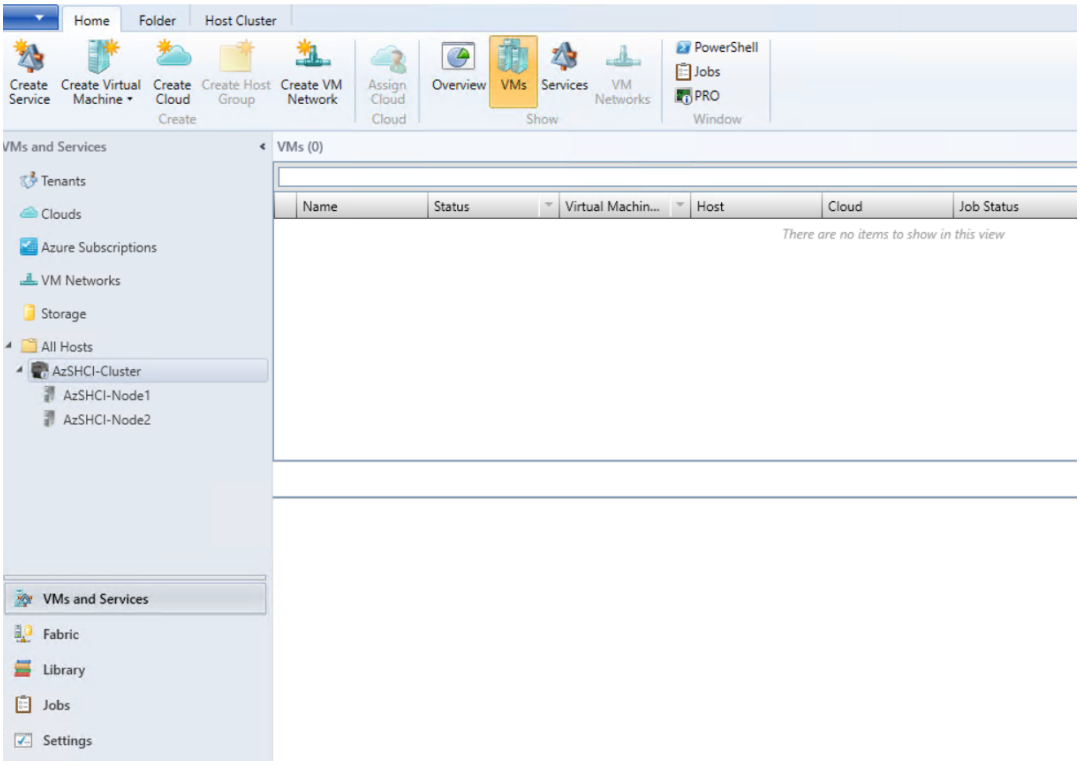
   b) Nella pagina **Settings** (Impostazioni) della console VMM, creare un account Esegui come.



   c) Eseguire i seguenti comandi PowerShell con privilegi amministrativi nel server SCVMM per aggiungere il cluster HCI di Azure Stack come host:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
```

   d) È ora possibile visualizzare il cluster HCI di Azure Stack insieme ai nodi nella console VMM.



e) Creare la connessione di hosting SCVMM in Web Studio, quindi creare un catalogo di macchine MCS.

Passaggi successivi

- Installare i componenti principali
- Installare i VDA
- Creare un sito
- Per informazioni su come creare e gestire una connessione in SCVMM, vedere Connessione a Microsoft System Center Virtual Machine Manager

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Creare cataloghi di macchine

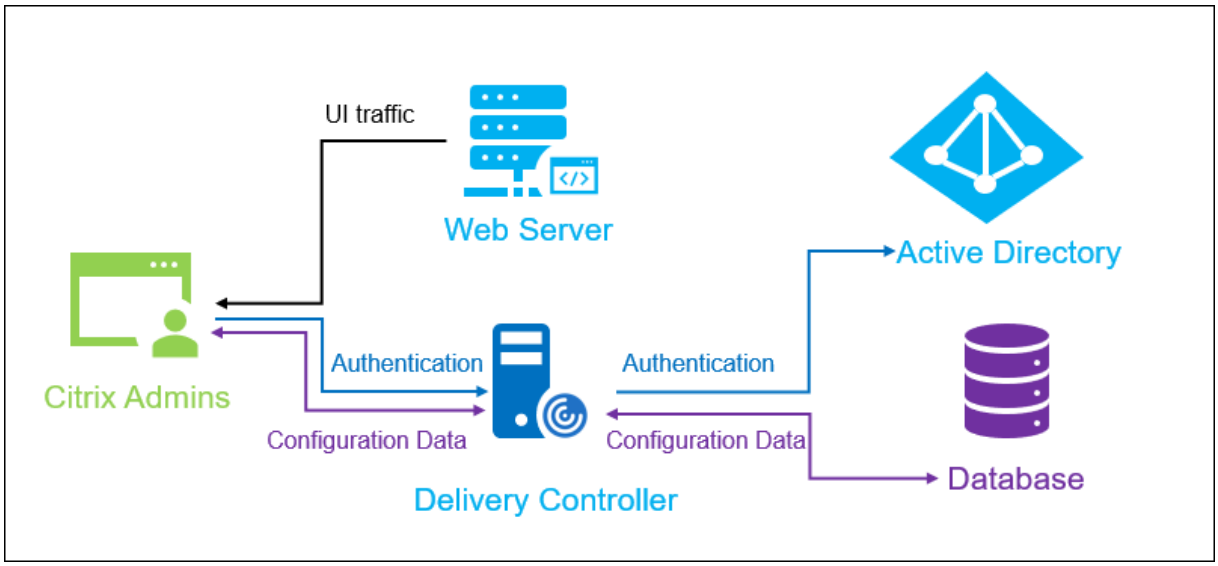
Installare Web Studio

August 23, 2024

Introduzione

Citrix Studio è una console di gestione basata su Windows che consente di configurare e gestire l'implementazione di Citrix Virtual Apps and Desktops. Web Studio è la nuova generazione di Citrix Studio, una console di gestione basata sul Web che offre la parità di funzionalità completa con Citrix Studio. Web Studio ha lo stesso aspetto dell'interfaccia Full Configuration di Citrix DaaS e modernizza l'esperienza di gestione fornendo un'esperienza Web nativa.

È possibile distribuire Web Studio su qualsiasi server Windows con Internet Information Service (IIS) installato. Per una distribuzione rapida, si consiglia di installare Web Studio insieme a un Delivery Controller. In tal caso, Web Studio viene installato come sito Web sul Delivery Controller. Consigliamo di seguire questa configurazione per semplificare l'architettura e ridurre i costi di gestione. Il diagramma seguente illustra l'architettura di Web Studio:



Un flusso di lavoro generale per rendere Web Studio operativo e funzionante è il seguente:

1. Installare Web Studio.
2. Configurare un sito.
3. Aggiungere i Delivery Controller a Web Studio per la gestione.
4. Accedere a Web Studio.

Per configurare una distribuzione di Web Studio con bilanciamento del carico, vedere questo articolo.

Nuove funzionalità disponibili in Web Studio

Vedere l'articolo Novità.

Requisiti di sistema

Sistemi operativi supportati:

- Windows Server 2022
- Windows Server 2019, edizioni Standard e Datacenter e con l'opzione Server Core
- Windows Server 2016, edizioni Standard e Datacenter e con l'opzione Server Core

Browser supportati:

- Microsoft Edge 92
- Firefox ESR (Extended Support Release) 90
- Google Chrome 92
- Safari 14

La risoluzione ottimale dello schermo consigliata per la visualizzazione di Web Studio è 1440 x 1024.

Prerequisiti

Questa versione di Web Studio è compatibile con le distribuzioni di Citrix Virtual Apps and Desktops 2212 e versioni successive.

Per le distribuzioni precedenti alla 2212, eseguire prima l'aggiornamento a 2212 e quindi installare Web Studio.

Limitazioni note

Se si utilizzano Web Studio e Citrix Studio in modo intercambiabile, tenere presente la seguente limitazione: un modello creato in Web Studio non viene visualizzato in Citrix Studio e viceversa. Questo perché Web Studio utilizza un database diverso da Citrix Studio per archiviare i modelli. Come soluzione alternativa, creare un criterio a partire da un modello in Web Studio e quindi creare un nuovo modello a partire da quel criterio in Citrix Studio e viceversa.

- Per garantire una corretta installazione di Web Studio, non modificare il nome del sito predefinito (**Default Web Site**) in Internet Information Services (IIS) Manager. Qualsiasi modifica al nome del sito predefinito comporta errori di installazione.

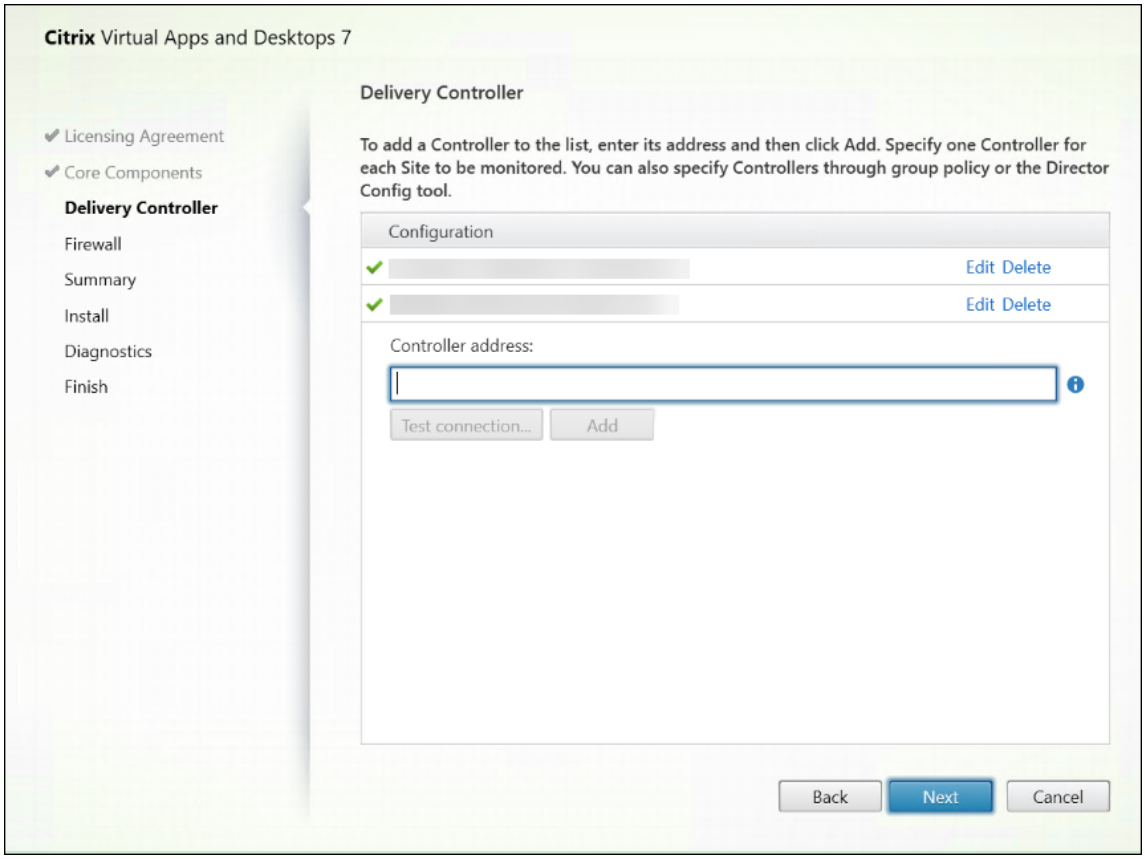
Installare Web Studio

Le seguenti informazioni completano la guida contenuta in Installare i componenti principali. Per installare Web Studio:

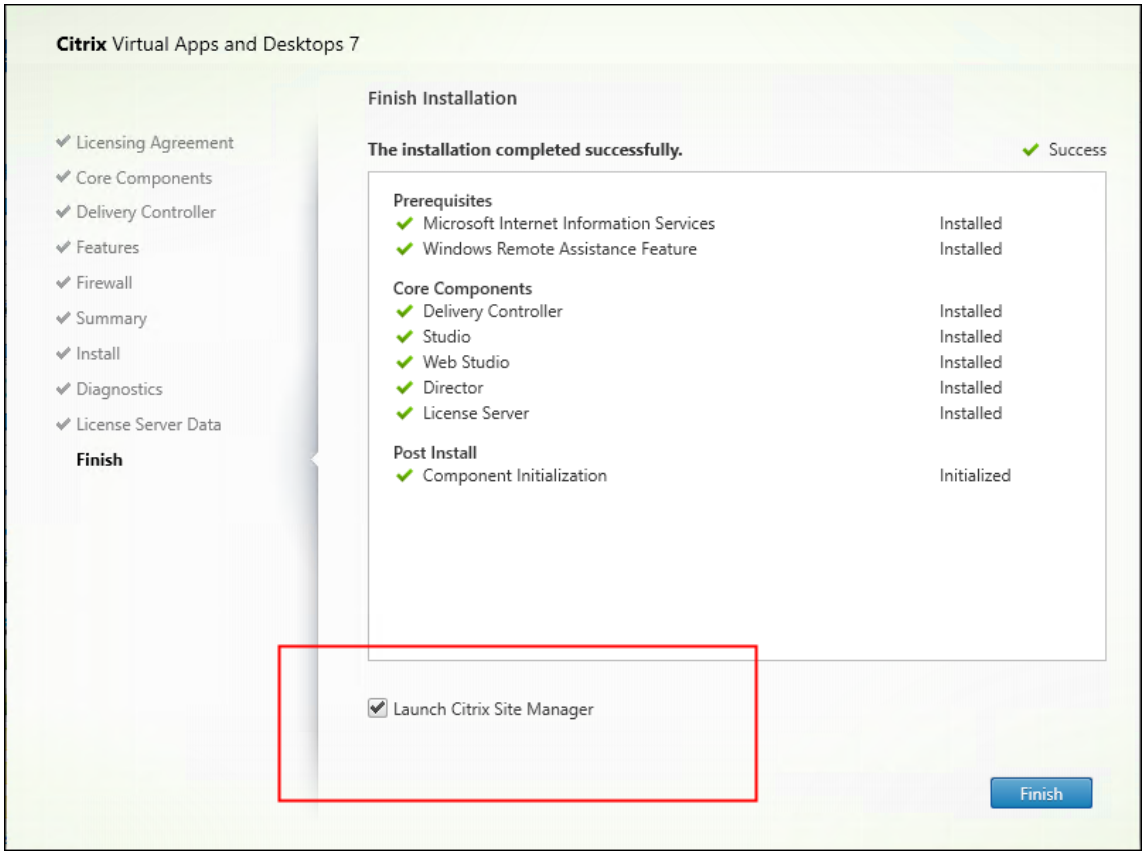
- Installare Web Studio utilizzando il programma di installazione ISO completo del prodotto per Citrix Virtual Apps and Desktops. L'installatore ISO verifica i prerequisiti, installa eventuali componenti mancanti, configura il sito Web di Web Studio (sul Delivery Controller se incluso nell'installazione del Delivery Controller) ed esegue la configurazione di base.
- Se Web Studio non è stato incluso durante l'installazione, utilizzare il programma di installazione per aggiungerlo.
- Quando si installa Web Studio, viene richiesto di digitare l'indirizzo di un Delivery Controller.

  Nota:

  - È possibile aggiungere più di un Delivery Controller. Web Studio tenta di connettersi a essi in ordine casuale. Se il Delivery Controller a cui Web Studio sta tentando di connettersi non è raggiungibile, Web Studio ricorre automaticamente ad altri Delivery Controller.
  - Se Director è stato selezionato in **Core Components** e installato, i Delivery Controller che si aggiungono qui vengono utilizzati sia per Web Studio che per Director.
  - Se non è stato configurato il certificato di attendibilità pubblico esterno e non si desidera richiedere il certificato a una CA aziendale, è sufficiente configurare l'FQDN del proprio Delivery Controller.
  - Se si dispone del certificato di attendibilità pubblico esterno e si è in grado di configurare il DNS pubblico per il proprio Delivery Controller, è possibile digitare il nome DNS come indirizzo del Delivery Controller.
  - Se si è in grado di richiedere il certificato alla propria CA aziendale e di specificare il proprio DNS personale, è possibile aggiungere il proprio DNS personale come indirizzo del Delivery Controller.



- Per proteggere le comunicazioni tra il browser e il server Web e tra il browser e il Delivery Controller, la crittografia TLS deve essere abilitata sul sito Web IIS che ospita Web Studio e sul Delivery Controller. Se non è configurato alcun certificato TLS per il Delivery Controller, il programma di installazione crea un certificato autofirmato, con il nome di dominio completo del Delivery Controller e localhost come certificato del nome DNS. Se è configurato un certificato TLS, il programma di installazione non apporta alcuna modifica. Per ulteriori informazioni sulla crittografia TLS, vedere Proteggere una distribuzione di Web Studio (facoltativo).
- Nella pagina **Finish**, la casella di controllo **Launch Site Manager** è selezionata per impostazione predefinita in modo che Citrix Site Manager si apra automaticamente. Per avviarlo in un secondo momento, aprire il menu Start del desktop e selezionare **Citrix > Citrix Site Manager**. Prima di avviare Web Studio, è necessario utilizzare Citrix Site Manager per creare un sito o unirsi a un sito esistente. Per ulteriori informazioni, vedere Configurare un sito.



> **Nota:**
>
> È inoltre possibile utilizzare la riga di comando per installare Web Studio. Esempio: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.

Configurare un sito

Per configurare la distribuzione di Citrix Virtual Apps and Desktops (noto anche come sito), utilizzare lo strumento Citrix Site Manager. Lo strumento viene installato automaticamente con un Delivery Controller.

Per configurare un sito, effettuare le seguenti operazioni:

1. Su un Delivery Controller, aprire il menu Start del desktop, quindi selezionare **Citrix > Citrix Site Manager**.
2. In Citrix Site Manager, selezionare **Create a site** (Crea un sito). Viene visualizzata la procedura guidata di configurazione del sito.
3. Creare un sito e configurarne le impostazioni come segue:

- Nella pagina **Introduction**, digitare un nome da dare al sito.
- La pagina **Databases** contiene le selezioni per l'impostazione dei database di registrazione del sito, del monitoraggio e della configurazione. Per ulteriori informazioni, vedere il Passaggio 3. Database.
- Nella pagina **Licensing** specificare l'indirizzo del server licenze e quindi indicare la licenza da utilizzare (installare). Per ulteriori informazioni, vedere il Passaggio 4. Licenze.

4. Nella pagina **Summary** (Riepilogo), controllare tutte le impostazioni e fare clic su **Submit** (Invia).

   L'indirizzo IP di questo Controller viene aggiunto automaticamente al sito.

   > **Nota:**
   >
   > L'utente che crea un sito ne diventa amministratore completo. Per ulteriori informazioni, vedere Amministrazione delegata.

Se si installa un nuovo controller dopo aver creato un sito, è necessario aggiungere il controller al sito. I passaggi dettagliati sono i seguenti:

1. Eseguire Citrix Site Manager su questo nuovo controller.
2. Selezionare **Join an existing site** (Unirsi a un sito esistente).
3. Digitare l'indirizzo di un controller già aggiunto al sito.
4. Fare clic su **Submit**.

Aggiungere Delivery Controller a Web Studio per la gestione

Utilizzare lo strumento di configurazione di Studio per aggiungere i Delivery Controller a Web Studio per la gestione. Questo strumento è disponibile nella cartella di installazione di Web Studio.

Per impostazione predefinita, lo strumento è installato nella seguente cartella predefinita.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Si supponga di voler configurare i seguenti due Delivery Controller per il sito che si desidera gestire con Web Studio: `ddc1.studio.local` e `ddc2.studio.local`. Eseguire il seguente comando PowerShell:

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **Nota:**
>
> - Lo strumento richiede le autorizzazioni dell'amministratore del computer.
> - Le modifiche apportate alla configurazione del Delivery Controller potrebbero non avere effetto immediato a causa delle impostazioni della cache sul server IIS. Per un effetto imme-

> diato, accedere al server Web Studio, aprire Gestione Internet Information Services (IIS), passare a Pagina iniziale > Siti > Sito Web predefinito e selezionare **Riavvia** nel riquadro Gestione del sito Web.
> - Per visualizzare tutti i parametri supportati, eseguire `StudioConfig.exe --help`.

Configurare Web Studio come proxy per i Delivery Controller (opzionale)

Per impostazione predefinita, quando si gestisce la distribuzione utilizzando la console Web Studio, ci si connette sia al server Web Studio che ai Delivery Controller tramite il browser Web. Offriamo un'opzione per configurare il server Web Studio come proxy per i Delivery Controller. Di conseguenza, quando si gestisce la distribuzione, ci si connette solo al server Web Studio.

Questa sezione guida l'utente alla configurazione del server Web Studio come proxy per i Delivery Controller. Si presume che Web Studio e Delivery Controller siano installati su server diversi.

Prima di iniziare, verificare di avere tutti i componenti principali necessari installati nella distribuzione. Per ulteriori informazioni, vedere Installare i componenti principali.

Per abilitare la modalità proxy per Web Studio, effettuare le seguenti operazioni:

1. Sul server Web Studio, eseguire Windows PowerShell come amministratore.
2. Eseguire il seguente comando sostituendo `fqdn_of_webstudio_machine` con il nome di dominio completo del proprio server Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"--enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **Nota:**
   >
   > Se si dispone di una distribuzione di Web Studio con bilanciamento del carico, sostituire `fqdn_of_webstudio_machine` con il nome di dominio completo del server di bilanciamento del carico (noto anche come server virtuale). Per ulteriori informazioni, vedere Configurare una distribuzione di Web Studio con bilanciamento del carico.

Per disattivare la modalità proxy per Web Studio, eseguire questo comando PowerShell:

```
`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```

> **Nota:**
>
> La procedura consigliata è proteggere la distribuzione di Web Studio utilizzando un certificato di attendibilità pubblico esterno o un certificato rilasciato da una CA (autorità di certificazione) aziendale. Per ulteriori informazioni, vedere Proteggere una distribuzione di Web Studio.

Accedere a Web Studio

Il sito Web Studio si trova all'indirizzo `https://<address of the server hosting Web Studio>/Citrix/Studio`.

Per accedere a Web Studio, aprire il menu Start del desktop e selezionare **Citrix > Citrix Web Studio**. Gli amministratori con autorizzazioni per Web Studio devono essere utenti del dominio Active Directory. Quando si accede a Web Studio, considerare i seguenti scenari:

- Se non si sono ancora specificati i Delivery Controller per il sito. Viene richiesto di specificare un Delivery Controller in modo da avere accesso temporaneo a Web Studio.
- Se i Delivery Controller specificati non sono attualmente raggiungibili, non è possibile accedere a Web Studio. Verificare le proprie connessioni per assicurarsi che i Delivery Controller siano raggiungibili. Oppure specificare un Delivery Controller alternativo in modo da avere accesso temporaneo a Web Studio.

Passaggi successivi

1. Installare i VDA
2. Utilizzare Web Studio per distribuire app e desktop virtuali ai propri utenti come segue:
   a) Creare un catalogo di macchine
   b) Creare un gruppo di consegna
   c) Creare un gruppo di applicazioni (facoltativo)

Connessione a Microsoft Azure

August 22, 2024

> **Nota:**
>
> Da luglio 2023, Microsoft ha rinominato Azure Active Directory (Azure AD) in Microsoft Entra ID. In questo documento, qualsiasi riferimento ad Azure Active Directory, Azure AD o AAD ora si riferisce a Microsoft Entra ID.

Creare e gestire connessioni e risorse descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Azure Resource Manager.

> **Nota:**
>
> Prima di creare una connessione a Microsoft Azure, è necessario completare la configurazione del proprio account Azure come posizione delle risorse. Vedere Ambienti cloud Microsoft Azure Resource Manager.

Creare entità servizio e connessioni

Prima di creare connessioni, è necessario configurare le entità servizio usate dalle connessioni per accedere alle risorse di Azure. È possibile creare una connessione in due modi:

- Creare un'entità servizio e una connessione allo stesso tempo utilizzando Web Studio
- Creare una connessione utilizzando un'entità servizio creata in precedenza

Questa sezione mostra come completare queste attività:

- Creare un'entità servizio e una connessione utilizzando Web Studio
- Creare un'entità servizio utilizzando PowerShell
- Ottenere il segreto dell'applicazione in Azure
- Creare una connessione utilizzando un'entità servizio esistente

Considerazioni

- Citrix consiglia di utilizzare Service Principal con ruolo di collaboratore. Tuttavia, consulta la sezione Autorizzazioni minime per ottenere l'elenco delle autorizzazioni minime.
- Quando si crea la prima connessione, Azure richiede di concederle le autorizzazioni necessarie. Per le connessioni future è comunque necessario autenticarsi, ma Azure ricorda il consenso precedente e non visualizza più la richiesta.
- Gli account utilizzati per l'autenticazione devono essere co-amministratori della sottoscrizione.
- L'account utilizzato per l'autenticazione deve essere un membro della directory della sottoscrizione. Esistono due tipi di account di cui tenere conto: "lavoro o scuola"e "account Microsoft personale". Vedere CTX219211 per i dettagli.
- Sebbene sia possibile utilizzare un account Microsoft esistente aggiungendolo come membro della directory della sottoscrizione, possono verificarsi complicazioni se all'utente è stato precedentemente concesso l'accesso come ospite a una delle risorse della directory. In questo caso, potrebbe essere presente una voce di segnaposto nella directory che non concede loro le autorizzazioni necessarie e viene restituito un errore.

  Correggere questo problema rimuovendo le risorse dalla directory e aggiungendole di nuovo esplicitamente. Tuttavia, utilizzare questa opzione con attenzione, perché ha effetti indesiderati su altre risorse a cui l'account può accedere.

- Esiste un problema noto per cui alcuni account vengono rilevati come ospiti della directory quando invece sono membri. Configurazioni come questa si verificano in genere con account di directory consolidati precedenti. Soluzione: aggiungere un account alla directory, che assume il valore di appartenenza corretto.
- I gruppi di risorse sono semplicemente contenitori per le risorse e possono contenere risorse provenienti da regioni diverse dalla propria. Ciò può creare potenzialmente confusione se si prevede che le risorse visualizzate nella regione di un gruppo di risorse siano disponibili.
- Assicurarsi che la rete e la subnet siano sufficientemente grandi da ospitare il numero di macchine necessarie. Ciò richiede una certa lungimiranza, ma Microsoft aiuta a specificare i valori corretti, con indicazioni sulla capacità dello spazio degli indirizzi.

Creare un'entità servizio e una connessione utilizzando Web Studio

> **Importante:**
>
> Questa funzionalità non è ancora disponibile per le sottoscrizioni di Azure in Cina.

Con Web Studio è possibile creare sia un'entità servizio che una connessione in un unico flusso di lavoro. Le entità servizio consentono alle connessioni di accedere alle risorse di Azure. Quando si esegue l'autenticazione in Azure per creare un'entità servizio, un'applicazione viene registrata in Azure. Viene creata una chiave segreta (chiamata segreto del client o segreto dell'applicazione) per l'applicazione registrata. L'applicazione registrata (in questo caso una connessione) utilizza il segreto del client per l'autenticazione in Azure AD.

Prima di iniziare, assicurarsi che siano soddisfatti questi prerequisiti:

- Avere un account utente nel tenant Azure Active Directory della propria sottoscrizione.
- L'account utente Azure AD sia anche co-amministratore per la sottoscrizione di Azure che si desidera utilizzare per il provisioning delle risorse.
- Si dispone delle autorizzazioni di amministratore globale, amministratore dell'applicazione o sviluppatore di applicazioni per l'autenticazione. Queste autorizzazioni possono essere revocate dopo aver creato una connessione host. Per ulteriori informazioni sui ruoli, vedere Ruoli predefiniti di Azure AD.

Utilizzare la procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse) per creare insieme un'entità servizio e una connessione allo stesso tempo:

1. Nella pagina **Connection** (Connessione), selezionare **Create a new connetion** (Crea una nuova connessione), il tipo di connessione **Microsoft Azure** e l'ambiente Azure.
2. Selezionare gli strumenti da utilizzare per creare le macchine virtuali, quindi selezionare **Next** (Avanti).

3. Nella pagina **Connection Details** (Dettagli connessione), inserire il proprio ID sottoscrizione di Azure e un nome per la connessione. Dopo aver inserito l'ID sottoscrizione, viene abilitato il pulsante **Create new** (Crea nuova).

   > **Nota:**
   >
   > Il nome della connessione può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.

4. Selezionare **Create new** (Crea nuova), quindi inserire il nome utente e la password dell'account Azure Active Directory.
5. Selezionare **Sign in** (Accedi).
6. Selezionare **Accept** (Accetta) per concedere a Citrix Virtual Apps and Desktops le autorizzazioni elencate. Citrix Virtual Apps and Desktops crea un'entità servizio che consente di gestire le risorse di Azure per conto dell'utente specificato.
7. Dopo aver selezionato **Accept** (Accetta), si torna alla pagina **Connection** (Connessione) della procedura guidata.

   > **Nota:**
   >
   > Dopo aver eseguito l'autenticazione in Azure, i pulsanti **Create new** (Crea nuova) e **Use existing** (Usa esistente) scompaiono. Viene visualizzato il testo **Connection successful** (Connessione riuscita), con un segno di spunta verde che indica la connessione riuscita alla sottoscrizione di Azure.

8. Nella pagina **Connection Details** (Dettagli connessione), selezionare **Next** (Avanti).

   > **Nota:**
   >
   > Non è possibile passare alla pagina successiva finché non ci si autentica correttamente in Azure e non si acconsente a concedere le autorizzazioni richieste.

9. Configurare le risorse per la connessione. Le risorse comprendono la regione e la rete.

   - Nella pagina **Region** (Regione), selezionare una regione.
   - Nella pagina **Network** (Rete), procedere come segue:
     - Digitare un nome da 1 a 64 caratteri per la risorsa, per semplificare l'identificazione della combinazione di regione e rete. Il nome di una risorsa non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.
     - Selezionare una coppia rete virtuale/gruppo di risorse (se si dispone di più di una rete virtuale con lo stesso nome, l'associazione del nome della rete con il gruppo di risorse fornisce combinazioni univoche). Se la regione selezionata nella pagina precedente non dispone di reti virtuali, tornare a quella pagina e selezionare una regione con reti virtuali.

10. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per completare la configurazione.

Visualizzare l'ID dell'applicazione Dopo aver creato una connessione, è possibile visualizzare l'ID dell'applicazione utilizzata dalla connessione per accedere alle risorse di Azure.

Nell'elenco **Add Connection and Resources** (Aggiungi connessione e risorse), selezionare la connessione per visualizzare i dettagli. La scheda **Details** (Dettagli) mostra l'ID dell'applicazione.

Creare un'entità servizio utilizzando PowerShell

Per creare un'entità servizio utilizzando PowerShell, connettersi alla sottoscrizione di Azure Resource Manager e utilizzare i cmdlet PowerShell forniti nelle sezioni seguenti.

Assicurarsi di avere a portata di mano quanto segue:

- **SubscriptionId:** `SubscriptionID` di Azure Resource Manager per la sottoscrizione in cui si desidera eseguire il provisioning di VDA.
- **ActiveDirectoryID**: ID tenant dell'applicazione registrata con Azure AD.
- **ApplicationName:** nome dell'applicazione da creare in Azure AD.

I passaggi dettagliati sono i seguenti:

Connettersi alla sottoscrizione Azure Resource Manager.

```
`Connect-AzAccount`
```

1. Selezionare la sottoscrizione Azure Resource Manager in cui si desidera creare l'entità servizio.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

2. Creare l'applicazione nel proprio tenant AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. Creare un'entità servizio.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. Assegnare un ruolo all'entità servizio.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. Dalla finestra di output della console PowerShell, prendere nota dell'ApplicationId. Fornire questo ID quando si crea la connessione host.

Ottenere il segreto dell'applicazione in Azure

Per creare una connessione utilizzando un'entità servizio esistente, è prima necessario ottenere l'ID e il segreto dell'applicazione dell'entità servizio nel portale di Azure.

I passaggi dettagliati sono i seguenti:

1. Ottenere l'**ID dell'applicazione** da Web Studio o utilizzando PowerShell.
2. Accedere al portale di Azure.
3. In Azure, selezionare **Azure Active Directory**.
4. Da **Registrazioni app** in Azure AD, selezionare la propria applicazione.
5. Andare a **Certificati e segreti**.
6. Fare clic su **Client secrets** (Segreti client).

Creare una connessione utilizzando un'entità servizio esistente

Se si dispone già di un'entità servizio, è possibile utilizzarla per creare una connessione utilizzando Web Studio.

Assicurarsi di avere a portata di mano quanto segue:

- SubscriptionId
- ActiveDirectoryID (tenant ID)
- ID applicazione
- Segreto dell'applicazione

  Per ulteriori informazioni, vedere Ottenere il segreto dell'applicazione.
- Data di scadenza del segreto

I passaggi dettagliati sono i seguenti:

Nella procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse):

1. Nella pagina **Connection** (Connessione), selezionare **Create a new connetion** (Crea una nuova connessione), il tipo di connessione **Microsoft Azure** e l'ambiente Azure.
2. Selezionare gli strumenti da utilizzare per creare le macchine virtuali, quindi selezionare **Next** (Avanti).
3. Nella pagina **Connection Details** (Dettagli connessione), inserire il proprio ID sottoscrizione di Azure e un nome per la connessione.

> **Nota:**
>
> Il nome della connessione può contenere da 1 a 64 caratteri e non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.

4. Selezionare **Use existing** (Usa esistente). Nella finestra **Existing Service Principal Details** (Dettagli entità servizio esistente), immettere le seguenti impostazioni per l'entità servizio esistente. Dopo aver inserito i dettagli, il pulsante **Save** (Salva) è abilitato. Selezionare **Save** (Salva). Non è possibile andare oltre questa pagina finché non si forniscono dettagli validi.

   - **Subscription ID** (ID sottoscrizione). Inserire il proprio ID sottoscrizione di Azure. Per ottenere l'ID sottoscrizione, accedere al portale di Azure e andare a **Sottoscrizioni > Panoramica**.
   - **Active Directory ID** (ID Active Directory) (ID tenant). Inserire l'ID Directory (tenant) dell'applicazione che si è registrata con Azure AD.
   - **Application ID** (ID applicazione). Inserire l'ID applicazione (client) dell'applicazione registrata con Azure AD.
   - **Application secret** (Segreto dell'applicazione). Creare una chiave segreta (segreto client). L'applicazione registrata utilizza la chiave per l'autenticazione in Azure AD. Si consiglia di cambiare le chiavi regolarmente per motivi di sicurezza. Assicurarsi di salvare la chiave, perché non è possibile recuperarla in un secondo momento.
   - **Secret expiration date** (Data di scadenza del segreto). Immettere la data dopo la quale il segreto dell'applicazione scade. Si riceverà un avviso sulla console prima della scadenza della chiave segreta. Tuttavia, se la chiave segreta scade, si ricevono errori.

     > **Nota:**
     >
     > Per motivi di sicurezza, il periodo di scadenza non può essere superiore a due anni da oggi.

   - **Authentication URL** (URL di autenticazione). Questo campo viene compilato automaticamente e non è modificabile.
   - **Management URL** (URL di gestione). Questo campo viene compilato automaticamente e non è modificabile.
   - **Storage suffix** (Suffisso di archiviazione). Questo campo viene compilato automaticamente e non è modificabile.

     L'accesso ai seguenti endpoint è necessario per creare un catalogo MCS in Azure. L'accesso a questi endpoint ottimizza la connettività tra la rete e il portale di Azure e i relativi servizi.

  - Authentication URL: https://login.microsoftonline.com/
  - Management URL: https://management.azure.com/. Questo è un URL di richiesta per le API del provider di Azure Resource Manager. L'endpoint per la gestione dipende dall'ambiente. Ad esempio, per Azure Global è https://management.azure.com/ e per Azure US Government è https://management.usgovcloudapi.net/.
  - Storage suffix: https://*.core.windows.net./. Questo (*) è un carattere jolly per il suffisso di archiviazione. Ad esempio, `https://demo.table.core.windows.net/`.

5. Dopo aver selezionato **Save** (Salva), si torna alla pagina **Connection Details** (Dettagli connessione). Selezionare **Next** (Avanti) per passare alla pagina successiva.
6. Configurare le risorse per la connessione. Le risorse comprendono la regione e la rete.
   - Nella pagina **Region** (Regione), selezionare una regione.
   - Nella pagina **Network** (Rete), procedere come segue:
     - Digitare un nome da 1 a 64 caratteri per la risorsa, per semplificare l'identificazione della combinazione di regione e rete. Il nome di una risorsa non può contenere solo spazi vuoti né i caratteri `\/;:#.*?=<>|[]{ } "'()'`.
     - Selezionare una coppia rete virtuale/gruppo di risorse (se si dispone di più di una rete virtuale con lo stesso nome, l'associazione del nome della rete con il gruppo di risorse fornisce combinazioni univoche). Se la regione selezionata nella pagina precedente non dispone di reti virtuali, tornare a quella pagina e selezionare una regione con reti virtuali.
7. Nella pagina **Summary** (Riepilogo), visualizzare un riepilogo delle impostazioni e selezionare **Finish** (Fine) per completare la configurazione.

Gestire le entità servizio e le connessioni

Questa sezione descrive in dettaglio come gestire le entità servizio e le connessioni:

- Configurare le impostazioni di limitazione delle richieste di Azure
- Abilitare la condivisione di immagini in Azure
- Aggiungere tenant condivisi a una connessione utilizzando Full Configuration
- Implementare la condivisione di immagini tramite PowerShell
- Gestire il segreto dell'applicazione e la data di scadenza del segreto

Configurare le impostazioni di limitazione delle richieste di Azure

Azure Resource Manager limita le richieste di sottoscrizione e tenant, instradando il traffico in base a limiti definiti, a seconda delle esigenze specifiche del provider. Per ulteriori informazioni, vedere Limi-

tazione delle richieste di Resource Manager sul sito Microsoft. Sono previsti dei limiti per sottoscrizioni e tenant, a causa dei quali la gestione di molte macchine può diventare problematica. Ad esempio, in una sottoscrizione contenente molte macchine potrebbero verificarsi dei problemi di prestazioni relativi alle operazioni di alimentazione.

> **Suggerimento:**
>
> Per ulteriori informazioni, vedere Miglioramento delle prestazioni di Azure con Machine Creation Services.

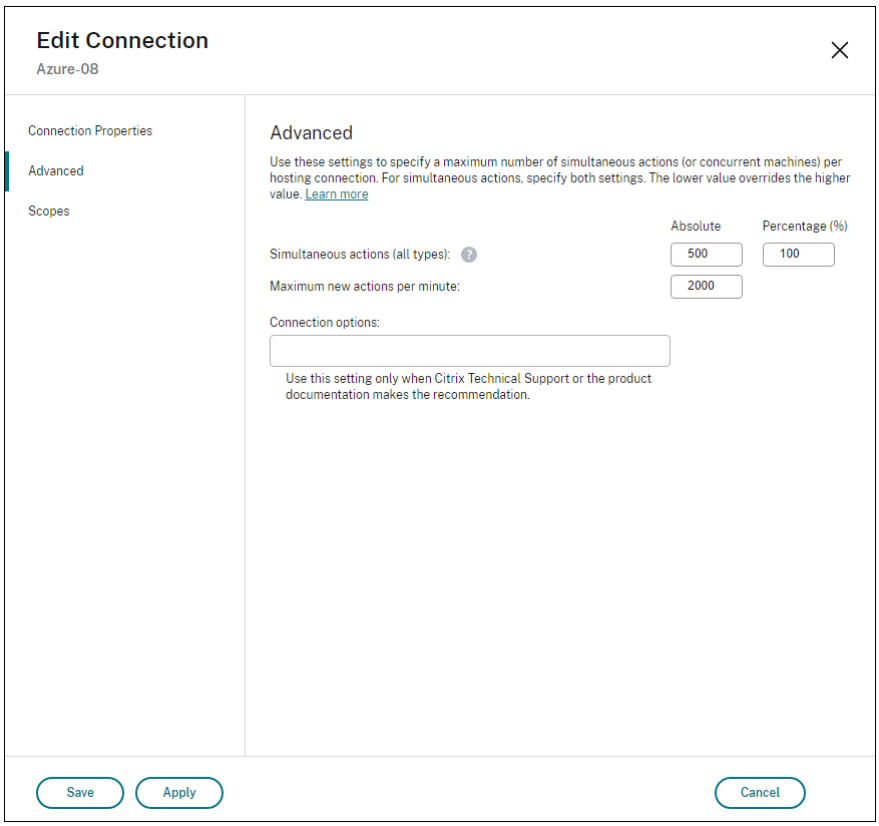
Per contribuire a mitigare questi problemi, è possibile rimuovere la limitazione delle richieste interna di MCS per utilizzare maggiormente la quota di richieste disponibile da Azure.

Si consigliano le seguenti impostazioni ottimali quando si accendono o si spengono le macchine virtuali in sottoscrizioni di grandi dimensioni, ad esempio quelle contenenti 1.000 macchine virtuali:

- Operazioni simultanee assolute: 500
- Numero massimo di nuove operazioni al minuto: 2.000
- Numero massimo di operazioni simultanee: 500

Utilizzare Web Studio per configurare le operazioni di Azure per una determinata connessione Azure:

1. In Web Studio, selezionare **Hosting** nel riquadro a sinistra.
2. Selezionare la connessione.
3. Nella procedura guidata **Edit Connection** (Modifica connessione), selezionare **Advanced** (Avanzate).
4. Nella pagina **Advanced** (Avanzate), utilizzare le opzioni di configurazione per specificare il numero di azioni simultanee e il numero massimo di nuove azioni al minuto, nonché eventuali opzioni di connessione aggiuntive.



MCS supporta massimo 500 operazioni simultanee per impostazione predefinita. In alternativa, è possibile utilizzare l'SDK Remote PowerShell per impostare il numero massimo di operazioni simultanee.

Utilizzare la proprietà **PowerShell** `MaximumConcurrentProvisioningOperations` per specificare il numero massimo di operazioni di provisioning simultanee di Azure. Quando si utilizza questa proprietà, considerare:

- Il valore predefinito di `MaximumConcurrentProvisioningOperations` è 500.
- Configurare il parametro `MaximumConcurrentProvisioningOperations` utilizzando il comando PowerShell `Set-item`.

Abilitare la condivisione di immagini in Azure

Quando si creano o si aggiornano cataloghi delle macchine, è possibile selezionare immagini condivise provenienti da diverse sottoscrizioni e tenant di Azure (condivise tramite la Raccolta di calcolo di Azure). Per abilitare la condivisione di immagini all'interno di tenant o fra uno e l'altro, è necessario configurare le impostazioni necessarie in Azure:

- Condividere immagini all'interno di un tenant (tra abbonamenti)
- Condividere immagini tra tenant

Condividere immagini all'interno di un tenant (tra abbonamenti) Perché sia possibile selezionare in Raccolta di calcolo di Azure un'immagine che appartiene a una sottoscrizione diversa, l'immagine deve essere condivisa con l'entità servizio (SPN) di quella sottoscrizione.

Ad esempio, se esiste un'entità servizio (SPN 1) configurata in Studio come:

Entità servizio: SPN 1

Subscription: subscription 1

Tenant: tenant 1

L'immagine è in una sottoscrizione diversa, che è configurata in Studio come:

Subscription: subscription 2

Tenant: tenant 1

Se si intende condividere l'immagine della sottoscrizione 2 con la sottoscrizione 1 (SPN 1), passare alla sottoscrizione2 e condividere il gruppo di risorse con SPN1.

L'immagine deve essere condivisa con un altro SPN utilizzando il controllo degli accessi in base al ruolo di Azure (RBAC). Azure RBAC è il sistema di autorizzazione usato per gestire l'accesso alle risorse di Azure. Per ulteriori informazioni su Azure RBAC, vedere il documento Microsoft Che cos'è il controllo degli accessi in base al ruolo di Azure. Per concedere l'accesso, si assegnano ruoli alle entità servizio nell'ambito del gruppo di risorse con il ruolo di collaboratore. Per assegnare i ruoli di Azure, è necessario disporre di un'autorizzazione `Microsoft.Authorization/roleAssignments/write`, come nel caso di un Amministratore Accesso utenti o un Proprietario. Per ulteriori informazioni sulla condivisione di immagini con un altro SPN, vedere il documento Microsoft Assegnare ruoli di Azure usando il portale di Azure.

Per informazioni sulla selezione di un'immagine da una sottoscrizione diversa mediante i comandi PowerShell, vedere Selezionare un'immagine da un'altra sottoscrizione.

Condividere immagini tra tenant Per condividere immagini tra tenant con la Raccolta di calcolo di Azure, creare una registrazione dell'applicazione.

Ad esempio, se ci sono due tenant (Tenant 1 e Tenant 2) e si desidera condividere la propria galleria di immagini con Tenant 1, allora:

1. Creare una domanda di registrazione per Tenant 1. Per ulteriori informazioni, vedere Creare la registrazione dell'app.
2. Consentire a Tenant 2 di accedere all'applicazione richiedendo l'accesso tramite un browser. Sostituire `Tenant2 ID` con l'ID tenant del Tenant 1. Sostituire `Application (client) ID` con l'ID dell'applicazione della registrazione dell'applicazione creata. Quando si sono completate le sostituzioni, incollare l'URL in un browser e seguire le istruzioni di accesso per accedere al Tenant 2. Ad esempio:


```
https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
    client_id=<Application (client) ID>&response_type=code&
    redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```

Per ulteriori informazioni, vedere Concedere l'accesso al tenant 2.

3. Concedere all'applicazione l'accesso al gruppo di risorse Tenant 2. Accedere come Tenant 2 e concedere alla registrazione dell'app l'accesso al gruppo di risorse che contiene l'immagine della raccolta. Per ulteriori informazioni, vedere Eseguire l'autenticazione delle richieste su più tenant.

Per creare un catalogo utilizzando un'immagine di un tenant diverso utilizzando i comandi PowerShell:

1. Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi.
2. Selezionare un'immagine da un altro tenant.

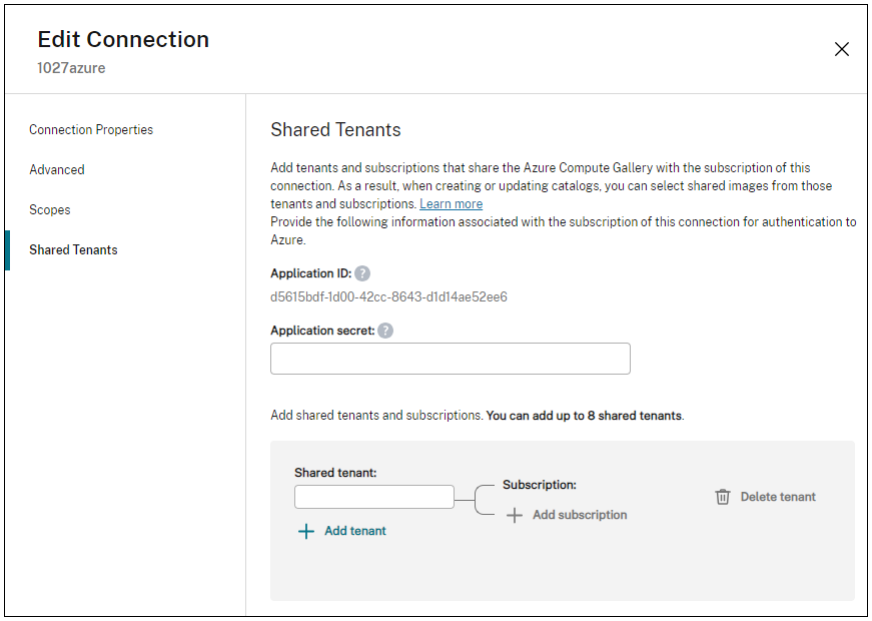
Aggiungere tenant condivisi a una connessione utilizzando Full Configuration

Quando si creano o si aggiornano cataloghi delle macchine in Web Studio, è possibile selezionare immagini condivise provenienti da diverse sottoscrizioni e tenant di Azure (condivise tramite la Raccolta di calcolo di Azure). La funzionalità richiede che vengano fornite informazioni condivise sul tenant e sulla sottoscrizione per le connessioni host associate.

> **Nota:**
>
> Assicurarsi di aver configurato le impostazioni necessarie in Azure per abilitare la condivisione di immagini tra tenant. Per ulteriori informazioni, vedere Condividere immagini tra tenant.

Completare i seguenti passaggi per una connessione:

1. In Web Studio, selezionare **Hosting** nel riquadro a sinistra.
2. Selezionare la connessione e quindi selezionare **Edit Connection** (Modifica connessione) nella barra delle azioni.



3. In **Shared Tenants** (Tenant condivisi), procedere come segue:

   - Fornire l'ID dell'applicazione e il segreto dell'applicazione associati alla sottoscrizione della connessione. Citrix Virtual Apps and Desktops utilizza queste informazioni per l'autenticazione in Azure AD.
   - Aggiungere tenant e sottoscrizioni che condividono la Raccolta di calcolo di Azure con la sottoscrizione della connessione. È possibile aggiungere fino a 8 tenant condivisi e 8 sottoscrizioni per ogni tenant.

4. Al termine, selezionare **Apply** (Applica) per applicare le modifiche apportate e mantenere aperta la finestra oppure selezionare **OK** per applicare le modifiche e chiudere la finestra.

Implementare la condivisione di immagini tramite PowerShell

Questa sezione illustra i processi di condivisione delle immagini tramite PowerShell:

- Selezionare un'immagine da un'altra sottoscrizione
- Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi
- Selezionare un'immagine da un altro tenant

Selezionare un'immagine da un'altra sottoscrizione È possibile selezionare un'immagine in Raccolta di calcolo di Azure che appartiene a una sottoscrizione condivisa diversa all'interno dello stesso tenant di Azure per creare e aggiornare i cataloghi MCS usando i comandi di PowerShell.

1. Nella cartella principale dell'unità di hosting, Citrix crea una nuova cartella di sottoscrizione condivisa chiamata `sharedsubscription`.

2. Elencare tutte le sottoscrizioni condivise di un tenant.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
```

3. Selezionare un abbonamento condiviso, quindi elencare tutti i gruppi di risorse condivise di quella sottoscrizione condivisa.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
```

4. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
```

5. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
```

6. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
```

7. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

   Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Aggiornare le proprietà personalizzate della connessione di hosting con ID tenant condivisi
Utilizzare `Set-Item` per aggiornare le proprietà personalizzate della connessione di hosting con ID tenant e ID di abbonamento condivisi. Aggiungere una proprietà `SharedTenants` in `CustomProperties`. Il formato di `Shared Tenants` è:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
```



```
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
]
```

Ad esempio:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
    123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
    =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
    Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
    core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
    " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
     {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
    advc345" -SecurePassword
$psd
```

> **Nota:**
>
> È possibile aggiungere più di un tenant. Ogni inquilino può avere più di una sottoscrizione.

Selezionare un'immagine da un altro tenant È possibile selezionare nella Raccolta di calcolo di Azure un'immagine che appartiene a un diverso tenant di Azure per creare e aggiornare i cataloghi MCS usando i comandi di PowerShell.

1. Nella cartella principale dell'unità di hosting, Citrix crea una nuova cartella di sottoscrizione condivisa chiamata `sharedsubscription`.
2. Elencare tutte le sottoscrizioni condivise.

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. Selezionare un abbonamento condiviso, quindi elencare tutti i gruppi di risorse condivise di quella sottoscrizione condivisa.

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
       sharedsubscription
   ```

4. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.


```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
```

5. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
```

6. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
```

7. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

   Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Gestire il segreto dell'applicazione e la data di scadenza del segreto

Accertarsi di aver modificato il segreto dell'applicazione per una connessione prima della scadenza del segreto. Si riceverà un avviso su Web Studio prima della scadenza della chiave segreta.

Creare un segreto dell'applicazione in Azure È possibile creare un segreto dell'applicazione per una connessione tramite il portale di Azure.

1. Selezionare **Azure Active Directory**.
2. Da **Registrazioni app** in Azure AD, selezionare la propria applicazione.
3. Andare a **Certificati e segreti**.
4. Fare clic su **Segreti client > Nuovo segreto client**.
5. Fornire una descrizione del segreto e specificare una durata. Al termine, selezionare **Add** (Aggiungi).

> **Nota:**
>
> Assicurarsi di salvare il segreto del client, perché non è possibile recuperarlo in un secondo momento.

6. Copiare il valore del segreto del client e la data di scadenza.
7. In Web Studio modificare la connessione corrispondente e sostituire il contenuto nei campi **Application secret** (Segreto applicazione) e **Secret expiration date** (Data di scadenza del segreto) con i valori copiati.

Modificare la data di scadenza del segreto È possibile utilizzare Web Studio per aggiungere o modificare la data di scadenza del segreto dell'applicazione in uso.

1. Nella procedura guidata **Add Connection and Resources** (Aggiungi connessione e risorse), fare clic con il pulsante destro del mouse su una connessione e fare clic su **Edit Connection** (Modifica connessione).
2. Nella pagina **Connection Properties** (Proprietà connessione), fare clic su **Secret expiration date** (Data di scadenza del segreto) per aggiungere o modificare la data di scadenza del segreto dell'applicazione in uso.

Autorizzazioni Azure richieste

Questa sezione contiene le autorizzazioni minime e generali richieste per Azure.

Autorizzazioni minime

Le autorizzazioni minime offrono un migliore controllo della sicurezza. Tuttavia, le nuove funzionalità che richiedono autorizzazioni aggiuntive non funzionano se si utilizzano solo le autorizzazioni minime.

Creazione di una connessione host Aggiungere una nuova connessione host utilizzando le informazioni ottenute da Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
```

Gestione dell'alimentazione delle macchine virtuali Accendere o spegnere le istanze della macchina.


```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
```

Creazione, aggiornamento o eliminazione di macchine virtuali Creare un catalogo delle macchine, quindi aggiungere, eliminare, aggiornare le macchine ed eliminare il catalogo delle macchine.

Di seguito è riportato l'elenco delle autorizzazioni minime richieste quando l'immagine master è un disco gestito o le snapshot si trovano nella stessa area geografica della connessione di hosting.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
```

Sono necessarie le seguenti autorizzazioni aggiuntive basate su autorizzazioni minime per le seguenti funzionalità:

- Se l'immagine master è un disco rigido virtuale (VHD) in un account di archiviazione situato nella stessa area geografica della connessione host:

  ```
  "Microsoft.Storage/storageAccounts/read",
  "Microsoft.Storage/storageAccounts/listKeys/action",
  ```


- Se l'immagine master è una ImageVersion della Raccolta immagini condivise:

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
```

- Se l'immagine master è un disco gestito, le snapshot o il VHD si trovano in una regione diversa dalla regione della connessione di hosting:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
```

- Se si utilizza un gruppo di risorse gestito da Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- Se si colloca l'immagine master nella Raccolta immagini condivise:

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
```

- Se si utilizza il supporto degli host dedicati di Azure:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
```

- Se si utilizza la crittografia lato server (SSE) con le chiavi gestite dal cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- Se si distribuiscono macchine virtuali utilizzando modelli ARM (profilo macchina):

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
```

- Se si utilizza la specifica del modello di Azure come profilo macchina:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
```


Creazione, aggiornamento ed eliminazione di macchine con disco non gestito Di seguito è riportato l'elenco delle autorizzazioni minime richieste quando l'immagine master è un VHD e utilizza il gruppo di risorse come fornito dall'amministratore:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action"
```

Autorizzazione generale

Il ruolo di collaboratore ha accesso completo per gestire tutte le risorse. Questo set di autorizzazioni non impedisce di ottenere nuove funzionalità.

Il seguente set di autorizzazioni fornisce la migliore compatibilità in futuro, sebbene includa più autorizzazioni del necessario con il set di funzionalità corrente:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
```



```
17  "Microsoft.Compute/hostGroups/read",
18  "Microsoft.Compute/hostGroups/write",
19  "Microsoft.Compute/snapshots/beginGetAccess/action",
20  "Microsoft.Compute/snapshots/delete",
21  "Microsoft.Compute/snapshots/endGetAccess/action",
22  "Microsoft.Compute/snapshots/read",
23  "Microsoft.Compute/snapshots/write",
24  "Microsoft.Compute/virtualMachines/deallocate/action",
25  "Microsoft.Compute/virtualMachines/delete",
26  "Microsoft.Compute/virtualMachines/read",
27  "Microsoft.Compute/virtualMachines/restart/action",
28  "Microsoft.Compute/virtualMachines/start/action",
29  "Microsoft.Compute/virtualMachines/write",
30  "Microsoft.Network/networkInterfaces/delete",
31  "Microsoft.Network/networkInterfaces/join/action",
32  "Microsoft.Network/networkInterfaces/read",
33  "Microsoft.Network/networkInterfaces/write",
34  "Microsoft.Network/networkSecurityGroups/delete",
35  "Microsoft.Network/networkSecurityGroups/join/action",
36  "Microsoft.Network/networkSecurityGroups/read",
37  "Microsoft.Network/networkSecurityGroups/write",
38  "Microsoft.Network/virtualNetworks/subnets/read",
39  "Microsoft.Network/virtualNetworks/read",
40  "Microsoft.Network/virtualNetworks/subnets/join/action",
41  "Microsoft.Resources/deployments/operationstatuses/read",
42  "Microsoft.Resources/deployments/read",
43  "Microsoft.Resources/deployments/validate/action",
44  "Microsoft.Resources/deployments/write",
45  "Microsoft.Resources/deployments/delete",
46  "Microsoft.Resources/subscriptions/resourceGroups/read",
47  "Microsoft.Resources/subscriptions/resourceGroups/write",
48  "Microsoft.Resources/subscriptions/resourceGroups/delete",
49  "Microsoft.Storage/storageAccounts/delete",
50  "Microsoft.Storage/storageAccounts/listKeys/action",
51  "Microsoft.Storage/storageAccounts/read",
52  "Microsoft.Storage/storageAccounts/write",
53  "Microsoft.Resources/templateSpecs/read",
54  "Microsoft.Resources/templateSpecs/versions/read",
```

Configurare le autorizzazioni di connessione host di Azure richieste

Si possono configurare facilmente tutte le autorizzazioni minime richieste per un'entità di servizio o un account utente in Azure collegato a una connessione host per eseguire tutte le operazioni MCS utilizzando un modello ARM. Questo modello ARM automatizza quanto segue:

- Creazione di un ruolo di Azure con le autorizzazioni minime necessarie per le operazioni.
- Assegnazione di questo ruolo a un'entità di servizio di Azure esistente a livello di sottoscrizione.

È possibile distribuire questo modello ARM utilizzando il portale di Azure o i comandi PowerShell. Per ulteriori informazioni, vedere Modello ARM per le operazioni CVAD.

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere Creare cataloghi delle macchine
- Per informazioni specifiche su Azure, vedere Creare un catalogo di Microsoft Azure

Ulteriori informazioni

- Connessioni e risorse
- Creare cataloghi di macchine

Gestione delle immagini (anteprima)

August 22, 2024

Introduzione

Il processo di creazione o aggiornamento del catalogo MCS prevede due fasi:

- Masterizzazione: un'immagine di origine viene convertita in immagine pubblicata
- Clonazione: vengono create nuove VM dall'immagine pubblicata

Con la funzionalità di gestione delle immagini, MCS separa la fase di masterizzazione dal generale flusso di lavoro di provisioning.

È possibile preparare varie versioni di immagini MCS (Immagine preparata) da un'unica immagine di origine e utilizzarla su più cataloghi di macchine MCS diversi. Questa implementazione riduce significativamente i costi di archiviazione e legati ai tempi; inoltre semplifica il processo di distribuzione delle VM e di aggiornamento delle immagini.

I vantaggi dell'utilizzo di questa funzionalità di gestione delle immagini sono:

- Generazione di immagini preparate in anticipo senza creare un catalogo.
- Riutilizzo delle immagini preparate in più scenari, come la creazione e l'aggiornamento di un catalogo.
- Significativa riduzione dei tempi di creazione o aggiornamento del catalogo.

> **Nota:**
>
> - Questa funzionalità è attualmente applicabile agli ambienti di virtualizzazione Azure e VMware.
> - È possibile creare un catalogo di macchine MCS senza utilizzare immagini preparate. In tal

> caso, non si ottengono i vantaggi della funzionalità.

Casi d'uso

Alcuni dei casi d'uso della funzionalità di gestione delle immagini sono:

- *Gestione delle versioni*: le versioni delle immagini consentono di:
  - gestire diverse iterazioni o aggiornamenti di una particolare immagine;
  - gestire più versioni di un'immagine per scopi diversi.
- *Raggruppamento logico*: è possibile creare più definizioni di immagini per:
  - raggruppare logicamente le versioni delle immagini in base a vari criteri come progetto, reparto o applicazione e tipo di desktop;
  - gestire le immagini in modo più efficiente all'interno di un'organizzazione.

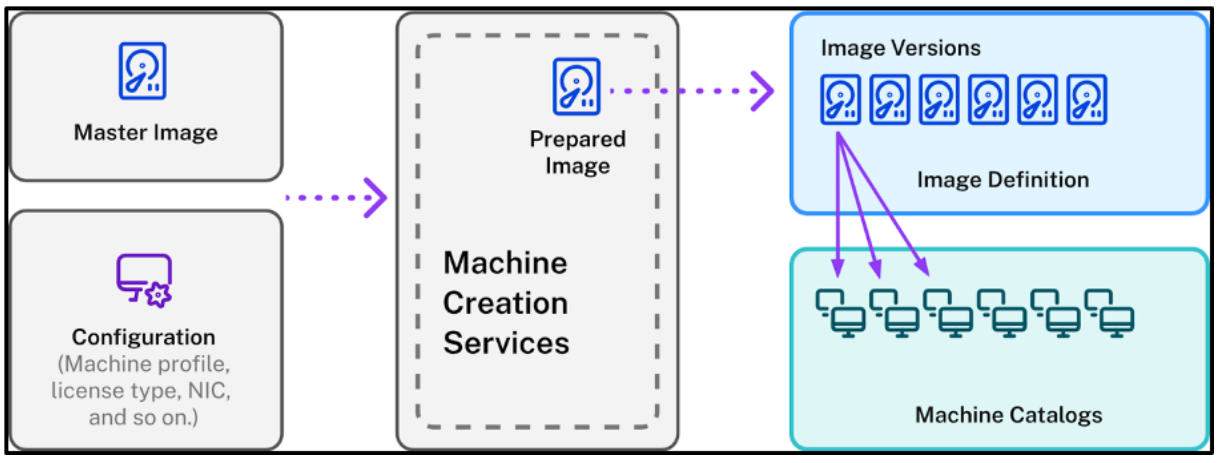
Cos'è un'immagine preparata?

Grazie alla funzionalità di gestione delle immagini, MCS separa la fase di masterizzazione dal flusso di lavoro complessivo di creazione o aggiornamento del catalogo e suddivide il processo in due fasi:

1. Creare immagini preparate da un'unica immagine sorgente.
2. Utilizzare l'immagine preparata per creare o aggiornare un catalogo di macchine MCS.

È possibile creare in anticipo le immagini preparate. È possibile utilizzare una singola immagine preparata per creare o aggiornare più cataloghi di macchine con provisioning MCS.

Scoprire come un'immagine preparata viene utilizzata in più cataloghi di macchine MCS quando si utilizza Web Studio dall'immagine:



Definizione dell'immagine: le definizioni delle immagini sono un raggruppamento logico di versioni di un'immagine. La definizione dell'immagine contiene informazioni quali:

- il motivo per cui l'immagine è stata creata;
- il sistema operativo a cui è destinata;
- altre informazioni sull'uso dell'immagine.

Un catalogo non viene creato a partire da una definizione di immagine, ma dalle versioni dell'immagine create in base alla definizione dell'immagine.

Versione dell'immagine: le versioni delle immagini gestiscono il controllo delle versioni della definizione dell'immagine. Una definizione di immagine può avere più versioni dell'immagine. Utilizzare le versioni delle immagini come immagini preparate per creare o aggiornare un catalogo.

In alternativa, se si desidera utilizzare i comandi PowerShell per creare uno schema di provisioning con cui creare o aggiornare un catalogo, è necessario creare una specifica della versione dell'immagine preparata basata sulla specifica della versione dell'immagine master necessaria per il proprio ambiente.

Partecipare all'anteprima tecnica

Se si è interessati a partecipare alla Tech Preview, fornire i propri recapiti qui.

Aiuteremo a configurare l'ambiente di test e forniremo supporto tecnico, se necessario.

Requisito

- Per l'immagine master di Windows, sono supportate solo le immagini VDA di versione 2311 e successive e MCS/IO abilitato.

Limitazioni

Attualmente, la funzionalità non supporta quanto segue:

- Più NIC in Azure
- Funzione disco dati persistente
- Ibernazione per il multisessione
- Modifica del tipo di immagine

Gestione del ciclo di vita delle immagini con Web Studio

Il ciclo di vita dell'immagine quando si utilizza Web Studio è:

1. Creare un'immagine preparata: creare una definizione dell'immagine e la sua versione iniziale.
2. Creare versioni dell'immagine a partire dalla versione iniziale.

3. Utilizzare una versione dell'immagine come immagine preparata per creare cataloghi.
4. Aggiornare un catalogo di macchine con un'immagine preparata diversa.
5. Gestire le definizioni e le versioni delle immagini: modificare il nome e la descrizione delle versioni delle immagini e la descrizione di una definizione dell'immagine.
6. Eliminare una versione dell'immagine.
7. Eliminare una definizione di immagine.

In alternativa, è anche possibile gestire le immagini utilizzando PowerShell. Vedere Gestione del ciclo di vita delle immagini con PowerShell.

Creare o aggiornare un catalogo utilizzando un'immagine preparata

Creare immagini preparate e utilizzarle per creare o aggiornare un catalogo di macchine MCS utilizzando:

- Web Studio
- Comandi PowerShell

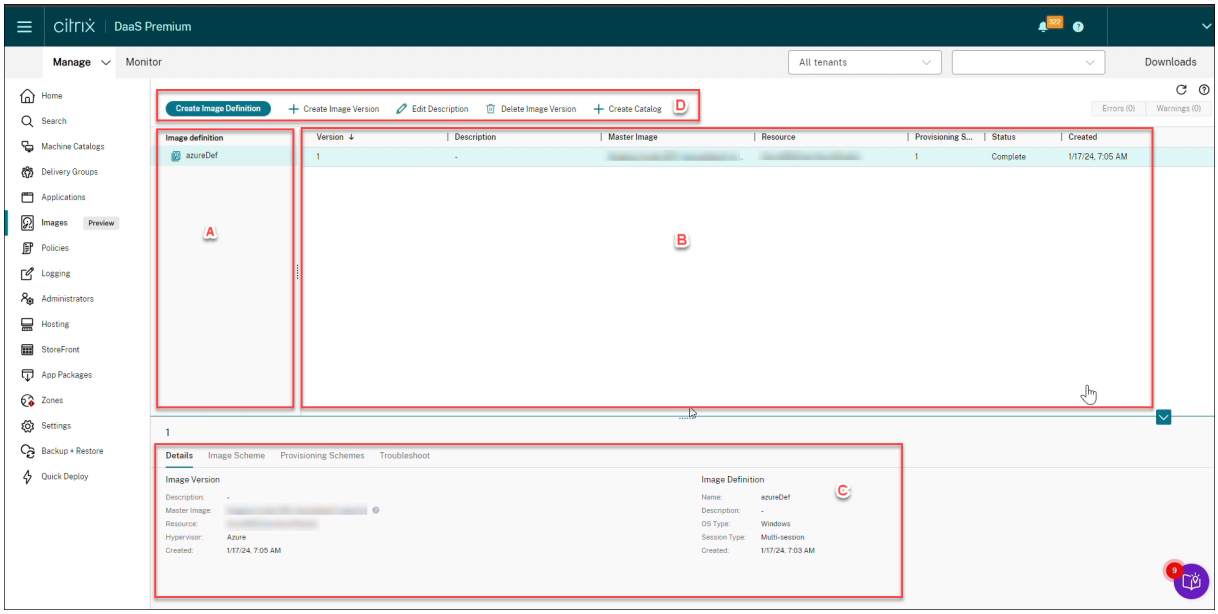
Utilizzare Web Studio

Vedere i seguenti argomenti:

- Comprendere il nodo delle immagini
- Creare una definizione e una versione iniziale dell'immagine
- Creare versioni di immagini
- Creare un catalogo di macchine dal nodo Images
- Creare un catalogo macchine dal nodo Machine Catalogs
- Aggiornare un catalogo di macchine con un'immagine preparata diversa
- Gestire le definizioni e le versioni delle immagini

Comprendere il nodo delle immagini

Utilizzare il nodo **Images** (Immagini) per creare e gestire immagini preparate per MCS. La sua visualizzazione principale è divisa in quattro parti:



Etichetta	Parte	Descrizione
A	Definizioni delle immagini	Elenca le definizioni delle immagini create in precedenza.
B	Versioni delle immagini	Visualizza le versioni dell'immagine della definizione immagine selezionata.
C	Dettagli	• La scheda **Details** (Dettagli) presenta informazioni dettagliate sulla definizione o la versione dell'immagine selezionata, ad esempio Immagine principale, Risorsa, Hypervisor, nome della definizione dell'immagine, tipo di sistema operativo e tipo di sessione. • La scheda **Schema immagini** visualizza informazioni sul modello utilizzato per la preparazione delle immagini, ad esempio disco rigido, dimensioni del computer, tipo di licenza, set di crittografia del disco, profilo del computer e così via. • La scheda **Provisioning**
D	Barra delle azioni	Elenca le azioni che è possibile eseguire sulle definizioni e sulle versioni delle immagini, ad esempio **Create Image Version** (Crea versione immagine), **Edit Description** (Modifica descrizione), **Delete Image Version** (Elimina versione immagine) e **Create Catalog** (Crea catalogo).

Creare un catalogo di macchine utilizzando l'immagine preparata

I passaggi chiave per creare un catalogo di macchine MCS utilizzando l'immagine preparata sono:

1. Creare la definizione dell'immagine e le versioni iniziali dell'immagine.
2. Usare la versione dell'immagine come immagine preparata per creare un catalogo.

Creare una definizione e una versione iniziale dell'immagine

Per creare una definizione dell'immagine e la sua versione iniziale, effettuare le seguenti operazioni:

1. Accedere a Web Studio e selezionare il nodo **Images** (Immagini). Fare clic su **Next** (Avanti) nella pagina **Introduction** (Introduzione).
2. Nella pagina **Image Definition** (Definizione dell'immagine), specificare il **tipo di sistema operativo** e il **tipo di sessione** per la definizione dell'immagine.
3. Nella pagina **Image**, selezionare **Resources** (Risorse) e un'immagine master da utilizzare come modello per creare la versione dell'immagine. È possibile selezionare la casella di controllo **Use a machine profile** (Usa un profilo macchina) e selezionare un profilo macchina.

   > **Nota:**
   >
   > Prima di selezionare un'immagine, verificare che sull'immagine master sia installato il VDA 2311 o versione successiva e che il driver MCSIO sia installato sul VDA.

4. (Solo per Azure) Nella pagina **torage and License Types** (Tipi di archiviazione e licenze), selezionare il tipo di archiviazione e licenza da utilizzare nell'ambito del processo di preparazione dell'immagine.

   > **Nota:**
   >
   > Se si seleziona un profilo macchina nella pagina **Image**, il tipo di licenza del profilo macchina viene preselezionato in base all'impostazione del profilo.

5. Nella pagina **Machine Specification** (Specifiche della macchina):

   - Per Azure, selezionare una dimensione computer. Se si seleziona un profilo macchina nella pagina **Image**, la dimensione della macchina del profilo macchina viene selezionata per impostazione predefinita.
   - Per VMware, se si seleziona un profilo macchina, è possibile visualizzare il numero di CPU virtuali derivato dal profilo della macchina ed è immutabile. Se non si seleziona un profilo macchina, è possibile visualizzare solo la dimensione della memoria derivata dall'immagine master.

6. Nella pagina **NIC** selezionare o aggiungere schede NIC per l'immagine di preparazione. Per ogni NIC, selezionare una rete virtuale associata.

   Per VMware, se non si seleziona un profilo macchina, per impostazione predefinita viene selezionata la scheda NIC associata all'immagine master. Se si seleziona un profilo macchina, le NIC sono derivate dal profilo macchina e il conteggio è immutabile.

   > **Nota:**
   >
   > In Azure non sono supportate più schede NIC.

7. (Solo per Azure) Nella pagina **Disk Settings** (Impostazioni disco), selezionare la chiave di crittografia gestita dal cliente (CMEK). Se il profilo macchina non ha un CMEK ma l'immagine master sì, preselezionare il CMEK dall'immagine master.
8. Nella pagina **Version Description** (Descrizione della versione), inserire una descrizione per la versione iniziale dell'immagine creata.
9. Nella pagina **Summary** (Riepilogo), controllare i dettagli della definizione dell'immagine e della versione iniziale dell'immagine creata. Immettere un nome e una descrizione per la definizione dell'immagine. Fare clic su **Finish**.

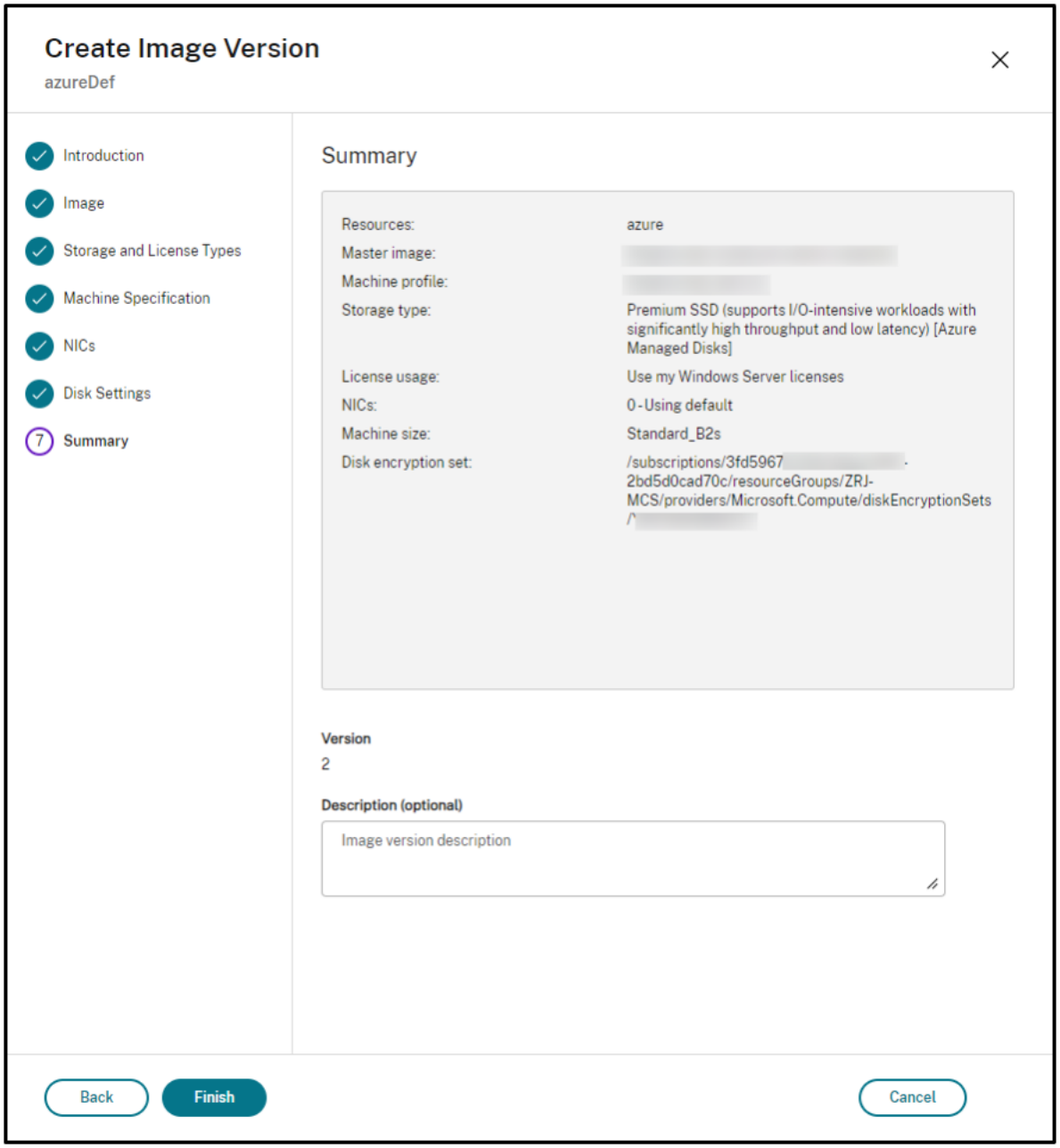
Creare versioni di immagini

Le versioni delle immagini consentono la gestione di diverse iterazioni o aggiornamenti di una particolare immagine. Questa funzionalità consente di gestire più versioni di un'immagine per scopi diversi.

Per creare versioni dell'immagine a partire dalla versione iniziale dell'immagine, procedere come segue:

> **Nota:**
>
> L'unità di hosting di tutte le versioni delle immagini deve essere la stessa.

1. Passare al nodo **Images**, selezionare una versione dell'immagine e selezionare **Create Image Version** (Crea versione immagine).
2. Se si desidera una configurazione della versione dell'immagine diversa dalla versione dell'immagine configurata inizialmente, configurare le impostazioni nelle pagine **Image**, **Storage and License Types** (Archiviazione e tipi di licenza), **Machine Specification** (Specifiche macchina), **NIC** e **Disk Settings** (Impostazioni disco) della finestra di dialogo **Create Image Version** (Crea versione immagine).
3. Aggiungere una descrizione per la versione dell'immagine. Fare clic su **Finish**.



Creare un catalogo di macchine dal nodo Images

Utilizzare l'opzione **Create catalog** (Crea catalogo) nel nodo **Images** per creare un catalogo utilizzando la versione dell'immagine.

In alternativa, è possibile selezionare la versione durante la creazione di un catalogo nel nodo **Machine Catalogs** (Cataloghi macchine), collegandosi all'opzione dell'immagine preparata nel flusso di creazione del catalogo. Vedere Creare un catalogo macchine dal nodo Machine Catalogs

Per creare un catalogo di macchine MCS dal nodo **Images**, effettuare le seguenti operazioni:

1. Selezionare una versione dell'immagine e fare clic su **Create catalog** (Crea catalogo). Fare clic su **Next** (Avanti) nella pagina **Introduction** (Introduzione).
2. Nella pagina **Desktop Experience** (Esperienza desktop), seleziona l'esperienza desktop richiesta.
3. Dalla pagina **Image** alla pagina **Disk Settings**, le impostazioni sono preselezionate in base alla versione dell'immagine selezionata.
4. (Per Azure) Nella pagina **Resource Group** (Gruppo risorse), è possibile scegliere di creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente per inserire le risorse di questo catalogo.
5. Completare le impostazioni nelle pagine successive.
6. Nella pagina **Summary** (Riepilogo), verificare i dettagli del catalogo delle macchine. Immettere un nome e una descrizione per il catalogo di macchine. Fare clic su **Finish**.
7. Passare al nodo **Machine Catalogs** per vedere il catalogo macchine creato.

Creare un catalogo macchine dal nodo Machine Catalogs

Per creare un catalogo macchine MCS dal nodo **Machine Catalogs**, effettuare le seguenti operazioni:

1. Fare clic su **Machine Catalogs** nel riquadro di navigazione a sinistra.
2. Fare clic su **Create Machine Catalog** (Crea catalogo di macchine). Viene visualizzata la pagina **Machine Catalog Setup**. Fare clic su **Next** (Avanti) nelle pagine **Introduction**, **Machine Type** (Tipo di macchina) e **Machine Management** (Gestione macchina).
3. Nella pagina **Image**:

    a) Selezionare **Prepared image** (Immagine preparata).
    b) In **Prepared image**, selezionare una versione dell'immagine di una definizione di immagine.
    c) Fare clic sul nome della versione dell'immagine. Per visualizzare ulteriori dettagli sulla versione dell'immagine selezionata, fare clic sul numero della versione, che è sottolineato.
    d) Se la versione dell'immagine selezionata è configurata con un profilo macchina, selezionare un profilo macchina. Se la versione dell'immagine selezionata non è configurata con un profilo macchina, non è possibile scegliere di utilizzare un profilo macchina.

4. Configurare le impostazioni nelle pagine successive.
5. Nella pagina **Disk Settings** (Impostazioni disco), se l'immagine preparata selezionata utilizza un set di crittografia del disco, non è possibile rimuovere il set di crittografia, ma è possibile modificare la chiave con un'altra chiave di crittografia.
6. (Per Azure) Nella pagina **Resource Group** (Gruppo risorse), è possibile scegliere di creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente per inserire le risorse di questo catalogo.

7. Completare le impostazioni nelle pagine successive.
8. Nella pagina **Summary** (Riepilogo), verificare i dettagli del catalogo delle macchine. Immettere un nome e una descrizione per il catalogo di macchine. Fare clic su **Finish**.

Aggiornare un catalogo di macchine con un'immagine preparata diversa

Per aggiornare un catalogo di macchine MCS esistente con un'immagine preparata diversa, effettuare le seguenti operazioni:

1. Fare clic su **Machine Catalogs** nel riquadro di navigazione a sinistra e selezionare un catalogo di macchine da aggiornare. Fare clic con il pulsante destro del mouse e selezionare **Change Prepared Image** (Modifica immagine preparata).
2. Nella pagina **Image** selezionare un'immagine preparata.
3. Nella pagina **Rollout strategy** (Strategia di rollout), selezionare quando si desidera aggiornare questo catalogo con l'immagine preparata selezionata.
4. Nella pagina **Summary** (Riepilogo), controllare i dettagli. Fare clic su **Finish**.

È possibile visualizzare la cronologia delle modifiche apportate alle immagini di un catalogo. Per visualizzare la cronologia, procedere come segue:

1. Selezionare un catalogo di macchine.
2. Nella scheda **Template Properties** (Proprietà modello) nel campo **Prepared image** (Immagine preparata), fare clic su **View Image history** (Visualizza cronologia immagini).

Gestire le definizioni e le versioni delle immagini

È possibile modificare ed eliminare le definizioni e le versioni delle immagini per gestire l'uso delle varie versioni e definizioni delle immagini create.

Modificare la definizione di un'immagine È possibile modificare il nome e la descrizione di una definizione di immagine.

Per modificare la definizione di un'immagine, effettuare le seguenti operazioni:

1. Passare al nodo **Images** (Immagini), selezionare una definizione di immagine e selezionare **Edit Image Definition** (Modifica definizione immagine).

Modificare la versione dell'immagine È possibile modificare la descrizione di una versione dell'immagine per specificarne lo scopo.

Per modificare una versione dell'immagine, procedere come segue:

1. Passare al nodo **Images**, seleziona una versione dell'immagine e selezionare **Edit Description** (Modifica descrizione).

Eliminare una versione dell'immagine Per eliminare una versione dell'immagine, procedere come segue:

1. Passare al nodo **Images**, selezionare una versione dell'immagine e selezionare **Delete Image Version** (Elimina versione immagine).

> **Nota:**
>
> Non è possibile eliminare una versione dell'immagine se è utilizzata da un catalogo di macchine.

Eliminare una definizione di immagine Per eliminare una definizione di immagine, effettuare le seguenti operazioni:

1. Passare al nodo **Images** (Immagini), selezionare una definizione di immagine e selezionare **Delete Image Definition** (Elimina definizione immagine).

> **Nota:**
>
> Non è possibile eliminare una definizione di immagine se contiene una versione dell'immagine.

Gestione del ciclo di vita delle immagini tramite PowerShell Se si desidera utilizzare i comandi PowerShell per creare uno schema di provisioning, è necessario creare una specifica della versione dell'immagine preparata basata sulla specifica della versione dell'immagine master necessaria per il proprio ambiente.

Specifica della versione dell'immagine master: si tratta di un'immagine specifica aggiunta o creata in una versione dell'immagine. È possibile aggiungere un'immagine esistente nell'hypervisor come specifica di versione dell'immagine master o creare una specifica di versione dell'immagine preparata basata sulla specifica della versione dell'immagine master in base alla specifica della versione dell'immagine master, se necessario per il proprio ambiente. La specifica della versione dell'immagine preparata può essere utilizzata per più schemi di provisioning.

Il ciclo di vita di un'immagine quando si utilizzano i comandi PowerShell è:

1. Creare un'immagine:
    a) Creare una definizione dell'immagine.
    b) Creare una versione dell'immagine.
    c) Aggiungere una specifica della versione dell'immagine principale.
    d) Creare una specifica di versione dell'immagine preparata.

2. Creare un catalogo di macchine MCS utilizzando una specifica di versione dell'immagine preparata:

    a) Creare un catalogo di broker.
    b) Creare un pool di identità.
    c) Creare uno schema di provisioning con il parametro della specifica della versione dell'immagine preparata Uid utilizzando il comando `New-ProvScheme`.
    d) Collegare il catalogo dei broker allo schema di provisioning.

3. Creare macchine virtuali nel catalogo delle macchine MCS.
4. Modificare la specifica della versione dell'immagine preparata di uno schema di provisioning utilizzando il comando `Set-ProvScheme`.
5. Gestire le definizioni e le versioni delle immagini: modificare le versioni e le definizioni delle immagini.
6. Eliminare un catalogo di macchine MCS: l'ordine di eliminazione è: specifica della versione dell'immagine preparata > specifica della versione dell'immagine master > versione dell'immagine > definizione dell'immagine. Prima di eliminare la specifica della versione dell'immagine, assicurarsi che la specifica della versione dell'immagine preparata non sia associata a nessun catalogo di macchine MCS.

Utilizzare PowerShell

È possibile effettuare le seguenti operazioni utilizzando i comandi PowerShell:

- Creare un'immagine preparata
- Creare un catalogo utilizzando le specifiche della versione dell'immagine preparata
- Aggiornare un catalogo utilizzando una specifica di versione dell'immagine preparata
- Eliminare la definizione dell'immagine, la versione dell'immagine e le specifiche della versione dell'immagine preparata
- Gestirei la definizione e la versione dell'immagine
- Ottenere la definizione dell'immagine, la versione dell'immagine, le specifiche della versione dell'immagine preparata e i dettagli dello schema di provisioning

Creare un'immagine preparata

I comandi PowerShell dettagliati per creare una specifica di versione dell'immagine preparata sono i seguenti:

1. Controllare i nomi delle definizioni delle immagini disponibili utilizzando `Test-ProvImageDefinition command`. Ad esempio,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string
    []>
```

2. Creare una definizione di immagine mediante il comando `New-ProvImageDefinition`. Ad esempio,

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType
    Windows -VdaSessionSupport MultiSession
```

3. Creare una versione dell'immagine usando il comando `New-ProvImageVersion`. Ad esempio,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "
    version 1"
```

4. Aggiungere una specifica della versione dell'immagine principale alla versione dell'immagine utilizzando il comando `Add-ProvImageVersionSpec`. Ad esempio,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
    ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "
    XDHyp:\HostingUnits\azure\image.folder\azureresourcegroup.
    resourcegroup\win2022-snapshot.snapshot"
```

> **Nota:**
>
> È possibile aggiungere una sola specifica della versione dell'immagine principale a una versione dell'immagine per un'unità di hosting.

5. Creare una specifica di versione dell'immagine preparata dalla specifica della versione dell'immagine principale utilizzando il comando `New-ProvImageVersionSpec`. Ad esempio,

```
New-ProvImageVersionSpec
-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network"
-ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder
    \Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
```

> **Nota:**
>
> Un'unità di hosting e un tipo di preparazione possono avere una sola istanza preparata.

Esempio del set completo di comandi Powershell per creare la definizione dell'immagine, la versione dell'immagine e le specifiche della versione dell'immagine preparata in Azure:

```
$ImageDefintion = New-ProvImageDefinition
-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
    MultiSession
 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
     $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
    azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName azure -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder\
      Standard_B2ms.serviceoffering" -CustomProperties "<
      CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
      machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
      instance`"></CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

Esempio del set completo di comandi Powershell per creare la definizione dell'immagine, la versione dell'immagine e le specifiche della versione dell'immagine preparata in VMware:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
    OsType Windows -VdaSessionSupport SingleSession
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
    master-snap.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

> **Nota:**
>
> - Tutte le specifiche della versione dell'immagine indicate in una definizione di immagine devono appartenere alla stessa unità di hosting.
> - Una versione dell'immagine può avere solo una specifica di versione dell'immagine princi-

> pale e una specifica di versione dell'immagine preparata.
> - Tutte le specifiche della versione dell'immagine devono avere un profilo macchina o nessuna delle specifiche della versione dell'immagine deve avere un profilo macchina.
> - Non è possibile specificare un gruppo di risorse durante la creazione di una specifica di versione dell'immagine.

Creare un catalogo utilizzando una specifica di versione dell'immagine preparata

Creare un catalogo di macchine MCS dalla specifica della versione dell'immagine preparata utilizzando il comando `New-ProvScheme`. Ad esempio,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <
    int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <
    Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable
    >] [-ServiceOffering <string>] [-SecurityGroup <string[]>] [-
    TenancyType <string>] [-MachineProfile <string>] [-CustomProperties
    <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

Oppure

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitName <string> -IdentityPoolName <string> [-
    VMCpuCount <int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-
    NetworkMapping <Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-
    Metadata <Hashtable>] [-ServiceOffering <string>] [-SecurityGroup <
    string[]>] [-TenancyType <string>] [-MachineProfile <string>] [-
    CustomProperties <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

Esempio di set completo di comandi Powershell per creare un catalogo in Azure:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
    $False  -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.
    local" -IdentityPoolName "azurecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "azure##" -NamingSchemeType "Numeric
    " -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
```



```
    HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -
    Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits\
    azure\serviceoffering.folder\Standard_B2s.serviceoffering" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.
     com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
     XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
     StorageAccountType`" Value=`"StandardSSD_LRS`" /></
     CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
```

Esempio di set completo di comandi Powershell per creare un catalogo in VMware:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
    $False  -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "vmware.
    local" -IdentityPoolName "vmwarecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "
    Numeric" -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
    -Scope @() -SecurityGroup @() -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
```

Aggiornare un catalogo utilizzando una specifica di versione dell'immagine preparata

È possibile aggiornare un catalogo utilizzando il comando `Set-ProvSchemeImage`. Ad esempio,

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
    <Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-
    PurgeJobOnSuccess]
```

Oppure


```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -
    ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
    ] [-PurgeJobOnSuccess]
```

Esempio di set completo di comandi Powershell per aggiornare un catalogo:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
    PreparationType -eq 'Mcs'"
Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
```

Eliminare la definizione dell'immagine, la versione dell'immagine e le specifiche della versione dell'immagine preparata

Considerare quanto segue prima di eliminare una definizione di immagine, una versione dell'immagine e una specifica della versione dell'immagine preparata:

- Una definizione di immagine non può essere eliminata se contiene una versione dell'immagine.
- Una versione dell'immagine non può essere eliminata se contiene una specifica di versione dell'immagine.
- Una specifica di versione dell'immagine master non può essere eliminata se viene utilizzata da qualsiasi altra specifica di versione dell'immagine preparata.
- Una specifica di versione dell'immagine preparata non può essere eliminata se utilizzata da uno schema di provisioning.

I passaggi dettagliati sono i seguenti:

1. Rimuovere una specifica di versione dell'immagine preparata. Ad esempio,

   ```
   $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
       ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
       PreparationType -eq 'Mcs'"
   Remove-ProvImageVersionSpec -ImageVersionSpecUid
       $PreparedImageVersionSpec.ImageVersionSpecUid -
       RunAsynchronously
   ```

   > **Nota:**
   >
   > La specifica della versione dell'immagine principale può essere eliminata solo quando non è associata ad alcuna specifica della versione dell'immagine preparata.

2. Rimuovere la specifica della versione dell'immagine principale. Ad esempio,

   ```
   $MasterImageVersionSpec = Get-ProvImageVersionSpec -
       ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
       PreparationType -eq 'None'"
   ```



```
2 Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
```

3. Rimuovere una versione dell'immagine. Ad esempio,

```
1 Remove-ProvImageVersion -ImageDefinitionName image1 -
    ImageVersionNumber 1
```

4. Rimuovere una definizione di immagine. Ad esempio,

```
1 Remove-ProvImageDefinition -ImageDefinitionName image1
```

Esempio del set completo di comandi PowerShell:

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
2 $Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
3 $MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
     image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"
4 $Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
5 Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
     1
6 Remove-ProvImageDefinition -ImageDefinitionName image1
```

Gestirei la definizione e la versione dell'immagine

È possibile rinominare e modificare la definizione di un'immagine e modificare una versione dell'immagine.

- Rinominare una definizione di immagine mediante il comando `Rename-ProvImageDefinition`. Ad esempio:

```
1 Rename-ProvImageDefinition -ImageDefinitionUid <Guid> -
    NewImageDefinitionName <string>
```

Oppure

```
1 Rename-ProvImageDefinition -ImageDefinitionName <string> -
    NewImageDefinitionName <string>
```

- Modificare una definizione di immagine mediante il comando `Set-ProvImageDefinition`. Ad esempio:

```
1 Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
    <string>]
```


Oppure

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-
    Description <string>]
```

- Modificare una versione dell'immagine usando il comando `Set-ProvImageVersion`. Ad esempio:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <
    string>]
```

Oppure

```
Set-ProvImageVersion -ImageDefinitionName <string> -
    ImageVersionNumber <int> [-Description <string>]
```

Ottenere la definizione dell'immagine, la versione dell'immagine, le specifiche della versione dell'immagine preparata e i dettagli dello schema di provisioning

- Ottenere dettagli sulla definizione dell'immagine usando il comando `Get-ProvImageDefinition`. Ad esempio:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
    ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-
    MaxRecordCount <int>] [-Skip <int>] [-SortBy <string>] [-
    Filter <string>]
```

- Ottenere i dettagli della versione dell'immagine usando il comando `Get-ProvImageVersion`. Ad esempio:
  - Per elencare le versioni delle immagini in una definizione di immagine,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    Oppure

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - Per ottenere i dettagli della versione dell'immagine,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    Oppure

    ```
    Get-ProvImageVersion -ImageDefinitionName <string> -
        ImageVersionNumber <int>
    ```

- Ottenere le specifiche della versione dell'immagine preparata usando il comando `Get-ProvImageVersionSpec`. Ad esempio:

- Per elencare tutte le specifiche della versione dell'immagine preparata in una versione dell'immagine,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

- Per elencare le specifiche della versione dell'immagine master in una specifica di versione dell'immagine preparata,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "None"'
```

- Per elencare le specifiche della versione dell'immagine preparata in una versione dell'immagine associata a un'immagine master,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

- Per ottenere le specifiche di versione dell'immagine preparate correttamente in una versione di immagine,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and
    ImageVersionSpecStatus -eq "Complete"'
```

- Per ottenere i dettagli delle specifiche della versione dell'immagine preparata,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Ottenere i dettagli dello schema di provisioning usando il comando `Get-ProvScheme`. Ad esempio:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
    ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <
    String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>]
    [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-
    FilterScope <Guid>]
```

- Ottenere la cronologia delle specifiche della versione dell'immagine preparata di uno schema di provisioning utilizzando il comando `Get-ProvSchemeImageVersionSpecHistory`. Ad esempio:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
    String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid
     <Guid>] [-ImageVersionSpecHistoryUid <Guid>] [-
    ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
    Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
    Guid>]
```


Creare un catalogo di Microsoft Azure

August 23, 2024

> **Nota:**
>
> Da luglio 2023, Microsoft ha rinominato Azure Active Directory (Azure AD) in Microsoft Entra ID. In questo documento, qualsiasi riferimento ad Azure Active Directory, Azure AD o AAD ora si riferisce a Microsoft Entra ID.

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Microsoft Azure Resource Manager.

> **Nota:**
>
> Prima di creare un catalogo di Microsoft Azure, è necessario completare la creazione di una connessione a Microsoft Azure. Vedere Connessione a Microsoft Azure.

Creare un catalogo di macchine

È possibile creare un catalogo di macchine in due modi:

- Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio
- Creare un catalogo di macchine usando PowerShell

Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio

Un'immagine può essere un disco, una snapshot o una versione immagine di una definizione di immagine all'interno della Raccolta di calcolo di Azure utilizzata per creare le macchine virtuali in un catalogo di macchine. Prima di creare il catalogo delle macchine, creare un'immagine in Azure Resource Manager. Per informazioni generali sulle immagini, vedere Creare cataloghi delle macchine.

> **Nota:**
>
> Il supporto per l'utilizzo di un'immagine master da una regione diversa da quella configurata nella connessione host è obsoleto. Utilizzare la Raccolta di calcolo di Azure per replicare l'immagine master nell'area desiderata.

Durante la preparazione dell'immagine, viene creata una macchina virtuale di preparazione basata sulla macchina virtuale originale. Questa macchina virtuale di preparazione è disconnessa dalla rete.

Per disconnettere la rete dalla macchina virtuale di preparazione, viene creato un gruppo di sicurezza di rete per negare tutto il traffico in entrata e in uscita. Il gruppo di sicurezza di rete viene creato automaticamente una volta per catalogo. Il nome del gruppo di sicurezza di rete è `Citrix-Deny-All-a3pgu-GUID`, dove il GUID viene generato casualmente. Ad esempio, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

Nella procedura guidata di creazione del catalogo delle macchine:

- Le pagine **Machine Type** (Tipo di macchina) e **Machine Management** (Gestione macchina) non contengono informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Image** scegliere un'immagine da utilizzare come modello per creare macchine in questo catalogo.

  Se si seleziona **Raccolta di calcolo di Azure** (Immagine master) come tipo di immagine da utilizzare, fare clic su **Select an image** (Selezionare un'immagine) e seguire questi passaggi per selezionare un'immagine master come necessario:

  1. (Applicabile solo alle connessioni configurate con immagini condivise all'interno di uno stesso tenant o tra tenant diversi) Selezionare un abbonamento in cui risiede l'immagine.
  2. Selezionare un gruppo di risorse.
  3. Passare ad Azure VHD, alla Raccolta di calcolo di Azure o alla versione immagine di Azure. Se necessario, aggiungere una nota per l'immagine selezionata.

  Quando selezionate un'immagine, tenere presente quanto segue:

  - Verificare che sull'immagine sia installato un Citrix VDA.
  - Se si seleziona un disco rigido virtuale collegato a una macchina virtuale, è necessario spegnere la VM prima di procedere al passaggio successivo.

  > **Nota:**
  >
  > - La sottoscrizione corrispondente alla connessione (host) che ha creato le macchine nel catalogo è contrassegnata da un punto verde. Le altre sottoscrizioni sono quelle con Raccolta di calcolo di Azure condivisa con quella sottoscrizione. In queste sottoscrizioni vengono mostrate solo le gallerie condivise. Per informazioni su come configurare gli abbonamenti condivisi, vedere Condividere immagini all'interno di un tenant (tra abbonamenti) e Condividere immagini tra tenant.
  > - L'uso di un profilo macchina con un avvio attendibile quale **Security Type** (Tipo di sicurezza) è obbligatorio quando si seleziona un'immagine o una snapshot con avvio attendibile abilitato. È quindi possibile abilitare o disabilitare SecureBoot e vTPM specificandone i valori nel profilo macchina. L'avvio attendibile non è supportato per la Raccolta immagini condivise. Per informazioni sull'avvio attendibile di Azure, vedere

https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

- È possibile creare uno schema di provisioning utilizzando il disco del sistema operativo temporaneo su Windows con avvio attendibile. Quando si seleziona un'immagine con avvio attendibile, è necessario selezionare un profilo macchina con avvio attendibile abilitato con vTPM. Per creare cataloghi delle macchine utilizzando un disco del sistema operativo temporaneo, vedere Come creare macchine utilizzando dischi del sistema operativo temporanei.
- Quando è in corso la replica dell'immagine, è possibile procedere e selezionare l'immagine come immagine master e completare la configurazione. Tuttavia, il completamento della creazione del catalogo potrebbe richiedere più tempo durante la replica dell'immagine. MCS richiede che la replica venga completata entro un'ora a partire dalla creazione del catalogo. In caso di timeout della replica, la creazione del catalogo non riesce. È possibile verificare lo stato della replica in Azure. Riprovare se la replica è ancora in sospeso o dopo il completamento della replica.
- Quando si seleziona un'immagine master per i cataloghi delle macchine in Azure, MCS identifica il tipo di sistema operativo in base all'immagine master e al profilo macchina selezionati. Se MCS non è in grado di identificarlo, selezionare il tipo di sistema operativo corrispondente all'immagine master.
- È possibile effettuare il provisioning di un catalogo di macchine virtuali Gen2 utilizzando un'immagine Gen2 per migliorare le prestazioni in fase di avvio. Tuttavia, la creazione di un catalogo di macchine Gen2 utilizzando un'immagine Gen1 non è supportata. Allo stesso modo, non è supportata la creazione di un catalogo di macchine Gen1 utilizzando un'immagine Gen2. Inoltre, qualsiasi immagine precedente che non contiene informazioni sulla generazione è un'immagine Gen1.

Se si seleziona **Prepared image** (Immagine preparata) come tipo di immagine da utilizzare, fare clic su **Select an image** e selezionare un'immagine preparata come necessario.

Per garantire la corretta creazione della VM, verificare che sull'immagine sia installato Citrix VDA 2311 o successivo e che MCSIO sia presente sul VDA.

Una volta selezionata un'immagine, la casella di controllo **Use a machine profile (mandatory for Azure Active Directory)** [Usa un profilo macchina (obbligatoria per Azure Active Directory)] è automaticamente selezionata. Fare clic su **Select a machine profile** (Seleziona un profilo macchina) per accedere a una VM o a una specifica di modello ARM da un elenco di gruppi di risorse. Le macchine virtuali nel catalogo possono ereditare le configurazioni dal profilo macchina selezionato.

Convalidare la specifica del modello ARM per accertarsi che possa essere utilizzata come profilo macchina per creare un catalogo delle macchine. Esistono due modi per convalidare la specifica di modello ARM:

- Dopo aver selezionato la specifica del modello ARM dall'elenco dei gruppi di risorse, fare clic su **Next** (Avanti). Se la specifica del modello ARM contiene errori, vengono visualizzati messaggi di errore.
- Eseguire uno dei seguenti comandi PowerShell:
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  * `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Alcuni esempi di configurazioni che le macchine virtuali possono ereditare da un profilo macchina includono:

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

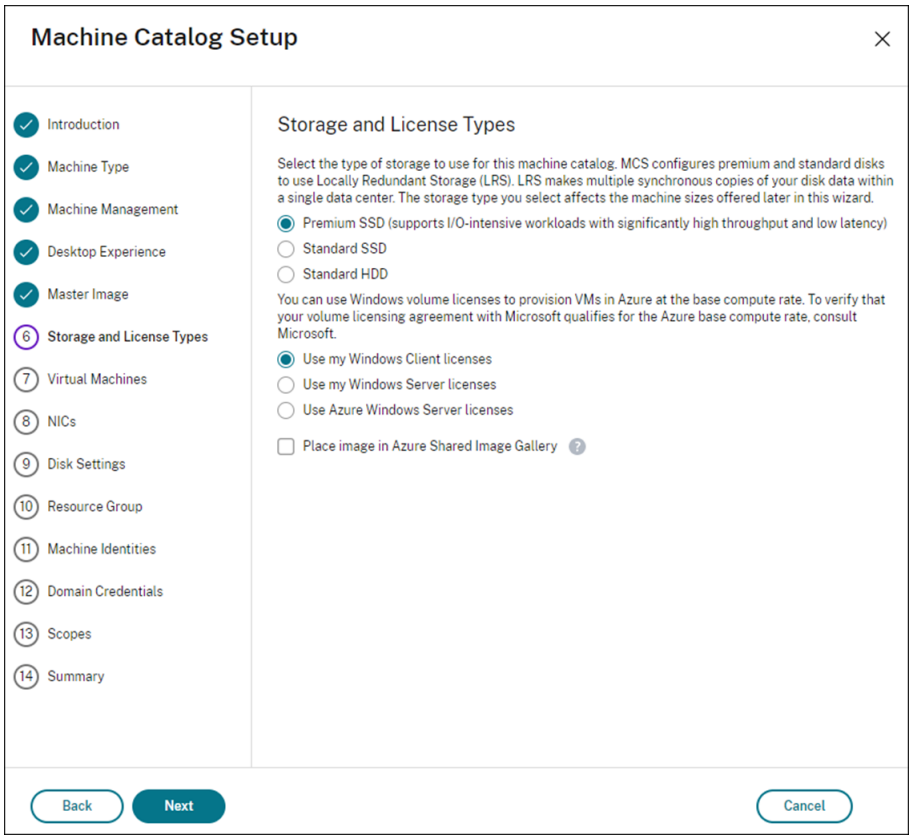
Dopo aver creato il catalogo, è possibile visualizzare le configurazioni che l'immagine eredita dal profilo della macchina. Nel nodo **Machine Catalogs** (Cataloghi delle macchine), selezionare il catalogo per visualizzare i relativi dettagli nel riquadro inferiore. Quindi, fare clic sulla scheda **Template Properties** (Proprietà modello) per visualizzare le proprietà del profilo della macchina. La sezione **Tags** (Tag) visualizza fino a tre tag. Per visualizzare tutti i tag posizionati sulla macchina virtuale, fare clic su **View all** (Visualizza tutto).

Se si desidera che MCS esegua il provisioning delle macchine virtuali in un host dedicato di Azure, abilitare la casella di controllo **Use a dedicated host group** (Utilizza un gruppo host dedicato) e quindi selezionare un gruppo host dall'elenco. Un gruppo di host è una risorsa che rappresenta una raccolta di host dedicati. Un host dedicato è un servizio che fornisce server fisici che ospitano una o più macchine virtuali. Il server dedicato alla sottoscrizione di Azure non è condiviso con altri sottoscrittori. Quando si utilizza un host dedicato, Azure garantisce che le macchine virtuali siano le uniche macchine in esecuzione su quell'host. Questa funzionalità è adatta per gli scenari in cui è necessario soddisfare i requisiti normativi o di sicurezza interni. Per ulteriori informazioni sui gruppi di host e sulle considerazioni per il loro utilizzo, vedere Host dedicati di Azure.

> **Importante:**
>
> - Vengono visualizzati solo i gruppi di host per i quali è abilitato il posizionamento automatico di Azure.
> - L'utilizzo di un gruppo host modifica la pagina **Virtual Machines** (Macchine virtuali)

> mostrata più avanti nella procedura guidata. In questa pagina vengono mostrate solo le dimensioni delle macchine contenute nel gruppo host selezionato. Inoltre, le zone di disponibilità vengono selezionate automaticamente e non sono disponibili per la selezione.

- La pagina **Storage and License Types** (Tipi di archiviazione e licenze) viene visualizzata solo quando si utilizza un'immagine di Azure Resource Manager.



Sono disponibili i seguenti tipi di archiviazione da utilizzare per il catalogo delle macchine:

- **SSD premium**. Offre un'opzione di archiviazione su disco ad alte prestazioni e a bassa latenza adatta per macchine virtuali con carichi di lavoro a uso intensivo di I/O.
- **SSD standard**. Offre un'opzione di archiviazione conveniente adatta a carichi di lavoro che richiedono prestazioni costanti a livelli di IOPS inferiori.
- **HDD standard**. Offre un'opzione di archiviazione su disco affidabile e a basso costo adatta per macchine virtuali che eseguono carichi di lavoro non sensibili alla latenza.
- **Disco del sistema operativo temporaneo di Azure**. Offre un'opzione di archiviazione conveniente che riutilizza il disco locale delle macchine virtuali per ospitare il disco del sistema operativo. In alternativa, è possibile utilizzare PowerShell per creare macchine che utilizzano dischi dei sistemi operativi temporanei. Per ulteriori informazioni, vedere Dischi temporanei di Azure. Tenere presenti le seguenti considerazioni quando si utilizza un disco del sistema operativo temporaneo:

  * Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.
  * Per aggiornare le macchine che utilizzano dischi dei sistemi operativi temporanei, è necessario selezionare un'immagine la cui dimensione non superi la dimensione del disco della cache o del disco temporaneo della macchina virtuale.
  * Non è possibile utilizzare l'opzione **Retain VM and system disk during power cycles** (Conserva la VM e il disco di sistema durante i cicli di alimentazione) disponibile più avanti nella procedura guidata.

> **Nota:**
>
> Il disco di identità viene sempre creato utilizzando SSD standard indipendentemente dal tipo di archiviazione scelto.

Il tipo di archiviazione determina le dimensioni delle macchine disponibili nella pagina **Virtual Machines** (Macchine virtuali) della procedura guidata. MCS configura dischi premium e standard per l'utilizzo dell'archiviazione con ridondanza locale (LRS). LRS esegue più copie sincrone dei dati del disco all'interno di un singolo centro dati. I dischi del sistema operativo temporaneo di Azure utilizzano il disco locale delle macchine virtuali per archiviare il sistema operativo. Per informazioni dettagliate sui tipi di archiviazione di Azure e sulla replica dell'archiviazione, vedere quanto segue:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Selezionare se utilizzare le licenze Windows o Linux esistenti.

- Licenze Windows: l'utilizzo di licenze Windows insieme a immagini Windows (immagini di supporto o immagini personalizzate della piattaforma Azure) consente di eseguire macchine virtuali Windows in Azure a un costo ridotto. Esistono due tipi di licenze:
  * **Licenza Windows Server**. Consente di utilizzare le licenze Windows Server o Azure Windows Server, consentendo l'utilizzo dei Vantaggi di Azure ibrido. Per i dettagli, vedere https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. I vantaggi di Azure ibrido riducono il costo di esecuzione delle macchine virtuali in Azure alla tariffa di elaborazione di base, eliminando il costo delle licenze aggiuntive di Windows Server dalla raccolta di Azure.
  * **Licenza client Windows**. Consente di trasferire le licenze di Windows 10 e Windows 11 in Azure, consentendo di eseguire macchine virtuali Windows 10 e Windows 11 in Azure senza la necessità di licenze aggiuntive. Per i dettagli, vedere Licenze di accesso client e licenze di gestione.

È possibile verificare che la macchina virtuale di cui è stato eseguito il provisioning stia utilizzando il vantaggio di licenza eseguendo il seguente comando PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Per il tipo di licenza Windows Server, verificare che il tipo di licenza sia **Windows_Server**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Per il tipo di licenza client Windows, verificare che il tipo di licenza sia **Windows_Client**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

In alternativa, è possibile utilizzare l'SDK PowerShell `Get-Provscheme` per eseguire la verifica. Ad esempio: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Per ulteriori informazioni su questo cmdlet, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licenze Linux: con le licenze Linux BYOS (Bring-Your-Own-Subscription), non è necessario pagare per il software. La tariffa BYOS include solo la tariffa per l'hardware di elaborazione. Esistono due tipi di licenze:
  - **RHEL_BYOS**: per utilizzare correttamente il tipo RHEL_BYOS, abilitare Red Hat Cloud Access nella sottoscrizione di Azure.
  - **SLES_BYOS**: le versioni BYOS di SLES includono il supporto di SUSE.

  È possibile impostare il valore LicenseType sulle opzioni Linux in `New-ProvScheme` e `Set-ProvScheme`.

  Esempio di impostazione di LicenseType su RHEL_BYOS per `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
    azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
    @() -CustomProperties '<CustomProperties xmlns="http://
    schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http
    ://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
```

  Esempio di impostazione di LicenseType su SLES_BYOS per `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
```



```
        StringProperty" Name="UseManagedDisks" Value="true" /><
        Property xsi:type="StringProperty" Name="StorageAccountType
        " Value="StandardSSD_LRS" /><Property xsi:type="
        StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
        /><Property xsi:type="StringProperty" Name="OsType" Value="
        Linux" /><Property xsi:type="StringProperty" Name="
        LicenseType" Value="SLES_BYOS" /></CustomProperties>'
```

> **Nota:**
>
> Se il valore `LicenseType` è vuoto, i valori predefiniti sono Azure Windows Server License (Licenza Azure Windows Server) o Azure Linux License (Licenza Azure Linux), a seconda del valore di OSType.

Esempio di impostazione di LicenseType su un valore vuoto:

```
1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
      CustomProperties '<CustomProperties xmlns="http://schemas.
      citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
      w3.org/2001/XMLSchema-instance"><Property xsi:type="
      StringProperty" Name="UseManagedDisks" Value="true" /><
      Property xsi:type="StringProperty" Name="StorageAccountType
      " Value="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
      /><Property xsi:type="StringProperty" Name="OsType" Value="
      Linux" /></CustomProperties>'
```

Consultare i seguenti documenti per comprendere i tipi di licenza e i relativi vantaggi:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise Azure) è un repository per la gestione e la condivisione di immagini. Consente di rendere disponibili le immagini in tutta l'organizzazione. Si consiglia di memorizzare un'immagine in SIG quando si creano cataloghi delle macchine di grandi dimensioni non persistenti, perché in questo modo è possibile reimpostare più velocemente i dischi del sistema operativo VDA. Dopo aver selezionato **Place image in Azure Compute Gallery** (Inserisci immagine nella Raccolta di calcolo di Azure), viene visualizzata la sezione **Azure Compute Gallery settings** (Impostazioni della Raccolta di calcolo di Azure), che consente di specificare altre impostazioni della Raccolta di calcolo di Azure:

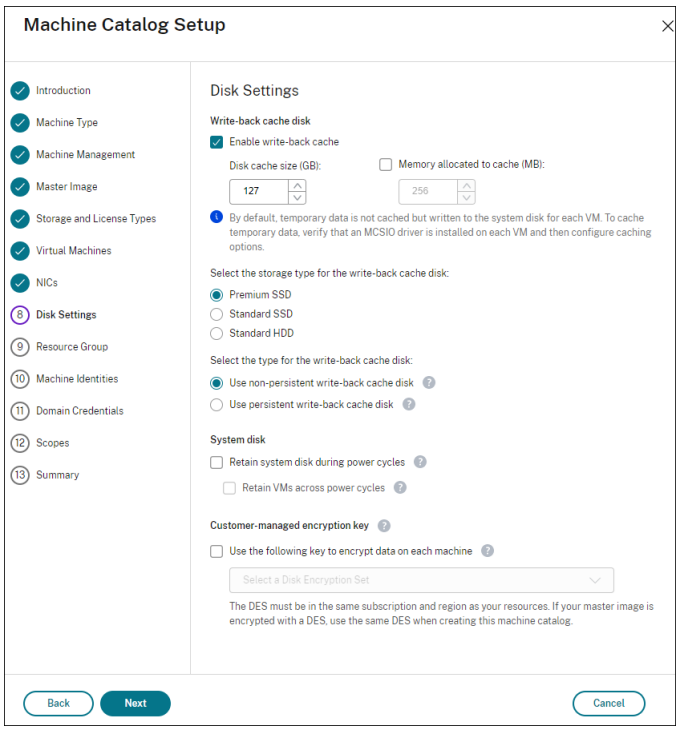
- **Ratio of virtual machines to image replicas** (Rapporto tra macchine virtuali e repliche di immagini). Consente di specificare il rapporto tra macchine virtuali e repliche di immagini che si desidera conservare in Azure. Per impostazione predefinita, Azure conserva una

singola replica di immagine ogni 40 macchine non persistenti. Per le macchine persistenti, l'impostazione predefinita del numero è 1.000.

– **Maximum replica count** (Numero massimo di repliche). Consente di specificare il numero massimo di repliche di immagini che si desidera conservare in Azure. L'impostazione predefinita è 10.

> **Nota:**
>
> In ACG viene creata una galleria per archiviare l'immagine. Questa galleria è accessibile solo a MCS per la creazione di macchine virtuali e non appare nella pagina **Select an image** (Selezionare un'immagine).

- Nella pagina **Virtual Machines** (Macchine virtuali), indicare quante macchine virtuali si desidera creare. È necessario specificarne almeno uno e selezionare una dimensione della macchina. Dopo la creazione del catalogo, è possibile modificare le dimensioni della macchina modificando il catalogo.
- La pagina **NIC** non contiene informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Disk Settings** (Impostazioni disco), scegliere se abilitare la cache write-back. Con la funzione di ottimizzazione dell'archiviazione MCS abilitata, è possibile configurare le seguenti impostazioni durante la creazione di un catalogo. Queste impostazioni si applicano sia agli ambienti Azure che agli ambienti GCP.



Dopo aver abilitato la cache write-back, è possibile procedere come segue:

- Configurare le dimensioni del disco e della RAM utilizzati per la memorizzazione nella cache dei dati temporanei. Per maggiori informazioni, consultare Configurare la cache per i dati temporanei.
- Selezionare il tipo di archiviazione per il disco della cache write-back. Sono disponibili le seguenti opzioni di archiviazione per il disco della cache write-back:
  * Premium SSD (SSD premium)
  * Standard SSD (SSD standard)
  * Standard HDD (HDD standard)
- Scegliere se si desidera che il disco della cache write-back venga mantenuto per le macchine virtuali di cui è stato eseguito il provisioning. Selezionare **Enable write-back cache** (Abilita cache write-back) per rendere disponibili le opzioni. Per impostazione predefinita, l'opzione **Use non-persistent write-back cache disk** (Usa disco della cache write-back non persistente) è selezionata.
- Selezionare il tipo per il disco della cache write-back.
  * **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se selezionato, il disco della cache write-back viene eliminato durante i cicli di alimentazione. Tutti i dati reindirizzati a tale disco andranno persi. Se il disco temporaneo della macchina virtuale dispone di spazio sufficiente, viene utilizzato per ospitare il disco della cache write-back per ridurre i costi. Dopo la creazione del catalogo, è possibile verificare se le macchine di cui è stato eseguito il provisioning utilizzano il disco temporaneo. A tale scopo, fare clic sul catalogo e verificare le informazioni nella scheda **Template Properties** (Proprietà modello). Se viene utilizzato il disco temporaneo, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **Yes (using VM's temporary disk)** (Sì, utilizzando il disco temporaneo della macchina virtuale). In caso contrario, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **No (not using VM's temporary disk)** (No, non utilizzando il disco temporaneo della macchina virtuale).
  * **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se questa opzione è selezionata, il disco della cache write-back persiste per le macchine virtuali di cui è stato eseguito il provisioning. L'abilitazione dell'opzione aumenta i costi di archiviazione.
- Scegliere se conservare le VM e i dischi di sistema per i VDA durante i cicli di alimentazione.

  Retain VM and system disk during power cycles (Conserva la VM e il disco di sistema durante i cicli di alimentazione). Disponibile quando si è selezionato **Enable write-back cache** (Abilita cache di write-back). Per impostazione predefinita, le VM e i dischi di sistema vengono eliminati all'arresto e ricreati all'avvio. Se si desidera ridurre i tempi di ri-

avvio delle VM, selezionare questa opzione. Tenere presente che l'attivazione di questa opzione aumenta anche i costi di archiviazione.

- Scegliere se abilitare **Storage cost savings** (Risparmi sui costi di archiviazione). Se abilitato, risparmia sui costi di archiviazione eseguendo il downgrade del disco di archiviazione ad HDD standard all'arresto della VM. La VM torna alle impostazioni originali al momento del riavvio. L'opzione si applica sia ai dischi di archiviazione che ai dischi cache write-back. In alternativa, è anche possibile usare PowerShell. Vedere Portare il tipo di archiviazione a un livello inferiore quando una VM viene arrestata.

  > **Nota:**
  >
  > Microsoft impone restrizioni sulla modifica del tipo di archiviazione durante l'arresto della macchina virtuale. È anche possibile che Microsoft in futuro blocchi le modifiche al tipo di archiviazione. Per ulteriori informazioni, vedere questo articolo di Microsoft.

- Scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Per ulteriori informazioni, vedere Crittografia lato server di Azure.

- Nella pagina **Resource Group** (Gruppo di risorse), scegliere se creare gruppi di risorse o utilizzare gruppi esistenti.
  - Se si sceglie di creare gruppi di risorse, selezionare **Next** (Avanti).
  - Se si sceglie di utilizzare gruppi di risorse esistenti, selezionare i gruppi dall'elenco **Available Provisioning Resource Groups** (Gruppi di risorse di provisioning disponibili). **Da ricordare**: selezionare un numero sufficiente di gruppi per ospitare le macchine che si stanno creando nel catalogo. Se se ne scelgono troppo pochi, viene visualizzato un messaggio. Si potrebbe voler selezionare un numero superiore al minimo richiesto se si prevede di aggiungere altre macchine virtuali al catalogo in un secondo momento. Non è possibile aggiungere altri gruppi di risorse a un catalogo dopo la creazione del catalogo.

  Per ulteriori informazioni, vedere Gruppi di risorse di Azure.

- Nella pagina **Machine Identities** (Identità macchine), scegliere un tipo di identità e configurare le identità per le macchine in questo catalogo. Se si selezionano le macchine virtuali come aggiunte ad **Azure Active Directory**, èpossibile aggiungerle a un gruppo di sicurezza di Azure AD. I passaggi dettagliati sono i seguenti:

  1. Nel campo **Identity type** (Tipo di identità), selezionare **Azure Active Directory joined**. Viene visualizzata l'opzione **Azure AD security group (optional)** [Gruppo di sicurezza di Azure AD (opzionale)].

2. Fare clic su **Azure AD security group: Create new** (Gruppo di sicurezza Azure AD: Crea nuovo).
3. Inserire un nome per il gruppo, quindi fare clic su **Create**.
4. Seguire le istruzioni sullo schermo per accedere ad Azure.
   Se il nome del gruppo non esiste in Azure, viene visualizzata un'icona verde. In caso contrario, viene visualizzato un messaggio di errore che richiede di inserire un nuovo nome.
5. Inserire lo schema di denominazione degli account macchina per le macchine virtuali.

Dopo la creazione del catalogo, Citrix Virtual Apps and Desktops accede ad Azure per conto dell'utente e crea il gruppo di sicurezza e una regola di appartenenza dinamica per il gruppo. In base alla regola, le macchine virtuali con lo schema di denominazione specificato in questo catalogo vengono aggiunte automaticamente al gruppo di sicurezza.

L'aggiunta di macchine virtuali con uno schema di denominazione diverso a questo catalogo richiede l'accesso ad Azure. Citrix Virtual Apps and Desktops può quindi accedere ad Azure e creare una regola di appartenenza dinamica basata sul nuovo schema di denominazione.

Quando si elimina questo catalogo, l'eliminazione del gruppo di sicurezza da Azure richiede anche l'accesso ad Azure.

- Le pagine **Domain Credentials** (Credenziali di dominio) e **Summary** (Riepilogo) non contengono informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.

Completare la procedura guidata.

Condizioni perché il disco temporaneo di Azure sia idoneo per il disco della cache write-back

È possibile utilizzare il disco temporaneo di Azure come disco della cache write-back solo se vengono soddisfatte tutte le seguenti condizioni:

- Il disco della cache write-back non deve persistere poiché il disco temporaneo di Azure non è appropriato per i dati persistenti.
- La dimensione della macchina virtuale di Azure scelta deve includere un disco temporaneo.
- Non è necessario abilitare il disco del sistema operativo temporaneo.
- Accettare di inserire il file della cache write-back sul disco temporaneo di Azure.
- La dimensione temporanea del disco di Azure deve essere maggiore della dimensione totale di (dimensione del disco della cache write-back + spazio riservato per il file di paging + 1 GB di spazio buffer).

Scenari relativi al disco della cache write-back non persistente

La tabella seguente descrive tre diversi scenari in cui il disco temporaneo viene utilizzato per la cache write-back durante la creazione del catalogo delle macchine.

Scenario	Risultato
Tutte le condizioni per utilizzare il disco temporaneo per la cache write-back sono soddisfatte.	Il file WBC `mcsdif.vhdx` viene inserito nel disco temporaneo.
Lo spazio sul disco temporaneo non è sufficiente per l'utilizzo della cache write-back.	Viene creato un disco VHD `MCSWCDisk` e il file WBC `mcsdif.vhdx` viene inserito su questo disco.
Il disco temporaneo ha spazio sufficiente per l'utilizzo della cache write-back, ma `UseTempDiskForWBC` è impostato su **false**.	Viene creato un disco VHD `MCSWCDisk` e il file WBC `mcsdif.vhdx` viene inserito su questo disco.

Creare una specifica del modello di Azure

È possibile creare una specifica del modello di Azure nel portale di Azure e utilizzarla in Web Studio e nei comandi PowerShell per creare o aggiornare un catalogo di macchine MCS.

Per creare una specifica del modello di Azure per una macchina virtuale esistente:

1. Andare al portale di Azure. Selezionare un gruppo di risorse, quindi selezionare la macchina virtuale e l'interfaccia di rete. Nel menu **...** in alto, fare clic su **Export template** (Esporta modello).
2. Deselezionare la casella di controllo **Include parameters** (Includi parametri) se si desidera creare una specifica del modello di provisioning del catalogo.
3. Fare clic su **Add to library** (Aggiungi alla libreria) per modificare le specifiche del modello in un secondo momento.
4. Nella pagina **Importing template** (Modello di importazione), inserire le informazioni richieste: **Name** (nome), **Subscription** (abbonamento), **Resource Group** (Gruppo di risorse), **Location** (Posizione) e **Version** (Versione). Fare clic su **Next: Edit Template** (Avanti: Modifica modello).
5. È inoltre necessaria un'interfaccia di rete come risorsa indipendente se si desidera effettuare il provisioning di cataloghi. Pertanto, è necessario rimuovere qualsiasi elemento `dependsOn` specificato nelle specifiche del modello. Ad esempio:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
```


6. Creare **Review+Create** (Rivedi+Crea) e le specifiche del modello.
7. Nella pagina **Template Specs** (Specifiche del modello), verificare le specifiche del modello appena creato. Fare clic sulle specifiche del modello. Nel pannello di sinistra, fare clic su **Versions** (Versioni).
8. È possibile creare una nuova versione facendo clic su **Create new version** (Crea nuova versione). Specificare un nuovo numero di versione, apportare le necessarie modifiche alle specifiche del modello corrente e fare clic su **Review + Create** per creare la nuova versione della specifica del modello.

È possibile ottenere informazioni sulle specifiche del modello e sulla versione del modello utilizzando i seguenti comandi PowerShell:

- Per ottenere informazioni sulle specifiche del modello, eseguire:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
```

- Per ottenere informazioni sulla versione delle specifiche del modello, eseguire:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
```

Utilizzare le specifiche del modello per creare o aggiornare un catalogo

È possibile creare o aggiornare un catalogo di macchine MCS utilizzando una specifica di modello come input del profilo della macchina. A tale scopo, è possibile utilizzare i comandi Web Studio o PowerShell.

- Per Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio
- Per PowerShell, vedere Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell

Crittografia lato server di Azure

Citrix Virtual Apps and Desktops supporta le chiavi di crittografia gestite dal cliente per i dischi gestiti di Azure tramite Azure Key Vault. Con questo supporto è possibile gestire i requisiti organizzativi e di conformità crittografando i dischi gestiti del catalogo delle macchine utilizzando la propria chiave di crittografia. Per ulteriori informazioni, vedere Crittografia lato server dell'archiviazione su disco di Azure.

Quando si utilizza questa funzionalità per i dischi gestiti:

- Per cambiare la chiave con cui è crittografato il disco, è necessario modificare la chiave corrente in `DiskEncryptionSet`. Tutte le risorse associate a tale modifica `DiskEncryptionSet` devono essere crittografate con la nuova chiave.
- Quando si disabilita o si elimina la chiave, tutte le macchine virtuali con dischi che utilizzano tale chiave si spengono automaticamente. Dopo lo spegnimento, le macchine virtuali non sono utilizzabili a meno che la chiave non venga nuovamente abilitata o non venga assegnata una nuova chiave. Qualsiasi catalogo che utilizza la chiave non può essere acceso e non è possibile aggiungervi macchine virtuali.

Considerazioni importanti quando si utilizzano chiavi di crittografia gestite dal cliente

Quando si utilizza questa funzionalità, tenere presente quanto segue:

- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono risiedere nella stessa sottoscrizione e area geografica.
- Dopo aver abilitato la chiave di crittografia gestita dal cliente, non è possibile disabilitarla in un secondo momento. Se si desidera disabilitare o rimuovere la chiave di crittografia gestita dal cliente, copiare tutti i dati su un disco gestito diverso che non utilizza la chiave di crittografia gestita dal cliente.
- I dischi creati da immagini personalizzate crittografate utilizzando la crittografia lato server e le chiavi gestite dal cliente devono essere crittografati utilizzando le stesse chiavi gestite dal cliente. Questi dischi devono trovarsi nella stessa sottoscrizione.
- Le snapshot create da dischi crittografati con crittografia lato server e chiavi gestite dal cliente devono essere crittografate con le stesse chiavi gestite dal cliente.
- I dischi, le snapshot e le immagini crittografati con chiavi gestite dal cliente non possono passare a un altro gruppo di risorse e a un'altra sottoscrizione.
- I dischi gestiti attualmente o precedentemente crittografati utilizzando Crittografia dischi di Azure non possono essere crittografati utilizzando chiavi gestite dal cliente.
- Fare riferimento al sito Microsoft per le limitazioni sui set di crittografia dei dischi per ciascuna regione.

> **Nota:**
>
> Per informazioni sulla configurazione della crittografia lato server di Azure, vedere Guida rapida: creare un insieme di credenziali delle chiavi utilizzando il portale di Azure.

Chiave di crittografia gestita dal cliente di Azure

Quando si crea un catalogo delle macchine, è possibile scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Un set di crittografia dei dischi (DES, Disk Encryption Set) rappresenta una chiave gestita dal cliente. Per utilizzare questa funzionalità, è necessario prima creare il DES in Azure. Un DES ha il formato seguente:

- /subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption

Selezionare un DES dall'elenco. Il DES selezionato deve essere nella stessa sottoscrizione e nella stessa regione delle risorse. Se l'immagine è crittografata con un DES, utilizzare lo stesso DES durante la creazione del catalogo delle macchine. Non è possibile modificare il DES dopo aver creato il catalogo.

Se si crea un catalogo con una chiave di crittografia e successivamente si disabilita il DES corrispondente in Azure, non si potrà più accendere alle macchine nel catalogo o aggiungervi macchine.

Vedere Creare un catalogo di macchine con chiave gestita dal cliente.

Crittografia del disco di Azure sull'host

È possibile creare un catalogo di macchine MCS con crittografia in modalità host. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità. È possibile utilizzare una VM o specifiche di modello come input per il profilo di una macchina.

Questo metodo di crittografia non crittografa i dati tramite l'archiviazione di Azure. Il server che ospita la macchina virtuale crittografa i dati e quindi i dati crittografati fluiscono attraverso il server di archiviazione di Azure. Quindi, questo metodo di crittografia crittografa i dati per tutto il loro percorso dall'inizio alla fine.

Restrizioni:

La crittografia del disco di Azure sull'host è:

- non supportata per tutte le dimensioni delle macchine di Azure
- incompatibile con la crittografia del disco di Azure

Per creare un catalogo di macchine con funzionalità di crittografia sull'host:

1. Verificare se l'abbonamento ha la funzionalità di crittografia sull'host abilitata o meno. A questo scopo, vedere https://learn.microsoft.com/en-us/rest/api/resources/features/get?tab

s=HTTP/. Se non è abilitata, è necessario abilitarla per l'abbonamento. Per informazioni sull'attivazione della funzionalità per l'abbonamento, vedere https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.

2. Verificare se una particolare dimensione di macchina virtuale di Azure supporta o meno la crittografia sull'host. A questo scopo, in una finestra di PowerShell, eseguire uno dei seguenti comandi:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
```

3. Creare una macchina virtuale o specifiche di modello come input per il profilo della macchina nel portale di Azure con la crittografia sull'host abilitata.

   - Se si desidera creare una macchina virtuale, selezionare una dimensione di macchina virtuale che supporti la crittografia sull'host. Dopo aver creato la macchina virtuale, viene abilitata la relativa proprietà **Encryption at host** (Crittografia sull'host).
   - Se si desidera utilizzare specifiche di modello, assegnare al parametro `Encryption at Host` il valore **true** all'interno di `securityProfile`.

4. Creare un catalogo di macchine MCS con il flusso di lavoro dei profili delle macchine, selezionando una VM o specifiche di modello.

   - Disco del sistema operativo/disco dati: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma
   - Disco del sistema operativo temporaneo: viene crittografato solo tramite chiave gestita dalla piattaforma
   - Disco cache: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma

   È possibile creare il catalogo delle macchine utilizzando Web Studio o eseguendo i comandi PowerShell.

Recuperare la crittografia delle informazioni sull'host da un profilo di macchina

È possibile recuperare le informazioni sulla crittografia sull'host da un profilo di macchina quando si esegue il comando PowerShell con il parametro `AdditionalData`. Se il parametro `EncryptionAtHost` è **True**, significa che la crittografia sull'host è abilitata per il profilo macchina.

Ad esempio: quando l'input del profilo macchina è una VM, eseguire il seguente comando:


```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def.vm).AdditionalData
```

Ad esempio: quando l'input del profilo macchina è una specifica di modello, eseguire il seguente comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
   templatespecversion).AdditionalData
```

Doppia crittografia su disco gestito

È possibile creare un catalogo di macchine con doppia crittografia. In tutti i cataloghi creati con questa funzionalità tutti i dischi lato server sono crittografati con chiavi gestite dalla piattaforma e dal cliente. L'utente possiede e gestisce Azure Key Vault, Encryption Key e Disk Encryption Sets (DES).

La doppia crittografia è la crittografia lato piattaforma (impostazione predefinita) e la crittografia gestita dal cliente (CMEK). Pertanto, se si è un cliente altamente sensibile alla sicurezza e si nutre preoccupazione per il rischio associato a qualsiasi algoritmo di crittografia, implementazione o chiave compromessa, è possibile optare per questa doppia crittografia. Il sistema operativo persistente e i dischi di dati, le snapshot e le immagini sono tutti crittografati quando inattivi con doppia crittografia.

> **Nota:**
>
> - È possibile creare e aggiornare un catalogo di macchine con doppia crittografia utilizzando Web Studio e i comandi PowerShell. Per i comandi di PowerShell vedere Creare un catalogo di macchine con doppia crittografia.
> - È possibile utilizzare un flusso di lavoro non basato su profili macchina o un flusso di lavoro basato sul profilo macchina per creare o aggiornare un catalogo di macchine con doppia crittografia.
> - Se si utilizza un flusso di lavoro non basato su profili di macchina per creare un catalogo di macchine, è possibile riutilizzare il valore `DiskEncryptionSetId` archiviato.
> - Se si utilizza un profilo macchina, è possibile utilizzare una VM o un specifica di modello come input per il profilo della macchina.

Limitazioni:

- La doppia crittografia non è supportata per i dischi Ultra Disks o Premium SSD v2.
- La doppia crittografia non è supportata sui dischi non gestiti.
- Se si disattiva una chiave del DiskEncryptionSet associata a un catalogo, le VM del catalogo vengono disattivate.

- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono essere nella stessa sottoscrizione e area geografica.
- È possibile creare solo fino a 50 set di crittografia del disco per regione per abbonamento.
- Non è possibile aggiornare un catalogo macchine che ha già `DiskEncryptionSetId` con un `DiskEncryptionSetId` diverso.

Gruppi di risorse di Azure

I gruppi di risorse di provisioning di Azure offrono un modo per eseguire il provisioning delle macchine virtuali che forniscono applicazioni e desktop agli utenti. È possibile aggiungere gruppi di risorse di Azure vuoti esistenti quando si crea un catalogo delle macchine MCS o quando vengono creati nuovi gruppi di risorse per conto dell'utente. Per informazioni sui gruppi di risorse di Azure, consultare la documentazione Microsoft.

Utilizzo dei gruppi di risorse di Azure

Non ci sono limiti al numero di macchine virtuali, dischi gestiti, snapshot e immagini per ciascun gruppo di risorse di Azure (il limite di 240 macchine virtuali per 800 dischi gestiti per ciascun gruppo di risorse di Azure è stato rimosso).

- Quando si utilizza un'entità servizio con ambito completo per creare un catalogo delle macchine, MCS crea un solo gruppo di risorse di Azure e utilizza tale gruppo per il catalogo.
- Quando si utilizza un'entità servizio con ambito limitato per creare un catalogo delle macchine, è necessario fornire un gruppo di risorse di Azure vuoto e pre-creato per il catalogo.

Dischi temporanei di Azure

Un disco temporaneo di Azure consente di riutilizzare il disco della cache o il disco temporaneo per archiviare il disco del sistema operativo per una macchina virtuale abilitata per Azure. Questa funzionalità è utile per gli ambienti Azure che richiedono un disco SSD a prestazioni più elevate rispetto a un disco rigido standard. Per informazioni su come creare un catalogo con un disco effimero di Azure, vedere Creare un catalogo con dischi effimeri di Azure.

> **Nota:**
>
> I cataloghi persistenti non supportano i dischi del sistema operativo temporanei.

I dischi del sistema operativo temporanei richiedono che lo schema di provisioning utilizzi dischi gestiti e una Raccolta immagini condivise.

Memorizzazione di un disco del sistema operativo temporaneo

È possibile memorizzare un disco del sistema operativo temporaneo sul disco temporaneo della macchina virtuale o su un disco di risorse. Questa funzionalità consente di utilizzare un disco del sistema operativo temporaneo con una macchina virtuale che non ha una cache o ha una cache insufficiente. Tali macchine virtuali dispongono di un disco temporaneo o di risorse per archiviare un disco del sistema operativo temporaneo, ad esempio `Ddv4`.

Considerare quanto segue:

- Un disco temporaneo viene memorizzato nel disco della cache della macchina virtuale o nel disco temporaneo (risorsa) della macchina virtuale. Il disco della cache è preferibile rispetto al disco temporaneo, a meno che il disco della cache non sia abbastanza grande da ospitare i contenuti del disco del sistema operativo.
- Per gli aggiornamenti, una nuova immagine più grande del disco della cache ma più piccola del disco temporaneo comporta la sostituzione del disco del sistema operativo temporaneo con il disco temporaneo della macchina virtuale.

Ottimizzazione dell'archiviazione di dischi temporanei di Azure e Machine Creation Services (MCS) (I/O MCS)

Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.

Le considerazioni importanti sono le seguenti:

- Non è possibile creare un catalogo delle macchine con il disco del sistema operativo temporaneo e l'I/O MCS abilitati contemporaneamente.
- I parametri PowerShell (`UseWriteBackCache` e `UseEphemeralOsDisk`) non hanno effetto e restituiscono un vero e proprio messaggio di errore se vengono impostati su **true** in `New-ProvScheme` o `Set-ProvScheme`.
- Per i cataloghi delle macchine esistenti creati con entrambe le funzionalità abilitate, è comunque possibile:
  - aggiornare un catalogo delle macchine
  - aggiungere o eliminare macchine virtuali
  - eliminare un catalogo delle macchine

Raccolta di calcolo di Azure

Utilizzare la Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise di Azure) come repository di immagini pubblicate per macchine di cui è stato eseguito il provisioning con MCS in

Azure. È possibile archiviare un'immagine pubblicata nella raccolta per accelerare la creazione e l'attivazione dei dischi del sistema operativo, migliorando i tempi di avvio del sistema e delle applicazioni per le macchine virtuali non persistenti. La Raccolta immagini condivise contiene i tre elementi seguenti:

- *Galleria*: le immagini vengono archiviate qui. MCS crea una raccolta per ogni catalogo delle macchine.
- *Gallery Image Definition* (Definizione dell'immagine in galleria): questa definizione include informazioni (tipo e stato del sistema operativo, regione di Azure) sull'immagine pubblicata. MCS crea una definizione di immagine per ogni immagine creata per il catalogo.
- *Gallery Image Version* (Versione immagine in galleria): ciascuna immagine di una Raccolta immagini condivise può avere più versioni e ogni versione può avere più repliche in regioni diverse. Ogni replica è una copia completa dell'immagine pubblicata.

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

Per altre informazioni, vedere Archiviare e condividere immagini in una raccolta di calcolo di Azure.

Per informazioni sulla creazione o l'aggiornamento di un catalogo di macchine utilizzando l'immagine della Raccolta di calcolo di Azure mediante PowerShell, vedere Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure.

VM riservate di Azure

Le macchine virtuali di Azure con elaborazione riservata garantiscono che il desktop virtuale sia crittografato in memoria e protetto durante l'uso.

È possibile utilizzare MCS per creare un catalogo con macchine virtuali riservate di Azure. È necessario utilizzare il flusso di lavoro del profilo macchina per creare un catalogo di questo tipo. È possibile utilizzare una macchina virtuale e una specifica di modello ARM come input del profilo macchina.

Considerazioni importanti per le macchine virtuali riservate

Le considerazioni importanti relative alle dimensioni delle macchine virtuali supportate e alla creazione di un catalogo di macchine con macchine virtuali riservate sono le seguenti:

- Dimensioni di VM supportate: le VM riservate supportano le seguenti dimensioni di VM:
  - DCasv5-series
  - DCadsv5-series

  - ECasv5-series
  - ECadsv5-series

- Creare cataloghi di macchine con macchine virtuali riservate.
  - È possibile creare un catalogo di macchine con VM riservate Azure utilizzando Web Studio e i comandi PowerShell.
  - È necessario utilizzare un flusso di lavoro basato sul profilo macchina per creare un catalogo di macchine virtuali riservate di Azure. È possibile utilizzare una macchina virtuale e una specifica di modello come input del profilo macchina.
  - L'immagine master e l'input del profilo macchina devono essere entrambi abilitati con lo stesso tipo di sicurezza riservato. I tipi di sicurezza sono:
    - **VMGuestStateOnly**: VM riservata con solo lo stato di ospite della VM crittografato
    - **DiskWithVMGuestState**: VM riservata con disco del sistema operativo e stato di ospite della VM crittografati con chiave gestita dalla piattaforma o chiave gestita dal cliente. È possibile crittografare sia il disco del sistema operativo normale che quello temporaneo.
  - È possibile ottenere informazioni sulle VM riservate di vari tipi di risorse quali disco gestito, snapshot, immagine di Azure Compute Gallery, VM e specifiche di modello ARM utilizzando il parametro AdditionalData. Ad esempio:

    ```
    PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
        \image.folder\username-dev-testing-rg.resourcegroup\
        username-dev-tsvda.vm).AdditionalData
    ```

    I campi dati aggiuntivi sono:
    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

    Per ottenere la proprietà di riservatezza delle dimensioni di una macchina, eseguire il comando seguente: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

    Il campo dati aggiuntivo è `ConfidentialComputingType`.
  - Non è possibile modificare l'immagine master o il profilo macchina passando dal tipo di protezione riservato a quello non riservato o dal tipo di protezione non riservato a quello riservato.
  - Vengono visualizzati i messaggi di errore appropriati per eventuali configurazioni errate.

Preparare immagini master e profili macchina

Prima di creare un set di VM riservate, preparare un'immagine master e un profilo macchina per esse seguendo questi passaggi:

1. Nel portale di Azure, creare una macchina virtuale riservata con impostazioni specifiche, ad esempio:

   - **Security Type** (Tipo di sicurezza): macchine virtuali riservate
   - **Confidential OS disk encryption** (Crittografia riservata del disco del sistema operativo): abilitata.
   - **Key management** (Gestione delle chiavi): crittografia riservata del disco con una chiave gestita dalla piattaforma
     Per ulteriori informazioni sulla creazione di macchine virtuali riservate, vedere questo articolo Microsoft.

2. Preparare l'immagine master sulla VM creata. Installare le applicazioni e il VDA necessari sulla VM creata.

   > **Nota:**
   >
   > La creazione di VM riservate utilizzando VHD non è supportata. Utilizzare invece Azure Compute Gallery, i dischi gestiti o le istantanee per questo scopo.

3. Creare il profilo della macchina in uno dei seguenti modi:

   - Utilizzare la VM esistente creata nel passaggio 1 se possiede le proprietà macchina necessarie.
   - Se si opta per una specifica del modello ARM come profilo macchina, creare la specifica del modello secondo necessità. In particolare, configurare i parametri che soddisfano i requisiti della VM riservata, come *SecurityEncryptionType* e *diskEncryptionSet* (per la chiave gestita dal cliente). Per ulteriori informazioni, vedere Creare una specifica del modello di Azure.

     > **Nota:**
     >
     > - Assicurarsi che l'immagine master e il profilo della macchina abbiano lo stesso tipo di chiave di sicurezza.
     > - Per creare macchine virtuali riservate che richiedono la crittografia riservata del disco del sistema operativo con una chiave gestita dal cliente, assicurarsi che gli ID del set di crittografia del disco nell'immagine master e nel profilo della macchina siano identici.

Creare macchine virtuali riservate utilizzando Web Studio o i comandi PowerShell

Per creare un set di VM riservate, creare un catalogo di macchine utilizzando un'immagine master e un profilo macchina derivati dalla VM riservata desiderata.

Per creare il catalogo utilizzando Web Studio, seguire i passaggi descritti in Creare cataloghi di macchine. Tenere presenti le seguenti considerazioni:

- Nella pagina **Image** selezionare un'immagine master e un profilo macchina preparati per la creazione riservata della VM. La selezione del profilo macchina è obbligatoria e solo i profili che corrispondono allo stesso tipo di crittografia di sicurezza dell'immagine master selezionata sono disponibili per la selezione.
- Nella pagina **diskEncryptionSet** vengono selezionate solo le dimensioni delle macchine che supportano le VM riservate.
- Nella pagina **Disk Settings** (Impostazioni disco) non è possibile specificare il set di crittografia del disco perché questo è ereditato dal profilo del computer selezionato.

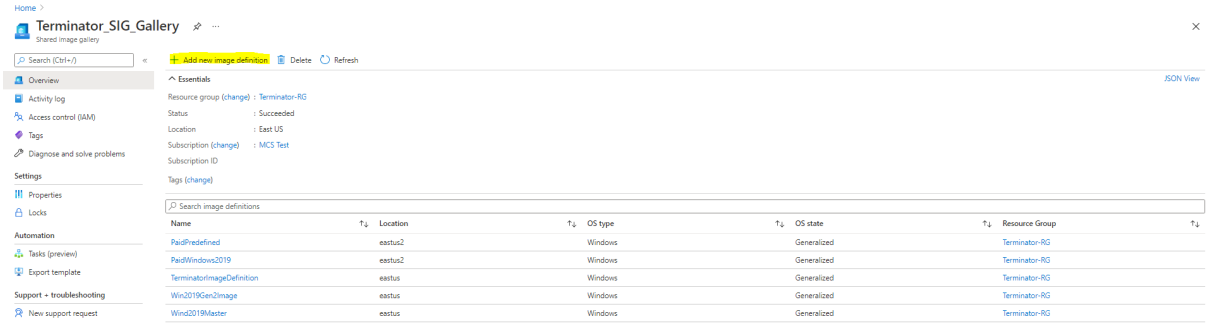
Azure Marketplace

Citrix Virtual Apps and Desktops supporta l'utilizzo di un'immagine master in Azure che contiene informazioni sul piano per creare un catalogo delle macchine. Per ulteriori informazioni, vedere Microsoft Azure Marketplace.

> **Suggerimento:**
>
> Alcune immagini che si trovano in Azure Marketplace, come l'immagine standard di Windows Server, non aggiungono informazioni sul piano. La funzionalità di Citrix Virtual Apps and Desktops è dedicata alle immagini a pagamento.

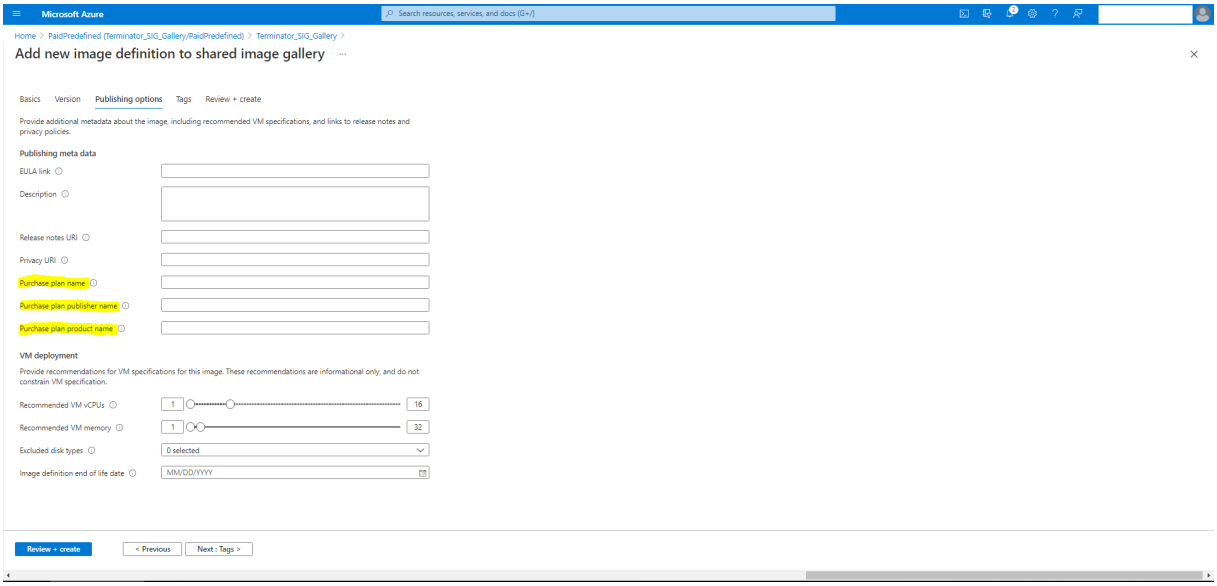
Assicurarsi che l'immagine creata nella Raccolta immagini condivise contenga informazioni sul piano di Azure

Utilizzare la procedura descritta in questa sezione per visualizzare le immagini della Raccolta immagini condivise in Web Studio. Facoltativamente, queste immagini possono essere utilizzate per un'immagine master. Per inserire l'immagine in una Raccolta immagini condivise, creare una definizione di immagine in una raccolta.

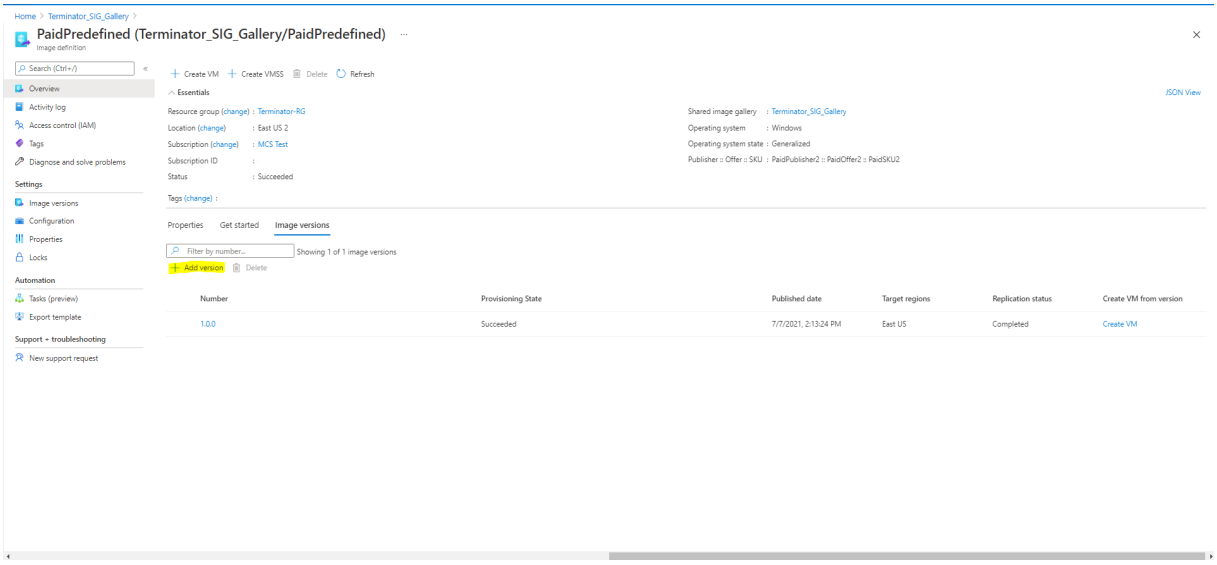


Nella pagina **Publishing options** (Opzioni di pubblicazione), verificare le informazioni sul piano di acquisto.

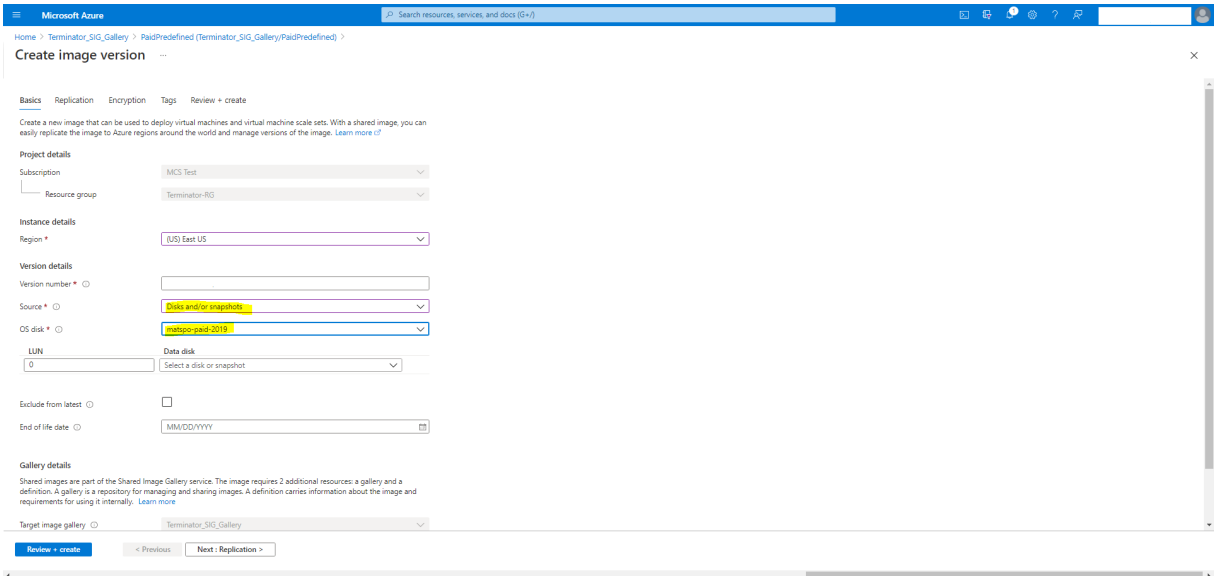
I campi relativi alle informazioni sul piano di acquisto sono inizialmente vuoti. Compilare questi campi con le informazioni sul piano di acquisto utilizzate per l'immagine. La mancata compilazione delle informazioni sul piano di acquisto può causare la mancata riuscita del processo del catalogo delle macchine.



Dopo aver verificato le informazioni sul piano di acquisto, creare una versione immagine all'interno della definizione. Viene utilizzata come immagine master. Fare clic su **Add version** (Aggiungi versione):



Nella sezione **Version details** (Dettagli versione), selezionare la snapshot dell'immagine o il disco gestito come origine:



Creare un catalogo di macchine usando PowerShell

Questa sezione descrive in dettaglio come creare cataloghi usando PowerShell:

- Creare un catalogo con un disco cache di write-back non persistente
- Creare un catalogo con un disco cache di write-back persistente
- Migliorare le prestazioni di avvio con MCSIO
- Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell
- Cataloghi di macchine con avvio attendibile
- Utilizzare i valori delle proprietà del profilo macchina

- Creare un catalogo di macchine con chiave di crittografia gestita dal cliente
- Creare un catalogo di macchine con doppia crittografia
- Creare un catalogo con dischi effimeri di Azure
- Host dedicati di Azure
- Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure
- Configurare la Raccolta immagini condivise
- Eseguire il provisioning delle macchine in zone di disponibilità specificate
- Tipologie di archiviazione
- Posizione del file di paging
- Aggiornare le impostazioni del file di paging
- Creare un catalogo usando le macchine virtuali Azure Spot
- Configurare le dimensioni delle VM di backup
- Copiare i tag su tutte le risorse
- Eseguire il provisioning delle macchine virtuali del catalogo con Azure Monitor Agent installato

Creare un catalogo con un disco cache di write-back non persistente

Per configurare un catalogo con il disco della cache write-back non persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. La proprietà personalizzata `UseTempDiskForWBC` indica se si sta accettando di utilizzare l'archiviazione temporanea di Azure per archiviare il file della cache write-back. Questo deve essere configurato su true durante l'esecuzione di `New-ProvScheme` se si desidera utilizzare il disco temporaneo come disco della cache write-back. Se questa proprietà non viene specificata, il parametro è impostato su **False** per impostazione predefinita.

Ad esempio, utilizzando il parametro `CustomProperties` per impostare `UseTempDiskForWBC` su **true**:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
   true"/> `
</CustomProperties>'
```


> **Nota:**
>
> Dopo aver eseguito il commit del catalogo delle macchine per l'utilizzo dell'archiviazione temporanea locale di Azure per il file della cache write-back, non può essere modificato per utilizzare l'unità disco rigido virtuale in un secondo momento.

Creare un catalogo con un disco cache di write-back persistente

Per configurare un catalogo con il disco della cache write-back persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. Questo parametro supporta una proprietà aggiuntiva, `PersistWBC`, utilizzata per determinare il modo in cui il disco della cache write-back persiste per le macchine di cui è stato eseguito il provisioning con MCS. La proprietà `PersistWBC` viene utilizzata solo quando viene specificato il parametro`UseWriteBackCache` e quando il parametro `WriteBackCacheDiskSize` è impostato per indicare che viene creato un disco.

Esempi di proprietà trovate nel parametro `CustomProperties` prima del supporto `PersistWBC` sono:

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

Quando si utilizzano queste proprietà, considerare che contengono valori predefiniti se le proprietà vengono omesse dal parametro `CustomProperties`. La proprietà `PersistWBC` ha due valori possibili: **true** o **false**.

L'impostazione della proprietà `PersistWBC` su **true** non elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops spegne la macchina utilizzando Web Studio.

L'impostazione della proprietà `PersistWBC` **su false** elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops arresta la macchina utilizzando Web Studio.

> **Nota:**
>
> Se la proprietà `PersistWBC` viene omessa, sarà **false** per impostazione predefinita e la cache write-back viene eliminata quando il computer viene arrestato utilizzando Web Studio.

Ad esempio, utilizzando il parametro `CustomProperties` per impostare `PersistWBC` su true:

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

> **Importante:**
>
> La proprietà `PersistWBC` può essere impostata solo utilizzando il cmdlet PowerShell `New-ProvScheme`. Il tentativo di modificare le `CustomProperties` di uno schema di provisioning dopo la creazione non ha alcun impatto sul catalogo macchine e sulla persistenza del disco della cache write-back quando un computer viene arrestato.

Ad esempio, impostare `New-ProvScheme` perché utilizzi la cache write-back mentre si imposta la proprietà `PersistWBC` su true:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```


Migliorare le prestazioni di avvio con MCSIO

È possibile migliorare le prestazioni di avvio per i dischi gestiti di Azure e GCP quando MCSIO è abilitato. Utilizzare la proprietà personalizzata di PowerShell `PersistOSDisk` nel comando `New-ProvScheme` per configurare questa funzionalità. Le opzioni associate a `New-ProvScheme` includono:

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

Per abilitare questa funzionalità, impostare la proprietà personalizzata `PersistOSDisk` su **`true`**. Ad esempio:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```


```

### Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell

È possibile creare o aggiornare un catalogo di macchine MCS utilizzando una specifica di modello come input del profilo della macchina. A tale scopo, è possibile utilizzare i comandi Web Studio o PowerShell.

Per Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio

Utilizzare i comandi PowerShell:

1. Aprire una finestra di **PowerShell**.
2. Eseguire `asnp citrix*`.
3. Creare o aggiornare un catalogo.

    - Per creare un catalogo:

        a) Utilizzare il comando `New-ProvScheme` con una specifica del modello come input per il profilo macchina. Ad esempio:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
    image.folder/fgthj.resourcegroup/nab-ws-
    vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>
[-LoggingId <Guid>]
[-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

        b) Completare la creazione del catalogo di macchine.

    - Per aggiornare un catalogo, utilizzare il comando `Set-ProvScheme` con una specifica di modello come input del profilo macchina. Ad esempio:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
    Us.region/vm.folder/MasterDisk.vm'
MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/testing.templatespec/V1.
    templatespecversion'
[-ProvisioningSchemeName] <String>
[-CustomProperties <String>][-ServiceOffering <String>] [-
    PassThru]
[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
    String>] [<CommonParameters>]
```


Cataloghi di macchine con avvio attendibile

Per creare correttamente un catalogo di macchine con avvio attendibile, utilizzare:

- Un profilo macchina con avvio attendibile
- Una dimensione di macchina virtuale che supporti l'avvio attendibile
- Una versione di macchina virtuale Windows che supporti l'avvio attendibile. Attualmente, Windows 10, Windows 11, Windows Server 2016, 2019 e 2022 supportano l'avvio attendibile.

> **Importante:**
>
> MCS supporta la creazione di un nuovo catalogo con macchine virtuali abilitate per l'avvio attendibile. Tuttavia, per aggiornare un catalogo persistente esistente e le macchine virtuali esistenti, è necessario utilizzare il portale di Azure. Non è possibile aggiornare l'avvio attendibile di un catalogo non persistente. Per ulteriori informazioni, vedere il documento Microsoft Abilitare l'avvio attendibile nelle macchine virtuali di Azure esistenti.

Per visualizzare gli elementi di inventario offerti da Citrix Virtual Apps and Desktops e determinare se le dimensioni della macchina virtuale supportano l'avvio attendibile, eseguire il seguente comando:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il seguente comando:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
```

4. Eseguire `$s | select -ExpandProperty Additionaldata`
5. Controllare il valore dell'attributo `SupportsTrustedLaunch`.
    - Se `SupportsTrustedLaunch` è **True**, la dimensione della macchina virtuale supporta l'avvio attendibile.
    - Se `SupportsTrustedLaunch` è **False**, la dimensione della macchina virtuale non supporta l'avvio attendibile.

Come da PowerShell di Azure, è possibile usare il seguente comando per determinare le dimensioni di macchina virtuale che supportano l'avvio attendibile:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
```

Di seguito sono riportati alcuni esempi che descrivono se la dimensione della macchina virtuale supporta l'avvio attendibile dopo l'esecuzione del comando Azure PowerShell.

- *Esempio 1*: se la macchina virtuale di Azure supporta solo la generazione 1, quella macchina virtuale non supporta l'avvio attendibile. Pertanto, la funzionalità `TrustedLaunchDisabled` non viene visualizzata dopo l'esecuzione del comando Azure PowerShell.
- *Esempio 2*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità`TrustedLaunchDisabled` è **True**, la dimensione della macchina virtuale di generazione 2 non è supportata per l'avvio attendibile.
- *Esempio 3*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità `TrustedLaunchDisabled` non viene visualizzata dopo l'esecuzione del comando PowerShell, la dimensione della VM di generazione 2 è supportata per l'avvio attendibile.

Per ulteriori informazioni sull'avvio attendibile per le macchine virtuali Azure, vedere il documento Microsoft Avvio attendibile per le macchine virtuali di Azure.

Creare un catalogo di macchine con l'avvio attendibile

1. Creare un'immagine master abilitata con l'avvio attendibile. Vedere la documentazione Microsoft Immagini di macchine virtuali ad avvio attendibile.
2. Creare una VM o una specifica di modello con il tipo di sicurezza impostato su **macchine virtuali con avvio attendibile**. Per ulteriori informazioni sulla creazione di una VM o di una specifica di modello, vedere il documento Microsoft Distribuire una macchina virtuale con avvio attendibile.
3. Creare un catalogo di macchine utilizzando Web Studio o i comandi PowerShell.

    - Se si desidera utilizzare Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio.
    - Se si desidera utilizzare i comandi PowerShell, utilizzare il comando `New-ProvScheme` con la VM o la specifica del modello come input del profilo macchina. Per l'elenco completo dei comandi per creare un catalogo, vedere Creare un catalogo.

      Esempio di `New-ProvScheme` con la VM come input del profilo macchina:

      ```
      New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
          IdentityPoolName "name" -InitialBatchSizeHint 1
      -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
          resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
      -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
          folder<def.resourcegroup><machine profile vm.vm>"
      -ProvisioningSchemeName <String>
      -HostingUnitName <String>
      -IdentityPoolName <String>
      [-ServiceOffering <String>][-CustomProperties <String>]
      [<CommonParameters>]
      ```

      Esempio di `New-ProvScheme` con le specifiche del modello come input del profilo macchina:


```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
```

Errori nella creazione di cataloghi di macchine con avvio attendibile

Si ottengono errori appropriati nei seguenti scenari durante la creazione di un catalogo di macchine con avvio attendibile:

Scenario	Errore
Se si seleziona un profilo macchina durante la creazione di un catalogo non gestito	`MachineProfileNotSupportedForUnmanagedCata`
Se si seleziona un profilo macchina che supporta l'avvio attendibile durante la creazione di un catalogo con un disco non gestito come immagine master	`SecurityTypeNotSupportedForUnmanagedDisk`
Se non si seleziona il profilo macchina durante la creazione di un catalogo gestito con un' immagine master con l'avvio attendibile come tipo di sicurezza	`MachineProfileNotFoundForTrustedLaunchMaste`
Se si seleziona un profilo macchina con un tipo di sicurezza diverso dal tipo di protezione dell' immagine master	`SecurityTypeConflictBetweenMasterImageAndMa`
Se si seleziona una dimensione di macchina virtuale che non supporta l'avvio attendibile, ma utilizza un'immagine master che supporta l' avvio attendibile durante la creazione di un catalogo	`MachineSizeNotSupportTrustedLaunch`

Utilizzare i valori delle proprietà del profilo macchina

Il catalogo delle macchine utilizza le seguenti proprietà definite nelle proprietà personalizzate:

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

Se queste proprietà personalizzate non sono definite in modo esplicito, i valori delle proprietà vengono impostati in base alla specifica del modello ARM o alla macchina virtuale, a seconda di quale sia utilizzata come profilo macchina. Inoltre, se non è specificato `ServiceOffering`, questo viene impostato in base al profilo della macchina.

> **Nota:**
>
> Se alcune delle proprietà non sono presenti nel profilo macchina e non sono definite nelle proprietà personalizzate, vengono adottati i valori predefiniti delle proprietà laddove è applicabile.

La sezione seguente descrive alcuni scenari in `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` hanno tutte le proprietà definite o qando i valori sono derivati da MachineProfile.

- Scenari New-ProvScheme
  - MachineProfile ha tutte le proprietà e le CustomProperties non sono definite. Esempio:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
          machinecreation" xmlns:xsi="http://www.w3.org/2001/
          XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
           Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
          -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
          "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
          " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
          DedicatedHostGroupId" Value="<mpA-value>"/>
    ```



```
8   <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
       value>"/>
9   </CustomProperties>
```

- MachineProfile ha alcune proprietà e le CustomProperties non sono definite. Esempio: MachineProfile ha solo LicenseType e OSType.

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  ```
  1   Get-ProvScheme | select CustomProperties
  2   <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
         machinecreation" xmlns:xsi="http://www.w3.org/2001/
         XMLSchema-instance">
  3   <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
         -value>"/>
  4   <Property xsi:type="StringProperty" Name="LicenseType" Value=
         "<mpA-value>"/>
  5   </CustomProperties>
  ```

- Sia MachineProfile che CustomProperties definiscono tutte le proprietà. Esempio:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Le proprietà personalizzate hanno la priorità. I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  ```
  1   Get-ProvScheme | select CustomProperties
  2   <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
         machinecreation" xmlns:xsi="http://www.w3.org/2001/
         XMLSchema-instance">
  3   <Property xsi:type="StringProperty" Name="StorageAccountType"
          Value="<CustomPropertiesA-value>"/>
  4   <Property xsi:type="StringProperty" Name="OSType" Value="<
         CustomPropertiesA-value>"/>
  5   <Property xsi:type="StringProperty" Name="LicenseType" Value=
         "<CustomPropertiesA-value>"/>
  6   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
         " Value="<CustomPropertiesA-value>"/>
  7   <Property xsi:type="StringProperty" Name="
         DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
  8   <Property xsi:type="StringProperty" Name="Zones" Value="<
         CustomPropertiesA-value>"/>
  9   </CustomProperties>
  ```

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Esempio:

* In CustomProperties sono definite LicenseType e StorageAccountType
* In MachineProfile sono definite LicenseType, OSType e Zones

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
   -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
   value>"/>
</CustomProperties>
```

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Inoltre, ServiceOffering non è definito. Esempio:

  * In CustomProperties è definito StorageType
  * In MachineProfile è definito LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
   \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
   serviceoffering.folder<explicit-machine-size>.
   serviceoffering"
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "value-from-machineprofile"/>
</CustomProperties>
```

- Se OsType e non si trova né in CustomProperties né in MachineProfile, allora:

  * Il valore viene letto dall'immagine master.
  * Se l'immagine master è un disco non gestito, OsType è impostato su Windows. Esempio:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

Il valore dell'immagine master viene scritto nelle proprietà personalizzate, in questo caso Linux.

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="OSType" Value="
      Linux"/>
4  </CustomProperties>
```

- Scenari Set-ProvScheme
  - Un catalogo esistente con:
    * CustomProperties per `StorageAccountType` e OsType
    * MachineProfile `mpA.vm` che definisce le zone
  - Aggiornamenti:
    * MachineProfile mpB.vm che definisce StorageAccountType
    * Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce LicenseType e OsType

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6      </CustomProperties>
```


- Un catalogo esistente con:
  - CustomProperties per StorageAccountType e OsType
  - MachineProfile mpA.vm che definisce StorageAccountType e LicenseType
- Aggiornamenti:
  - Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce StorageAccountType e OsType.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mp-A-value>"/>
</CustomProperties>
```

- Un catalogo esistente con:
  - CustomProperties per StorageAccountType e OsType
  - MachineProfile mpA.vm che definisce le zone
- Aggiornamenti:
  - Un MachineProfile mpB.vm che definisce StorageAccountType e LicenseType
  - ServiceOffering non è specificato

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<value-from-machineprofile>.
   serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   prior-CustomProperties-value>"/>
```



```
8   <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpB-value>"/>
9   </CustomProperties>
```

Eseguire il provisioning delle macchine virtuali del catalogo con Azure Monitor Agent installato

Il monitoraggio di Azure è un servizio utilizzabile per raccogliere, analizzare e agire sui dati di telemetria dai propri ambienti Azure e locali.

L'agente di Monitoraggio di Azure (AMA) raccoglie i dati di monitoraggio da risorse di elaborazione come le macchine virtuali e li fornisce ad Azure Monitor. Attualmente supporta la raccolta di metriche Event Logs, Syslog e Performance e la invia alle fonti dati di Azure Monitor Metrics e Azure Monitor Logs.

Per abilitare il monitoraggio identificando in modo univoco le VM nei dati di monitoraggio, è possibile effettuare il provisioning delle VM di un catalogo di macchine MCS con AMA installato come estensione.

Requisiti

- Autorizzazioni: assicurarsi di disporre delle autorizzazioni minime di Azure come specificato in Autorizzazioni richieste per Azure e le seguenti autorizzazioni all'uso di Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Regola di raccolta dati: impostare una regola di raccolta dati nel portale di Azure. Per informazioni sulla configurazione di un DCR, vedere Creare una regola di raccolta dati. Un DCR è specifico per una piattaforma (Windows o Linux). Assicurarsi di creare un DCR corretto per la piattaforma richiesta.
  L'AMA utilizza le regole di raccolta dati (DCR) per gestire la mappatura tra le risorse, quali le macchine virtuali, e le fonti di dati, quali Azure Monitor Metrics e Azure Monitor Logs.
- Area di lavoro predefinita: creare un'area di lavoro nel portale di Azure. Per informazioni sulla creazione di un'area di lavoro, vedere Creare un'area di lavoro Log Analytics. Quando si raccolgono registri e dati, le informazioni vengono archiviate in un'area di lavoro. Un'area di lavoro ha un ID dell'area di lavoro e un ID risorsa univoci. Il nome dell'area di lavoro deve essere univoco per un determinato gruppo di risorse. Dopo aver creato un'area di lavoro, configurare le fonti di dati e le soluzioni in modo che archivino i relativi dati in essa.

- L'estensione del monitor inserita nella whitelist: le estensioni `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` sono estensioni inserite nella whitelist definite da Citrix. Per visualizzare l'elenco delle estensioni inserite nella whitelist, utilizzare il comando PoSH `Get-ProvMetadataConfiguration`.
- Immagine master: Microsoft consiglia di rimuovere le estensioni da una macchina esistente prima di crearne una nuova da essa. Se le estensioni non vengono rimosse, si potrebbero riscontrare file rimanenti e comportamenti imprevisti. Per ulteriori informazioni, vedere Se la macchina virtuale viene ricreata da una macchina virtuale esistente.

Per eseguire il provisioning delle VM del catalogo con AMA abilitato:

1. Configurare un modello di profilo macchina.
   - Se si desidera utilizzare una macchina virtuale come modello di profilo macchina:
     a) Creare una macchina virtuale nel portale di Azure.
     b) Accendere la VM.
     c) Aggiungere la VM alla regola di raccolta dati in **Resources**. Ciò richiama l'installazione dell'agente sulla macchina virtuale modello.

     > **Nota:**
     >
     > Se si deve creare un catalogo Linux, configurare una macchina Linux.

   - Se si desidera utilizzare una specifica di modello come modello di profilo macchina:
     a) Impostare una specifica di modello.
     b) Aggiungere la seguente associazione di regole di estensione e raccolta dati alla specifica di modello generata:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

```



```
}
,
{

   "type": "Microsoft.Insights/
      dataCollectionRuleAssociations",
   "apiVersion": "2021-11-01",
   "name": "<associatio-name>",
   "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
   "dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>",
   "Microsoft.Compute/virtualMachines/<vm-name>/extensions
      /AzureMonitorWindowsAgent"
   ],
   "properties": {

      "description": "Association of data collection rule.
          Deleting this association will break the data
         collection for this Arc server.",
    "dataCollectionRuleId": "/subscriptions/<azure-
       subscription>/resourcegroups/<azure-resource-group
       >/providers/microsoft.insights/datacollectionrules
       /<azure-data-collection-rule>"
     }

    }
```

2. Creare o aggiornare un catalogo di macchine MCS esistente.

   - Per creare un nuovo catalogo MCS:

     a) Selezionare la specifica della VM o del modello come profilo macchina in Web Studio.
     b) Procedere ai passaggi successivi per creare il catalogo.

   - Per aggiornare un catalogo MCS esistente, utilizzare i seguenti comandi PoSH:

     – Per fare in modo che le nuove VM ottengano il modello di profilo macchina aggiornato, eseguire il seguente comando:

     ```
     Set-ProvScheme -ProvisioningSchemeName "name"
     -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
        folder\abc.resourcegroup\ab-machine-profile.vm"
     ```

     – Per aggiornare le macchine virtuali esistenti con il modello di profilo macchina aggiornato:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
        catalog -StartsNow -DurationInMinutes -1
     ```

3. Accendere le macchine virtuali del catalogo.
4. Passare al portale di Azure e controllare se l'estensione del monitor è installata sulla macchina

virtuale e se la macchina virtuale viene visualizzata nelle risorse di DCR. Dopo alcuni minuti i dati di monitoraggio vengono visualizzati su Azure Monitor.

Risoluzione dei problemi

Per informazioni sulle linee guida alla risoluzione dei problemi per l'agente di Monitoraggio di Azure, vedere quanto segue:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Creare un catalogo di macchine con chiave di crittografia gestita dal cliente

I passaggi dettagliati per creare un catalogo di macchine con chiave di crittografia gestita dal cliente sono:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Inserire `cd xdhyp:/`.
4. Inserire `cd .\HostingUnits\(your hosting unit)`.
5. Inserire `cd diskencryptionset.folder`.
6. Immettere `dir` per ottenere l'elenco dei set di crittografia del disco.
7. Copiare l'ID di un set di crittografia del disco.
8. Creare una stringa di proprietà personalizzata che includa l'ID del set di crittografia del disco. Ad esempio:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value=`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
```



```
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
    Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
   resourceGroups/abc/providers/Microsoft.Compute/
   diskEncryptionSets/abc-des`"/>
</CustomProperties>
```

9. Creare un pool di identità se non è già stato creato. Ad esempio:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
   Domain def.local -NamingSchemeType Numeric
```

10. Eseguire il comando New-ProvScheme: Ad esempio:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
   IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
   resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
    def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
    " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
   folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
   def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
```

11. Completate la creazione del catalogo di macchine.

Creare un catalogo di macchine con doppia crittografia

È possibile creare e aggiornare un catalogo di macchine con doppia crittografia utilizzando Web Studio e i comandi PowerShell.

I passaggi dettagliati per creare un catalogo di macchine con doppia crittografia sono:

1. Creare un Azure Key Vault e DES con chiavi gestite dalla piattaforma e gestite dal cliente. Per informazioni su come creare un Azure Key Vault e un DES, vedere Usare il portale di Azure per abilitare la doppia crittografia dei dati inattivi per i dischi gestiti.
2. Per sfogliare i DiskEncryptionSet disponibili nella propria connessione di hosting:
   a) Aprire una finestra di **PowerShell**.
   b) Eseguire i seguenti comandi PowerShell:
      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`

iv. `cd YourHostingUnitName` (es. azure-east)
v. `cd diskencryptionset.folder`
vi. `dir`

È possibile utilizzare un ID del `DiskEncryptionSet` per creare o aggiornare un catalogo utilizzando proprietà personalizzate.

3. Se si desidera utilizzare il flusso di lavoro del profilo macchina, creare una VM o una specifica di modello come input per il profilo della macchina.

   - Se si desidera utilizzare una VM come input del profilo macchina:
     a) Creare una macchina virtuale nel portale di Azure.
     b) Passare a **Dischi > Gestione delle chiavi** per crittografare la VM direttamente con qualsiasi `DiskEncryptionSetID`.
   - Se si desidera utilizzare una specifica di modello come input del profilo della macchina:
     a) Nel modello, in `properties>storageProfile>osDisk>managedDisk`, aggiungere il parametro `diskEncryptionSet` e l'ID del DES a doppia crittografia.

4. Creare il catalogo di macchine.

   - Se si utilizza Web Studio, eseguire una delle seguenti operazioni oltre alla procedura descritta in Creare cataloghi di macchine.
     - Se non si utilizza un flusso di lavoro basato sul profilo macchina, nella pagina **Impostazioni disco** selezionare **Use the following key to encrypt data on each machine** (Usa la seguente chiave per crittografare i dati su ciascuna macchina). Quindi, selezionare il proprio DES a doppia crittografia dal menu a discesa. Continuare a creare il catalogo.
     - Se si utilizza il flusso di lavoro del profilo macchina, nella pagina **Image** selezionare un'immagine master e un profilo macchina. Assicurarsi che il profilo macchina abbia un ID set crittografia disco nelle sue proprietà.

     Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

   - Se si utilizlzano i comandi di PowerShell, eseguire una delle seguenti operazioni:
     - Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata `DiskEncryptionSetId` nel comando `New-ProvScheme`. Ad esempio:

```
1  New-ProvScheme -CleanOnBoot -CustomProperties '<
       CustomProperties xmlns="http://schemas.citrix.com/2014/
       xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
```



```
<Property xsi:type="StringProperty" Name="UseManagedDisks"
    Value="true" />
<Property xsi:type="StringProperty" Name="
   StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando `New-ProvScheme`. Ad esempio:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
```

5. Completare la creazione di un catalogo utilizzando l'SDK Remote PowerShell. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

Convertire un catalogo non crittografato per utilizzare la doppia crittografia

È possibile aggiornare il tipo di crittografia di un catalogo di macchine (utilizzando proprietà personalizzate o il profilo macchina) solo se il catalogo in precedenza non era crittografato.

- Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata DiskEncryptionSetId nel comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
    .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
    resourceGroups/Sample-RG/providers/Microsoft.Compute/
    diskEncryptionSets/SampleEncryptionSet" />
</CustomProperties>'
```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando `Set-ProvScheme`. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
    XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
    resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
```

Una volta completata l'operazione, tutte le nuove macchine virtuali aggiunte al catalogo vengono crittografate due volte dalla chiave associata al DES selezionato.

Verificare che il catalogo sia crittografato con doppia crittografia

- In Web Studio:
  1. Passare a **Machine Catalogs** (Cataloghi di macchine).
  2. Selezionare il catalogo da verificare. Fare clic sulla scheda **Template Properties** (Proprietà del modello) situata nella parte inferiore dello schermo.
  3. In **Azure Details** (Dettagli di Azure) verificare l'ID del set di crittografia del disco in **Disk Encryption Set**. Se l'ID DES del catalogo è vuoto, il catalogo non è crittografato.
  4. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.
- Utilizzando i comandi PowerShell:
  1. Aprire una finestra di **PowerShell**.
  2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
  3. Utilizzare `Get-ProvScheme` per ottenere le informazioni del proprio catalogo macchine. Ad esempio:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  4. Recuperare la proprietà personalizzata DES Id del catalogo di macchine. Ad esempio:


```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
     Value="/subscriptions
    /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
    -RG/providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
```

5. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.

Creare un catalogo con dischi effimeri di Azure

Per utilizzare dischi temporanei, è necessario impostare la proprietà personalizzata `UseEphemeralOsDisk` su **true** durante l'esecuzione di `New-ProvScheme`.

> **Nota:**
>
> Se la proprietà personalizzata `UseEphemeralOsDisk` è impostata su **false** o non viene specificato un valore, tutti i VDA di cui è stato eseguito il provisioning continuano a utilizzare un disco del sistema operativo di cui è stato eseguito il provisioning.

Di seguito è riportato un esempio di set di proprietà personalizzate da utilizzare nello schema di provisioning:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {
```



```
27
28                  "Name": "SharedImageGalleryReplicaMaximum",
29                  "Value": "10"
30               }
31   ,
32              {
33
34                  "Name": "LicenseType",
35                  "Value": "Windows_Server"
36               }
37   ,
38              {
39
40                  "Name": "UseEphemeralOsDisk",
41                  "Value": "true"
42               }
43
44          ],
```

Configurare un disco temporaneo per un catalogo

Per configurare un disco del sistema operativo temporaneo di Azure per un catalogo, utilizzare il parametro `UseEphemeralOsDisk` in `Set-ProvScheme`. Impostare il valore del parametro `UseEphemeralOsDisk` su **true**.

> **Nota:**
>
> Per utilizzare questa funzionalità, è necessario abilitare anche i parametri `UseManagedDisks` e `UseSharedImageGallery`.

Ad esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
     CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
     "true" />
4 <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
     true" />
5 </CustomProperties>'
```

Considerazioni importanti per i dischi temporanei

Per eseguire il provisioning di dischi del sistema operativo temporanei utilizzando `New-ProvScheme`, considerare i seguenti vincoli:

- La dimensione della macchina virtuale utilizzata per il catalogo deve supportare i dischi operativi temporanei.
- La dimensione della cache o del disco temporaneo associato alla dimensione della macchina virtuale deve essere maggiore o uguale alla dimensione del disco del sistema operativo.
- La dimensione del disco temporaneo deve essere maggiore della dimensione del disco della cache.

Tenere presenti questi problemi anche quando:

- Si crea lo schema di provisioning.
- Si modifica lo schema di provisioning.
- Si aggiorna l'immagine.

Host dedicati di Azure

È possibile utilizzare MCS per eseguire il provisioning di macchine virtuali su host dedicati di Azure. Prima di eseguire il provisioning delle macchine virtuali su host dedicati di Azure:

- Creare un gruppo host.
- Creare host nel gruppo host.
- Assicurarsi che la capacità host sia sufficiente per la creazione di cataloghi e macchine virtuali.

È possibile creare un catalogo di macchine con tenancy host definita tramite il seguente script PowerShell:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
```

Quando si utilizza MCS per eseguire il provisioning di macchine virtuali su host Azure dedicati, tenere in considerazione quanto segue:

- Un *host dedicato* è una proprietà del catalogo e non può essere modificata una volta creato il catalogo. La tenancy dedicata non è attualmente supportata in Azure.
- Quando si utilizza il parametro `HostGroupId`, è necessario un gruppo host di Azure preconfigurato nella regione dell'unità di hosting.
- È necessario il posizionamento automatico di Azure. Questa funzionalità invia una richiesta di eseguire l'onboarding della sottoscrizione associata al gruppo host. Per ulteriori informazioni, vedere Set di scalabilità VM negli host dedicati di Azure - Anteprima pubblica. Se il posizionamento automatico non è abilitato, MCS genererà un errore durante la creazione del catalogo.

Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure

Quando si seleziona un'immagine da utilizzare per la creazione di un catalogo delle macchine, è possibile selezionare le immagini create nella Raccolta di calcolo di Azure.

Per visualizzare queste immagini, è necessario:

1. Configurare un sito Citrix Virtual Apps and Desktops.
2. Connettersi ad Azure Resource Manager.
3. Nel portale di Azure, creare un gruppo di risorse. Per ulteriori informazioni, vedere Creare una raccolta per l'archiviazione e la condivisione delle risorse.
4. Nel gruppo di risorse, creare una Raccolta di calcolo di Azure.
5. Nella Raccolta di calcolo di Azure, creare una definizione di immagine.
6. Nella definizione dell'immagine, creare una versione dell'immagine.

Usa i seguenti comandi PowerShell per creare o aggiornare un catalogo di macchine utilizzando un'immagine tratta dalla Raccolta di calcolo di Azure:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
```

4. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
```

5. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
```

6. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:
   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Configurare la Raccolta immagini condivise

Utilizzare il comando `New-ProvScheme` per creare uno schema di provisioning con il supporto della Raccolta immagini condivise. Utilizzare il comando `Set-ProvScheme` per abilitare o disabilitare questa funzionalità per uno schema di provisioning e per modificare il rapporto di replica e i valori massimi della replica.

Sono state aggiunte tre proprietà personalizzate agli schemi di provisioning per supportare la funzionalità Raccolta immagini condivise:

`UseSharedImageGallery`

- Definisce se utilizzare la Raccolta immagini condivise per archiviare le immagini pubblicate. Se impostata su **True**, l'immagine viene memorizzata come immagine della Raccolta immagini condivise, altrimenti viene memorizzata come snapshot.
- I valori validi sono **True** e **False**.
- Se la proprietà non è definita, il valore predefinito è **False**.

`SharedImageGalleryReplicaRatio`

- Definisce il rapporto tra macchine e repliche di versioni di immagini della raccolta.
- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, vengono utilizzati i valori predefiniti. Il valore predefinito per i dischi del sistema operativo persistenti è 1.000 e il valore predefinito per i dischi del sistema operativo non persistenti è 40.

`SharedImageGalleryReplicaMaximum`

- Definisce il numero massimo di repliche per ogni versione dell'immagine della raccolta.
- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, il valore predefinito è 10.
- Azure attualmente supporta fino a 10 repliche per una singola versione dell'immagine della raccolta. Se la proprietà è impostata su un valore maggiore di quello supportato da Azure, MCS tenta di utilizzare il valore specificato. Azure genera un errore, che viene registrato da MCS, e lascia invariato il numero di repliche corrente.

> **Suggerimento:**
>
> Quando si utilizza la Raccolta immagini condivise per archiviare un'immagine pubblicata per i cataloghi di cui è stato eseguito il provisioning con MCS, MCS imposta il numero di repliche delle

> versioni delle immagini della raccolta in base al numero di macchine nel catalogo, al rapporto di replica e al numero massimo di repliche. Il conteggio delle repliche viene calcolato dividendo il numero di macchine nel catalogo per il rapporto di replica (arrotondando per eccesso al valore intero più vicino) e quindi limitando il valore al numero massimo di repliche. Ad esempio, con un rapporto di replica di 20 e un massimo di 5, per 0-20 macchine viene creata una replica, per 21-40 macchine vengono create 2 repliche, per 41-60 macchine vengono create 3 repliche, per 61-80 macchine vengono create 4 repliche e per 81 macchine o più vengono create 5 repliche.

Caso d'uso: aggiornamento del rapporto di replica e della replica massima della Raccolta immagini condivise

Il catalogo delle macchine esistente utilizza la Raccolta immagini condivise. Utilizzare il comando `Set-ProvScheme` per aggiornare le proprietà personalizzate per tutte le macchine esistenti nel catalogo e per tutte le macchine future:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

Caso d'uso: conversione di un catalogo di snapshot in un catalogo della Raccolta immagini condivise

Per questo caso d'uso:

1. Eseguire `Set-ProvScheme` con il contrassegno `UseSharedImageGallery` impostato su **True**. Facoltativamente, includere le proprietà `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
```



```
        Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
        IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
        Property xsi:type="IntProperty" Name="
        SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

> **Suggerimento:**
>
> I parametri `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` non sono richiesti. Al completamento del comando `Set-ProvScheme`, l'immagine della Raccolta immagini condivise non è stata ancora creata. Una volta configurato il catalogo per l'utilizzo della raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata nella raccolta. Il comando di aggiornamento del catalogo crea la raccolta, l'immagine della raccolta e la versione dell'immagine. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto il conteggio delle repliche viene aggiornato, se appropriato. Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando l'immagine della Raccolta immagini condivise e tutte le macchine di cui è stato eseguito il provisioning vengono create utilizzando l'immagine. La vecchia snapshot viene ripulita automaticamente entro poche ore.

Caso d'uso: conversione di un catalogo della Raccolta immagini condivise in un catalogo di snapshot

Per questo caso d'uso:

1. Eseguire `Set-ProvScheme` con il contrassegno `UseSharedImageGallery` impostato su **False** o non definito.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

> **Suggerimento:**
>
> A differenza dell'aggiornamento da una snapshot a un catalogo della Raccolta immagini condivise, i dati personalizzati per ogni macchina non sono ancora aggiornati per riflettere le nuove proprietà personalizzate. Eseguire il comando seguente per visualizzare le

> proprietà personalizzate originali della Raccolta immagini condivise: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Dopo il completamento del comando `Set-ProvScheme`, la snapshot dell'immagine non è stata ancora creata. Una volta configurato il catalogo per non utilizzare la raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata come snapshot. Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando la snapshot e tutte le macchine di cui è stato eseguito il provisioning vengono create dalla snapshot. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto i dati della macchina personalizzati vengono aggiornati per riflettere che `UseSharedImageGallery` è impostato su **False**. Le vecchie risorse della Raccolta immagini condivise (raccolta, immagine e versione) vengono ripulite automaticamente nel giro di poche ore.

Eseguire il provisioning delle macchine in zone di disponibilità specificate

È possibile effettuare il provisioning delle macchine in zone di disponibilità specifiche in ambienti Azure. È possibile raggiungere questo obiettivo utilizzando PowerShell.

> **Nota:**
>
> Se non viene specificata alcuna zona, MCS consente ad Azure di posizionare le macchine all'interno della regione. Se viene specificata più di una zona, MCS distribuisce in modo casuale le macchine nelle zone.

Configurare le zone di disponibilità tramite PowerShell

Utilizzando PowerShell, è possibile visualizzare gli articoli di inventario offerti utilizzando `Get-Item`. Ad esempio, per visualizzare l'offerta di servizi *Eastern US region* `Standard_B1ls` (Regione degli Stati Uniti orientali):

```
1 $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
     name\East US.region\serviceoffering.folder\Standard_B1ls.
     serviceoffering"
```

Per visualizzare le zone, utilizzare il parametro `AdditionalData` per l'elemento:

```
$serviceOffering.AdditionalData
```

Se le zone di disponibilità non sono specificate, non vi è alcun cambiamento nel modo in cui viene eseguito il provisioning delle macchine.

Per configurare le zone di disponibilità tramite PowerShell, utilizzare la proprietà personalizzata **Zones** (Zone) disponibile con l'operazione `New-ProvScheme`. La proprietà **Zones** (Zone) definisce un elenco di zone di disponibilità in cui eseguire il provisioning delle macchine. Tali

zone possono includere una o più zone di disponibilità. Ad esempio, <Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/> per le zone 1 e 3.

Utilizzare il comando Set-ProvScheme per aggiornare le zone per uno schema di provisioning.

Se viene fornita una zona non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore che fornisce istruzioni su come correggere il comando non valido.

> **Suggerimento:**
>
> Se si specifica una proprietà personalizzata non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore pertinente.

Tipologie di archiviazione

Selezionare diversi tipi di archiviazione per le macchine virtuali negli ambienti di Azure che utilizzano MCS. Per le macchine virtuali di destinazione, MCS supporta:

- Disco del sistema operativo: SSD premium, SSD o HDD
- Disco della cache write-back: SSD premium, SSD o HDD

Quando si utilizzano questi tipi di archiviazione, considerare quanto segue:

- Assicurarsi che la macchina virtuale supporti il tipo di archiviazione selezionato.
- Se la configurazione utilizza un disco temporaneo di Azure, non è disponibile l'opzione per l'impostazione del disco della cache write-back.

> **Suggerimento:**
>
> StorageType è configurato per un tipo di sistema operativo e un account di archiviazione. WBCDiskStorageType è configurato per il tipo di archiviazione della cache write-back. Per un catalogo normale, è necessario StorageType. Se WBCDiskStorageType non è configurato, StorageType viene utilizzato come impostazione predefinita per WBCDiskStorageType.

Se WBCDiskStorageType non è configurato, StorageType viene utilizzato come impostazione predefinita per WBCDiskStorageType.

Configurare i tipi di archiviazione

Per configurare i tipi di archiviazione per le macchine virtuali, utilizzare il parametro StorageType in New-ProvScheme. Impostare il valore del parametro StorageType su uno dei tipi di archiviazione supportati.

Di seguito è riportato un set di esempio del parametro CustomProperties in uno schema di provisioning:


```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
</CustomProperties>'
```

Abilitare l'archiviazione con ridondanza della zona

È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione del catalogo. Replica il disco gestito di Azure in modo sincrono in più zone di disponibilità, il che consente di effettuare il ripristino dopo che si è verificato un errore in una zona utilizzando la ridondanza di altre.

È possibile specificare **Premium_ZRS** e **StandardSSD_ZRS** nelle proprietà personalizzate del tipo di archiviazione. L'archiviazione ZRS può essere impostata utilizzando le proprietà personalizzate esistenti o tramite il modello **MachineProfile**. L'archiviazione ZRS è supportata anche con il comando `Set-ProvVMUpdateTimeWindow` accompagnato dai parametri `-StartsNow` e `-DurationInMinutes -1`, ed è possibile modificare il computer esistente dall'archiviazione LRS a quello ZRS.

Limitazioni:

- Supportato solo nei dischi gestiti
- Supportato solo se si utilizzano unità a stato solido (SSD) premium e standard
- Non supportato in `StorageTypeAtShutdown`
- Disponibile solo in alcune aree geografiche.
- Le prestazioni di Azure diminuiscono quando si creano dischi ZRS su larga scala. Pertanto, alla prima accensione, accendere le macchine in batch più piccoli (meno di 300 macchine alla volta)

Imposta l'archiviazione con ridondanza della zona come tipo di archiviazione su disco È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione iniziale del catalogo oppure aggiornare il tipo di archiviazione in un catalogo esistente.

Seleziona l'archiviazione con ridondanza della zona utilizzando i comandi PowerShell Quando si crea un nuovo catalogo in Azure usando il comando `New-ProvScheme` di PowerShell, utilizzare il valore `Standard_ZRS` in `StorageAccountType`.
Ad esempio:


```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
```

Quando lo si imposta, questo valore viene convalidato da un'API dinamica che determina se può essere utilizzato correttamente. Le seguenti eccezioni possono verificarsi se l'uso di ZRS non è valido per il proprio catalogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: la proprietà personalizzata StorageTypeAtShutdown non può essere utilizzata con l'archiviazione ZRS.
- **StorageAccountTypeNotSupportedInRegion**: questa eccezione si verifica se si tenta di utilizzare l'archiviazione ZRS in un'area di Azure che non supporta ZRS
- **ZrsRequiresManagedDisks**: è possibile utilizzare l'archiviazione con ridondanza della zona solo con dischi gestiti.

È possibile impostare il tipo di archiviazione su disco utilizzando le seguenti proprietà personalizzate:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante la creazione del catalogo, viene utilizzato il disco del sistema operativo del profilo macchina `StorageType` se non sono impostate le proprietà personalizzate.

Acquisire le impostazioni diagnostiche su VM e NIC da un profilo macchina

È possibile acquisire le impostazioni diagnostiche su VM e NIC da un profilo macchina durante la creazione di un catalogo di macchine, l'aggiornamento di un catalogo di macchine esistente e l'aggiornamento delle macchine virtuali esistenti.

È possibile creare una specifica di VM o di modello come origine del profilo macchina.

Passaggi chiave

1. Configurare gli ID richiesti in Azure. È necessario fornire questi ID nella specifica del modello.
    - Account di archiviazione
    - Area di lavoro per l'analisi dei log
    - Spazio dei nomi dell'hub degli eventi con prezzi di livello standard
2. Creare un'origine del profilo macchina.

3. Creare un nuovo catalogo di macchine, aggiornare un catalogo esistente o aggiornare le VM esistenti.

Configurare gli ID richiesti in Azure

Configurare una delle seguenti opzioni in Azure:

- Account di archiviazione
- Area di lavoro per l'analisi dei log
- Spazio dei nomi dell'hub degli eventi con prezzi di livello Standard

Configurare un account di archiviazione Creare un account di archiviazione standard in Azure. Nelle specifiche del modello, inserire il resourceID completo per l'account di archiviazione come. `storageAccountId`

Una volta che le VM sono configurate per registrare i dati nell'account di archiviazione, i dati sono reperibili nel contenitore `insights-metrics-pt1m`.

Configurare uno spazio di lavoro per l'analisi dei log Creare un'area di lavoro per l'analisi dei log. Nelle specifiche del modello, specificare il resourceID completo per l'area di lavoro di analisi dei log come workspaceID.

Una volta che le macchine virtuali sono configurate per registrare i dati nell'area di lavoro, i dati possono essere sottoposti a query in Logs all'interno di Azure. È possibile eseguire il seguente comando in Logs all'interno di Azure per mostrare il conteggio di tutte le metriche registrate da una risorsa:

'AzureMetrics
| summarize Count=count() by ResourceId# Creare un catalogo di Microsoft Azure

> **Nota:**
>
> Da luglio 2023, Microsoft ha rinominato Azure Active Directory (Azure AD) in Microsoft Entra ID. In questo documento, qualsiasi riferimento ad Azure Active Directory, Azure AD o AAD ora si riferisce a Microsoft Entra ID.

In Creare cataloghi di macchine sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud di Microsoft Azure Resource Manager.

> **Nota:**
>
> Prima di creare un catalogo di Microsoft Azure, è necessario completare la creazione di una connessione a Microsoft Azure. Vedere Connessione a Microsoft Azure.

Creare un catalogo di macchine

È possibile creare un catalogo di macchine in due modi:

- Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio
- Creare un catalogo di macchine usando PowerShell

Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio

Un'immagine può essere un disco, una snapshot o una versione immagine di una definizione di immagine all'interno della Raccolta di calcolo di Azure utilizzata per creare le macchine virtuali in un catalogo di macchine. Prima di creare il catalogo delle macchine, creare un'immagine in Azure Resource Manager. Per informazioni generali sulle immagini, vedere Creare cataloghi delle macchine.

> **Nota:**
>
> Il supporto per l'utilizzo di un'immagine master da una regione diversa da quella configurata nella connessione host è obsoleto. Utilizzare la Raccolta di calcolo di Azure per replicare l'immagine master nell'area desiderata.

Durante la preparazione dell'immagine, viene creata una macchina virtuale di preparazione basata sulla macchina virtuale originale. Questa macchina virtuale di preparazione è disconnessa dalla rete. Per disconnettere la rete dalla macchina virtuale di preparazione, viene creato un gruppo di sicurezza di rete per negare tutto il traffico in entrata e in uscita. Il gruppo di sicurezza di rete viene creato automaticamente una volta per catalogo. Il nome del gruppo di sicurezza di rete è <!JEKYLL@6100@0>, dove il GUID viene generato casualmente. Ad esempio, <!JEKYLL@6100@1>.

Nella procedura guidata di creazione del catalogo delle macchine:

- Le pagine **Machine Type** (Tipo di macchina) e **Machine Management** (Gestione macchina) non contengono informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Image** scegliere un'immagine da utilizzare come modello per creare macchine in questo catalogo.

  Se si seleziona **Raccolta di calcolo di Azure** (Immagine master) come tipo di immagine da utilizzare, fare clic su **Select an image** (Selezionare un'immagine) e seguire questi passaggi per selezionare un'immagine master come necessario:

  1. (Applicabile solo alle connessioni configurate con immagini condivise all'interno di uno stesso tenant o tra tenant diversi) Selezionare un abbonamento in cui risiede l'immagine.

2. Selezionare un gruppo di risorse.
3. Passare ad Azure VHD, alla Raccolta di calcolo di Azure o alla versione immagine di Azure. Se necessario, aggiungere una nota per l'immagine selezionata.

Quando selezionate un'immagine, tenere presente quanto segue:

- Verificare che sull'immagine sia installato un Citrix VDA.
- Se si seleziona un disco rigido virtuale collegato a una macchina virtuale, è necessario spegnere la VM prima di procedere al passaggio successivo.

> **Nota:**
>
> - La sottoscrizione corrispondente alla connessione (host) che ha creato le macchine nel catalogo è contrassegnata da un punto verde. Le altre sottoscrizioni sono quelle con Raccolta di calcolo di Azure condivisa con quella sottoscrizione. In queste sottoscrizioni vengono mostrate solo le gallerie condivise. Per informazioni su come configurare gli abbonamenti condivisi, vedere Condividere immagini all'interno di un tenant (tra abbonamenti) e Condividere immagini tra tenant.
> - L'uso di un profilo macchina con un avvio attendibile quale **Security Type** (Tipo di sicurezza) è obbligatorio quando si seleziona un'immagine o una snapshot con avvio attendibile abilitato. È quindi possibile abilitare o disabilitare SecureBoot e vTPM specificandone i valori nel profilo macchina. L'avvio attendibile non è supportato per la Raccolta immagini condivise. Per informazioni sull'avvio attendibile di Azure, vedere https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
> - È possibile creare uno schema di provisioning utilizzando il disco del sistema operativo temporaneo su Windows con avvio attendibile. Quando si seleziona un'immagine con avvio attendibile, è necessario selezionare un profilo macchina con avvio attendibile abilitato con vTPM. Per creare cataloghi delle macchine utilizzando un disco del sistema operativo temporaneo, vedere Come creare macchine utilizzando dischi del sistema operativo temporanei.
> - Quando è in corso la replica dell'immagine, è possibile procedere e selezionare l'immagine come immagine master e completare la configurazione. Tuttavia, il completamento della creazione del catalogo potrebbe richiedere più tempo durante la replica dell'immagine. MCS richiede che la replica venga completata entro un'ora a partire dalla creazione del catalogo. In caso di timeout della replica, la creazione del catalogo non riesce. È possibile verificare lo stato della replica in Azure. Riprovare se la replica è ancora in sospeso o dopo il completamento della replica.
> - Quando si seleziona un'immagine master per i cataloghi delle macchine in Azure, MCS identifica il tipo di sistema operativo in base all'immagine master e al profilo macchina selezionati. Se MCS non è in grado di identificarlo, selezionare il tipo di sistema operativo corrispondente all'immagine master.

> – È possibile effettuare il provisioning di un catalogo di macchine virtuali Gen2 utilizzando un'immagine Gen2 per migliorare le prestazioni in fase di avvio. Tuttavia, la creazione di un catalogo di macchine Gen2 utilizzando un'immagine Gen1 non è supportata. Allo stesso modo, non è supportata la creazione di un catalogo di macchine Gen1 utilizzando un'immagine Gen2. Inoltre, qualsiasi immagine precedente che non contiene informazioni sulla generazione è un'immagine Gen1.

Se si seleziona **Prepared image** (Immagine preparata) come tipo di immagine da utilizzare, fare clic su **Select an image** e selezionare un'immagine preparata come necessario.

Per garantire la corretta creazione della VM, verificare che sull'immagine sia installato Citrix VDA 2311 o successivo e che MCSIO sia presente sul VDA.

Una volta selezionata un'immagine, la casella di controllo **Use a machine profile (mandatory for Azure Active Directory)** [Usa un profilo macchina (obbligatoria per Azure Active Directory)] è automaticamente selezionata. Fare clic su **Select a machine profile** (Seleziona un profilo macchina) per accedere a una VM o a una specifica di modello ARM da un elenco di gruppi di risorse. Le macchine virtuali nel catalogo possono ereditare le configurazioni dal profilo macchina selezionato.

Convalidare la specifica del modello ARM per accertarsi che possa essere utilizzata come profilo macchina per creare un catalogo delle macchine. Esistono due modi per convalidare la specifica di modello ARM:

- Dopo aver selezionato la specifica del modello ARM dall'elenco dei gruppi di risorse, fare clic su **Next** (Avanti). Se la specifica del modello ARM contiene errori, vengono visualizzati messaggi di errore.
- Eseguire uno dei seguenti comandi PowerShell:
  * <!JEKYLL@6100@2>
  * <!JEKYLL@6100@3>

Alcuni esempi di configurazioni che le macchine virtuali possono ereditare da un profilo macchina includono:

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

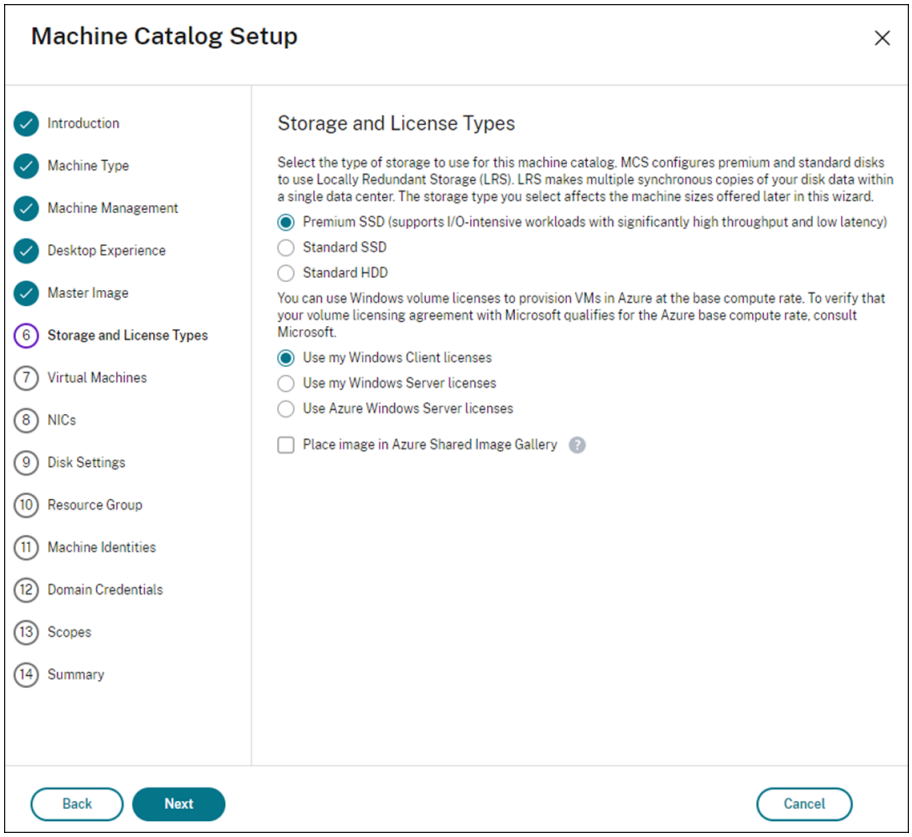
Dopo aver creato il catalogo, è possibile visualizzare le configurazioni che l'immagine eredita dal profilo della macchina. Nel nodo **Machine Catalogs** (Cataloghi delle macchine), selezionare il catalogo per visualizzare i relativi dettagli nel riquadro inferiore. Quindi, fare clic

sulla scheda **Template Properties** (Proprietà modello) per visualizzare le proprietà del profilo della macchina. La sezione **Tags** (Tag) visualizza fino a tre tag. Per visualizzare tutti i tag posizionati sulla macchina virtuale, fare clic su **View all** (Visualizza tutto).

Se si desidera che MCS esegua il provisioning delle macchine virtuali in un host dedicato di Azure, abilitare la casella di controllo **Use a dedicated host group** (Utilizza un gruppo host dedicato) e quindi selezionare un gruppo host dall'elenco. Un gruppo di host è una risorsa che rappresenta una raccolta di host dedicati. Un host dedicato è un servizio che fornisce server fisici che ospitano una o più macchine virtuali. Il server dedicato alla sottoscrizione di Azure non è condiviso con altri sottoscrittori. Quando si utilizza un host dedicato, Azure garantisce che le macchine virtuali siano le uniche macchine in esecuzione su quell'host. Questa funzionalità è adatta per gli scenari in cui è necessario soddisfare i requisiti normativi o di sicurezza interni. Per ulteriori informazioni sui gruppi di host e sulle considerazioni per il loro utilizzo, vedere Host dedicati di Azure.

> **Importante:**
>
> – Vengono visualizzati solo i gruppi di host per i quali è abilitato il posizionamento automatico di Azure.
> – L'utilizzo di un gruppo host modifica la pagina **Virtual Machines** (Macchine virtuali) mostrata più avanti nella procedura guidata. In questa pagina vengono mostrate solo le dimensioni delle macchine contenute nel gruppo host selezionato. Inoltre, le zone di disponibilità vengono selezionate automaticamente e non sono disponibili per la selezione.

- La pagina **Storage and License Types** (Tipi di archiviazione e licenze) viene visualizzata solo quando si utilizza un'immagine di Azure Resource Manager.



Sono disponibili i seguenti tipi di archiviazione da utilizzare per il catalogo delle macchine:

- **SSD premium**. Offre un'opzione di archiviazione su disco ad alte prestazioni e a bassa latenza adatta per macchine virtuali con carichi di lavoro a uso intensivo di I/O.
- **SSD standard**. Offre un'opzione di archiviazione conveniente adatta a carichi di lavoro che richiedono prestazioni costanti a livelli di IOPS inferiori.
- **HDD standard**. Offre un'opzione di archiviazione su disco affidabile e a basso costo adatta per macchine virtuali che eseguono carichi di lavoro non sensibili alla latenza.
- **Disco del sistema operativo temporaneo di Azure**. Offre un'opzione di archiviazione conveniente che riutilizza il disco locale delle macchine virtuali per ospitare il disco del sistema operativo. In alternativa, è possibile utilizzare PowerShell per creare macchine che utilizzano dischi dei sistemi operativi temporanei. Per ulteriori informazioni, vedere Dischi temporanei di Azure. Tenere presenti le seguenti considerazioni quando si utilizza un disco del sistema operativo temporaneo:
  - Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.
  - Per aggiornare le macchine che utilizzano dischi dei sistemi operativi temporanei, è necessario selezionare un'immagine la cui dimensione non superi la dimensione del disco della cache o del disco temporaneo della macchina virtuale.
  - Non è possibile utilizzare l'opzione **Retain VM and system disk during power cycles**

(Conserva la VM e il disco di sistema durante i cicli di alimentazione) disponibile più avanti nella procedura guidata.

> **Nota:**
>
> Il disco di identità viene sempre creato utilizzando SSD standard indipendentemente dal tipo di archiviazione scelto.

Il tipo di archiviazione determina le dimensioni delle macchine disponibili nella pagina **Virtual Machines** (Macchine virtuali) della procedura guidata. MCS configura dischi premium e standard per l'utilizzo dell'archiviazione con ridondanza locale (LRS). LRS esegue più copie sincrone dei dati del disco all'interno di un singolo centro dati. I dischi del sistema operativo temporaneo di Azure utilizzano il disco locale delle macchine virtuali per archiviare il sistema operativo. Per informazioni dettagliate sui tipi di archiviazione di Azure e sulla replica dell'archiviazione, vedere quanto segue:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Selezionare se utilizzare le licenze Windows o Linux esistenti.

- Licenze Windows: l'utilizzo di licenze Windows insieme a immagini Windows (immagini di supporto o immagini personalizzate della piattaforma Azure) consente di eseguire macchine virtuali Windows in Azure a un costo ridotto. Esistono due tipi di licenze:
  - **Licenza Windows Server**. Consente di utilizzare le licenze Windows Server o Azure Windows Server, consentendo l'utilizzo dei Vantaggi di Azure ibrido. Per i dettagli, vedere https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. I vantaggi di Azure ibrido riducono il costo di esecuzione delle macchine virtuali in Azure alla tariffa di elaborazione di base, eliminando il costo delle licenze aggiuntive di Windows Server dalla raccolta di Azure.
  - **Licenza client Windows**. Consente di trasferire le licenze di Windows 10 e Windows 11 in Azure, consentendo di eseguire macchine virtuali Windows 10 e Windows 11 in Azure senza la necessità di licenze aggiuntive. Per i dettagli, vedere Licenze di accesso client e licenze di gestione.

È possibile verificare che la macchina virtuale di cui è stato eseguito il provisioning stia utilizzando il vantaggio di licenza eseguendo il seguente comando PowerShell: <!JEKYLL@6100@4>.

- Per il tipo di licenza Windows Server, verificare che il tipo di licenza sia **Windows_Server**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.

- Per il tipo di licenza client Windows, verificare che il tipo di licenza sia **Windows_Client**. Ulteriori istruzioni sono disponibili alla pagina https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

In alternativa, è possibile utilizzare l'SDK PowerShell <!JEKYLL@6100@5> per eseguire la verifica. Ad esempio: <!JEKYLL@6100@6>. Per ulteriori informazioni su questo cmdlet, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licenze Linux: con le licenze Linux BYOS (Bring-Your-Own-Subscription), non è necessario pagare per il software. La tariffa BYOS include solo la tariffa per l'hardware di elaborazione. Esistono due tipi di licenze:

  * **RHEL_BYOS**: per utilizzare correttamente il tipo RHEL_BYOS, abilitare Red Hat Cloud Access nella sottoscrizione di Azure.
  * **SLES_BYOS**: le versioni BYOS di SLES includono il supporto di SUSE.

  È possibile impostare il valore LicenseType sulle opzioni Linux in <!JEKYLL@6100@7> e <!JEKYLL@6100@8>.

  Esempio di impostazione di LicenseType su RHEL_BYOS per <!JEKYLL@6100@9>:

  <!JEKYLL@6100@10>

  Esempio di impostazione di LicenseType su SLES_BYOS per <!JEKYLL@6100@11>:

  <!JEKYLL@6100@12>

  > **Nota:**
  >
  > Se il valore <!JEKYLL@6100@13> è vuoto, i valori predefiniti sono Azure Windows Server License (Licenza Azure Windows Server) o Azure Linux License (Licenza Azure Linux), a seconda del valore di OSType.

  Esempio di impostazione di LicenseType su un valore vuoto:

  <!JEKYLL@6100@14>

Consultare i seguenti documenti per comprendere i tipi di licenza e i relativi vantaggi:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

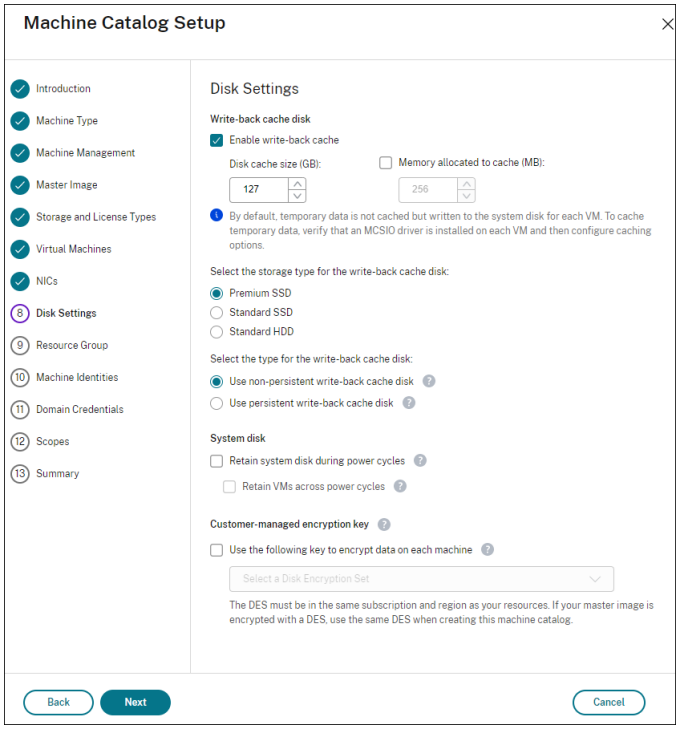
Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise Azure) è un repository per la gestione e la condivisione di immagini. Consente di rendere disponibili le immagini in

tutta l'organizzazione. Si consiglia di memorizzare un'immagine in SIG quando si creano cataloghi delle macchine di grandi dimensioni non persistenti, perché in questo modo è possibile reimpostare più velocemente i dischi del sistema operativo VDA. Dopo aver selezionato **Place image in Azure Compute Gallery** (Inserisci immagine nella Raccolta di calcolo di Azure), viene visualizzata la sezione **Azure Compute Gallery settings** (Impostazioni della Raccolta di calcolo di Azure), che consente di specificare altre impostazioni della Raccolta di calcolo di Azure:

  - **Ratio of virtual machines to image replicas** (Rapporto tra macchine virtuali e repliche di immagini). Consente di specificare il rapporto tra macchine virtuali e repliche di immagini che si desidera conservare in Azure. Per impostazione predefinita, Azure conserva una singola replica di immagine ogni 40 macchine non persistenti. Per le macchine persistenti, l'impostazione predefinita del numero è 1.000.
  - **Maximum replica count** (Numero massimo di repliche). Consente di specificare il numero massimo di repliche di immagini che si desidera conservare in Azure. L'impostazione predefinita è 10.

  > **Nota:**
  >
  > In ACG viene creata una galleria per archiviare l'immagine. Questa galleria è accessibile solo a MCS per la creazione di macchine virtuali e non appare nella pagina **Select an image** (Selezionare un'immagine).

- Nella pagina **Virtual Machines** (Macchine virtuali), indicare quante macchine virtuali si desidera creare. È necessario specificarne almeno uno e selezionare una dimensione della macchina. Dopo la creazione del catalogo, è possibile modificare le dimensioni della macchina modificando il catalogo.
- La pagina **NIC** non contiene informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.
- Nella pagina **Disk Settings** (Impostazioni disco), scegliere se abilitare la cache write-back. Con la funzione di ottimizzazione dell'archiviazione MCS abilitata, è possibile configurare le seguenti impostazioni durante la creazione di un catalogo. Queste impostazioni si applicano sia agli ambienti Azure che agli ambienti GCP.



Dopo aver abilitato la cache write-back, è possibile procedere come segue:

- Configurare le dimensioni del disco e della RAM utilizzati per la memorizzazione nella cache dei dati temporanei. Per maggiori informazioni, consultare Configurare la cache per i dati temporanei.
- Selezionare il tipo di archiviazione per il disco della cache write-back. Sono disponibili le seguenti opzioni di archiviazione per il disco della cache write-back:
  - Premium SSD (SSD premium)
  - Standard SSD (SSD standard)
  - Standard HDD (HDD standard)
- Scegliere se si desidera che il disco della cache write-back venga mantenuto per le macchine virtuali di cui è stato eseguito il provisioning. Selezionare **Enable write-back cache** (Abilita cache write-back) per rendere disponibili le opzioni. Per impostazione predefinita, l'opzione **Use non-persistent write-back cache disk** (Usa disco della cache write-back non persistente) è selezionata.
- Selezionare il tipo per il disco della cache write-back.
  - **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se selezionato, il disco della cache write-back viene eliminato durante i cicli di alimentazione. Tutti i dati reindirizzati a tale disco andranno persi. Se il disco temporaneo della macchina virtuale dispone di spazio sufficiente, viene utilizzato per ospitare il disco della cache write-back per ridurre i costi. Dopo la creazione del catalogo,

è possibile verificare se le macchine di cui è stato eseguito il provisioning utilizzano il disco temporaneo. A tale scopo, fare clic sul catalogo e verificare le informazioni nella scheda **Template Properties** (Proprietà modello). Se viene utilizzato il disco temporaneo, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **Yes (using VM's temporary disk)** (Sì, utilizzando il disco temporaneo della macchina virtuale). In caso contrario, viene visualizzato **Non-persistent Write-back Cache Disk** (Disco della cache write-back non persistente) e il relativo valore è **No (not using VM's temporary disk)** (No, non utilizzando il disco temporaneo della macchina virtuale).

* **Use persistent write-back cache disk** (Utilizza disco della cache write-back persistente). Se questa opzione è selezionata, il disco della cache write-back persiste per le macchine virtuali di cui è stato eseguito il provisioning. L'abilitazione dell'opzione aumenta i costi di archiviazione.

– Scegliere se conservare le VM e i dischi di sistema per i VDA durante i cicli di alimentazione.

Retain VM and system disk during power cycles (Conserva la VM e il disco di sistema durante i cicli di alimentazione). Disponibile quando si è selezionato **Enable write-back cache** (Abilita cache di write-back). Per impostazione predefinita, le VM e i dischi di sistema vengono eliminati all'arresto e ricreati all'avvio. Se si desidera ridurre i tempi di riavvio delle VM, selezionare questa opzione. Tenere presente che l'attivazione di questa opzione aumenta anche i costi di archiviazione.

– Scegliere se abilitare **Storage cost savings** (Risparmi sui costi di archiviazione). Se abilitato, risparmia sui costi di archiviazione eseguendo il downgrade del disco di archiviazione ad HDD standard all'arresto della VM. La VM torna alle impostazioni originali al momento del riavvio. L'opzione si applica sia ai dischi di archiviazione che ai dischi cache write-back. In alternativa, è anche possibile usare PowerShell. Vedere Portare il tipo di archiviazione a un livello inferiore quando una VM viene arrestata.

> **Nota:**
>
> Microsoft impone restrizioni sulla modifica del tipo di archiviazione durante l'arresto della macchina virtuale. È anche possibile che Microsoft in futuro blocchi le modifiche al tipo di archiviazione. Per ulteriori informazioni, vedere questo articolo di Microsoft.

– Scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Per ulteriori informazioni, vedere Crittografia lato server di Azure.

- Nella pagina **Resource Group** (Gruppo di risorse), scegliere se creare gruppi di risorse o utilizzare gruppi esistenti.

  - Se si sceglie di creare gruppi di risorse, selezionare **Next** (Avanti).
  - Se si sceglie di utilizzare gruppi di risorse esistenti, selezionare i gruppi dall'elenco **Available Provisioning Resource Groups** (Gruppi di risorse di provisioning disponibili). **Da ricordare**: selezionare un numero sufficiente di gruppi per ospitare le macchine che si stanno creando nel catalogo. Se se ne scelgono troppo pochi, viene visualizzato un messaggio. Si potrebbe voler selezionare un numero superiore al minimo richiesto se si prevede di aggiungere altre macchine virtuali al catalogo in un secondo momento. Non è possibile aggiungere altri gruppi di risorse a un catalogo dopo la creazione del catalogo.

  Per ulteriori informazioni, vedere Gruppi di risorse di Azure.

- Nella pagina **Machine Identities** (Identità macchine), scegliere un tipo di identità e configurare le identità per le macchine in questo catalogo. Se si selezionano le macchine virtuali come aggiunte ad **Azure Active Directory**, èpossibile aggiungerle a un gruppo di sicurezza di Azure AD. I passaggi dettagliati sono i seguenti:

  1. Nel campo **Identity type** (Tipo di identità), selezionare **Azure Active Directory joined**. Viene visualizzata l'opzione **Azure AD security group (optional)** [Gruppo di sicurezza di Azure AD (opzionale)].
  2. Fare clic su **Azure AD security group: Create new** (Gruppo di sicurezza Azure AD: Crea nuovo).
  3. Inserire un nome per il gruppo, quindi fare clic su **Create**.
  4. Seguire le istruzioni sullo schermo per accedere ad Azure.
     Se il nome del gruppo non esiste in Azure, viene visualizzata un'icona verde. In caso contrario, viene visualizzato un messaggio di errore che richiede di inserire un nuovo nome.
  5. Inserire lo schema di denominazione degli account macchina per le macchine virtuali.

  Dopo la creazione del catalogo, Citrix Virtual Apps and Desktops accede ad Azure per conto dell'utente e crea il gruppo di sicurezza e una regola di appartenenza dinamica per il gruppo. In base alla regola, le macchine virtuali con lo schema di denominazione specificato in questo catalogo vengono aggiunte automaticamente al gruppo di sicurezza.

  L'aggiunta di macchine virtuali con uno schema di denominazione diverso a questo catalogo richiede l'accesso ad Azure. Citrix Virtual Apps and Desktops può quindi accedere ad Azure e creare una regola di appartenenza dinamica basata sul nuovo schema di denominazione.

  Quando si elimina questo catalogo, l'eliminazione del gruppo di sicurezza da Azure richiede anche l'accesso ad Azure.

- Le pagine **Domain Credentials** (Credenziali di dominio) e **Summary** (Riepilogo) non contengono informazioni specifiche di Azure. Seguire le linee guida riportate nell'articolo Creare cataloghi di macchine.

Completare la procedura guidata.

Condizioni perché il disco temporaneo di Azure sia idoneo per il disco della cache write-back

È possibile utilizzare il disco temporaneo di Azure come disco della cache write-back solo se vengono soddisfatte tutte le seguenti condizioni:

- Il disco della cache write-back non deve persistere poiché il disco temporaneo di Azure non è appropriato per i dati persistenti.
- La dimensione della macchina virtuale di Azure scelta deve includere un disco temporaneo.
- Non è necessario abilitare il disco del sistema operativo temporaneo.
- Accettare di inserire il file della cache write-back sul disco temporaneo di Azure.
- La dimensione temporanea del disco di Azure deve essere maggiore della dimensione totale di (dimensione del disco della cache write-back + spazio riservato per il file di paging + 1 GB di spazio buffer).

Scenari relativi al disco della cache write-back non persistente

La tabella seguente descrive tre diversi scenari in cui il disco temporaneo viene utilizzato per la cache write-back durante la creazione del catalogo delle macchine.

Scenario	Risultato
Tutte le condizioni per utilizzare il disco temporaneo per la cache write-back sono soddisfatte.	Il file WBC <!JEKYLL@6100@15> viene inserito nel disco temporaneo.
Lo spazio sul disco temporaneo non è sufficiente per l'utilizzo della cache write-back.	Viene creato un disco VHD <!JEKYLL@6100@16> e il file WBC <!JEKYLL@6100@17> viene inserito su questo disco.
Il disco temporaneo ha spazio sufficiente per l'utilizzo della cache write-back, ma <!JEKYLL@6100@18> è impostato su **false**.	Viene creato un disco VHD <!JEKYLL@6100@19> e il file WBC <!JEKYLL@6100@20> viene inserito su questo disco.

Creare una specifica del modello di Azure

È possibile creare una specifica del modello di Azure nel portale di Azure e utilizzarla in Web Studio e nei comandi PowerShell per creare o aggiornare un catalogo di macchine MCS.

Per creare una specifica del modello di Azure per una macchina virtuale esistente:

1. Andare al portale di Azure. Selezionare un gruppo di risorse, quindi selezionare la macchina virtuale e l'interfaccia di rete. Nel menu **...** in alto, fare clic su **Export template** (Esporta modello).
2. Deselezionare la casella di controllo **Include parameters** (Includi parametri) se si desidera creare una specifica del modello di provisioning del catalogo.
3. Fare clic su **Add to library** (Aggiungi alla libreria) per modificare le specifiche del modello in un secondo momento.
4. Nella pagina **Importing template** (Modello di importazione), inserire le informazioni richieste: **Name** (nome), **Subscription** (abbonamento), **Resource Group** (Gruppo di risorse), **Location** (Posizione) e **Version** (Versione). Fare clic su **Next: Edit Template** (Avanti: Modifica modello).
5. È inoltre necessaria un'interfaccia di rete come risorsa indipendente se si desidera effettuare il provisioning di cataloghi. Pertanto, è necessario rimuovere qualsiasi elemento <!JEKYLL@6100@21> specificato nelle specifiche del modello. Ad esempio:

   <!JEKYLL@6100@22>
6. Creare **Review+Create** (Rivedi+Crea) e le specifiche del modello.
7. Nella pagina **Template Specs** (Specifiche del modello), verificare le specifiche del modello appena creato. Fare clic sulle specifiche del modello. Nel pannello di sinistra, fare clic su **Versions** (Versioni).
8. È possibile creare una nuova versione facendo clic su **Create new version** (Crea nuova versione). Specificare un nuovo numero di versione, apportare le necessarie modifiche alle specifiche del modello corrente e fare clic su **Review + Create** per creare la nuova versione della specifica del modello.

È possibile ottenere informazioni sulle specifiche del modello e sulla versione del modello utilizzando i seguenti comandi PowerShell:

- Per ottenere informazioni sulle specifiche del modello, eseguire:

  <!JEKYLL@6100@23>
- Per ottenere informazioni sulla versione delle specifiche del modello, eseguire:

  <!JEKYLL@6100@24>

Utilizzare le specifiche del modello per creare o aggiornare un catalogo

È possibile creare o aggiornare un catalogo di macchine MCS utilizzando una specifica di modello come input del profilo della macchina. A tale scopo, è possibile utilizzare i comandi Web Studio o PowerShell.

- Per Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio
- Per PowerShell, vedere Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell

Crittografia lato server di Azure

Citrix Virtual Apps and Desktops supporta le chiavi di crittografia gestite dal cliente per i dischi gestiti di Azure tramite Azure Key Vault. Con questo supporto è possibile gestire i requisiti organizzativi e di conformità crittografando i dischi gestiti del catalogo delle macchine utilizzando la propria chiave di crittografia. Per ulteriori informazioni, vedere Crittografia lato server dell'archiviazione su disco di Azure.

Quando si utilizza questa funzionalità per i dischi gestiti:

- Per cambiare la chiave con cui è crittografato il disco, è necessario modificare la chiave corrente in <!JEKYLL@6100@25>. Tutte le risorse associate a tale modifica <!JEKYLL@6100@26> devono essere crittografate con la nuova chiave.
- Quando si disabilita o si elimina la chiave, tutte le macchine virtuali con dischi che utilizzano tale chiave si spengono automaticamente. Dopo lo spegnimento, le macchine virtuali non sono utilizzabili a meno che la chiave non venga nuovamente abilitata o non venga assegnata una nuova chiave. Qualsiasi catalogo che utilizza la chiave non può essere acceso e non è possibile aggiungervi macchine virtuali.

Considerazioni importanti quando si utilizzano chiavi di crittografia gestite dal cliente

Quando si utilizza questa funzionalità, tenere presente quanto segue:

- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono risiedere nella stessa sottoscrizione e area geografica.
- Dopo aver abilitato la chiave di crittografia gestita dal cliente, non è possibile disabilitarla in un secondo momento. Se si desidera disabilitare o rimuovere la chiave di crittografia gestita dal cliente, copiare tutti i dati su un disco gestito diverso che non utilizza la chiave di crittografia gestita dal cliente.
- I dischi creati da immagini personalizzate crittografate utilizzando la crittografia lato server e le chiavi gestite dal cliente devono essere crittografati utilizzando le stesse chiavi gestite dal cliente. Questi dischi devono trovarsi nella stessa sottoscrizione.
- Le snapshot create da dischi crittografati con crittografia lato server e chiavi gestite dal cliente devono essere crittografate con le stesse chiavi gestite dal cliente.

- I dischi, le snapshot e le immagini crittografati con chiavi gestite dal cliente non possono passare a un altro gruppo di risorse e a un'altra sottoscrizione.
- I dischi gestiti attualmente o precedentemente crittografati utilizzando Crittografia dischi di Azure non possono essere crittografati utilizzando chiavi gestite dal cliente.
- Fare riferimento al sito Microsoft per le limitazioni sui set di crittografia dei dischi per ciascuna regione.

> **Nota:**
>
> Per informazioni sulla configurazione della crittografia lato server di Azure, vedere Guida rapida: creare un insieme di credenziali delle chiavi utilizzando il portale di Azure.

Chiave di crittografia gestita dal cliente di Azure

Quando si crea un catalogo delle macchine, è possibile scegliere se crittografare i dati sulle macchine di cui è stato eseguito il provisioning nel catalogo. La crittografia lato server con una chiave di crittografia gestita dal cliente consente di gestire la crittografia a livello di disco gestito e di proteggere i dati sulle macchine del catalogo. Un set di crittografia dei dischi (DES, Disk Encryption Set) rappresenta una chiave gestita dal cliente. Per utilizzare questa funzionalità, è necessario prima creare il DES in Azure. Un DES ha il formato seguente:

- <!JEKYLL@6100@27>

Selezionare un DES dall'elenco. Il DES selezionato deve essere nella stessa sottoscrizione e nella stessa regione delle risorse. Se l'immagine è crittografata con un DES, utilizzare lo stesso DES durante la creazione del catalogo delle macchine. Non è possibile modificare il DES dopo aver creato il catalogo.

Se si crea un catalogo con una chiave di crittografia e successivamente si disabilita il DES corrispondente in Azure, non si potrà più accendere alle macchine nel catalogo o aggiungervi macchine.

Vedere Creare un catalogo di macchine con chiave gestita dal cliente.

Crittografia del disco di Azure sull'host

È possibile creare un catalogo di macchine MCS con crittografia in modalità host. Attualmente, MCS supporta solo il flusso di lavoro dei profili macchina per questa funzionalità. È possibile utilizzare una VM o specifiche di modello come input per il profilo di una macchina.

Questo metodo di crittografia non crittografa i dati tramite l'archiviazione di Azure. Il server che ospita la macchina virtuale crittografa i dati e quindi i dati crittografati fluiscono attraverso il server di

archiviazione di Azure. Quindi, questo metodo di crittografia crittografa i dati per tutto il loro percorso dall'inizio alla fine.

Restrizioni:

La crittografia del disco di Azure sull'host è:

- non supportata per tutte le dimensioni delle macchine di Azure
- incompatibile con la crittografia del disco di Azure

Per creare un catalogo di macchine con funzionalità di crittografia sull'host:

1. Verificare se l'abbonamento ha la funzionalità di crittografia sull'host abilitata o meno. A questo scopo, vedere https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Se non è abilitata, è necessario abilitarla per l'abbonamento. Per informazioni sull'attivazione della funzionalità per l'abbonamento, vedere https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Verificare se una particolare dimensione di macchina virtuale di Azure supporta o meno la crittografia sull'host. A questo scopo, in una finestra di PowerShell, eseguire uno dei seguenti comandi:

   <!JEKYLL@6100@28>

   <!JEKYLL@6100@29>
3. Creare una macchina virtuale o specifiche di modello come input per il profilo della macchina nel portale di Azure con la crittografia sull'host abilitata.

   - Se si desidera creare una macchina virtuale, selezionare una dimensione di macchina virtuale che supporti la crittografia sull'host. Dopo aver creato la macchina virtuale, viene abilitata la relativa proprietà **Encryption at host** (Crittografia sull'host).
   - Se si desidera utilizzare specifiche di modello, assegnare al parametro <!JEKYLL@6100@30> il valore **true** all'interno di <!JEKYLL@6100@31>.
4. Creare un catalogo di macchine MCS con il flusso di lavoro dei profili delle macchine, selezionando una VM o specifiche di modello.

   - Disco del sistema operativo/disco dati: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma
   - Disco del sistema operativo temporaneo: viene crittografato solo tramite chiave gestita dalla piattaforma
   - Disco cache: viene crittografato tramite chiave gestita dal cliente e chiave gestita dalla piattaforma

   È possibile creare il catalogo delle macchine utilizzando Web Studio o eseguendo i comandi PowerShell.

Recuperare la crittografia delle informazioni sull'host da un profilo di macchina

È possibile recuperare le informazioni sulla crittografia sull'host da un profilo di macchina quando si esegue il comando PowerShell con il parametro <!JEKYLL@6100@32>. Se il parametro <!JEKYLL@6100@33> è **True**, significa che la crittografia sull'host è abilitata per il profilo macchina.

Ad esempio: quando l'input del profilo macchina è una VM, eseguire il seguente comando:

<!JEKYLL@6100@34>

Ad esempio: quando l'input del profilo macchina è una specifica di modello, eseguire il seguente comando:

<!JEKYLL@6100@35>

Doppia crittografia su disco gestito

È possibile creare un catalogo di macchine con doppia crittografia. In tutti i cataloghi creati con questa funzionalità tutti i dischi lato server sono crittografati con chiavi gestite dalla piattaforma e dal cliente. L'utente possiede e gestisce Azure Key Vault, Encryption Key e Disk Encryption Sets (DES).

La doppia crittografia è la crittografia lato piattaforma (impostazione predefinita) e la crittografia gestita dal cliente (CMEK). Pertanto, se si è un cliente altamente sensibile alla sicurezza e si nutre preoccupazione per il rischio associato a qualsiasi algoritmo di crittografia, implementazione o chiave compromessa, è possibile optare per questa doppia crittografia. Il sistema operativo persistente e i dischi di dati, le snapshot e le immagini sono tutti crittografati quando inattivi con doppia crittografia.

> **Nota:**
>
> - È possibile creare e aggiornare un catalogo di macchine con doppia crittografia utilizzando Web Studio e i comandi PowerShell. Per i comandi di PowerShell vedere Creare un catalogo di macchine con doppia crittografia.
> - È possibile utilizzare un flusso di lavoro non basato su profili macchina o un flusso di lavoro basato sul profilo macchina per creare o aggiornare un catalogo di macchine con doppia crittografia.
> - Se si utilizza un flusso di lavoro non basato su profili di macchina per creare un catalogo di macchine, è possibile riutilizzare il valore <!JEKYLL@6100@36> archiviato.
> - Se si utilizza un profilo macchina, è possibile utilizzare una VM o un specifica di modello come input per il profilo della macchina.

Limitazioni:

- La doppia crittografia non è supportata per i dischi Ultra Disks o Premium SSD v2.
- La doppia crittografia non è supportata sui dischi non gestiti.
- Se si disattiva una chiave del DiskEncryptionSet associata a un catalogo, le VM del catalogo vengono disattivate.
- Tutte le risorse correlate alle chiavi gestite dal cliente (Azure Key Vault, set di crittografia dei dischi, macchine virtuali, dischi e snapshot) devono essere nella stessa sottoscrizione e area geografica.
- È possibile creare solo fino a 50 set di crittografia del disco per regione per abbonamento.
- Non è possibile aggiornare un catalogo macchine che ha già <!JEKYLL@6100@37> con un <!JEKYLL@6100@38> diverso.

Gruppi di risorse di Azure

I gruppi di risorse di provisioning di Azure offrono un modo per eseguire il provisioning delle macchine virtuali che forniscono applicazioni e desktop agli utenti. È possibile aggiungere gruppi di risorse di Azure vuoti esistenti quando si crea un catalogo delle macchine MCS o quando vengono creati nuovi gruppi di risorse per conto dell'utente. Per informazioni sui gruppi di risorse di Azure, consultare la documentazione Microsoft.

Utilizzo dei gruppi di risorse di Azure

Non ci sono limiti al numero di macchine virtuali, dischi gestiti, snapshot e immagini per ciascun gruppo di risorse di Azure (il limite di 240 macchine virtuali per 800 dischi gestiti per ciascun gruppo di risorse di Azure è stato rimosso).

- Quando si utilizza un'entità servizio con ambito completo per creare un catalogo delle macchine, MCS crea un solo gruppo di risorse di Azure e utilizza tale gruppo per il catalogo.
- Quando si utilizza un'entità servizio con ambito limitato per creare un catalogo delle macchine, è necessario fornire un gruppo di risorse di Azure vuoto e pre-creato per il catalogo.

Dischi temporanei di Azure

Un disco temporaneo di Azure consente di riutilizzare il disco della cache o il disco temporaneo per archiviare il disco del sistema operativo per una macchina virtuale abilitata per Azure. Questa funzionalità è utile per gli ambienti Azure che richiedono un disco SSD a prestazioni più elevate rispetto a un disco rigido standard. Per informazioni su come creare un catalogo con un disco effimero di Azure, vedere Creare un catalogo con dischi effimeri di Azure.

> **Nota:**
>
> I cataloghi persistenti non supportano i dischi del sistema operativo temporanei.

I dischi del sistema operativo temporanei richiedono che lo schema di provisioning utilizzi dischi gestiti e una Raccolta immagini condivise.

Memorizzazione di un disco del sistema operativo temporaneo

È possibile memorizzare un disco del sistema operativo temporaneo sul disco temporaneo della macchina virtuale o su un disco di risorse. Questa funzionalità consente di utilizzare un disco del sistema operativo temporaneo con una macchina virtuale che non ha una cache o ha una cache insufficiente. Tali macchine virtuali dispongono di un disco temporaneo o di risorse per archiviare un disco del sistema operativo temporaneo, ad esempio <!JEKYLL@6100@39>.

Considerare quanto segue:

- Un disco temporaneo viene memorizzato nel disco della cache della macchina virtuale o nel disco temporaneo (risorsa) della macchina virtuale. Il disco della cache è preferibile rispetto al disco temporaneo, a meno che il disco della cache non sia abbastanza grande da ospitare i contenuti del disco del sistema operativo.
- Per gli aggiornamenti, una nuova immagine più grande del disco della cache ma più piccola del disco temporaneo comporta la sostituzione del disco del sistema operativo temporaneo con il disco temporaneo della macchina virtuale.

Ottimizzazione dell'archiviazione di dischi temporanei di Azure e Machine Creation Services (MCS) (I/O MCS)

Il disco del sistema operativo temporaneo di Azure e l'I/O MCS non possono essere abilitati contemporaneamente.

Le considerazioni importanti sono le seguenti:

- Non è possibile creare un catalogo delle macchine con il disco del sistema operativo temporaneo e l'I/O MCS abilitati contemporaneamente.
- I parametri PowerShell (<!JEKYLL@6100@40> e <!JEKYLL@6100@41>) non hanno effetto e restituiscono un vero e proprio messaggio di errore se vengono impostati su **true** in <!JEKYLL@6100@42> o <!JEKYLL@6100@43>.
- Per i cataloghi delle macchine esistenti creati con entrambe le funzionalità abilitate, è comunque possibile:
  - aggiornare un catalogo delle macchine

- aggiungere o eliminare macchine virtuali
- eliminare un catalogo delle macchine

Raccolta di calcolo di Azure

Utilizzare la Raccolta di calcolo di Azure (in precedenza Raccolta immagini condivise di Azure) come repository di immagini pubblicate per macchine di cui è stato eseguito il provisioning con MCS in Azure. È possibile archiviare un'immagine pubblicata nella raccolta per accelerare la creazione e l'attivazione dei dischi del sistema operativo, migliorando i tempi di avvio del sistema e delle applicazioni per le macchine virtuali non persistenti. La Raccolta immagini condivise contiene i tre elementi seguenti:

- *Galleria*: le immagini vengono archiviate qui. MCS crea una raccolta per ogni catalogo delle macchine.
- *Gallery Image Definition* (Definizione dell'immagine in galleria): questa definizione include informazioni (tipo e stato del sistema operativo, regione di Azure) sull'immagine pubblicata. MCS crea una definizione di immagine per ogni immagine creata per il catalogo.
- *Gallery Image Version* (Versione immagine in galleria): ciascuna immagine di una Raccolta immagini condivise può avere più versioni e ogni versione può avere più repliche in regioni diverse. Ogni replica è una copia completa dell'immagine pubblicata.

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

Per altre informazioni, vedere Archiviare e condividere immagini in una raccolta di calcolo di Azure.

Per informazioni sulla creazione o l'aggiornamento di un catalogo di macchine utilizzando l'immagine della Raccolta di calcolo di Azure mediante PowerShell, vedere Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure.

VM riservate di Azure

Le macchine virtuali di Azure con elaborazione riservata garantiscono che il desktop virtuale sia crittografato in memoria e protetto durante l'uso.

È possibile utilizzare MCS per creare un catalogo con macchine virtuali riservate di Azure. È necessario utilizzare il flusso di lavoro del profilo macchina per creare un catalogo di questo tipo. È possibile utilizzare una macchina virtuale e una specifica di modello ARM come input del profilo macchina.

Considerazioni importanti per le macchine virtuali riservate

Le considerazioni importanti relative alle dimensioni delle macchine virtuali supportate e alla creazione di un catalogo di macchine con macchine virtuali riservate sono le seguenti:

- Dimensioni di VM supportate: le VM riservate supportano le seguenti dimensioni di VM:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Creare cataloghi di macchine con macchine virtuali riservate.
  - È possibile creare un catalogo di macchine con VM riservate Azure utilizzando Web Studio e i comandi PowerShell.
  - È necessario utilizzare un flusso di lavoro basato sul profilo macchina per creare un catalogo di macchine virtuali riservate di Azure. È possibile utilizzare una macchina virtuale e una specifica di modello come input del profilo macchina.
  - L'immagine master e l'input del profilo macchina devono essere entrambi abilitati con lo stesso tipo di sicurezza riservato. I tipi di sicurezza sono:
    - **VMGuestStateOnly**: VM riservata con solo lo stato di ospite della VM crittografato
    - **DiskWithVMGuestState**: VM riservata con disco del sistema operativo e stato di ospite della VM crittografati con chiave gestita dalla piattaforma o chiave gestita dal cliente. È possibile crittografare sia il disco del sistema operativo normale che quello temporaneo.
  - È possibile ottenere informazioni sulle VM riservate di vari tipi di risorse quali disco gestito, snapshot, immagine di Azure Compute Gallery, VM e specifiche di modello ARM utilizzando il parametro AdditionalData. Ad esempio:

    <!JEKYLL@6100@44>

    I campi dati aggiuntivi sono:

    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

    Per ottenere la proprietà di riservatezza delle dimensioni di una macchina, eseguire il comando seguente: <!JEKYLL@6100@45>

    Il campo dati aggiuntivo è <!JEKYLL@6100@46>.

- Non è possibile modificare l'immagine master o il profilo macchina passando dal tipo di protezione riservato a quello non riservato o dal tipo di protezione non riservato a quello riservato.
- Vengono visualizzati i messaggi di errore appropriati per eventuali configurazioni errate.

Preparare immagini master e profili macchina

Prima di creare un set di VM riservate, preparare un'immagine master e un profilo macchina per esse seguendo questi passaggi:

1. Nel portale di Azure, creare una macchina virtuale riservata con impostazioni specifiche, ad esempio:
   - **Security Type** (Tipo di sicurezza): macchine virtuali riservate
   - **Confidential OS disk encryption** (Crittografia riservata del disco del sistema operativo): abilitata.
   - **Key management** (Gestione delle chiavi): crittografia riservata del disco con una chiave gestita dalla piattaforma
     Per ulteriori informazioni sulla creazione di macchine virtuali riservate, vedere questo articolo Microsoft.
2. Preparare l'immagine master sulla VM creata. Installare le applicazioni e il VDA necessari sulla VM creata.

   > **Nota:**
   >
   > La creazione di VM riservate utilizzando VHD non è supportata. Utilizzare invece Azure Compute Gallery, i dischi gestiti o le istantanee per questo scopo.

3. Creare il profilo della macchina in uno dei seguenti modi:
   - Utilizzare la VM esistente creata nel passaggio 1 se possiede le proprietà macchina necessarie.
   - Se si opta per una specifica del modello ARM come profilo macchina, creare la specifica del modello secondo necessità. In particolare, configurare i parametri che soddisfano i requisiti della VM riservata, come *SecurityEncryptionType* e *diskEncryptionSet* (per la chiave gestita dal cliente). Per ulteriori informazioni, vedere Creare una specifica del modello di Azure.

     > **Nota:**
     >
     > - Assicurarsi che l'immagine master e il profilo della macchina abbiano lo stesso tipo di chiave di sicurezza.

> – Per creare macchine virtuali riservate che richiedono la crittografia riservata del disco del sistema operativo con una chiave gestita dal cliente, assicurarsi che gli ID del set di crittografia del disco nell'immagine master e nel profilo della macchina siano identici.

Creare macchine virtuali riservate utilizzando Web Studio o i comandi PowerShell

Per creare un set di VM riservate, creare un catalogo di macchine utilizzando un'immagine master e un profilo macchina derivati dalla VM riservata desiderata.

Per creare il catalogo utilizzando Web Studio, seguire i passaggi descritti in Creare cataloghi di macchine. Tenere presenti le seguenti considerazioni:

- Nella pagina **Image** selezionare un'immagine master e un profilo macchina preparati per la creazione riservata della VM. La selezione del profilo macchina è obbligatoria e solo i profili che corrispondono allo stesso tipo di crittografia di sicurezza dell'immagine master selezionata sono disponibili per la selezione.
- Nella pagina **diskEncryptionSet** vengono selezionate solo le dimensioni delle macchine che supportano le VM riservate.
- Nella pagina **Disk Settings** (Impostazioni disco) non è possibile specificare il set di crittografia del disco perché questo è ereditato dal profilo del computer selezionato.

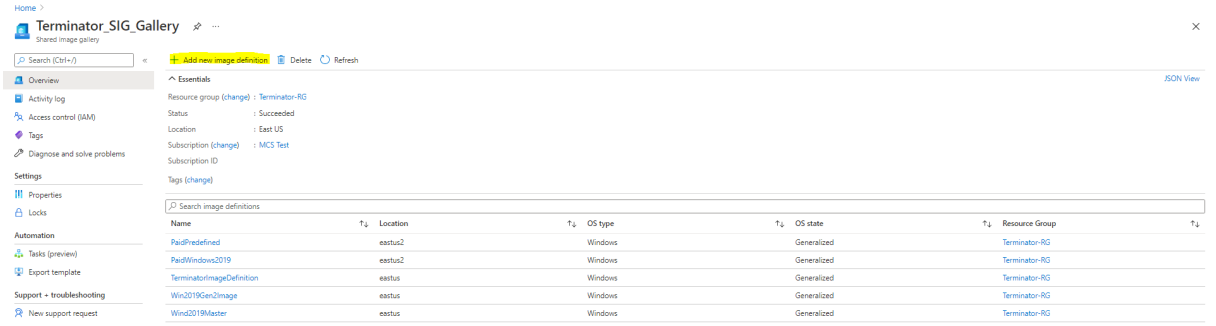
Azure Marketplace

Citrix Virtual Apps and Desktops supporta l'utilizzo di un'immagine master in Azure che contiene informazioni sul piano per creare un catalogo delle macchine. Per ulteriori informazioni, vedere Microsoft Azure Marketplace.

> **Suggerimento:**
>
> Alcune immagini che si trovano in Azure Marketplace, come l'immagine standard di Windows Server, non aggiungono informazioni sul piano. La funzionalità di Citrix Virtual Apps and Desktops è dedicata alle immagini a pagamento.

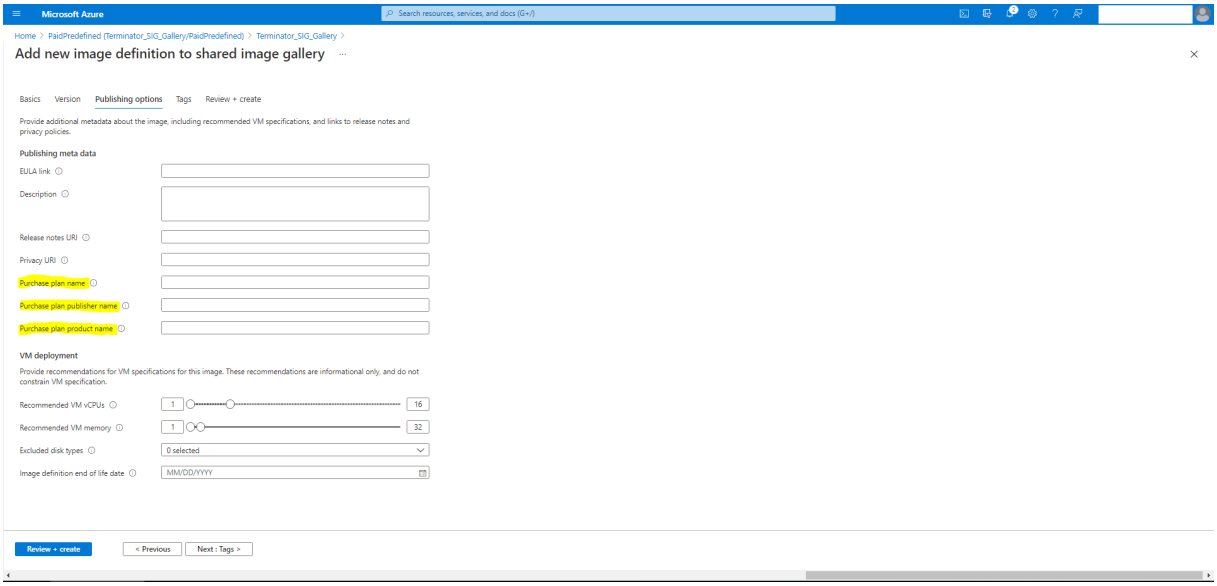
Assicurarsi che l'immagine creata nella Raccolta immagini condivise contenga informazioni sul piano di Azure

Utilizzare la procedura descritta in questa sezione per visualizzare le immagini della Raccolta immagini condivise in Web Studio. Facoltativamente, queste immagini possono essere utilizzate per un'immagine master. Per inserire l'immagine in una Raccolta immagini condivise, creare una definizione di immagine in una raccolta.

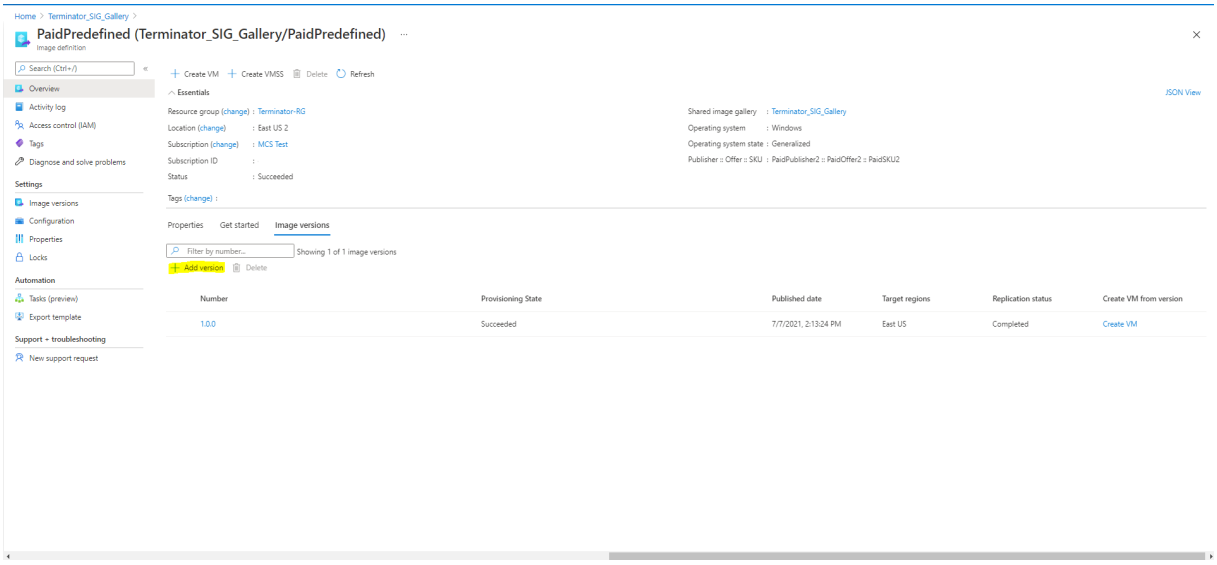


Nella pagina **Publishing options** (Opzioni di pubblicazione), verificare le informazioni sul piano di acquisto.

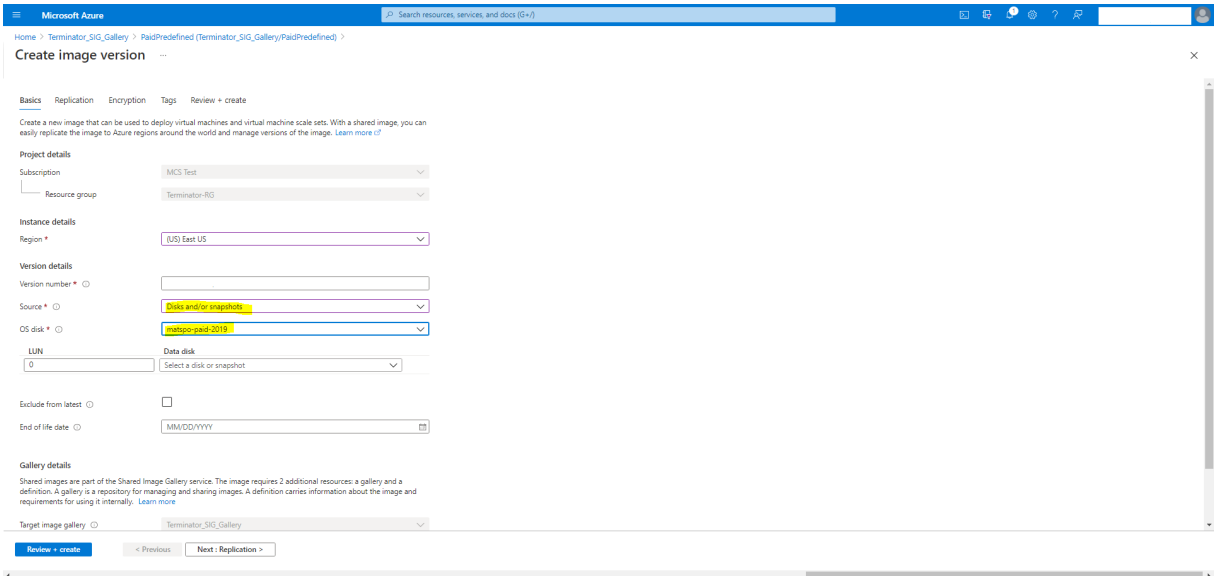
I campi relativi alle informazioni sul piano di acquisto sono inizialmente vuoti. Compilare questi campi con le informazioni sul piano di acquisto utilizzate per l'immagine. La mancata compilazione delle informazioni sul piano di acquisto può causare la mancata riuscita del processo del catalogo delle macchine.



Dopo aver verificato le informazioni sul piano di acquisto, creare una versione immagine all'interno della definizione. Viene utilizzata come immagine master. Fare clic su **Add version** (Aggiungi versione):



Nella sezione **Version details** (Dettagli versione), selezionare la snapshot dell'immagine o il disco gestito come origine:



Creare un catalogo di macchine usando PowerShell

Questa sezione descrive in dettaglio come creare cataloghi usando PowerShell:

- Creare un catalogo con un disco cache di write-back non persistente
- Creare un catalogo con un disco cache di write-back persistente
- Migliorare le prestazioni di avvio con MCSIO
- Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell
- Cataloghi di macchine con avvio attendibile
- Utilizzare i valori delle proprietà del profilo macchina

- Creare un catalogo di macchine con chiave di crittografia gestita dal cliente
- Creare un catalogo di macchine con doppia crittografia
- Creare un catalogo con dischi effimeri di Azure
- Host dedicati di Azure
- Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure
- Configurare la Raccolta immagini condivise
- Eseguire il provisioning delle macchine in zone di disponibilità specificate
- Tipologie di archiviazione
- Posizione del file di paging
- Aggiornare le impostazioni del file di paging
- Creare un catalogo usando le macchine virtuali Azure Spot
- Configurare le dimensioni delle VM di backup
- Copiare i tag su tutte le risorse
- Eseguire il provisioning delle macchine virtuali del catalogo con Azure Monitor Agent installato

Creare un catalogo con un disco cache di write-back non persistente

Per configurare un catalogo con il disco della cache write-back non persistente, utilizzare il parametro PowerShell <!JEKYLL@6100@47>. La proprietà personalizzata <!JEKYLL@6100@48> indica se si sta accettando di utilizzare l'archiviazione temporanea di Azure per archiviare il file della cache write-back. Questo deve essere configurato su true durante l'esecuzione di <!JEKYLL@6100@49> se si desidera utilizzare il disco temporaneo come disco della cache write-back. Se questa proprietà non viene specificata, il parametro è impostato su **False** per impostazione predefinita.

Ad esempio, utilizzando il parametro <!JEKYLL@6100@50> per impostare <!JEKYLL@6100@51> su **true**:

<!JEKYLL@6100@52>

> **Nota:**
>
> Dopo aver eseguito il commit del catalogo delle macchine per l'utilizzo dell'archiviazione temporanea locale di Azure per il file della cache write-back, non può essere modificato per utilizzare l'unità disco rigido virtuale in un secondo momento.

Creare un catalogo con un disco cache di write-back persistente

Per configurare un catalogo con il disco della cache write-back persistente, utilizzare il parametro PowerShell <!JEKYLL@6100@53>. Questo parametro supporta una proprietà aggiuntiva, <!JEKYLL@6100@54>, utilizzata per determinare il modo in cui il disco della cache write-back persiste per le macchine di cui è stato eseguito il provisioning con MCS. La proprietà <!JEKYLL@6100@55>

viene utilizzata solo quando viene specificato il parametro<!JEKYLL@6100@56> e quando il parametro <!JEKYLL@6100@57> è impostato per indicare che viene creato un disco.

Esempi di proprietà trovate nel parametro <!JEKYLL@6100@58> prima del supporto <!JEKYLL@6100@59> sono:

<!JEKYLL@6100@60>

Quando si utilizzano queste proprietà, considerare che contengono valori predefiniti se le proprietà vengono omesse dal parametro <!JEKYLL@6100@61>. La proprietà <!JEKYLL@6100@62> ha due valori possibili: **true** o **false**.

L'impostazione della proprietà <!JEKYLL@6100@63> su **true** non elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops spegne la macchina utilizzando Web Studio.

L'impostazione della proprietà <!JEKYLL@6100@64> **su false** elimina il disco della cache write-back quando l'amministratore di Citrix Virtual Apps and Desktops arresta la macchina utilizzando Web Studio.

> **Nota:**
>
> Se la proprietà <!JEKYLL@6100@65> viene omessa, sarà **false** per impostazione predefinita e la cache write-back viene eliminata quando il computer viene arrestato utilizzando Web Studio.

Ad esempio, utilizzando il parametro <!JEKYLL@6100@66> per impostare <!JEKYLL@6100@67> su true:

<!JEKYLL@6100@68>

> **Importante:**
>
> La proprietà <!JEKYLL@6100@69> può essere impostata solo utilizzando il cmdlet PowerShell <!JEKYLL@6100@70>. Il tentativo di modificare le <!JEKYLL@6100@71> di uno schema di provisioning dopo la creazione non ha alcun impatto sul catalogo macchine e sulla persistenza del disco della cache write-back quando un computer viene arrestato.

Ad esempio, impostare <!JEKYLL@6100@72> perché utilizzi la cache write-back mentre si imposta la proprietà <!JEKYLL@6100@73> su true:

<!JEKYLL@6100@74>

Migliorare le prestazioni di avvio con MCSIO

È possibile migliorare le prestazioni di avvio per i dischi gestiti di Azure e GCP quando MCSIO è abilitato. Utilizzare la proprietà personalizzata di PowerShell <!JEKYLL@6100@75> nel

comando <!JEKYLL@6100@76> per configurare questa funzionalità. Le opzioni associate a <!JEKYLL@6100@77> includono:

<!JEKYLL@6100@78><!JEKYLL@6100@79><!JEKYLL@6100@80>

Per abilitare questa funzionalità, impostare la proprietà personalizzata <!JEKYLL@6100@81> su <!JEKYLL@6100@82>. Ad esempio:

<!JEKYLL@6100@83>

Utilizzare le specifiche del modello per creare o aggiornare un catalogo mediante PowerShell

È possibile creare o aggiornare un catalogo di macchine MCS utilizzando una specifica di modello come input del profilo della macchina. A tale scopo, è possibile utilizzare i comandi Web Studio o PowerShell.

Per Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio

Utilizzare i comandi PowerShell:

1. Aprire una finestra di **PowerShell**.
2. Eseguire <!JEKYLL@6100@84>.
3. Creare o aggiornare un catalogo.
    - Per creare un catalogo:
        a) Utilizzare il comando <!JEKYLL@6100@85> con una specifica del modello come input per il profilo macchina. Ad esempio:
        <!JEKYLL@6100@86>
        b) Completare la creazione del catalogo di macchine.
    - Per aggiornare un catalogo, utilizzare il comando <!JEKYLL@6100@87> con una specifica di modello come input del profilo macchina. Ad esempio:
    <!JEKYLL@6100@88>

Cataloghi di macchine con avvio attendibile

Per creare correttamente un catalogo di macchine con avvio attendibile, utilizzare:

- Un profilo macchina con avvio attendibile
- Una dimensione di macchina virtuale che supporti l'avvio attendibile
- Una versione di macchina virtuale Windows che supporti l'avvio attendibile. Attualmente, Windows 10, Windows 11, Windows Server 2016, 2019 e 2022 supportano l'avvio attendibile.

> **Importante:**
>
> MCS supporta la creazione di un nuovo catalogo con macchine virtuali abilitate per l'avvio attendibile. Tuttavia, per aggiornare un catalogo persistente esistente e le macchine virtuali esistenti, è necessario utilizzare il portale di Azure. Non è possibile aggiornare l'avvio attendibile di un catalogo non persistente. Per ulteriori informazioni, vedere il documento Microsoft Abilitare l'avvio attendibile nelle macchine virtuali di Azure esistenti.

Per visualizzare gli elementi di inventario offerti da Citrix Virtual Apps and Desktops e determinare se le dimensioni della macchina virtuale supportano l'avvio attendibile, eseguire il seguente comando:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il seguente comando:

   <!JEKYLL@6100@89>
4. Eseguire <!JEKYLL@6100@90>
5. Controllare il valore dell'attributo <!JEKYLL@6100@91>.
   - Se <!JEKYLL@6100@92> è **True**, la dimensione della macchina virtuale supporta l'avvio attendibile.
   - Se <!JEKYLL@6100@93> è **False**, la dimensione della macchina virtuale non supporta l'avvio attendibile.

Come da PowerShell di Azure, è possibile usare il seguente comando per determinare le dimensioni di macchina virtuale che supportano l'avvio attendibile:

<!JEKYLL@6100@94>

Di seguito sono riportati alcuni esempi che descrivono se la dimensione della macchina virtuale supporta l'avvio attendibile dopo l'esecuzione del comando Azure PowerShell.

- *Esempio 1*: se la macchina virtuale di Azure supporta solo la generazione 1, quella macchina virtuale non supporta l'avvio attendibile. Pertanto, la funzionalità <!JEKYLL@6100@95> non viene visualizzata dopo l'esecuzione del comando Azure PowerShell.
- *Esempio 2*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità<!JEKYLL@6100@96> è **True**, la dimensione della macchina virtuale di generazione 2 non è supportata per l'avvio attendibile.
- *Esempio 3*: se la macchina virtuale di Azure supporta solo la generazione 2 e la funzionalità <!JEKYLL@6100@97> non viene visualizzata dopo l'esecuzione del comando PowerShell, la dimensione della VM di generazione 2 è supportata per l'avvio attendibile.

Per ulteriori informazioni sull'avvio attendibile per le macchine virtuali Azure, vedere il documento Microsoft Avvio attendibile per le macchine virtuali di Azure.

Creare un catalogo di macchine con l'avvio attendibile

1. Creare un'immagine master abilitata con l'avvio attendibile. Vedere la documentazione Microsoft Immagini di macchine virtuali ad avvio attendibile.
2. Creare una VM o una specifica di modello con il tipo di sicurezza impostato su **macchine virtuali con avvio attendibile**. Per ulteriori informazioni sulla creazione di una VM o di una specifica di modello, vedere il documento Microsoft Distribuire una macchina virtuale con avvio attendibile.
3. Creare un catalogo di macchine utilizzando Web Studio o i comandi PowerShell.
   - Se si desidera utilizzare Web Studio, vedere Creare un catalogo delle macchine utilizzando un'immagine di Azure Resource Manager in Web Studio.
   - Se si desidera utilizzare i comandi PowerShell, utilizzare il comando <!JEKYLL@6100@98> con la VM o la specifica del modello come input del profilo macchina. Per l'elenco completo dei comandi per creare un catalogo, vedere Creare un catalogo.

     Esempio di <!JEKYLL@6100@99> con la VM come input del profilo macchina:

     <!JEKYLL@6100@100>

     Esempio di <!JEKYLL@6100@101> con le specifiche del modello come input del profilo macchina:

     <!JEKYLL@6100@102>

Errori nella creazione di cataloghi di macchine con avvio attendibile

Si ottengono errori appropriati nei seguenti scenari durante la creazione di un catalogo di macchine con avvio attendibile:

Scenario	Errore
Se si seleziona un profilo macchina durante la creazione di un catalogo non gestito	<!JEKYLL@6100@103>
Se si seleziona un profilo macchina che supporta l'avvio attendibile durante la creazione di un catalogo con un disco non gestito come immagine master	<!JEKYLL@6100@104>
Se non si seleziona il profilo macchina durante la creazione di un catalogo gestito con un' immagine master con l'avvio attendibile come tipo di sicurezza	<!JEKYLL@6100@105>

Scenario	Errore
Se si seleziona un profilo macchina con un tipo di sicurezza diverso dal tipo di protezione dell'immagine master	<!JEKYLL@6100@106>
Se si seleziona una dimensione di macchina virtuale che non supporta l'avvio attendibile, ma utilizza un'immagine master che supporta l'avvio attendibile durante la creazione di un catalogo	<!JEKYLL@6100@107>

Utilizzare i valori delle proprietà del profilo macchina

Il catalogo delle macchine utilizza le seguenti proprietà definite nelle proprietà personalizzate:

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

Se queste proprietà personalizzate non sono definite in modo esplicito, i valori delle proprietà vengono impostati in base alla specifica del modello ARM o alla macchina virtuale, a seconda di quale sia utilizzata come profilo macchina. Inoltre, se non è specificato <!JEKYLL@6100@108>, questo viene impostato in base al profilo della macchina.

> **Nota:**
>
> Se alcune delle proprietà non sono presenti nel profilo macchina e non sono definite nelle proprietà personalizzate, vengono adottati i valori predefiniti delle proprietà laddove è applicabile.

La sezione seguente descrive alcuni scenari in <!JEKYLL@6100@109> e <!JEKYLL@6100@110> quando <!JEKYLL@6100@111> hanno tutte le proprietà definite o qando i valori sono derivati da MachineProfile.

- Scenari New-ProvScheme
  - MachineProfile ha tutte le proprietà e le CustomProperties non sono definite. Esempio:

    <!JEKYLL@6100@112>

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

<!JEKYLL@6100@113>

- MachineProfile ha alcune proprietà e le CustomProperties non sono definite. Esempio: MachineProfile ha solo LicenseType e OSType.

  <!JEKYLL@6100@114>

  I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  <!JEKYLL@6100@115>

- Sia MachineProfile che CustomProperties definiscono tutte le proprietà. Esempio:

  <!JEKYLL@6100@116>

  Le proprietà personalizzate hanno la priorità. I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  <!JEKYLL@6100@117>

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Esempio:

  * In CustomProperties sono definite LicenseType e StorageAccountType
  * In MachineProfile sono definite LicenseType, OSType e Zones

  <!JEKYLL@6100@118>

  I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  <!JEKYLL@6100@119>

- Alcune proprietà sono definite in MachineProfile e alcune proprietà sono definite in CustomProperties. Inoltre, ServiceOffering non è definito. Esempio:

  * In CustomProperties è definito StorageType
  * In MachineProfile è definito LicenseType

  <!JEKYLL@6100@120>

  I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

  <!JEKYLL@6100@121>

- Se OsType e non si trova né in CustomProperties né in MachineProfile, allora:

  * Il valore viene letto dall'immagine master.
  * Se l'immagine master è un disco non gestito, OsType è impostato su Windows. Esempio:

  <!JEKYLL@6100@122>

  Il valore dell'immagine master viene scritto nelle proprietà personalizzate, in questo caso Linux.

<!JEKYLL@6100@123>

- Scenari Set-ProvScheme
  - Un catalogo esistente con:
    - CustomProperties per <!JEKYLL@6100@124> e OsType
    - MachineProfile <!JEKYLL@6100@125> che definisce le zone
  - Aggiornamenti:
    - MachineProfile mpB.vm che definisce StorageAccountType
    - Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce LicenseType e OsType

    <!JEKYLL@6100@126>

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

    <!JEKYLL@6100@127>
  - Un catalogo esistente con:
    - CustomProperties per S<!JEKYLL@6100@128> e OsType
    - MachineProfile <!JEKYLL@6100@129> che definisce StorageAccountType e LicenseType
  - Aggiornamenti:
    - Un nuovo insieme di proprietà personalizzate $CustomPropertiesB che definisce StorageAccountType e OsType.

    <!JEKYLL@6100@130>

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

    <!JEKYLL@6100@131>
  - Un catalogo esistente con:
    - CustomProperties per <!JEKYLL@6100@132> e OsType
    - MachineProfile <!JEKYLL@6100@133> che definisce le zone
  - Aggiornamenti:
    - Un MachineProfile mpB.vm che definisce StorageAccountType e LicenseType
    - <!JEKYLL@6100@134> non è specificato

    <!JEKYLL@6100@135>

    I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

    <!JEKYLL@6100@136>

Eseguire il provisioning delle macchine virtuali del catalogo con Azure Monitor Agent installato

Il monitoraggio di Azure è un servizio utilizzabile per raccogliere, analizzare e agire sui dati di telemetria dai propri ambienti Azure e locali.

L'agente di Monitoraggio di Azure (AMA) raccoglie i dati di monitoraggio da risorse di elaborazione come le macchine virtuali e li fornisce ad Azure Monitor. Attualmente supporta la raccolta di metriche Event Logs, Syslog e Performance e la invia alle fonti dati di Azure Monitor Metrics e Azure Monitor Logs.

Per abilitare il monitoraggio identificando in modo univoco le VM nei dati di monitoraggio, è possibile effettuare il provisioning delle VM di un catalogo di macchine MCS con AMA installato come estensione.

Requisiti

- Autorizzazioni: assicurarsi di disporre delle autorizzazioni minime di Azure come specificato in Autorizzazioni richieste per Azure e le seguenti autorizzazioni all'uso di Azure Monitor:
  - <!JEKYLL@6100@137>
  - <!JEKYLL@6100@138>
  - <!JEKYLL@6100@139>
  - <!JEKYLL@6100@140>
  - <!JEKYLL@6100@141>
- Regola di raccolta dati: impostare una regola di raccolta dati nel portale di Azure. Per informazioni sulla configurazione di un DCR, vedere Creare una regola di raccolta dati. Un DCR è specifico per una piattaforma (Windows o Linux). Assicurarsi di creare un DCR corretto per la piattaforma richiesta.
  L'AMA utilizza le regole di raccolta dati (DCR) per gestire la mappatura tra le risorse, quali le macchine virtuali, e le fonti di dati, quali Azure Monitor Metrics e Azure Monitor Logs.
- Area di lavoro predefinita: creare un'area di lavoro nel portale di Azure. Per informazioni sulla creazione di un'area di lavoro, vedere Creare un'area di lavoro Log Analytics. Quando si raccolgono registri e dati, le informazioni vengono archiviate in un'area di lavoro. Un'area di lavoro ha un ID dell'area di lavoro e un ID risorsa univoci. Il nome dell'area di lavoro deve essere univoco per un determinato gruppo di risorse. Dopo aver creato un'area di lavoro, configurare le fonti di dati e le soluzioni in modo che archivino i relativi dati in essa.
- L'estensione del monitor inserita nella whitelist: le estensioni <!JEKYLL@6100@142> e <!JEKYLL@6100@143> sono estensioni inserite nella whitelist definite da Citrix. Per vi-

sualizzare l'elenco delle estensioni inserite nella whitelist, utilizzare il comando PoSH <!JEKYLL@6100@144>.

- Immagine master: Microsoft consiglia di rimuovere le estensioni da una macchina esistente prima di crearne una nuova da essa. Se le estensioni non vengono rimosse, si potrebbero riscontrare file rimanenti e comportamenti imprevisti. Per ulteriori informazioni, vedere Se la macchina virtuale viene ricreata da una macchina virtuale esistente.

Per eseguire il provisioning delle VM del catalogo con AMA abilitato:

1. Configurare un modello di profilo macchina.
    - Se si desidera utilizzare una macchina virtuale come modello di profilo macchina:
        a) Creare una macchina virtuale nel portale di Azure.
        b) Accendere la VM.
        c) Aggiungere la VM alla regola di raccolta dati in **Resources**. Ciò richiama l'installazione dell'agente sulla macchina virtuale modello.

        > **Nota:**
        >
        > Se si deve creare un catalogo Linux, configurare una macchina Linux.

    - Se si desidera utilizzare una specifica di modello come modello di profilo macchina:
        a) Impostare una specifica di modello.
        b) Aggiungere la seguente associazione di regole di estensione e raccolta dati alla specifica di modello generata:

        <!JEKYLL@6100@145>

2. Creare o aggiornare un catalogo di macchine MCS esistente.
    - Per creare un nuovo catalogo MCS:
        a) Selezionare la specifica della VM o del modello come profilo macchina in Web Studio.
        b) Procedere ai passaggi successivi per creare il catalogo.
    - Per aggiornare un catalogo MCS esistente, utilizzare i seguenti comandi PoSH:
        - Per fare in modo che le nuove VM ottengano il modello di profilo macchina aggiornato, eseguire il seguente comando:

          <!JEKYLL@6100@146>

        - Per aggiornare le macchine virtuali esistenti con il modello di profilo macchina aggiornato:

          <!JEKYLL@6100@147>

3. Accendere le macchine virtuali del catalogo.
4. Passare al portale di Azure e controllare se l'estensione del monitor è installata sulla macchina virtuale e se la macchina virtuale viene visualizzata nelle risorse di DCR. Dopo alcuni minuti i dati di monitoraggio vengono visualizzati su Azure Monitor.

Risoluzione dei problemi

Per informazioni sulle linee guida alla risoluzione dei problemi per l'agente di Monitoraggio di Azure, vedere quanto segue:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Creare un catalogo di macchine con chiave di crittografia gestita dal cliente

I passaggi dettagliati per creare un catalogo di macchine con chiave di crittografia gestita dal cliente sono:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando <!JEKYLL@6100@148> per caricare i moduli PowerShell specifici di Citrix.
3. Inserire <!JEKYLL@6100@149>.
4. Inserire <!JEKYLL@6100@150>.
5. Inserire <!JEKYLL@6100@151>.
6. Immettere <!JEKYLL@6100@152> per ottenere l'elenco dei set di crittografia del disco.
7. Copiare l'ID di un set di crittografia del disco.
8. Creare una stringa di proprietà personalizzata che includa l'ID del set di crittografia del disco. Ad esempio:

   <!JEKYLL@6100@153>
9. Creare un pool di identità se non è già stato creato. Ad esempio:

   <!JEKYLL@6100@154>
10. Eseguire il comando New-ProvScheme: Ad esempio:

    <!JEKYLL@6100@155>
11. Completate la creazione del catalogo di macchine.

Creare un catalogo di macchine con doppia crittografia

È possibile creare e aggiornare un catalogo di macchine con doppia crittografia utilizzando Web Studio e i comandi PowerShell.

I passaggi dettagliati per creare un catalogo di macchine con doppia crittografia sono:

1. Creare un Azure Key Vault e DES con chiavi gestite dalla piattaforma e gestite dal cliente. Per informazioni su come creare un Azure Key Vault e un DES, vedere Usare il portale di Azure per abilitare la doppia crittografia dei dati inattivi per i dischi gestiti.
2. Per sfogliare i DiskEncryptionSet disponibili nella propria connessione di hosting:

   a) Aprire una finestra di **PowerShell**.
   b) Eseguire i seguenti comandi PowerShell:

      i. <!JEKYLL@6100@156>
      ii. <!JEKYLL@6100@157>
      iii. <!JEKYLL@6100@158>
      iv. <!JEKYLL@6100@159> (es. azure-east)
      v. <!JEKYLL@6100@160>
      vi. <!JEKYLL@6100@161>

   È possibile utilizzare un ID del <!JEKYLL@6100@162> per creare o aggiornare un catalogo utilizzando proprietà personalizzate.
3. Se si desidera utilizzare il flusso di lavoro del profilo macchina, creare una VM o una specifica di modello come input per il profilo della macchina.

   - Se si desidera utilizzare una VM come input del profilo macchina:
     a) Creare una macchina virtuale nel portale di Azure.
     b) Passare a **Dischi > Gestione delle chiavi** per crittografare la VM direttamente con qualsiasi <!JEKYLL@6100@163>.
   - Se si desidera utilizzare una specifica di modello come input del profilo della macchina:
     a) Nel modello, in <!JEKYLL@6100@164>, aggiungere il parametro <!JEKYLL@6100@165> e l'ID del DES a doppia crittografia.
4. Creare il catalogo di macchine.

   - Se si utilizza Web Studio, eseguire una delle seguenti operazioni oltre alla procedura descritta in Creare cataloghi di macchine.
     - Se non si utilizza un flusso di lavoro basato sul profilo macchina, nella pagina **Impostazioni disco** selezionare **Use the following key to encrypt data on each machine** (Usa la seguente chiave per crittografare i dati su ciascuna macchina). Quindi,

selezionare il proprio DES a doppia crittografia dal menu a discesa. Continuare a creare il catalogo.

- Se si utilizza il flusso di lavoro del profilo macchina, nella pagina **Image** selezionare un'immagine master e un profilo macchina. Assicurarsi che il profilo macchina abbia un ID set crittografia disco nelle sue proprietà.

Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

- Se si utilizlzano i comandi di PowerShell, eseguire una delle seguenti operazioni:
  - Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata <!JEKYLL@6100@166> nel comando <!JEKYLL@6100@167>. Ad esempio:

    <!JEKYLL@6100@168>

  - Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando <!JEKYLL@6100@169>. Ad esempio:

    <!JEKYLL@6100@170>

5. Completare la creazione di un catalogo utilizzando l'SDK Remote PowerShell. Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Tutte le macchine create nel catalogo sono criptate due volte dalla chiave associata al DES selezionato.

Convertire un catalogo non crittografato per utilizzare la doppia crittografia

È possibile aggiornare il tipo di crittografia di un catalogo di macchine (utilizzando proprietà personalizzate o il profilo macchina) solo se il catalogo in precedenza non era crittografato.

- Se non si utilizza un flusso di lavoro basato sul profilo macchina, aggiungere la proprietà personalizzata DiskEncryptionSetId nel comando <!JEKYLL@6100@171>. Ad esempio:

  <!JEKYLL@6100@172>

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input di profilo macchina nel comando <!JEKYLL@6100@173>. Ad esempio:

  <!JEKYLL@6100@174>

Una volta completata l'operazione, tutte le nuove macchine virtuali aggiunte al catalogo vengono crittografate due volte dalla chiave associata al DES selezionato.

Verificare che il catalogo sia crittografato con doppia crittografia

- In Web Studio:
  1. Passare a **Machine Catalogs** (Cataloghi di macchine).
  2. Selezionare il catalogo da verificare. Fare clic sulla scheda **Template Properties** (Proprietà del modello) situata nella parte inferiore dello schermo.
  3. In **Azure Details** (Dettagli di Azure) verificare l'ID del set di crittografia del disco in **Disk Encryption Set**. Se l'ID DES del catalogo è vuoto, il catalogo non è crittografato.
  4. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.
- Utilizzando i comandi PowerShell:
  1. Aprire una finestra di **PowerShell**.
  2. Eseguire il comando <!JEKYLL@6100@175> per caricare i moduli PowerShell specifici di Citrix.
  3. Utilizzare <!JEKYLL@6100@176> per ottenere le informazioni del proprio catalogo macchine. Ad esempio:

     <!JEKYLL@6100@177>
  4. Recuperare la proprietà personalizzata DES Id del catalogo di macchine. Ad esempio:

     <!JEKYLL@6100@178>
  5. Nel portale di Azure, verificare che il tipo di crittografia del DES associato all'ID DES sia costituito da chiavi gestite dalla piattaforma e dal cliente.

Creare un catalogo con dischi effimeri di Azure

Per utilizzare dischi temporanei, è necessario impostare la proprietà personalizzata <!JEKYLL@6100@179> su **true** durante l'esecuzione di <!JEKYLL@6100@180>.

> **Nota:**
>
> Se la proprietà personalizzata <!JEKYLL@6100@181> è impostata su **false** o non viene specificato un valore, tutti i VDA di cui è stato eseguito il provisioning continuano a utilizzare un disco del sistema operativo di cui è stato eseguito il provisioning.

Di seguito è riportato un esempio di set di proprietà personalizzate da utilizzare nello schema di provisioning:

<!JEKYLL@6100@182>

Configurare un disco temporaneo per un catalogo

Per configurare un disco del sistema operativo temporaneo di Azure per un catalogo, utilizzare il parametro <!JEKYLL@6100@183> in <!JEKYLL@6100@184>. Impostare il valore del parametro <!JEKYLL@6100@185> su **true**.

> **Nota:**
>
> Per utilizzare questa funzionalità, è necessario abilitare anche i parametri <!JEKYLL@6100@186> e <!JEKYLL@6100@187>.

Ad esempio:

<!JEKYLL@6100@188>

Considerazioni importanti per i dischi temporanei

Per eseguire il provisioning di dischi del sistema operativo temporanei utilizzando <!JEKYLL@6100@189>, considerare i seguenti vincoli:

- La dimensione della macchina virtuale utilizzata per il catalogo deve supportare i dischi operativi temporanei.
- La dimensione della cache o del disco temporaneo associato alla dimensione della macchina virtuale deve essere maggiore o uguale alla dimensione del disco del sistema operativo.
- La dimensione del disco temporaneo deve essere maggiore della dimensione del disco della cache.

Tenere presenti questi problemi anche quando:

- Si crea lo schema di provisioning.
- Si modifica lo schema di provisioning.
- Si aggiorna l'immagine.

Host dedicati di Azure

È possibile utilizzare MCS per eseguire il provisioning di macchine virtuali su host dedicati di Azure. Prima di eseguire il provisioning delle macchine virtuali su host dedicati di Azure:

- Creare un gruppo host.
- Creare host nel gruppo host.
- Assicurarsi che la capacità host sia sufficiente per la creazione di cataloghi e macchine virtuali.

È possibile creare un catalogo di macchine con tenancy host definita tramite il seguente script PowerShell:

<!JEKYLL@6100@190>

Quando si utilizza MCS per eseguire il provisioning di macchine virtuali su host Azure dedicati, tenere in considerazione quanto segue:

- Un *host dedicato* è una proprietà del catalogo e non può essere modificata una volta creato il catalogo. La tenancy dedicata non è attualmente supportata in Azure.
- Quando si utilizza il parametro <!JEKYLL@6100@191>, è necessario un gruppo host di Azure preconfigurato nella regione dell'unità di hosting.
- È necessario il posizionamento automatico di Azure. Questa funzionalità invia una richiesta di eseguire l'onboarding della sottoscrizione associata al gruppo host. Per ulteriori informazioni, vedere Set di scalabilità VM negli host dedicati di Azure - Anteprima pubblica. Se il posizionamento automatico non è abilitato, MCS genererà un errore durante la creazione del catalogo.

Creare o aggiornare un catalogo di macchine usando un'immagine della Raccolta di calcolo di Azure

Quando si seleziona un'immagine da utilizzare per la creazione di un catalogo delle macchine, è possibile selezionare le immagini create nella Raccolta di calcolo di Azure.

Per visualizzare queste immagini, è necessario:

1. Configurare un sito Citrix Virtual Apps and Desktops.
2. Connettersi ad Azure Resource Manager.
3. Nel portale di Azure, creare un gruppo di risorse. Per ulteriori informazioni, vedere Creare una raccolta per l'archiviazione e la condivisione delle risorse.
4. Nel gruppo di risorse, creare una Raccolta di calcolo di Azure.
5. Nella Raccolta di calcolo di Azure, creare una definizione di immagine.
6. Nella definizione dell'immagine, creare una versione dell'immagine.

Usa i seguenti comandi PowerShell per creare o aggiornare un catalogo di macchine utilizzando un'immagine tratta dalla Raccolta di calcolo di Azure:

1. Aprire una finestra di PowerShell.
2. Eseguire il comando <!JEKYLL@6100@192> per caricare i moduli PowerShell specifici di Citrix.
3. Selezionare un gruppo di risorse, quindi elencare tutte le gallerie di quel gruppo di risorse.

   <!JEKYLL@6100@193>
4. Selezionare una raccolta, quindi elencare tutte le definizioni delle immagini di quella raccolta.

   <!JEKYLL@6100@194>

5. Selezionare una definizione di immagine, quindi elencare tutte le versioni dell'immagine in questione.

   <!JEKYLL@6100@195>

6. Creare e aggiornare un catalogo MCS utilizzando i seguenti elementi:

   - Gruppo di risorse
   - Raccolta
   - Definizione delle immagini della raccolta
   - Versione delle immagini della raccolta.

   Per informazioni su come creare un catalogo utilizzando l'SDK Remote PowerShell, vedere https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Configurare la Raccolta immagini condivise

Utilizzare il comando <!JEKYLL@6100@196> per creare uno schema di provisioning con il supporto della Raccolta immagini condivise. Utilizzare il comando <!JEKYLL@6100@197> per abilitare o disabilitare questa funzionalità per uno schema di provisioning e per modificare il rapporto di replica e i valori massimi della replica.

Sono state aggiunte tre proprietà personalizzate agli schemi di provisioning per supportare la funzionalità Raccolta immagini condivise:

<!JEKYLL@6100@198>

- Definisce se utilizzare la Raccolta immagini condivise per archiviare le immagini pubblicate. Se impostata su **True**, l'immagine viene memorizzata come immagine della Raccolta immagini condivise, altrimenti viene memorizzata come snapshot.
- I valori validi sono **True** e **False**.
- Se la proprietà non è definita, il valore predefinito è **False**.

<!JEKYLL@6100@199>

- Definisce il rapporto tra macchine e repliche di versioni di immagini della raccolta.
- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, vengono utilizzati i valori predefiniti. Il valore predefinito per i dischi del sistema operativo persistenti è 1.000 e il valore predefinito per i dischi del sistema operativo non persistenti è 40.

<!JEKYLL@6100@200>

- Definisce il numero massimo di repliche per ogni versione dell'immagine della raccolta.

- I valori validi sono numeri interi maggiori di 0.
- Se la proprietà non è definita, il valore predefinito è 10.
- Azure attualmente supporta fino a 10 repliche per una singola versione dell'immagine della raccolta. Se la proprietà è impostata su un valore maggiore di quello supportato da Azure, MCS tenta di utilizzare il valore specificato. Azure genera un errore, che viene registrato da MCS, e lascia invariato il numero di repliche corrente.

> **Suggerimento:**
>
> Quando si utilizza la Raccolta immagini condivise per archiviare un'immagine pubblicata per i cataloghi di cui è stato eseguito il provisioning con MCS, MCS imposta il numero di repliche delle versioni delle immagini della raccolta in base al numero di macchine nel catalogo, al rapporto di replica e al numero massimo di repliche. Il conteggio delle repliche viene calcolato dividendo il numero di macchine nel catalogo per il rapporto di replica (arrotondando per eccesso al valore intero più vicino) e quindi limitando il valore al numero massimo di repliche. Ad esempio, con un rapporto di replica di 20 e un massimo di 5, per 0-20 macchine viene creata una replica, per 21-40 macchine vengono create 2 repliche, per 41-60 macchine vengono create 3 repliche, per 61-80 macchine vengono create 4 repliche e per 81 macchine o più vengono create 5 repliche.

Caso d'uso: aggiornamento del rapporto di replica e della replica massima della Raccolta immagini condivise

Il catalogo delle macchine esistente utilizza la Raccolta immagini condivise. Utilizzare il comando <!JEKYLL@6100@201> per aggiornare le proprietà personalizzate per tutte le macchine esistenti nel catalogo e per tutte le macchine future:

<!JEKYLL@6100@202>

Caso d'uso: conversione di un catalogo di snapshot in un catalogo della Raccolta immagini condivise

Per questo caso d'uso:

1. Eseguire <!JEKYLL@6100@203> con il contrassegno <!JEKYLL@6100@204> impostato su **True**. Facoltativamente, includere le proprietà <!JEKYLL@6100@205> e <!JEKYLL@6100@206>.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

<!JEKYLL@6100@207>

> **Suggerimento:**
>
> I parametri <!JEKYLL@6100@208> e <!JEKYLL@6100@209> non sono richiesti. Al completamento del comando <!JEKYLL@6100@210>, l'immagine della Raccolta immagini condivise non è stata ancora creata. Una volta configurato il catalogo per l'utilizzo della raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata nella raccolta. Il comando di aggiornamento del catalogo crea la raccolta, l'immagine della raccolta e la versione dell'immagine. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto il conteggio delle repliche viene aggiornato, se appropriato. Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando l'immagine della Raccolta immagini condivise e tutte le macchine di cui è stato eseguito il provisioning vengono create utilizzando l'immagine. La vecchia snapshot viene ripulita automaticamente entro poche ore.

Caso d'uso: conversione di un catalogo della Raccolta immagini condivise in un catalogo di snapshot

Per questo caso d'uso:

1. Eseguire <!JEKYLL@6100@211> con il contrassegno <!JEKYLL@6100@212> impostato su **False** o non definito.
2. Aggiornare il catalogo.
3. Spegnere e riaccendere le macchine per forzare un aggiornamento.

Ad esempio:

<!JEKYLL@6100@213>

> **Suggerimento:**
>
> A differenza dell'aggiornamento da una snapshot a un catalogo della Raccolta immagini condivise, i dati personalizzati per ogni macchina non sono ancora aggiornati per riflettere le nuove proprietà personalizzate. Eseguire il comando seguente per visualizzare le proprietà personalizzate originali della Raccolta immagini condivise: <!JEKYLL@6100@214>. Dopo il completamento del comando <!JEKYLL@6100@215>, la snapshot dell'immagine non è stata ancora creata. Una volta configurato il catalogo per non utilizzare la raccolta, la successiva operazione di aggiornamento del catalogo memorizza l'immagine pubblicata come snapshot. Da quel momento, tutte le macchine non persistenti esistenti vengono reimpostate utilizzando la snapshot e tutte le macchine di cui è stato eseguito il provisioning vengono create dalla snapshot. Lo spegnimento e la riaccensione delle macchine le aggiorna, a quel punto i dati della macchina personalizzati vengono aggiornati per riflettere che <!JEKYLL@6100@216> è impostato su **False**. Le vecchie risorse della Raccolta immagini condivise (raccolta, immagine e versione) vengono ripulite automaticamente nel giro di poche ore.

Eseguire il provisioning delle macchine in zone di disponibilità specificate

È possibile effettuare il provisioning delle macchine in zone di disponibilità specifiche in ambienti Azure. È possibile raggiungere questo obiettivo utilizzando PowerShell.

> **Nota:**
>
> Se non viene specificata alcuna zona, MCS consente ad Azure di posizionare le macchine all'interno della regione. Se viene specificata più di una zona, MCS distribuisce in modo casuale le macchine nelle zone.

Configurare le zone di disponibilità tramite PowerShell

Utilizzando PowerShell, è possibile visualizzare gli articoli di inventario offerti utilizzando <!JEKYLL@6100@217>. Ad esempio, per visualizzare l'offerta di servizi *Eastern US region* <!JEKYLL@6100@218> (Regione degli Stati Uniti orientali):

<!JEKYLL@6100@219>

Per visualizzare le zone, utilizzare il parametro <!JEKYLL@6100@220> per l'elemento:

<!JEKYLL@6100@221>

Se le zone di disponibilità non sono specificate, non vi è alcun cambiamento nel modo in cui viene eseguito il provisioning delle macchine.

Per configurare le zone di disponibilità tramite PowerShell, utilizzare la proprietà personalizzata **Zones** (Zone) disponibile con l'operazione <!JEKYLL@6100@222>. La proprietà **Zones** (Zone) definisce un elenco di zone di disponibilità in cui eseguire il provisioning delle macchine. Tali zone possono includere una o più zone di disponibilità. Ad esempio, <!JEKYLL@6100@223> per le zone 1 e 3.

Utilizzare il comando <!JEKYLL@6100@224> per aggiornare le zone per uno schema di provisioning.

Se viene fornita una zona non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore che fornisce istruzioni su come correggere il comando non valido.

> **Suggerimento:**
>
> Se si specifica una proprietà personalizzata non valida, lo schema di provisioning non viene aggiornato e viene visualizzato un messaggio di errore pertinente.

Tipologie di archiviazione

Selezionare diversi tipi di archiviazione per le macchine virtuali negli ambienti di Azure che utilizzano MCS. Per le macchine virtuali di destinazione, MCS supporta:

- Disco del sistema operativo: SSD premium, SSD o HDD
- Disco della cache write-back: SSD premium, SSD o HDD

Quando si utilizzano questi tipi di archiviazione, considerare quanto segue:

- Assicurarsi che la macchina virtuale supporti il tipo di archiviazione selezionato.
- Se la configurazione utilizza un disco temporaneo di Azure, non è disponibile l'opzione per l'impostazione del disco della cache write-back.

> **Suggerimento:**
>
> <!JEKYLL@6100@225> è configurato per un tipo di sistema operativo e un account di archiviazione. <!JEKYLL@6100@226> è configurato per il tipo di archiviazione della cache write-back. Per un catalogo normale, è necessario <!JEKYLL@6100@227>. Se <!JEKYLL@6100@228> non è configurato, <!JEKYLL@6100@229> viene utilizzato come impostazione predefinita per <!JEKYLL@6100@230>.

Se WBCDiskStorageType non è configurato, StorageType viene utilizzato come impostazione predefinita per WBCDiskStorageType.

Configurare i tipi di archiviazione

Per configurare i tipi di archiviazione per le macchine virtuali, utilizzare il parametro <!JEKYLL@6100@231> in <!JEKYLL@6100@232>. Impostare il valore del parametro <!JEKYLL@6100@233> su uno dei tipi di archiviazione supportati.

Di seguito è riportato un set di esempio del parametro <!JEKYLL@6100@234> in uno schema di provisioning:

<!JEKYLL@6100@235>

Abilitare l'archiviazione con ridondanza della zona

È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione del catalogo. Replica il disco gestito di Azure in modo sincrono in più zone di disponibilità, il che consente di effettuare il ripristino dopo che si è verificato un errore in una zona utilizzando la ridondanza di altre.

È possibile specificare **Premium_ZRS** e **StandardSSD_ZRS** nelle proprietà personalizzate del tipo di archiviazione. L'archiviazione ZRS può essere impostata utilizzando le proprietà personalizzate esistenti o tramite il modello **MachineProfile**. L'archiviazione ZRS è supportata anche con il comando <!JEKYLL@6100@236> accompagnato dai parametri <!JEKYLL@6100@237> e <!JEKYLL@6100@238>, ed è possibile modificare il computer esistente dall'archiviazione LRS a quello ZRS.

Limitazioni:

- Supportato solo nei dischi gestiti
- Supportato solo se si utilizzano unità a stato solido (SSD) premium e standard
- Non supportato in <!JEKYLL@6100@239>
- Disponibile solo in alcune aree geografiche.
- Le prestazioni di Azure diminuiscono quando si creano dischi ZRS su larga scala. Pertanto, alla prima accensione, accendere le macchine in batch più piccoli (meno di 300 macchine alla volta)

Imposta l'archiviazione con ridondanza della zona come tipo di archiviazione su disco È possibile selezionare l'archiviazione con ridondanza della zona durante la creazione iniziale del catalogo oppure aggiornare il tipo di archiviazione in un catalogo esistente.

Seleziona l'archiviazione con ridondanza della zona utilizzando i comandi PowerShell Quando si crea un nuovo catalogo in Azure usando il comando <!JEKYLL@6100@240> di PowerShell, utilizzare il valore <!JEKYLL@6100@241> in <!JEKYLL@6100@242>.
Ad esempio:

<!JEKYLL@6100@243>

Quando lo si imposta, questo valore viene convalidato da un'API dinamica che determina se può essere utilizzato correttamente. Le seguenti eccezioni possono verificarsi se l'uso di ZRS non è valido per il proprio catalogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: la proprietà personalizzata StorageTypeAtShutdown non può essere utilizzata con l'archiviazione ZRS.
- **StorageAccountTypeNotSupportedInRegion**: questa eccezione si verifica se si tenta di utilizzare l'archiviazione ZRS in un'area di Azure che non supporta ZRS
- **ZrsRequiresManagedDisks**: è possibile utilizzare l'archiviazione con ridondanza della zona solo con dischi gestiti.

È possibile impostare il tipo di archiviazione su disco utilizzando le seguenti proprietà personalizzate:

- <!JEKYLL@6100@244>
- <!JEKYLL@6100@245>
- <!JEKYLL@6100@246>

> **Nota:**
>
> Durante la creazione del catalogo, viene utilizzato il disco del sistema operativo del profilo macchina <!JEKYLL@6100@247> se non sono impostate le proprietà personalizzate.

Acquisire le impostazioni diagnostiche su VM e NIC da un profilo macchina

È possibile acquisire le impostazioni diagnostiche su VM e NIC da un profilo macchina durante la creazione di un catalogo di macchine, l'aggiornamento di un catalogo di macchine esistente e l'aggiornamento delle macchine virtuali esistenti.

È possibile creare una specifica di VM o di modello come origine del profilo macchina.

Passaggi chiave

1. Configurare gli ID richiesti in Azure. È necessario fornire questi ID nella specifica del modello.
    - Account di archiviazione
    - Area di lavoro per l'analisi dei log
    - Spazio dei nomi dell'hub degli eventi con prezzi di livello standard
2. Creare un'origine del profilo macchina.
3. Creare un nuovo catalogo di macchine, aggiornare un catalogo esistente o aggiornare le VM esistenti.

Configurare gli ID richiesti in Azure

Configurare una delle seguenti opzioni in Azure:

- Account di archiviazione
- Area di lavoro per l'analisi dei log
- Spazio dei nomi dell'hub degli eventi con prezzi di livello Standard

Configurare un account di archiviazione Creare un account di archiviazione standard in Azure. Nelle specifiche del modello, inserire il resourceID completo per l'account di archiviazione come. <!JEKYLL@6100@248>

Una volta che le VM sono configurate per registrare i dati nell'account di archiviazione, i dati sono reperibili nel contenitore <!JEKYLL@6100@249>.

Configurare uno spazio di lavoro per l'analisi dei log Creare un'area di lavoro per l'analisi dei log. Nelle specifiche del modello, specificare il resourceID completo per l'area di lavoro di analisi dei log come workspaceID.

Una volta che le macchine virtuali sono configurate per registrare i dati nell'area di lavoro, i dati possono essere sottoposti a query in Logs all'interno di Azure. È possibile eseguire il seguente comando in Logs all'interno di Azure per mostrare il conteggio di tutte le metriche registrate da una risorsa:

'AzureMetrics

Configurare un hub per eventi Effettuare le seguenti operazioni per configurare un hub di eventi nel portale di Azure:

1. Creare un spazio dei nomi per l'hub degli eventi con i prezzi di livello standard.
2. Creare un hub di eventi sotto lo spazio dei nomi.
3. Passare a **Capture** nell'hub degli eventi. Impostare lo switch su ON per acquisire con il tipo di output Avro.
4. Creare un nuovo contenitore in un account di archiviazione esistente per acquisire i log.
5. Nelle specifiche del modello, specificare `eventHubAuthorizationRuleId` nel formato seguente: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Specificare il nome dell'hub degli eventi.

Una volta che le VM sono configurate per registrare i dati nell'hub degli eventi, i dati vengono acquisiti nel contenitore di archiviazione configurato.

Creare un'origine di profilo macchina

È possibile creare una specifica di VM o di modello come origine del profilo macchina.

Creare un profilo macchina basato su VM con impostazioni diagnostiche Se si desidera creare una VM come profilo macchina, configurare prima le impostazioni di diagnostica sulla VM modello stessa. È possibile fare riferimento alle istruzioni dettagliate fornite nella documentazione Microsoft Impostazioni di diagnostica in Monitoraggio di Azure.

È possibile eseguire i seguenti comandi per verificare che siano presenti impostazioni diagnostiche associate alla VM o alla NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

Creare un profilo macchina basato su specifica di modello con impostazioni diagnostiche Se si desidera utilizzare una macchina virtuale con impostazioni di diagnostica già abilitate ed esportarla in

una specifica di modello ARM, queste impostazioni non verranno incluse automaticamente nel modello. È necessario aggiungere o modificare manualmente le impostazioni diagnostiche all'interno del modello ARM.

Tuttavia, se si desidera una macchina virtuale come profilo macchina, MCS garantisce che le impostazioni diagnostiche critiche vengano acquisite e applicate con precisione alle risorse all'interno del catalogo MCS.

1. Creare una specifica di modello standard che definisca una VM e una o più NIC.
2. Aggiungere risorse aggiuntive per distribuire le impostazioni di diagnostica in base alle specifiche: Microsoft.InsightsDiagnosticSettings. Per l'ambito, fare riferimento a una VM o a una NIC presente nel modello per nome con un ID parziale. Ad esempio, per creare impostazioni diagnostiche collegate a una VM denominata test-VM nelle specifiche del modello, specificare l'ambito come:

   ```
   1 "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. Usare le specifiche del modello come origine del profilo macchina.

Creare o aggiornare un catalogo con impostazioni diagnostiche

Dopo aver creato un'origine del profilo macchina, è ora possibile creare un catalogo di macchine mediante il comando `New-ProvScheme`, aggiornare un catalogo di macchine esistente mediante il comando `Set-ProvScheme` e aggiornare le VM esistenti mediante il comando `Request-ProvVMUpdate`.

Posizione del file di paging

Negli ambienti Azure, il file di paging viene impostato in una posizione appropriata al momento della creazione della macchina virtuale. L'impostazione del file di paging è configurata nel formato `<page file location>[min size] [max size]` (la dimensione è in MB). Per ulteriori informazioni, vedere il documento Microsoft Come determinare le dimensioni del file di paging appropriate.

Quando si crea `ProvScheme` durante la preparazione dell'immagine, MCS determina la posizione del file di paging in base a determinate regole. Dopo aver creato `ProvScheme`:

- La modifica delle dimensioni della macchina virtuale viene bloccata se la dimensione della macchina virtuale in ingresso causa una diversa impostazione del file di paging.
- L'aggiornamento del profilo macchina viene bloccato se la gamma di servizi offerti viene modificata a causa dell'aggiornamento del profilo macchina che determina una diversa impostazione del file di paging.

- Le proprietà del disco operativo effimero (EOS) e di MCSIO non possono essere modificate.

Determinazione della posizione del file di paging

Le funzionalità come EOS e MCSIO hanno la propria posizione prevista per il file di paging e si escludono a vicenda. La tabella mostra la posizione prevista del file di paging per ciascuna funzione:

Funzione	Posizione prevista del file di paging
EOS	Disco del sistema operativo
MCSIO	Prima il disco temporaneo di Azure, altrimenti il Disco cache di write-back

> **Nota:**
>
> Anche se la preparazione dell'immagine è disaccoppiata dalla creazione dello schema di provisioning, MCS determina correttamente la posizione del file di paging. Il percorso predefinito del file di paging è sul disco del sistema operativo.

Scenari di configurazione del file di paging

La tabella descrive alcuni possibili scenari di configurazione del file di paging durante la preparazione dell'immagine e l'aggiornamento dello schema di provisioning:

Durante	Scenario	Risultato
Preparazione delle immagini	Il file di paging dell'immagine di origine è impostato sul disco temporaneo, mentre la dimensione della macchina virtuale specificata nello schema di provisioning non ha un disco temporaneo	Il file di paging viene inserito nel disco del sistema operativo
Preparazione delle immagini	Il file di paging dell'immagine di origine è impostato sul disco del sistema operativo, mentre la dimensione della macchina virtuale specificata nello schema di provisioning ha un disco temporaneo.	Il file di paging viene inserito nel disco temporaneo

Durante	Scenario	Risultato
Preparazione delle immagini	Il file di paging dell'immagine di origine è impostato sul disco temporaneo, mentre il disco temporaneo del sistema operativo è abilitato nello schema di provisioning.	Il file di paging viene inserito nel disco del sistema operativo
Aggiornamento dello schema di provisioning	Si tenta di aggiornare lo schema di provisioning, la dimensione originale della macchina virtuale ha un disco temporaneo e la macchina virtuale di destinazione non ha alcun disco temporaneo.	Rifiuta la modifica con un messaggio di errore
Aggiornamento dello schema di provisioning	Si tenta di aggiornare lo schema di provisioning, la dimensione originale della macchina virtuale non ha un disco temporaneo e la macchina virtuale di destinazione ha un disco temporaneo	Rifiuta la modifica con un messaggio di errore

Aggiornare le impostazioni del file di paging

È inoltre possibile specificare l'impostazione del file di paging, inclusa la posizione e le dimensioni, utilizzando il comando PowerShell in modo esplicito. Questo sostituisce il valore determinato da MCS. È possibile farlo eseguendo il comando `New-ProvScheme` e includendo le seguenti proprietà personalizzate:

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

Esempio di utilizzo delle proprietà personalizzate:

```
1 -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
```



```
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
</CustomProperties>'
```

Vincoli:

- È possibile aggiornare l'impostazione del file di paging solo quando si crea lo schema di provisioning eseguendo il comando `New-ProvScheme` e l'impostazione del file di paging non può essere modificata in seguito.
- Fornire tutte le proprietà relative dell'impostazione del file di paging (`PageFileDiskDriveLetterOver` , `InitialPageFileSizeInMB` e `MaxPageFileSizeInMB`) nelle proprietà personalizzate o non fornire alcuna di esse.
- La dimensione iniziale del file di paging deve essere compresa tra 16 MB e 16777216 MB.
- La dimensione massima del file di paging deve essere maggiore o uguale alla dimensione iniziale del file di paging e inferiore a 16777216 MB.
- Questa funzione non è supportata in Web Studio.

Creare un catalogo usando le macchine virtuali Azure Spot

Le macchine virtuali Azure Spot consentono di sfruttare la capacità di elaborazione inutilizzata di Azure con un notevole risparmio sui costi. Tuttavia, la capacità di allocare una macchina virtuale Azure Spot dipende dalla capacità e dai prezzi attuali. Pertanto, Azure potrebbe eliminare la macchina virtuale in esecuzione, non riuscire a creare la macchina virtuale o non riuscire ad accenderla secondo il criterio di sfratto. Pertanto, le macchine virtuali Azure Spot sono adatte per alcune applicazioni e desktop non critici. Per ulteriori informazioni, vedere Usare macchine virtuali Azure Spot.

Limitazioni

- Non tutte le dimensioni delle macchine virtuali sono supportate per le macchine virtuali Azure Spot. Per maggiori informazioni, vedere Limiti.

  È possibile eseguire il seguente comando PowerShell per verificare se una dimensione di VM supporta o meno le VM Spot. Se la dimensione di una VM supporta le VM Spot,

`SupportsSpotVM` è **True**.

```
(Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
   folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
```

- Attualmente, le macchine virtuali Azure Spot non supportano l'ibernazione.

Requisito

Durante la creazione dell'origine del profilo macchina (VM o specifica del modello) per il catalogo delle macchine virtuali Azure Spot, è necessario selezionare l'istanza Azure Spot (se si usa una macchina virtuale) o impostare `priority`su `Spot` (se si usa la specifica del modello).

Passaggi per creare un catalogo utilizzando le macchine virtuali Azure Spot

1. Creare un'oriine di profilo macchina (VM o modello di avvio).
   - Per creare una macchina virtuale usando il portale di Azure, vedere Distribuire macchine virtuali Azure Spot usando il portale di Azure.
   - Per creare una specifica del modello, aggiungere le seguenti proprietà in **resources > type: Microsoft.Compute/virtualMachines > properties** nella specifica del modello. Ad esempio:

```
"priority": "Spot",
"evictionPolicy": "Deallocate",
"billingProfile": {

"maxPrice": 0.01
 }
```

> **Nota:**
>
> - Il criterio di sfratto può essere **Deallocate** (Rimuovi allocazione) o **Delete** (Elimina).
>   - Nel caso delle VM non persistenti, MCS imposta sempre il criterio di sfratto su **Delete**. Se viene sfrattata, la VM viene eliminata insieme a tutti i dischi non persistenti (ad esempio, il disco del sistema operativo). Tutti i dischi persistenti (ad esempio, il disco di identità) non vengono eliminati. Tuttavia, un disco del sistema operativo è persistente se il tipo di catalogo è persistente o la proprietà personalizzata`PersistOsDisk` è impostata su True. Analogamente, un disco WBC è persistente se la proprietà personalizzata `PersistWbc` è impostata su **True**.
>   - Nel caso delle VM persistenti, MCS imposta sempre il criterio di sfratto su Deallocate. Se la VM viene sfrattata, ne viene rimossa l'allocazione. Non viene apportata alcuna modifica ai dischi.

> - Il prezzo massimo è il prezzo che si è disposti a pagare all'ora. Se si sta usando **Capacity Only** (Solo capacità), questo è **-1**. Il prezzo massimo può essere solo nullo, -1 o un numero decimale maggiore di zero. Per ulteriori informazioni, vedere Prezzi.

2. È possibile eseguire il seguente comando PowerShell per verificare se un profilo macchina è abilitato o meno alla macchina virtuale Azure Spot. Se il parametro `SpotEnabled` è **True** e `SpotEvictionPolicy` è impostato su **Deallocate** o **Delete**, il profilo della macchina è abilitato per la macchina virtuale Azure Spot. Ad esempio,

   - Se l'origine del profilo della macchina è una VM, eseguire il comando seguente:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
       AdditionalData
   ```

   - Se l'origine del profilo macchina è una specifica di modello, eseguire il comando seguente:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
       templatespec\14.0.0-spot-delete.templatespecversion").
       AdditionalData
   ```

3. Creare un catalogo di macchine utilizzando un profilo macchina con il comando PowerShell `New-ProvScheme`.

È possibile aggiornare un catalogo utilizzando il comando `Set-ProvScheme`. È inoltre possibile aggiornare le VM esistenti utilizzando il comando PowerShell `Set-ProvVmUpdateTimeWindow`. Il profilo della macchina viene aggiornato alla successiva accensione.

Sfratti su una macchina virtuale Azure Spot in esecuzione

Se la capacità di calcolo non è disponibile o il prezzo orario è superiore al prezzo massimo configurato, Azure sfratta una macchina virtuale Spot in esecuzione. Per impostazione predefinita, non viene notificato lo sfratto. La VM semplicemente si blocca e viene sfrattata. Microsoft consiglia di utilizzare gli eventi pianificati per monitorare gli sfratti. Vedere Monitoraggio continuo degli sfratti. È possibile anche eseguire script dall'interno di una VM per ricevere una notifica prima dello sfratto. Ad esempio, Microsoft ha uno script di polling in Python denominato ScheduledEvents.cs.

Risoluzione dei problemi

- È possibile visualizzare le proprietà della VM Spot nei customMachineData della VM di cui è stato eseguito il provisioning utilizzando il comando `Get-ProvVM`. Se il campo di priorità è impostato su **Spot**, allora Spot è in uso.

- È possibile verificare se una macchina virtuale utilizza Spot nel portale di Azure:
  1. Trovare la macchina virtuale nel portale di Azure.
  2. Passare alla pagina **Overview** (Panoramica).
  3. Scorrere verso il basso e individuare la sezione **Azure Spot**.
     - Se Spot non è in uso, questo campo è vuoto.
     - Se Spot è in uso, vengono impostati i campi **Azure Spot** e **Azure Spot eviction policy** (Criterio di sfratto di Azure Spot).

1. È possibile controllare il profilo di fatturazione o il prezzo massimo orario per la VM nella pagina di configurazione.

Configurare le dimensioni delle VM di backup

A volte i cloud pubblici possono esaurire la capacità per una specifica dimensione di VM. Inoltre, se si utilizzano macchine virtuali Azure Spot, le macchine virtuali vengono sfrattate in qualsiasi momento in base alle esigenze di capacità di Azure. In questo caso di capacità insufficiente su Azure o su una macchina virtuale Spot in caso di guasto, MCS effettua il fallback alle dimensioni delle VM di backup. È possibile fornire un elenco delle dimensioni delle VM di backup utilizzando una proprietà personalizzata `BackupVmConfiguration` durante la creazione o l'aggiornamento di un catalogo di macchine MCS. MCS tenta di ricorrere alle dimensioni delle VM di backup nell'ordine fornito dall'utente nell'elenco.

MCS, quando utilizza una particolare configurazione di backup per la VM, continua a utilizzare tale configurazione fino al successivo arresto. Alla successiva accensione, MCS tenta di avviare la configurazione primaria della VM. In caso di errore, MCS tenta nuovamente di avviare una configurazione delle dimensioni della VM di backup come indicato nell'elenco.

Questa funzionalità è supportata su:

- un catalogo che utilizza un profilo macchina
- i cataloghi di macchine MCS persistenti e non persistenti
- Ambienti Azure attualmente

Considerazioni importanti

- È possibile fornire più di una dimensione di VM di backup nell'elenco.
- L'elenco deve essere univoco.
- È possibile aggiungere la proprietà del tipo di istanza per ciascuna delle VM nell'elenco. Il tipo è **Spot** o **Regular**. Se il tipo non è specificato, MCS considera la VM **Regular**.

- È possibile modificare l'elenco delle dimensioni delle VM di backup di un catalogo esistente utilizzando i comandi PowerShell `Set-ProvScheme`.
- È possibile aggiornare le VM esistenti create dallo schema di provisioning associato al catalogo utilizzando il comando `Set-ProvVMUpdateTimeWindow`.
- È possibile configurare l'elenco delle dimensioni delle VM di backup per un numero selezionato di VM MCS esistenti utilizzando il comando `Set-ProvVM`. Tuttavia, per applicare gli aggiornamenti, impostare una finestra temporale di aggiornamento per le VM che utilizzano `Set-ProvVMUpdateTimeWindow` e avviare le VM all'interno di quella finestra. Se il comando `Set-ProvVm` viene utilizzato su una VM, la VM continua a utilizzare l'elenco delle dimensioni delle VM di backup impostato su quella particolare VM anche se l'elenco sullo schema di provisioning viene successivamente aggiornato. È possibile utilizzare `Set-ProvVM` con `-RevertToProvSchemeConfiguration` per fare in modo che la VM utilizzi l'elenco di backup contenuto nello schema di provisioning.

Creare un catalogo con le dimensioni delle VM di backup

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Creare un catalogo di broker. Questo catalogo è popolato da macchine che stanno per essere create.
4. Creare un pool di identità. Questo diventa un contenitore per gli account AD creati per le macchine da creare.
5. Creare uno schema di provisioning con il profilo macchina. Ad esempio:

    - Se si desidera fornire un elenco delle sole dimensioni normali delle VM, eseguire i seguenti comandi:

```
1  New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
       MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
       folder\helenli.resourcegroup\helenli-master1-mcsio-
       snapshot.snapshot"
2  -CustomProperties
3  "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
       machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/
       XMLSchema-instance`">
4  <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`
       " Value=`"true`" />
5  <Property xsi:type=`"StringProperty`" Name=`"
       StorageAccountType`" Value=`"Premium_LRS`" />
6  <Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
       Value=`"Windows_Server`"/>
7  <Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
       Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
```



```
        Name=`"BackupVmConfiguration`" Value=`"['ServiceOffering':
         'Standard_D2as_v4', 'ServiceOffering': 'Standard_D2s_v3',
         'ServiceOffering': 'C']`"/>
8   </CustomProperties>"
```

- Se si desidera fornire un elenco di VM di dimensioni miste (VM normali e Spot), eseguire i seguenti comandi:

```
1   New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
       MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
       folder\helenli.resourcegroup\helenli-master1-mcsio-
       snapshot.snapshot"
2   -CustomProperties
3   "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
       machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/
       XMLSchema-instance`">
4   <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`
       " Value=`"true`" />
5   <Property xsi:type=`"StringProperty`" Name=`"
       StorageAccountType`" Value=`"Premium_LRS`" />
6   <Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
       Value=`"Windows_Server`"/>
7   <Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
       Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
       Name=`"BackupVmConfiguration`" Value=`"[{
8   'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
9   , {
10  'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
11  , {
12  'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
13  ]`"/>
14  </CustomProperties>"
```

6. Aggiornare il BrokerCatalog con l'ID univoco dello schema di provisioning.
7. Creare e aggiungere VM al catalogo.

Aggiornare un catalogo esistente

È possibile aggiornare uno schema di provisioning utilizzando il comando `Set-ProvScheme`. Ad esempio:

```
1   Set-ProvScheme -ProvisioningSchemeName "azure-catalog"
2   -CustomProperties
3   "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
       machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
       instance`">
4   <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
       true`" />
5   <Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value
       =`"Premium_LRS`" />
```



```
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
    Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
    "/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
    Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```

Aggiornare le macchine virtuali esistenti

È possibile aggiornare le VM esistenti di un catalogo utilizzando il comando PowerShell `Set-ProvVMUpdateTimeWindow`. Il comando aggiorna le VM create dallo schema di provisioning associato al catalogo alla successiva accensione entro la finestra temporale specificata. Ad esempio:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am"-DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **Nota:**
>
> `StartsNow` indica l'ora di inizio pianificata. `DurationInMinutes` è la finestra temporale programmata.

È possibile configurare l'elenco delle dimensioni delle VM di backup per un numero selezionato di VM MCS esistenti utilizzando il comando `Set-ProvVM`. Tuttavia, per applicare gli aggiornamenti, impostare una finestra temporale di aggiornamento per le VM che utilizzano `Set-ProvVMUpdateTimeWindow` e avviare le VM all'interno di quella finestra. Ad esempio:

1. Esegui il `Set-ProvVM` comando per configurare l'elenco delle dimensioni delle VM di backup per una VM MCS esistente selezionata. Ad esempio:

```
Set-ProvVM -VMName "Vm-001"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
```



```
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
    Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`
    "Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    true`"/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration
    `" Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```

2. Eseguire il comando `Set-ProvVMUpdateTimeWindow` per applicare gli aggiornamenti. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    StartsNow -DurationInMinutes 60
```

Copiare i tag su tutte le risorse

È possibile copiare i tag specificati in un profilo macchina per tutte le risorse, ad esempio più NIC e dischi (disco del sistema operativo, disco di identità e disco della cache di write-back) di una nuova macchina virtuale o di una macchina virtuale esistente inclusa in un catalogo di macchine. L'origine del profilo macchina può essere una VM o una specifica di modello ARM.

> **Nota:**
>
> È necessario aggiungere il criterio sui tag (vedere Assegnare definizioni di criteri per la conformità dei tag) o aggiungere i tag in un'origine del profilo della macchina per conservare i tag sulle risorse.

Prerequisiti

Creare l'origine del profilo macchina (VM o specifica di modello ARM) per avere tag sulle VM, sui dischi e le NIC di quella VM.

- Se si desidera avere una macchina virtuale come input del profilo macchina, applicare i tag sulla macchina virtuale e su tutte le risorse nel portale di Azure. Vedere Applicare i tag con il portale di Azure.
- Se si desidera utilizzare le specifiche di modello ARM come input del profilo macchina, aggiungere il seguente blocco di tag sotto ogni risorsa.


```
 "tags": {

"TagC": "Value3"
 }
,
```

> **Nota:**
>
> È possibile avere un massimo di un disco e almeno una NIC nella specifica di modello.

Copiare i tag nelle risorse di una macchina virtuale in un nuovo catalogo di macchine

1. Creare un catalogo non persistente o persistente con una macchina virtuale o una specifica di modello ARM come input del profilo macchina.
2. Aggiungere una macchina virtuale al catalogo e accenderla. È necessario vedere che i tag specificati nel profilo della macchina sono stati copiati nelle risorse corrispondenti di quella VM.

   > **Nota:**
   >
   > Viene visualizzato un errore se c'è una mancata corrispondenza tra il numero di NIC fornite nel profilo del computer e il numero di NIC che si desidera che le macchine virtuali utilizzino.

Modificare i tag sulle risorse di una macchina virtuale esistente

1. Creare un profilo macchina con i tag su tutte le risorse.
2. Aggiornare il catalogo macchine esistente con il profilo macchina aggiornato. Ad esempio:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
```

3. Disattivare la macchina virtuale a cui si intende applicare gli aggiornamenti.
4. Richiedere un aggiornamento pianificato per la macchina virtuale. Ad esempio:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
```

5. Accendere la VM.
6. È necessario vedere che i tag specificati nel profilo della macchina sono stati copiati nelle risorse corrispondenti.

> **Nota:**
>
> Viene visualizzato un errore se c'è una mancata corrispondenza tra il numero di NIC fornite nel profilo macchina e il numero di NIC fornite in `Set-ProvScheme`.

Passaggi successivi

- Se questo è il primo catalogo creato, Web Studio guida l'utente a creare gruppi di consegna
- Per rivedere l'intero processo di configurazione, vedere Installazione e configurazione
- Per informazioni su come gestire i cataloghi, vedere Gestire i cataloghi delle macchine e Gestire un catalogo di Microsoft Azure

Ulteriori informazioni

- Creare e gestire connessioni e risorse
- Connessione a Microsoft Azure Resource Manager
- Creare cataloghi di macchine

Accesso remoto al PC

August 22, 2024

> **Nota:**
>
> È possibile gestire l'implementazione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basato sul Web) e Citrix Studio (basato su Windows). Questo articolo riguarda solo Web Studio. Per informazioni su Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Accesso remoto PC è una funzionalità di Citrix Virtual Apps and Desktops che consente alle organizzazioni di consentire ai dipendenti di accedere facilmente alle risorse aziendali in remoto in modo sicuro. La piattaforma Citrix rende possibile questo accesso sicuro offrendo agli utenti l'accesso ai PC fisici dell'ufficio. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work. Accesso remoto PC elimina la necessità di introdurre e fornire altri strumenti per il telelavoro. Ad esempio, desktop o applicazioni virtuali e la relativa infrastruttura associata.

Accesso remoto PC utilizza gli stessi componenti Citrix Virtual Apps and Desktops che forniscono desktop e applicazioni virtuali. Di conseguenza, i requisiti e il processo di distribuzione e configurazione di

Accesso remoto PC sono gli stessi richiesti per la distribuzione di Citrix Virtual Apps and Desktops per la distribuzione di risorse virtuali. Questa uniformità offre un'esperienza amministrativa coerente e unificata. Gli utenti ricevono la migliore esperienza utente utilizzando Citrix HDX per offrire la propria sessione PC da ufficio.

La funzionalità è costituita da un catalogo di macchine di tipo **Accesso remoto PC** che fornisce le seguenti funzionalità:

- Possibilità di aggiungere macchine specificando le OE. Questa capacità facilita l'aggiunta di PC in blocco.
- Assegnazione automatica degli utenti in base all'utente che accede al PC Windows dell'ufficio. Supportiamo le assegnazioni di utenti singoli e più utenti. Per impostazione predefinita, assegniamo automaticamente più utenti alla successiva macchina non assegnata. Per limitare l'assegnazione automatica a un singolo utente, accedere a Web Studio, andare a **Settings** e disattiva l'impostazione **Enable automatic assignment of multiple users for Remote PC Access** (Abilita l'assegnazione automatica di più utenti per l'accesso remoto al PC).

Citrix Virtual Apps and Desktops può gestire più casi d'uso per PC fisici utilizzando altri tipi di cataloghi di macchine. Questi casi d'uso includono:

- PC Linux fisici
- PC fisici in pool (ovvero assegnati in modo casuale, non dedicati)

> **Note:**
>
> Per i dettagli sulle versioni del sistema operativo supportate, vedere i requisiti di sistema per il VDA per il sistema operativo a sessione singola e Linux VDA.
>
> Per le distribuzioni locali, Accesso remoto PC è valido solo per le licenze Advanced o Premium di Citrix Virtual Apps and Desktops. Le sessioni consumano licenze allo stesso modo delle altre sessioni di Citrix Virtual Desktops. Per Citrix Cloud, Accesso remoto PC è valido per Citrix DaaS (in precedenza Citrix Virtual Apps and Desktops Service) e Workspace Premium Plus.

Considerazioni

Anche se tutti i requisiti tecnici e le considerazioni che si applicano a Citrix Virtual Apps and Desktops in generale si applicano anche all'accesso remoto al PC, alcuni potrebbero essere più rilevanti o esclusivi per il caso di utilizzo fisico del PC.

> **Importante:**
>
> I sistemi fisici Windows 11 (e alcuni che eseguono Windows 10) includono funzionalità di sicurezza basate sulla virtualizzazione che fanno sì che il software VDA li rilevi erroneamente come macchine virtuali. Per mitigare questo problema, sono disponibili le seguenti opzioni:

> - Utilizzare l'opzione "/physicalmachine"insieme all'opzione "/remotepc"nell'ambito dell'installazione del VDA mediante la riga di comando
> - Se l'opzione sopra indicata non è stata utilizzata, dopo l'installazione del VDA aggiungere il seguente valore di registro
> `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
> - Nome: ForceEnableRemotePC
> - Tipo: DWORD
> - Dati: 1

Considerazioni sulla distribuzione

Durante la pianificazione della distribuzione di Accesso remoto PC, prendere alcune decisioni generali.

- È possibile aggiungere Accesso remoto PC a una distribuzione esistente di Citrix Virtual Apps and Desktops. Prima di scegliere questa opzione, considerare quanto segue:
  - I Delivery Controller o i Cloud Connector correnti sono adeguatamente dimensionati per supportare il carico aggiuntivo associato ai VDA di Accesso remoto PC?
  - I database del sito locali e i server di database sono adeguatamente dimensionati per supportare il carico aggiuntivo associato ai VDA di Accesso remoto PC?
  - I VDA esistenti e i nuovi VDA di Accesso remoto PC supereranno il numero massimo di VDA supportati per sito?
- È necessario distribuire il VDA sui PC dell'ufficio tramite un processo automatizzato. Di seguito sono riportate le opzioni disponibili:
  - Strumenti di distribuzione elettronica del software (ESD) come SCCM: installare i VDA utilizzando SCCM.
  - Script di distribuzione: installare i VDA utilizzando gli script.
- Vedere le Considerazioni sulla sicurezza di Remote PC Access (Accesso remoto PC).

> **Nota:**
>
> Quando si progetta l'accesso remoto al PC, è necessario considerare il numero di monitor fisici collegati alla GPU sul PC remoto e attualmente configurati/operativi. Anche se un monitor non viene utilizzato nella sessione Citrix, ma viene rilevato dalla GPU, la sua presenza viene conteggiata ai fini del limite massimo di monitor supportato dalla GPU.

Considerazioni sul catalogo di macchine

Il tipo di catalogo di macchine richiesto dipende dal caso d'uso:

- Catalogo macchine Accesso remoto PC
  - PC dedicati Windows
  - PC multiutente dedicati Windows. Questo caso d'uso si applica ai PC fisici dell'ufficio a cui più utenti possono accedere da remoto in turni diversi.
  - PC Windows in pool. Questo caso d'uso si applica ai PC fisici a cui possono accedere più utenti casuali, come i laboratori informatici.
- Catalogo macchine con sistema operativo a sessione singola
  - Statico - PC Linux dedicati
  - Casuale - PC Linux in pool

Una volta identificato il tipo di catalogo di macchine, considerare quanto segue:

- Una macchina può essere assegnata a un solo catalogo di macchine alla volta.
- Per facilitare l'amministrazione delegata, è consigliabile creare cataloghi di macchine in base alla posizione geografica, al reparto o a qualsiasi altro raggruppamento che faciliti la delega dell'amministrazione di ciascun catalogo agli amministratori appropriati.
- Quando si scelgono le unità organizzative (OU) in cui risiedono gli account macchina, selezionare quelle di livello inferiore per una maggiore granularità. Se tale granularità non è richiesta, è possibile scegliere OU di livello superiore. Ad esempio, nel caso di banca/funzionari/cassieri, selezionare i **Tellers** (Cassieri) per una maggiore granularità. In caso contrario, è possibile selezionare **Officers** (Funzionari) o **Bank** (banca) in base a quanto è richiesto.
- Lo spostamento o l'eliminazione di unità organizzative dopo l'assegnazione a un catalogo di macchine Accesso remoto PC influisce sulle associazioni VDA e causa problemi per le assegnazioni future. Pertanto, assicurarsi di pianificare di conseguenza in modo che gli aggiornamenti delle assegnazioni alle unità organizzative dei cataloghi di macchine siano contabilizzati nel piano di modifica di Active Directory.
- Se non è facile scegliere unità organizzative per aggiungere macchine al catalogo macchine a causa della struttura delle unità organizzative, non è necessario selezionare alcuna unità organizzativa. È possibile utilizzare PowerShell per aggiungere macchine al catalogo in seguito. Le assegnazioni automatiche di utenti continuano a funzionare se l'assegnazione desktop è configurata correttamente nel gruppo di consegna. Uno script di esempio per aggiungere macchine al catalogo macchine insieme alle assegnazioni utente è disponibile in GitHub.
- La funzione Wake on LAN integrata è disponibile solo con il catalogo di macchine di tipo **Accesso remoto PC**.

Considerazioni su Linux VDA

Queste considerazioni sono specifiche per Linux VDA:

- Usare Linux VDA su macchine fisiche solo in modalità non 3D. A causa delle limitazioni del driver NVIDIA, la schermata locale del PC non può essere oscurata e visualizza le attività della sessione quando è abilitata la modalità HDX 3D. Visualizzare questa schermata è un rischio per la sicurezza.
- Utilizzare cataloghi di macchine del tipo con sistema operativo a sessione singola per le macchine Linux fisiche.
- L'assegnazione automatica degli utenti non è disponibile per le macchine Linux.
- Se gli utenti sono già connessi al proprio PC localmente, i tentativi di avviare i PC da StoreFront non riescono.
- Le opzioni di risparmio energetico non sono disponibili per le macchine Linux.

Requisiti tecnici e considerazioni

Questa sezione contiene i requisiti tecnici e le considerazioni per i PC fisici.

- I seguenti dispositivi non sono supportati:
  - Switch KVM o altri componenti che possono disconnettere una sessione.
  - PC ibridi, inclusi computer portatili e PC All-in-One e NVIDIA Optimus.
  - Macchine a doppio avvio.
- Collegare la tastiera e il mouse direttamente al PC. Il collegamento al monitor o ad altri componenti che possono essere spenti o scollegati può rendere queste periferiche non disponibili. Se è necessario collegare i dispositivi di input a componenti quali monitor, non spegnere tali componenti.
- I PC devono far parte di un dominio di Servizi di dominio Active Directory.
- Secure Boot è supportato solo su Windows 10 e Windows 11.
- Il PC deve disporre di una connessione di rete attiva. Una connessione cablata è preferibile per una maggiore affidabilità e larghezza di banda.
- Se si utilizza il Wi-Fi, effettuare le seguenti operazioni:
  1. Impostare l'alimentazione in modo che la scheda di rete wireless sia accesa.
  2. Configurare la scheda di rete wireless e il profilo di rete per consentire la connessione automatica alla rete wireless prima dell'accesso dell'utente. In caso contrario, il VDA non si registra finché l'utente non esegue l'accesso. Il PC non è disponibile per l'accesso remoto fino a quando un utente non ha effettuato l'accesso.
  3. Assicurarsi che i Delivery Controller o i connettori cloud possano essere raggiunti dalla rete Wi-Fi.

- È possibile utilizzare Accesso remoto PC sui computer portatili. Assicurarsi che il computer portatile sia collegato a una fonte di alimentazione anziché funzionare a batteria. Configurare le opzioni di alimentazione del laptop in modo che corrispondano alle opzioni di un PC desktop. Ad esempio:

  1. Disattivare la funzionalità di ibernazione.
  2. Disattivare la funzione di sospensione.
  3. Impostare l'azione di chiusura del coperchio su **Non intervenire**.
  4. Impostare l'azione di pressione del pulsante di accensione su **Arresta sistema**.
  5. Disabilitare le funzioni di risparmio energetico della scheda video e della scheda NIC.

- Accesso remoto PC è supportato sui dispositivi Surface Pro con Windows 10. Seguire le stesse linee guida per i computer portatili citati sopra.

- Se si utilizza una docking station, è possibile disancorare e reinserire i computer portatili. Quando si disancora il computer portatile, il VDA si registra nuovamente nei Delivery Controller o nei connettori cloud tramite Wi-Fi. Tuttavia, quando si reinserisce il computer portatile, il VDA non passa all'uso della connessione cablata a meno che non si disconnetta la scheda wireless. Alcuni dispositivi offrono una funzionalità integrata di disconnessione della scheda wireless dopo che è stata stabilita una connessione cablata. Gli altri dispositivi richiedono soluzioni personalizzate o utilità di terze parti per disconnettere la scheda wireless. Leggere le considerazioni sulle reti Wi-Fi menzionate in precedenza.

  Eseguire le seguenti operazioni per abilitare l'inserimento e il disancoraggio per i dispositivi di Accesso remoto PC:

  1. Nel menu **Start**, selezionare **Impostazioni > Sistema > Alimentazione e sospensione** e impostare **Sospensione** su **Mai**.
  2. In **Gestione periferiche > Schede di rete > Adattatore Ethernet** andare su **Risparmio energia** e deselezionare **Consenti al computer di spegnere il dispositivo per risparmiare energia**. Assicurarsi che l'opzione **Consenti al dispositivo di riattivare il computer** sia selezionata.

- Più utenti con accesso allo stesso PC dell'ufficio vedono la stessa icona in Citrix Workspace. Quando un utente accede a Citrix Workspace, tale risorsa appare come non disponibile se già in uso da parte di un altro utente.

- Installare l'app Citrix Workspace su ciascun dispositivo client (ad esempio, un PC di casa) che accede al PC dell'ufficio.

Sequenza di configurazione

Questa sezione contiene una panoramica su come configurare Accesso remoto PC quando si utilizza il catalogo di macchine di **Accesso remoto PC**. Per informazioni su come creare altri tipi di cataloghi

delle macchine, vedere Creare cataloghi delle macchine.

1. Solo sito locale: per utilizzare la funzionalità di riattivazione LAN integrata, configurare i prerequisiti descritti in Riattivazione LAN.
2. Se è stato creato un nuovo sito Citrix Virtual Apps and Desktops per l'accesso remoto PC:

   a) Selezionare il tipo di sito **Accesso remoto PC**.
   b) Nella pagina **Risparmio energia** scegliere di attivare o disattivare la gestione del risparmio energia per il catalogo di macchine Accesso remoto PC predefinito. È possibile modificare questa impostazione in un secondo momento modificando le proprietà del catalogo macchine. Per informazioni dettagliate sulla configurazione della riattivazione LAN, vedere Riattivazione LAN.
   c) Completare le informazioni nelle pagine **Users** e **Machine Accounts**.

   Completando questa procedura viene creato un catalogo macchine denominato **Remote PC Access Machines** e un gruppo di consegna denominato **Remote PC Access Desktops**.
3. Se si aggiungono elementi a un sito Citrix Virtual Apps and Desktops esistente:

   a) Creare un catalogo macchine di tipo **Accesso remoto PC** (pagina Operating System della procedura guidata). Per informazioni dettagliate su come creare un catalogo delle macchine, vedere Creare cataloghi delle macchine. Assicurarsi di assegnare l'unità organizzativa corretta in modo che i PC di destinazione siano resi disponibili per l'utilizzo con Accesso remoto PC.
   b) Creare un gruppo di consegna per fornire agli utenti l'accesso ai PC inclusi nel catalogo macchine. Per i dettagli su come creare un gruppo di consegna, vedere Creare gruppi di consegna. Assicurarsi di assegnare il gruppo di consegna a un gruppo di Active Directory che contenga gli utenti che richiedono l'accesso ai propri PC.
4. Distribuire il VDA nei PC dell'ufficio.

   - Si consiglia di utilizzare il programma di installazione VDA principale con sistema operativo a sessione singola (VDAWorkstationCoreSetup.exe).
   - È inoltre possibile utilizzare il programma di installazione VDA completo per sessione singola (VDAWorkstationSetup.exe) con l'opzione `/remotepc/physicalmachine`, che ottiene lo stesso risultato dell'utilizzo del programma di installazione VDA principale.

     > **Nota:**
     >
     > Per l'installazione RemotePC, utilizzare l'argomento `/physicalmachine` con `/remotepc` perché VDA si comporti come previsto in determinati scenari utente.

   - È possibile abilitare Assistenza remota di Windows per consentire ai team dell'help desk di fornire supporto remoto tramite Citrix Director. A tale scopo, utilizzare l'

opzione /enable_remote_assistance. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.

- Per poter visualizzare le informazioni sulla durata dell'accesso in Director, è necessario utilizzare il programma di installazione VDA completo per sessione singola e includere il componente **Citrix User Profile Management WMI Plugin**. Includere questo componente utilizzando l'opzione /includeadditional. Per ulteriori informazioni, vedere Installare utilizzando la riga di comando.
- Per informazioni sulla distribuzione di VDA utilizzando SCCM, vedere Installare i VDA utilizzando SCCM.
- Per informazioni sulla distribuzione di VDA tramite script di distribuzione, vedere Installare i VDA utilizzando gli script.

Dopo aver completato i passaggi da 2 a 4, gli utenti vengono assegnati automaticamente ai propri computer quando effettuano l'accesso locale sui PC.

5. Chiedere agli utenti di scaricare e installare l'app Citrix Workspace su ciascun dispositivo client utilizzato per accedere al PC dell'ufficio in remoto. L'app Citrix Workspace è disponibile presso https://www.citrix.com/downloads/ o negli store delle applicazioni per i dispositivi mobili supportati.

Funzionalità gestite tramite il Registro di sistema

> **Attenzione:**
>
> La modifica non corretta del Registro di sistema può causare seri problemi che potrebbero richiedere la reinstallazione del sistema operativo. Citrix non può garantire che i problemi derivanti dall'uso non corretto dell'Editor del Registro di sistema possano essere risolti. Utilizzare l'Editor del Registro di sistema a proprio rischio. Assicurarsi di eseguire il backup del Registro di sistema prima di modificarlo.

Disabilitare le assegnazioni automatiche di più utenti

In ogni Delivery Controller, aggiungere la seguente impostazione del Registro di sistema:

HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer

- Nome: AllowMultipleRemotePCAssignments
- Tipo: DWORD
- Dati: 0

Modalità sospensione (versione minima 7.16)

Per consentire a un computer Accesso remoto PC di passare a uno stato di sospensione, aggiungere questa impostazione del Registro di sistema sul VDA e quindi riavviare il computer. Dopo il riavvio, vengono rispettate le impostazioni di risparmio energetico del sistema operativo. La macchina entra in modalità di sospensione dopo al termine del periodo di inattività preconfigurato. Dopo che si è svegliata, la macchina si registra nuovamente nel Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Dati: 1

Gestione delle sessioni

Per impostazione predefinita, la sessione di un utente remoto viene disconnessa automaticamente quando un utente locale avvia una sessione su tale computer (premendo CTRL+ALT+CANC). Per evitare questa azione automatica, aggiungere la seguente voce del Registro di sistema nel PC dell'ufficio e quindi riavviare il computer.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Dati: 1

Per impostazione predefinita, l'utente remoto ha la preferenza rispetto all'utente locale quando il messaggio di connessione non viene riconosciuto entro il periodo di timeout. Per configurare il comportamento, utilizzare questa impostazione:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Dati:
  - 1 - L'utente remoto ha sempre la preferenza se non risponde all'interfaccia utente di messaggistica nel periodo di timeout specificato. Questo comportamento è l'impostazione predefinita se questa impostazione non viene configurata.
  - 2 - L'utente locale ha la preferenza.

Il timeout per l'applicazione della modalità Accesso remoto PC è di 30 secondi per impostazione predefinita. È possibile configurare questo timeout, ma si consiglia di non impostarlo a meno di 30 secondi. Per configurare il timeout, utilizzare questa impostazione del Registro di sistema:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dati: numero di secondi al timeout in valori decimali

Quando un utente desidera ottenere forzatamente l'accesso alla console: l'utente locale può premere Ctrl+Alt+Canc due volte in un intervallo di 10 secondi per ottenere il controllo locale su una sessione remota e forzare un evento di disconnessione.

Dopo la modifica del Registro di sistema e il riavvio del computer, se un utente locale preme Ctrl+Alt+Canc per accedere al PC mentre è utilizzato da un utente remoto, l'utente remoto riceve un messaggio di richiesta. Il messaggio di richiesta chiede se consentire o negare la connessione dell'utente locale. Consentendo la connessione, viene disconnessa la sessione dell'utente remoto.

Registrazione della gestione delle sessioni

Remote PC Access ora dispone di funzionalità mediante le quali effettua una registrazione quando qualcuno tenta di accedere a un PC con una sessione ICA attiva. Ciò consente di monitorare l'ambiente alla ricerca di attività indesiderate o impreviste e di essere in grado di controllare tali eventi se è necessario indagare su eventuali incidenti.

Gli eventi vengono registrati utilizzando il Visualizzatore eventi di Windows e si trovano in **Applicazioni e servizi > Citrix > HostCore > ICA Service > Admin**.

Esistono tre eventi distinti che vengono registrati quando si utilizza Remote PC Access.

Evento Ctrl+Alt+Canc

Questo evento appare quando l'utente locale preme Ctrl+Alt+Canc sulla tastiera della console quando è attiva una sessione remota.

Dettagli evento

- Nome registro: Applicazione e servizi
- ID evento: 43, 44, 45
- Fonte: ICA Service

ID evento 43 Questo ID evento viene visualizzato quando il valore del Registro di sistema SasNotification non esiste o quando il valore del Registro di sistema SasNotification è 0.

- Messaggio:


```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to automatically
               disconnect the remote session.
```

ID evento 44 Questo ID evento viene visualizzato quando il valore del Registro di sistema SasNotification è 1 e il valore del Registro di sistema RpcaMode è 1 o il valore del Registro di sistema RpcaMode non esiste.

- Messaggio:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user. The user preference is set to remote user
               .
```

ID evento 45 Questo ID evento viene visualizzato quando il valore del registro SasNotification è 1 e il valore del Registro di sistema RpcaMode è 2.

- Messaggio:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user.
3          The user preference is set to local user.
```

Evento disconnessione sessione remota

Questo evento viene visualizzato quando la sessione remota è stata disconnessa per vari motivi.

Dettagli evento

- Nome registro: Applicazione e servizi
- ID evento: 46, 47, 48
- Fonte: ICA Service

ID evento 46 Questo ID evento viene visualizzato quando la sessione remota è stata disconnessa e quando il valore del Registro di sistema SasNotification non esiste o il valore del Registro di sistema SasNotification è 0.

- Messaggio:


```
1          The remote session for <remoteUserName> has been
               disconnected.
```

ID evento 47 Questo ID evento viene visualizzato quando l'utente remoto accetta di disconnettere la sessione e quando il valore del Registro di sistema SasNotification è 1 e il valore del Registro di sistema RpcaMode è 1 o il valore del Registro di sistema RpcaMode è 2 o il valore del Registro di sistema RpcaMode non esiste.

- Messaggio:

```
1          The remote session for <remoteUserName> has been
               disconnected because the user accepted the request to
               disconnect the session.
```

ID evento 48 Questo ID evento viene visualizzato quando l'utente remoto non rifiuta la richiesta di disconnessione entro il periodo di timeout specifico e quando il valore del Registro di sistema SasNotification è 1 e il valore del Registro di sistema RpcaMode è 2.

- Messaggio:

```
1          The remote session for <remoteUserName> has been
               disconnected because the user did not decline the
               disconnection request within the configured timeout
               period (<timeout period>).
```

Evento di Ctrl+Alt+Canc premuto due volte Questo evento appare quando Ctrl+Alt+Canc viene premuto due volte entro 10 secondi.

Dettagli evento

- Nome registro: Applicazione e servizi
- ID evento: 49
- Fonte: ICA Service

ID evento 49 Questo ID evento appare quando Ctrl+Alt+Canc viene premuto due volte entro 10 secondi.

- Messaggio:

```
1          The remote session for <remoteUserName> has been forcibly
               disconnected.
```


Riattivare su LAN

Accesso remoto PC supporta la funzione di riattivazione su LAN, che offre agli utenti la possibilità di accendere i PC fisici da remoto. Questa funzionalità consente agli utenti di mantenere spenti i PC dell'ufficio quando non sono in uso per risparmiare sui costi energetici. Consente inoltre l'accesso remoto quando una macchina è stata spenta inavvertitamente.

Con la funzione di riattivazione su LAN, i Magic Packet vengono inviati direttamente dal VDA in esecuzione sul PC alla sottorete in cui risiede il PC quando viene richiesto dal controller di consegna. Ciò consente alla funzione di agire senza dipendere da componenti aggiuntivi dell'infrastruttura o da soluzioni di terze parti per la distribuzione di Magic Packet.

La funzione di riattivazione su LAN è diversa dalla funzione di riattivazione su LAN basata su SCCM precedente. Per informazioni sulla riattivazione LAN basata su SCCM, vedere Riattivazione LAN - integrata con SCCM.

Requisiti di sistema

Di seguito sono riportati i requisiti di sistema per l'utilizzo della funzione di riattivazione su LAN:

- Piano di controllo:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 o versioni successive
- PC fisici:
  - VDA versione 2009 o successiva
  - Windows 10 o Windows 11. Per i dettagli relativi al supporto, vedere i requisiti di sistema del VDA.
  - Riattivazione su LAN abilitata in BIOS/UEFI
  - Riattivazione su LAN abilitata nelle proprietà della scheda di rete all'interno della configurazione di Windows

Configurare la riattivazione su LAN

Se si utilizza Citrix Virtual Apps and Desktops in locale, la configurazione della riattivazione su LAN integrata è supportata solo utilizzando PowerShell.

Per configurare la riattivazione su LAN:

1. Creare il catalogo di macchine Accesso remoto PC se non è già disponibile.
2. Creare la connessione host di riattivazione LAN se è già disponibile.

> **Nota:**
>
> Per utilizzare la funzionalità di riattivazione su LAN, se si dispone di una connessione host del tipo "Microsoft Configuration Manager Wake on LAN", creare una nuova connessione host.

3. Recuperare l'identificatore univoco della connessione host di Riattivazione LAN.
4. Associare la connessione host di riattivazione su LAN a un catalogo di macchine.

Per creare la connessione host di riattivazione su LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                    >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
        $hypHc.HypervisorConnectionUid
 }
```

Quando la connessione host è pronta, eseguire i seguenti comandi per recuperare l'identificatore univoco della connessione host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
```

Dopo aver recuperato l'identificatore univoco della connessione, eseguire i comandi seguenti per associare la connessione al catalogo del computer Accesso remoto PC:


```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
```

Considerazioni di progettazione

Quando si prevede di utilizzare la riattivazione su LAN con Accesso remoto PC, considerare quanto segue:

- Più cataloghi di macchine possono utilizzare la stessa connessione host di riattivazione su LAN.
- Perché un PC possa riattivare un altro PC, entrambi i PC devono trovarsi nella stessa sottorete e utilizzare la stessa connessione host di riattivazione su LAN. Non importa se i PC si trovano nello stesso catalogo di macchine o cataloghi diversi.
- Le connessioni host vengono assegnate a zone specifiche. Se la distribuzione contiene più di una zona, è necessaria una connessione host di riattivazione su LAN in ciascuna zona. Lo stesso vale per i cataloghi di macchine.
- I Magic Packet vengono trasmessi utilizzando l'indirizzo di trasmissione globale 255.255.255.255. Assicurarsi che l'indirizzo non sia bloccato.
- Deve essere presente almeno un PC acceso nella sottorete, per ciascuna connessione di riattivazione su LAN, per poter riattivare le macchine in quella sottorete.

Considerazioni operative

Di seguito sono riportate considerazioni sull'impiego della funzione di riattivazione su LAN:

- Il VDA deve registrarsi almeno una volta prima che il PC possa essere riattivato utilizzando la funzione di riattivazione su LAN integrata.
- La funzione di riattivazione su LAN può essere utilizzata solo per riattivare i PC. Non supporta altre azioni di alimentazione, ad esempio il riavvio o l'arresto.
- Dopo essere stata creata, la connessione di riattivazione su LAN è visibile in Web Studio. Tuttavia, la modifica delle sue proprietà all'interno di Web Studio non è supportata se si utilizza Citrix Virtual Apps and Desktops in locale.
- I Magic Packet vengono inviati in uno di due modi:
  1. Quando un utente tenta di avviare una sessione sul proprio PC e il VDA non è registrato
  2. Quando un amministratore invia manualmente un comando di accensione da Web Studio o PowerShell
- Poiché il controller di distribuzione non è a conoscenza dello stato di alimentazione di un PC, Web Studio visualizza **Not Supported** nello stato di alimentazione. Il controller di consegna utilizza lo stato di registrazione del VDA per determinare se un PC è acceso o spento.

Riattivazione su LAN integrata con SCCM

La funzione di riattivazione su LAN integrata con SCCM è un'opzione alternativa di riattivazione su LAN per l'accesso remoto PC disponibile solo con Citrix Virtual Apps and Desktops locali.

Requisiti di sistema

Di seguito sono riportati i requisiti di sistema per l'utilizzo della funzione di riattivazione su LAN integrata con SCCM:

- Citrix Virtual Apps and Desktops 1912 o versioni successive
- PC fisici:
  - VDA versione 1912 o successiva
  - Windows 10. Per i dettagli relativi al supporto, vedere i requisiti di sistema del VDA.
  - Riattivazione su LAN abilitata in BIOS/UEFI
  - Riattivazione su LAN abilitata nelle proprietà della scheda di rete all'interno della configurazione di Windows
- System Center Configuration Manager (SCCM) 2012 R2 o versione successiva

Configurare la funzione di riattivazione su LAN integrata con SCCM

Completare i seguenti prerequisiti:

1. Configurare SCCM 2012 R2, 2016 o 2019 all'interno dell'organizzazione. Quindi distribuire il client SCCM su tutti i computer Accesso remoto PC, lasciando trascorrere il tempo necessario per l'esecuzione del ciclo di inventario SCCM pianificato o forzarne uno manualmente, se necessario.
2. Per il supporto del proxy di riattivazione, attivare l'opzione in SCCM. Per ogni sottorete dell'organizzazione che contiene PC che utilizzano la funzione Accesso remoto PC su LAN, assicurarsi che tre o più computer possano fungere da macchine sentinella.
3. Per il supporto dei Magic Packet, configurare i router e i firewall della rete perché consentano l'invio di Magic Packet, utilizzando una trasmissione diretta in sottorete o unicast.
4. Configurare la riattivazione su LAN nelle impostazioni BIOS/UEFI di ciascun PC.
5. Distribuire il VDA sui PC fisici se non lo si è già fatto.

Dopo aver soddisfatto i prerequisiti, completare la procedura seguente per consentire al Delivery Controller di comunicare con SCCM:

1. Creare una connessione host per SCCM. Per ulteriori informazioni, vedere Connessioni e risorse.
   - Selezionare **Microsoft Configuration Manager Wake on LAN** come tipo di connessione.

- Le credenziali immesse devono includere l'accesso alle raccolte nell'ambito e devono avere il ruolo **Remote Tools Operator**.

2. Selezionare la connessione in Web Studio, quindi selezionare **Edit Connection** (Modifica connessione) e fare clic su **Advanced**.
3. Selezionare l'opzione appropriata per la gestione della riattivazione su LAN:
    - Se si utilizza il proxy di riattivazione, selezionare la prima opzione: **Microsoft System Center Configuration Manager Wake-up proxy** (Proxy di riattivazione di Microsoft System Center Configuration Manager).
    - Se si utilizzano Magic Packet, selezionare la seconda opzione: **Wake on LAN packets transmitted by the Delivery Controller** (Pacchetti di riattivazione su LAN trasmessi dal Delivery Controller).
        - Selezionare il metodo di trasmissione appropriato: **subnet-directed broadcasts** (trasmissioni dirette dalla sottorete) o **unicast**.

Dopo aver creato la connessione host, associare la connessione a un catalogo di Accesso remoto PC:

- Se si sta creando un nuovo catalogo di Accesso remoto PC, nella pagina **Operating System** della creazione guidata catalogo selezionare **Remote PC Access** come tipo di catalogo e scegliere la connessione appropriata dall'elenco a discesa.
- Per aggiungere la riattivazione da LAN a un catalogo di Accesso remoto PC esistente:
    1. Andare al nodo **Machine Catalogs** (Cataloghi macchine) in Web Studio, selezionare il catalogo macchine e quindi selezionare **Edit Machine Catalog** (Modifica catalogo macchine).
    2. Selezionare la scheda **Modifica catalogo macchine** (Risparmio energia) e scegliere **Yes** per abilitare la gestione del risparmio energia per il catalogo macchine.
    3. Selezionare la connessione appropriata dall'elenco a discesa e fare clic su **OK**.

Risoluzione dei problemi

Lo schermo nero del monitor non funziona

Se il monitor locale del PC Windows non ha lo schermo nero mentre è attiva una sessione HDX (il monitor locale mostra ciò che sta accadendo nella sessione), ciò è probabilmente dovuto a problemi del driver del fornitore della GPU. Per risolvere il problema, assegnare al driver di visualizzazione indiretta Citrix (IDD) una priorità maggiore rispetto al driver del fornitore della scheda grafica impostando il seguente valore del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD

- Dati: 3

Per ulteriori informazioni sulle priorità della scheda video e sulla creazione del monitor, vedere l'articolo del Knowledge Center CTX237608.

La sessione si disconnette quando si seleziona Ctrl+Alt+Canc nel computer in cui è attivata la notifica di gestione della sessione

La notifica di gestione della sessione controllata dal valore del Registro di sistema **SasNotification** funziona solo quando la modalità Accesso remoto PC è attivata sul VDA. Se il PC fisico ha il ruolo di Hyper-V o qualsiasi funzionalità di sicurezza basata sulla virtualizzazione abilitata, il PC si segnala come macchina virtuale. Se il VDA rileva che è in esecuzione su una macchina virtuale, disattiva automaticamente la modalità Accesso remoto PC. Per attivare la modalità Accesso remoto PC, aggiungere il seguente valore del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dati: 1

Riavviare il PC affinché l'impostazione abbia effetto.

Informazioni diagnostiche

Le informazioni diagnostiche su Accesso remoto PC vengono scritte nel registro eventi applicazioni di Windows. I messaggi informativi non vengono limitati. I messaggi di errore vengono limitati eliminando i messaggi duplicati.

- 3300 (informativo): Macchina aggiunta al catalogo
- 3301 (informativo): Macchina aggiunta al gruppo di consegna
- 3302 (informativo): Macchina assegnata all'utente
- 3303 (errore): Eccezione

Gestione dell'alimentazione

Se è attivata la gestione dell'alimentazione per Accesso remoto PC, le trasmissioni dirette dalla sottorete potrebbero non riuscire ad avviare i computer che si trovano in una sottorete diversa dal controller. Se è necessaria la gestione dell'alimentazione tra sottoreti che utilizzano trasmissioni dirette da sottoreti e il supporto AMT non è disponibile, provare il proxy di riattivazione o il metodo Unicast. Verificare che tali impostazioni siano abilitate nelle proprietà avanzate per la connessione di gestione dell'alimentazione.

La sessione remota attiva registra gli input del touchscreen locale

Quando il VDA abilita la modalità Accesso remoto PC, il computer ignora l'input del touchscreen locale durante una sessione attiva. Se il PC fisico ha il ruolo di Hyper-V o qualsiasi funzionalità di sicurezza basata sulla virtualizzazione abilitata, il PC si segnala come macchina virtuale. Se il VDA rileva che è in esecuzione su una macchina virtuale, disattiva automaticamente la modalità Accesso remoto PC. Per attivare la modalità Accesso remoto PC, aggiungere la seguente impostazione del Registro di sistema:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dati: 1

Riavviare il PC affinché l'impostazione abbia effetto.

Altre risorse

Di seguito sono elencate altre risorse per Accesso remoto PC:

- Guida alla progettazione della soluzione: decisioni sulla progettazione di Remote PC Access (Accesso remoto PC).
- Esempi di architetture di Remote PC Access (Accesso remoto PC): architettura di riferimento per la soluzione Citrix Remote PC Access (Accesso remoto PC).

Aggiornamento e migrazione

August 22, 2024

Introduzione

L'aggiornamento modifica la distribuzione in Citrix Virtual Apps and Desktops 7 **versione corrente (CR)** senza dover configurare nuove macchine o siti. Questo è noto come aggiornamento sul posto.

L'aggiornamento consente di accedere alle funzionalità e alle tecnologie più recenti per le quali si è idonei. Gli aggiornamenti possono anche contenere correzioni, chiarimenti e miglioramenti delle versioni precedenti.

Panoramica dell'aggiornamento

1. Vedere l'articolo Aggiornare una distribuzione prima di iniziare l'aggiornamento. Questa è la fonte di informazioni principale per imparare a prepararsi per un aggiornamento e per implementarlo.
2. Assicurarsi che le date attuali di Customer Success Services siano valide e non siano scadute. Per ulteriori informazioni, vedere l'articolo Customer Success Services renewal licenses.
3. Completare la guida alla preparazione.
4. Eseguire i programmi di installazione per aggiornare i componenti principali.
5. Aggiornare i database di sistema e il sito.
6. Aggiornare i VDA sulle immagini (o direttamente sulle macchine).
7. Aggiornare gli altri componenti.

Ogni fase di preparazione e aggiornamento è descritta in dettaglio in Aggiornare una distribuzione.

Versioni che è possibile aggiornare

È possibile eseguire l'aggiornamento a Citrix Virtual Apps and Desktops 2402 LTSR da:

- Virtual Apps and Desktops 2203 LTSR con o senza CU, fino a CU4 incluso
- Virtual Apps and Desktops 1912 LTSR con o senza CU, fino a CU8 incluso
- Versioni CR attualmente supportate di Citrix Virtual Apps and Desktops

> Nota:
>
> - Prima di iniziare il processo di aggiornamento, Citrix consiglia ai clienti di collaudare l'aggiornamento in un ambiente controllato e verificare che soddisfi i loro requisiti specifici. Inoltre, consigliamo di esaminare tutta la documentazione pertinente del prodotto, incluso l'elenco dei prodotti obsoleti e i problemi noti, per garantire una transizione senza interruzioni. Questo approccio aiuta a mitigare le potenziali interruzioni dei sistemi di produzione e migliora l'esperienza complessiva di aggiornamento.
> - Citrix Virtual Apps and Desktops 1912 LTSR raggiungerà presto la fine del ciclo di vita. Per ulteriori informazioni sull'elenco delle versioni supportate, vedere Matrice dei prodotti.

Domande frequenti

In questa sezione si trovano le risposte ad alcune domande frequenti sull'aggiornamento di Citrix Virtual Apps and Desktops.

- **Qual è l'ordine corretto per aggiornare l'ambiente Virtual Apps and Desktops?**

  Per un'illustrazione e una descrizione della sequenza di aggiornamento consigliata, vedere Sequenza di aggiornamento e Procedura di aggiornamento.

- **Il mio sito comprende svariati Delivery Controller (in diverse zone). Cosa succede se aggiorno solo alcuni di essi? Devo aggiornare tutti i Controller presenti nel sito durante la stessa sessione di manutenzione?**

  La procedura migliore consiste nell'aggiornare tutti i Delivery Controller durante la stessa sessione di manutenzione, poiché vari servizi presenti in ciascun Controller comunicano tra loro. Mantenere versioni diverse potrebbe causare problemi. Durante una sessione di manutenzione, si consiglia di aggiornare metà dei Controller, aggiornare il sito e quindi aggiornare i Controller rimanenti. Per ulteriori informazioni, vedere Procedura di aggiornamento.

- **Posso passare direttamente alla versione più recente o devo eseguire aggiornamenti incrementali?**

  È quasi sempre possibile eseguire l'aggiornamento alla versione più recente saltando le versioni intermedie, a meno che non sia esplicitamente indicato nell'articolo **Novità** della versione a cui si effettua l'aggiornamento.

- **Un cliente può eseguire l'aggiornamento da un ambiente LTSR (Long Term Service Release) a una versione corrente?**

  Sì. I clienti non sono tenuti a continuare a utilizzare una LTSR per un periodo prolungato. I clienti possono spostare un ambiente LTSR a una versione corrente, in base ai requisiti e alle caratteristiche dell'azienda.

- **Sono consentite versioni miste dei componenti?**

  All'interno di ogni sito, Citrix consiglia di aggiornare tutti i componenti alla stessa versione. Sebbene sia possibile utilizzare versioni precedenti di alcuni componenti, così facendo potrebbero non essere disponibili tutte le funzionalità della versione più recente. Per ulteriori informazioni, vedere Considerazioni sull'ambiente misto.

- **Con quale frequenza deve essere aggiornata una versione corrente?**

  Le versioni correnti raggiungono la fine della manutenzione (EOM) 6 mesi dopo la data di rilascio. Citrix consiglia ai clienti di adottare l'ultima versione corrente. Le versioni correnti raggiungono la fine del ciclo di vita (EOL) 18 mesi dopo la data di rilascio.

- **Cosa è consigliato: aggiornamento a LTSR o CR?**

  Le versioni correnti (CR) offrono le funzionalità di virtualizzazione di app, desktop e server più recenti e innovative. Questo permette di continuare a utilizzare tecnologia all'avanguardia e di rimanere un passo avanti rispetto alla concorrenza.

  Le LTSR (Long Term Service Release) sono ideali per ambienti di produzione aziendali di grandi dimensioni che preferiscono mantenere la stessa versione di base per un periodo prolungato.

- **Devo aggiornare le mie licenze?**

Assicurarsi che la data della licenza corrente non sia scaduta e che sia valida per la versione a cui si sta eseguendo l'aggiornamento. Vedere CTX111618. Per informazioni sul rinnovo, vedere Licenze di rinnovo di Customer Success Services.

- **Quanto tempo richiede un aggiornamento?**

  Il tempo necessario per aggiornare una distribuzione varia a seconda dell'infrastruttura e della rete. Quindi, non possiamo fornire una durata esatta.

- **Quali sono le migliori pratiche?**

  Assicurarsi di comprendere e seguire la guida alla preparazione.

- **Quali sistemi operativi sono supportati?**

  L'articolo Requisiti di sistema relativo alla versione a cui si sta eseguendo l'aggiornamento elenca i sistemi operativi supportati.

  Se la distribuzione corrente utilizza sistemi operativi non più supportati, vedere Sistemi operativi precedenti.

- **Quali versioni di VMware vSphere (vCenter + ESXi) sono supportate?**

  CTX131239 elenca gli host e le versioni supportati, oltre a collegamenti a problemi noti.

- **La mia versione quando raggiunge l'EOL?**

  Controllare la matrice del prodotto.

- **Quali sono i problemi noti dell'ultima versione?**

  - Citrix Virtual Apps and Desktops
  - StoreFront
  - Citrix Provisioning
  - Citrix License Server
  - App Citrix Workspace per Windows

Ulteriori informazioni

Gli aggiornamenti della distribuzione di **Long Term Service Release (LTSR)** utilizzano gli aggiornamenti cumulativi (CU). Un CU aggiorna i componenti di base di LTSR e ogni CU include il proprio metainstaller.

Ogni CU ha una documentazione dedicata. Ad esempio, per LTSR 2203, seguire il collegamento alla pagina **Novità** di LTSR per visualizzare l'ultimo CU. Ogni pagina CU include informazioni sulla versione supportata, istruzioni e un collegamento al pacchetto di download del CU.

Migrazione

Migrazione al cloud

È possibile utilizzare lo strumento di configurazione automatica per Citrix Virtual Apps and Desktops per eseguire la migrazione della distribuzione locale nel cloud. Per ulteriori informazioni, vedere Migrazione al cloud.

Migrazione legacy

La migrazione consente di spostare i dati da una distribuzione precedente a una versione più recente. Il processo include l'installazione di componenti più recenti e la creazione di un nuovo sito, l'esportazione di dati dalla farm precedente e quindi l'importazione dei dati nel nuovo sito.

Non sono disponibili strumenti o script supportati per la migrazione delle versioni XenApp e XenDesktop o per la migrazione delle versioni precedenti di Citrix Virtual Apps and Desktops. L'*aggiornamento* è supportato per le versioni di Citrix Virtual Apps and Desktops descritte in questa documentazione del prodotto.

Per i contenuti di migrazione XenApp 6.x precedenti, vedere quanto segue. Né gli script né gli articoli sono supportati né sottoposti a manutenzione.

- Gli script di migrazione open source per le versioni XenApp 6.x sono disponibili all'indirizzo https://github.com/citrix/xa65migrationtool. Citrix non supporta né sottopone a manutenzione questi script di migrazione
- Modifiche di 7.x
- Aggiornamento di un worker XenApp 6.5 a un nuovo VDA
- Migrazione di XenApp 6.x

Ottimizzazione di Microsoft Teams (nuovo)

August 22, 2024

Microsoft ha lanciato una nuova versione di Microsoft Teams (Teams 2.x) per ambienti VDI. Citrix ora supporta l'ottimizzazione per questa nuova versione di Teams. Questa documentazione si concentra principalmente sull'ottimizzazione Citrix HDX con il nuovoTeams e offre informazioni essenziali per la transizione all'ottimizzazione Microsoft SlimCore.

Terminologia e transizione

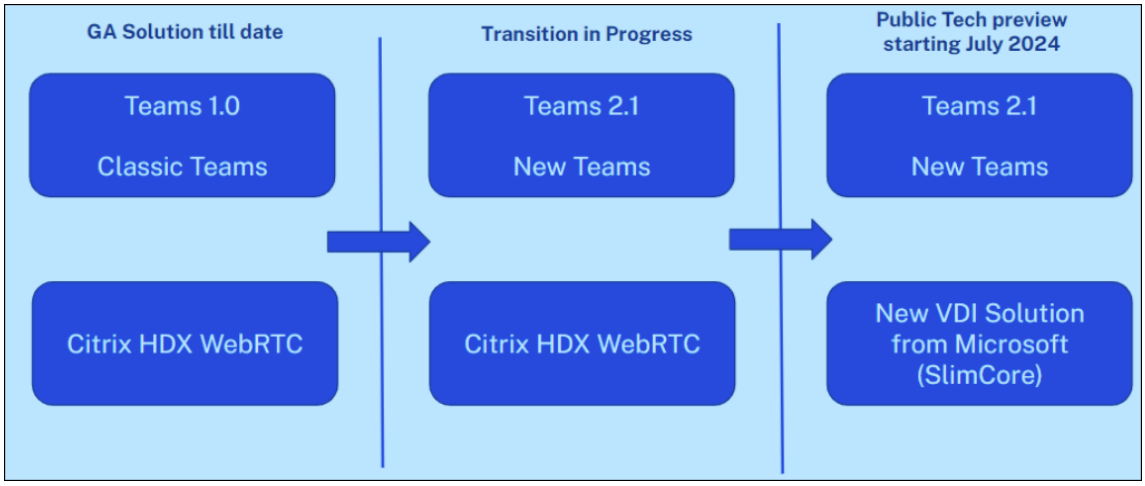
Transizione in Microsoft Teams

Attualmente ci sono due transizioni nello spazio Microsoft Teams:

- **Transizione da Teams Classic a nuovo Teams**: questa transizione è destinata sia ai client nativi che a quelli VDI
  - Teams Classic raggiungerà la fine del supporto e la fine del ciclo di vita. Per informazioni sulla tempistica di questa transizione, vedere Fine della disponibilità per il client Teams classico.
  - La documentazione completa per l'implementazione di New Teams è disponibile alla pagina Nuovo Teams per VDI.
- **Transizione da Citrix HDX Optimization all'ottimizzazione Microsoft SlimCore**: questa transizione è specifica per gli ambienti VDI.
  - Introduciamo i termini `VDI 1.0` e `VDI 2.0` per distinguere tra l'ottimizzazione esistente con Citrix HDX e la nuova soluzione VDI di Microsoft.
  - Colloquialmente VDI 1.0 si riferisce a Citrix HDX Optimization e VDI 2.0 si riferisce alla nuova soluzione VDI per Teams (ottimizzazione Microsoft SlimCore).

Cronologie

- Per ulteriori informazioni sulla cronologia di fine vita di Classic Teams, vedere Fine della disponibilità per il client Classic Teams.
- Per partecipare all'anteprima pubblica per l'ottimizzazione SlimCore, gli amministratori devono spostare gli utenti sul canale di anteprima pubblico come descritto in questo articolo.



Principali distinzioni

Ottimizzazione di Citrix HDX	Ottimizzazione Microsoft SlimCore
L'ottimizzazione è una soluzione combinata di Citrix e Microsoft e utilizza un canale virtuale creato da Citrix. Lo scaricamento dei contenuti multimediali viene gestito da `HdxRtcEngine` che risiede nell'app Citrix Workspace.	La soluzione di ottimizzazione è di proprietà e gestita da Microsoft e utilizza canali virtuali creati da Microsoft. Lo scaricamento dei file multimediali è gestito dal motore multimediale Microsoft SlimCore.
Non sono necessari componenti aggiuntivi sull'endpoint tranne l'installazione dell'app Citrix Workspace.	Componente aggiuntivo: il **plug-in VDI di Teams** deve essere distribuito sull'endpoint con vari mezzi. Questo plug-in gestisce il download e gli aggiornamenti del motore SlimCore.
Disponibile su piattaforme endpoint: Windows, macOS, Linux e ChromeOS. Le nuove funzionalità vengono gestite in collaborazione da Citrix e Microsoft.	Disponibile su piattaforme endpoint: Windows a partire dalla data attuale. Le nuove funzionalità sono gestite da Microsoft. Gli utenti hanno accesso ad alcune nuove funzionalità non disponibili con Citrix HDX Optimization.

Interoperabilità e roaming

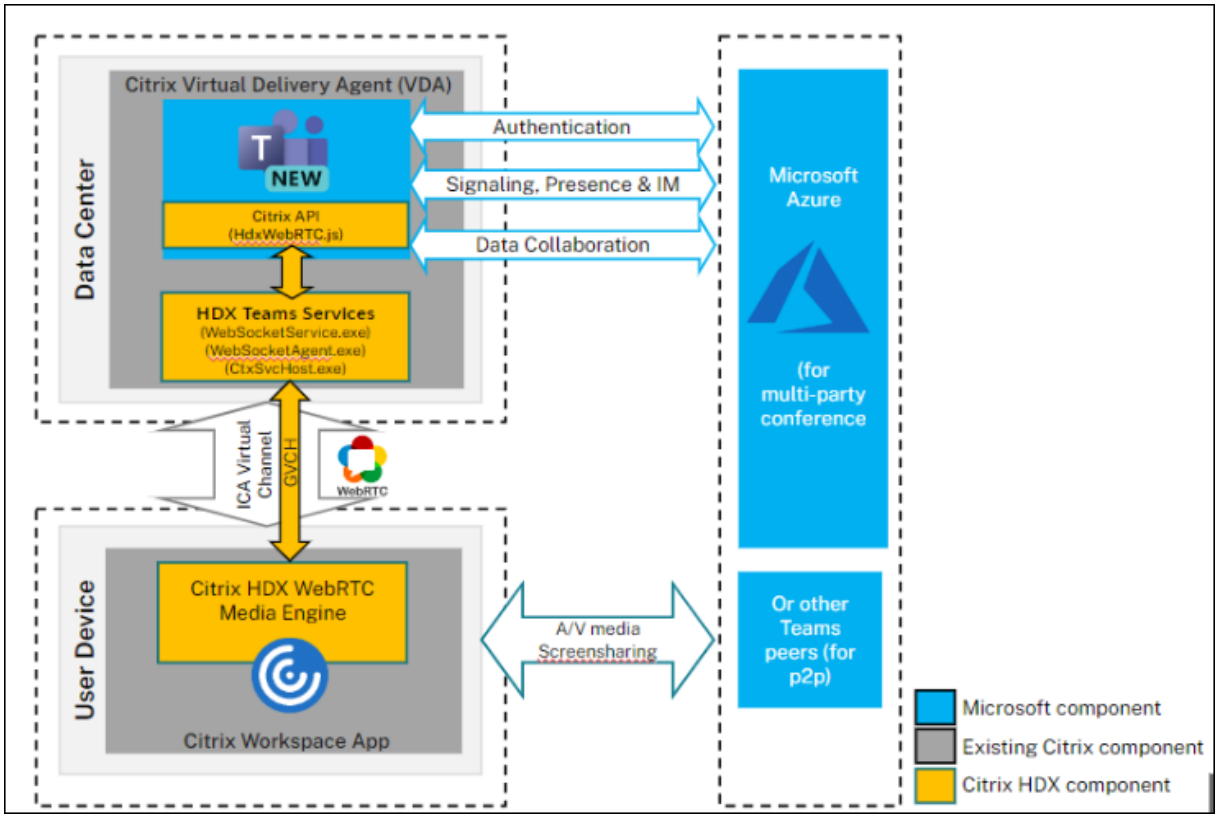
L'ottimizzazione Citrix HDX (WebRTC) e l'ottimizzazione Microsoft SlimCore possono esistere in parallelo, tuttavia il nuovo client Teams può essere ottimizzato con un solo una delle due alla volta.

- Il nuovo Teams carica WebRTC o SlimCore in fase di esecuzione. In fase di esecuzione, viene presa una decisione nel seguente ordine: SlimCore > WebRTC > Reindirizzamento audio/video standard.
- Il processo di selezione non è dinamico. Ad esempio: nel caso in cui il nuovo Teams abbia iniziato l'ottimizzazione con SlimCore e poi si verifichi un problema, torna al reindirizzamento audio/video standard. È necessario riavviare l'app Teams per completare il processo decisionale e ottimizzarlo con WebRTC.
- Lo stesso scenario si applica agli scenari di roaming. Ad esempio: se un utente si connette da un endpoint con ottimizzazione SlimCore ed effettua il roaming verso un endpoint senza il plug-in o un endpoint Mac/Linux, Teams esegue il reindirizzamento audio/video standard. È necessario riavviare l'app Teams per effettuare il fallback all'ottimizzazione WebRTC.
- Gli scenari di roaming tra endpoint già ottimizzati per SlimCore sono senza interruzioni.

Ottimizzazione di Citrix HDX

August 23, 2024

In Citrix HDX (WebRTC Optimization), il motore multimediale (HDXRTCEngine) sull'endpoint responsabile della gestione dei contenuti multimediali offload è integrato nell'app Citrix Workspace e l'installazione dell'app Citrix Workspace installa automaticamente anche il motore.



Requisiti di sistema

Questa sezione illustra le versioni minime e consigliate necessarie per supportare il nuovo client Teams. Tenere presente che nelle versioni minime alcune correzioni di bug critici o funzionalità più recenti potrebbero non essere disponibili. Distribuire le versioni consigliate per avere la migliore esperienza con le correzioni e le funzionalità più recenti.

Sistemi operativi VDI

Per informazioni dettagliate, vedere i consigli forniti nella documentazione Microsoft.

> **Nota:**
>
> - Windows Server 2016 non è supportato. Citrix consiglia di pianificare gli aggiornamenti di conseguenza.
> - Poiché le versioni vengono aggiornate frequentemente, le versioni qui menzionate potrebbero aver raggiunto la fine del ciclo di vita. Vedere quindi le pagine sul ciclo di vita del prodotto dell'app Citrix Workspace e di Citrix Virtual Apps and Desktops per assicurarsi di utilizzare versioni supportate dei diversi componenti.
> - Se si utilizza Citrix Virtual Apps and Desktops 1912 LTSR, Citrix consiglia di pianificare un aggiornamento poiché il suo ciclo di vita terminerà nel dicembre del 2024.

Virtual Delivery Agent (VDA)

Versioni minime	Versioni consigliate
1912 LTSR CU8+; 2203 LTSR (qualsiasi CU); 2212 CR	2203 LTSR CU5+ o 2402 LTSR e qualsiasi versione CR precedente

App Citrix Workspace

Versioni minime	Versioni consigliate
Windows 2203 LTSR (CU più recente); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301	Windows 2402 LTSR; Windows 2405 CR; Linux 2405; Mac 2405; ChromeOS/HTML5 2405

Distribuzione

1. Installare il nuovo client Teams su VDI Per informazioni dettagliate, vedere Deploy new Teams for VDI.
2. Configurare la seguente chiave di registro sul VDA per ottimizzare il nuovo Teams.
   - **Posizione**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **Chiave (REG_Multi_SZ):** `ProcessWhitelist`
   - **Valore:** `msedgewebview2.exe`

     > **Nota:**
     >
     > A partire da Citrix Virtual Apps and Desktops 2402 LTSR (o) Citrix Virtual Apps and Desktops 2203 LTSR CU5+, non è necessario configurare manualmente la voce di reg-

> istro `msedgewebview2.exe` poiché è inserita nell'elenco degli elementi consentiti per impostazione predefinita.

3. Assicurarsi che il criterio Microsoft Teams redirection (Reindirizzamento di Microsoft Teams) sia abilitato. Questo criterio è attivato per impostazione predefinita.
4. Non è necessaria alcuna configurazione aggiuntiva sul lato client. Seguire le istruzioni della procedura guidata per installare l'app Citrix Workspace.

App Layering

Il nuovo Microsoft Teams ha cambiato il metodo di installazione e ora viene installato in C:\Programmi\WindowsApps. Per supportare questa modifica, è necessario eseguire App Layering versione 2403.2 o successiva. È possibile scaricare un disco di aggiornamento nella pagina App Layering downloads che include questa correzione.

Per informazioni dettagliate, vedere la documentazione di App Layering.

Citrix Profile Management

Per informazioni su come abilitare il roaming per New Microsoft Teams, vedere la documentazione di Citrix Profile Management. La versione minima attualmente indicata per Citrix Profile Management è 2402 LTSR (o) 2203 LTSR CU5+.

Considerazioni sul networking

I requisiti di rete per il nuovo Teams non differiscono da quelli di Teams Classic. Vedere quindi la sezione Requisiti di rete nella documentazione di Teams Classic.

Supporto delle funzionalità e versioni supportate

Poiché le versioni vengono aggiornate frequentemente, alcune versioni precedenti menzionate qui potrebbero aver raggiunto il termine del ciclo di vita. Vedere quindi le pagine sul ciclo di vita del prodotto dell'app Citrix Workspace e di Citrix Virtual Apps and Desktops per assicurarsi di utilizzare versioni supportate dei diversi componenti.

> **Nota:**
>
> - Le versioni qui menzionate sono le versioni minime a partire dalle quali è supportata la particolare funzionalità o la versione minima in cui è supportato il nuovo Teams, a seconda di quale sia la superiore.
> - Citrix Virtual Apps and Desktops 1912 LTSR CU8+ indicato nella sezione delle versioni min-

> ime non è menzionato nella tabella seguente poiché raggiungerà la fine del ciclo di vita nel dicembre 2024. Tuttavia, è ancora una versione supportata fino ad allora.
> - Le funzionalità in cui le versioni minime di Citrix Virtual Apps and Desktops sono indicate come N/A implicano semplicemente che la funzionalità non ha comportato alcuna modifica dal lato VDA.

Funzione	VDA (versione minima)	Citrix Workspace App per Windows (versione minima)	App Citrix Workspace per Mac (versione minima)	App Citrix Workspace per Linux (versione minima)	App Citrix Workspace per ChromeOS (versione minima)
Audio/Video (P2P e conferenze)	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2301
Condivisione dello schermo	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2301
i. Indicatore schermo con bordo rosso	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2207	No
ii. Limita l' acquisizione in Desktop Viewer	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2207	No
iii. Multimonitor	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2207	No
DTMF	N/A	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2301

Funzione	VDA (versione minima)	Citrix Workspace App per Windows (versione minima)	App Citrix Workspace per Mac (versione minima)	App Citrix Workspace per Linux (versione minima)	App Citrix Workspace per ChromeOS (versione minima)
Supporto dei server proxy	N/A	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2305
Condivisione di app	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2209	No
Sottotitoli live	N/A	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2303
e911 dinamico	N/A	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2301
Concedere il controllo	N/A	CU più recente di 2203 LTSR, 2302 CR	2302	2207	No
Richiedi il controllo	N/A	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2303
Multifinestra	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2303
Trascrizioni delle riunioni	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2207	2303

Funzione	VDA (versione minima)	Citrix Workspace App per Windows (versione minima)	App Citrix Workspace per Mac (versione minima)	App Citrix Workspace per Linux (versione minima)	App Citrix Workspace per ChromeOS (versione minima)
Sfocatura dello sfondo	2203 LTSR (qualsiasi CU), 2212 CR	CU più recente di 2203 LTSR, 2302 CR	2302	2212	2303
Condivisione dello schermo (con App Protection)	2203 LTSR (qualsiasi CU), 2212 CR	2402 LTSR, 2309.1 CR	2308	2311	No
Simulcast	2203 LTSR (qualsiasi CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
Suoneria secondaria	2203 LTSR (qualsiasi CU), 2212 CR	2402 LTSR, 2307.1 CR	2308	2308	2312
Condividere l'audio del sistema	2203 LTSR (qualsiasi CU), 2212 CR	2402 LTSR, 2403 CR	2405	2402	No

Risoluzione dei problemi e altre considerazioni

Per il nuovo Teams, vedere CTX253754, Risoluzione dei problemi di Microsoft Teams; per gli ultimi aggiornamenti su tutto ciò che riguarda New Teams, vedere CTX585013.

Limitazioni note

Limitazioni sull'app Citrix Workspace

- Supporto HID: la risposta e la conclusione delle chiamate non sono supportate. I tasti per abbassare e alzare il volume sono supportati.
- Gli utenti non possono acquisire schermate dei contenuti di Microsoft Teams quando utilizzano uno strumento di cattura su VDA. Tuttavia, se viene utilizzato uno strumento di cattura sul lato client, il contenuto può essere acquisito.

- Limitazioni della condivisione dell'audio del sistema
  - L'audio non può essere condiviso utilizzando questa funzione quando si condivide lo schermo con app o schede reindirizzate RAVE e BCR.
  - Questa funzionalità è supportata solo sui desktop pubblicati

Limitazioni sul VDA

- Il nuovo Teams come applicazione pubblicata (senza interruzioni) non è supportato
  - Risolto in CVAD 2402 LTSR, 2203 LTSR CU5 e versioni successive
- Quando si configura l'impostazione High DPI (DPI elevato) dell'app Citrix Workspace su Yes (Sì), la finestra video reindirizzata non è nella posizione corretta. Questa limitazione si verifica quando il fattore di ridimensionamento DPI del monitor è impostato su un valore superiore al 100%

Limitazioni dell'app Citrix Workspace e del VDA

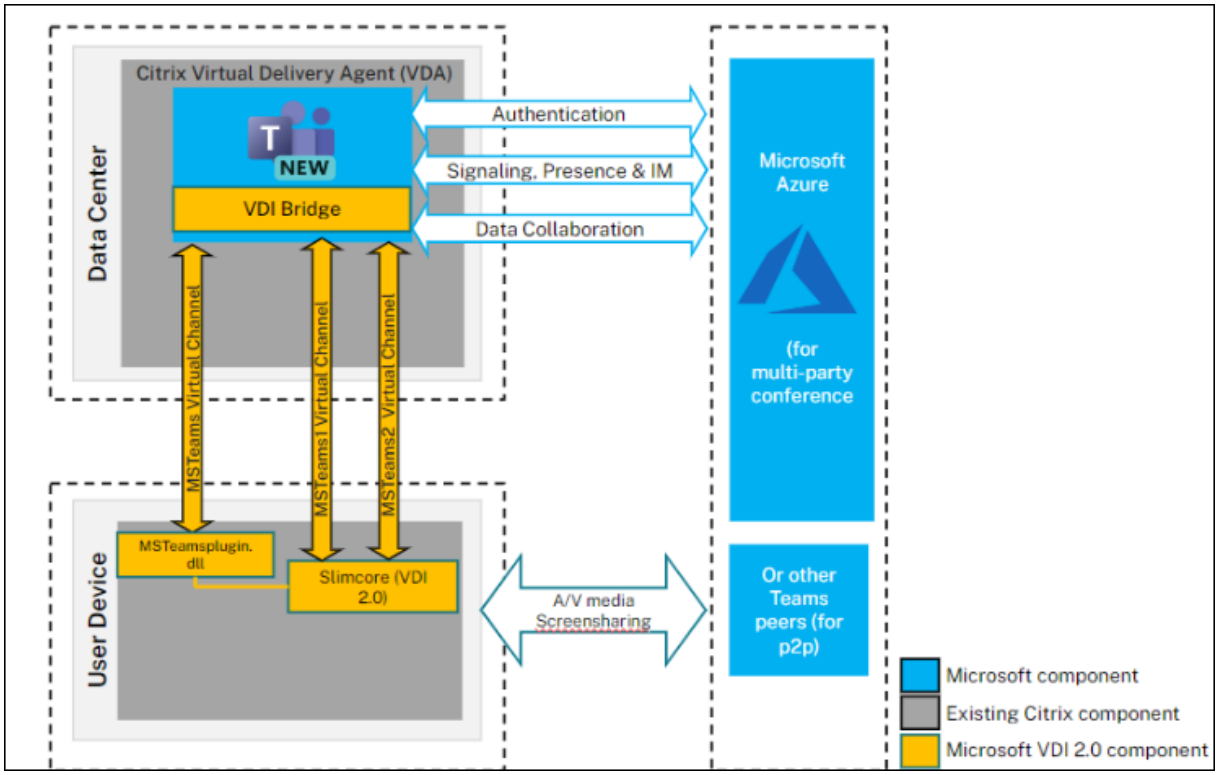
- È possibile controllare il volume di una chiamata ottimizzata solo utilizzando la barra del volume sul computer client, non sul VDA.

Per maggiori dettagli sulle limitazioni, vedere la pagina Microsoft Funzionalità non supportate in VDI.

Ottimizzazione Microsoft SlimCore

August 22, 2024

Nella nuova soluzione VDI per Teams, Microsoft ha sfruttato Citrix Virtual Channel SDK per creare canali virtuali personalizzati e, dal lato endpoint, Microsoft utilizza SlimCore, il Media Engine che oggi alimenta Microsoft Teams (client nativo). In questa ottimizzazione, il responsabile della gestione dei media scaricati è SlimCore anziché HdxRtcEngine. I canali virtuali personalizzati creati da Microsoft fungono da canale di comunicazione tra Teams sul VDI e il SlimCore Media Engine.
Per ulteriori informazioni, vedere Nuova soluzione VDI per Teams e Il futuro di Microsoft Teams.



Requisiti di sistema

Questa sezione illustra le versioni minime e consigliate necessarie per supportare l'ottimizzazione SlimCore per Microsoft Teams. Tenere presente che nelle versioni minime alcune correzioni di bug critici o funzionalità più recenti potrebbero non essere disponibili. Distribuire le versioni consigliate per avere la migliore esperienza con le correzioni e le funzionalità più recenti.

Virtual Delivery Agent (VDA)

> **Nota:**
>
> Se si utilizza 2203 LTSR CU2 o inferiore o 2303 CR o inferiore, vedere CTX682593 per comprendere le limitazioni di tali versioni e pianificare l'aggiornamento alle versioni minime menzionate di seguito per ottenere il supporto dell'ottimizzazione SlimCore.

Versioni minime	Versioni consigliate
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+ o 2402 LTSR e qualsiasi versione CR precedente

App Citrix Workspace (CWA)

> **Nota:**
>
> L'ottimizzazione SlimCore è attualmente disponibile solo per gli endpoint Windows.

Versioni minime	Versioni consigliate
Windows 2203 LTSR (ultima CU); Windows 2302 CR	Windows 2402 LTSR; Windows 2405 CR

Per consigli sulle versioni minime di Teams, sui requisiti del sistema operativo degli endpoint e sui requisiti hardware, vedere la documentazione Microsoft.

Componenti

- New Teams VdiBridge - Questo è il modulo del canale virtuale lato server
- Canale virtuale (VC) personalizzato: questo è il VC personalizzato di proprietà di Microsoft Teams
- Plugin - dll del VC lato client. Questo plug-in è responsabile del download di SlimCore e della pulizia.
- SlimCore - Motore multimediale specifico per il sistema operativo

Distribuzione

1. Assicurarsi di disporre della nuova versione di Microsoft Teams come consigliato nei Prerequisiti.
2. Configurare i criteri dell'elenco degli elementi consentiti dei canali virtuali per consentire i canali virtuali specifici di Microsoft Teams. Questi canali virtuali sono necessari affinché il nuovo client Teams possa connettersi al plug-in lato client. Per ulteriori informazioni sull'elenco dei canali virtuali consentiti, vedere Sicurezza dei canali virtuali.

   Per l'ottimizzazione SlimCore, il nuovo Microsoft Teams necessita di tre canali virtuali personalizzati. Utilizzare i caratteri jolly per consentire l'eseguibile `ms-teams.exe` e i canali virtuali personalizzati:

   ```
   MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   ```


> **Nota:**
>
> - I caratteri jolly per i criteri delle liste di elementi consentiti del canale virtuale sono disponibili in CVAD 2203 LTSR CU2 e versioni successive o in Citrix Virtual Apps and Desktops 2206 CR e versioni successive.
> - Le macchine VDA devono essere riavviate perché il criterio abbia effetto.
> - Il percorso per l'installazione di MSTeams cambia in quanto si tratta di un'applicazione MSIX e quindi sono necessari caratteri jolly. Assicurarsi di inserire nell'elenco degli elementi consentiti le righe esattamente come consigliate sopra.

3. Abilitare il criterio per il nuovo Teams se necessario per un gruppo di utenti specifico (è abilitato per impostazione predefinita a livello globale)
4. Implementare `MSTeamsplugin` sugli endpoint. Per informazioni dettagliate, vedere la sezione Opzioni per installare il plug-in MSTeams. Per ottimizzare con SlimCore sugli endpoint Citrix, Citrix offre ai clienti diversi modi per implementare `MSTeamsplugin`.
5. Vedere la documentazione Microsoft per ulteriori passaggi relativi alla gestione temporanea e alla registrazione di SlimCore in quanto potrebbero esserci casi in cui viene bloccata l'installazione di nuovi pacchetti MSIX del motore multimediale.

Opzioni per installare il plug-in MSTeams

Indipendentemente dal metodo di installazione, il file MSI del plug-in rileva automaticamente la cartella di installazione dell'app Citrix Workspace e colloca MsTeamsPluginCitrix.dll in quella posizione:

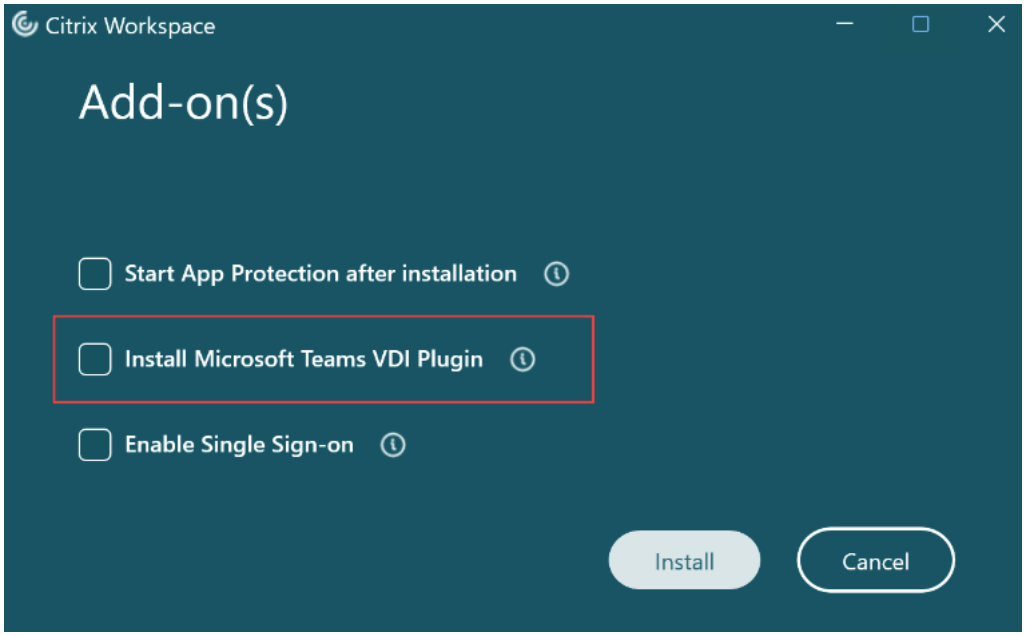
Posizioni del plug-in dll quando il plug-in viene installato tramite le seguenti opzioni con l'installazione dell'amministratore dell'app Citrix Workspace:

- 64 bit: C:\Programmi (x86)\Citrix\ICA Client
- 32 bit: C:\Programmi\Citrix\ICA Client

> **Nota:**
>
> - Assicurarsi che l'app Citrix Workspace sia installata in modalità amministratore. In questo modo ci si assicura che i canali virtuali vengano aperti correttamente.
> - L'installazione del plug-in si interrompe se non viene trovata alcuna app Citrix Workspace sull'endpoint
> - Per le prime esperienze di esecuzione, sono necessari due riavvii dell'app Teams per accedere all'ottimizzazione SlimCore. Per ulteriori informazioni, vedere Verifica che il punto finale sia ottimizzato.

Opzione 1: distribuire il plug-in tramite l'installazione dell'app Citrix Workspace

- Il plug-in MSTeams può essere installato tramite l'interfaccia utente durante la nuova installazione o l'aggiornamento manuale.



- È inoltre possibile installare il plug-in MSTeams tramite l'installazione dalla riga di comando
  - Utilizzare la seguente opzione della riga di comando: /installMSTeamsPlugin
    Esempio: CitrixWorkspaceApp.exe /installMSTeamsPlugin
- Per una nuova installazione, il requisito minimo è l'app Citrix Workspace per Windows 2402 LTSR. Per gli scenari di aggiornamento sul posto, il requisito minimo è l'app Citrix Workspace per Windows 2405 CR.

Opzione 2: scaricare direttamente il file MSI del plug-in

Se non si utilizzano le versioni più recenti in cui è supportata l'installazione del plug-in tramite CWA, è possibile scaricare il file MSI del plug-in da qui e distribuirlo utilizzando strumenti come SCCM in aggiunta a qualsiasi versione dell'app Citrix Workspace supportata esistente.

Opzione 3: distribuire il plug-in utilizzando il Global App Configuration Service

Global App Configuration Service aiuta a gestire le impostazioni delle app per endpoint gestiti e non gestiti e ora è possibile distribuire il plug-in Teams negli endpoint anche tramite GACS.

Vedere la documentazione Microsoft Teams VDI Plug-in Management per dettagli sulla gestione del plug-in Teams tramite GACS.

Considerazioni sul networking

Per i dettagli necessari per l'ottimizzazione SlimCore, vedere Considerazioni sulla rete nella documentazione Microsoft.

Supporto delle funzionalità e versioni supportate

Nel caso dell'ottimizzazione SlimCore, poiché le funzionalità e l'implementazione della soluzione VDI sono di proprietà di Microsoft, vedere la documentazione Microsoft.

Risoluzione dei problemi e altre considerazioni

Per informazioni sul nuovo Teams con l'ottimizzazione Microsoft SlimCore, vedere la documentazione Microsoft.

Limitazioni note

Con l'ottimizzazione SlimCore, poiché le funzionalità e l'implementazione della soluzione VDI sono di proprietà di Microsoft, vedere i Problemi noti documentati da Microsoft.

Ottimizzazione di Microsoft Teams (Classic)

August 22, 2024

> **Nota:**
>
> Il nuovo Microsoft Teams 2.1 è ora disponibile al pubblico per VDA. Questa versione di Microsoft Teams è compatibile con Citrix Microsoft Teams Optimization tramite WebRTC. Per ulteriori informazioni sull'ottimizzazione per il nuovo Teams, vedere Nuovo MS Teams
>
> A partire da Citrix Virtual Apps and Desktops 2402, non è necessario configurare manualmente la voce di registro `msedgewebview2.exe` poiché è consentita per impostazione predefinita.
>
> Le app pubblicate sono ora supportate con il nuovo Microsoft Teams.

Citrix offre ottimizzazione per Microsoft Teams basato su desktop utilizzando Citrix Virtual Apps and Desktops e l'app Citrix Workspace. Per impostazione predefinita, tutti i componenti necessari vengono raggruppati nell'app Citrix Workspace e nel Virtual Delivery Agent (VDA).

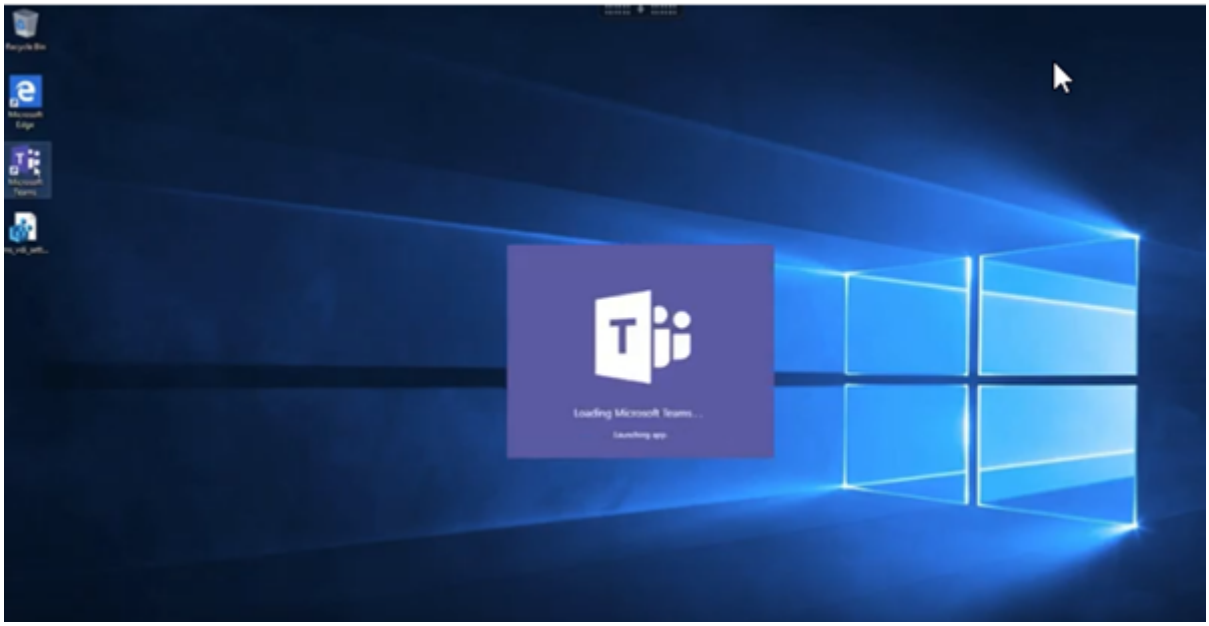
L'ottimizzazione di Citrix per Microsoft Teams include servizi HDX lato VDA e un'API per interfacciarsi con l'app ospitata Microsoft Teams per ricevere comandi. Questi componenti aprono un canale virtuale di controllo (CTXMTOP) verso il motore multimediale sul lato dell'app Citrix Workspace. L'endpoint decodifica i contenuti multimediali e ne esegue il provisioning localmente, spostando nuovamente la finestra dell'app Citrix Workspace nell'app Microsoft Teams ospitata.

L'autenticazione e la segnalazione si verificano in modo nativo nell'app ospitata Microsoft Teams, proprio come gli altri servizi Microsoft Teams (ad esempio chat o collaborazione). Il reindirizzamento audio/video non influisce.

`CTXMTOP` è un comando e un canale virtuale di controllo. Ciò significa che i contenuti multimediali non vengono scambiati tra l'app Citrix Workspace e il VDA.

È disponibile solo il recupero dal client e il rendering sul client.

Questo video dimostrativo dà un'idea di come Microsoft Teams funziona in un ambiente virtuale Citrix.



Installazione di Microsoft Teams

Citrix e Microsoft consigliano di utilizzare l'ultima versione disponibile di Microsoft Teams e di mantenerla aggiornata.
Le versioni dell'app desktop Microsoft Teams con date di rilascio più vecchie di 90 giorni rispetto alla data di rilascio della versione corrente non sono supportate.
Le versioni dell'app desktop Microsoft Teams non supportate presentano agli utenti una pagina di blocco e richiedono di aggiornare l'app.

Per informazioni sulle ultime versioni disponibili, vedere la cronologia degli aggiornamenti per la versione dell'app Microsoft Teams (desktop e Mac).

Si consiglia di seguire le linee guida per l'installazione di Microsoft Teams a livello di macchina. Evitare di utilizzare il programma di installazione .exe che installa Microsoft Teams in `AppData`. Installare invece in `C:\Program Files (x86)\Microsoft\Teams` utilizzando il flag `ALLUSER=1` dalla riga di comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

In questo esempio viene utilizzato anche il parametro `ALLUSERS=1`. Quando si imposta questo parametro, il programma di installazione di Microsoft Teams a livello di macchina viene visualizzato in **Programmi e funzionalità** nel **Pannello di controllo**. Inoltre, in **App e funzionalità** nelle Impostazioni di Windows per tutti gli utenti del computer. Tutti gli utenti possono quindi disinstallare Microsoft Teams se dispongono di credenziali di amministratore.

È importante capire la differenza tra `ALLUSERS=1` e `ALLUSER=1`. È possibile utilizzare il parametro `ALLUSERS=1` in ambienti non VDI e VDI. Utilizzare il parametro `ALLUSER=1` solo negli ambienti VDI per specificare un'installazione per ogni macchina.

In modalità `ALLUSER=1` l'applicazione Microsoft Teams non si aggiorna automaticamente ogni volta che è disponibile una nuova versione. Questa modalità è consigliata per ambienti non persistenti, come app o desktop condivisi ospitati di Windows Server o cataloghi random/in pool di Windows 10. Per ulteriori informazioni, vedere Installare Microsoft Teams utilizzando MSI (sezione Installazione VDI).

Supponiamo che si disponga di un ambiente VDI persistente Windows 10 dedicato. Si desidera che l'applicazione Microsoft Teams si aggiorni automaticamente e si preferisce che Microsoft Teams si installi per ciascun utente in `Appdata/Local`. In questo caso, utilizzare il programma di installazione di `.exe` o il file MSI senza `ALLUSER=1`.

> **Nota:**
>
> Citrix consiglia di installare il VDA prima di installare Microsoft Teams nell'immagine golden. Questo ordine di installazione è necessario perché il flag `ALLUSER=1` abbia effetto. Se è stato installato Microsoft Teams sulla macchina virtuale prima di installare il VDA, disinstallare e reinstallare Microsoft Teams.

Per l'accesso remoto al PC

Si consiglia di installare Microsoft Teams versione 1.4.00.22472 o successiva, dopo aver installato il VDA. In caso contrario, è necessario disconnettersi e accedere nuovamente in modo che Microsoft Teams rilevi il VDA come previsto. La versione 1.4.00.22472 e le successive includono la logica aumentata eseguita al momento dell'avvio di Microsoft Teams e il tempo di accesso per il rilevamento del

VDA. Queste versioni includono anche l'identificazione del tipo di sessione attiva (HDX, RDP o connessione locale alla macchina client). Se si è connessi localmente, le versioni precedenti di Microsoft Teams potrebbero non riuscire a rilevare e disabilitare determinate funzionalità o elementi dell'interfaccia utente. Ad esempio, stanze per sottogruppi di lavoro, finestre a comparsa per riunioni e chat o reazioni alle riunioni.

> **Importante:**
>
> Quando si esegue il roaming da una sessione locale a una sessione HDX e Microsoft Teams viene mantenuto aperto e in esecuzione in background, è necessario uscire e riavviare Microsoft Teams per ottimizzare correttamente con HDX.
> Al contrario, se si utilizza Microsoft Teams in remoto tramite una sessione HDX ottimizzata, disconnettere la sessione HDX e riconnettersi alla stessa sessione di Windows localmente sul dispositivo. Quando si lavora dall'ufficio, è necessario riavviare Microsoft Teams in modo che possa rilevare correttamente lo stato di Remote PC Access (HDX o locale). poiché Microsoft Teams può valutare la modalità VDI solo al momento dell'avvio dell'app e non mentre è già in esecuzione in background. Senza un riavvio, Microsoft Teams potrebbe non riuscire a caricare funzionalità come finestre disancorate, stanze di lavoro o reazioni alle riunioni.

Per App Layering

Se si utilizza Citrix App Layering per gestire le installazioni di VDA e Microsoft Teams in livelli diversi, è necessario creare una chiave del Registro di sistema sui VDA Windows prima di installare Microsoft Teams con il flag `ALLUSER=1` dalla riga di comando. Per ulteriori informazioni, vedere la sezione *Ottimizzazione per Microsoft Teams con Citrix App Layering* in Multimedia.

Consigli per la gestione dei profili

Si consiglia di utilizzare il programma di installazione a livello di macchina per ambienti Windows Server e Windows 10 VDI in pool.

Quando il flag **ALLUSER=1** viene trasferito all'MSI dalla riga di comando (il programma di installazione a livello di macchina), l'app Microsoft Teams viene installata in `C:\Program Files (x86)` (~300 MB). L'app utilizza `AppData\Local\Microsoft\TeamsMeetingAddin` per i log e `AppData\Roaming\Microsoft\Teams` (~ 600-700 MB) per le configurazioni specifiche dell'utente, la memorizzazione nella cache degli elementi nell'interfaccia utente e così via.

> **Importante:**
>
> Se non si trasferisce il flag **ALLUSER=1**, il file MSI inserisce il programma di installazione Teams.exe e `setup.json` in `C:\Program Files (x86)\Teams Installer`. Una chiave del Registro di sistema (TeamsMachineInstaller) viene aggiunta in: `HKEY_LOCAL_MACHINE`

> \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
>
> Un successivo accesso utente attiva invece l'installazione finale in **AppData**.

Programma di installazione a livello di macchina

Di seguito è riportato un esempio di cartelle, collegamenti sul desktop e chiavi del Registro di sistema creati installando un programma di installazione di Microsoft Teams a livello di macchina in una macchina virtuale Windows Server 2016 a 64 bit:

Cartella:

- C:\Program Files (x86)\Microsoft\Teams
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

Collegamento sul desktop:

C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

Registry:

- HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Nome: Teams
- Tipo: REG_SZ
- Valore: C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

> **Nota:**
>
> La posizione del Registro di sistema varia in base ai sistemi operativi sottostanti e al numero di bit.

Consigli

- Si consiglia di disabilitare l'avvio automatico eliminando le chiavi del Registro di sistema di Microsoft Teams. Ciò impedisce che molti accessi che si verificano contemporaneamente (ad esempio, all'inizio della giornata lavorativa) sovraccarichino la CPU della VM.
- Se il desktop virtuale non dispone di una GPU/vGPU, si consiglia di impostare l'opzione **Disable GPU hardware acceleration** (Disabilita l'accelerazione hardware della GPU) nelle **impostazioni** di Microsoft Teams per migliorare le prestazioni. Questa impostazione ("disableGpu":**true**) è memorizzata in %Appdata%\Microsoft\Teams in desktop-config.json. È possibile utilizzare uno script di accesso per modificare tale file e impostare il valore su **true**.

- Se si utilizza Citrix Workspace Environment Management (WEM), abilitare **CPU Spikes Protection** (Protezione dai picchi di utilizzo della CPU) per gestire il consumo del processore per Microsoft Teams.

Programma di installazione per ciascun utente

Quando si utilizza il programma di installazione di `.exe`, il processo di installazione è diverso. Tutti i file sono inseriti in AppData.

Cartella:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Collegamento sul desktop:

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

Registry:

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Procedure consigliate

I consigli sulle procedure consigliate si basano sugli scenari di utilizzo.
L'utilizzo di Microsoft Teams con una configurazione non persistente richiede un gestore di memorizzazione nella cache dei profili per una sincronizzazione efficiente dei dati di runtime di Microsoft Teams. Con un gestore di memorizzazione nella cache dei profili, le informazioni appropriate specifiche dell'utente vengano memorizzate nella cache durante la sessione utente. Ad esempio, le informazioni specifiche dell'utente includono dati utente, profilo e impostazioni. Sincronizzare i dati in queste due cartelle:

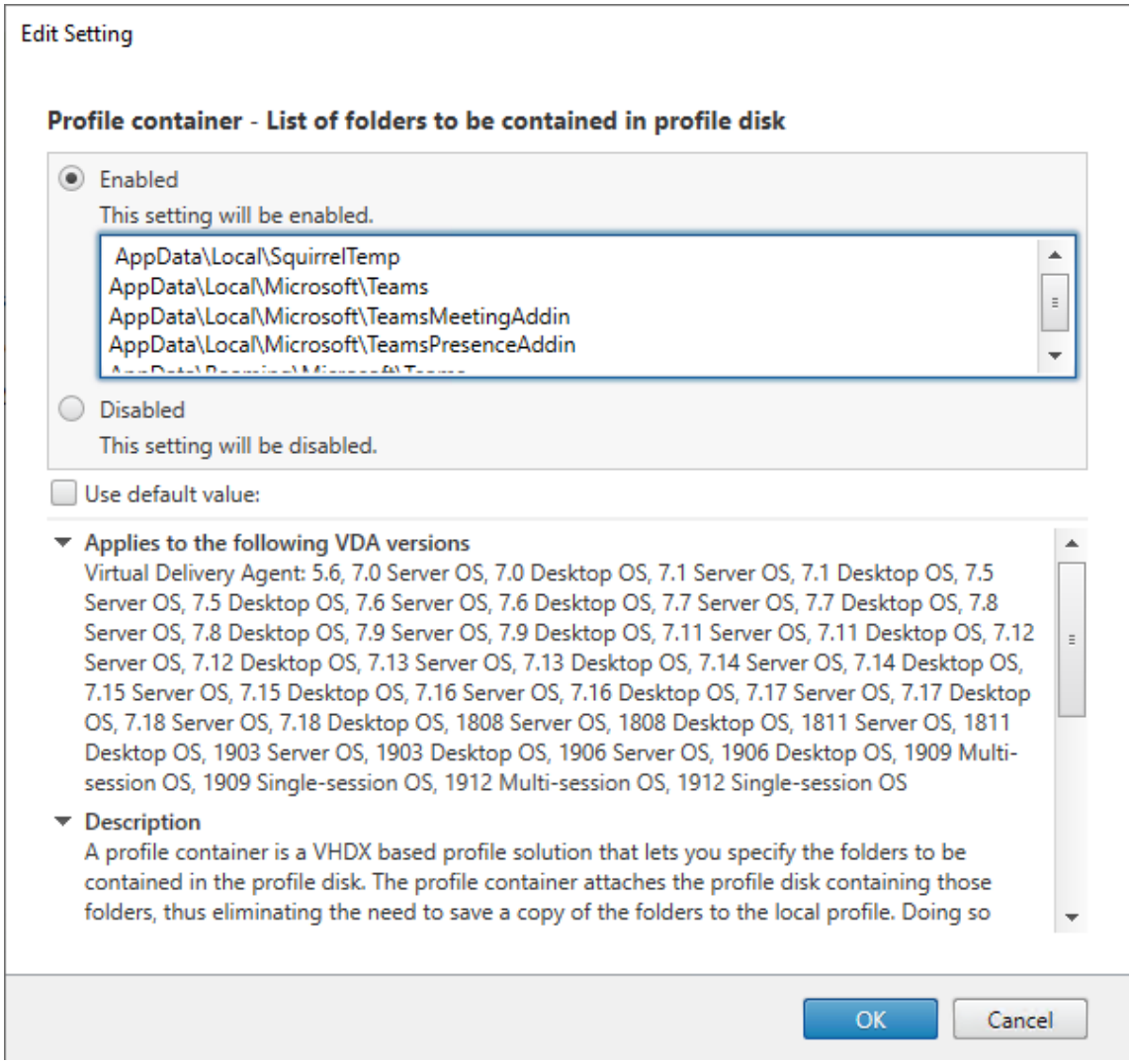
- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Elenco di esclusione dei contenuti di Microsoft Teams memorizzati nella cache per la configurazione non persistente Escludere i file e le directory dalla cartella di memorizzazione nella cache di Microsoft Teams come descritto nella documentazione Microsoft. Questa azione consente di ridurre

le dimensioni della memorizzazione nella cache dell'utente per ottimizzare ulteriormente la configurazione non persistente.

Caso d'uso: scenario con sessione singola In questo scenario, l'utente finale utilizza Microsoft Teams in una posizione alla volta. Non è necessario eseguire Microsoft Teams in due sessioni Windows contemporaneamente. In una distribuzione di desktop virtuale comune, ogni utente viene assegnato a un desktop e Microsoft Teams viene distribuito all'interno del desktop virtuale come un'unica applicazione.
Si consiglia di abilitare il contenitore Citrix Profile e di reindirizzare nel contenitore le directory per utente elencate in Per-user installer.

1. Distribuire il programma di installazione a livello di macchina di Microsoft Teams (**ALLUSER=1**) nell'immagine golden.
2. Abilitare Citrix Profile Management e configurare l'archivio dei profili utente con le autorizzazioni appropriate.
3. Abilitare la seguente impostazione dei criteri di Profile Management (Gestione profili): **File system > Synchronization (Sincronizzazione) > Profile container –List of folders to be contained in profile disk (Contenitore profilo - Elenco delle cartelle che devono essere contenute nel disco del profilo)**.



Elencare tutte le directory per ciascun utente in questa configurazione. È anche possibile configurare queste impostazioni utilizzando il servizio Citrix WEM (Workspace Environment Management).

4. Applicare le impostazioni al gruppo di consegna corretto.
5. Accedere per convalidare la distribuzione.

Requisiti di sistema

Versione minima consigliata - Delivery Controller (DDC) 1906.2

Se si utilizza una versione precedente, vedere Abilitare l'ottimizzazione di Microsoft Teams:

Sistemi operativi supportati:

- Windows Server 2022, 2019, 2016, 2012R2 edizioni Standard e per centri dati e con l'opzione Server Core

Versione minima - Virtual Delivery Agent (VDA) 1906.2

Sistemi operativi supportati:

- Windows 11
- Windows 10 a 64 bit, versioni 1607 e successive. Le app ospitate da VM sono supportate nell'app Citrix Workspace per Windows 2109.1 e versioni successive.
- Windows Server 2022, 2019, 2016 e 2012 R2 (edizioni standard e per data center).

Requisiti:

- BCR_x64.msi: file MSI che include il codice di ottimizzazione di Microsoft Teams e viene avviato automaticamente dalla GUI. Se si utilizza l'interfaccia della riga di comando per l'installazione del VDA, non escluderlo.

Versione consigliata: versione corrente più recente dell'app Citrix Workspace per Windows e versione minima: app Citrix Workspace 1907 per Windows

- Windows 11.
- Windows 10 (edizioni a 32 bit e 64 bit, incluse le edizioni Embedded) (il supporto di Windows 7 è stato interrotto alla versione 2006) (il supporto di Windows 8.1 è stato interrotto alla versione 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Architetture di processore (CPU) supportate: x86 e x64 (ARM non è supportato).
- Requisiti dell'endpoint: CPU dual core di circa 2,2-2,4 GHz in grado di supportare una risoluzione HD a 720p durante una chiamata in videoconferenza peer-to-peer.
- CPU dual o quad-core con velocità base più basse (~1,5 GHz) dotate di Intel Turbo Boost o AMD Turbo Core con possibile aumento fino ad almeno 2,4 GHz.
- Thin client HP verificati: t630/t640, t730/t740, mt44/mt45.
- Thin client Dell verificati: 5070, 5470 Mobile TC e AIO.
- Thin Client 10ZiG verificati: 4510 e 5810q.
- Per un elenco completo degli endpoint verificati, vedere Thin client.
- L'app Citrix Workspace richiede almeno 600 MB di spazio libero su disco e 1 GB di RAM.
- Il requisito minimo di Microsoft .NET Framework è la versione 4.8. L'app Citrix Workspace scarica e installa automaticamente .NET Framework se non è presente sul sistema.

Gli amministratori possono abilitare/disabilitare Microsoft Teams a partire dalla modalità ottimizzata modificando il criterio Optimization for Microsoft Teams. Gli utenti che iniziano in modalità ottimizzata nell'app Citrix Workspace non possono di disabilitare Microsoft Teams.

Versione minima: app Citrix Workspace 2006 per Linux

Per ulteriori informazioni, vedere Ottimizzazione per Microsoft Teams nella documentazione dell'app Citrix Workspace per Linux.

Software:

- `GStreamer` 1.0 o versione successiva o Cairo 2
- `libc++-9.0` o più versione successiva
- `libgdk` 3.22 o versione successiva
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 o versione successiva

Miglioramento dell'autenticazione:

- Libreria Libsecret
- libreria libunwind-12. Per ulteriori informazioni, vedere Adding the libunwind-12 library dependency for llvm-12.

Hardware:

- CPU dual-core da almeno 1,8 GHz in grado di supportare una risoluzione HD a 720p durante una chiamata in videoconferenza peer-to-peer
- CPU dual o quad-core con una velocità base di 1,8 GHz e un'alta velocità Intel Turbo Boost di almeno 2,9 GHz

Per un elenco completo degli endpoint verificati, vedere Thin client.

Per ulteriori informazioni, vedere Prerequisiti per installare l'app Citrix Workspace.

È possibile disabilitare l'ottimizzazione di Microsoft Teams aggiornando il valore del campo **VDWEBRTC** su Off nel file `/opt/Citrix/ICAClient/config/module.ini`. Il valore predefinito è VDWEBRTC=On. Una volta completato l'aggiornamento, riavviare la sessione. (è richiesta l'autorizzazione root).

Versione minima: app Citrix Workspace 2012 per Mac

Sistemi operativi supportati:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 e versione successiva.
- macOS Monterey.

Funzionalità supportate:

- Audio
- Video
- Ottimizzazione della condivisione dello schermo (in entrata e in uscita)

> **Nota:**
>
> L'app Citrix Viewer richiede l'accesso alle preferenze di sicurezza e privacy di macOS perché la condivisione dello schermo possa funzionare. Gli utenti configurano questa preferenza accedendo al **menu Apple > Preferenze di sistema > Sicurezza e privacy > scheda Privacy > Registrazione dello schermo** e selezionando **Citrix Viewer**.

L'ottimizzazione di Microsoft Teams funziona per impostazione predefinita con l'app Citrix Workspace 2012 o versioni successive e macOS 10.15.

Se si desidera disabilitare l'ottimizzazione di Microsoft Teams, eseguire questo comando nel terminale e riavviare l'app Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Versione minima: l'ultima versione dell'app Citrix Workspace per ChromeOS in esecuzione sull'ultima versione di ChromeOS

Hardware:

- Processori che funzionano alla pari o meglio del processore Intel i3, quad core da 2,4 GHz.

Funzionalità supportate:

- Audio
- Video
- Ottimizzazione della condivisione dello schermo (in entrata e in uscita): disabilitata per impostazione predefinita. Consultare queste impostazioni per istruzioni su come abilitarla.

Scalabilità di un singolo server

Questa sezione fornisce consigli e indicazioni su come stimare il numero di utenti o macchine virtuali (VM) che possono essere supportati su un singolo host fisico. Questo è comunemente indicato come Scalabilità per server singolo di Citrix Virtual Apps and Desktops (SSS). Nel contesto di Citrix Virtual Apps (CVA) o della virtualizzazione delle sessioni, è anche comunemente noto come densità degli utenti. L'idea è scoprire quanti utenti o quante macchine virtuali possono essere eseguiti su un singolo componente hardware che esegue un hypervisor principale.

> **Nota:**
>
> Questa sezione include una guida per stimare l'SSS. La guida è di alto livello e potrebbe non essere necessariamente specifica per la propria situazione o il proprio ambiente specifico. L'unico modo per comprendere veramente l'SSS di Citrix Virtual Apps and Desktops è utilizzare uno strumento di test di scalabilità o carico come Login VSI. Citrix consiglia di utilizzare questa guida e queste semplici regole per stimare rapidamente solo l'SSS. Tuttavia, Citrix consiglia di utilizzare Login VSI o lo strumento di test di carico preferito per convalidare i risultati, soprattutto prima di acquistare hardware o prendere decisioni finanziarie.

Hardware (sistema in prova)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (max Turbo 3,70 GHz), 12 core per socket, doppio socket con Hyperthreading abilitato
- 382 GB di RAM
- Archiviazione RAID 0 SSD locale (11 dischi) 6 TB

Software

Una singola macchina virtuale (40 processori logici) con Windows 2019 (TSVDA) che esegue Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

Terminologia

- Carico di lavoro del lavoratore della conoscenza: include Acrobat Reader, Freemind/Java, Photo Viewer, Edge e app MS Office come Excel, Outlook, PowerPoint e Word.
- Baseline: test di scalabilità server eseguiti con il carico di lavoratore della conoscenza (senza Microsoft Teams)
- Carico di lavoro di Microsoft Teams: carico di lavoro tipico dei lavoratori della conoscenza + Microsoft Teams

Come Microsoft Teams viene sottoposto a test di stress

- Microsoft Teams è ottimizzato con HDX. Pertanto, tutta l'elaborazione multimediale viene scaricata sull'endpoint o sul client e non fa parte della misurazione.
- Tutti i processi di Microsoft Teams sono stati arrestati o interrotti prima dell'inizio del carico di lavoro.

- Aprire Microsoft Teams (avvio a freddo).
- Misurare il tempo impiegato da Microsoft Teams per caricare e catturare l'attenzione della finestra principale di Microsoft Teams.
- Passare alla finestra di chat usando i tasti di scelta rapida.
- Passare alla finestra del calendario usando i tasti di scelta rapida.
- Inviare il messaggio di chat a un utente specifico utilizzando le scorciatoie da tastiera.
- Passare alla finestra di Microsoft Teams utilizzando i tasti di scelta rapida.

Risultati

- Impatto sulla scalabilità del 40% con Microsoft Teams Workload (81 utenti) rispetto a Baseline (137 utenti).
- L'aumento della capacità del server di circa il 40% (in CPU) ripristina il numero di utenti come con il carico di lavoro Baseline.
- 20% di memoria extra richiesta con Microsoft Teams Workload, rispetto a Baseline.
- Aumento delle dimensioni di archiviazione per utente di 512-1024 MB.
- circa il 50% di incremento in scrittura IOPS, circa il 100% di incremento nelle letture IOPS. Microsoft Teams può avere un impatto significativo in un ambiente con archiviazione più lenta.

Supporto delle funzionalità e versioni supportate

Funzione	Microsoft Teams (versione minima)	VDA (versione minima)	App Citrix Workspace per Windows CR (versione minima)	App Citrix Workspace per Mac (versione minima)	App Citrix Workspace per Linux (versione minima)	App Citrix Workspace per ChromeOS (versione minima)
Audio/Video (P2P e conferenza)	versione attuale meno 90 giorni	1906	1907	2009	2004	2105.5
Condivisione dello schermo	Versione attuale meno 90 giorni	1906	1907	2012	2006	2105.5

Funzione	Microsoft Teams (versione minima)	VDA (versione minima)	App Citrix Workspace per Windows CR (versione minima)	App Citrix Workspace per Mac (versione minima)	App Citrix Workspace per Linux (versione minima)	App Citrix Workspace per ChromeOS (versione minima)
i. Indicatore schermo Bordo rosso	Versione attuale meno 90 giorni	1906	2002	2012	2006	No
ii. Limita l' acqui-sizione in Desktop Viewer	Versione attuale meno 90 giorni	1906	2009.5	2012	2006	No
iii. Multi-monitor	Versione attuale meno 90 giorni	1912 CU6+	2106 (1)	2106	2106	No
DTMF	Versione attuale meno 90 giorni	N/A	2102	2101	2101	2111.1
Supporto dei server proxy	Versione attuale meno 90 giorni	N/A	2012 (2)	2104 (3)	2101 (3)	2305
Condivisione di app	Versione attuale meno 90 giorni	2109	2109.1	2203.1	2209	No
Sottotitoli live	Versione attuale meno 90 giorni	N/A (4)	2109.1	2109	2109	2303

Funzione	Microsoft Teams (versione minima)	VDA (versione minima)	App Citrix Workspace per Windows CR (versione minima)	App Citrix Workspace per Mac (versione minima)	App Citrix Workspace per Linux (versione minima)	App Citrix Workspace per ChromeOS (versione minima)
e911 dinamico	Versione attuale meno 90 giorni	N/A	2112.1	2112	2112	2112
Concedere il controllo	Versione attuale meno 90 giorni	N/A	2112.1	2203.1	No	No
Richiedi il controllo	Versione attuale meno 90 giorni	N/A	2112.1	2203.1	2203	2303
Multifinestra	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Trascrizioni delle riunioni	Versione attuale meno 90 giorni	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Sfocatura dello sfondo	Versione attuale meno 90 giorni	2112, 1912 CU6+	2207	2301	2212	2303

1. Visualizzatore CD solo in modalità a schermo intero. MAIUSC+F2 non è supportato.
2. Negotiate/Kerberos, NTLM, Basic e Digest. Sono supportati anche i file Pac.
3. Solo anonimo.
4. Se il VDA è la versione 2112 o una versione superiore, Live Captions funziona solo se la versione dell'app Citrix Workspace è 2203.1 per MAC e 2203 Linux o 2112 per Windows. Questo perché Live Captions si comporta in modo diverso se Microsoft Teams è in modalità interfaccia utente a finestra singola o multifinestra.
5. La modalità multifinestra è stata introdotta nel VDA versione 2112, ma è stata trasferita alla versione VDA 1912 LTSR CU6.

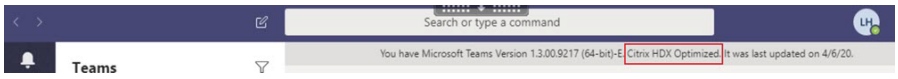
> **Nota:**
>
> - Tutte le funzionalità elencate nell'**app Citrix Workspace per Windows 1912 CU6 (o versione successiva)** sono applicabili all'app Citrix Workspace per Windows 2203.1 LTSR CU1.
> - Microsoft ha reso obsoleto il supporto della modalità a finestra singola in Microsoft Teams. Per garantire la conformità, è necessario aggiornare il VDA alla versione 1912 CU6+ LTSR e all'app Citrix Workspace 2203 CU2+ o superiore, che supporta la modalità multifinestra.

Abilitare l'ottimizzazione di Microsoft Teams

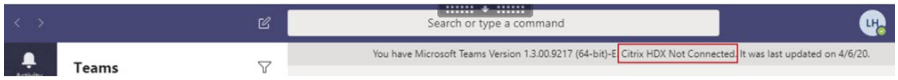
Per abilitare l'ottimizzazione per Microsoft Teams, utilizzare i criteri di gestione della console descritti nel criterio di reindirizzamento di Microsoft Teams. Questo criterio è **ON** (attivato) per impostazione predefinita. Oltre all'abilitazione di questo criterio, HDX verifica che la versione dell'app Citrix Workspace corrisponda almeno alla versione minima richiesta. Se il criterio è stato abilitato e la versione dell'app Citrix Workspace è supportata, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRe** viene impostato automaticamente su **1** sul VDA. Microsoft Teams legge la chiave per caricarsi in modalità VDI.

> **Nota:**
>
> Se si utilizzano VDA versione 1906.2 o successiva con versioni precedenti del controller (ad esempio, versione 7.15) che non dispongono del criterio disponibile in Manage console (Gestione console) (Studio), il VDA può comunque essere ottimizzato. L'ottimizzazione HDX per Microsoft Teams è abilitata per impostazione predefinita nel VDA.

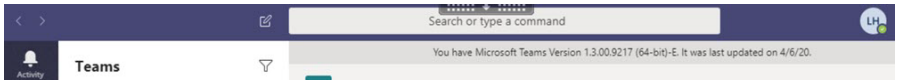
Se si fa clic su **About (Informazioni) > Version (Versione)**, viene visualizzata la legenda **Citrix HDX Optimized (Ottimizzato per Citrix HDX)**:



Se viene visualizzato il messaggio **Citrix HDX Not Connected** (Citrix HDX non connesso), l'API Citrix viene caricata in Microsoft Teams. Il caricamento dell'API è il primo passo verso il reindirizzamento. Ma c'è un errore nelle parti successive dello stack. L'errore è molto probabilmente nei servizi VDA o nell'app Citrix Workspace.



Se non viene visualizzata alcuna legenda, Microsoft Teams non è riuscito a caricare l'API Citrix. Uscire da Microsoft Teams facendo clic con il pulsante destro del mouse sull'icona dell'area di notifica e riavviare l'applicazione. Assicurarsi che il criterio Manage console (Gestisci console) non sia impostato su **Prohibited** (Non consentito) e che la versione dell'app Citrix Workspace sia supportata.



Importante: riconnessioni di sessione

- Potrebbe essere necessario riavviare Microsoft Teams per ottenere una sessione ottimizzata per HDX quando la connettività cambia. Ad esempio, se si sta eseguendo il roaming da un endpoint non supportato (app Workspace per iOS, Android o versioni precedenti di Windows/Linux/Mac) a uno supportato (app Workspace per Windows/Linux/Mac/ChromeOS/HTML5) o nella direzione opposta.
- Un rilancio di Microsoft Teams è necessario anche se è stata installata l'app utilizzando il programma di installazione .exe di Microsoft Teams nel VDA. Il programma di installazione .exe è consigliato per le distribuzioni VDI persistenti. In questi casi, Microsoft Teams può aggiornarsi automaticamente mentre la sessione HDX è in stato disconnesso. Pertanto, gli utenti che si riconnettono a una sessione HDX trovano che l'esecuzione di Microsoft Teams non è ottimizzata.
- Quando si passa da una sessione locale a una sessione HDX, si deve riavviare Microsoft Teams per l'ottimizzazione con HDX. Questa azione è necessaria in uno scenario di accesso remoto al PC.

Requisiti di rete

Microsoft Teams si affida ai server del processore di contenuti multimediali di Microsoft 365 per riunioni o chiamate con più partecipanti. Inoltre, Microsoft Teams si basa sui relè di trasporto di Microsoft 365 per questi scenari:

- Due peer in una chiamata point-to-point non hanno connettività diretta
- Un partecipante non dispone di connettività diretta al processore multimediale.

Di conseguenza, l'integrità della rete tra il peer e il cloud di Microsoft 365 determina le prestazioni della chiamata. Per linee guida dettagliate sulla pianificazione della rete, fare riferimento all'articolo Principi di connettività di rete di Microsoft 365.

Si consiglia di valutare l'ambiente per identificare eventuali rischi e requisiti che possono influenzare la distribuzione globale di voce e video nel cloud.
Utilizzare lo strumento di valutazione della rete Skype for Business per verificare se la rete è pronta per Microsoft Teams. Per informazioni sull'assistenza, vedere Supporto.

Riepilogo delle principali raccomandazioni di rete per il traffico RTP (Real Time Protocol)

- Connettersi alla rete di Microsoft 365 il più direttamente possibile dalla filiale.
- Pianificare e fornire una larghezza di banda sufficiente presso la filiale.

- Verificare la connettività e la qualità della rete di ogni filiale.
- Se è necessario utilizzare uno dei seguenti elementi presso la filiale, assicurarsi che il traffico RTP/UDP (gestito da HdxRtcEngine.exe nell'app Citrix Workspace) non sia ostacolato.
  - Ignorare i server proxy
  - Intercettazione SSL di rete
  - Dispositivi di ispezione profonda dei pacchetti
  - Hairpin VPN (utilizzare lo split tunneling se possibile)

> **Importante: configurazione VPN Split tunnel**
>
> Il traffico di HdxRtcEngine.exe deve essere deviato dal tunnel VPN e autorizzato a utilizzare la connessione Internet locale dell'utente per connettersi direttamente al servizio. Il modo in cui ciò viene realizzato dipende dal prodotto VPN e della piattaforma della macchina utilizzati, ma la maggior parte delle soluzioni VPN consente una semplice configurazione dei criteri per applicare questa logica. Per ulteriori informazioni sulla guida allo split tunnelling specifico per la piattaforma VPN, vedere questo articolo Microsoft.

Il motore multimediale WebRTC nell'app Workspace (HdxRtcEngine.exe) utilizza il protocollo SRTP (Secure Real-Time Transport Protocol) per i flussi multimediali di cui viene eseguito l'offloading nel client. SRTP assicura riservatezza e autenticazione all'RTP. Per questa funzione, vengono utilizzate le chiavi simmetriche (negoziate con DTLS) per crittografare i media e controllare i messaggi utilizzando il cifrario di crittografia AES.

Le seguenti metriche sono consigliate per un'esperienza utente positiva:

Metrica	Endpoint a Microsoft 365
Latenza (a senso unico)	< 50 msec
Latenza (RTT)	< 100 msec
Perdita di pacchetti	<1% durante ogni intervallo di 15 secondi
Jitter inter-arrivo dei pacchetti	<30 ms durante ogni intervallo di 15 secondi

Per ulteriori informazioni, vedere Preparare la rete dell'organizzazione per Microsoft Teams.

Per quanto riguarda i requisiti di larghezza di banda, l'ottimizzazione per Microsoft Teams può utilizzare un'ampia gamma di codec per audio (OPUS/G.722/PCM G711) e video (H264).

I peer negoziano questi codec durante il processo di creazione delle chiamate utilizzando l'offerta/risposta SDP (Session Description Protocol).
Le raccomandazioni minime di Citrix per utente sono:

Tipo	Larghezza di banda	Codec
Audio (tutte le direzioni)	~ 90 kbps	G.722
Audio (tutte le direzioni)	~ 60 kbps	Opus*
Video (tutte le direzioni)	~ 700 kbps	H264 360p @ 30 fps 16:9
Condivisione dello schermo	~ 300 kbps	H264 1080p @ 15 fps

* Opus supporta la codifica dei bitrate costante e variabile da 6 kbps fino a 510 kbps.

Opus e H264 sono i codec preferiti per le chiamate peer-to-peer e in conferenza.

> **Importante:**
>
> Per quanto riguarda le prestazioni, la codifica è più costosa della decodifica per l'uso della CPU sul computer client. È possibile codificare la massima risoluzione di codifica nell'app Citrix Workspace per Linux e Windows. Vedere Stima delle prestazioni dell'encoder e Ottimizzazione per Microsoft Teams.

Server proxy

A seconda della posizione del proxy, considerare quanto segue:

- Configurazione proxy sul VDA:

  Se si configura un server proxy esplicito nel VDA e si instradano le connessioni all'host locale tramite un proxy, il reindirizzamento non riesce. Per configurare correttamente il proxy, è necessario selezionare l'impostazione **Bypass proxy servers for local address** (Ignora i server proxy per l'indirizzo locale) in **Opzioni Internet > Connessioni > Impostazioni LAN > Server proxy** e ignorare `127.0.0.1:9002`.

  Se si utilizza un file PAC, lo script di configurazione del proxy VDA del file PAC deve restituire **DIRECT** per `wss://127.0.0.1:9002`. In caso contrario, l'ottimizzazione non riesce. Per assicurarsi che lo script restituisca **DIRECT**, utilizzare `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configurazione proxy sull'app Citrix Workspace:

  Se la filiale è configurata per accedere a Internet tramite un proxy, queste versioni supportano i server proxy:

  - App Citrix Workspace per Windows versione 2012 (Negotiate/Kerberos, NTLM, Basic e Digest; sono supportati anche i file Pac)

- App Citrix Workspace per Windows versione 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Sono supportati anche i file Pac)
- App Citrix Workspace per Linux versione 2101 (autenticazione anonima)
- App Citrix Workspace per Mac versione 2104 (autenticazione anonima)

I dispositivi client con versioni precedenti dell'app Citrix Workspace non possono leggere le configurazioni proxy. Questi dispositivi inviano il traffico direttamente ai server TURN di Microsoft 365.

> **Importante:**
>
> - Verificare che il dispositivo client possa connettersi al server DNS per effettuare le risoluzioni DNS. Un dispositivo client deve essere in grado di risolvere i seguenti FQDN del server Microsoft Teams Relay:
>
>   - `worldaz.relay.teams.microsoft.com`
>   - `inaz.relay.teams.microsoft.com`
>   - `uaeaz.relay.teams.microsoft.com`
>   - `euaz.relay.teams.microsoft.com`
>   - `usaz.relay.teams.microsoft.com`
>   - `turn.dod.teams.microsoft.us`
>   - `turn.gov.teams.microsoft.us`
>
> Se le richieste DNS non hanno esito positivo, le chiamate P2P con utenti esterni e la creazione di supporti per le teleconferenze con la creazione di media non riescono.
>
> - La posizione del server della conferenza viene selezionata in base alla posizione del desktop virtuale (non al client) del primo partecipante.

Percorsi per l'avvio di chiamate e il flusso di contenuti multimediali

Quando possibile, il motore multimediale HDX WebRTC nell'app Citrix Workspace (HdxRtcEngine.exe) tenta di stabilire una connessione SRTP (Secure Real-Time Transport Protocol) di rete diretta tramite UDP (User Datagram Protocol) in una chiamata peer-to-peer. Se le porte UDP alte sono bloccate, il motore multimediale torna a TCP/TLS 443.

Il motore multimediale HDX supporta ICE, STUN (Session Traversal Utilities for NAT) e TURN (Traversal Using Relays around NAT) per individuare candidati e stabilire connessioni. Questo supporto significa che l'endpoint deve essere in grado di eseguire risoluzioni DNS.

Si consideri uno scenario in cui non esiste un percorso diretto tra i due peer o tra un peer e un server di conferenza e si sta partecipando a una chiamata o a una riunione con più parti. HdxRtcEngine.exe utilizza un relé server di trasporto Microsoft Teams in Microsoft 365 per raggiungere l'altro peer o il processore multimediale, dove sono ospitate le riunioni. Il computer client deve avere accesso a tre intervalli di indirizzi IP di subnet di Microsoft 365 e quattro porte UDP (o TCP/TLS 443 come fallback se

UDP è bloccato). Per ulteriori informazioni, vedere il diagramma Architettura in Configurazione delle chiamate e URL di Office 365 e intervalli di indirizzi IP ID 11.

ID	Categoria	Indirizzi	Porte di destinazione
11	Ottimizzazione richiesta	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (fallback)

Questi intervalli includono sia i relè di trasporto che i processori multimediali, con un sistema di bilanciamento del carico di Azure come front-end.
I relè di trasporto di Microsoft Teams forniscono funzionalità STUN e TURN, ma non sono endpoint ICE. Inoltre, i relè di trasporto di Microsoft Teams non interrompono gli elementi multimediali o TLS e non eseguono alcuna transcodificazione. Possono collegare TCP (se HdxRtcEngine.exe utilizza TCP) a UDP quando inoltrano il traffico ad altri peer o processori multimediali.

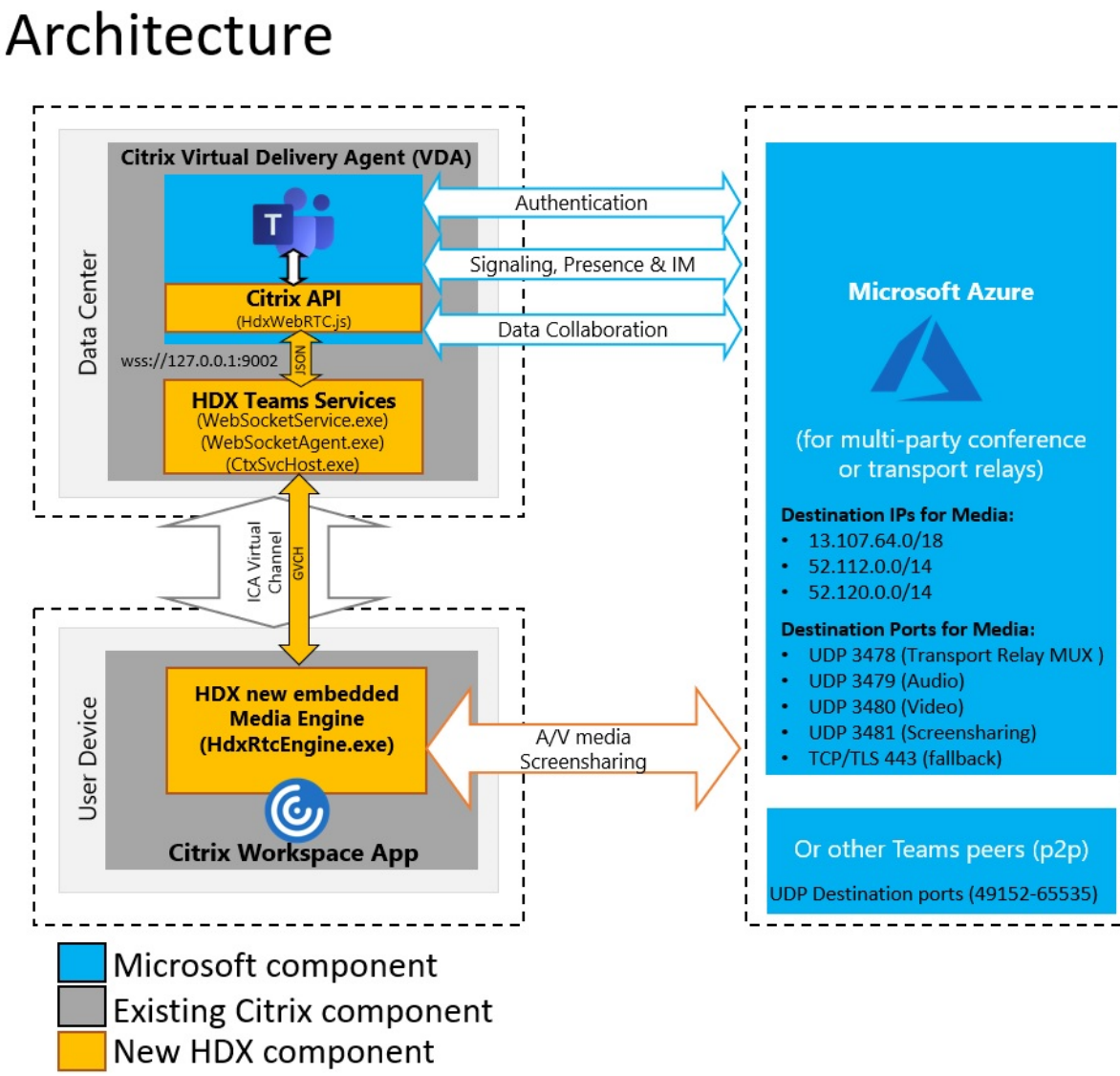
Il motore multimediale WebRTC dell'app Workspace contatta il relè di trasporto di Microsoft Teams più vicino nel cloud di Microsoft 365. Il motore multimediale utilizza IP anycast e le porte UDP 3478-3481 (porte UDP diverse per carico di lavoro, anche se può verificarsi il multiplexing) o 443 TCP/TLS per i fallback. La qualità delle chiamate dipende dal protocollo di rete sottostante. Poiché UDP è sempre consigliato su TCP, si consiglia di progettare le reti in modo da supportare il traffico UDP nella filiale.

Se Microsoft Teams è stato caricato in modalità ottimizzata e HdxRtcEngine.exe è in esecuzione sull'endpoint, gli errori ICE potrebbero causare un errore di configurazione delle chiamate o audio/video monodirezionale. Quando una chiamata non può essere completata o i flussi multimediali non sono full duplex, controllare prima la **traccia Wireshark** sull'endpoint. Per ulteriori informazioni sul processo di raccolta dei candidati ICE, vedere "Raccolta dei log"nella sezione Supporto.

> **Nota:**
>
> Se gli endpoint non hanno accesso a Internet, potrebbe comunque essere possibile per gli utenti effettuare una chiamata peer-to-peer se si trovano entrambi sulla stessa LAN. Non è possibile tenere riunioni. In questo caso, c'è un timeout di 30 secondi prima dell'inizio della configurazione della chiamata.

Configurazione delle chiamate

Utilizzare questo diagramma di architettura come riferimento visivo per la sequenza del flusso di chiamata. I passaggi corrispondenti sono indicati nel diagramma.



Architettura

1. Avviare Microsoft Teams.
2. Microsoft Teams si autentica in O365. I criteri tenant vengono spostati al client Microsoft Teams e le informazioni pertinenti relative a TURN e al canale di segnalazione vengono inoltrate all'app.
3. Microsoft Teams rileva che è in esecuzione in un VDA ed effettua chiamate API all'API JavaScript Citrix.
4. Il JavaScript Citrix in Microsoft Teams apre una connessione WebSocket sicura a WebSocketService.exe in esecuzione sul VDA, che genera WebSocketAgent.exe all'interno della sessione utente.
5. WebSocketAgent.exe crea un'istanza di un canale virtuale generico chiamando il servizio di reindirizzamento di Microsoft Teams Citrix HDX (CtxSvcHost.exe).

6. wfica32.exe (motore HDX) dell'app Citrix Workspace genera un nuovo processo chiamato HdxRtcEngine.exe, che è il nuovo motore WebRTC utilizzato per l'ottimizzazione di Microsoft Teams.
7. Il motore multimediale Citrix e Teams.exe hanno un percorso di canale virtuale a 2 vie e possono iniziare a elaborare le richieste multimediali.

   ——Chiamate dell'utente——

8. Il **peer A** fa clic sul pulsante di **chiamata**. Teams.exe comunica con i servizi Microsoft Teams in Microsoft 365 stabilendo un percorso di segnalazione end-to-end con il **peer B**. Microsoft Teams chiede a HdxRtcEngine una serie di parametri di chiamata supportati (codec, risoluzioni e così via, questo è noto come offerta SDP [Session Description Protocol]). Questi parametri di chiamata vengono quindi inoltrati utilizzando il percorso di segnalazione ai servizi Microsoft Teams in Microsoft 365 e da lì all'altro peer.
9. L'offerta/risposta SDP (negoziazione a passaggio singolo) avviene attraverso il canale di segnalazione e vengono completati i controlli di connettività ICE (attraversamenti NAT e firewall utilizzando le richieste di associazione STUN). Quindi, i contenuti multimediali SRTP (Secure Real-time Transport Protocol) vanno direttamente da HdxRtcEngine.exe all'altro peer e viceversa (o i Conference Server Microsoft 365 se si tratta di una riunione).

Microsoft Phone System

Phone System è la tecnologia Microsoft che consente il controllo delle chiamate e PBX nel cloud di Microsoft 365 con Microsoft Teams. L'ottimizzazione per Microsoft Teams supporta Phone System, utilizzando i piani di chiamata di Microsoft 365 o il routing diretto. Con il routing diretto è possibile connettere il session border controller supportato da Microsoft Phone System direttamente senza alcun software locale aggiuntivo.
Sono supportati code di chiamata, trasferimento, inoltro, messa in pausa, disattivazione dell'audio e ripresa di una chiamata.

DTMF

La funzione DTMF (Dual Tone Multi Frequency) è supportata con queste versioni dell'app Citrix Workspace (e versioni successive):

- App Citrix Workspace per Windows versione 2102
- App Citrix Workspace per Windows LTSR 1912 CU5 (solo sistema operativo Windows 10)
- App Citrix Workspace per Linux versione 2101
- App Citrix Workspace per Mac versione 2101
- App Citrix Workspace per ChromeOS versione 2111.1

Supporto di e911 dinamico

A partire dalla versione 2112, l'app Citrix Workspace supporta le chiamate di emergenza dinamiche. Se utilizzato in Microsoft Calling Plans, Operator Connect e Direct Routing, consente di eseguire le seguenti operazioni:

- Configurare e indirizzare le chiamate di emergenza.
- Informare il personale di sicurezza.

La notifica viene fornita in base alla posizione corrente dell'app Citrix Workspace in esecuzione sull'endpoint, anziché sul client Microsoft Teams in esecuzione sul VDA.

La legge di Ray Baum richiede che la posizione inviabile di chi chiama il 911 sia trasmessa al Public Safety Answering Point (PSAP) appropriato. L'ottimizzazione di Microsoft Teams con HDX è conforme alla legge di Ray Baum se utilizzata con le seguenti versioni dell'app Citrix Workspace:

- App Citrix Workspace per Windows versione 2112.1 e successiva
- App Citrix Workspace per Linux versione 2112 e successiva
- App Citrix Workspace per Mac versione 2112 e successiva
- App Citrix Workspace per ChromeOS versione 2112 e successiva

Per abilitare le chiamate di emergenza dinamiche, l'amministratore deve utilizzare l'interfaccia di amministrazione di Microsoft Teams e configurare quanto segue per creare una mappa della posizione di rete o di emergenza:

- Impostazioni di rete
- Servizio informazioni sulla posizione (LIS)

Per ulteriori informazioni sulle chiamate di emergenza dinamiche, vedere la documentazione di Microsoft.

Le informazioni sulla posizione inviabili che l'app Citrix Workspace inoltra a Microsoft Teams sono:

- ID chassis/ID porta utilizzando il Link Layer Discovery Protocol (LLDP) per le connessioni Ethernet/Switch. Ethernet/Switch (LLDP) è supportato su:
  - Versioni Windows 8.1 e 10
  - macOS, che richiede il software di abilitazione LLDP. Per scaricare il software di abilitazione LLDP, passare a `www.microsoft.com` e cercare il software di abilitazione LLDP.
  - Linux, che richiede che la libreria LLDP sia inclusa nella distribuzione del sistema operativo (OS) del Thin Client.
- WLAN BBSID e {IPv4-IPv6; Subnet; MAC Address} dell'endpoint in cui è installata l'app Citrix Workspace.

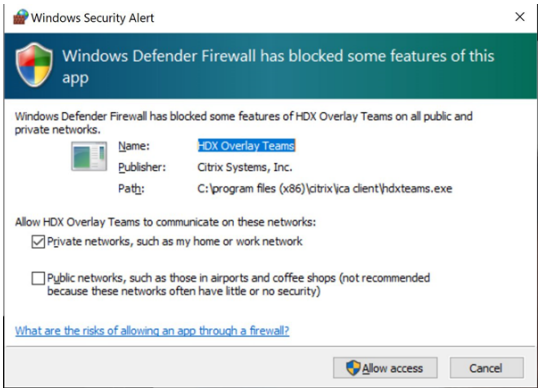
  - Le posizioni basate su subnet e WiFi sono supportate nell'app Workspace per Windows, Linux e Mac.

- Latitude e Longitude, se l'autorizzazione dell'utente è concessa a livello di sistema operativo in cui è installata l'app Citrix Workspace (l'autorizzazione è impostata su HDX RTC Engine)

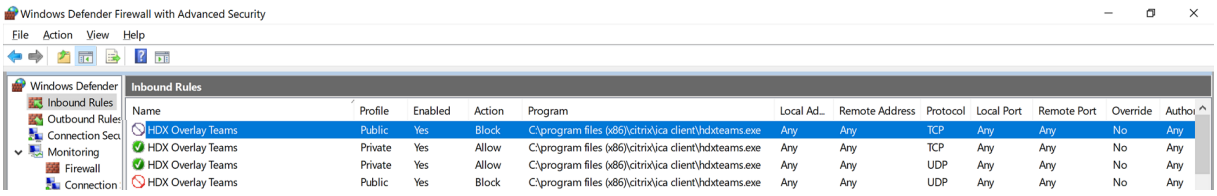
  - Funzionalità supportata su tutte le piattaforme app Workspace. Tuttavia, in Citrix Workspace for Linux, è necessario includere la libreria `libgps` nella distribuzione del sistema operativo del Thin Client (>sudo apt-get install libgps23 gpsd lldpd).

Considerazioni sul firewall

Quando gli utenti avviano una chiamata ottimizzata utilizzando il client Microsoft Teams per la prima volta, potrebbero notare un avviso nelle impostazioni del **firewall di Windows**. L'avviso richiede agli utenti di consentire la comunicazione per HdxTeams.exe o HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



Le quattro voci seguenti vengono aggiunte in **Regole in entrata** nella console **Windows Defender Firewall > Sicurezza avanzata**. Se si desidera, è possibile applicare regole più restrittive.

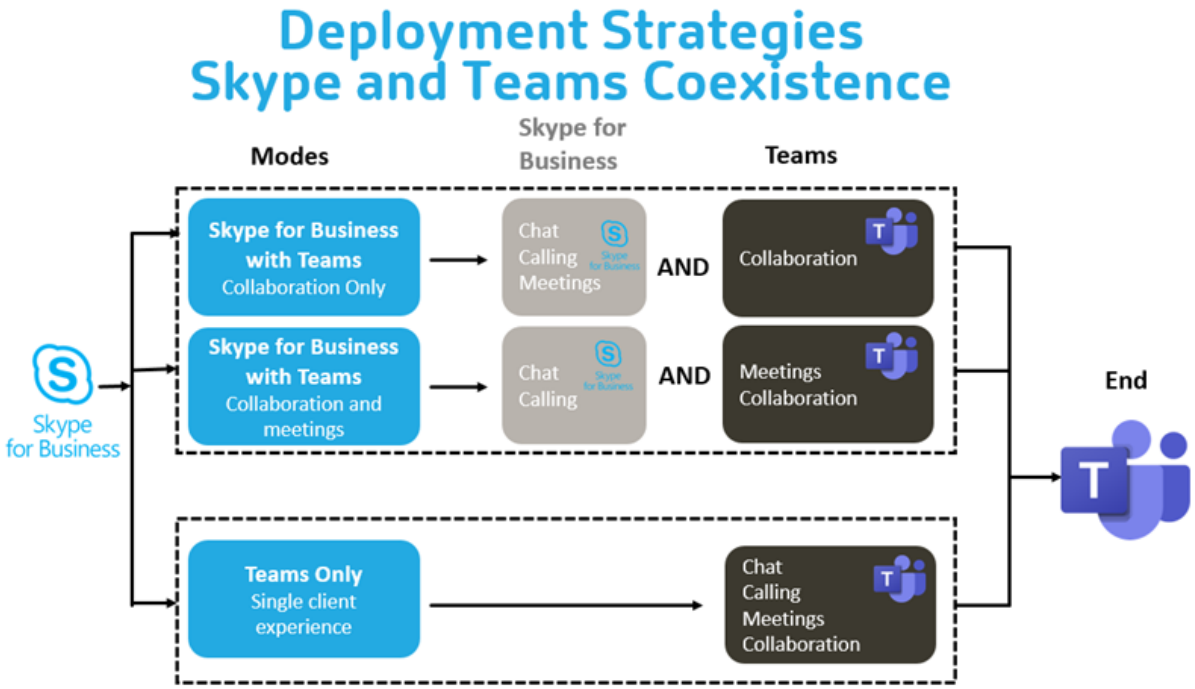


Coesistenza di Microsoft Teams e Skype for Business

È possibile distribuire Microsoft Teams e Skype for Business fianco a fianco, come due soluzioni separate con funzionalità sovrapposte.
Per ulteriori informazioni, vedere Comprendere la coesistenza e l'interoperabilità di Microsoft Teams e Skype for Business.

Citrix RealTime Optimization Pack e l'ottimizzazione HDX per i motori multimediali di Microsoft Teams rispettano quindi la configurazione impostata nell'ambiente. Gli esempi includono le modalità isola e Skype for Business con la collaborazione in Microsoft Teams. Inoltre, Skype for Business con la collaborazione e le riunioni di Microsoft Teams.

L'accesso alle periferiche può essere concesso solo a una singola applicazione alla volta. Ad esempio, l'accesso alla webcam da parte di RealTime Media Engine durante una chiamata blocca il dispositivo di imaging durante una chiamata. Quando il dispositivo viene rilasciato, diventa disponibile per Microsoft Teams.



Citrix SD-WAN: connettività di rete ottimizzata per Microsoft Teams

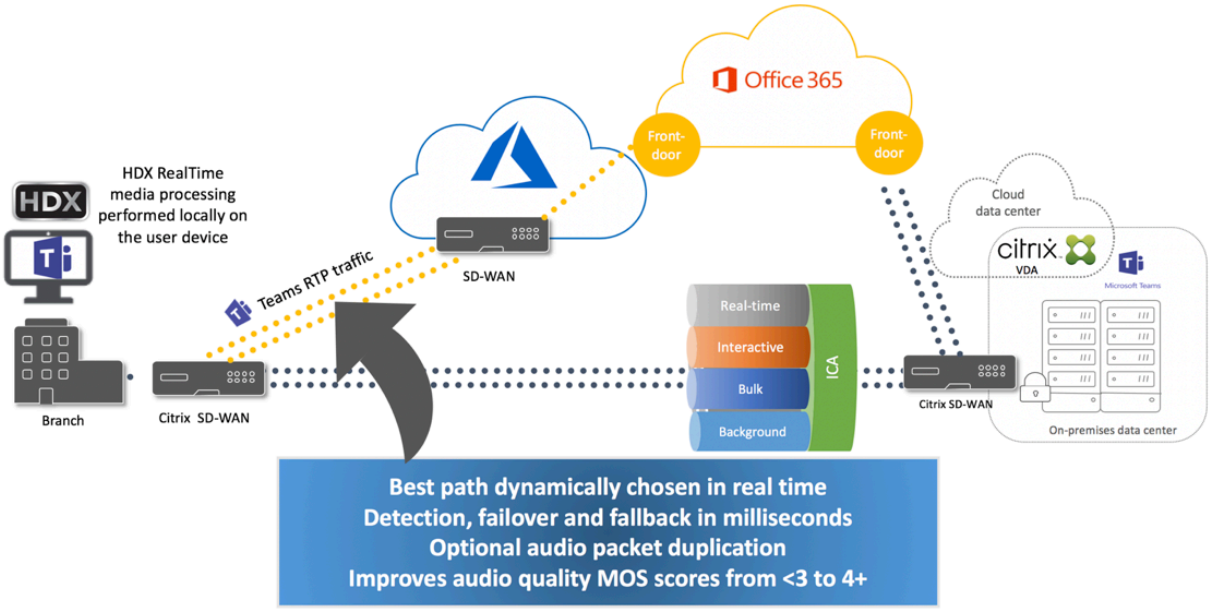
La qualità audio e video ottimale richiede una connessione di rete al cloud di Microsoft 365 con bassa latenza, basso jitter e bassa perdita di pacchetti. Il backhauling del traffico RTP audio-video di Microsoft Teams dagli utenti dell'app Citrix Workspace nelle sedi delle filiali a un centro dati prima del passaggio a Internet può aggiungere latenza eccessiva. Potrebbe anche causare congestione sui collegamenti WAN. Citrix SD-WAN ottimizza la connettività per Microsoft Teams seguendo i principi di connettività di rete di Microsoft 365. Citrix SD-WAN utilizza l'indirizzo IP e il servizio web di Microsoft 365 basati su Microsoft REST e il DNS di prossimità. Tutto questo serve a identificare, classificare e indirizzare il traffico di Microsoft Teams.

Le connessioni a Internet aziendali a banda larga in molte zone soffrono di perdite intermittenti di pacchetti, periodi di jitter eccessivo e interruzioni.

Citrix SD-WAN offre due soluzioni per preservare la qualità audio-video di Microsoft Teams quando lo stato della rete è variabile o degradato.

- Se si utilizza Microsoft Azure, un'appliance virtuale Citrix SD-WAN (VPX) distribuita nella rete virtuale di Azure fornisce ottimizzazioni di connettività avanzate. Queste ottimizzazioni includono il failover dei collegamenti senza soluzione di continuità e il racing dei pacchetti audio.
- I clienti Citrix SD-WAN possono connettersi a Microsoft 365 tramite il servizio Citrix Cloud Direct. Questo servizio offre una consegna affidabile e sicura per tutto il traffico collegato a Internet.

Se la qualità della connessione internet della filiale non è un problema, potrebbe essere sufficiente per ridurre al minimo la latenza. Indirizzare il traffico di Microsoft Teams direttamente dall'appliance della filiale Citrix SD-WAN alla porta principale di Microsoft 365 più vicina per ridurre al minimo la latenza. Per ulteriori informazioni, vedere Ottimizzazione di Citrix SD-WAN Office 365.



Riunioni e chat con più finestre

È possibile utilizzare più finestre di riunione o chat per Microsoft Teams in Windows. Per informazioni dettagliate sulla funzionalità pop-out, vedere You can use multiple meetings or chat windows for Microsoft Teams in Windows sul sito di Microsoft 365.

> **Nota:**
>
> Questa funzione è supportata con l'app Citrix Workspace per Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Richiede VDA 2112 o versioni successive ed è stato trasferito su 1912 CU6+ LTSR.

Sfocatura dello sfondo ed effetti di sfondo

L'app Citrix Workspace per Windows, Mac, Linux e ChromeOS/HTML5 supporta la sfocatura dello sfondo e gli effetti per gli effetti di sfondo presenti nell'ottimizzazione di Microsoft Teams con HDX.

È possibile sfocare lo sfondo o sostituirlo con un'immagine predefinita ed evitare distrazioni impreviste aiutando la conversazione a rimanere concentrata sulla silhouette (corpo e viso). È possibile utilizzare questa funzionalità con chiamate P2P o in conferenza.

> **Nota:**
>
> Questa funzionalità è integrata con i pulsanti dell'interfaccia utente di Microsoft Teams. Il supporto MultiWindow è un prerequisito che richiede un aggiornamento del VDA alla versione 2112 o a una versione successiva. Per ulteriori informazioni, vedere Riunioni e chat con più finestre.

I controlli dell'interfaccia utente di Microsoft Teams sulla sfocatura e gli effetti dello sfondo richiedono le seguenti versioni minime:

- App Citrix Workspace per Windows 2207
- App Citrix Workspace per Mac 2301
- App Citrix Workspace per Linux versione 2307
- App Citrix Workspace per ChromeOS 2303

Limitazioni:

- Il client deve essere connesso a Internet mentre si sostituisce l'immagine di sfondo con un'immagine predefinita di Microsoft Teams.
- La sostituzione dell'immagine di sfondo definita dall'amministratore e dall'utente non è supportata nell'interfaccia utente di Microsoft Teams. Le immagini di sfondo personalizzate possono essere configurate utilizzando le impostazioni del client, se anche l'immagine è memorizzata sul client.

Impostare un'immagine di sfondo personalizzata

Le seguenti chiavi di registro sono necessarie solo se non si prevede di utilizzare l'interfaccia utente di Microsoft Teams per controllare la funzionalità o se un amministratore desidera ignorare i comportamenti predefiniti. Ad esempio, è possibile disabilitare la sfocatura dello sfondo quando l'endpoint non è abbastanza potente.

In Windows Per impostare un'immagine di sfondo personalizzata, gli amministratori o gli utenti finali devono configurare la seguente chiave del Registro di sistema sul client o sull'endpoint:

Posizione:`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valore: 0 (disabilitato), 1 (abilitato), 2 (sostituzione immagine di sfondo)

Un valore impostato su 1 sfoca lo sfondo. L'utente finale o l'amministratore possono impostare questo valore.

Il valore impostato su 2 richiede anche la presenza della chiave **VideoBackgroundImage**. Solo l'amministratore può impostare questo valore. La chiave seguente è necessaria solo se si desidera sostituire l'immagine di sfondo e non per la sfocatura:

- Nome: VideoBackgroundImage
- Tipo: REG_SZ
- Valore: my_image_name.jpeg

L'immagine di sfondo video deve essere presente nella directory `C:\Program Files (x86)\Citrix\ICA Client`.

Questa configurazione del Registro di sistema può essere utilizzata anche per abilitare la sfocatura dello sfondo o la sostituzione dell'immagine nell'app Citrix Workspace 2206 senza il selettore dell'interfaccia utente di Microsoft Teams. In altre parole, se l'ambiente o il VDA non supporta più finestre, è comunque possibile applicare la soluzione alternativa del registro HKCU con l'app Citrix Workspace 2206 o superiore per ottenere un risultato simile, sebbene l'utente non possa controllare la funzionalità durante la sessione HDX o della chiamata di Microsoft Teams.

Le modifiche delle chiavi di registro hanno effetto solo quando la sessione HDX si connette.

Su Mac Posizione dell'immagine scaricata dall'utente: */Users/username/Downloads/any_image.png*

Eseguire i seguenti comandi per impostare l'immagine personalizzata come immagine predefinita:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2

defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

Su Linux Posizione dell'immagine scaricata dall'utente: */home/username/Downloads/any_image.jpg*

Creare il file */var/.config/citrix/hdx_rtc_engine/config.json* e aggiungere le seguenti chiavi di configurazione in formato JSON. Ad esempio,

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
```



```
7
8   }
```

Su HTML5

1. Accedere al file **configuration.js** nella cartella **HTML5Client**.
2. Aggiungere l'attributo **backgroundEffects** e impostare l'attributo su **true**. Ad esempio,

```
1  'features' : {
2
3      'msTeamsOptimization' :
4      {
5
6          'backgroundEffects' : true
7       }
8
9   }
```

3. Salvare le modifiche.

Considerazioni sul consumo di CPU client

Sebbene la funzionalità di sfocatura non sfrutti eccessivamente la CPU, ci si può aspettare un aumento dei consumi. Ad esempio, su un thin client con chip Intel® Pentium® Silver 4 Core da 1,5 GHz con TurboBoost fino a 2,8 GHz, la sfocatura dello sfondo aggiunge circa il 2% all'utilizzo della CPU. L'utilizzo medio della CPU è inferiore al 20%.

Visualizzazione Raccolta e altoparlanti attivi in Microsoft Teams

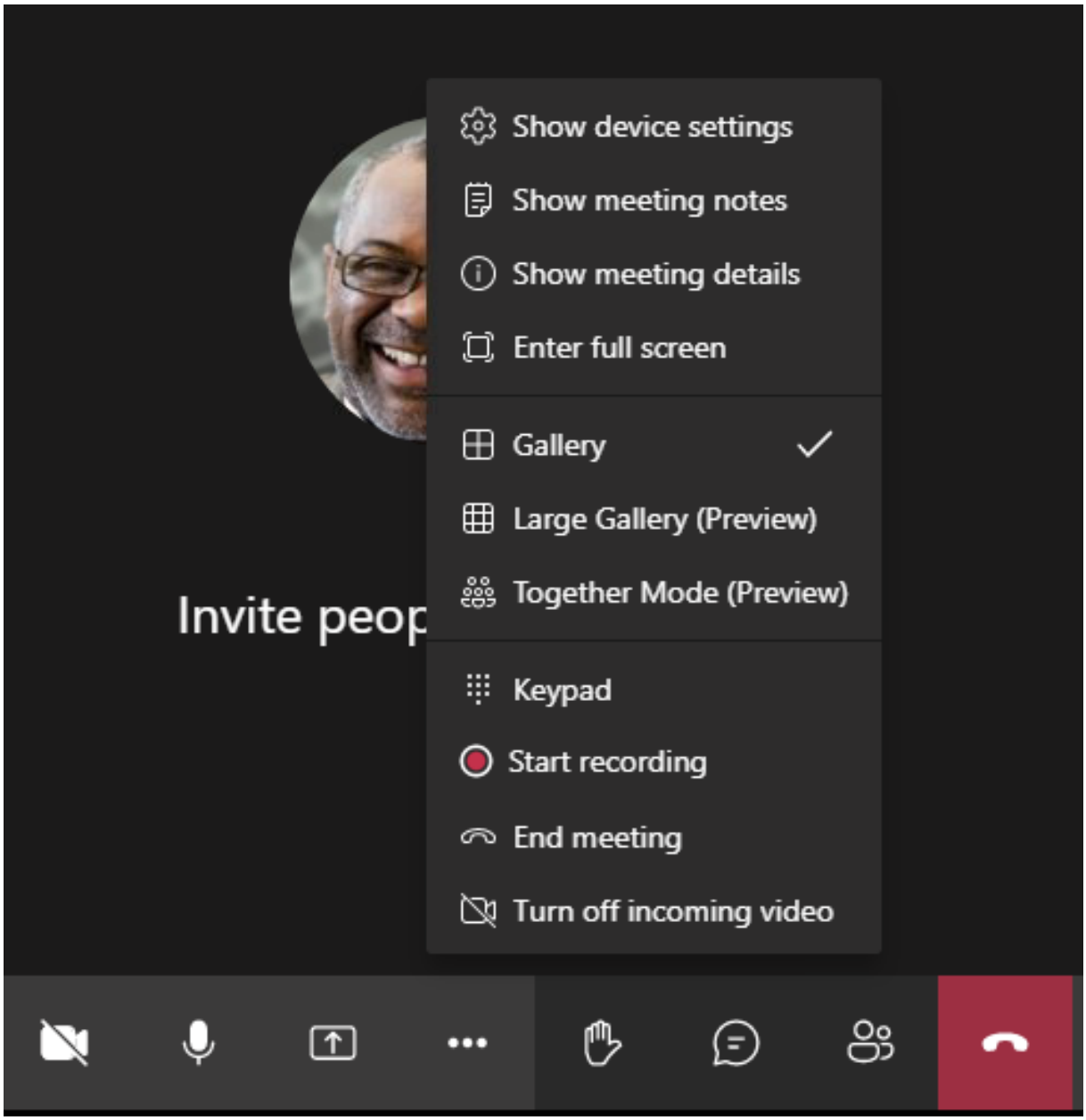
Microsoft Teams supporta i layout **Gallery** (Galleria), **Large gallery** (Galleria ampia) e la **modalità Together** (Insieme).

Microsoft Teams visualizza una griglia 2x2 con flussi video di quattro partecipanti (nota come **Gallery** [Galleria]). In questo caso, Microsoft Teams invia quattro flussi video al dispositivo client per la decodifica. Quando più di quattro partecipanti condividono un video, sullo schermo appaiono solo gli ultimi quattro partecipanti che hanno parlato di più.

Microsoft Teams fornisce inoltre un'ampia vista galleria con una griglia fino a 7x7. Di conseguenza, il Conference Server di Microsoft Teams combina un singolo feed video e lo invia al dispositivo client per la decodifica, con conseguente riduzione del consumo della CPU. Questo feed singolo in stile matrice potrebbe includere anche video con anteprima automatica degli utenti.

Infine, Microsoft Teams supporta la **modalità Together** (Insieme), che fa parte della nuova esperienza di riunione. Utilizzando la tecnologia di segmentazione IA per posizionare digitalmente i partecipanti in un background condiviso, Microsoft Teams mette tutti i partecipanti nello stesso auditorium.

L'utente può controllare queste modalità durante una chiamata in conferenza selezionando i layout **Gallery** (Galleria), **Large gallery** (Galleria ampia) o la **modalità Together** (Insieme) nel menu con i tre puntini.



Supporto delle limitazioni delle proporzioni video (app Citrix Workspace per Windows 2102, app Citrix Workspace per Linux 2106, app Citrix Workspace per MAC 2106 e versioni successive):

- L'opzione **Fill to frame** (Riempi inquadratura) è disponibile nelle viste Gallery (Galleria)/Large

Gallery (Galleria ampia). Questa opzione ritaglia le dimensioni del video per adattarlo alla sottofinestra. **Fit to frame** (Adatta all'inquadratura), invece, visualizza barre nere (formato 16:9) sui lati del video in modo che non ci siano ritagli.

La tabella seguente fornisce un confronto tra i layout Gallery (Galleria) e Large gallery (Galleria ampia):

	Vista Gallery (Galleria) 2x2 (impostazione predefinita)	Vista Large Gallery (Galleria ampia)
Layout/Griglia	Visualizza una griglia 2x2 con flussi video di quattro partecipanti. Sullo schermo vengono visualizzati solo gli ultimi quattro altoparlanti più attivi e gli altri partecipanti non appaiono sulla griglia.	Visualizza una griglia 7x7 con flussi video di 49 partecipanti.
Tecnica di mixing	Un router multimediale inoltra i singoli flussi di ciascun partecipante a ogni utente.	Un server centrale per conferenze mixa e transcodifica tutto l'audio o il video per creare un layout composito su misura per ogni partecipante. Questa azione introduce una certa latenza aggiuntiva.
Altoparlante attivo	Il nuovo altoparlante attivo sostituisce l'altoparlante meno attivo nella griglia.	Visualizza tutti i partecipanti indipendentemente dal fatto che siano attivi o inattivi.
Codifica in corrispondenza dell'endpoint	Sull'endpoint potrebbero essere codificati uno o più flussi video se Simulcast è abilitato. Per ulteriori informazioni sul supporto di Simulcast, vedere Simulcast.	Sull'endpoint potrebbero essere codificati uno o più flussi video se Simulcast è abilitato. Per ulteriori informazioni sul supporto di Simulcast, vedere Simulcast.
Decodifica in corrispondenza dell'endpoint	Ogni partecipante riceve fino a quattro flussi multimediali individuali. Ciò aumenta il consumo di CPU nell'endpoint di HdxRtcEngine.exe (per decodifica/rendering).	Ogni partecipante riceve un solo flusso per audio e video. Questa impostazione riduce il consumo di CPU nell'endpoint.

	Vista Gallery (Galleria) 2x2 (impostazione predefinita)	Vista Large Gallery (Galleria ampia)
Risoluzione massima	720p. Quando quattro partecipanti condividono video, la risoluzione massima è di 360p per feed video. Se meno di quattro partecipanti condividono video, la risoluzione per feed video potrebbe essere più alta.	720p per il layout composito o il mixaggio. Non è necessario un flusso video di alta qualità per partecipante in un layout composito. A causa di questa condizione, ogni mittente riduce la risoluzione o la velocità in bit di caricamento.
Problema di "utente lento"	Il mittente modifica la qualità di ciascuna modalità (audio/video/condivisione dello schermo) sulla qualità di rete più bassa comune tra i partecipanti. Questo flusso multimediale viene quindi inoltrato a tutti gli altri partecipanti. Di conseguenza, un partecipante con cattive condizioni di rete influisce sulla qualità di tutti gli altri partecipanti alla chiamata.	Meno suscettibile allo scenario di qualità della rete più bassa comune. Il server per conferenze offre qualità diverse in base alle condizioni di rete dei singoli partecipanti.
Anteprima automatica	L'utente viene visualizzato in una piccola miniatura in tempo reale.	L'utente viene visualizzato in una miniatura e mescolato con il resto dei feed video. Di conseguenza, l'utente potrebbe vedersi incluso nel layout del video principale con un ritardo aggiuntivo.

Condivisione dello schermo in Microsoft Teams

Microsoft Teams si basa sulla condivisione dello schermo basata su video (VBSS), codificando essenzialmente il desktop condiviso con codec video come H264 e creando un flusso ad alta definizione. Con l'ottimizzazione HDX, la condivisione dello schermo in entrata viene considerata come un flusso video.

A partire dall'app Citrix Workspace 2109 o versione successiva per Windows, Linux, Mac e dall'app

Citrix Workspace 2303 per ChromeOS, gli utenti possono condividere gli schermi e la videocamera contemporaneamente.

Con le versioni precedenti, se ci si trova nel mezzo di una videochiamata e l'altro peer inizia a condividere il desktop, il feed video della videocamera originale viene sospeso. Viene invece visualizzato il feed video per la condivisione dello schermo. Il peer deve quindi riprendere manualmente la condivisione della videocamera.

> **Nota per PowerPoint Live**
>
> Questa limitazione non esiste se si condividono contenuti da PowerPoint Live. In tal caso, gli altri colleghi possono ancora vedere la webcam e i contenuti e navigare avanti e indietro per esaminare altre diapositive. In questo scenario, le diapositive vengono renderizzate sul VDA. Per accedere a una presentazione PowerPoint Live, fare clic sul pulsante del pannello di condivisione e selezionare una delle diapositive di PowerPoint suggerite, oppure fare clic su "Sfoglia"e trovare un file PowerPoint sul proprio computer o in OneDrive.

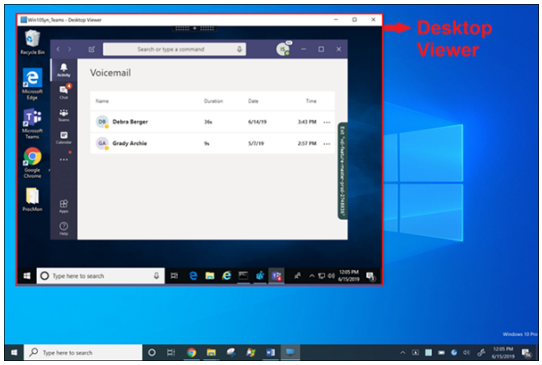
Anche la condivisione dello schermo in uscita è ottimizzata e assegnata all'app Citrix Workspace. In questo caso, il motore multimediale acquisisce e trasmette solo la finestra Citrix Desktop Viewer (CDViewer.exe), con un bordo rosso disegnato all'intorno. Qualsiasi applicazione locale che si sovrappone a Desktop Viewer non viene acquisita.

> **Nota**
>
> Impostare autorizzazioni specifiche nell'app Citrix Workspace per Mac per abilitare la condivisione dello schermo. Per ulteriori informazioni, vedere Requisiti di sistema.

Limitazione nota:

- Se Desktop Viewer è disabilitato o se viene utilizzato Desktop Lock, la selezione multimonitor non è disponibile nel selettore dello schermo di Microsoft Teams. Desktop Viewer potrebbe essere disabilitato modificando il modello di file `.ICA` o `StoreFront web.config`. Il tasto di scelta rapida MAIUSC+F2 non è compatibile con la condivisione dello schermo multimonitor.
- Nelle versioni dell'app Workspace precedenti alla 2106, viene condiviso solo il monitor principale. Trascinare l'applicazione nel desktop virtuale sul monitor principale in modo che gli altri peer nella chiamata la vedano.
- La condivisione dello schermo multimonitor potrebbe non funzionare se si configura l'app Citrix Workspace con la funzionalità di layout del monitor virtuale (partizione logica di un singolo monitor fisico). In questo caso, tutti i monitor virtuali vengono condivisi come immagine composita.
- Le versioni precedenti dell'app Citrix Workspace per Windows (dalla 1907 alla 2008) condividono anche un'applicazione locale che viene eseguita nel computer client. Questa condivisione è possibile solo se l'app locale è stata sovrapposta a Desktop Viewer. Questo comportamento è stato rimosso nella versione 2009.6 o superiore e nella versione 1912 CU5 o superiore.

- Durante la condivisione dello schermo, se si passa dalla modalità finestra alla modalità a schermo intero, la condivisione dello schermo si interrompe. È necessario interrompere e condividere di nuovo affinché la condivisione dello schermo funzioni.
- Non è possibile aggiungere i controlli di condivisione a una posizione specifica in Microsoft Teams ottimizzato.
- Quando si condivide un'app ridotta a icona, è possibile che venga condivisa anche la barra del titolo dell'app.



Condivisione dello schermo da un'applicazione senza soluzione di continuità:

Se si pubblica Microsoft Teams come applicazione autonoma senza soluzione di continuità, la condivisione dello schermo acquisisce il desktop locale dell'endpoint fisico. La versione minima dell'app Citrix Workspace deve essere 1909.

Condivisione di app

A partire dall'app Citrix Workspace per Windows 2112.1 e dal VDA 2112, Microsoft Teams supporta la condivisione delle app.

A partire dall'app Citrix Workspace per Windows 2109, Mac 2203, Linux 2209 e VDA 2109, Microsoft Teams supporta la condivisione sullo schermo di app specifiche in esecuzione nella sessione virtuale. È anche possibile condividere applicazioni interne personalizzate, come Java, utilizzando Microsoft Teams ottimizzato. Per condividere un'app specifica:

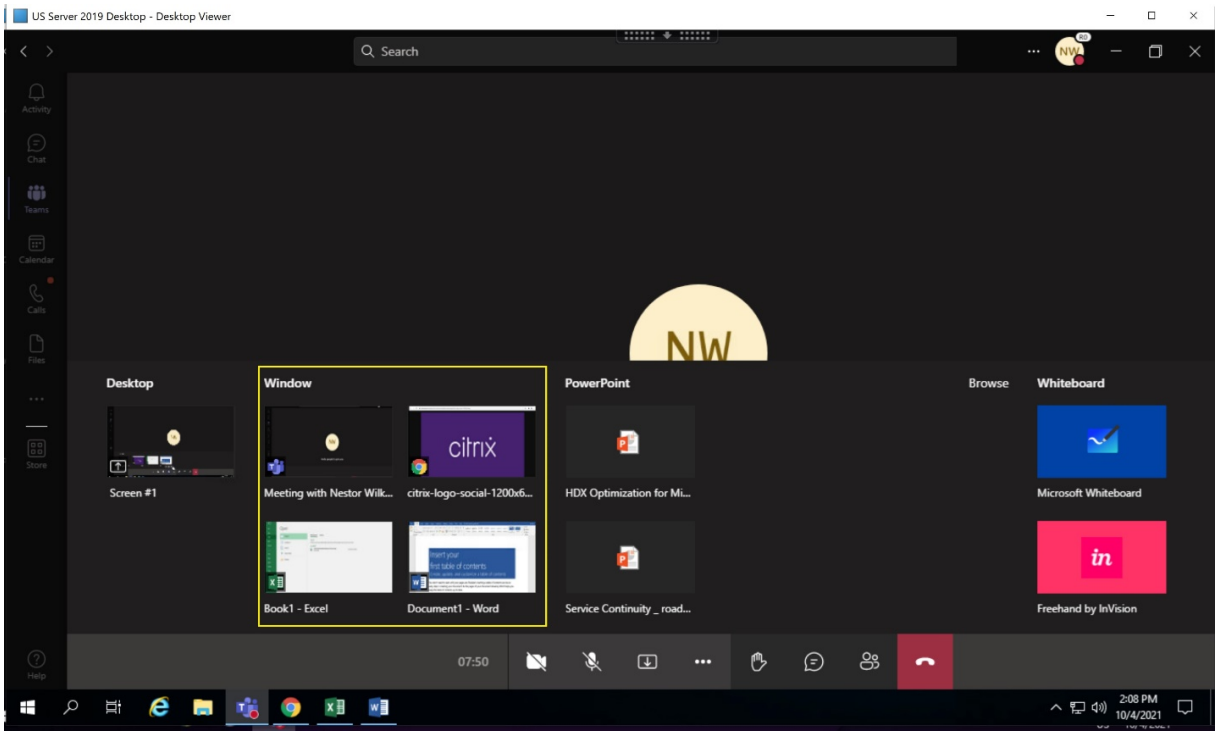
1. Accedere all'app Microsoft Teams nella sessione remota.
2. Fare clic su **Condividi contenuto** nell'interfaccia utente di Microsoft Teams.
3. Selezionare un'app da condividere durante la riunione. Viene visualizzato un bordo rosso intorno all'app che si è selezionata e i partecipanti alla chiamata possono vedere l'app condivisa.

Per condividere un'altra app, fare nuovamente clic su **Condividi contenuto** e selezionare una nuova app.

Se si desidera disabilitare la condivisione delle app, creare la seguente chiave di registro sul VDA all'indirizzo `HKLM\SOFTWARE\Citrix\Graphics`:

Nome: `UseWsProvider`
Tipo: `DWORD`
Valore: 0

> **Nota:**
>
> - Se si riduce a icona un'app, Microsoft Teams visualizza l'ultima immagine dell'app condivisa. È possibile ingrandire la finestra per riprendere la condivisione dello schermo.
> - La condivisione dello schermo fa affidamento sull'acquisizione della finestra lato VDA. Il contenuto viene quindi inoltrato alla velocità massima all'app Citrix Workspace. La velocità massima è di 30 frame al secondo. L'app Citrix Workspace inoltra il contenuto al collega o al server della conferenza.



Limitazioni note della condivisione dello schermo di app specifiche:

- Il puntatore del mouse non è visibile quando si condivide un'app sullo schermo.
- Se si riduce a icona un'app quando la si condivide, nel selettore dello schermo viene visualizzata solo l'icona dell'app. La miniatura dell'app non viene visualizzata in anteprima nel selettore dello schermo. Non è possibile condividere il contenuto e non viene visualizzato il bordo rosso finché non si ingrandisce l'app.
- Nelle app LAA è visualizzato un elenco delle app che possono essere condivise con le app desktop nel Microsoft Teams ottimizzato nel VDA. Tuttavia, quando si seleziona l'app dall'elenco, il risultato potrebbe non essere quello previsto.

Compatibilità con la protezione delle app

La condivisione sullo schermo di un'app specifica è compatibile con la funzione di protezione delle app in Microsoft Teams ottimizzato per HDX. È possibile condividere lo schermo di un'app specifica, se l'app o il desktop è stato avviato da un gruppo di consegna per il quale è abilitata la protezione delle app.

Quando si fa clic su **Condividi contenuto** nell'interfaccia utente di Microsoft Teams, il selettore dello schermo rimuove l'opzione **Desktop**. È possibile selezionare l'opzione **Finestra** solo per condividere qualsiasi app aperta.

> **Nota:**
>
> Quando si avviano app o desktop da un gruppo di consegna con protezione app abilitata, non è possibile vedere il video in arrivo o la condivisione dello schermo se si utilizza l'app Citrix Workspace per Windows 2202 o versioni precedenti.

Dare e richiedere il controllo in Microsoft Teams Questa funzione è supportata nelle seguenti versioni dell'app Citrix Workspace (non vi è alcuna dipendenza dalla versione del VDA o dal sistema operativo, a sessione singola o multisessione):

- App Citrix Workspace per Windows versione 2112.1 o successiva
- App Citrix Workspace per Mac versione 2203.1 o successiva
- App Citrix Workspace per Linux versione 2203 o successiva
- App Citrix Workspace per ChromeOS versione 2303 o successiva

È possibile richiedere il controllo durante una chiamata di Microsoft Teams quando un partecipante condivide lo schermo. Una volta ottenuto il controllo, è possibile effettuare selezioni, modifiche o altre attività con tastiera e mouse sullo schermo condiviso.

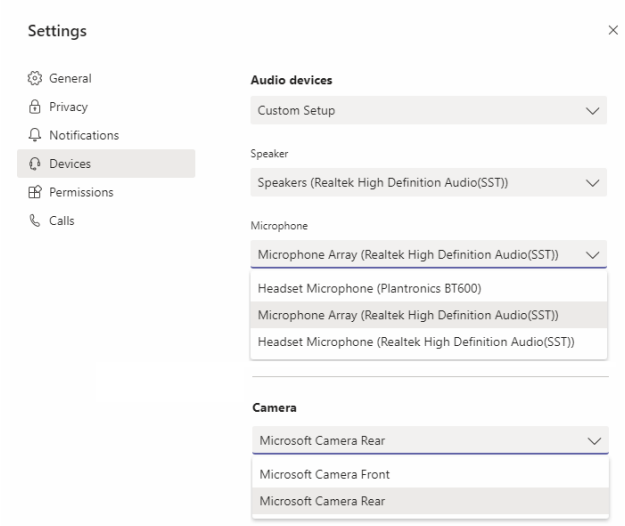
Per assumere il controllo quando uno schermo viene condiviso, fare clic sul pulsante **Richiedi controllo** nell'interfaccia utente di Microsoft Teams. Il partecipante alla riunione che condivide lo schermo può accettare o rifiutare la richiesta.

Mentre si dispone del controllo, è possibile effettuare selezioni, modifiche e altre alterazioni nello schermo condiviso. Per queste azioni, è possibile usare sia la tastiera che il mouse. Al termine fare clic su **Richiedi controllo**.

> **Limitazioni:**
>
> - I comandi Concedi controllo e Richiedi controllo non sono disponibili se l'utente sta condividendo una singola app (nota anche come condivisione app). È necessario condividere il desktop o il monitor completo.
> - La funzione per fissare la barra di controllo in una posizione specifica non è disponibile.

Periferiche in Microsoft Teams

Quando l'ottimizzazione per Microsoft Teams è attiva, l'app Citrix Workspace accede alle periferiche (cuffie, microfono, videocamere, altoparlanti e così via). Quindi le periferiche vengono elencate correttamente nell'interfaccia utente di Microsoft Teams (**Impostazioni > Dispositivi**).



Microsoft Teams non accede direttamente ai dispositivi. Si basa invece sul motore multimediale WebRTC dell'app Workspace per l'acquisizione e l'elaborazione dei contenuti multimediali. Microsoft Teams elenca i dispositivi che l'utente può selezionare.

Le periferiche inserite mentre Microsoft Teams è attivo non sono selezionate per impostazione predefinita. È necessario selezionare manualmente le periferiche dalla schermata **Impostazioni** > **Dispositivi** dell'interfaccia utente di Microsoft Teams. Dopo che le periferiche sono state selezionate, Microsoft Teams ne memorizza le informazioni nella cache. Di conseguenza, le periferiche vengono selezionate automaticamente quando ci si riconnette a una sessione dallo stesso endpoint.

Raccomandazioni:

- Cuffie certificate Microsoft Teams con cancellazione dell'eco integrata. Nelle configurazioni con periferiche aggiuntive, in cui il microfono e gli altoparlanti si trovano su dispositivi separati, potrebbe essere presente un'eco. Un esempio è una webcam con un microfono incorporato e un monitor con altoparlanti. Quando si utilizzano altoparlanti esterni, posizionarli il più lontano possibile dal microfono. Inoltre, posizionarli lontano da qualsiasi superficie che potrebbe rifrangere il suono nel microfono. Per ulteriori informazioni, passare a `www.microsoft.com` e cercare le cuffie certificate Microsoft Teams.
- Fotocamere certificate Microsoft Teams, sebbene le periferiche certificate Skype for Business siano compatibili con Microsoft Teams. Per ulteriori informazioni, andare al sito Web e cercare le fotocamere certificate Microsoft Teams e le periferiche certificate Skype for Business.
- Il motore multimediale dell'app Citrix Workspace non può sfruttare l'offload della CPU con we-

bcam che eseguono la codifica H.264 on-board UVC 1.1 e 1.5.

> **Nota:**
>
> L'app Workspace 2009.6 per Windows è ora in grado di acquisire periferiche con formati audio a 24 bit o con frequenze superiori a 96 kHz.
>
> HdxTeams.exe (nell'app Citrix Workspace per Windows 2009 o versioni precedenti) supporta solo questi formati specifici dei dispositivi audio (canali, profondità di bit e frequenza di campionamento):
>
> - Dispositivi di riproduzione: fino a 2 canali, 16 bit, frequenze fino a 96.000 Hz
> - Dispositivi di registrazione: fino a 4 canali, 16 bit, frequenze fino a 96.000 Hz
>
> Anche se un solo altoparlante o microfono non corrisponde alle impostazioni previste, l'enumerazione dei dispositivi in Microsoft Teams non va a buon fine e viene visualizzato **Nessuno** in **Impostazioni > Dispositivi**.
> I log
> **Webrpc** in **HdxTeams.exe** mostrano questo tipo di informazioni:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```
>
> Come soluzione alternativa, disabilitare il dispositivo specifico oppure:
>
> 1. Aprire **Audio nel Pannello di controllo** (mmsys.cpl).
> 2. Selezionare il dispositivo di riproduzione o registrazione.
> 3. Andare a **Proprietà > Avanzate** e modificare le impostazioni su una modalità supportata.

Modalità di fallback

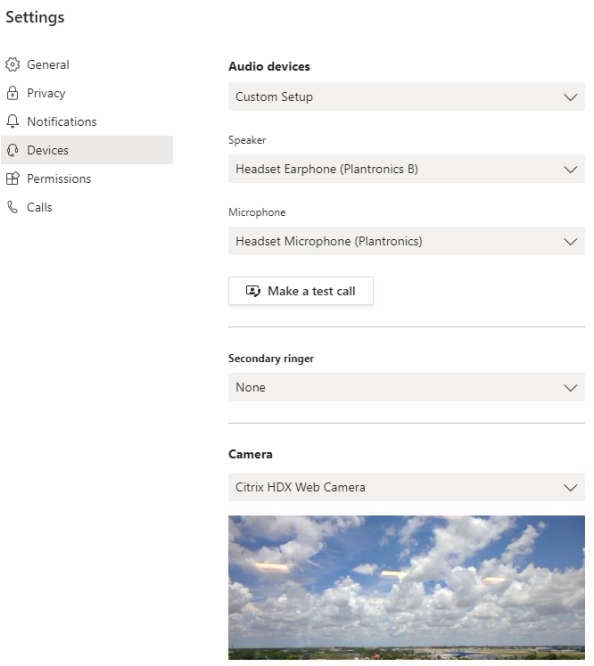
Se Microsoft Teams non riesce a caricarsi in modalità VDI ottimizzata ("Citrix HDX Not Connected" [Citrix HDX non connesso] in Microsoft Teams/Informazioni/Versione), il VDA torna a utilizzare le tecnologie HDX legacy. Le tecnologie HDX legacy potrebbero essere il reindirizzamento della webcam e il reindirizzamento del microfono e dell'audio del client. Se si utilizza una versione dell'app Workspace/un sistema operativo della piattaforma che non supporta l'ottimizzazione di Microsoft Teams, le chiavi del Registro di sistema di fallback non si applicano.
In modalità di fallback, le periferiche sono mappate al VDA. Le periferiche vengono visualizzate nell'app Microsoft Teams come se fossero collegate localmente al desktop virtuale.

Ora è possibile controllare granularmente il meccanismo di fallback impostando le chiavi del Registro di sistema nel VDA. Per ulteriori informazioni, vedere Modalità di fallback di Microsoft Teams nell'

elenco delle funzionalità gestite tramite il Registro di sistema.

Questa funzionalità richiede Microsoft Teams versione 1.3.0.13565 o successiva.

Per determinare se si è in modalità ottimizzata o non ottimizzata quando si esamina la scheda **Impostazioni > Dispositivi** nell'app Microsoft Teams, la differenza più significativa è il nome della videocamera. Se Microsoft Teams è stato caricato in modalità non ottimizzata, vengono avviate le tecnologie HDX legacy. Il nome della webcam presenta il suffisso **Citrix HDX**, come mostrato nell'immagine seguente. I nomi dell'altoparlante e del microfono potrebbero essere leggermente diversi (o troncati) rispetto alla modalità ottimizzata.



Quando vengono utilizzate tecnologie HDX legacy, Microsoft Teams non esegue l'offload dell'elaborazione di audio, video e condivisione dello schermo nel motore multimediale WebRTC dell'app Citrix Workspace dell'endpoint. Le tecnologie HDX utilizzano invece il rendering lato server. È previsto un elevato consumo di CPU sul VDA quando viene attivato il video. Le prestazioni audio in tempo reale potrebbero non essere ottimali.

Limitazioni note

Limitazioni Citrix

Limitazioni sull'app Citrix Workspace:

- Pulsanti HID: risposta e fine chiamata non sono supportate. I tasti per abbassare e alzare il volume sono supportati.

- Le impostazioni QoS nell'interfaccia di amministrazione per Microsoft Teams non sono valide per gli utenti VDI.
- Gli utenti non possono acquisire schermate dei contenuti di Microsoft Teams quando utilizzano uno strumento di cattura su VDA. Tuttavia, se viene utilizzato uno strumento di cattura sul lato client, il contenuto può essere acquisito.

Limitazione sul VDA:

- Quando si configura l'**impostazione High DPI (DPI elevato) dell'app Citrix Workspace** su `Yes`, la finestra video reindirizzata non è nella posizione corretta. Questa limitazione si verifica quando il fattore di ridimensionamento DPI del monitor è impostato su un valore superiore al 100%

Limitazioni sull'app Citrix Workspace e sul VDA:

- È possibile controllare il volume di una chiamata ottimizzata solo utilizzando la barra del volume sul computer client, non sul VDA.

Simulcast

Il supporto di Simulcast è abilitato per videoconferenze Microsoft Teams ottimizzate su Windows e Mac. Per Linux, rivolgersi al proprio fornitore di thin client.
Con Simulcast, la qualità e l'esperienza delle videoconferenze su diversi endpoint vengono migliorate adattandosi alla risoluzione corretta per la migliore esperienza di chiamata per tutti i chiamanti.

Con questa esperienza migliorata, ogni utente potrebbe fornire più flussi video con risoluzioni diverse (ad esempio 720p, 360p e così via) a seconda di diversi fattori, tra cui la capacità dell'endpoint, le condizioni della rete e così via. L'endpoint ricevente richiede quindi la massima risoluzione di qualità che può gestire, offrendo così a tutti gli utenti un'esperienza video ottimale.

> **Nota:**
>
> Questa funzionalità è disponibile solo dopo l'implementazione di un aggiornamento di Microsoft Teams. Per informazioni sulla data di pubblicazione, passare a https://www.microsoft.com/ e cercare la roadmap di Microsoft 365. Quando l'aggiornamento verrà implementato da Microsoft, sarà possibile leggere l'articolo CTX253754 per il relativo annuncio e l'aggiornamento della documentazione.

Limitazioni Microsoft

- La vista galleria 3x3 non è supportata. Dipendenza di Microsoft Teams: contattare Microsoft per sapere quando sarà disponibile la griglia 3x3.

- L'interoperabilità con Skype for Business è limitata alle chiamate audio, nessuna modalità video.
- La risoluzione massima del flusso video in entrata e in uscita è 720p.
- Il tono di suoneria delle chiamate PSTN non è supportato.
- Il bypass dei contenuti multimediali per il routing diretto non è supportato.
- I ruoli di produttore e presentatore di eventi broadcast e live non sono supportati. Il ruolo di partecipante è supportato ma non ottimizzato (viene invece eseguito il rendering sul VDA).
- La funzione zoom avanti e zoom indietro in Microsoft Teams non è supportata.
- Il routing basato sulla posizione e il bypass dei supporti non sono supportati.
- L'unione delle chiamate non è supportata (opzione non visualizzata nell'interfaccia utente).

Limitazioni Citrix e Microsoft

- Quando si esegue la condivisione dello schermo, l'opzione **Includi audio di sistema** non è disponibile.
- Simulcast non è supportato su ChromeOS.

Imminente la fine del ciclo di vita di Microsoft Teams a finestra singola

Il 31 gennaio 2024, Microsoft ritirerà il supporto di Microsoft Teams per l'interfaccia utente a finestra singola quando si utilizza l'ottimizzazione VDI Microsoft Teams e supporterà solo l'esperienza multi-finestra. Microsoft ha comunicato tale deprecazione l'8 settembre 2023 nell'M365s Admin Center (ID post: MC674419).
I dettagli pubblici sulla funzionalità multifinestra sono disponibili nell'articolo della Tech Community New Meeting and Calling Experience in Microsoft Teams (Nuova esperienza di riunioni e chiamate in Microsoft Teams).

> **Nota:**
>
> Citrix consiglia di aggiornare l'app VDA e Citrix Workspace alle versioni supportate per continuare a utilizzare Microsoft Teams in modalità ottimizzata per la condivisione di video e schermo. Se non si aggiornano l'infrastruttura e gli endpoint per supportare più finestre, le chiamate, le videochiamate e la condivisione dello schermo non saranno ottimizzate. Ciò può comportare problemi di qualità delle chiamate, maggiore latenza e aumento del carico sul server.

La tabella seguente illustra le versioni minime, LTSR e consigliate dei VDA e dell'app Citrix Workspace necessarie per continuare a utilizzare le chiamate ottimizzate in Microsoft Teams su Citrix VDI:

Componente	Versione minima (1)	Versione supportata dalla LTSR (2)	Versione consigliata (3)
Microsoft Teams	1.5.00.11865	Non applicabile	Più recente
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
App Citrix Workspace per Windows	2112.1 CR	2203 CU2+ (4)	2309 CR+
App Citrix Workspace per Mac	2203 CR	Non applicabile	2308 CR+
App Citrix Workspace per Linux	2202 CR	Non applicabile	2308 CR+
App Citrix Workspace per ChromeOS o HTML5	2303 CR	Non applicabile	2309 CR+

Note:

1. Versione minima: questa è la versione in cui è stata introdotta per la prima volta la funzionalità multi-finestra. Alcune versioni minime elencate qui potrebbero aver raggiunto la fine del ciclo di vita.
2. Versione supportata LTSR: questa è la versione LTSR supportata da Citrix per la funzionalità multi-finestra. Le versioni precedenti di queste versioni LTSR potrebbero funzionare, ma il supporto non è più disponibile per tali versioni una volta rilasciata una nuova versione LTSR CU. Per ulteriori informazioni sui criteri di supporto LTSR, vedere https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr.
3. Versione consigliata: questa è la versione del software consigliata da Citrix se l'utente/-cliente sceglie di aggiornare il proprio software. Sono tutte versioni CR.
4. La versione 2203 LTSR per le versioni base di VDA e CWA include la funzionalità multi-finestra. Queste versioni sono state sostituite dall'ultima CU, che è la versione ufficialmente supportata. I clienti possono continuare a utilizzare queste versioni non supportate a loro discrezione. Citrix incoraggia i clienti che utilizzano la versione LTSR a passare alla CU più recente.

Annuncio di obsolescenza del formato SDP (Piano B) di WebRTC

Citrix prevede di eliminare l'attuale supporto del formato SDP (Piano B) di WebRTC nelle versioni future. È necessario utilizzare Unified Plan in WebRTC per supportare le funzionalità ottimizzate di Microsoft Teams.

Prodotti interessati

In una delle versioni future dell'applicazione Citrix Workspace, le chiamate tra endpoint con la prossima versione dell'app Citrix Workspace e gli endpoint con l'app Citrix Workspace 2108 o versioni precedenti non saranno supportate. Questa incompatibilità di chiamata include i client dell'app Citrix Workspace (CWA) 1912 LTSR. Sono interessati i seguenti client CWA:

- App Citrix Workspace per Windows
- App Citrix Workspace per Linux
- App Citrix Workspace per Mac
- App Citrix Workspace per Chrome

Sostituto per Plan B

Se si utilizza una versione dell'app Citrix Workspace precedente alla 2109, è necessario eseguire l'aggiornamento a una versione supportata (preferibilmente l'ultima versione CR). In caso contrario, le chiamate con una versione futura o con endpoint più recenti non riusciranno a connettersi. Potrebbe inoltre non essere possibile completare le chiamate tra le versioni future e i partner di comunicazione federati se il partner federato non ha aggiornato il proprio Citrix Workspace.

La versione 2108 dell'app Citrix Workspace ha completato la data di supporto in marzo 2023 e deve essere aggiornata a una versione più recente. Per ulteriori informazioni, vedere App Workspace che illustra i dettagli sul supporto della versione dell'app Citrix Workspace.

Per ulteriori informazioni sulla deprecazione del Piano B, consulta la documentazione di WebRTC.

Informazioni aggiuntive

- Monitorare, risolvere i problemi e supportare Microsoft Teams
- Distribuire l'app desktop Microsoft Teams nella macchina virtuale
- Installare Microsoft Teams utilizzando MSI (sezione Installazione VDI)
- Thin client
- Strumento di valutazione della rete di Skype for Business
- Comprendere la coesistenza e l'interoperabilità di Microsoft Teams e Skype for Business