



Citrix Virtual Apps e Desktop 7 2402 LTSR

Contents

Citrix Virtual Apps and Desktops 7 2402 Rilascio del servizio a lungo termine (LTSR)	3
Cosa c'è di nuovo	4
Cumulative Update 1 (CU1)	4
Problemi risolti	9
2402 LTSR (versione iniziale)	13
Problemi risolti	23
Problemi noti	29
Deprecazione	34
Requisiti di sistema	51
Installazione e configurazione	63
Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager	65
Installare utilizzando la riga di comando	67
Installa Web Studio	84
Installare i VDA	91
Installare VDA utilizzando SCCM	109
Connessione ad AWS	127
Connessione a Microsoft Azure	141
Gestione delle immagini (anteprima)	161
Creare cataloghi di macchine	181
Crea un catalogo AWS	212
Creare un catalogo di Microsoft Azure	223
Gestire i cataloghi delle macchine	295
Gestire i gruppi di consegna	319

Accesso remoto al PC	353
Aggiornare e migrare	371
Aggiornare una distribuzione	375
Secure HDX (anteprima)	400
Dispositivi compositi e divisione dei dispositivi	403
Configurazione del reindirizzamento USB legacy	409
Ottimizzazione di Microsoft Teams (nuovo)	415
Ottimizzazione di Citrix HDX	417
Ottimizzazione Microsoft SlimCore	424
Ottimizzazione di Microsoft Teams (Classic)	429
Timeout dinamici delle sessioni	473
Impostazioni	476
Distribuzione sicura di Director	480
Matrice di compatibilità delle funzionalità	483
Cause di errori e risoluzione dei problemi di Citrix Director	488
SDK e API	513

Citrix Virtual Apps and Desktops 7 2402 Rilascio del servizio a lungo termine (LTSR)

January 24, 2025

Importante:

La strategia del ciclo di vita del prodotto per le versioni correnti (CR) e le versioni di servizi a lungo termine (LTSR) è descritta in [Milestone del ciclo di vita](#).

Citrix Virtual Apps and Desktops fornisce una soluzione di virtualizzazione per la distribuzione di applicazioni e desktop su qualsiasi dispositivo, su qualsiasi rete, migliorando al contempo la sicurezza dei dati, riducendo i costi e potenziando la produttività.

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

Cumulative Update 4 (CU4) è l'aggiornamento più recente del LTSR 2203. Gli LTSR sono disponibili anche per Citrix Virtual Apps and Desktops 1912.

- Per informazioni sui casi d'uso, vedere <https://www.citrix.com/products/citrix-virtual-apps-and-desktops/>.
- Per ulteriori informazioni sui componenti e sulle tecnologie nelle distribuzioni di Citrix Virtual Apps and Desktops, vedere [Panoramica tecnica](#).

Versioni precedenti

La documentazione per le altre versioni attualmente disponibili si trova in [Citrix Virtual Apps and Desktops](#).

Anche per le versioni precedenti, la documentazione è archiviata in [Documentazione legacy](#).

App e desktop virtuali Citrix in Citrix Cloud

L'offerta Citrix Cloud Virtual Apps and Desktops è Citrix DaaS. Per ulteriori informazioni, vedere [Citrix DaaS](#).

Link utili

- [Pacchetto di supporto Citrix](#)
- [Domande frequenti su LTSR](#)

- [Opzioni di manutenzione di Citrix Virtual Apps and Desktops](#)
- [Date del ciclo di vita del prodotto](#)
- [Programma LTSR per l'app Citrix Workspace](#)

Cosa c'è di nuovo

January 24, 2025

Informazioni su questa versione

L'aggiornamento cumulativo 1 (CU1) è l'aggiornamento più recente del LTSR 2402.

Informazioni su [Aggiornamento cumulativo 1 \(CU1\)](#)

Informazioni su [2402 LTSR \(versione iniziale\)](#)

Cumulative Update 1 (CU1)

September 11, 2024

Data di rilascio: 20 agosto 2024

Novità

Supporto dell'autenticazione con smart card

Web Studio ora supporta l'autenticazione tramite smart card, consentendo agli amministratori di accedere a Web Studio utilizzando schede PIV e CAC. Per ulteriori informazioni, vedere [Configurare l'autenticazione con smart card per Web Studio](#).

Miglioramento dei report di telemetria sull'utilizzo

Con il miglioramento della funzionalità di telemetria dell'utilizzo delle licenze, vengono raccolti ed elaborati i dati sull'utilizzo delle licenze per i prodotti, i componenti e le funzionalità Citrix distribuiti negli ambienti gestiti da Citrix. Questa implementazione serve a confermare la conformità delle licenze e i dati vengono gestiti tramite il Citrix License Server. È necessario eseguire l'aggiornamento

alla versione più recente del server di licenza e disporre di un account Citrix Cloud. Per ulteriori informazioni, vedere:

- [Telemetria delle licenze Citrix] (<https://docs.citrix.com/en-us/licensing/current-release/license-server/licensing-data-collection-programs.html#citrix-licensing-telemetry>)
- [Aggiornamenti richiesti del server di licenza] (<https://support.citrix.com/article/CTX477636/required-license-server-update>)
- [Domande frequenti sulla telemetria delle licenze Citrix] (<https://support.citrix.com/article/CTX477614/citrix-license-telemetry-faq>)

Per l'elenco degli elementi di dati di telemetria delle licenze, vedere [Citrix Licensing Telemetry data elements](#) (Elementi di dati della telemetria delle licenze Citrix).

Informazioni sulla versione

Citrix Virtual Apps and Desktops 7 2402 LTSR Cumulative Update 1 (CU1) corregge più di 30 problemi segnalati a partire dalla versione iniziale del 2402 LTSR.

[2402 LTSR \(informazioni generali\)](#)

[2402 LTSR \(caratteristiche e informazioni sull'aggiornamento\)](#)

[Problemi risolti a partire da Citrix Virtual Apps and Desktops 7 2402 LTSR \(versione iniziale\)](#)

[Problemi noti di questa versione](#)

[Deprecazioni e rimozioni](#)

[Date di idoneità dell'abbonamento ai prodotti Citrix Subscription Advantage](#)

Download

[Citrix Virtual Apps and Desktops 7 2402 LTSR CU1](#)

Linux Virtual Delivery Agent 2402 LTSR CU1

Linux Virtual Delivery Agent 2402 CU1 contiene [correzioni](#).

Profile Management 2402 LTSR CU1

Profile Management 2402 CU1 contiene [correzioni](#).

Session Recording 2402 LTSR CU1

Session Recording 2402 CU1 contiene [correzioni](#).

StoreFront 2402 LTSR CU1

StoreFront 2402 CU1 contiene [correzioni](#).

Nuove distribuzioni

Come faccio a distribuire CU1 da zero?

È possibile configurare un ambiente Citrix Virtual Apps and Desktops completamente nuovo basato su CU1, utilizzando il metainstaller di CU1. Prima di farlo, consigliamo di prendere dimestichezza con il prodotto:

Consultare la sezione [Citrix Virtual Apps and Desktops 7 2402 LTSR \(versione iniziale\)](#) prestando particolare attenzione alle sezioni [Panoramica tecnica](#), [Installazione e configurazione](#) e [Sicurezza](#) prima di iniziare a pianificare la distribuzione. Assicurarsi che la configurazione soddisfi i [requisiti di sistema](#) di tutti i componenti.

Implementazioni esistenti

Cosa si deve aggiornare?

CU1 fornisce aggiornamenti a 15 componenti di base della versione 2402 LTSR. Ricordare: Citrix consiglia di aggiornare tutti i componenti LTSR della distribuzione a CU1. Ad esempio, se Citrix Provisioning fa parte della distribuzione LTSR, aggiornare i componenti di Citrix Provisioning a CU1. Se Citrix Provisioning non fa parte della distribuzione, non è necessario installarlo o aggiornarlo.

Componenti di base della versione 2402 LTSR CU1

Componente di base 2402 CU1	Versione come indicato in Programmi e funzionalità	Documentazione
VDA a sessione singola	2402.0.1100.1256	VDA a sessione singola
VDA multisessione	2402.0.1100.1256	VDA multisessione
Delivery Controller	2402.0.1100.1256	Delivery Controller
Citrix Studio	7.41.1100.48	Citrix Studio

Componente di base 2402 CU1	Versione come indicato in Programmi e funzionalità	Documentazione
Citrix Director	7.41.1100.33	Citrix Director
Gestione dei criteri di gruppo Citrix	7.41.1100.34	Gestione dei criteri di gruppo Citrix
Estensione lato client dei Criteri di gruppo Citrix	7.41.1100.34	
Citrix StoreFront	2402.0.1100.8	Citrix StoreFront
Universal Print Server	7.41.1100.58	Universal Print Server
Registrazione della sessione	24.2.1100	Registrazione della sessione
VDA Linux	22.03.1000.7	Virtual Delivery Agent per Linux
Profile Management	24.2.1100.23	Profile Management
Federated Authentication Service Citrix	10.17.1100.16	Citrix Federated Authentication Service (FAS)
Reindirizzamento del contenuto del browser	15.48.1100.65	Reindirizzamento del contenuto del browser
Citrix Probe Agent 2206	7.41.1100.15	Download

Componenti compatibili con 2402 LTSR CU1

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
App Layering	2206.0.0	Citrix App Layering
HDX RealTime Optimization Pack	2.9.400.2702	HDX RealTime Optimization Pack
License Server	11.17.2.0_BUILD_48000	License Server
Livello di personalizzazione utente	24.3.2	Livello di personalizzazione utente

Componenti e caratteristiche compatibili	Versione come indicato in Programmi e funzionalità	Documentazione
Lettore Web di registrazione della sessione	24.2.1100.16	Lettore Web di registrazione della sessione
Ottimizzazione di Microsoft Teams	15.32.1000.9	Ottimizzazione di Microsoft Teams
Workspace Environment Management	2402.1.100.1	Workspace Environment Management
VDA XenApp e XenDesktop 7.15 LTSR (versione più recente)*	Solo aggiornamento cumulativo più recente	Documentazione

Esclusioni notevoli di 2402 LTSR CU1

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

November 5, 2024

Sono stati risolti i seguenti problemi dalla versione Citrix Virtual Apps and Desktops 7 2402 LTSR (versione iniziale):

Citrix Director

- Nella pagina Filtri - Tutti i computer, quando si selezionano tutti i computer elencati sullo schermo e si tenta di scorrere l'elenco verso il basso, la selezione degli oggetti non funziona correttamente dopo un aggiornamento. [CVADHELP-25259]
- Il layout della tabella appare limitato a una piccola porzione dello schermo. [CVADHELP-25473]
- Nella pagina Director Filter Machine, dopo aver scelto la scheda «Multisessione» e aver visitato un'altra pagina, viene selezionata la scheda Desktop Machines a sessione singola predefinita quando si torna alla pagina Computer. [CVADHELP-25439]
- È possibile che si verifichi un problema quando si fa clic sui dettagli del profilo utente e si tenta di selezionare il testo per far scomparire UserProfileBox, impedendo la copia dei dati [CVADHELP-25211]
- Potresti notare che l'opzione UI.TaskManager.enableApplications viene ignorata nell'interfaccia utente, facendo sì che l'elenco delle applicazioni venga ancora visualizzato in Director. [CVADHELP-25178]
- Potrebbero verificarsi occasionali errori SSON in un Director con bilanciamento del carico dopo l'aggiornamento da 2203 CU4 a 2402. [CVADHELP-25646]
- Potresti notare che Director non viene più visualizzato se la connessione HDX è stata stabilita utilizzando Secure ICA. [CVADHELP-25253]

Criteri Citrix

- È possibile portare GPOScanner su 2404 senza alterare GpfxSettings.dll [CVADHELP-25384]
- È possibile che si verifichi un utilizzo elevato della memoria dal processo CseEngine.exe, che può causare problemi di registrazione del computer. [CVADHELP-25488]
- Potrebbe non essere possibile modificare o creare una policy dopo l'aggiornamento a 2402 da una versione precedente. Il problema non si verifica in un nuovo sito di installazione. [CVADHELP-25696]

- Potreste riscontrare problemi in cui il reindirizzamento bidirezionale dei contenuti non riesce dopo l'aggiornamento a Citrix Virtual Apps and Desktops 2402 LTSR [CVADHELP-25455]

Citrix Studio

- La console di Studio potrebbe bloccarsi quando si utilizza Studio come applicazione pubblicata o lo si utilizza in un VDA pubblicato nella sessione ICA. [CVADHELP-24990]

Delivery Controller

- Il servizio «Citrix.Analytics» non riesce quando si disinstalla la versione Desktop Delivery Controller (DDC) LTSR 2203 CU5 o si interrompono i servizi «Citrix.Analytics». [CVADHELP-25344]

Servizio di creazione di macchine

- Durante l'aggiornamento di un sito Multi-Delivery Controller da alcune versioni LTSR precedenti alla 2402 (incluse le versioni 2302, 2305, 2308, 2311) alla 2402 LTSR, le azioni di alimentazione su una VM potrebbero non riuscire se il sito viene aggiornato solo parzialmente. Per ulteriori informazioni, vedere [CTX666299](#). [CVADHELP-25301]

Grafica

- È possibile che si verifichino blackout intermittenti dello schermo della durata di circa 10 secondi durante il lavoro, durante i quali il processo grafico del software Citrix (Ctxgfx.exe) si ripristina. Il thread twencode presenta un'eccezione di violazione dell'accesso, che fa sì che CTXExceptionHandler registri i minidump e causi questo problema. CTXExceptionHandler è impostato per generare dump completi per l'esame. [CVADHELP-24877]
- Quando si avvia il desktop, è possibile che si verifichi una schermata nera a causa del guasto del ctxgfx. [CVADHELP-25145]

Metainstaller

- Quando si installa Citrix Rendezvous V2 utilizzando VDAWorkstationSetup_2402.exe, VDAServerSetup_2402.exe o VDAWorkstationCoreSetup_2402.exe, l'installazione potrebbe non riuscire poiché il file Citrix.Diagnostics.Tracing.dll non è presente in questi pacchetti. [CVADHELP-25368]

- Quando si tenta di installare Citrix Virtual Apps and Desktops 2402 tramite la riga di comando, il comando `Exclude «Local Host Cache Storage (LocalDB)»` non funziona come previsto. [CVADHELP-25270]
- A partire da Citrix Virtual Apps and Desktops 2402, quando si utilizza il comando `/exclude «Local Host Cache Storage (LocalDB)»` nel Delivery Controller, l'installazione del software del database SQL Server Express LocalDB si interrompe invece di continuare l'installazione senza LocalDB. [CVADHELP-25349]

Universal Print Server

Stampa

- È possibile che i servizi Windows Print spooler si blocchino sui VDA con `cpmon.dll`, con conseguente perdita delle stampanti e impossibilità di stampare dopo l'invio dei lavori di stampa. [CVADHELP-25484]

VDA per sistema operativo a sessione singola

Appunti

- Quando si utilizza VDA 2203 LTSR CU4 e quando si copiano e si incollano contenuti in formato WebP, `WFSHELL` smette di funzionare. [CVADHELP-25356]

Sessione/connessione

- L'applicazione OpenTEXT ETX non si apre a causa di una violazione di accesso con il seguente modulo: `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll` [CVADHELP-24985]
- È possibile che si verifichino spegnimenti casuali della macchina a sessione singola durante la transizione da un periodo di interruzione all'altro in cui non è attiva alcuna sessione. [CVADHELP-25615]

Smart card

- È possibile che si verifichi un problema di perdita di memoria con il servizio Citrix Smart Card su istanze VDA Server, in cui il consumo di memoria raggiunge il 100%. [CVADHELP-25389]

VDA per sistema operativo multisessione

Appunti

- Quando si utilizza VDA 2203 LTSR Cu4 e quando si copiano e si incollano contenuti in formato WebP, [WFShe11](#) smette di funzionare. [CVADHELP-25356]

Sessione/connessione

- L'applicazione OpenTEXT ETX non si apre a causa di una violazione di accesso con il seguente modulo: C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll [CVADHELP-24985]
- Potrebbero verificarsi arresti anomali di TermService con Citrix VDA. [CVADHELP-25104]
- I VDA potrebbero non rispondere in modo intermittente. [CVADHELP-25107]
- È possibile che si verifichi un errore in cui i dati del cloud broker non sono sincronizzati con il VDA, facendo apparire una sessione attiva sul VDA come disconnessa nel Director. [CVADHELP-25479]

Smart card

- È possibile che si verifichi un problema di perdita di memoria con il servizio Citrix Smart Card su istanze VDA Server, in cui il consumo di memoria raggiunge il 100%. [CVADHELP-25389]

VDA Linux

La [documentazione di Linux VDA 2402 CU1](#) fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Profile Management

La [documentazione di Profile Management 2402 CU1](#) fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

Registrazione della sessione

La [documentazione di Session Recording 2402 CU1](#) fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

StoreFront

La [documentazione di StoreFront 2402 CU1](#) fornisce informazioni specifiche sugli aggiornamenti presenti in questa versione.

2402 LTSR (versione iniziale)

September 11, 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 \(anteprima\)](#).

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
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

Componente di base 2402	Versione come indicato in Programmi e funzionalità	Documentazione
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
License Server	11.17.2.0_BUILD_47000	License Server
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
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

September 11, 2024

Sono stati risolti i seguenti problemi dopo la versione Citrix Virtual Apps and Desktops 7 2311:

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 (condizione 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]

Critério

- 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 `Wfshe11.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 `Wfshe11.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 [documentazione di 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.

Problemi noti

January 24, 2025

Appunti

- I problemi noti descritti nelle sezioni relative alla versione iniziale 2402 di questo articolo continuano a essere presenti in CU1, a meno che non siano inclusi nell'elenco dei problemi risolti.
- Se per un problema noto esiste una soluzione alternativa, questa viene fornita dopo la descrizione del problema.
- Il seguente avviso si applica a qualsiasi soluzione alternativa che suggerisce di modificare una voce del registro:

Avvertimento:

Una modifica errata del registro può causare gravi 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. Utilizza l'Editor del Registro di sistema a tuo rischio e pericolo. Assicuratevi di eseguire il backup del registro prima di modificarlo.

Problemi noti in 2402 CU1

- La funzionalità Virtual Channel Dynamini Plugin Manager è presente nell'interfaccia utente, ma non è supportata nella versione corrente. [LCM-14914]
- Quando si accede a Web Studio con Delivery Groups Administrator e Delivery Groups Scope personalizzato, potrebbe verificarsi un errore quando si tenta di eliminare un tag da una macchina con sistema operativo a sessione singola o da una macchina multisessione selezionando Gestisci tag.[LCM-15079]
- Dopo aver aggiornato StoreFront 2402 a 2402 CU1, gli utenti di dispositivi di lingua tedesca potrebbero non essere in grado di accedere all'app Citrix Workspace e al client Web Citrix Work-

space sui browser. La pagina di accesso potrebbe caricarsi senza alcun risultato. Per ulteriori informazioni, vedere [CTX691873](#). [CVADHELP-26301]

Problemi noti nella versione iniziale 2402

- Il seguente avviso si applica a qualsiasi soluzione alternativa che suggerisce di modificare una voce del registro:

Avvertimento:

Una modifica errata del registro può causare gravi 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. Utilizza l'Editor del Registro di sistema a tuo rischio e pericolo. Assicuratevi di eseguire il backup del registro prima di modificarlo.

Generale

- Se Citrix Files per Windows e/o Citrix Files per Office vengono installati prima dell'aggiornamento di VDA, questi componenti verranno disinstallati durante il processo di aggiornamento. Per risolvere il problema, reinstallare i componenti una volta completato l'aggiornamento VDA. [HDX-65579]
- Se si avvia la barra delle applicazioni e poi si apre il menu Connection Center nell'app Citrix Workspace per Windows, la barra delle applicazioni non viene visualizzata sotto il server che la ospita. [HDX-27504]
- Se si utilizza l'app Citrix Workspace per Windows e si avvia la barra delle applicazioni in posizione verticale, la barra copre il menu Start o la barra dell'orologio di sistema. [HDX-27505]
- La casella combinata potrebbe non essere visualizzata correttamente quando un utente seleziona una casella combinata che è già in evidenza sull'host. Come soluzione alternativa, seleziona un altro elemento dell'interfaccia utente e poi seleziona la casella combinata. [HDX-21671]
- Citrix Desktop Service potrebbe non avviarsi dopo aver eseguito un aggiornamento del sistema operativo da Windows 10 a Windows 11. Per risolvere il problema, riavviare la macchina. [HDX-58399]
- Le impostazioni dei limiti di sessione **** per VDA multisessione vengono rifiutate negli host di sessione che eseguono Windows Server 2022, Windows 10 Enterprise multisessione e Windows 11 Enterprise multisessione. Come soluzione alternativa, puoi configurare **limiti di tempo della sessione RDS** tramite GPO. [HDX-47001]

- La finestra di dialogo Sicurezza di Windows associata a FIDO2 non verrà visualizzata davanti alla finestra della sessione ICA se si esegue l'applicazione con privilegi di amministratore. È la progettazione del sistema operativo a far sì che la finestra di dialogo Sicurezza di Windows venga nascosta dietro la finestra della sessione ICA se è in esecuzione come processo con privilegi elevati. [HDX-26794]
- Le operazioni di copia e incolla negli appunti potrebbero non riuscire se i dati sono più grandi di 100 MB dal client alla sessione ICA. Le copie buffer di grandi dimensioni non sono supportate. [HDX-59028]
- I sistemi operativi multiseSSIONE Windows 10 o Windows 11 non supportano Ripristino configurazione di sistema di Windows. Pertanto, l'opzione per creare un punto di ripristino non è disponibile nell'interfaccia utente. Le opzioni della riga di comando `/EnableRestore` o `/EnableRestoreCleanup` vengono ignorate e viene registrato il messaggio **Disabilitazione del Ripristino configurazione di sistema** come attualmente non supportato sui sistemi operativi multiseSSIONE Windows 10/11". [HDX-58915]
- Citrix firma sia i file binari generati da Citrix sia quelli di terze parti. Ciò significa che i file binari sono autenticati da Citrix. Le versioni dei file binari di terze parti rimangono le stesse poiché vengono acquisite da terze parti. Se un binario è già installato, un aggiornamento VDA non installa i binari perché le versioni corrispondono. Per evitare questa limitazione:
 1. Includere i binari in un elenco consentito **. In questo modo si elimina la necessità di firmare i file binari.
 2. Disinstallare il vecchio VDA e installare quello nuovo. Ciò assomiglia a una nuova installazione VDA e vengono applicate le versioni firmate.

[HDX-62302]

- In alcuni scenari, quando si utilizza il filtro dei criteri IP client, l'indirizzo IP utilizzato per valutare il criterio non è corretto. [HDX-62375]
- Quando si utilizza il pass-through di dominio avanzato per l'accesso Single Sign-On, l'accesso Single Sign-On alla sessione potrebbe non riuscire se il dispositivo client o l'host della sessione esegue Windows 11. [HDX-62973]
- Vi è un ritardo di 5 minuti tra l'aggiornamento di qualsiasi impostazione di policy e la generazione del BLOB nel servizio del sito. Di conseguenza, potrebbe volerci del tempo prima che le policy vengano aggiornate e recepite nelle sessioni.

Politiche

- Se si esegue l'aggiornamento da una qualsiasi versione precedente di Citrix Virtual Apps and Desktops alla versione 2311 o 2402 LTSR, i dati della policy potrebbero andare persi se sono

presenti valori di dati non validi nelle impostazioni [Policy](#) . Per saperne di più sul problema e sulle soluzioni alternative correlate, vedere [CTX666304](#). [GP-1671]

Grafica

- Se si avvia un'anteprima video utilizzando un'app webcam a 64 bit con compressione Theora, la sessione potrebbe bloccarsi. [HDX-21443]
- Potresti notare delle webcam aggiuntive collegate al desktop remoto nell'app Skype per desktop. Per motivi di sicurezza, l'anteprima di queste webcam extra è bloccata e potrebbe mostrare una schermata nera. È possibile ignorare la webcam aggiuntiva e continuare a utilizzare la webcam per l'endpoint. [HDX-58807]
- H265 444 su Intel e alcune GPU NVIDIA potrebbe causare artefatti visibili nella sessione. Per i problemi relativi alle GPU Intel, esiste una soluzione temporanea che consiste nel ridimensionare la sessione o attivare la modalità a schermo intero. [PMCS-41084]

Servizi di creazione di macchine

- In un ambiente VMware ospitato su AWS, la creazione del catalogo macchine MCS fallisce se l'immagine master è abilitata per vTPM. Questo problema riguarda tutte le versioni di Citrix Virtual Apps and Desktops ed è dovuto a un problema nell'ambiente VMware. Per assistenza, contattare [supporto VMware](#). [PMCS-38514]
- Durante l'aggiornamento di un sito Multi-Delivery Controller da alcune versioni LTSR precedenti alla 2402 (incluse le versioni 2302, 2305, 2308, 2311) alla versione LTSR 2402, le azioni di alimentazione su una VM potrebbero non riuscire se il sito viene aggiornato solo parzialmente. Per ulteriori informazioni vedere [CTX666299](#).

Stampa

- Le stampanti Universal Print Server selezionate sul desktop virtuale non vengono visualizzate nella finestra **Dispositivi e stampanti** del pannello di controllo. Tuttavia, quando gli utenti lavorano sulle applicazioni, possono utilizzare tali stampanti. Questo problema si verifica solo su Windows 10. Per ulteriori informazioni, vedere [CTX213540](#). [HDX-5043, 335153]
- La stampante predefinita potrebbe non essere contrassegnata correttamente nella finestra di dialogo di stampa. Questo problema non riguarda i lavori di stampa inviati alla stampante predefinita. [HDX-12755]
- Alcuni processi di stampa provenienti da stampanti di rete con bilanciamento del carico potrebbero non riuscire quando sono abilitate le connessioni SSL ai server di stampa universali. Ciò accade quando i lavori di stampa vengono eseguiti rapidamente uno dopo l'altro. [HDX-58316]

Problemi di terze parti

- Chrome supporta l'automazione dell'interfaccia utente solo per le barre degli strumenti, le schede, i menu e i pulsanti presenti in una pagina web. A causa di questo problema di Chrome, la funzionalità di visualizzazione automatica della tastiera potrebbe non funzionare nel browser Chrome sui dispositivi touch. Come soluzione alternativa, esegui `chrome --force-renderer-accessibility` oppure puoi aprire una nuova scheda del browser, digitare `chrome://accessibility` e abilitare il supporto **Native Accessibility API** per pagine specifiche o per tutte le pagine. Inoltre, quando pubblichi un'app senza interruzioni, puoi pubblicare Chrome con l'opzione `--force-renderer-accessibility`. [HDX-20858]
- Se FSLogix 2201 HF1 è installato sull'host della sessione, è possibile che venga visualizzata una schermata nera quando si avvia una sessione. Per risolvere questo problema, è necessario aggiornare FSLogix a una versione più recente. [HDX-46159]

Gestione del profilo

- [La documentazione di Profile Management 2402 LTSR](#) fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Linux VDA

- [La documentazione Linux VDA 2402 LTSR](#) fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Registrazione della sessione

- [La documentazione di Session Recording 2402 LTSR](#) fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Gestione dell'ambiente di lavoro

- [La documentazione di Workspace Environment Management 2402 LTSR](#) fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Fornitura Citrix

- [La documentazione di Citrix Provisioning 2402 LTSR](#) fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Servizio di autenticazione federata

- [La documentazione del Federated Authentication Service 2402 LTSR](#) fornisce informazioni specifiche sugli aggiornamenti di questa versione.

Deprecazione

January 24, 2025

Gli annunci contenuti in questo articolo hanno lo scopo di informarti in anticipo sulle piattaforme, sui prodotti Citrix e sulle funzionalità che verranno gradualmente eliminati, in modo da consentirti di prendere decisioni aziendali tempestive. Citrix monitora l'utilizzo e il feedback dei clienti per determinare quando tali servizi vengono ritirati. Gli annunci potrebbero cambiare nelle versioni successive e potrebbero non includere tutte le funzionalità o caratteristiche deprecate. Per maggiori dettagli sul supporto del ciclo di vita del prodotto, consultare l'articolo [Politica di supporto del ciclo di vita del prodotto](#). Per informazioni sull'opzione di manutenzione Long Term Service Release (LTSR), vedere <https://support.citrix.com/article/CTX205549>.

Deprecazioni e rimozioni

Nella tabella seguente sono riportate le piattaforme, i prodotti Citrix e le funzionalità deprecate o rimosse. Le date in grassetto ** indicano le modifiche apportate in questa versione.

Deprecazioni

Deprecazione significa che intendiamo rimuovere la funzionalità o la capacità da una versione futura. La funzionalità o capacità continuerà a funzionare e sarà pienamente supportata finché non verrà ufficialmente rimossa. Questa notifica di abbandono può durare alcuni mesi o anni. Dopo la rimozione, la funzionalità o capacità non sarà più attiva. Questa nota informativa ha lo scopo di darti il tempo necessario per pianificare e aggiornare il tuo codice prima che la funzionalità o la capacità venga rimossa. Ove possibile, vengono suggerite alternative per gli elementi deprecati.

Articolo	Deprecazione annunciata nella versione	Alternativa
Appuntamento V1	2402	Utilizzare Rendezvous V2.

Articolo	Deprecazione annunciata nella versione	Alternativa
ICA sicuro	2402	-
Supporto VDA su Windows Server 2016	2402	Eseguire l'aggiornamento alle ultime versioni di Windows Server.
Supporto per Delivery Controller, Web Studio, Citrix Director, Citrix License Server, Citrix StoreFront, Server VDI per sistemi operativi a sessione singola, VDA per sistemi operativi multisessione, foresta e dominio Active Directory e Universal Print Server su Windows Server 2016	2402	Eseguire l'aggiornamento all'ultima versione di Windows Server.
Supporto per le versioni 2016 e 2017 di Microsoft SQL Server per la configurazione del sito, la registrazione della configurazione e il monitoraggio dei database	2402	Eseguire l'aggiornamento all'ultima versione di Microsoft SQL Server.
Supporto per la configurazione della cache write-back per includere solo una cache del disco e nessuna cache di memoria	2402	Utilizzare l'opzione di configurazione della dimensione della cache di memoria e allocare una dimensione diversa da zero.

Articolo	Deprecazione annunciata nella versione	Alternativa
Supporto per i cataloghi di Azure creati prima della funzionalità di provisioning su richiesta (cataloghi “legacy”)	2402	Ricareare le VM del catalogo legacy di Azure. I cataloghi vengono forniti su richiesta, consentendo così di risparmiare sui costi di archiviazione.
La politica Target Minimum Frame Rate	2311	Utilizzare Indicatore di stato grafico per modificare il frame rate minimo di destinazione.
Supporto per Citrix Connector 3.1 per System Center Configuration Manager	2311	Aggiornare manualmente l’immagine o l’applicazione.
Supporto per l’utilizzo di un’immagine master in una regione diversa da quella in cui è stato creato il catalogo	2311	Utilizzare Azure Compute Gallery per replicare l’immagine master nella regione desiderata.
Impostazione del limite di memoria del display grafico HDX	2311	Viene allocata la quantità minima di memoria richiesta per garantire che il layout di visualizzazione del client sia pienamente supportato.
Supporto della modalità progressiva in HDX Graphics	2311	Utilizzare Thinwire. Vedere Modalità progressiva .

Articolo	Deprecazione annunciata nella versione	Alternativa
Supporto per il reindirizzamento del contenuto del browser in Internet Explorer 11	2311	Utilizza il reindirizzamento dei contenuti del browser basato su Google Chrome.
Rimosso il supporto per AWS Volume Worker	2311	Utilizzare caricamento e download diretto su disco. Vedere Caricamento e download diretto su disco .
Supporto per SQL Server 2016 in Broker	2308	Utilizzare le versioni più recenti. Per ulteriori informazioni, vedere Requisiti di sistema .
Supporto per XenApp 5.x in Director	2308	—
Supporto per XenApp 6.x in Director	2308	—
Pacchetto SCOM per gli avvisi in Director	2308	—
Supporto per plug-in in Director	2308	—
Supporto per il formato WebRTC SDP (Piano B)	2308	Aggiornare l'app Citrix Workspace a una versione supportata.

Articolo	Deprecazione annunciata nella versione	Alternativa
Supporto per la modalità Finestra singola in Microsoft Teams Optimization	2308	Aggiornare l'app Citrix Workspace a una versione che supporti la modalità MultiWindow. Per ulteriori informazioni, vedere Matrice delle funzionalità e supporto della versione .
Supporto per <code>AwsCaptureInstanceProperties</code> utilizzato negli ambienti AWS	2308	Utilizzare un profilo macchina. Vedere Creare un catalogo utilizzando un profilo macchina .
<code>Schedule-ProvVMUpdate</code> Comando PowerShell	2305	Utilizzare <code>Set-ProvVMUpdateTimeWindow</code> .
<code>Richiesta-ProvVMUpdate</code> Comando PowerShell	2305	Utilizzare <code>Set-ProvVMUpdateTimeWindow</code> con i parametri <code>-StartsNow</code> e <code>-DurationInMinutes -1</code> .
<code>Annulla-ProvVMUpdate</code> Comando PowerShell	2305	Utilizzare <code>Clear-ProvVMUpdateTimeWindow</code> .
<code>DedicatedTenancy</code> parametro utilizzato nel comando <code>New-ProvScheme</code>	2303	Utilizzare il parametro <code>TenancyType</code> .
Server di licenza VPX	2206	—
Disco non gestito per il provisioning delle VM negli ambienti Azure.	2206	Utilizza dischi gestiti .

Articolo	Deprecazione annunciata nella versione	Alternativa	
Reindirizzamento da host a client (URL)	2203	Reindirizzamento bidirezionale del contenuto.	
Supporto per quattro comandi specifici di AWS: <code>Revoke-HypSecurityGroupIngress</code> , <code>Revoke-HypSecurityGroupEgress</code> , <code>Grant-HypSecuritygroupegress</code> e <code>Grant-HypSecurityGroupIngress</code> utilizzati nell'ambiente cloud e locale.	2203	—	
File Citrix per Windows e file Citrix per Outlook dal metainstallatore VDA.	2203	Utilizzare gli installatori autonomi .	
Componente WEM Agent dal metainstallatore VDA.	2203	—	
Opzione Wake on LAN integrata in SCCM per l'accesso remoto al PC.	2012	Utilizzare la funzionalità Wake on LAN autonoma .	
Supporto per la procedura guidata di importazione PVS in Citrix Studio	1912 LTSR	—	Esegui il provisioning delle macchine Citrix Provisioning utilizzando uno dei seguenti metodi: Esegui il provisioning delle macchine utilizzando Citrix Provisioning Console ed esportale in Citrix ³⁹ Virtual Apps and Desktops utilizzando Citrix Provisioning Devices Export Wizard

Articolo	Deprecazione annunciata nella versione	Alternativa
Citrix SCOM Management Pack per XenApp e XenDesktop, Provisioning Services e StoreFront. Per le versioni del prodotto che possono essere monitorate, vedere documentazione di Citrix SCOM Management Packs .	1912	Utilizza Director per monitorare e gestire la tua distribuzione. Per ulteriori informazioni su SCOM EOL e sulle alternative, vedere https://support.citrix.com/article/CTX266943 .
Mobility SDK / Mobile SDK (dall'ex Citrix Labs)	7.16	Sostituito dalle impostazioni dei criteri di esperienza mobile e dalle esperienze native per desktop/app ospitati.

Traslochi

Gli elementi rimossi vengono rimossi oppure non sono più supportati in Citrix Virtual Apps and Desktops.

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Applicazione Citrix Workspace per Windows 1912	—	2402	Utilizzare le versioni più recenti.
Grafica HDX FullScreen + Ottimizzazione del testo	2311	2311	

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto per NVIDIA Frame Buffer Capture (NVFBC) con HDX 3D Pro	2308	2311	Utilizzare Desktop Duplication API (DDAPI).
Supporto VDA per l'impostazione del criterio "Installazione automatica dei driver della stampante in dotazione".	7.16	2311	Nessuno. Impostazione dei criteri supportata con VDA solo sui sistemi operativi precedenti (Windows 7, Windows Server 2012 R2 e precedenti).
Codifica hardware GPU NVIDIA (NVENC) con: vGPU 11 e versioni precedenti e driver versione 466.77 e versioni precedenti.	2305	2305	Utilizzare i driver NVIDIA attualmente supportati: vGPU 13 o successiva, versione 471.41 o successiva.
Citrix Supportability Tools (Supportability-Tool_x64 .msi) da VDA Meta-Installer.	—	2212	—
Citrix License Administration Console (inclusa per l'ultima volta in Windows License Server 11.16.3 build 30000 e rimossa in Windows License Server v11.16.6 build 31000).	2003	2006	Utilizzare Citrix Licensing Manager.

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto della scheda grafica Citrix Indirect Display Driver (IDD) su Windows 10 versione 1709 e precedenti.	2003	2003	Utilizzare Citrix Virtual Apps and Desktops 7 1912 LTSR VDA.
Codifica hardware con GPU NVIDIA (NVENC) utilizzando driver di visualizzazione GRID 9 o precedenti.	2003	2003	Utilizzare i driver di visualizzazione GRID 10 con Citrix Virtual Apps and Desktops 7 2003 o VDA successivi, oppure utilizzare Citrix Virtual Apps and Desktops 7 1912 LTSR VDA.
Funzionalità di reimpostazione self-service della password (SSPR).	2003	2006	—
Supporto per le versioni di Microsoft .NET Framework precedenti alla versione 4.8 per VDA e componenti server principali. Include Delivery Controller, Studio e Regista.	1912	2003	Aggiornare alla versione 4.8 di .NET Framework.
VDA su Windows Server 2012 R2.	1912	2003	Installare VDA su un sistema operativo supportato.
Componente di migrazione delle applicazioni AppDNA di Citrix Virtual Apps and Desktops Premium Edition.	1909	2003	—

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Installazione di Studio su macchine a 32 bit (x86).	1909	2003	Installare su un sistema operativo x64 supportato.
Supporto per l'hook di Excel nelle applicazioni senza soluzione di continuità. Questa funzione è stata utilizzata per creare icone separate sulla barra delle applicazioni per ogni cartella di lavoro di Microsoft Excel 2010.	1909	1909	—
Componenti server principali su Windows Server 2012 R2 (inclusi i Service Pack). Include: Delivery Controller, Studio e Regista.	1906	2003	Installare su un sistema operativo supportato più recente.
Supporto per i database di configurazione del sito, registrazione della configurazione e monitoraggio su Microsoft SQL Server versioni 2008 R2, 2012 e 2014 (inclusi tutti i Service Pack e le edizioni).	1906	2003	Installare i database su una versione supportata di Microsoft SQL Server.

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto per VDA su Windows 10 su piattaforme x86.	1906	1909*	Installare VDA su un sistema operativo x64 supportato. *Questa funzionalità è ancora supportata in Citrix Virtual Apps and Desktops 7 1912 LTSR.
Rimozione di Citrix Smart Tools Agent dal supporto di installazione di Citrix Virtual Apps and Desktops.	1903	1906	—
Rimozione delle opzioni Delivery Controller per i seguenti prodotti a fine ciclo di vita all'interno di StoreFront: VDI-in-a-Box e XenMobile (9.0 e versioni precedenti).	1903	1903	—
Supporto per Linux VDA su Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Installa Linux VDA su una versione successiva di Red Hat Enterprise Linux.
Supporto StoreFront per i protocolli TLS 1.0 e TLS 1.1 tra Citrix Virtual Apps and Desktops (in precedenza XenApp e XenDesktop) e Citrix Receiver e Workspace Hub.	7.17	2203	Aggiornare Citrix Receiver a un'app Citrix Workspace che supporti il protocollo TLS 1.2. Per ulteriori informazioni sull'app Citrix Workspace, vedere https://docs.citrix.com/en-us/citrix-workspace-app .

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto VDA per l'impostazione del criterio "Installazione automatica dei driver della stampante in dotazione".	7.16	2311	Nessuno. Impostazione dei criteri supportata con VDA solo sui sistemi operativi precedenti (Windows 7, Windows Server 2012 R2 e precedenti).
Supporto StoreFront per consentire agli utenti di accedere ai desktop sui siti Desktop Appliance	1811	1912	Utilizzare Blocco desktop per casi d'uso non appartenenti a un dominio.
Supporto per la tecnologia di controllo remoto del display Framehawk	1811	1903	Utilizzare Thinwire con trasporto adattivo abilitato.
Supporto per Citrix Smart Scale in tutte le versioni di Citrix Virtual Apps and Desktops (e XenApp e XenDesktop). Questa funzionalità raggiungerà la fine del suo ciclo di vita il 31 maggio 2019.	1808	1906	Si consiglia di utilizzare il servizio Virtual Apps and Desktops su Citrix Cloud per una migliore funzionalità di gestione dell'alimentazione.
Supporto per le versioni 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 e 4.7 di Microsoft .NET Framework da parte di Citrix StoreFront, Citrix VDAs, Citrix Studio, Citrix Director e Citrix Delivery Controller.	7.18	1808	Eseguire l'aggiornamento a .NET Framework versione 4.7.1 o successiva. (Il programma di installazione installa automaticamente .NET Framework 4.7.1 se non è già installato.)

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto per Linux VDA su Red Hat Enterprise Linux 7.3.	7.18	1808	Installa Linux VDA su una versione successiva di Red Hat Enterprise Linux.
Supporto per Linux VDA su SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Installa Linux VDA sulla versione SUSE supportata.
Supporto per il driver Citrix WDDM su VDA	7.16	7.16	Il driver Citrix WDDM non viene più installato con i VDA.
VDA su Windows 10 versione 1511 (Threshold 2) e versioni precedenti del sistema operativo Windows Single-session, inclusi Windows 8.x e Windows 7 (vedere https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	7.15 LTSR (e 7.12)	7.16	Installare VDA del sistema operativo a sessione singola su Windows 10 versione minima 1607 (Redstone 1) o canali semestrali più recenti. Se si utilizza 1607 LTSB, si consiglia un VDA 7.15. Vedere CTX224843 .
VDA su Windows Server 2008 R2 e Windows Server 2012 (inclusi i Service Pack)	7.15 LTSR (e 7.12)	7.16	Installare VDA su un sistema operativo supportato.
Reindirizzamento della composizione del desktop (precedentemente noto come DirectX Command Remoting) (DCR)	7.15 LTSR	7.16	Utilizzare Thinwire .

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Citrix Receiver per l'esperienza Web classica (interfaccia utente "bolle verdi")	7.15 LTSR (e StoreFront 3.12)	1903	Citrix Receiver per un'esperienza Web unificata.
Componenti principali di Windows Server 2012 e Windows Server 2008 R2 (inclusi i Service Pack). Include: Delivery Controller, Studio, Director, StoreFront, License Server e Universal Print Server.	7.15 LTSR	7.18	Installa i componenti su un sistema operativo supportato.
Funzionalità di reimpostazione della password self-service (SSPR) su Windows Server 2012 e Windows Server 2008 R2 (inclusi i Service Pack)	7.15 LTSR	7.18	Installare su un sistema operativo supportato più recente.
Studio su Windows 7, Windows 8 e Windows 8.1 (inclusi i Service Pack)	7.15 LTSR	7.18	Installa Studio su un sistema operativo supportato.

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Reindirizzamento Flash	7.15 LTSR	1912	Crea contenuti video come video HTML5. Utilizzare il reindirizzamento video HTML5 per i contenuti gestiti e il reindirizzamento dei contenuti del browser per i siti Web pubblici. Per ulteriori informazioni, vedere la nota sulla fine del ciclo di vita del reindirizzamento Flash .
Integrazione Citrix Online (prodotto Goto) con StoreFront	7.14 (e StoreFront 3.11)	NegozioFront 3.12	—
L'account utente CtxAppVCOMAdmin, creato durante l'installazione di VDA e aggiunto al gruppo Amministratori locali sulla macchina VDA, non viene più creato. Viene rimosso anche il meccanismo "COM" sottostante.	7.14	7.14	Il servizio Windows CtxAppVService esegue la stessa funzione. Viene installato e configurato automaticamente e non richiede alcuna interazione da parte dell'utente.
Supporto del componente Universal Print Server UpsServer su Windows Server 2008 a 32 bit	7.14	7.14	Installare su un sistema operativo supportato più recente.

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
StoreFront e Receiver per Web su Internet Explorer 8	7.13	7.13	—
Opzione di installazione della riga di comando VDA /no_appv per impedire l'installazione dei componenti Citrix App-V	7.13	7.13	Utilizzare l'opzione di installazione della riga di comando /exclude "Citrix Personalization for App-V –VDA".
Il programma di installazione completo del prodotto non installa più lo snap-in Citrix.Common.Commands nelle nuove installazioni e lo rimuove automaticamente durante l'aggiornamento delle installazioni esistenti.	7.13	7.13	Alcuni comandi di PowerShell forniti dallo snap-in Citrix.Common.Commands sono ancora disponibili nell'SDK XenApp 6.5.
Funzionalità parziale per manipolare i dati delle icone fornita dai cmdlet *-CtxIcon.	7.13	7.13	Ora fornito dai cmdlet *-BrokerIcon nel servizio Broker.
Modalità Thinwire legacy	7.12	7.16	Utilizzare Thinwire . Se si utilizza la modalità Legacy Thinwire su Windows Server 2008 R2, eseguire la migrazione a Windows Server 2012 R2 o Windows Server 2016 e utilizzare Thinwire.

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Aggiornamenti in loco da StoreFront 2.0, 2.1, 2.5 e 2.5.2	7.13	7.16	Eseguire l'aggiornamento da una di queste versioni a una versione supportata successiva e quindi a XenApp e XenDesktop 7.16.
Aggiornamenti in loco da XenDesktop 5.6 o 5.6 FP1	7.12	7.16	Esegui la migrazione della distribuzione XenDesktop 5.6 o 5.6 FP1 alla versione corrente di XenDesktop. Per fare ciò, eseguire prima l'aggiornamento a XenDesktop 7.6 LTSR (con l'ultima CU), quindi eseguire l'aggiornamento all'ultima versione di Citrix Virtual Desktops (in precedenza XenDesktop) o LTSR.
Installazione di Delivery Controller, Director, StoreFront o License Server su computer a 32 bit (x86).	7.12	7.16	Installare su un sistema operativo x64 supportato.
Leasing di collegamento XenDesktop 5.6	7.12	7.16	Utilizzare Cache host locale .
utilizzato su Windows XP. Le installazioni VDA su Windows XP non sono supportate.	7.12	7.16	Installare VDA su un sistema operativo supportato.

Articolo	Deprecazione annunciata nella versione	Rimosso nella versione	Alternativa
Supporto per le connessioni CloudPlatform	7.12	2003	Utilizzare un hypervisor o un servizio cloud supportato diverso.
Supporto per le connessioni di Azure Classic (noto anche come Azure Service Management)	7.12	2003	Si consiglia di utilizzare il servizio Virtual Apps and Desktops su Citrix Cloud.
Funzionalità AppDisks (e l'integrazione AppDNA in Studio, che la supporta)	7.13	2003	Utilizzare Citrix App Layering.
Funzionalità vDisk personale	7.15	2006†	Utilizzare la tecnologia Citrix App Layering livello utente o livello di personalizzazione utente .

† In Citrix Virtual Apps and Desktops 7 2003, il driver Personal vDisk è stato rimosso dal programma di installazione VDA. In Citrix Virtual Apps and Desktops 7 2006, il flusso di lavoro del driver Personal vDisk è stato rimosso da Studio.

Requisiti di sistema

September 11, 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
License Server	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 2022 LocalDB da utilizzare con la funzionalità Local Host Cache. 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.

Installazione e configurazione

November 5, 2024

Leggere gli articoli a cui si fa riferimento prima di avviare ciascuna fase di distribuzione per informazioni su ciò che viene visualizzato e specificato durante la distribuzione.

Utilizzare la sequenza seguente per distribuire Citrix Virtual Apps and Desktops.

Preparazione

Revisione [Preparati a installare](#) e completa tutte le attività necessarie.

- Dove trovare informazioni su concetti, caratteristiche, differenze rispetto alle versioni precedenti, requisiti di sistema e database.
- Aspetti da considerare quando si decide dove installare i componenti principali.
- Requisiti delle autorizzazioni e di Active Directory.
- Informazioni sui programmi di installazione, gli strumenti e le interfacce disponibili.

Installare i componenti principali

Installate Delivery Controller, [Web Studio](#), Citrix Director e Citrix License Server. È inoltre possibile installare Citrix StoreFront. Per i dettagli, consulta [Installare i componenti principali](#) o [Install utilizzando la riga di comando](#).

Crea un sito

Dopo aver installato i componenti principali e avviato Studio, viene richiesto di creare un sito .

Installazione di uno o più Virtual Delivery Agent (VDA)

Installare un VDA su un computer che esegue un sistema operativo Windows, su un'immagine master o direttamente su ciascun computer. Vedi [Installare i VDA](#) o [Install utilizzando la riga di comando](#). Gli script [di esempio](#) sono forniti se si desidera installare i VDA tramite Active Directory.

Per le macchine con sistema operativo Linux, segui le indicazioni fornite in [Linux Virtual Delivery Agent](#).

Per una distribuzione di Remote PC Access, installa un VDA per un sistema operativo a sessione singola su ogni PC dell'ufficio. Se sono necessari solo i servizi VDA di base, utilizzare il programma di installazione autonomo `VDAWorkstationCoreSetup.exe` e i metodi di distribuzione elettronica del software (ESD) esistenti. ([Prepare to install](#) descrive i programmi di installazione VDA disponibili.)

Installazione dei componenti opzionali

Se si prevede di utilizzare Citrix Universal Print Server, installare il componente server sui server di stampa. Vedi [Installare i componenti principali](#) o [Install utilizzando la riga di comando](#).

Per consentire a StoreFront di utilizzare opzioni di autenticazione come le asserzioni SAML, installare [Citrix Federated Authentication Service](#).

Per consentire agli utenti finali di avere un maggiore controllo sui propri account utente, installare [Reimpostazione password self-service](#).

Facoltativamente, è possibile integrare più componenti Citrix nella distribuzione di Citrix Virtual Apps and Desktops.

- [Citrix Provisioning](#) è un componente opzionale che esegue il provisioning delle macchine trasmettendo un'immagine master ai dispositivi di destinazione.
- [Citrix Gateway](#) è una soluzione sicura per l'accesso alle applicazioni che fornisce agli amministratori criteri e controlli di azione granulari a livello di applicazione per proteggere l'accesso alle applicazioni e ai dati.
- [Citrix SD-WAN](#) è un insieme di appliance che ottimizzano le prestazioni WAN.

Creare un catalogo di macchine

Dopo aver creato un sito in Studio, sei guidato a [creare un catalogo di macchine](#).

Un catalogo può contenere macchine fisiche o virtuali (VM). Le macchine virtuali possono essere create a partire da un'immagine master. Quando si utilizza un hypervisor o un altro servizio per fornire macchine virtuali, è innanzitutto necessario creare un'immagine master su tale host. Quindi, quando si crea il catalogo, si specifica tale immagine, che viene utilizzata durante la creazione di macchine virtuali.

Creare un gruppo di consegna

Dopo aver creato il tuo primo catalogo di macchine in Web Studio, sei guidato a [creare un gruppo di consegna](#).

Un gruppo di consegna specifica quali utenti possono accedere ai computer in un catalogo selezionato e quali applicazioni sono disponibili per tali utenti.

Creare un gruppo di applicazioni (facoltativo)

Dopo aver creato un gruppo di consegna, puoi facoltativamente [creare un gruppo di applicazioni](#). È possibile creare gruppi di applicazioni per applicazioni condivise tra gruppi di consegna diversi o utilizzate da un sottoinsieme di utenti all'interno di gruppi di consegna.

Limitazione nota

Quando si utilizza l'app Citrix Workspace per Windows versione 1912 o precedente, la sessione si interrompe dopo un po'. Questo problema è stato risolto nelle versioni più recenti LTSR e CR dell'app Citrix Workspace. Per ulteriori informazioni sulle versioni di rilascio supportate, vedere [App Citrix Workspace per Windows/Citrix Receiver for Windows Long Term Service Releases](#).

Ambienti di virtualizzazione di Microsoft System Center Virtual Machine Manager

November 5, 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.

Ulteriori informazioni

- [Crea e gestisci connessioni e risorse](#)

- [Creare cataloghi di macchine](#)

Installare utilizzando la riga di comando

November 5, 2024

Importante:

- Se stai effettuando l'aggiornamento e la tua versione attuale utilizza o ha installato il software Personal vDisk o AppDisks, vedi [Rimozione di PvD, AppDisks e host non supportati](#).
- Citrix raccoglie i dati di licenza di base necessari per i suoi interessi legittimi, inclusa la conformità delle licenze. Per ulteriori informazioni, vedere [Citrix Licensing Data](#).

Introduzione

Questo articolo si applica all'installazione di componenti su macchine con sistemi operativi Windows. Per informazioni sui VDA per i sistemi operativi Linux, vedere [Linux Virtual Delivery Agent](#).

In questo articolo viene descritto come emettere i comandi di installazione del prodotto. Prima di iniziare qualsiasi installazione, rivedi [Prepararsi all'installazione](#). Quell'articolo include le descrizioni dei programmi di installazione disponibili.

Per visualizzare l'avanzamento dell'esecuzione dei comandi e i valori restituiti, è necessario essere l'amministratore originale oppure utilizzare **Esegui come amministratore**. Per ulteriori informazioni, vedere la documentazione dei comandi Microsoft.

Come complemento all'utilizzo diretto dei comandi di installazione, nella ISO del prodotto vengono forniti script di esempio che installano, aggiornano o rimuovono i VDA sui computer in Active Directory. Per i dettagli, vedere [Installare i VDA utilizzando gli script](#).

Se si tenta di installare o eseguire l'aggiornamento su una versione del sistema operativo Windows non supportata per questa versione di Citrix Virtual Apps and Desktops, viene visualizzato un messaggio di informazioni sulle opzioni disponibili. Vedi [Sistemi operativi precedenti](#).

Per informazioni su come Citrix riporta i risultati delle installazioni dei componenti, vedere [Citrix installation return codes](#).

Utilizzare il programma di installazione del prodotto completo

Per accedere all'interfaccia della riga di comando del programma di installazione del prodotto completo:

1. Scaricare il pacchetto del prodotto da Citrix. Per accedere al sito di download, sono necessarie le credenziali dell'account Citrix.
2. Decomprimere il file. Facoltativamente, masterizzare un DVD con il file ISO.
3. Accedere al server in cui si stanno installando i componenti utilizzando un account amministratore locale.
4. Inserire il DVD nell'unità o montare il file ISO.
5. Dalla directory `\x64\XenDesktop Setup` sul supporto, esegui il comando appropriato.

Per installare i componenti principali: Esegui `XenDesktopServerSetup.exe`, con le opzioni elencate in Opzioni della riga di comando per l'installazione dei componenti principali.

Per installare un VDA: Esegui `XenDesktopVDASetup.exe` con le opzioni elencate in Opzioni della riga di comando per l'installazione di un VDA.

Per installare StoreFront: Esegui `CitrixStoreFront-x64.exe` nella cartella `x64 > StoreFront` sul supporto di installazione.

Per installare Universal Print Server: seguire le istruzioni riportate in Opzioni della riga di comando per l'installazione di un Universal Print Server.

Per installare Federated Authentication Service: Citrix consiglia di utilizzare l'interfaccia grafica.

Per installare Session Recording: seguire le istruzioni riportate in [Session Recording](#).

Per installare Workspace Environment Management: Segui le indicazioni in [Workspace Environment Management](#).

Per installare Secure Private Access: Esegui `XenDesktopSPASetup.exe` nella cartella `x64 > XenDesktop Setup` sul supporto di installazione. Segui le indicazioni nelle opzioni della riga di comando per l'installazione di [Secure Private Access](#).

Opzioni della riga di comando per l'installazione dei componenti principali

Le seguenti opzioni di parametro sono valide quando si installano i componenti principali con il comando `XenDesktopServerSetup.exe`. Per maggiori dettagli sulle opzioni, vedi [Installare i componenti principali](#).

- `/ceipoptin ceipoptin [,ceipoptin]...`

Consente la raccolta di dati Call Home e dati CEIP (Programma di miglioramento dell'esperienza cliente). I valori validi sono:

- **DIAGNOSTIC:** Scegliete questo valore per consentire a Citrix Licensing di raccogliere i dati Call Home.

- **ANONYMOUS**: Scegliete questo valore per consentire a Citrix Licensing di raccogliere dati CEIP non identificati (che non identificano gli utenti).
- **NONE**: Scegliete questo valore per disabilitare la raccolta di dati CEIP di Citrix Licensing.

Per ulteriori informazioni sulla raccolta dei dati Call Home, vedere [Citrix Licensing Call Home](#).

Per maggiori dettagli sulla raccolta dei dati CEIP, vedere [Citrix Licensing Customer Experience Improvement Program](#).

Per maggiori dettagli sui dati CEIP, vedere [Citrix Licensing CEIP data elements](#).

Per maggiori dettagli sui dati sulle licenze di License Server, vedere [Citrix Licensing Data](#).

- **/components** *componente* [,*componente*]...

Elenco separato da virgole di componenti da installare o rimuovere. I valori validi sono:

- **CONTROLLER**: Controller
- **DESKTOPSTUDIO**: Studio
- **WEBSTUDIO**: Studio Web
- **DESKTOPDIRECTOR**: Direttore
- **LICENSESERVER**: Citrix License Server
- **SECUREPRIVATEACCESS**: Accesso privato sicuro

Se questa opzione viene omessa, tutti i componenti vengono installati (o rimossi, se viene specificata anche l'opzione `/remove`).

(Nelle versioni precedenti al 2003, i valori validi includevano **STOREFRONT**. Per la versione 2003 e successive, utilizzare il comando di installazione StoreFront dedicato indicato in Utilizzare il programma di installazione completo del prodotto.

- **/configure_firewall**

Apri tutte le porte del firewall di Windows utilizzate dai componenti installati, se il servizio Windows Firewall è in esecuzione, anche se il firewall non è abilitato. Se si utilizza un firewall di terze parti o non si utilizza un firewall, è necessario aprire manualmente le porte.

- **/disableexperiencemetrics**

Impedisce l'invio automatico a Citrix delle analisi raccolte durante l'installazione, l'aggiornamento o la rimozione.

- **/exclude** «*feature*»\ [,»*feature*«]

Impedisce l'installazione di una o più funzionalità, servizi o tecnologie separate da virgole, ciascuna racchiusa tra virgolette diritte. I valori validi sono:

- «**Local Host Cache Storage (LocalDB)**»: impedisce l'installazione del database utilizzato per Local Host Cache. Questa opzione non ha alcun effetto sul fatto che SQL Server Express sia installato o meno per l'utilizzo come database del sito.

- **/help o /h**

Visualizza la Guida dei comandi.

- **/ignore_hw_check_failure**

Consente di continuare l'installazione o l'aggiornamento del Delivery Controller, anche se i controlli hardware non riescono (ad esempio, a causa di RAM insufficiente). Per ulteriori informazioni, vedere [Hardware check](#).

- **/ignore_sito_test_fallimento**

Valido solo durante l'aggiornamento del controller. In genere, tutti gli errori di test del sito vengono ignorati e l'aggiornamento procede. Se omissa (o impostata su false), qualsiasi errore di test del sito causa il fallimento del programma di installazione, senza eseguire l'aggiornamento. Predefinito = false

Durante un aggiornamento, questa opzione viene ignorata se viene rilevata una versione di SQL Server non supportata. Per i dettagli, vedere [Controllo della versione di SQL Server](#).

- **/installdir directory****

Directory vuota esistente in cui verranno installati i componenti. Predefinito = c:\ Programmi\Citrix.

- **/logpath percorso****

Percorso del file di registro. La cartella specificata deve esistere. Il programma di installazione non la crea. Predefinito = TEMP%\ Citrix\XenDesktop Installer

- **/no_remote_assistance**

Valido solo quando si installa Director. Disattiva la funzionalità di shadowing utente che utilizza Assistenza remota di Windows.

- **/noreboot**

Impedisce un riavvio dopo l'installazione. Per la maggior parte dei componenti principali, il riavvio non è abilitato per impostazione predefinita.

- **/noresume**

Per impostazione predefinita, quando è necessario un riavvio della macchina durante un'installazione, il programma di installazione riprende automaticamente al termine del riavvio. Per sovrascrivere l'impostazione predefinita, specificate [/noresume](#). Ciò può risultare utile se è necessario rimontare il supporto o acquisire informazioni durante un'installazione automatica.

- **/nosql**

Impedisce l'installazione di Microsoft SQL Server Express sul server in cui si sta installando il controller. Se questa opzione viene omissa, SQL Server Express viene installato per l'utilizzo come database del sito.

Questa opzione non influisce sull'installazione di SQL Server Express LocalDB utilizzato per Local Host Cache.

- **/quiet o /passive**

Durante l'installazione non viene visualizzata alcuna interfaccia utente. L'unica prova del processo di installazione è in Task Manager (Gestione attività) di Windows. Se questa opzione viene omessa, viene avviata l'interfaccia grafica.

- **/remove**

Rimuove i componenti principali specificati con l'opzione `/components`.

- **/removeall**

Rimuove tutti i componenti principali installati.

- **/SKIPHDXDRIVERCHECK**

Salta il controllo dei driver HDX nel Meta-installer VDA.

- **/sendexperiencemetrics**

Invia automaticamente a Citrix le analisi raccolte durante l'installazione, l'aggiornamento o la rimozione. Se questa opzione viene omessa (o viene specificato `/disableexperiencemetrics`), le analisi vengono raccolte localmente, ma non inviate automaticamente.

- **/tempdir** *directory*

Directory che contiene i file temporanei durante l'installazione. Predefinito = `c:\Windows\Temp`.

- **/xenapp**

Installa Citrix Virtual Apps. Se questa opzione viene omessa, viene installato Citrix Virtual Apps and Desktops.

Esempi di installazione di componenti principali

Il comando seguente installa un Delivery Controller, Studio, Licensing Citrix e SQL Server Express su un server. Le porte del firewall necessarie per le comunicazioni dei componenti vengono aperte automaticamente.

```
\x64\XenConfigurazione\Desktop\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserfer /configure_firewall
```

Il comando seguente installa un Citrix Virtual Apps Controller, Studio e SQL Server Express sul server. Le porte del firewall necessarie per la comunicazione dei componenti vengono aperte automaticamente.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

Il comando seguente installa un Delivery Controller, Secure Private Access e SQL Server Express su un server. Le porte del firewall necessarie per la comunicazione dei componenti vengono aperte automaticamente.

```
\x64\XenConfigurazione Desktop XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall
```

Utilizzare un programma di installazione VDA autonomo

Per accedere al sito di download, sono necessarie le credenziali dell'account Citrix. È necessario disporre di privilegi amministrativi elevati prima di avviare l'installazione oppure utilizzare **Esegui come amministratore**.

1. Scaricare il pacchetto appropriato da Citrix:
 - Virtual Delivery Agent del sistema operativo multisessione: `VDAServerSetup_xxxx.exe`
 - Virtual Delivery Agent del sistema operativo a sessione singola: `VDAWorkstationSetup_xxxx.exe`
 - Agente di distribuzione virtuale dei servizi di base del sistema operativo a sessione singola: `VDAWorkstationCoreSetup_xxxx.exe`
2. Estrarre prima i file dal pacchetto in una directory esistente e quindi eseguire il comando di installazione o semplicemente eseguire il pacchetto.

Per estrarre i file prima di installarli, utilizzate `/extract` con il percorso assoluto, ad esempio `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAinstallMedia`. La directory deve esistere. In caso contrario, l'estrazione non riesce. Quindi, in un comando separato, eseguire il comando appropriato, utilizzando le opzioni valide elencate in questo articolo.

- Per `VDAServerSetup_XXXX.exe`, esegui `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- Per `VDAWorkstationCoreSetup_XXXX.exe`, esegui `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- Per `VDAWorkstationSetup_XXXX.exe`, esegui `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

Per eseguire il pacchetto scaricato, esegui il suo nome: `VDA ServerSetup.exe`, `VDA WorkstationSetup.exe` o `VDA WorkstationCoreSetup.exe`. Utilizzare le opzioni valide elencate in questo articolo.

Se si ha familiarità con il programma di installazione del prodotto completo:

- Esegui il programma di installazione autonomo `VDA ServerSetup.exe` o `VDA WorkstationSetup.exe` come se fosse il comando `XenDesktopVdaSetup.exe` in tutto tranne il nome.
- Il programma di installazione `VDA WorkstationCoreSetup.exe` è diverso, perché supporta un sottoinsieme delle opzioni disponibili per gli altri programmi di installazione.

Opzioni della riga di comando per l'installazione di un VDA

Le seguenti opzioni sono valide con uno o più dei seguenti comandi (programmi di installazione): `VDA ServerSetup_xxxx.exe`, `VDA WorkstationSetup_xxxx.exe` o `VDA WorkstationCoreSetup_xxxx.exe`.

Per maggiori dettagli sulle opzioni, vedere [Install VDA](#).

- **/components** *componente* \ [,componente]

Elenco separato da virgole di componenti da installare o rimuovere. I valori validi sono:

- **VDA**: Virtual Delivery Agent
- **PLUGINS**: app Citrix Workspace per Windows

Per installare l'app VDA e Citrix Workspace per Windows, specificate `/components vda, plugins` o non specificate alcun componente. Se non viene specificato alcun componente, per impostazione predefinita verrà installato solo il VDA.

Per installare solo il VDA ed escludere l'installazione dell'app Citrix Workspace, specificare `/components vda`.

Questa opzione non è valida quando si utilizza il programma di installazione `VDA WorkstationCoreSetup.exe`. Tale programma di installazione non può installare l'app Citrix Workspace.

- **/controllers** “*controller* \ [*controller*]»

FQDN separati da spazi dei controller con cui il VDA può comunicare, racchiusi tra virgolette diritte. Non specificate entrambe le opzioni `/site_guid` e `/controllers`.

- **/disableexperiencemetrics**

Impedisce l'invio automatico a Citrix delle analisi raccolte durante l'installazione, l'aggiornamento o la rimozione.

- **/abilita_hdx_porte**

Apri le porte del firewall di Windows richieste dal VDA e dalle funzionalità abilitate (ad eccezione di Assistenza remota di Windows), se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall. Per informazioni sulle porte, vedere [Porte di rete](#).

Per aprire le porte UDP utilizzate dal trasporto adattivo HDX, specificate l'opzione `/enable_hdx_udp_ports`, oltre a questa opzione `/enable_hdx_ports`.

- **/abilita_hdx_udp_porte**

Apri le porte UDP del firewall di Windows utilizzate dal trasporto adattivo HDX, se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall. Per informazioni sulle porte, vedere [Porte di rete](#).

Per aprire porte aggiuntive utilizzate dal VDA, specificate l'opzione `/enable_hdx_ports`, oltre a questa opzione `/enable_hdx_udp_ports`.

- **/abilitare_hdx_tls_dtls**

Apri la porta TCP e UDP 443 per HDX Direct V1.

- **/enable_real_time_transport**

Abilita o disabilita l'uso di UDP per i pacchetti audio (RealTime Audio Transport for audio). L'attivazione di questa funzione può migliorare le prestazioni audio. Includi l'opzione `/enable_hdx_ports` se desideri che le porte UDP si aprano automaticamente quando viene rilevato il servizio Windows Firewall.

- **/enable_remote_assistance**

Attiva la funzionalità di shadowing in Assistenza remota di Windows per l'utilizzo con Director. Se si specifica questa opzione, Assistenza remota di Windows apre le porte dinamiche del firewall.

- **/enablerestore o /enablerestorecleanup**

(valido solo per VDA a sessione singola) Abilita il ritorno automatico al punto di ripristino, se l'installazione o l'aggiornamento del VDA non vanno a buon fine.

Se l'installazione/aggiornamento viene completato correttamente:

- `/enablerestorecleanup` indica all'installatore di rimuovere il punto di ripristino.
- `/enablerestore` indica all'installatore di conservare il punto di ripristino, anche se non è stato utilizzato.

Per i dettagli, vedi [Ripristino in caso di errore di installazione o aggiornamento](#).

- **/abilita_ss_porte**

Apri le porte del firewall Windows necessarie per la condivisione dello schermo, se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall.

- **/exclude** “component«\[,»component«]

Impedisce l’installazione di uno o più componenti opzionali separati da virgolette, ciascuno racchiuso tra virgolette diritte. Ad esempio, l’installazione o l’aggiornamento di un VDA su un’immagine non gestita da MCS non richiede il componente Machine Identity Service. I valori validi sono i seguenti:

Sistema operativo multisessione	Sistema operativo a sessione singola	Core Services per sistema operativo a sessione singola
Componente di protezione delle app Citrix	Componente di protezione delle app Citrix	Componente di protezione delle app Citrix
Plug-in VDA di asserzione di identità di autenticazione Citrix	Plug-in VDA di asserzione di identità di autenticazione Citrix	Plug-in VDA di asserzione di identità di autenticazione Citrix
Citrix Backup and Restore	Citrix Backup and Restore	
Reindirizzamento dei contenuti del browser Citrix	Reindirizzamento dei contenuti del browser Citrix	Reindirizzamento dei contenuti del browser Citrix
Driver del filtro Citrix HyperV	Driver del filtro Citrix HyperV	
Citrix MCS IODriver	Citrix MCS IODriver	
Personalizzazione Citrix per App-V - VDA	Personalizzazione Citrix per App-V - VDA	Personalizzazione Citrix per App-V - VDA
Citrix Profile Management	Citrix Profile Management	
Plug-in WMI Citrix Profile Management	Plug-in WMI Citrix Profile Management	
Citrix Rendezvous V2	Citrix Rendezvous V2	

Sistema operativo multisessione	Sistema operativo a sessione singola	Core Services per sistema operativo a sessione singola
Servizio di telemetria Citrix	Servizio di telemetria Citrix	Servizio di telemetria Citrix
Citrix Universal Print Client	Citrix Universal Print Client	Citrix Universal Print Client
Servizio di acquisizione dei registri Citrix VDA	Servizio di acquisizione dei registri Citrix VDA	Servizio di acquisizione dei registri Citrix VDA
Agente di aggiornamento Citrix VDA	Agente di aggiornamento Citrix VDA	
Componente CSE	Componente CSE	Componente CSE
Direttore VDA Plug-in	Direttore VDA Plug-in	Direttore VDA Plug-in
Machine Identity Service	Machine Identity Service	
Fornitore di gestione delle macchine	Fornitore di gestione delle macchine	Fornitore di gestione delle macchine
	Livello di personalizzazione utente	
Plug-in del monitor VDA	Plug-in del monitor VDA	Plug-in del monitor VDA
Plug-in proxy VDA WMI	Plug-in proxy VDA WMI	Plug-in proxy VDA WMI

L'esclusione di Citrix Profile Management dall'installazione (`/exclude «Citrix Profile Management»`) influisce sul monitoraggio e sulla risoluzione dei problemi dei VDA con Citrix Director. Nelle pagine **User details** (Dettagli utente) ed **EndPoint**, i pannelli Personalization e Logon Duration riportano errori. Nelle pagine **Dashboard** e **Trends**, il pannello Average Logon Duration visualizza i dati solo per i computer in cui è installato Profile Management.

Anche se si utilizza una soluzione di gestione dei profili utente di terze parti, Citrix consiglia di installare ed eseguire Citrix Profile Management Service. L'attivazione del servizio Citrix Profile Management non è necessaria.

Se si specificano sia `/exclude` che `/includeadditional` con lo stesso nome di compo-

nente, tale componente non viene installato.

Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Tale programma di installazione esclude automaticamente molti di questi elementi.

- **`/h o /help`**

Visualizza la Guida dei comandi.

- **`/includeadditional`** “*componente*” [,»*componente*»]

Include l'installazione di uno o più componenti opzionali separati da virgole, ciascuno racchiuso tra virgolette diritte. Questa opzione può risultare utile quando si crea una distribuzione di Accesso remoto PC e si desidera installare altri componenti non inclusi per impostazione predefinita. I valori validi sono i seguenti:

Sistema operativo multisessione	Sistema operativo a sessione singola
Citrix Backup and Restore	Citrix Backup and Restore
Citrix MCS IODriver	Citrix MCS IODriver
Personalizzazione Citrix per App-V - VDA	Personalizzazione Citrix per App-V - VDA
Citrix Profile Management	Citrix Profile Management
Plug-in WMI Citrix Profile Management	Plug-in WMI Citrix Profile Management
Citrix Rendezvous V2	Citrix Rendezvous V2
Agente di aggiornamento Citrix VDA	Agente di aggiornamento Citrix VDA
Strumento di registrazione Citrix Web Socket VDA	Strumento di registrazione Citrix Web Socket VDA
Machine Identity Service	Machine Identity Service
	Livello di personalizzazione utente

Se si specificano sia `/exclude` che `/includeadditional` con lo stesso nome di componente, tale componente non viene installato.

- **`/installdir`** *directory*

Directory vuota esistente in cui verranno installati i componenti. Predefinito = `c:\Programmi\Citrix`.

- **/install_mcsio_driver**

Non utilizzare. Utilizzate invece `/includeadditional «Citrix MCS IODriver»` o `/exclude «Citrix MCS IODriver»`

- **/logpath** *percorso*

Percorso del file di registro. La cartella specificata deve esistere. Il programma di installazione non la crea. Predefinito = “%TEMP%\ Citrix\XenDesktop Installer»

Questa opzione non è disponibile nell’interfaccia grafica.

- **/masterimage**

Valido solo quando si installa un VDA in una macchina virtuale. Imposta il VDA come immagine da utilizzare per creare altre macchine. Questa opzione è equivalente a `/mastermcsimage`.

Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`.

- **/mastermcsimage**

Specifica che questa macchina verrà utilizzata come immagine con Machine Creation Services. Questa opzione è equivalente a `/masterimage`.

- **/masterpvsimage**

Specifica che il computer verrà utilizzato come immagine con Citrix Provisioning o uno strumento di provisioning di terze parti (ad esempio Microsoft System Center Configuration Manager) per eseguire il provisioning delle macchine virtuali.

- **/websockettoken** *WebSocketToken*

Crea un Web Socket VDA. Il WebSocketToken è per il token richiesto.

- **/no_mediafoundation_ack**

Riconosce che Microsoft Media Foundation non è installato e diverse funzionalità multimediali HDX non verranno installate e non funzioneranno. Se questa opzione viene omessa e Media Foundation non è installato, l’installazione del VDA viene terminata poiché i prerequisiti non sono soddisfatti. La maggior parte delle edizioni di Windows supportate ha Media Foundation già installato, ad eccezione delle edizioni N. Se si abilita Windows Features > Media Features *manualmente*, la chiave di registro richiesta da Citrix Meta Installer potrebbe non avere un valore impostato. Controllare la chiave di registro `SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Setup\ Windows-Features\ WindowsMediaVersion` prima di avviare il processo di installazione per confermare che il valore esiste e non è vuoto.

- **/nodesktopexperience**

La funzionalità Enhanced desktop experience non è più disponibile. Questa opzione (e l’impostazione dei criteri) viene ignorata, se specificato.

Valida solo quando si installa un VDA per un sistema operativo multisessione. Impedisce l'attivazione della funzionalità Enhanced desktop experience. Questa funzione è inoltre controllata con l'impostazione dei criteri Enhanced Desktop Experience Citrix.

- **/noreboot**

Impedisce un riavvio dopo l'installazione. Il VDA non può essere utilizzato fino a dopo un riavvio.

- **/noresume**

Per impostazione predefinita, quando è necessario un riavvio della macchina durante un'installazione, il programma di installazione riprende automaticamente al termine del riavvio. Per sovrascrivere l'impostazione predefinita, specificate **/noresume**. Ciò può risultare utile se è necessario rimontare il supporto o acquisire informazioni durante un'installazione automatica.

- **/physicalmachine**

Usa questo argomento insieme a **/remotepc** per l'installazione di RemotePC. In caso contrario, il VDA potrebbe non comportarsi come previsto in alcuni scenari utente.

- **/portnumber** *porta*

Valido solo quando è specificata l'opzione **/reconfig**. Numero di porta da abilitare per le comunicazioni tra il VDA e il Controller. La porta configurata in precedenza è disabilitata, a meno che non sia la porta 80.

- **/proxyconfig** *“indirizzo o percorso del file PAC”*

Se prevedi di utilizzare il protocollo Rendezvous con Gateway Service, VDA Upgrade Service, ecc. nel tuo ambiente e hai un proxy non trasparente nella tua rete per le connessioni in uscita, specifica il proxy qui. Sono supportati solo i proxy HTTP. L'indirizzo o il percorso del file PAC del proxy da utilizzare con il protocollo Rendezvous. Per dettagli delle funzionalità, vedere [Protocollo Rendezvous](#).

- Formato dell'indirizzo proxy: `http://<url-or-ip>:<port>`
- Formato file PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** o **/passive**

Durante l'installazione non viene visualizzata alcuna interfaccia utente. L'unica prova del processo di installazione e configurazione è in Task Manager di Windows. Se questa opzione viene omessa, viene avviata l'interfaccia grafica.

- **/reconfigure**

Personalizza le impostazioni VDA configurate in precedenza se utilizzate con le opzioni **/portnumber**, **/controllerso** **/enable_hdx_ports**. Se si specifica questa opzione senza specificare anche l'opzione **/quiet**, viene avviata l'interfaccia grafica per la personalizzazione del VDA.

- **/remotepc**

Valido solo per le distribuzioni di Accesso remoto PC (sistema operativo a sessione singola) o per le connessioni mediate (sistema operativo multisessione). Esclude l'installazione di qualsiasi componente aggiuntivo (vedere gli elenchi dei componenti con le opzioni `/exclude` e `/includeadditional`).

Questa opzione non è valida quando si utilizza il programma di installazione `VDAWorkstationCoreSetup.exe`. Tale programma di installazione esclude automaticamente l'installazione di questi componenti.

`/remotepc` non è compatibile con l'opzione `/servervdi`.

- **/remove**

Rimuove i componenti specificati con l'opzione `/components`.

- **/remove_appdisk_ack**

Autorizza il programma di installazione del VDA a disinstallare il plug-in VDA AppDisks, se è installato.

- **/remove_pvd_ack**

Autorizza il programma di installazione VDA a disinstallare Personal vDisk se è installato.

- **/removeall**

Rimuove il VDA. Non rimuove l'app Citrix Workspace (se installata).

- **/RIMUOVI TUTTO CON CWA**

Rimuove il CWA insieme al VDA.

- **/sendexperiencemetrics**

Invia automaticamente a Citrix le analisi raccolte durante l'installazione, l'aggiornamento o la rimozione. Se questa opzione viene omessa (o viene specificata l'opzione `/disableexperiencemetrics`), le analisi vengono raccolte localmente, ma non inviate automaticamente.

- **/servervdi**

Installa un VDA per sistema operativo a sessione singola in un computer multisessione Windows supportato. Omettere questa opzione quando si installa un VDA per sistema operativo multisessione su un computer multisessione Windows.

Prima di utilizzare questa opzione, vedere [Server VDI](#).

Utilizzare questa opzione solo con il programma di installazione del VDA completo.

- **/sito_guid guid**

Identificatore univoco globale (GUID) dell'unità organizzativa (OU) di Active Directory del sito. Questo associa un desktop virtuale a un sito quando si utilizza Active Directory per l'individuazione (l'aggiornamento automatico è il metodo di individuazione consigliato e predefinito). Il GUID del sito è una proprietà del sito visualizzata in Studio. Non specificate entrambe le opzioni `/site_guide` e `/controllers`.

- **`/tempdir`** *directory*

Directory in cui contenere i file temporanei durante l'installazione. Predefinito = c:\Windows\Temp.

Questa opzione non è disponibile nell'interfaccia grafica.

- **`/virtualmachine`**

Valido solo quando si installa un VDA in una macchina virtuale. Sovrascrive l'individuazione da parte del programma di installazione di una macchina fisica, in cui le informazioni del BIOS passate alle macchine virtuali le fanno apparire come macchine fisiche.

Questa opzione non è disponibile nell'interfaccia grafica.

- **`/xendesktopcloud`**

Indica che il VDA è installato in una distribuzione di Citrix DaaS (Citrix Cloud).

Esempi di installazione di un VDA

Installare un VDA con il programma di installazione del prodotto completo:

Il comando seguente installa un VDA per sistema operativo a sessione singola e l'app Citrix Workspace nella posizione predefinita in una macchina virtuale. Questo VDA verrà utilizzato come immagine e utilizzerà MCS per eseguire il provisioning delle macchine virtuali. Il VDA si registrerà inizialmente presso il Controller sul server denominato `Contr-Main` nel dominio `mydomain`. Il VDA utilizzerà il livello di personalizzazione utente e Assistenza remota di Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,  
plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /  
includeadditional "livello di personalizzazione utente"/mastermcsimage  
/enable_remote_assistance
```

Installare un VDA con sistema operativo a sessione singola con il programma di installazione autonomo di VDAWorkstationCoreSetup:

Il comando seguente installa un VDA di Core Services in un sistema operativo a sessione singola per l'utilizzo in una distribuzione VDI o Accesso remoto PC. L'app Citrix Workspace e altri servizi non core non vengono installati. Viene specificato l'indirizzo di un controller e le porte del servizio Windows Firewall verranno aperte automaticamente. L'amministratore gestirà i riavvii.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com"/enable_hdx_ports /noreboot
```

Personalizzare un VDA

Dopo aver installato un VDA, è possibile personalizzare diverse impostazioni. Dalla directory `\x64\XenDesktop_Setup` sul supporto del prodotto, eseguire `XenDesktopVdaSetup.exe`, utilizzando una o più delle seguenti opzioni, descritte in Opzioni della riga di comando per l'installazione di un VDA.

- `/reconfigure` (richiesto per la personalizzazione di un VDA)
- `/h o /help`
- `/Tranquillo`
- `/noreboot`
- `/controllori`
- `/portnumber porta`
- `/enable_hdx_ports`

Risoluzione dei problemi relativi ai VDA

- Nella visualizzazione Studio per un gruppo di consegna, la voce **Installed VDA version** (Versione VDA installata) nel riquadro **Details** potrebbe non essere la versione installata nei computer. La visualizzazione Programmi e funzionalità di Windows della macchina mostra la versione VDA effettiva.
- Dopo l'installazione di un VDA, non è possibile distribuire app o un desktop agli utenti fino a quando non si registra con un Delivery Controller.

Per informazioni sui metodi di registrazione VDA e su come risolvere i problemi di registrazione, vedere [Registrazione VDA](#).

Opzioni della riga di comando per l'installazione di un Universal Print Server

L'opzione seguente è valida con il comando `XenDesktopPrintServerSetup.exe`.

- **`/enable_upsserver_port`**

Quando questa opzione non è specificata, il programma di installazione visualizza la pagina **Firewall** dell'interfaccia grafica. Selezionare **Automatically** perché il programma di installazione aggiunga automaticamente le regole firewall di Windows o **Manually** per consentire all'amministratore di configurare manualmente il firewall.

Dopo aver installato il software sui server di stampa, configurate Universal Print Server utilizzando le indicazioni contenute in [Provision printers](#).

Opzioni della riga di comando per l'installazione di un accesso privato sicuro

Le seguenti opzioni sono valide con:

1. Programma di installazione CVAD: [XenDesktopSPASetup.exe](#)
2. Programma di installazione locale SPA: [SecurePrivateAccessSetup_XXXX.exe](#)

- **/abilitare_porte_spa**

Apri le porte nel firewall di Windows richiesto dal Secure Private Access, se viene rilevato il servizio Windows Firewall, anche se il firewall non è abilitato. Se si utilizza un firewall diverso o nessun firewall, è necessario configurare manualmente il firewall. Per informazioni sulle porte, vedere [Porte di rete](#).

- **/nosql**

Impedisce l'installazione di Microsoft SQL Server Express sul server in cui si sta installando Secure Private Access. Se questa opzione viene omessa, SQL Server Express viene installato per l'utilizzo come database del sito.

- **/help o /h o/?**

Visualizza la Guida dei comandi

- **/noreboot**

Impedisce un riavvio dopo l'installazione. L'accesso privato sicuro può essere utilizzato solo dopo il riavvio.

- **/quiet o /passive**

Durante l'installazione non viene visualizzata alcuna interfaccia utente. L'unica prova del processo di installazione e configurazione è in Task Manager di Windows. Se questa opzione viene omessa, viene avviata l'interfaccia grafica.

- **/remove**

Rimuove l'accesso privato sicuro.

Per maggiori dettagli sulle opzioni, consulta il programma di installazione [Secure Private Access](#).

Ulteriori informazioni

Per informazioni su come Citrix riporta il risultato delle installazioni dei componenti, vedere [Citrix installation return codes](#).

Installa Web Studio

January 24, 2025

Introduzione

Citrix Studio è una console di gestione basata su Windows che consente di configurare e gestire la distribuzione di Citrix Virtual Apps and Desktops. Web Studio è la nuova generazione di Citrix Studio: una console di gestione basata sul Web che offre tutte le stesse funzionalità di Citrix Studio. Con lo stesso aspetto grafico dell'interfaccia di [Citrix DaaS Studio](#), Web Studio modernizza la vostra esperienza di gestione fornendo un'esperienza web nativa.

È possibile distribuire Web Studio su qualsiasi server Windows su cui sia installato Internet Information Service (IIS). Esistono due opzioni di distribuzione:

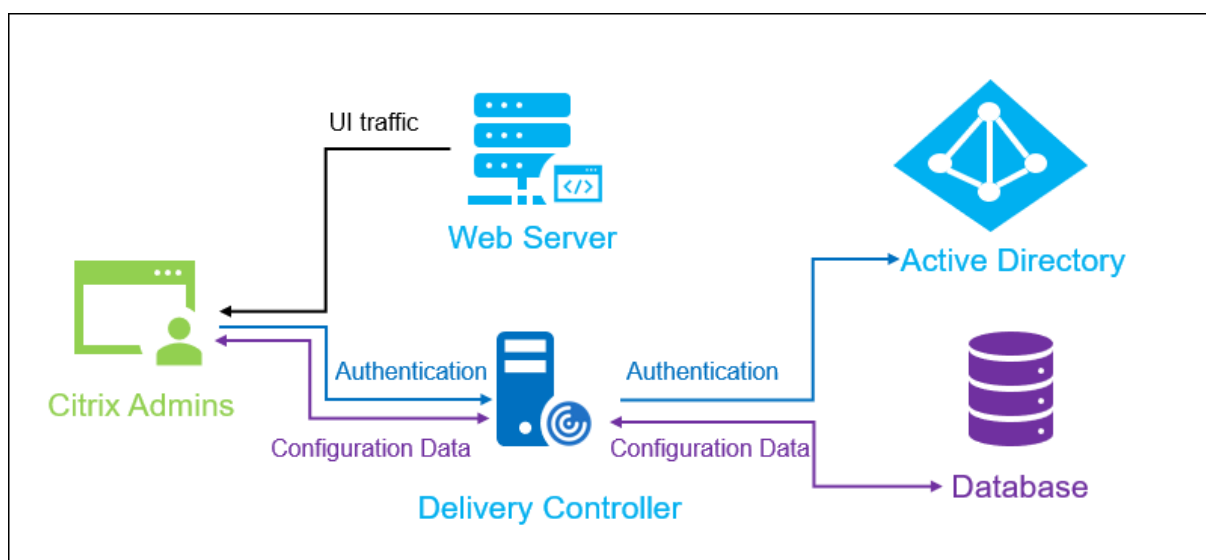
- Installato su un server dedicato:

Per ambienti più grandi in cui prestazioni e scalabilità sono essenziali, consigliamo di installare Web Studio su un server dedicato. Facoltativamente, questo server può ospitare anche il Director.

- Integrato con un Delivery Controller:

Per distribuzioni rapide e ambienti più semplici, installa Web Studio direttamente su un Delivery Controller. Questo approccio è ideale per distribuzioni di piccole dimensioni in cui è prioritario ridurre al minimo i costi amministrativi.

Il diagramma seguente mostra l'architettura di Web Studio:



Un flusso di lavoro generale per avviare e far funzionare Web Studio è il seguente:

1. Installa Web Studio.
2. Imposta un sito.
3. Aggiungi Delivery Controller a Web Studio per la gestione.
4. Accedi a Web Studio.

Per impostare una distribuzione di Web Studio con bilanciamento del carico, vedere [questo articolo](#).

Nuove funzionalità disponibili in Web Studio

Consulta l'articolo [Novità](#).

Requisiti di sistema

Sistemi operativi supportati:

- Versione di 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 (versione con supporto esteso) 90
- Versione 92 di Google Chrome
- 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 Citrix Virtual Apps and Desktops 2212 e successive.

Per le distribuzioni precedenti alla versione 2212, eseguire prima l'aggiornamento alla versione 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 una policy da un modello in Web Studio e quindi creare un modello da questa policy in Citrix Studio e viceversa.

- Per garantire un'installazione corretta di Web Studio, non modificare il nome del sito predefinito (**Sito Web predefinito**) in Gestione Internet Information Services (IIS). Qualsiasi modifica al nome predefinito del sito causerà errori di installazione.

Installa Web Studio

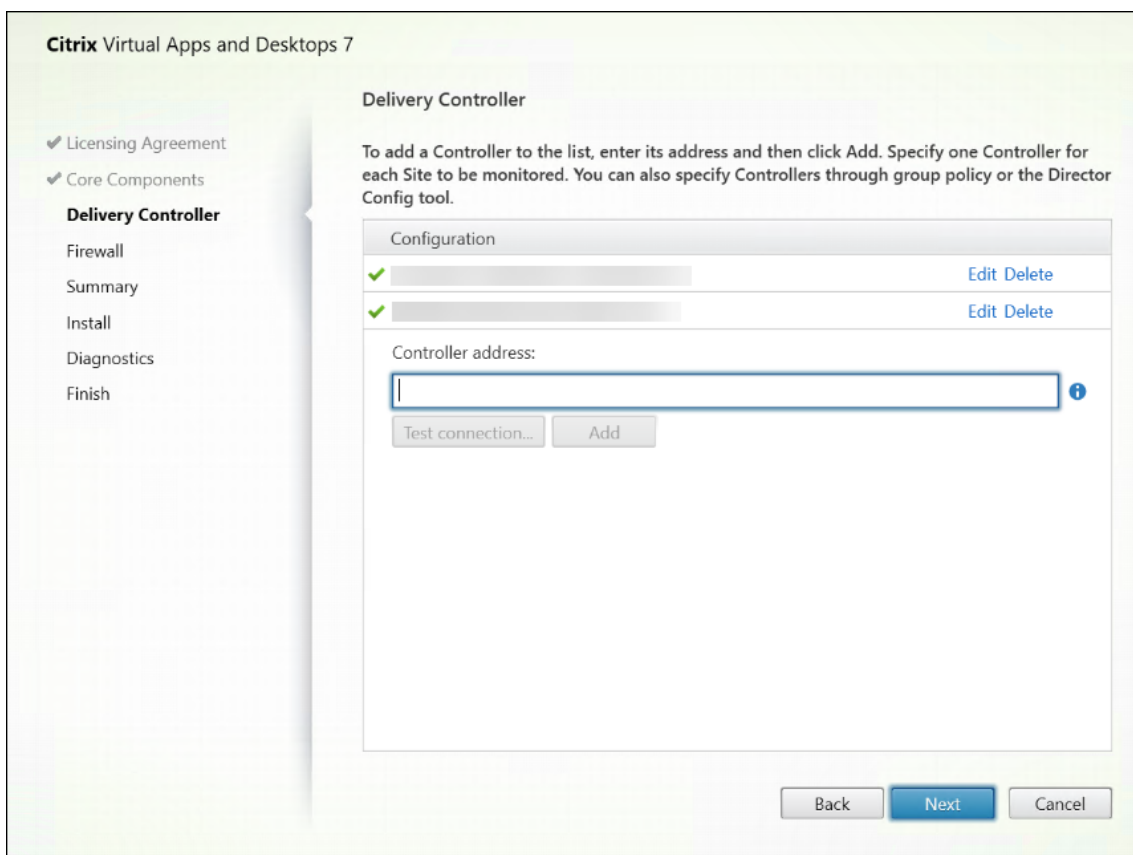
Le seguenti informazioni sono un'integrazione alla guida in [Installa i componenti principali](#). Per installare Web Studio:

- Installa Web Studio utilizzando il programma di installazione ISO completo del prodotto per Citrix Virtual Apps and Desktops. Il programma di installazione ISO verifica i prerequisiti, installa eventuali componenti mancanti, configura il sito Web di Web Studio (sul Delivery Controller se incluso nell'installazione di 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.
- Durante l'installazione di Web Studio, ti verrà chiesto di digitare l'indirizzo di un Delivery Controller.

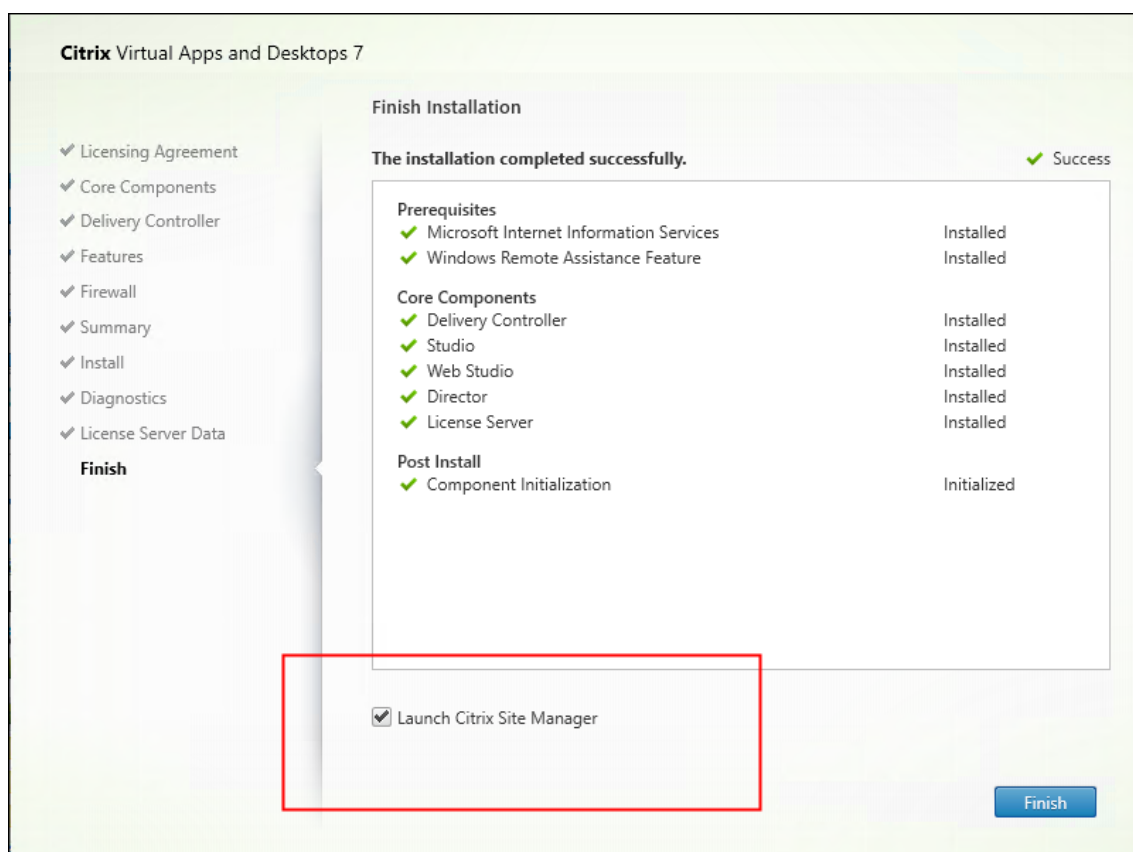
Nota:

- È possibile aggiungere più di un Delivery Controller. Web Studio tenta di connettersi a loro 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 **Componenti principali** e installato, i Delivery Controller aggiunti qui verranno utilizzati sia per Web Studio sia per Director.
- Se non hai configurato il certificato di attendibilità pubblica esterna e non vuoi richiederlo a una CA aziendale, devi solo configurare l'FQDN del tuo Delivery Controller.
- Se disponi del certificato di attendibilità pubblica esterno e puoi configurare il DNS pubblico per il tuo Delivery Controller, puoi digitare il nome DNS come indirizzo del Delivery Controller.
- Se puoi richiedere il certificato alla CA aziendale e puoi specificare il tuo DNS person-

ale, puoi aggiungere il tuo 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, è necessario abilitare la crittografia TLS sul sito Web IIS che ospita Web Studio e sul Delivery Controller. Se non è configurato alcun certificato TLS per Delivery Controller, il programma di installazione crea un certificato autofirmato, con l'FQDN di 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 **Termina**, la casella di controllo **Avvia Site Manager** è selezionata per impostazione predefinita, in modo che Citrix Site Manager si apra automaticamente. Per avviarlo in un secondo momento, apri il menu Start del desktop e seleziona **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 [Configura un sito](#).

**Nota:**

È possibile installare Web Studio anche tramite la riga di comando. Esempio: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. Per ulteriori informazioni, vedere [Installazione tramite riga di comando](#).

Imposta un sito

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

Per creare un sito, segui questi passaggi:

1. Su un Delivery Controller, aprire il menu Start del desktop, quindi selezionare **Citrix > Citrix Site Manager**.
2. In Citrix Site Manager, seleziona **Crea un sito**. Viene visualizzata la procedura guidata Configurazione sito.
3. Crea un sito e configurane le impostazioni come segue:

- Nella pagina **Introduzione** , digita un nome per il sito.
 - La pagina **Database** contiene selezioni per l'impostazione del sito, il monitoraggio e i database di registrazione della configurazione. Per ulteriori informazioni, vedere [Passaggio 3. Anche dati](#).
 - Nella pagina **Licenze** , specificare l'indirizzo del server licenze e quindi indicare quale licenza utilizzare (installare). Per ulteriori informazioni, vedere [Passaggio 4. Licenza](#).
4. Nella pagina **Riepilogo** , controlla tutte le impostazioni e clicca su **Invia**.

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

Nota:

L'utente che crea un sito ne diventa amministratore a pieno titolo. 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. Esegui Citrix Site Manager su questo nuovo controller.
2. Seleziona **Unisciti a un sito esistente**.
3. Digitare l'indirizzo di un Controller già aggiunto al sito.
4. Fai clic su **Invia**.

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 viene installato nella seguente cartella predefinita.

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

Supponiamo di voler configurare i due Delivery Controller seguenti per il sito che vuoi 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 di amministratore del computer.
- Le modifiche alla configurazione del Delivery Controller potrebbero non avere effetto immediato a causa delle impostazioni della cache sul server IIS. Per un effetto immediato, vai al server Web Studio, apri Gestione Internet Information Services (IIS), vai a Pagina iniziale

- > Siti > Sito Web predefinito e seleziona **Riavvia** nel riquadro Gestisci sito Web.
- Per visualizzare tutti i parametri supportati, eseguire `StudioConfig.exe --help`.

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

Per impostazione predefinita, quando si gestisce la distribuzione tramite la console di Web Studio, ci si connette sia al server di Web Studio sia ai Delivery Controller tramite il browser Web. Ti offriamo la possibilità di configurare il server Web Studio come proxy per i Delivery Controller. Di conseguenza, quando gestisci la distribuzione ti connetti solo al server Web Studio.

Questa sezione illustra come configurare un server Web Studio come proxy per i Delivery Controller. Supponiamo che Web Studio e Delivery Controller siano installati su server diversi.

Prima di iniziare, verifica di aver installato tutti i componenti principali necessari nella tua distribuzione. Per ulteriori informazioni, vedere [Installa i componenti principali](#).

Per abilitare la modalità proxy per Web Studio, segui questi passaggi:

1. Sul server Web Studio, eseguire Windows PowerShell come amministratore.
2. Esegui il seguente comando sostituendo `fqdn_of_webstudio_machine` con il nome di dominio completo (FQDN) del tuo 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 Web Studio con bilanciamento del carico, sostituire `fqdn_of_webstudio_machine` con l'FQDN del server di bilanciamento del carico (noto anche come server virtuale). Per ulteriori informazioni, vedere [Impostare una distribuzione Web Studio con bilanciamento del carico](#).

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

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

Nota:

Come buona pratica, ti consigliamo di proteggere la distribuzione di Web Studio utilizzando un certificato di attendibilità pubblica esterno o un certificato rilasciato da un'autorità di certificazione (CA) aziendale. Per ulteriori informazioni, vedere [Proteggere una distribuzione di Web Studio](#).

Accedi a Web Studio

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

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

- Se non hai ancora specificato i Delivery Controller per il sito. Ti verrà richiesto di specificare un Delivery Controller per ottenere l'accesso temporaneo a Web Studio.
- Se i Delivery Controller specificati non sono al momento raggiungibili, non è possibile accedere a Web Studio. Testare le connessioni per accertarsi che i Delivery Controller siano raggiungibili. Oppure specifica un Delivery Controller alternativo in modo da ottenere l'accesso temporaneo a Web Studio.

Prossimi passi

1. [Installare VDA](#)
2. Utilizza Web Studio per distribuire app e desktop virtuali ai tuoi utenti:
 - a) [Creazione di un catalogo macchine](#)
 - b) [Creazione di un gruppo di consegna](#)
 - c) [Creazione di un gruppo di applicazioni \(facoltativo\)](#)

Installare i VDA

November 5, 2024

Importante:

- Se stai eseguendo l'aggiornamento e nella versione corrente è installato il software Personal vDisk o AppDisks, vedi [Rimozione di PvD, AppDisks e host non supportati](#).
- 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.

Esistono due tipi di VDA per computer Windows: VDA per sistema operativo multisessione e VDA per sistema operativo a sessione singola (Per informazioni sui VDA per macchine Linux, consulta la documentazione [di Linux Virtual Delivery Agent](#)).

Prima di iniziare un'installazione, rivedi [Prepare to install](#) e completa tutte le attività di preparazione.

Prima di installare i VDA, installare i componenti principali. È inoltre possibile creare il sito prima di installare i VDA.

In questo articolo viene descritta la sequenza di installazione guidata di un VDA. Vengono forniti equivalenti della riga di comando. Per ulteriori informazioni, vedere [Installare utilizzando la riga di comando](#).

Passaggio 1 Scaricare il software del prodotto e avviare la procedura guidata

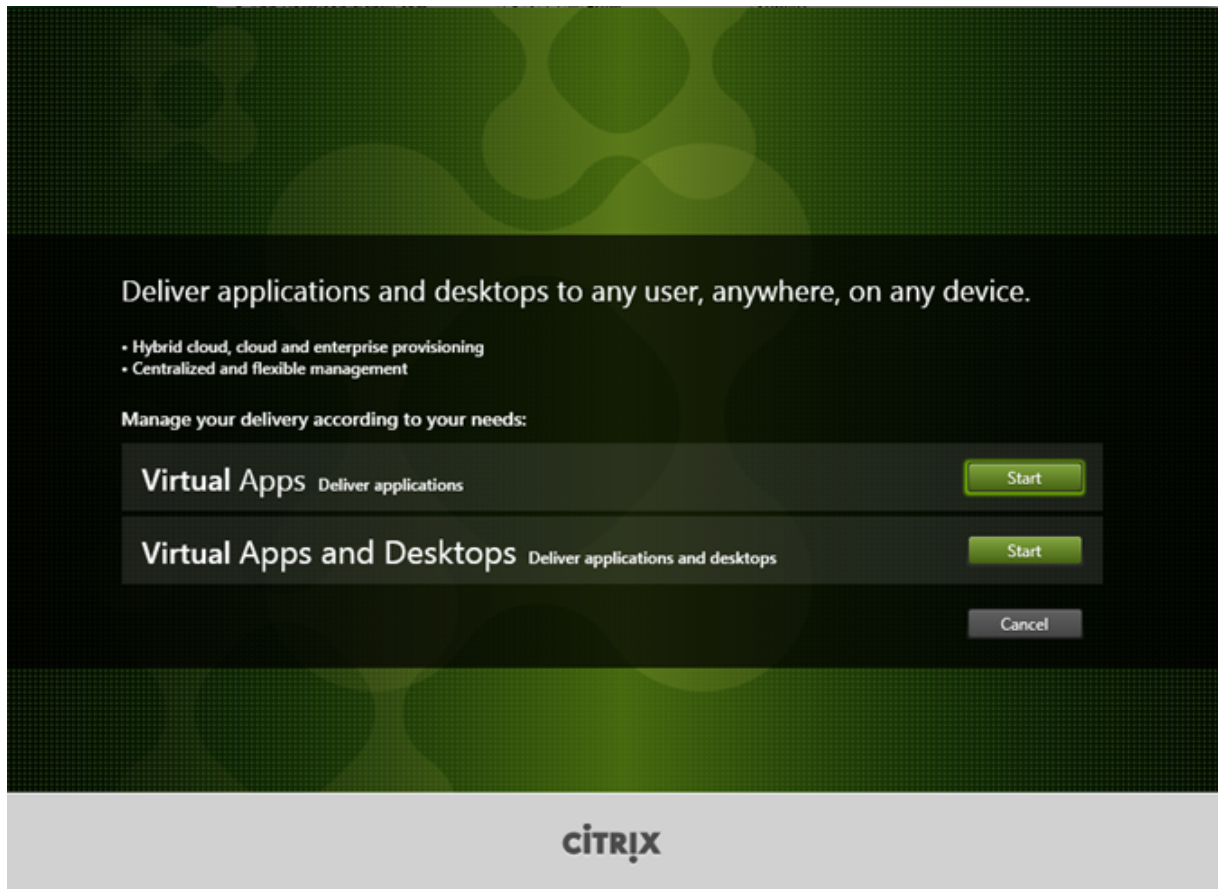
Se si utilizza il programma di installazione del prodotto completo:

1. Se non si è ancora scaricato l'ISO del prodotto:
 - Utilizzare le credenziali dell'account Citrix per accedere alla pagina di download di Citrix Virtual Apps and Desktops. Scaricare il file ISO del prodotto.
 - Decomprimere il file. Facoltativamente, masterizzare un DVD con il file ISO.
2. Utilizzare un account amministratore locale sull'immagine o sul computer in cui si sta installando il VDA. Inserire il DVD nell'unità o montare il file ISO. Se il programma di installazione non si avvia automaticamente, fate doppio clic sull'applicazione **AutoSelect** sull'unità montata.
Viene avviata l'installazione guidata.

Se si utilizza un pacchetto autonomo:

1. Utilizzare le credenziali dell'account Citrix per accedere alla pagina di download di Citrix Virtual Apps and Desktops. Scaricare il pacchetto appropriato:
 - `VDAServerSetup_2402.exe`: sistema operativo multisessione VDA *versione*
 - `VDAWorkstationSetup_2402.exe`: sistema operativo a sessione singola VDA *versione*
 - `VDAWorkstationCoreSetup_2402.exe`: OS Core Services a sessione singola VDA *versione*
2. Fare clic con il pulsante destro del mouse sul pacchetto e scegliere **Esegui come amministratore**.
Viene avviata l'installazione guidata.

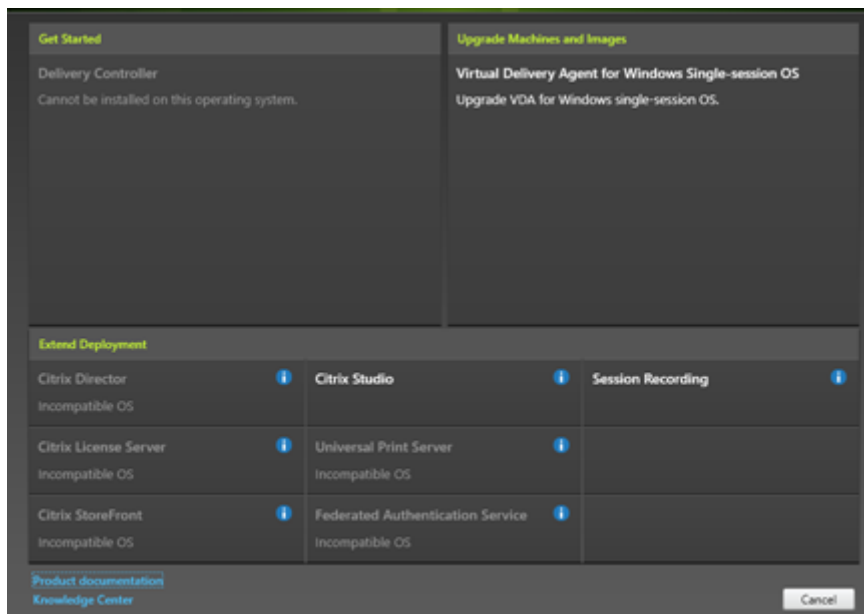
Passaggio 2. Scegliere il prodotto da installare



Fare clic su **Start** accanto al prodotto da installare: Citrix Virtual Apps o Citrix Virtual Desktops. Se nel computer è già installato un componente di Citrix Virtual Apps o Citrix Virtual Desktops, questa pagina non viene visualizzata.

Opzione della riga di comando: `/xenapp` per installare Citrix Virtual Apps. Viene installato Citrix Virtual Desktops se questa opzione viene omessa.

Passaggio 3 Selezionare il VDA

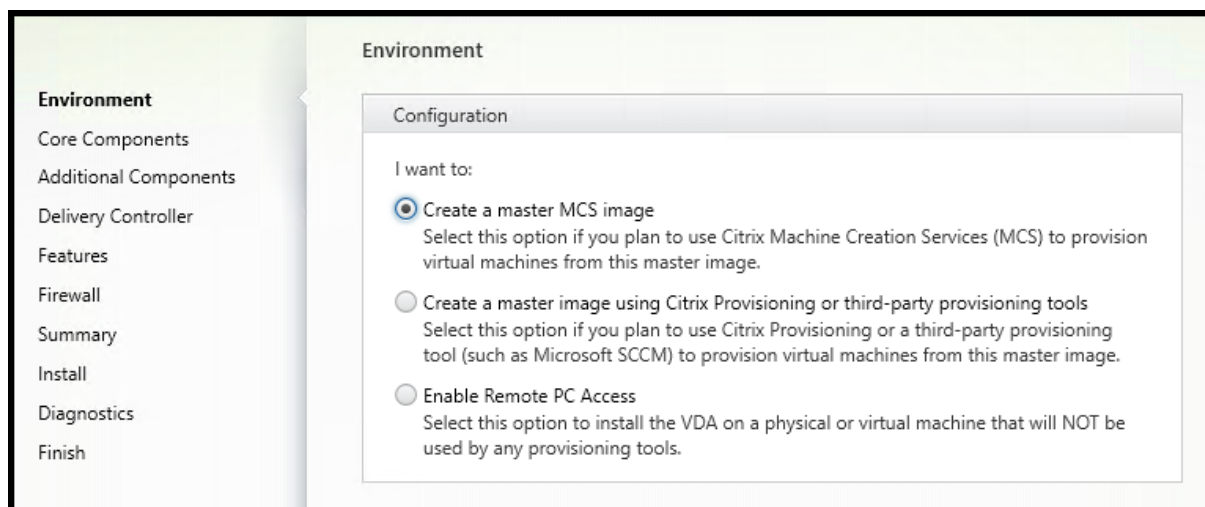


Selezionare la voce **Virtual Delivery Agent**. Il programma di installazione rileva se è in esecuzione su un sistema operativo a sessione singola o multisezione, quindi offre solo il tipo di VDA appropriato.

Ad esempio, quando si esegue il programma di installazione su un computer Windows Server 2019, è disponibile l'opzione di VDA per sistema operativo multisezione. L'opzione VDA per sistema operativo a sessione singola non è disponibile.

Se si tenta di installare (o eseguire l'aggiornamento a) un VDA per Windows su un sistema operativo non supportato per questa versione di Citrix Virtual Apps and Desktops, viene visualizzato un messaggio di informazioni sulle opzioni.

Passaggio 4. Specificare come verrà utilizzato il VDA



Nella pagina **Environment**, specifica come intendi utilizzare il VDA, indicando se usi questa macchina come immagine per eseguire il provisioning di più macchine.

L'opzione scelta influisce sugli strumenti Citrix Provisioning installati automaticamente (se presenti) e sui valori predefiniti nella pagina Componenti aggiuntivi del programma di installazione del VDA.

Diversi MSI (di provisioning e altri) vengono installati automaticamente quando si installa un VDA. L'unico modo per impedirne l'installazione è con l'opzione `/exclude` in un'installazione da riga di comando.

Scegliere una delle seguenti opzioni:

- **Create a master MCS image (Crea un'immagine MCS master):** selezionare questa opzione per installare un VDA in un'immagine di macchina virtuale, se si prevede di utilizzare Machine Creation Services per eseguire il provisioning delle macchine virtuali. Questa opzione installa Machine Identity Service. Questa è l'opzione predefinita.

Opzione della riga di comando: `/mastermcsimage` o `/masterimage`

Importante:

Il supporto di installazione o l'immagine ISO devono essere montati localmente. Il montaggio di un'immagine ISO da un'unità di rete ai fini dell'installazione del software non è supportato.

- **Create a master image using Citrix Provisioning or third-party provisioning tools (Creare un'immagine master utilizzando Citrix Provisioning o strumenti di provisioning di terze parti):** selezionare questa opzione per installare un VDA su un'immagine VM, se si prevede di utilizzare Citrix Provisioning o strumenti di provisioning di terze parti (ad esempio Microsoft System Center Configuration Manager) per eseguire il provisioning delle macchine virtuali.

Opzione della riga di comando: `/masterpvsimage`

- (Viene visualizzato solo su macchine con sistema operativo multisessione) **Abilita le connessioni intermedie a un server:** Seleziona questa opzione per installare un VDA su una macchina fisica o virtuale che non verrà utilizzato come immagine per il provisioning di altre macchine.

Opzione della riga di comando: `/remotepc`

- (Appare solo su computer con sistema operativo a sessione singola) **Enable Remote PC Access (Abilita accesso remoto PC):** selezionare questa opzione per installare un VDA su un computer fisico da utilizzare con Accesso remoto PC.

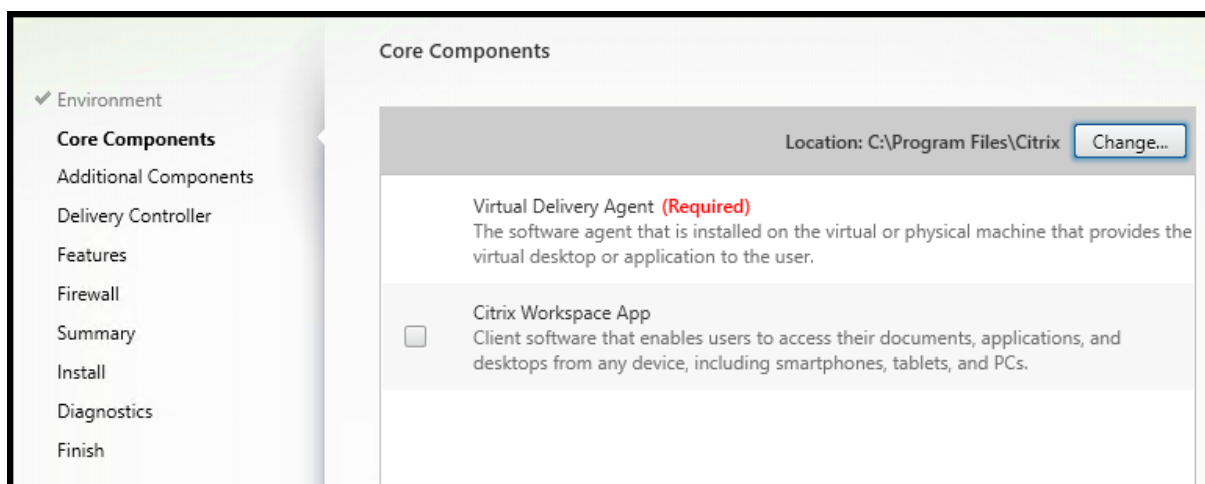
Opzione della riga di comando: `/remotepc`

Fare clic su **Next** (Avanti).

Questa pagina non viene visualizzata:

- Se si sta aggiornando un VDA
- Se si utilizza il programma di installazione `VDAWorkstationCoreSetup_2308.exe`, `VDAServerSetup_2308.exe` o `VDAWorkstationSetup_2308.exe`

Passaggio 5. Selezionare i componenti da installare e il percorso di installazione



Nella pagina **Core components:**

- **Posizione:** Per impostazione predefinita, i componenti sono installati in `C:\Program Files\Citrix`. Questa impostazione predefinita va bene per la maggior parte delle distribuzioni. Se si specifica una posizione diversa, tale posizione deve disporre delle autorizzazioni `execute` per il servizio di rete.
- **Componenti:** per impostazione predefinita, l'app Citrix Workspace per Windows non è installata con il VDA. Se si utilizza il programma di installazione `VDAWorkstationCoreSetup`.

`exe` , l'app Citrix Workspace per Windows non viene mai installata, quindi questa casella di controllo non viene visualizzata.

Fare clic su **Next** (Avanti).

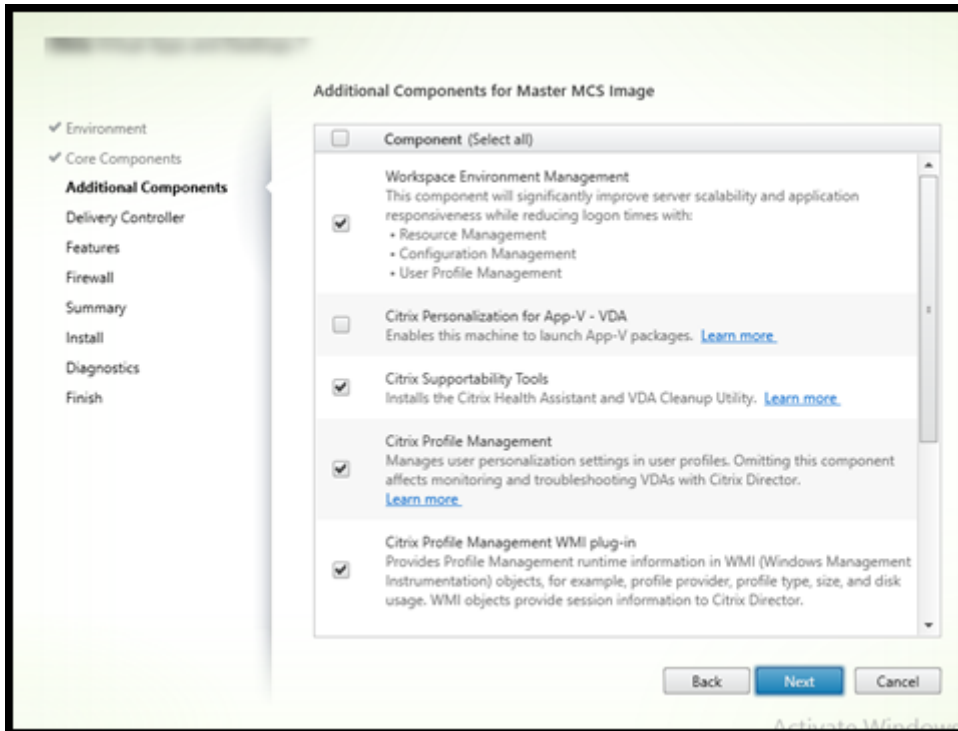
Opzioni della riga di comando: `/installdir,/components vda, plugin` per installare il VDA e l'app Citrix Workspace per Windows

Nota:

È possibile 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 Citrix Workspace App.
- Durante un aggiornamento VDA, se la versione dell'app Citrix Workspace può essere aggiornata, viene visualizzata l'opzione per aggiornare l'app Citrix Workspace.
- 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.

Passaggio 6. Installare componenti aggiuntivi



La pagina **Componenti aggiuntivi** contiene caselle di controllo per abilitare o disabilitare l’installazione di altre funzionalità e tecnologie con il VDA. In un’installazione da riga di comando, è possibile utilizzare l’opzione `/exclude` o `/includeadditional` per omettere o includere espressamente uno o più componenti disponibili.

Nella tabella seguente è indicata l’impostazione predefinita degli elementi presenti in questa pagina. L’impostazione predefinita dipende dall’opzione selezionata nella pagina **Environment**.

	Pagina Environment: opzione “Enable brokered connections to server”(Abilita connessioni negoziate al server) (per sistema operativo multisessione) o “Remote PC Access”(Accesso remoto PC) (per sistema operativo a sessione singola) selezionata
Pagina Additional Components	Pagina Environment: opzione “Master image with MCS” (Immagine master con MCS) o “Master image with Citrix Provisioning”(Immagine master con Citrix Provisioning) selezionata
Personalizzazione Citrix per App-V - VDA	Non selezionato
Livello di personalizzazione utente	Non visualizzato perché non valido per questo caso d’uso.

Pagina Additional Components	Pagina Environment: opzione “Master image with MCS” (Immagine master con MCS) o “Master image with Citrix Provisioning” (Immagine master con Citrix Provisioning) selezionata	Pagina Environment: opzione “Enable brokered connections to server” (Abilita connessioni negoziate al server) (per sistema operativo multisessione) o “Remote PC Access” (Accesso remoto PC) (per sistema operativo a sessione singola) selezionata
Citrix Profile Management	Selezionato	Non selezionato
Plug-in WMI Citrix Profile Management	Selezionato	Non selezionato
Agente di aggiornamento Citrix VDA	Non selezionato	Non selezionato
Citrix Backup and Restore	Non selezionato	Non selezionato
Citrix MCS IODriver	Non selezionato	Non selezionato
Citrix Rendezvous V2	Non selezionato	Non selezionato

Questa pagina non viene visualizzata se:

- Stai usando il programma di installazione [VDAWorkstationCoreSetup.exe](#). Inoltre, le opzioni della riga di comando per i componenti aggiuntivi non sono valide con tale programma di installazione.
- Si sta aggiornando un VDA e tutti i componenti aggiuntivi sono già installati. Se alcuni dei componenti aggiuntivi sono già installati, nella pagina vengono elencati solo i componenti non installati.

Selezionare o deselezionare le seguenti caselle di controllo (i componenti potrebbero apparire in un ordine diverso nel programma di installazione).

- **Citrix Personalization for App-V (Personalizzazione Citrix per App-V):** installare questo componente se si utilizzano applicazioni provenienti da pacchetti Microsoft App-V. Per i dettagli, consulta [Distribuire e distribuire applicazioni App-V](#).

Opzione della riga di comando: `/includeadditional «Citrix Personalization for App-V — VDA»` per abilitare l’installazione dei componenti, `/exclude «Citrix Personalization for App-V — VDA»` per impedire l’installazione dei componenti.

- **Livello di personalizzazione utente Citrix:** installa MSI per il livello di personalizzazione utente. Per i dettagli, vedere [Livello di personalizzazione utente](#).

Questo componente viene visualizzato solo quando si installa un VDA su una macchina Windows 10 a sessione singola.

Opzione della riga di comando: `/includeadditional «User Personalization Layer»` per abilitare l'installazione dei componenti, `/exclude «User Personalization Layer»` per impedire l'installazione dei componenti.

- **Citrix Profile Management:** questo componente gestisce le impostazioni di personalizzazione degli utenti nei profili utente. Per ulteriori informazioni, vedere [Profile Management](#).

L'esclusione di Citrix Profile Management dall'installazione influisce sul monitoraggio e la risoluzione dei problemi dei VDA con Citrix Director. Nelle pagine **User details** (Dettagli utente) ed **End Point** (Punto finale), saranno riportati errori del pannello **Personalization** e del pannello **Logon Duration** (Durata accesso). Nelle pagine **Dashboard** e **Trends**, il pannello **Average Logon Duration** (Durata media dell'accesso) visualizza i dati solo per le macchine su cui è installato Profile Management.

Anche se si utilizza una soluzione di gestione dei profili utente di terze parti, Citrix consiglia di installare ed eseguire Citrix Profile Management Service. L'attivazione del servizio Citrix Profile Management non è necessaria.

Opzione della riga di comando: `/includeadditional «Citrix Profile Management»` per abilitare l'installazione dei componenti, `/exclude «Citrix Profile Management»` per impedire l'installazione dei componenti.

- **Plug-in WMI Citrix Profile Management:** Questo plug-in fornisce informazioni di runtime di Profile Management negli oggetti WMI (Windows Management Instrumentation) (ad esempio, provider di profilo, tipo di profilo, dimensione e utilizzo del disco). Gli oggetti WMI forniscono informazioni sulla sessione a Director.

Opzione della riga di comando: `/includeadditional «Citrix Profile Management WMI Plug-in»` per abilitare l'installazione dei componenti, `/exclude «Citrix Profile Management WMI Plug-in»` per impedire l'installazione dei componenti.

- **VDA Upgrade Agent (Agente di aggiornamento VDA):** valido solo per le distribuzioni di Citrix DaaS (precedentemente servizi Citrix Virtual Apps and Desktops). Consente al VDA di partecipare alla [funzione di aggiornamento VDA](#). È possibile utilizzare questa funzione per aggiornare i VDA di un catalogo dalla console di gestione, immediatamente o in un orario pianificato. Se questo agente non è installato, è possibile aggiornare un VDA eseguendo il programma di installazione VDA sulla macchina.

Opzioni della riga di comando: `/includeadditional «Citrix VDA Upgrade Agent»` per abilitare l'installazione dei componenti, `/exclude «Citrix VDA Upgrade Agent»` per impedire l'installazione dei componenti.

- **Cache di scrittura MCSIO per l'ottimizzazione dello storage:** Installa il driver I/O Citrix MCS.

Per ulteriori informazioni, vedere [Storage condiviso dagli hypervisor](#) e [Configurare la cache per i dati temporanei](#).

Opzioni della riga di comando: `/includeadditional «Citrix MCS IODriver»` per abilitare l'installazione dei componenti, `/exclude «Citrix MCS IODriver»` per impedire l'installazione dei componenti.

- **Configurazione proxy:** Installa questo componente se prevedi di utilizzare il protocollo Rendezvous con Gateway Service, VDA Upgrade Service e così via, nel tuo ambiente e hai un proxy non trasparente nella tua rete per le connessioni in uscita, specifica il proxy qui. Sono supportati solo i proxy HTTP.

Se si installa questo componente, specificare l'indirizzo del proxy o il percorso del file PAC nella pagina **Rendezvous Proxy Configuration** (Configurazione del proxy Rendezvous). Per dettagli delle funzionalità, vedere [Protocollo Rendezvous](#).

Opzione della riga di comando: `/includeadditional «Citrix Rendezvous V2" per abilitare l'installazione dei componenti, /exclude «Citrix Rendezvous V2" per impedire l'installazione dei componenti.`

- **Citrix Backup and Restore:** Se l'installazione o l'aggiornamento di un VDA fallisce, questo componente può riportare la macchina a un backup eseguito prima dell'installazione o dell'aggiornamento.

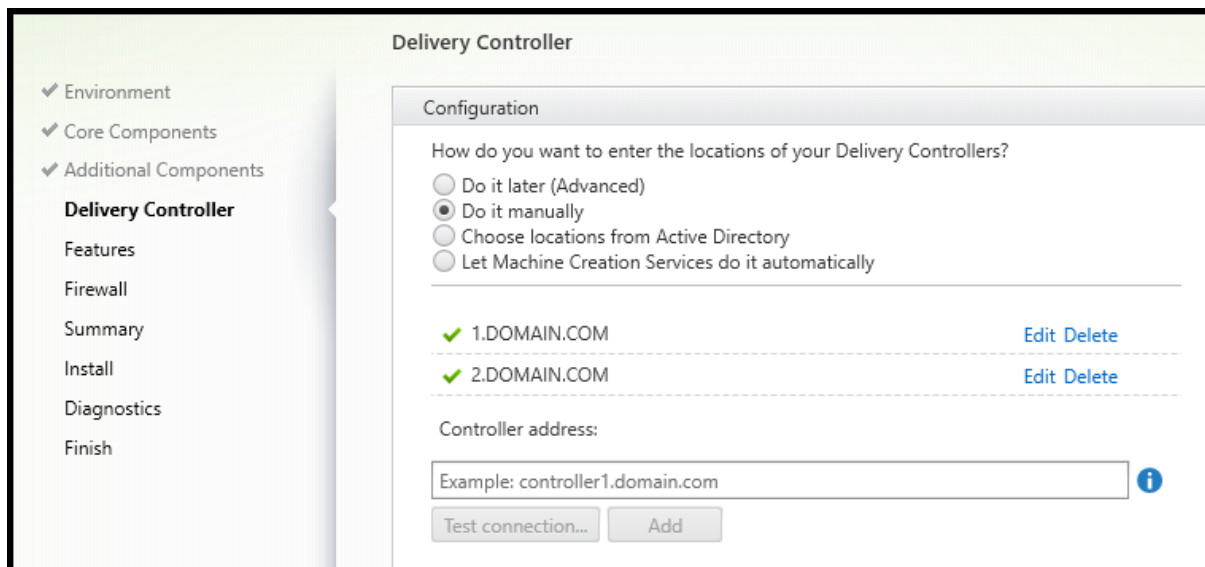
Assicurati che i prerequisiti Microsoft siano soddisfatti come indicato in [Prepararsi all'installazione](#).

Opzione della riga di comando: `/includeadditional «Citrix Backup and Restore»` per abilitare l'installazione dei componenti, `/exclude «Citrix Backup and Restore»` per impedire l'installazione dei componenti.

Nota:

Se l'ottimizzazione dello storage MCS è abilitata, il backup o il ripristino per il server o il sistema operativo desktop Windows può fallire. Per risolvere questo problema, disabilitate l'opzione di ottimizzazione dello storage MCS nel meta installer.

Passaggio 7 Indirizzi dei Delivery Controller



Nella pagina **Delivery Controller**, scegliere come inserire gli indirizzi dei controller installati. Citrix consiglia di specificare gli indirizzi durante l'installazione del VDA (**Do it manually** (Eseguire manualmente)). Il VDA non può registrarsi con un controller fino a quando non dispone di queste informazioni. Se un VDA non è in grado di registrarsi, gli utenti non possono accedere alle applicazioni e ai desktop su tale VDA.

- **Do it manually** (Eseguire manualmente): (impostazione predefinita) immettere il nome di dominio completo di un controller installato e quindi fare clic su **Add**. Se sono stati installati più controller, aggiungerne gli indirizzi.
- **Do it later (Advanced)**: (Eseguirlo più tardi (avanzato)) se si sceglie questa opzione, la procedura guidata chiede una conferma prima di continuare. Per specificare gli indirizzi in un secondo momento, è possibile eseguire nuovamente il programma di installazione o utilizzare i Criteri di gruppo Citrix. La procedura guidata inserisce anche un promemoria nella pagina **Summary**.
- **Choose locations from Active Directory** (Scegliere i percorsi da Active Directory): valido solo quando il computer viene aggiunto a un dominio e l'utente è un utente di dominio.
- **Usa il token WebSocket (anteprima tecnica)**: Crea un VDA WebSocket. Il WebSocketToken è per il token richiesto.
- **Let Machine Creation Services do it automatically** (Farlo eseguire automaticamente da Machine Creation Services): valido solo quando si utilizza MCS per eseguire il provisioning delle macchine.

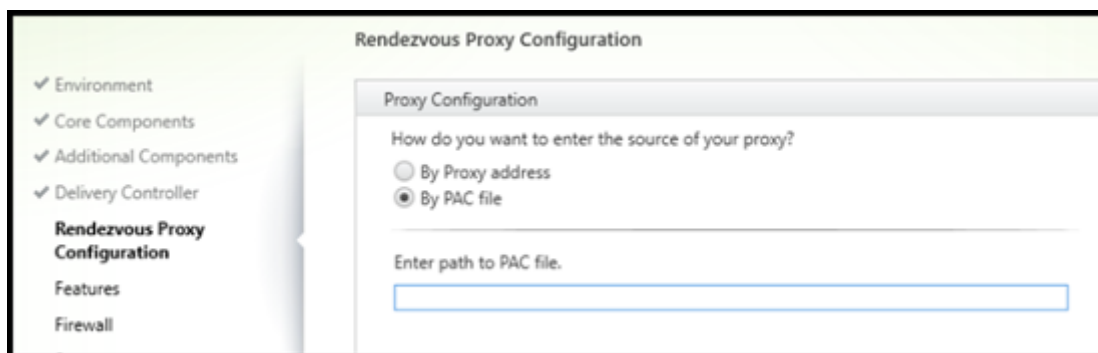
Fare clic su **Next** (Avanti). Se è stata selezionata l'opzione **Do it later (Advanced)**, verrà richiesto di confermare che verranno specificati gli indirizzi del controller in un secondo momento.

Altre considerazioni:

- L'indirizzo non può contenere caratteri non alfanumerici.
- Se si specificano gli indirizzi durante l'installazione del VDA e in Criteri di gruppo, le impostazioni dei criteri sostituiscono le impostazioni fornite durante l'installazione.
- La corretta registrazione del VDA richiede che le porte firewall utilizzate per comunicare con il controller siano aperte. Tale azione è abilitata per impostazione predefinita nella pagina **Firewall** della procedura guidata.
- Dopo aver specificato le posizioni dei controller (durante o dopo l'installazione del VDA), è possibile utilizzare la funzionalità di aggiornamento automatico per aggiornare i VDA quando i controller vengono aggiunti o rimossi. Per informazioni dettagliate su come i VDA rilevano e si registrano con i controller, vedere [VDA registration](#).

Opzione della riga di comando: `/controllers`

Passaggio 8. Configurazione proxy



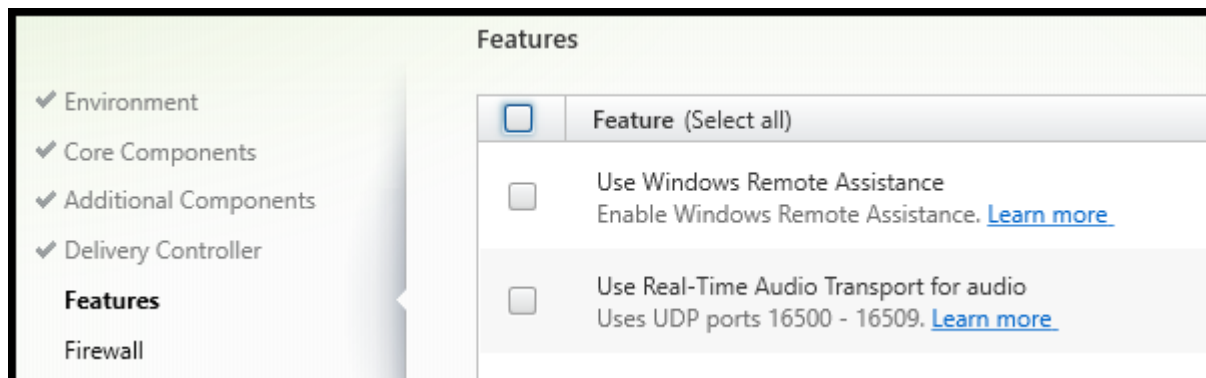
La pagina **Proxy Configuration** viene visualizzata solo se è stata abilitata la casella di controllo **Proxy Configuration** nella pagina **Componenti aggiuntivi**.

1. Selezionare se si dovrà specificare l'origine del proxy mediante l'indirizzo proxy o il percorso del file PAC.
2. Specificare l'indirizzo del proxy o il percorso del file PAC.
 - Formato dell'indirizzo proxy: `http://<url-or-ip>:<port>`
 - Formato file PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

Il firewall per la porta proxy deve essere aperto affinché il test di connessione abbia esito positivo. Se non è possibile stabilire una connessione al proxy, è possibile scegliere se continuare l'installazione di VDA.

Opzione della riga di comando: `/proxyconfig`

Passaggio 9 Attivare o disattivare funzionalità



Nella pagina **Features** utilizzare le caselle di controllo per attivare o disattivare le funzionalità che si desidera utilizzare.

- **Use Windows Remote Assistance (Utilizzare Assistenza remota di Windows):** quando questa funzionalità è abilitata, Assistenza remota di Windows viene utilizzata con la funzionalità di shadowing utente di Director. Assistenza remota di Windows apre le porte dinamiche nel firewall. (Impostazione predefinita= disabilitato)

Opzione della riga di comando: `/enable_remote_assistance`

- **Use Real-Time Audio Transport for audio** (Utilizza il trasporto audio in tempo reale per l'audio): abilitare questa funzione se la funzionalità voice-over-IP è ampiamente utilizzata nella rete. La funzione riduce la latenza e migliora la resilienza audio sulle reti con perdita di dati. Consente di trasmettere i dati audio utilizzando RTP su trasporto UDP. (Impostazione predefinita= disabilitato)

Opzione della riga di comando: `/enable_real_time_transport`

- **Use screen sharing (Usa la condivisione dello schermo):** se abilitata, le porte utilizzate dalla condivisione dello schermo vengono aperte nel firewall di Windows. (Impostazione predefinita= disabilitato)

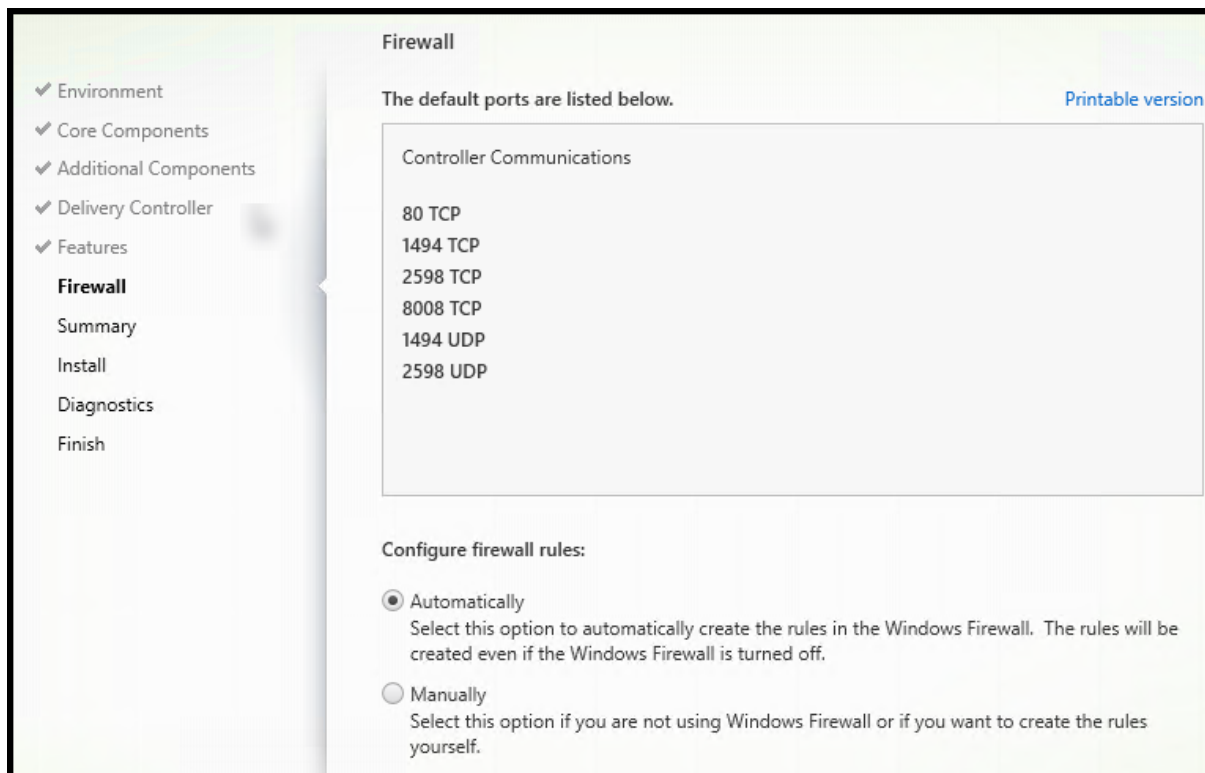
Opzione della riga di comando: `/enable_ss_ports`

- **Is this VDA installed on a VM in a cloud (Questo VDA è installato su una macchina virtuale in un cloud?)** Questa impostazione aiuta Citrix a identificare correttamente le posizioni delle risorse per le distribuzioni VDA on-premise e come servizio (Citrix Cloud) a scopi di telemetria. Questa funzionalità non ha alcuna ripercussione sull'utilizzo da parte del cliente. Attivare questa impostazione se la distribuzione utilizza Citrix DaaS (predefinito= disabilitato).

Opzione della riga di comando: `/xendesktopcloud`

Fare clic su **Next** (Avanti).

Passaggio 10. Porte del firewall

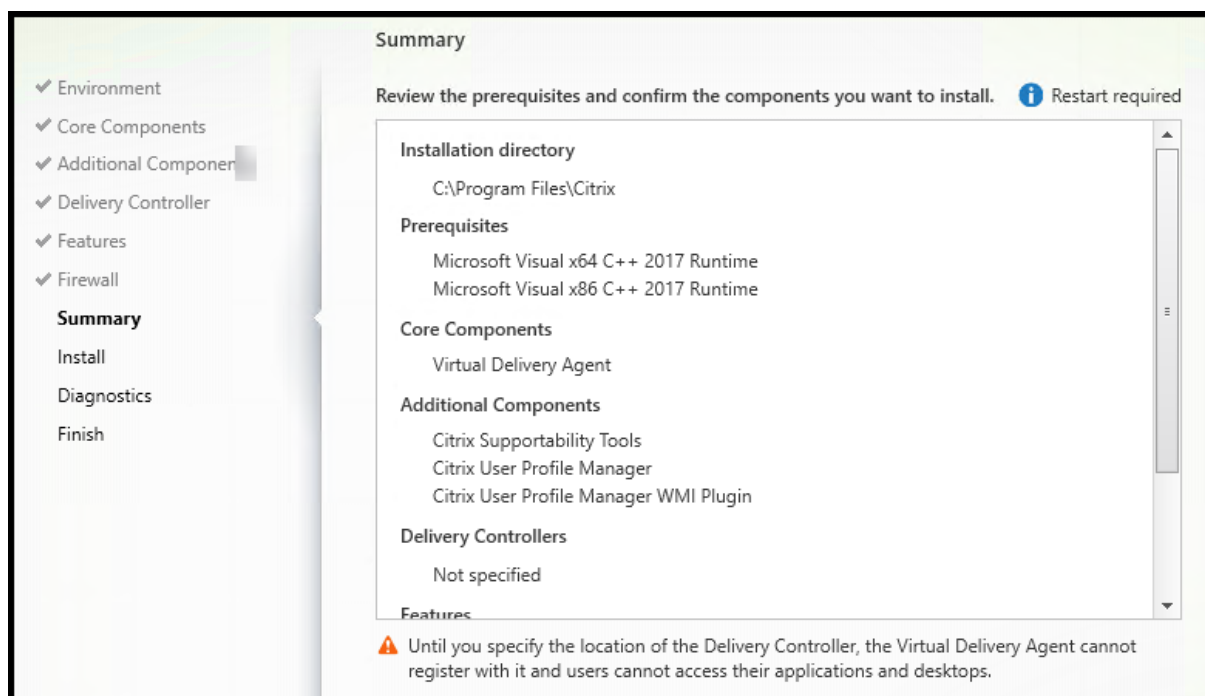


Nella pagina **Firewall**, per impostazione predefinita, le porte vengono aperte automaticamente se il servizio Windows Firewall è in esecuzione, anche se il firewall non è abilitato. Questa impostazione predefinita è adatta alla maggior parte delle distribuzioni. Per informazioni sulle porte, vedere [Porte di rete](#).

Fare clic su **Next** (Avanti).

Opzione della riga di comando: `/enable_hdx_ports`

Passaggio 11. Esaminare i prerequisiti e confermare l'installazione

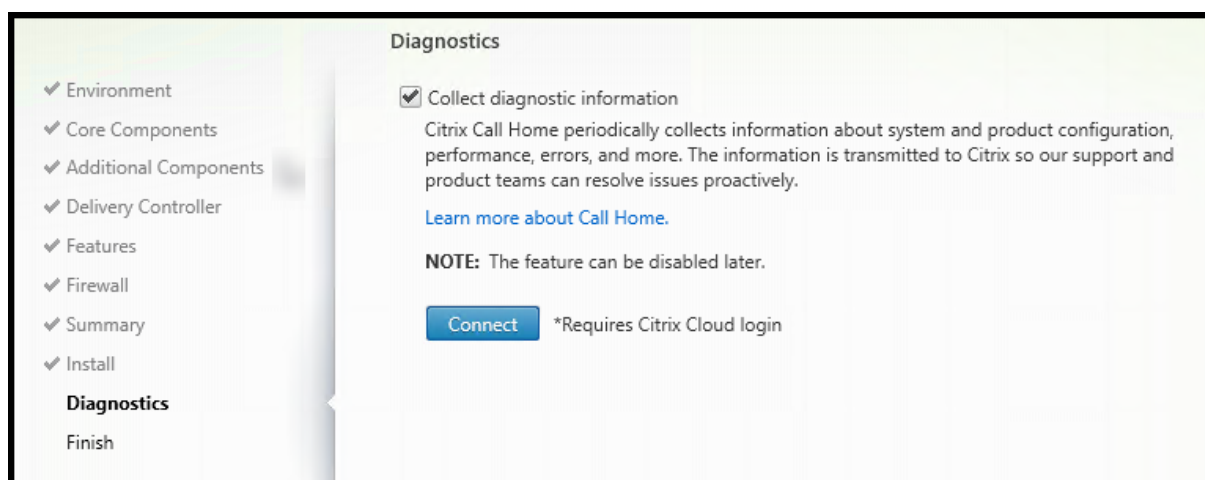


Nella pagina **Summary** sono elencati gli elementi che verranno installati. Utilizzare il pulsante **Back** per tornare alle pagine precedenti della procedura guidata e modificare le selezioni.

Quando si è pronti, fare clic su **Install**.

Se i prerequisiti non sono già installati o abilitati, il computer potrebbe riavviarsi una o più volte. Vedi [Prepararsi all'installazione di](#).

Passaggio 12. Diagnostica



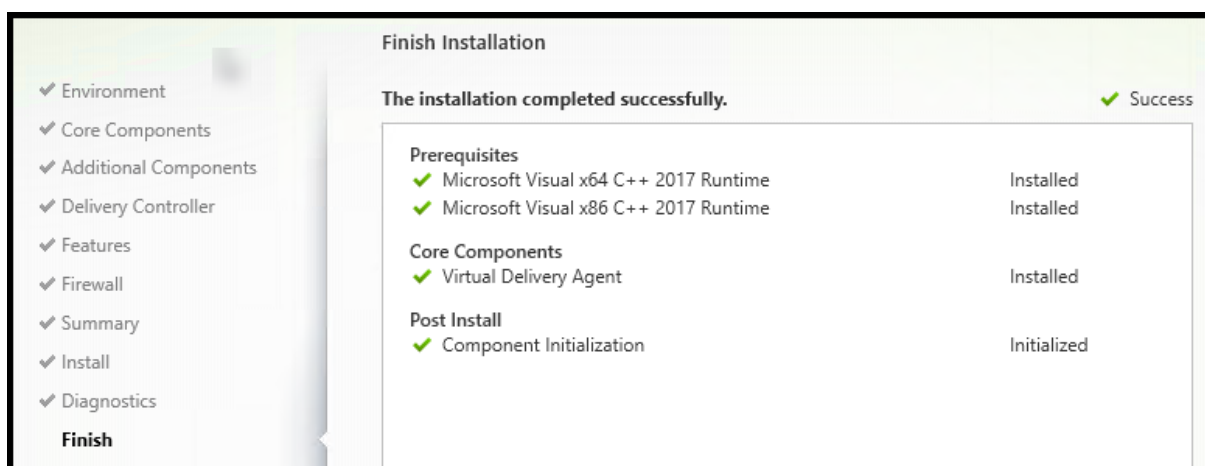
Nella pagina **Diagnostics** (Diagnostics), scegliere se partecipare a Citrix Call Home. Se si sceglie di partecipare (impostazione predefinita), fare clic su **Connect**. Quando richiesto, immettere le credenziali dell'account Citrix.

Dopo aver convalidato le credenziali (o se si sceglie di non partecipare), fare clic su **Next**.

Quando si utilizza il programma di installazione completo del prodotto, se si fa clic su **Connect** (Connetti) nella pagina **Diagnostics** (Diagnostica) senza prima selezionare **Collect diagnostic information** (Raccogli informazioni diagnostiche), dopo aver chiuso la finestra di dialogo **Connect to Citrix Insight Services** (Connetti a Citrix Insight Services) il pulsante **Next** (Avanti) è disabilitato. Non è possibile passare alla pagina successiva. Per riattivare il pulsante **Next** (Avanti), selezionare e deselezionare immediatamente **Collect diagnostic information** (Raccogli informazioni diagnostiche).

Per ulteriori informazioni, vedere [Call Home](#).

Passaggio 13. Completare questa installazione



La pagina **Finish** contiene segni di spunta verdi per tutti i prerequisiti e i componenti installati e inizializzati correttamente.

Fare clic su **Finish**. Per impostazione predefinita, la macchina si riavvia automaticamente. Sebbene sia possibile disattivare questo riavvio automatico, il VDA non può essere utilizzato fino al completamento del riavvio della macchina.

Passaggi successivi

Ripetere la procedura precedente per installare i VDA su altri computer o altre immagini, se necessario.

Dopo aver installato tutti i VDA, avviare Studio. Se non si è ancora creato un sito, Studio guida automaticamente allo svolgimento di tale attività. Al termine di questa operazione, Studio guida alla

creazione di un catalogo macchine e quindi un gruppo di consegna. Vedere:

- [Crea un sito](#)
- [Creare cataloghi di macchine](#)
- [Creare gruppi di consegna](#)

Citrix Optimizer

Citrix Optimizer è uno strumento per il sistema operativo Windows che aiuta gli amministratori Citrix a ottimizzare i VDA rimuovendo e ottimizzando vari componenti.

Dopo aver installato un VDA e completato il riavvio finale, scaricare e installare Citrix Optimizer. Vedere [CTX224676](#). L'articolo CTX contiene il pacchetto di download, oltre a istruzioni sull'installazione e l'utilizzo di Citrix Optimizer.

Personalizzare un VDA

Per personalizzare un VDA installato:

1. Dalla funzione Windows per la rimozione o la modifica dei programmi, selezionare **Citrix Virtual Delivery Agent** o **Citrix Remote PC Access/VDI Core Services VDA**. Quindi fare clic con il pulsante destro del mouse e selezionare **Modifica**.
2. Selezionare **Customize Virtual Delivery Agent Settings** (Personalizza impostazioni del Virtual Delivery Agent). All'avvio del programma di installazione è possibile modificare:
 - Indirizzi dei controller
 - Porta TCP/IP da registrare con il controller (impostazione predefinita= 80)
 - Se aprire automaticamente le porte di Windows Firewall

Risoluzione dei problemi

- Per informazioni su come Citrix riporta i risultati delle installazioni dei componenti, vedere [Citrix installation return codes](#).
- Nella visualizzazione Studio per un gruppo di consegna, la voce **Installed VDA version** (Versione VDA installata) nel riquadro **Details** potrebbe non essere la versione installata nei computer. La visualizzazione Programmi e funzionalità di Windows della macchina mostra la versione VDA effettiva.
- Dopo l'installazione di un VDA, non è possibile distribuire app o un desktop agli utenti fino a quando non si registra con un Delivery Controller.

Per informazioni sui metodi di registrazione VDA e su come risolvere i problemi di registrazione, vedere [Registrazione VDA](#).

Limitazione nota

Quando si utilizza l'app Citrix Workspace per Windows versione 1912 o precedente, la sessione si interrompe dopo un po'. Questo problema è stato risolto nelle versioni più recenti LTSR e CR dell'app Citrix Workspace. Per ulteriori informazioni sulle versioni di rilascio supportate, vedere [App Citrix Workspace per Windows/Citrix Receiver for Windows Long Term Service Releases](#).

Installare VDA utilizzando SCCM

January 24, 2025

Panoramica

Microsoft Endpoint Configuration Manager, in precedenza System Center Configuration Manager (SCCM), è un prodotto Windows che consente la gestione, la distribuzione e la sicurezza di dispositivi e applicazioni in tutta l'azienda.

Nota:

Nel seguente articolo vengono fornite solo raccomandazioni basate sul modo in cui Citrix ha testato l'ambiente. Puoi personalizzare questi passaggi in base alle tue esigenze. Citrix non è responsabile di eventuali aggiornamenti o modifiche necessari per soddisfare le esigenze dei clienti.

Raccomandazioni

- Per distribuire correttamente un Virtual Delivery Agent (VDA) utilizzando SCCM o strumenti di distribuzione software simili, Citrix consiglia di utilizzare il programma di installazione VDA [in una sequenza di passaggi](#).
- Citrix sconsiglia di utilizzare VDA Cleanup Utility come parte di un'installazione o di un aggiornamento VDA. Utilizzare VDA Cleanup Utility solo nel caso limitato in cui il programma di installazione VDA abbia precedentemente fallito.

Prima di iniziare

Il numero di riavvii richiesti durante l'installazione del VDA dipende dall'ambiente. Per esempio:

- Potrebbe essere necessario un riavvio per gli aggiornamenti in sospeso o per i riavvii da installazioni software precedenti.
- I file precedentemente bloccati da altri processi potrebbero aver bisogno di aggiornamenti, costringendo a un ulteriore riavvio.
- Alcuni componenti opzionali nel programma di installazione VDA (ad esempio Citrix Profile Management e Citrix Files) potrebbero richiedere un riavvio.
- Quando si aggiorna un VDA, la macchina su cui è installato deve essere in modalità di manutenzione, senza sessioni.
- Quando un'installazione VDA viene eseguita per la prima volta su una macchina, il programma di installazione VDA utilizzato viene copiato su quella macchina. Per maggiori informazioni sull'installazione di VDA, vedere [Programmi di installazione](#).

SCCM Task Sequencer gestisce tutti i riavvii richiesti.

Passaggi chiave per distribuire VDA utilizzando SCCM

I passaggi seguenti descrivono come distribuire VDA utilizzando SCCM sulla macchina virtuale.

1. [Installa VDA](#).
2. [Crea un'unità organizzativa \(OU\)](#).
3. Verifica le macchine.
4. Usa VDA per distribuire contenuti.

Passaggio 1: installare VDA

Dopo aver identificato tutti i prerequisiti, utilizzare **SCCM Task Sequencer** per completare le seguenti attività:

1. Installare VDA da una copia accessibile del supporto di installazione o da uno degli installatori autonomi VDA:
 - [VDAWorkstationSetup_XXXX.exe](#)
 - [VDA ServerSetup_XXXX.exe](#)
 - [VDAWorkstationCoreSetup_XXXX.exe](#)

Per maggiori informazioni sugli installatori VDA, vedere [Installatori](#).

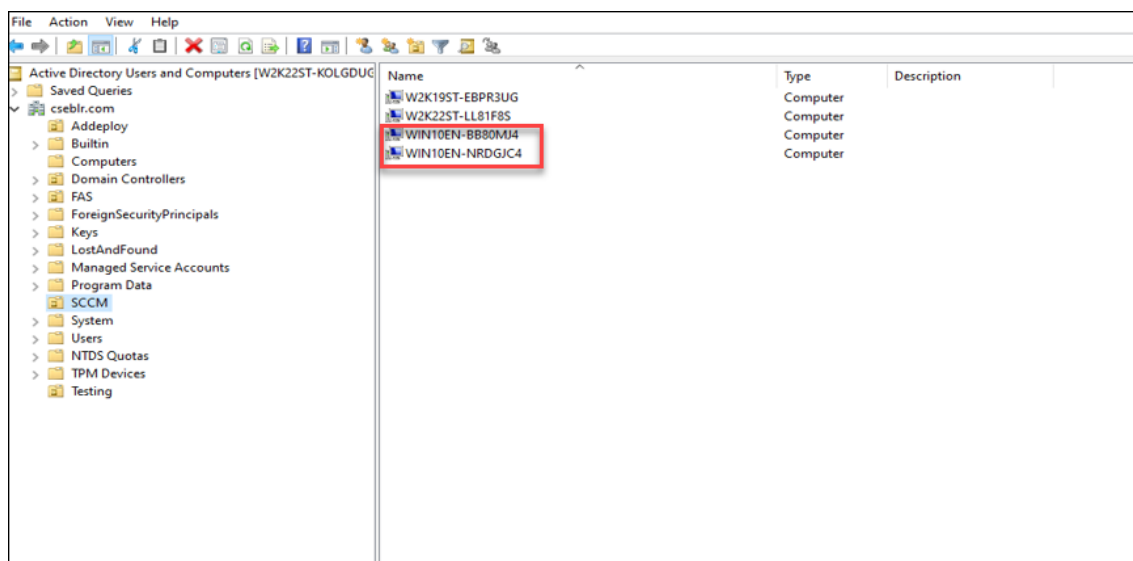
Nota:

Quando si aggiorna un VDA, la macchina su cui è installato deve essere in modalità di manutenzione, senza sessioni.

2. Quando un'installazione VDA viene eseguita per la prima volta su una macchina, il programma di installazione VDA utilizzato viene copiato su quella macchina.
 - Quando si utilizza un programma di installazione VDA diverso da `VDAWorkstationCoreSetup_XXXX.exe`, il programma di installazione VDA viene copiato in `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
 - Quando si utilizza `VDAWorkstationCoreSetup_XXXX.exe`, il programma di installazione VDA viene copiato in `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.
3. Il percorso della directory del programma di installazione VDA è memorizzato anche nel registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall` "MetaInstallerInstallLocation".
4. Aggiungere le opzioni della riga di comando `/NOREBOOT`, `/NORESUME` e `/QUIET` alle opzioni della riga di comando.
 - `/QUIET`: Non mostrare l'interfaccia utente durante l'installazione, in modo che SCCM abbia il controllo del processo di installazione.
 - `/NOREBOOT`: Impedisce il riavvio automatico del programma di installazione VDA. SCCM attiva i riavvii quando necessario.
 - `/NORESUME`: Solitamente, quando è necessario un riavvio durante l'installazione, il programma di installazione VDA imposta una chiave di registro `RunOnce` (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`). Windows utilizza la chiave per aprire il programma di installazione VDA quando il computer si riavvia. Questo rappresenta un problema per SCCM, poiché SCCM non è in grado di monitorare l'installazione e di acquisire il codice di uscita.


Passaggio 2: creare un'unità organizzativa (OU)

1. Crea due macchine virtuali aggiunte al dominio che desideri aggiungere all'OU. Quando le macchine virtuali vengono create inizialmente, si trovano nella cartella **Computer**. Spostare le macchine virtuali nella cartella **SCCM**. Esempio: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com



2. In Microsoft Configuration Manager, andare a `\Amministrazione\Panoramica\Configurazione gerarchia\Metodi di individuazione\`.
3. Fare clic su **Rilevamento sistema Active Directory** e selezionare la casella di controllo **Abilita rilevamento sistema Active Directory** per abilitare il rilevamento automatico delle macchine virtuali appena create.



4. Fare clic sull'icona  per selezionare nuovi contenitori.
5. Nella sezione **Location**, aggiungi il **Path** in cui si trovano le tue macchine virtuali SCCM.
6. Andare su `\Amministrazione\Panoramica\Configurazione sito\Siti` e fare clic con il pulsante destro del mouse su SCCM VDA.
7. Seleziona **Impostazioni di installazione client > Installazione push client**. Si apre la finestra **Proprietà di installazione push del client**.
8. Una volta impostate le VM su **Abilitate**, è possibile visualizzare l'elenco delle VM come illustrato nelle immagini seguenti.

Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity
	x86 Unknown Computer...	No			CSE	
	x64 Unknown Computer...	No			CSE	
	WIN10EN-NRDGJ4	Yes			CSE	Active
	WIN10EN-8880M4	No			CSE	
	W2K22ST-LL81F85	Yes			CSE	Active
	W2K19ST-EBPR3UG	No			CSE	
	W2K19ST-6CBDO9Q	Yes			CSE	Active
	TSVDA-SCCM19	Yes			CSE	Active
	SCCM-VDA	Yes			CSE	Active
	Provisioning Device(Pro...	No			CSE	
	2019-SCCM	No			CSE	

Create Package and Program Wizard

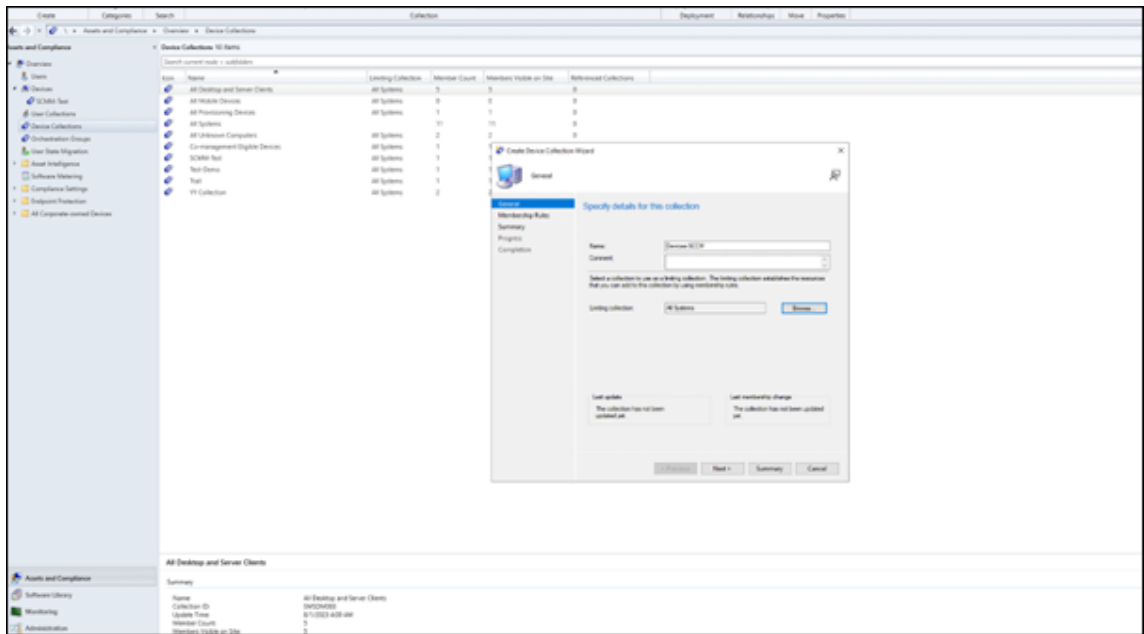
Program Type

Choose the program type that you want to create

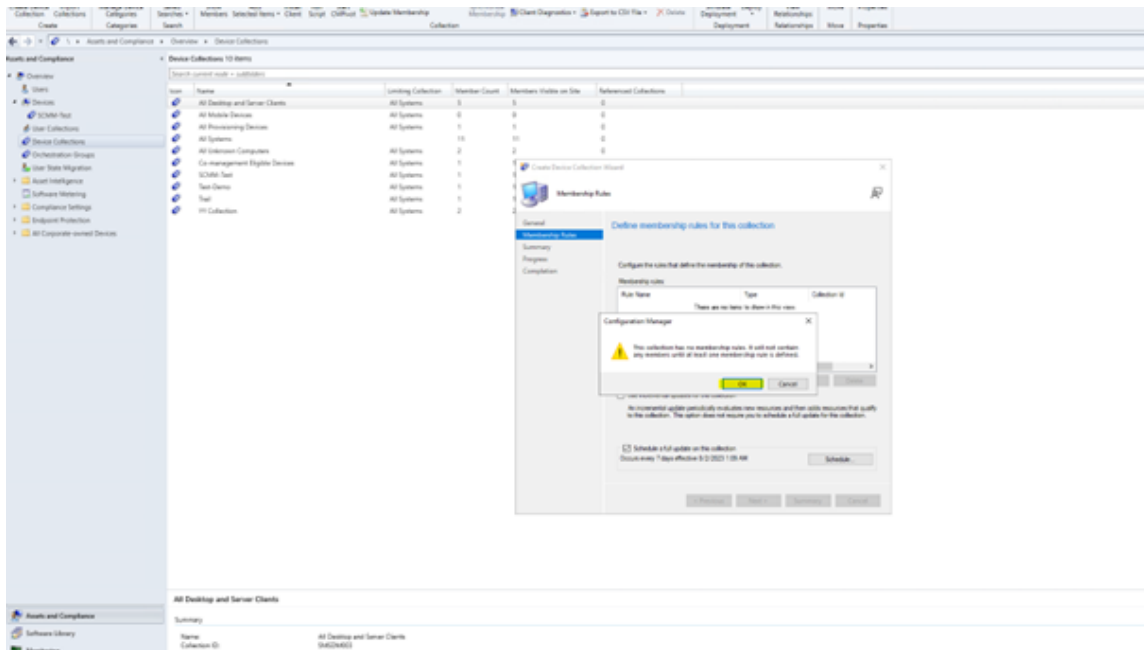
- Standard program
Create a program for a client computer.
- Program for device
Create a program for a device.
- Do not create a program
Create a package, but do not create a program. You can use the Create Program Wizard to add a program later.

< Previous **Next >** Summary Cancel

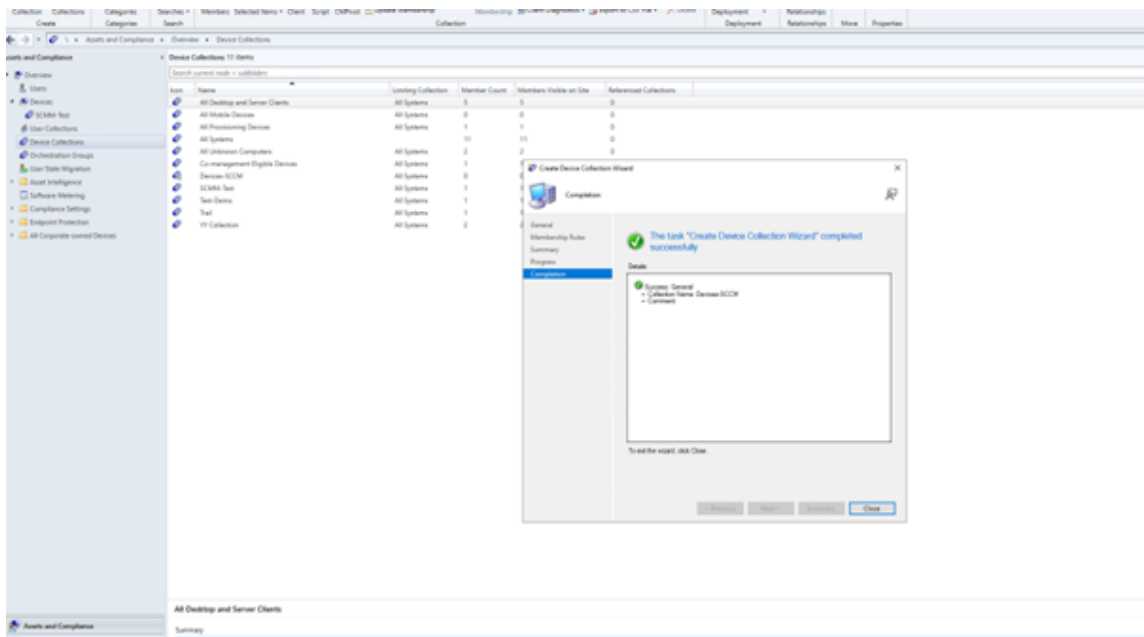
9. Crea la raccolta di dispositivi **** per creare l'OU. Inserisci il nome**** della raccolta.



10. Seguire le istruzioni della procedura guidata.

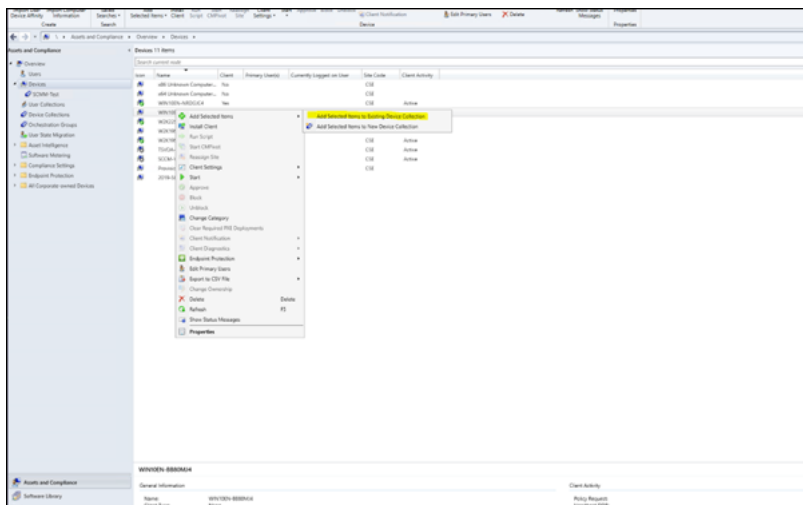


Viene creata l'UO.

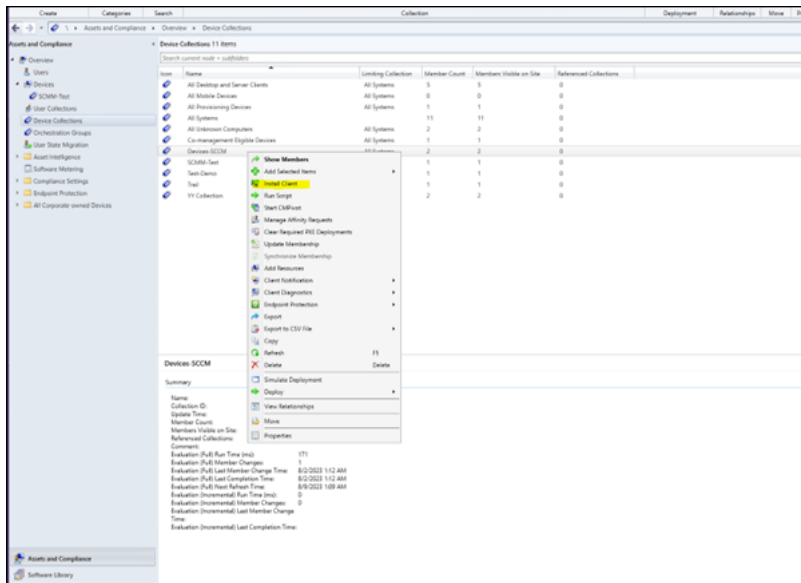


11. Aggiungere le VM create alla raccolta dispositivi appena creata.

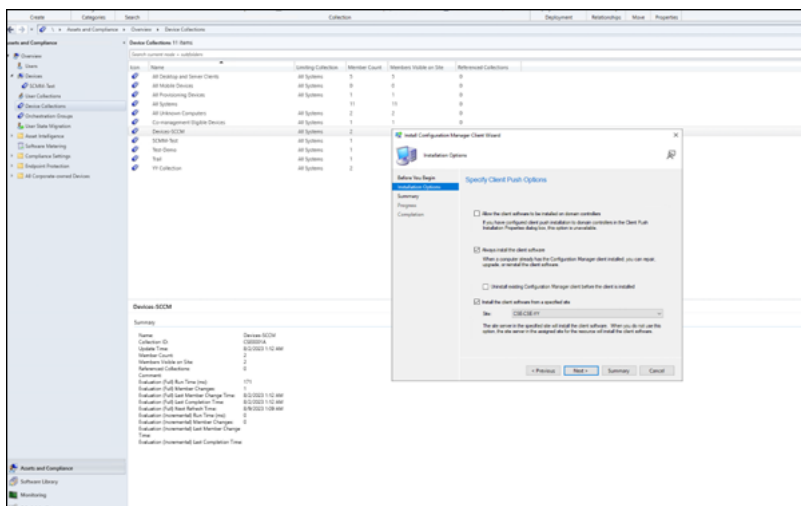
- a) Fare clic con il pulsante destro del mouse sulla VM. Seleziona **Aggiungi elementi selezionati > Aggiungi elementi selezionati alla raccolta dispositivi esistente**.



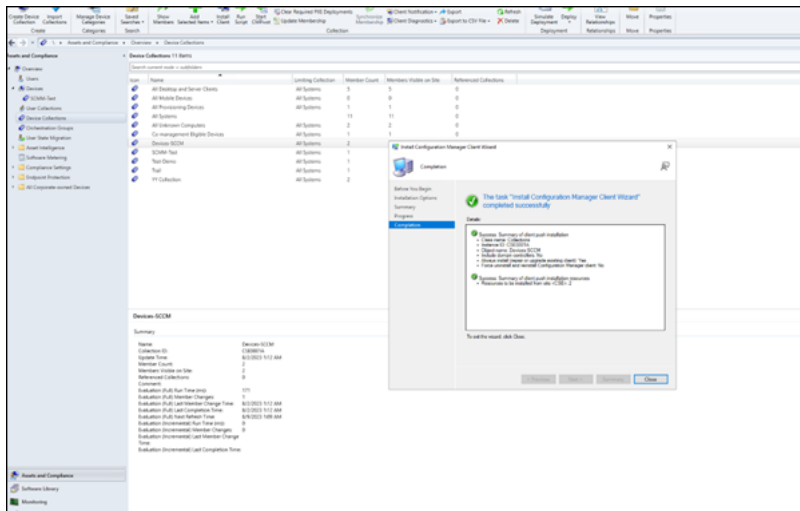
- b) Nella finestra **Seleziona raccolta**, seleziona il nome del dispositivo richiesto. In questo esempio, è **Devices-SCCM**.



13. Selezionare il sito di installazione **richiesto**.



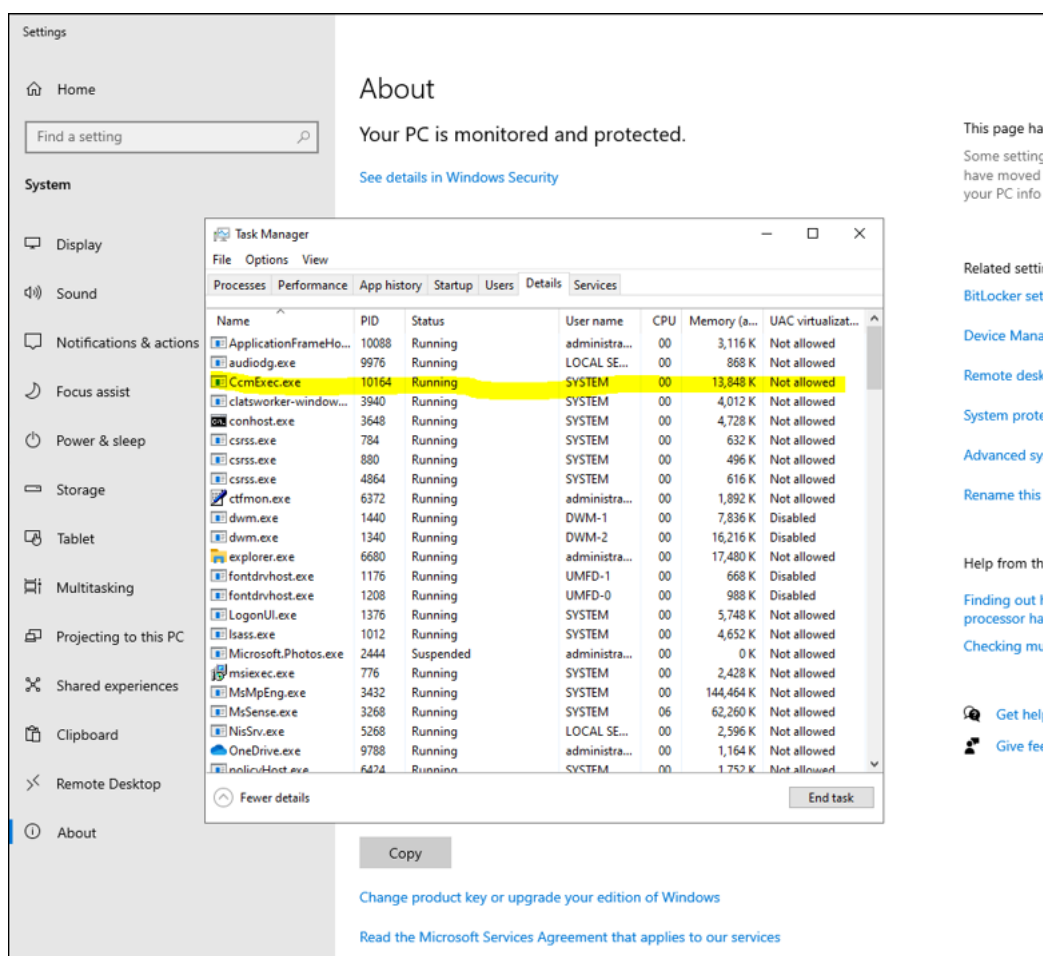
14. Seguire le istruzioni della procedura guidata. **L'installazione guidata del client Configuration Manager** è stata completata correttamente.



Per informazioni dettagliate, vedere [Gestisci raccolte](#) nella documentazione Microsoft.

Fase 3: verificare le macchine

1. Sul computer client, verificare che il client sia installato controllando se il processo **CCMExec** è in esecuzione.



2. Verificare se il client è in esecuzione per le VM su SCCM.

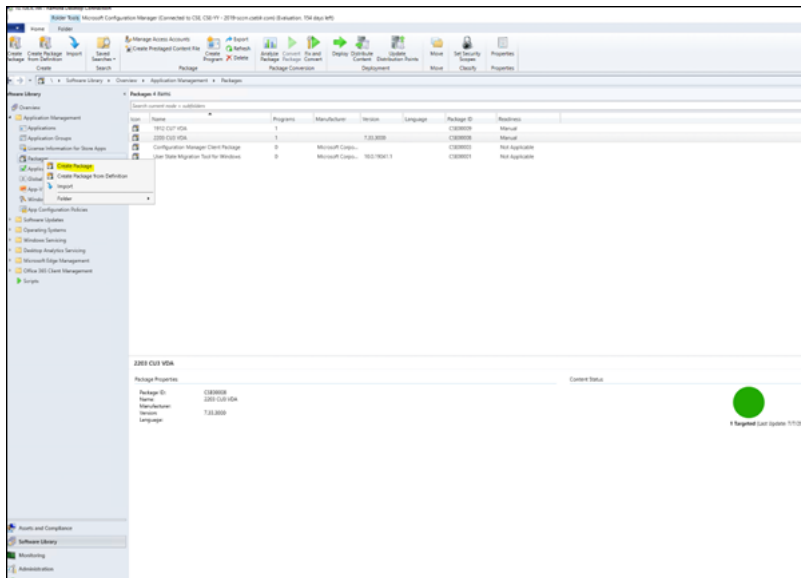
Passaggio 4: utilizzare VDA per distribuire i contenuti

I passaggi seguenti descrivono come utilizzare il VDA distribuito per distribuire contenuti sulle macchine virtuali associate.

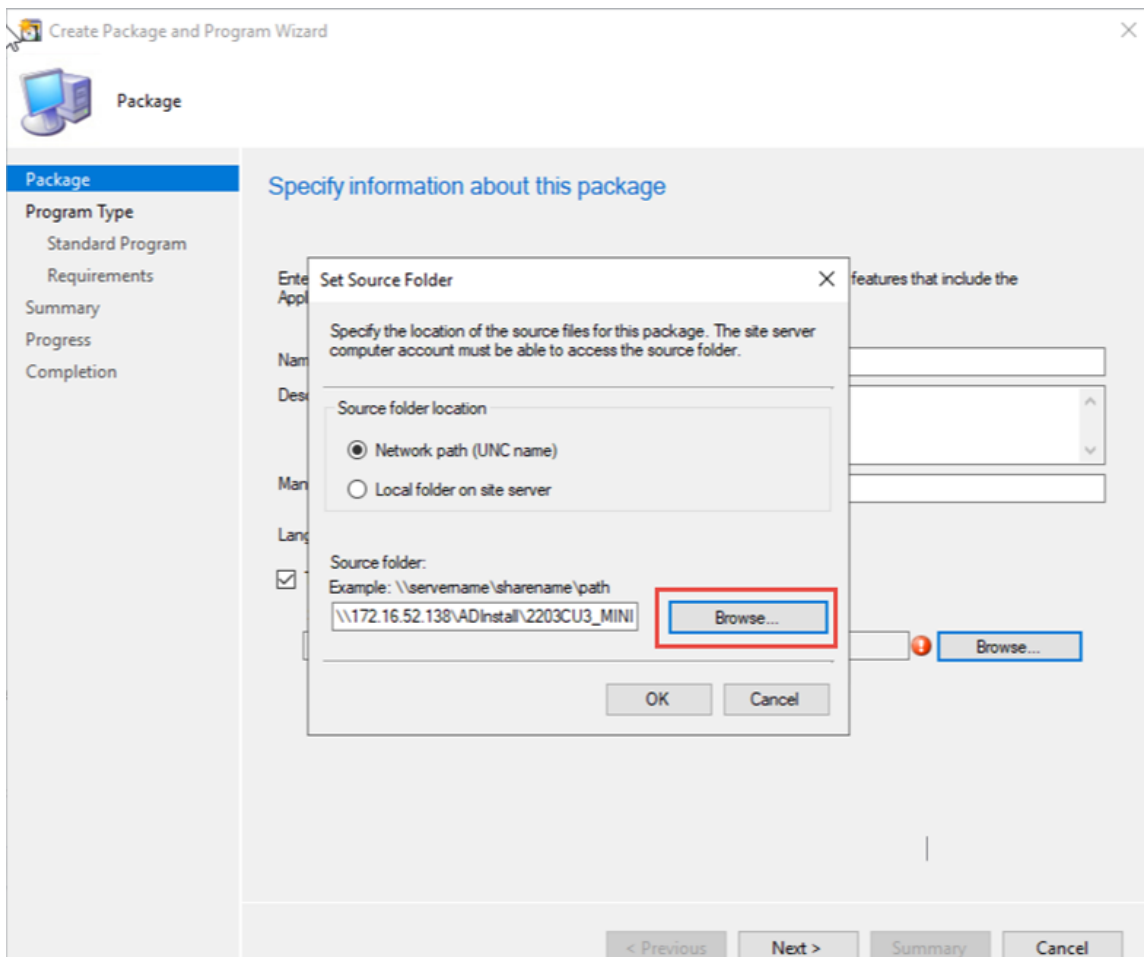
1. Crea un pacchetto
2. Distribuire il contenuto

Crea un pacchetto

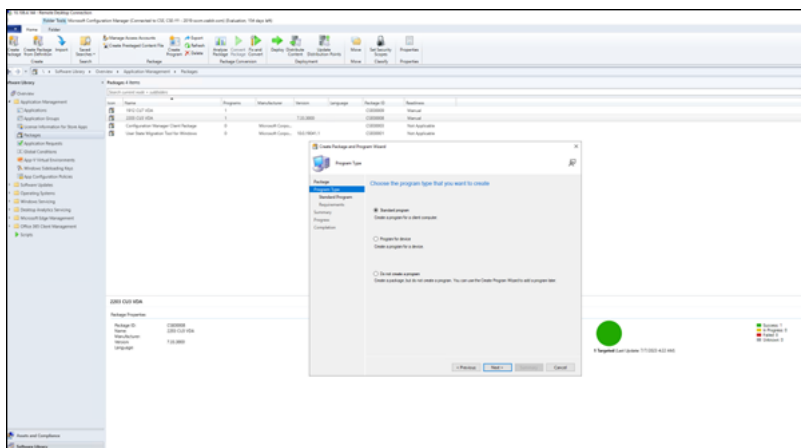
1. Per creare un pacchetto, fai clic con il pulsante destro del mouse sul VDA desiderato e fai clic su **Crea pacchetto**.



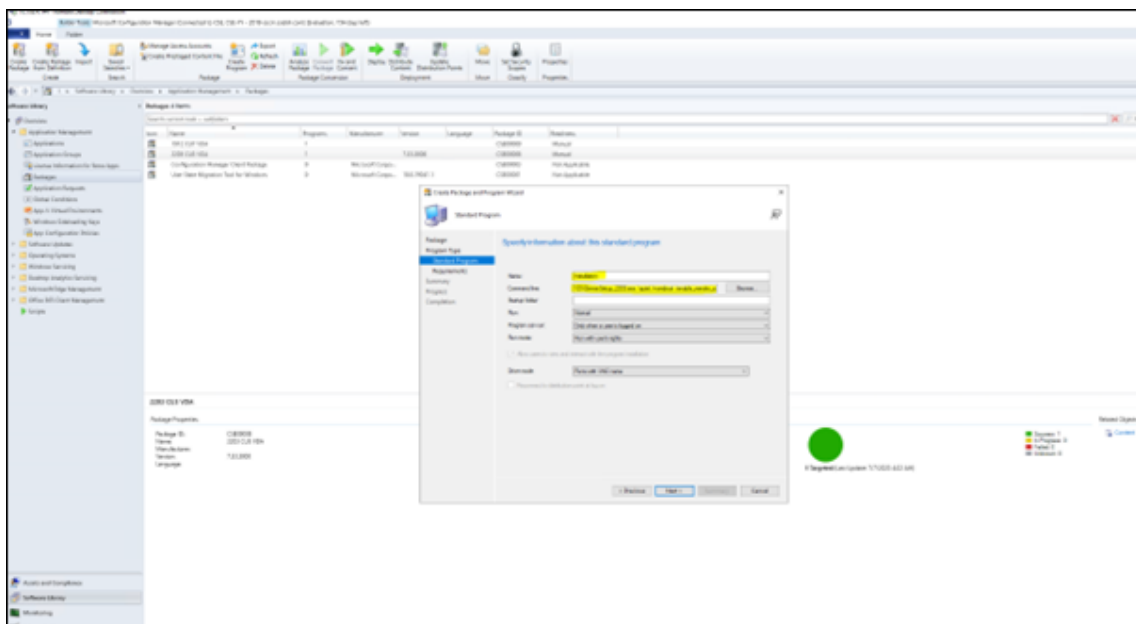
2. Specificare la posizione dei file sorgente per questo pacchetto facendo clic su **Sfoggia**.



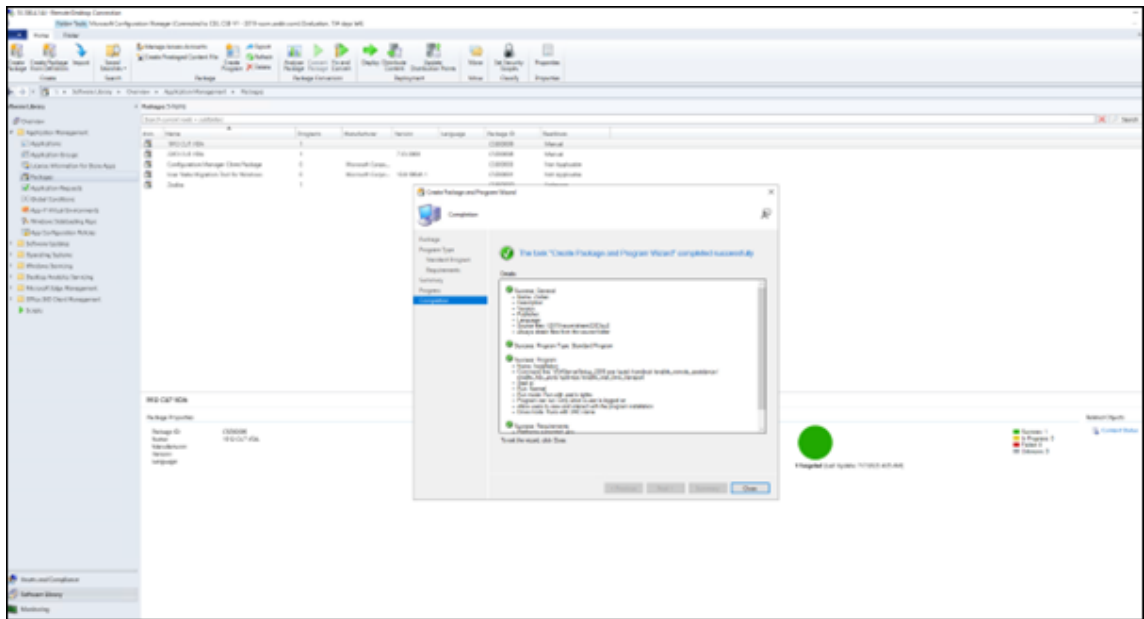
3. Seleziona il tipo di pacchetto desiderato.



4. Immettere il pacchetto **Nome** e **Riga di comando**.



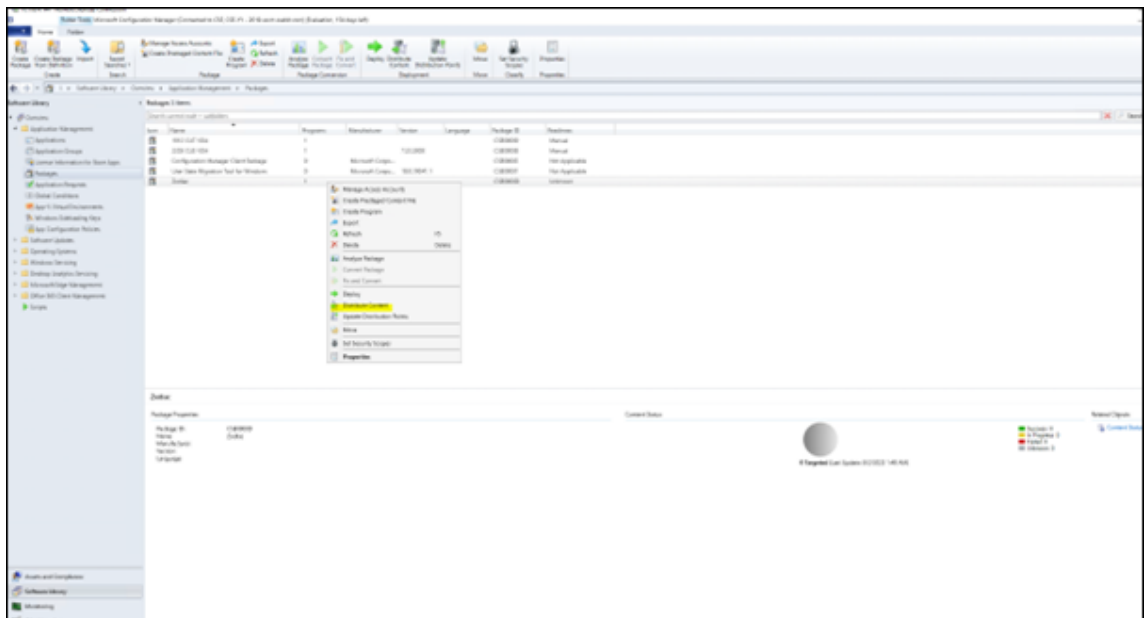
5. Fai clic su **Avanti**.



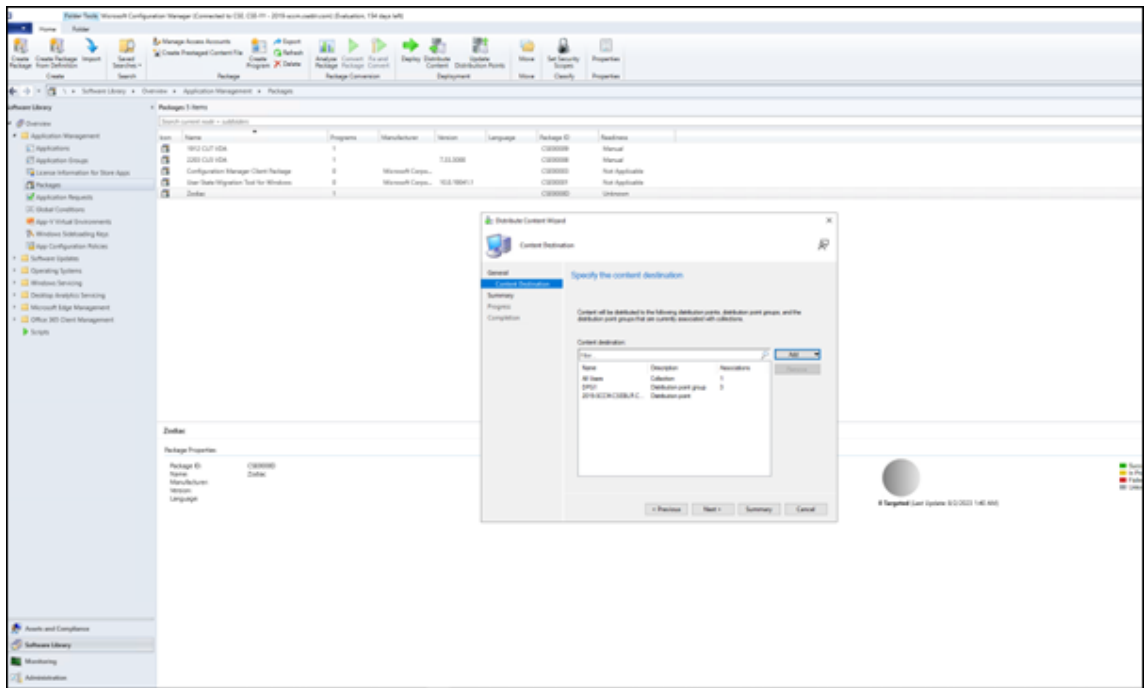
Per informazioni dettagliate, vedere [Pacchetti e programmi in Configuration Manager](#) nella documentazione Microsoft.

Distribuire il contenuto

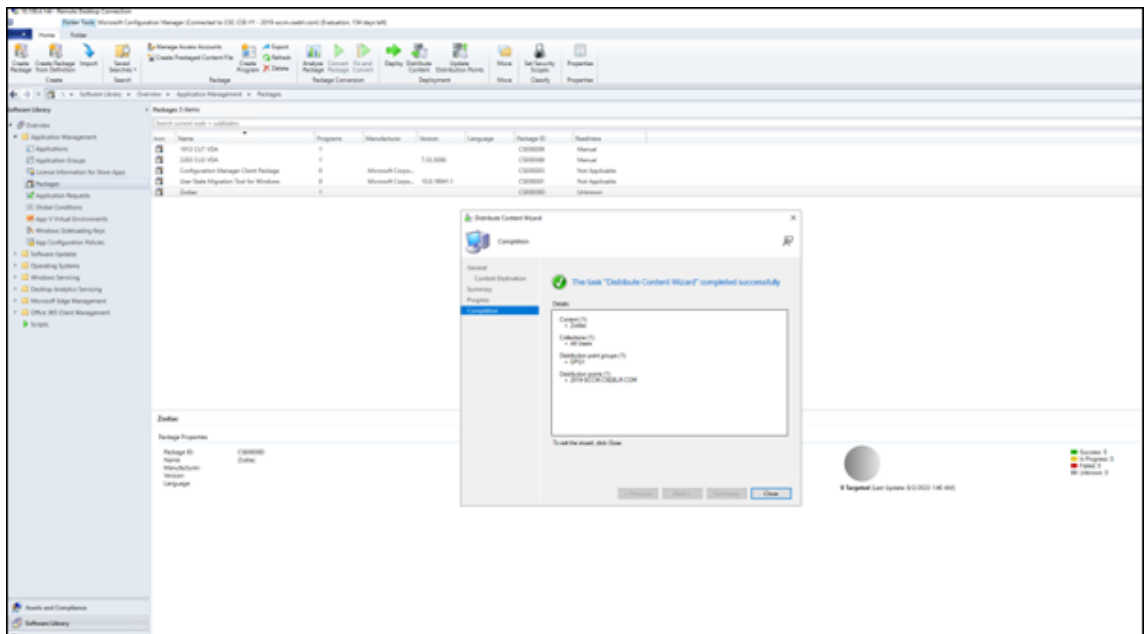
1. Fare clic con il pulsante destro del mouse sul nome del pacchetto creato.
2. Seleziona **Distribuisci contenuto**.



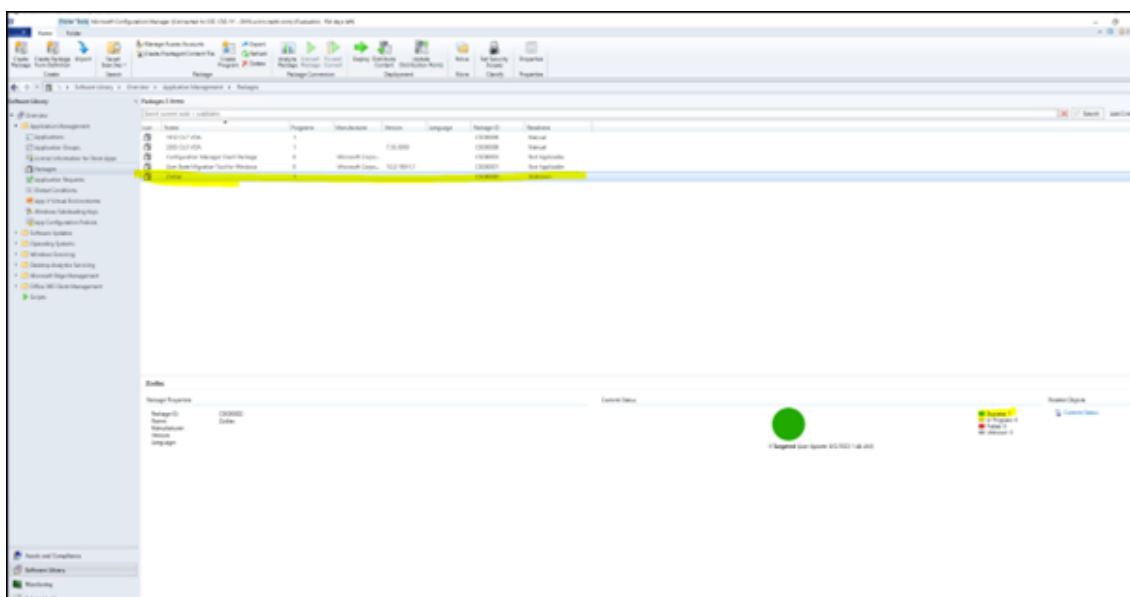
3. Nella finestra **Distribuire Content Wizard**, seleziona il percorso dei file sorgente per il pacchetto che hai creato. In questo esempio, è 2019-SCCM. Fai clic su **Avanti**.



4. Verificare che il pacchetto (in questo esempio, Zodiac) sia disponibile per la distribuzione.



L'immagine seguente illustra che il pacchetto è disponibile per la distribuzione.

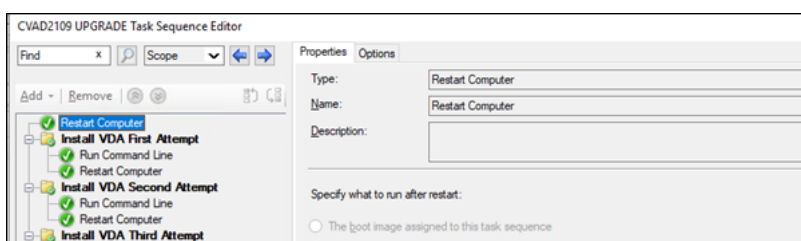


Per informazioni dettagliate, vedere [Distribuire e gestire i contenuti per Configuration Manager](#) nella documentazione Microsoft.

Esempio di sequenza di installazione utilizzando SCCM

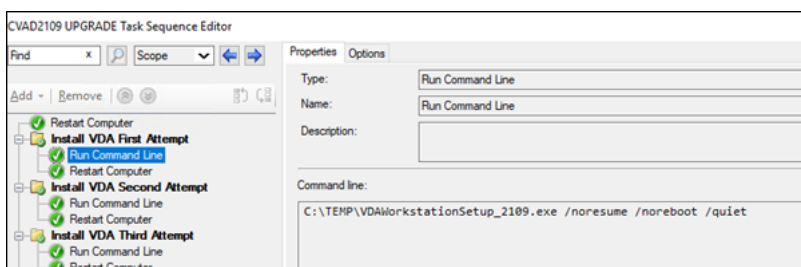
L'esempio seguente mostra la sequenza di installazione.

1. **Riavvia il computer:** Prepara la macchina riavviandola.



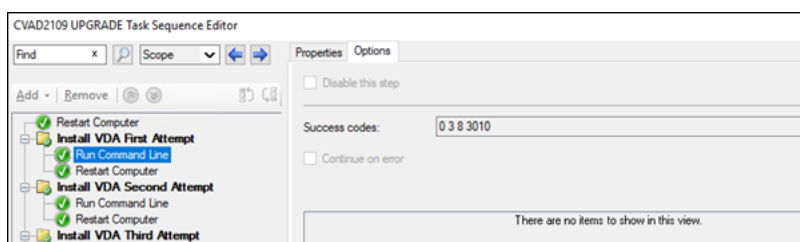
2. **Installa VDA Primo tentativo:** Avvia l'installazione di VDA.

- a) Aggiungere le opzioni `/quiet`, `/noreboot` /`noresume` alle opzioni della riga di comando.
- b) Esegui il programma di installazione VDA di tua scelta (immagine locale o uno dei programmi di installazione minimi).

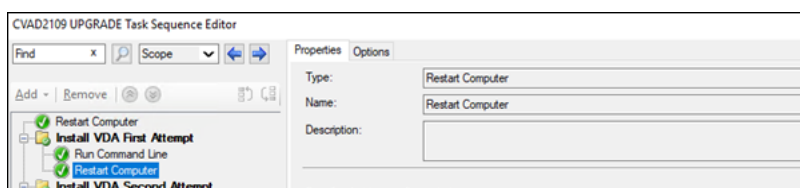


c) SCCM deve catturare il codice di ritorno.

- Se il codice di ritorno è 0 o 8, l'installazione è completa ed è necessario riavviare.

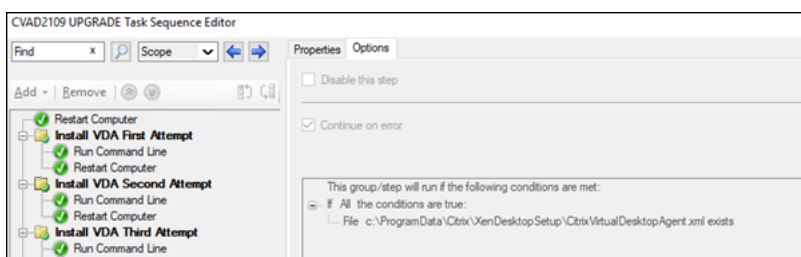


- Se il codice di ritorno è 3, riavvia la macchina e quindi passa il controllo a **Installa VDA Secondo tentativo**.



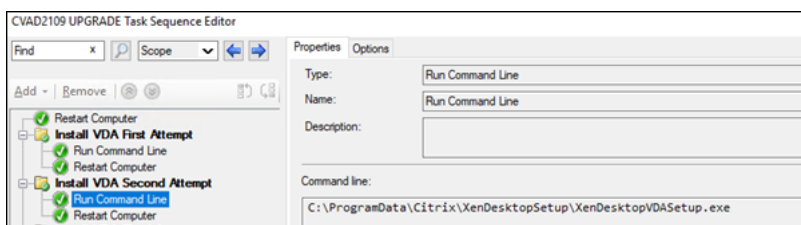
3. **Installa VDA Secondo tentativo:** Continua l'installazione di VDA.

a) Dopo **Installa VDA Primo tentativo** se il file `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` esiste, l'installazione non è completa e deve essere continuata dopo il riavvio.



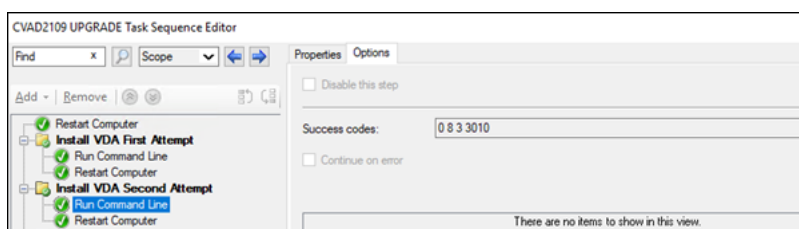
- b) **Installa VDA Secondo tentativo** si ripete finché il file `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` non esiste o viene restituito un codice di ritorno diverso da 0 o 8. Tratta qualsiasi altro codice di ritorno come un errore e **INSTALL VDA SECOND ATTEMPT** dovrebbe segnalare un errore e interrompersi.
- c) Riprendere l'installazione di VDA eseguendo il programma di installazione VDA appropriato (`XenDesktopVdaSetup.exe` nella maggior parte dei casi, o `XenDesktopRemotePCSetup`

.exe se è stato utilizzato `VDAWorkstationCoreSetup_XXXX.exe`) dal file `%programdata%\ Citrix\XenDesktopSetup\` directory senza parametri della riga di comando. (Il programma di installazione VDA utilizza i parametri salvati durante la prima esecuzione del programma di installazione.)



d) Attendere il codice di ritorno del programma di installazione VDA.

- 0 o 8: Successo, installazione completata, è necessario riavviare.



- 3: L'installazione non è completa. Riavviare la macchina e ripetere `INSTALL VDA SECONDO TENTATIVO` finché il file `%programdata%\ Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` non esiste più o finché non viene restituito 0 o 8. Tratta qualsiasi altro codice di ritorno come un errore e `INSTALL VDA SECONDO TENTATIVO` dovrebbe segnalare un errore e terminare.

Per ulteriori informazioni sui codici di ritorno, vedere [Codici di ritorno dell'installazione di Citrix](#).

Esempi di comandi di installazione VDA

Le opzioni di installazione disponibili variano a seconda del programma di installazione utilizzato. Per maggiori dettagli sulle opzioni della riga di comando, consultare i seguenti articoli.

- [Installare VDA](#)
- [Installare tramite riga di comando](#)

Comandi di installazione per l'accesso remoto al PC

- Il seguente comando utilizza il programma di installazione VDA core a sessione singola (`VDAWorkstationCoreSetup.exe`):

```
VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
```

- Il seguente comando utilizza il programma di installazione VDA completo a sessione singola (VDAWorkstationSetup.exe):

```
VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /  
controllers "control.domain.com" /enable_hdx_ports /noresume /  
noreboot
```

Comando di installazione per VDI dedicato

- Il seguente comando utilizza il programma di installazione VDA completo a sessione singola (VDAWorkstationSetup.exe):

```
VDAWorkstationSetup.exe /quiet /components vda /controllers "  
control.domain.com" /enable_hdx_ports /enable_remote_assistance /  
noresume /noreboot
```

Connessione ad AWS

November 5, 2024

[Creare e gestire connessioni e risorse](#) descrive le procedure guidate che creano una connessione. Le seguenti informazioni riguardano i dettagli specifici degli ambienti cloud AWS.

Nota:

Prima di creare una connessione ad AWS, è prima necessario completare la configurazione del proprio account AWS come posizione delle risorse. Vedi [Ambienti cloud AWS](#).

Creare una connessione

Quando si crea una connessione da Web Studio:

- È necessario fornire la chiave API e i valori della chiave segreta. È possibile esportare il file chiave contenente tali valori da AWS e quindi importarli. È inoltre necessario fornire la regione, la zona di disponibilità, il nome del VPC, gli indirizzi delle subnet, il nome di dominio, i nomi dei gruppi di sicurezza e le credenziali.
- Il file delle credenziali per l'account AWS radice (recuperato dalla console AWS) non è formattato come i file delle credenziali scaricati per gli utenti AWS standard. Pertanto, la gestione di Citrix Virtual Apps and Desktops non può utilizzare il file per popolare i campi della chiave API e della chiave segreta. Assicurarsi di utilizzare i file delle credenziali di AWS Identity Access Management (IAM).

Nota:

Dopo aver creato una connessione, i tentativi di aggiornamento della chiave API e della chiave segreta potrebbero non riuscire. Per risolvere il problema, controlla le restrizioni del server proxy o del firewall e assicurati che il seguente indirizzo sia contattabile: https://*.amazonaws.com.

Valori predefiniti della connessione host

Quando si creano connessioni host in ambienti cloud AWS, vengono visualizzati i seguenti valori predefiniti:

Opzione	Valore assoluto	Percentuale
Azioni simultanee (tutti i tipi)	125	100
Numero massimo di nuove azioni al minuto	125	

MCS supporta 100 operazioni di provisioning simultanee massime per impostazione predefinita.

URL dell'endpoint del servizio**URL dell'endpoint del servizio di zona standard**

Quando si utilizza MCS, viene aggiunta una nuova connessione AWS con una chiave API e un segreto API. Con queste informazioni, insieme all'account autenticato, MCS interroga AWS per le zone supportate utilizzando la chiamata API EC2 AWS DescribeRegions. La query viene effettuata utilizzando un URL generico dell'endpoint del servizio EC2 <https://ec2.amazonaws.com/>. Utilizzare MCS per selezionare la zona per la connessione dall'elenco delle zone supportate. L'URL dell'endpoint del servizio AWS preferito viene selezionato automaticamente per la zona. Tuttavia, dopo aver creato l'URL dell'endpoint del servizio, non è più possibile impostarlo o modificarlo.

Definire le autorizzazioni IAM

Utilizzare le informazioni in questa sezione per definire le autorizzazioni IAM per Citrix Virtual Apps and Desktops in AWS. Il servizio IAM di Amazon consente account con più utenti, che possono essere ulteriormente organizzati in gruppi. Questi utenti possono disporre di autorizzazioni diverse per controllare la loro capacità di eseguire operazioni associate all'account. Per ulteriori informazioni sulle autorizzazioni IAM, vedere [Riferimento alla policy JSON IAM](#).

Per applicare la policy delle autorizzazioni IAM a un nuovo gruppo di utenti:

1. Accedi alla console di gestione AWS e seleziona il servizio IAM ** dall'elenco a discesa.
2. Selezionare **Create a New Group of Users** (Crea un nuovo gruppo di utenti).
3. Digitare un nome per il nuovo gruppo di utenti e selezionare **Continue** (Continua).
4. Nella pagina **Permissions** (Autorizzazioni), scegliere **Custom Policy** (Criterio personalizzato). Selezionare **Select** (Seleziona).
5. Digitare un nome per il **criterio Permissions** (Autorizzazioni).
6. Nella sezione **Policy Document** (Documento del criterio), immettere le autorizzazioni pertinenti.

Dopo aver inserito le informazioni sul criterio, selezionare **Continue** (Continua) per completare il gruppo di utenti. Agli utenti del gruppo vengono concesse le autorizzazioni per eseguire solo le azioni richieste per Citrix Virtual Apps and Desktops.

Importante:

Utilizzare il testo del criterio fornito nell'esempio precedente per elencare le azioni utilizzate da Citrix Virtual Apps and Desktops per eseguire azioni all'interno di un account AWS senza limitare tali azioni a risorse specifiche. Citrix consiglia di utilizzare l'esempio a scopo di test. Per gli ambienti di produzione, è possibile scegliere di aggiungere ulteriori restrizioni sulle risorse.

Impostare le autorizzazioni IAM

Impostare le autorizzazioni nella sezione **IAM** della Console di gestione AWS:

1. Nel pannello **Summary** (Riepilogo), selezionare la scheda **Permissions** (Autorizzazioni).
2. Selezionare **Add permissions** (Aggiungi autorizzazioni).

Identity and Access Management (IAM)

- Dashboard
- Access management
 - Groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzer details
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

Search IAM

AWS account ID:

Users > Summary

User ARN: arn:aws:iam::
 Path: /
 Creation time: 2019-07-17 09:59 EST

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Permissions policies (2 policies applied)

Add permissions

Policy name
Attached from group
▶ Billing
▶ AdministratorAccess
▶ Permissions boundary (not set)

Nella schermata **Add Permissions to** (Aggiungi autorizzazioni a), concedere le autorizzazioni:

Add permissions to

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Filter policies	Policy name	Type	Used as
<input type="checkbox"/>	▶ AdministratorAccess	Job function	Permissions policy (8)
<input type="checkbox"/>	▶ AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	▶ AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	▶ AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	▶ AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	▶ AlexaForBusinessReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	▶ AmazonAPIGatewayAdministrator	AWS managed	None
<input type="checkbox"/>	▶ AmazonAPIGatewayInvokeFullAccess	AWS managed	None

Utilizzare il seguente come esempio nella scheda **JSON**:

Create policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:CreateTags",
9         "ec2:DeleteTags",
10        "ec2:DescribeTags",
11        "ec2:PutObjectTagging",
12        "ec2:PutBucketTagging"
13      ],
14      "Resource": "*"
15    },
16    {
17      "Sid": "VisualEditor1",
18      "Effect": "Allow",
19      "Action": "iam:PassRole",
20      "Resource": "arn:aws:iam:*:role/*"
21    }
22  ]
23 }

```

Character count: 304 of 6,144.

Cancel

Review policy

Mancia:

L'esempio JSON indicato potrebbe non includere tutte le autorizzazioni per l'ambiente. Per ulteriori informazioni, consultare l'articolo su come [definire le autorizzazioni di gestione delle identità e degli accessi che eseguono Citrix Virtual Apps and Desktops su AWS](#).

Autorizzazioni AWS richieste

Questa sezione contiene l'elenco completo delle autorizzazioni AWS.

Nota:

L'autorizzazione `iam:PassRole` è necessaria solo per `role_based_auth`.

Creazione di una connessione host

Viene aggiunta una nuova connessione host utilizzando le informazioni provenienti da AWS.

```

1 {
2
3   "Version": "2012-10-17",
4   "Istruzione": [
5     {

```



```
6
7     "Azione": [
8         "ec2:DescribeAvailabilityZones",
9         "ec2:DescribeImages",
10        "ec2:DescribeInstances",
11        "ec2:DescribeInstanceTypes",
12        "ec2:DescribeSecurityGroups",
13        "ec2:DescribeSubnets",
14        "ec2:DescribeVpcs",
15        "ec2:DescribeRegions",
16        "ec2:DescribeSnapshots",
17        "ec2:DescribeLaunchTemplates"
18    ],
19    "Effetto": "Consenti",
20    "Risorsa": "*"
21 }
22
23 ]
24 }
```

Gestione dell'alimentazione delle macchine virtuali

Le istanze delle macchine sono accese o spente.

```
1 {
2
3     "Versione": "2012-10-17",
4     "Istruzione": [
5         {
6
7             "Azione": [
8                 "ec2:AttachVolume",
9                 "ec2:CreateVolume",
10                "ec2>DeleteVolume",
11                "ec2:DescribeInstances",
12                "ec2:DescribeVolumes",
13                "ec2:DetachVolume",
14                "ec2:StartInstances",
15                "ec2:StopInstances"
16            ],
17            "Effetto": "Consenti",
18            "Risorsa": "*"
19        }
20    ]
21 }
22 }
```

Creazione, aggiornamento o eliminazione di macchine virtuali

Un catalogo delle macchine viene creato, aggiornato o eliminato con macchine virtuali di cui viene eseguito il provisioning come istanze AWS.

```

1 {
2
3   «Versione»: «2012-10-17»,
4   «Dichiarazione»: [
5     {
6
7       «Azione»: [
8         «ec2:attachVolume»,
9         «ec2:associateIAMInstanceProfile»,
10        «ec2:AuthorizeSecurityGroupEgress»,
11        «ec2:AuthorizeSecurityGroupIngress»,
12        «ec2:createImage»,
13        «EC2:CreateLaunchTemplate»,
14        «ec2:CreateSecurity Group»,
15        «ec2:CreateTags», «ec2:CreateVolume», «ec2>DeleteVolume
16        », «EC2:DescribeAccountAttributes», ↑ «EC2:
17        DescribeAvailabilityZones», upload"ec2:
18        describeIamInstance Profile Associations», klickr «
19        ec
20
21        2: Descrizione delle immagini»,
22        «EC2: descrizione delle istanze», «ec2: descrizione dei
23        tipi di istanza», ↑ «EC2: descrizione dei modelli
24        di avvio», «ec2: descrizione delle versioni del
25        modello», «ec2: descrizione delle interfacce di rete
26        », «EC2: descrizione delle regioni», ↑ «ec2:
27        descrizione dei gruppi di sicurezza», Istantanee»,
28
29
30        «EC2:describeSubnet»,
31        «EC2:describeTags»,
32        «ec2:describVolumes»,
33        «ec2:describeVPCS», ↑ «ec2:detachVolume», «ec2:
34        dissociateIAMInstanceProfile», «ec2:runInstances», ↑
35        «ec2:startInstances»,
36
37

```

```
38
39         «EC2:terminateInstances»
40     ],
41     «Effect»: «Allow», delete «Resource»: «*» 193 }
42 , {
43 «Action»: [hl «EC2:AuthorizeSecurityGroupEgress», «ec2:
44     AuthorizeSecurityGroupIngress», picture «EC2:CreateSecurityGroup»,
45
46
47
48
49
50
51     "EC2:DeleteSecurityGroup»,
52     «ec2:RevokeSecurityGroupEgress», «EC2:
53     RevokeSecurityGroupIngress», «Effect»: «Allow», ↑ «
54     Resource»: «*» Hull }
55 , column/product/Action: [
56     «S3:createBucket»,
57
58
59
60
61
62     "S3:DeleteBucket»,
63     «S3:putBucketACL», «s3:putBucketTagging», rd« s3:
64     putObject», ▲ «s3:getObject», ↑ «s3:deleteObject»,
65     S3:putObjectTagging», «s3:putObjectTagging», «s3:
66     putObject», ▲ «Effect»: «Allow», «Resource»: «arn:
67     aws:s3: :citriz» x*»
68
69
70
71
72     }
73 ,
74     {
75     break «Action»: [bold «EBS:startSnapshot», «ebs:getSnapshotBlock», ↑ «
76     ebs:putSnapshotBlock», «ebs:completeSnapshot», column «ebs:
77     ListSnapshotBlocks», «ebs:ListSnapshotBlocks», «EC2:createSnapshot»
78
79
80
81
```

```
82
83
84     ],
85     «Effetto»: «Consenti», feriore"Risorsa»: «*» 193 }
```

Nota:

La sezione EC2 relativa ai gruppi di sicurezza è necessaria solo se occorre creare un gruppo di sicurezza di isolamento per la macchina virtuale di preparazione durante la creazione del catalogo. Una volta completata questa operazione, queste autorizzazioni non sono necessarie.

Caricamento e download diretti del disco Il caricamento diretto del disco elimina il requisito del Volume Worker per il provisioning del catalogo delle macchine e utilizza invece le API pubbliche fornite da AWS. Questa funzionalità riduce i costi associati agli account di archiviazione aggiuntivi e alla complessità di gestire le operazioni di Volume Worker.

Nota:

Il supporto di Volume Worker è obsoleto.

Le seguenti autorizzazioni devono essere aggiunte al criterio:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:EliminaSnapshot`
- `ec2:DescribeLaunchTemplates`

Importante:

- È possibile aggiungere una macchina virtuale ai cataloghi delle macchine esistenti senza alcuna operazione di Volume Worker, come l'AMI Volume Worker e la macchina virtuale del Volume Worker.
- Se si elimina un catalogo esistente che utilizzava Volume Worker in precedenza, vengono eliminati tutti gli artefatti, inclusi quelli correlati a Volume Worker.

Crittografia EBS dei volumi creati

EBS può crittografare automaticamente i volumi appena creati se l'AMI è crittografata o EBS è configurato per crittografare tutti i nuovi volumi. Tuttavia, per implementare la funzionalità, è necessario

includere le seguenti autorizzazioni nel criterio IAM.

```
1 {
2
3   "Versione": "2012-10-17",
4   "Istruzione": [
5     {
6
7       "Effetto": "Consenti",
8       "Azione": [
9         "kms:CreateGrant",
10        "kms:Decrypt",
11        "kms:DescribeKey",
12        "kms:GenerateDataKeyWithoutPlainText",
13        "kms:ReEncryptTo",
14        "kms:ReEncryptFrom"
15      ],
16      "Risorsa": "*"
17    }
18  ]
19 }
20 }
```

Nota:

Le autorizzazioni possono essere limitate a chiavi specifiche includendo un blocco di risorse e condizioni a discrezione dell'utente. Ad esempio, **autorizzazioni KMS con condizione:**

```
1 {
2
3   "Versione": "2012-10-17",
4   "Istruzione": [
5     {
6
7       "Effetto": "Consenti",
8       "Azione": [
9         "kms:CreateGrant",
10        "kms:Decrypt",
11        "kms:DescribeKey",
12        "kms:GenerateDataKeyWithoutPlainText",
13        "kms:ReEncryptTo",
14        "kms:ReEncryptFrom"
15      ],
16      "Risorsa": [
17        "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-a123b4cd56ef"
18      ],
19      "Condizione": {
20
21        "Bool": {
22
23          "kms:GrantIsForAWSResource": true
24        }
25      }
26    }
27  ]
28 }
```

```

25
26     }
27
28     }
29
30 ]
31 }

```

La seguente dichiarazione dei criteri chiave è l'intero criterio chiave predefinito per le chiavi KMS necessario per consentire all'account di utilizzare i criteri IAM per delegare l'autorizzazione per tutte le azioni (kms:*) sulla chiave KMS.

```

1 {
2
3   "Sid": "Abilita policy IAM",
4   "Effetto": "Consenti",
5   "Principale": {
6
7     "AWS": "arn:aws:iam::111122223333:root"
8   }
9   ,
10  "Azione": "kms:",
11  "Risorsa": ""
12 }

```

Per ulteriori informazioni, consultare la [documentazione ufficiale di AWS Key Management Service](#).

Autenticazione basata su ruoli IAM

Le seguenti autorizzazioni vengono aggiunte per supportare l'autenticazione basata sui ruoli.

```

1 {
2
3   "Versione": "2012-10-17",
4   "Istruzione": [
5     {
6
7       "Effetto": "Consenti",
8       "Azione": "iam:PassRole",
9       "Risorsa": "arn:aws:iam::*:role/*"
10    }
11  ]
12 }
13 }

```

Criteri minimi delle autorizzazioni IAM

Il seguente JSON può essere utilizzato per tutte le funzionalità attualmente supportate. È possibile creare connessioni host, creare, aggiornare o eliminare macchine virtuali ed eseguire la gestione dell'

alimentazione utilizzando questo criterio. La policy può essere applicata agli utenti come spiegato nelle sezioni Definizione delle autorizzazioni IAM oppure puoi anche utilizzare l'autenticazione basata sui ruoli utilizzando la chiave di sicurezza e la chiave segreta **role_based_auth**.

Importante:

Per utilizzare **role_based_auth**, configura innanzitutto il ruolo IAM desiderato su tutti i Delivery Controller del nostro sito. Utilizzando Web Studio, aggiungere la connessione di hosting e fornire `role_based_auth` per la chiave di autenticazione e il segreto. Una connessione di hosting con queste impostazioni utilizza quindi l'autenticazione basata su ruoli.

```
1 {
2
3   "Versione": "2012-10-17",
4   "Dichiarazione": [
5     {
6
7       "Azione": [
8         "ec2:AttachVolume",
9         "ec2:AssociateIamInstanceProfile",
10        "ec2:AuthorizeSecurityGroupEgress",
11        "ec2:AuthorizeSecurityGroupIngress",
12        "ec2:CreateImage",
13        "ec2:CreateLaunchTemplate",
14        "ec2:CreateNetworkInterface",
15        "ec2:CreateTags",
16        "ec2:CreateVolume",
17        "ec2>DeleteLaunchTemplate",
18        "ec2>DeleteNetworkInterface",
19        "ec2>DeleteSecurityGroup",
20        "ec2>DeleteSnapshot",
21        "ec2>DeleteTags",
22        "ec2>DeleteVolume",
23        "ec2:DeregisterImage",
24        "ec2:DescribeAccountAttributes",
25        "ec2:DescribeAvailabilityZones",
26        "ec2:DescribeIamInstanceProfileAssociations",
27        "ec2:DescribeImages",
28        "ec2:DescribeInstances",
29        "ec2:DescribeInstanceTypes",
30        "ec2:DescribeLaunchTemplates",
31        "ec2:DescribeLaunchTemplateVersions",
32        "ec2:DescribeNetworkInterfaces",
33        "ec2:DescribeRegions",
34        "ec2:DescribeSecurityGroups",
35        "ec2:DescribeSnapshots",
36        "ec2:DescribeSubnets",
37        "ec2:DescribeTags",
38        "ec2:DescribeVolumes",
39        "ec2:DescribeVpcs",
40        "ec2:DetachVolume",
41        "ec2:DisassociateIamInstanceProfile",
```

```
42         "ec2:RebootInstances",
43         "ec2:RunInstances",
44         "ec2:StartInstances",
45         "ec2:StopInstances",
46         "ec2:TerminateInstances"
47     ],
48     "Effetto": "Consenti",
49     "Risorsa": "*"
50 },
51 ,
52 {
53
54     "Azione": [
55         "ec2:AuthorizeSecurityGroupEgress",
56         "ec2:AuthorizeSecurityGroupIngress",
57         "ec2:CreateSecurityGroup",
58         "ec2>DeleteSecurityGroup",
59         "ec2:RevokeSecurityGroupEgress",
60         "ec2:RevokeSecurityGroupIngress"
61     ],
62     "Effetto": "Consenti",
63     "Risorsa": "*"
64 },
65 ,
66 {
67
68     "Azione": [
69         "s3:CreateBucket",
70         "s3>DeleteBucket",
71         "s3>DeleteObject",
72         "s3:GetObject",
73         "s3:PutBucketAcl",
74         "s3:PutObject",
75         "s3:PutBucketTagging",
76         "s3:PutObjectTagging"
77     ],
78     "Effetto": "Consenti",
79     "Risorsa": "arn:aws:s3:::citrix*"
80 },
81 ,
82 {
83
84     "Azione": [
85         "ebs:StartSnapshot",
86         "ebs:GetSnapshotBlock",
87         "ebs:PutSnapshotBlock",
88         "ebs:CompleteSnapshot",
89         "ebs:ListSnapshotBlocks",
90         "ebs:ListChangedBlocks",
91         "ec2:CreateSnapshot"
92     ],
93     "Effetto": "Consenti",
94     "Risorsa": "*"

```



```
95     }
96   ,
97     {
98
99       "Effetto": "Consenti",
100      "Azione": [
101        "kms:CreateGrant",
102        "kms:Decrittografare",
103        "kms:DescribeKey",
104        "kms:GenerateDataKeyWithoutPlainText",
105        "kms:GenerateDataKey",
106        "kms:ReEncryptTo",
107        "kms:ReEncryptFrom"
108      ],
109      "Risorsa": "*"
110    }
111  ,
112    {
113
114      "Effetto": "Consenti",
115      "Azione": "iam:PassRole",
116      "Risorsa": "arn:aws:iam::*:role/*"
117    }
118  ]
119 ]
120 }
```

Nota:

- La sezione EC2 relativa a SecurityGroups è necessaria solo se occorre creare un gruppo di sicurezza di isolamento per la macchina virtuale di preparazione durante la creazione del catalogo. Una volta completata questa operazione, queste autorizzazioni non sono necessarie.
- La sezione KMS è necessaria solo quando si utilizza la crittografia del volume EBS.
- La sezione delle autorizzazioni iam:PassRole è necessaria solo per **role_based_auth**.
- È possibile aggiungere autorizzazioni specifiche a livello di risorsa anziché l'accesso completo in base ai requisiti e all'ambiente. Per maggiori dettagli, consultare i documenti AWS [Demystifying EC2 Resource-Level Permissions](#) (Sfatare i miti relativi alle autorizzazioni a livello di risorsa EC2) e [Gestione degli accessi per le risorse AWS](#).

Passaggi successivi

- Se ci si trova nel processo di distribuzione iniziale, vedere [Creare cataloghi delle macchine](#)
- Per informazioni specifiche su AWS, consulta [Creare un catalogo AWS](#)

Ulteriori informazioni

- [Connessioni e risorse](#)
- [Creare cataloghi di macchine](#)

Connessione a Microsoft Azure

January 24, 2025

Nota:

Da luglio 2023, Microsoft ha rinominato Azure Active Directory (Azure AD) in Microsoft Entra ID. Nel presente documento, qualsiasi riferimento ad Azure Active Directory, Azure AD o AAD fa ora riferimento a Microsoft Entra ID.

[Crea e gestisci connessioni e risorse](#) descrive le procedure guidate che creano una connessione. Le informazioni seguenti 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 dell'account Azure come posizione della risorsa. Vedere [Ambienti cloud di Microsoft Azure Resource Manager](#).

Creare principi di servizio e connessioni

Prima di creare connessioni, è necessario configurare le entità servizio che le connessioni utilizzeranno per accedere alle risorse di Azure. Puoi creare una connessione in due modi:

- Crea un'entità di servizio e una connessione insieme utilizzando Web Studio
- Crea una connessione utilizzando un'entità di servizio creata in precedenza

Questa sezione mostra come completare queste attività:

- [Creare un'entità di servizio e una connessione utilizzando Web Studio](#)
- [Creare un'entità servizio tramite PowerShell](#)
- [Ottieni il segreto dell'applicazione in Azure](#)
- [Crea una connessione utilizzando un'entità di servizio esistente](#)

Considerazioni

- Citrix consiglia di utilizzare Service Principal con ruolo di collaboratore. Tuttavia, vedere la sezione Autorizzazioni minime per ottenere l'elenco delle autorizzazioni minime.
- Quando si crea la prima connessione, Azure chiede di concedere le autorizzazioni necessarie. Per le connessioni future dovrai comunque autenticarti, ma Azure ricorderà il tuo consenso precedente e non visualizzerà più la richiesta.
- Gli account utilizzati per l'autenticazione devono disporre delle autorizzazioni per assegnare ruoli nella sottoscrizione tramite Azure RBAC. Ad esempio, proprietario, amministratore del controllo degli accessi basato sui ruoli o amministratore dell'accesso utente dell'abbonamento.
- L'account utilizzato per l'autenticazione deve essere membro della directory dell'abbonamento. Ci sono due tipi di account di cui essere a conoscenza: "Lavoro o scuola" e "account Microsoft personale". Per i dettagli, vedere [CTX219211](#).
- Sebbene sia possibile utilizzare un account Microsoft esistente aggiungendolo come membro della directory dell'abbonamento, potrebbero verificarsi delle complicazioni se all'utente è stato precedentemente concesso l'accesso come ospite a una delle risorse della directory. In questo caso, potrebbero avere una voce segnaposto nella directory che non concede loro le autorizzazioni necessarie e viene restituito un errore.

Per risolvere il problema, rimuovere le risorse dalla directory e aggiungerle nuovamente in modo esplicito. Tuttavia, è opportuno utilizzare questa opzione con cautela, poiché 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 in realtà ne sono membri. Configurazioni di questo tipo si verificano in genere con account di directory più vecchi. Soluzione alternativa: aggiungere un account alla directory, che assume il valore di appartenenza corretto.
- I gruppi di risorse sono semplicemente contenitori per risorse e possono contenere risorse provenienti da regioni diverse dalla propria. Ciò potrebbe potenzialmente creare confusione se ci si aspetta che le risorse visualizzate nella regione di un gruppo di risorse siano disponibili.
- Assicurati che la tua rete e la tua subnet siano sufficientemente grandi da ospitare il numero di macchine di cui hai bisogno. Ciò richiede una certa lungimiranza, ma Microsoft aiuta a specificare i valori corretti, con indicazioni sulla capacità dello spazio degli indirizzi.

Creare un'entità di servizio e una connessione utilizzando Web Studio

Importante:

Questa funzionalità non è ancora disponibile per gli abbonamenti ad Azure Cina.

Con Web Studio puoi creare sia un'entità servizio sia una connessione in un unico flusso di lavoro. I principi di 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. Per l'applicazione registrata viene creata una chiave segreta (denominata segreto client o segreto dell'applicazione). L'applicazione registrata (in questo caso una connessione) utilizza il segreto client per l'autenticazione ad Azure AD.

Prima di iniziare, assicurati di aver soddisfatto questi prerequisiti:

- Hai un account utente nel tenant di Azure Active Directory del tuo abbonamento.
- Gli account utilizzati per l'autenticazione devono disporre delle autorizzazioni per assegnare ruoli nella sottoscrizione tramite Azure RBAC. Ad esempio, proprietario, amministratore del controllo degli accessi basato sui ruoli o amministratore dell'accesso utente dell'abbonamento.
- Per l'autenticazione disponi delle autorizzazioni di amministratore globale, amministratore dell'applicazione o sviluppatore dell'applicazione. Queste autorizzazioni possono essere revocate dopo aver creato la connessione host. Per ulteriori informazioni sui ruoli, vedere [Ruoli predefiniti di Azure AD](#).

Utilizzare la procedura guidata **Aggiungi connessione e risorse** per creare insieme un'entità servizio e una connessione:

1. Nella pagina **Connessione**, seleziona **Crea una nuova connessione**, il tipo di connessione **Microsoft Azure** e il tuo ambiente Azure.
2. Seleziona gli strumenti da utilizzare per creare le macchine virtuali, quindi seleziona **Avanti**.
3. Nella pagina **Dettagli connessione**, immetti l'ID della tua sottoscrizione di Azure e un nome per la connessione. Dopo aver inserito l'ID dell'abbonamento, il pulsante **Crea nuovo** viene abilitato.

Nota:

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

4. Selezionare **Crea nuovo**, quindi immettere il nome utente e la password dell'account Azure Active Directory.
5. Seleziona **Accedi**.
6. Selezionare **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 **Accetta**, si torna alla pagina **Connessione** della procedura guidata.

Nota:

Dopo aver eseguito correttamente l'autenticazione ad Azure, i pulsanti **Crea nuovo** e **Usa esistente** scompaiono. Viene visualizzato il testo **Connessione riuscita**, con un segno di spunta verde, a indicare la connessione riuscita alla sottoscrizione di Azure.

8. Nella pagina **Dettagli connessione**, seleziona **Avanti**.

Nota:

Non è possibile procedere alla pagina successiva finché non si esegue correttamente l'autenticazione ad Azure e non si acconsente alla concessione delle autorizzazioni richieste.

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

- Nella pagina **Regione**, seleziona una regione.
- Nella pagina **Rete**, procedi come segue:
 - Digitare un nome di risorsa di 1–64 caratteri per facilitare 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 hai più di una rete virtuale con lo stesso nome, l'associazione del nome della rete al gruppo di risorse fornisce combinazioni univoche.) Se la regione selezionata nella pagina precedente non ha reti virtuali, torna a quella pagina e seleziona una regione che abbia reti virtuali.

10. Nella pagina **Riepilogo**, visualizza un riepilogo delle impostazioni e seleziona **Fine** per completare la configurazione.

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

Nell'elenco **Aggiungi connessione e risorse**, seleziona la connessione per visualizzarne i dettagli. La scheda **Dettagli** mostra l'ID applicazione.

Creare un'entità servizio tramite PowerShell

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

Assicurati di avere pronti questi elementi:

- **SubscriptionId:** Azure Resource Manager [SubscriptionID](#) per la sottoscrizione in cui si desidera effettuare 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:

Connettiti al tuo abbonamento ad Azure Resource Manager.

```
1 `Connect-AzAccount`
```

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

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

2. Crea l'applicazione nel tuo tenant AD.

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

3. Creare un'entità di servizio.

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

4. Assegnare un ruolo al servizio principale.

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

5. Dalla finestra di output della console di PowerShell, annotare l'ApplicationId. Tale ID viene fornito durante la creazione della connessione host.

Ottieni il segreto dell'applicazione in Azure

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

I passaggi dettagliati sono i seguenti:

1. Ottieni l'ID applicazione ** da Web Studio o tramite PowerShell.
2. Accedi al portale di Azure.
3. In Azure, seleziona **Azure Active Directory**.
4. Da **Registrazioni app** in Azure AD, seleziona la tua applicazione.
5. Vai a **Certificati & segreti**.
6. Fare clic su **Segreti client**.

Crea una connessione utilizzando un'entità di servizio esistente

Se disponi già di un'entità servizio, puoi utilizzarla per creare una connessione tramite Web Studio.

Assicurati di avere pronti questi elementi:

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

Per ulteriori informazioni, vedere Ottieni il segreto dell'applicazione.

- Data di scadenza segreta

I passaggi dettagliati sono i seguenti:

Nella procedura guidata **Aggiungi connessione e risorse** :

1. Nella pagina **Connessione** , seleziona **Crea una nuova connessione**, il tipo di connessione **Microsoft Azure** e il tuo ambiente Azure.
2. Seleziona gli strumenti da utilizzare per creare le macchine virtuali, quindi seleziona **Avanti**.
3. Nella pagina **Dettagli connessione** , immetti l'ID della tua 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 né i caratteri \ / ; : # . * ? = < > | [] { } " ' () ' .

4. Seleziona **Usa esistente**. Nella finestra **Dettagli del servizio principale esistente** , immettere le seguenti impostazioni per il servizio principale esistente. Dopo aver inserito i dettagli, il pulsante **Salva** viene abilitato. Seleziona **Salva**. Non puoi procedere oltre questa pagina finché non fornisca dati validi.
 - **ID abbonamento**. Inserisci l'ID della tua sottoscrizione Azure. Per ottenere l'ID della sottoscrizione, accedi al portale di Azure e vai a **Sottoscrizioni > Panoramica**.
 - **ID di Active Directory** (ID tenant). Immetti l'ID directory (tenant) dell'applicazione registrata con Azure AD.
 - **ID applicazione**. Immetti l'ID applicazione (client) dell'applicazione registrata con Azure AD.

- **Segreto dell'applicazione.** Creare una chiave segreta (segreto client). L'applicazione registrata utilizza la chiave per l'autenticazione ad Azure AD. Per motivi di sicurezza, ti consigliamo di cambiare regolarmente le chiavi. Assicuratevi di conservare la chiave perché non potrete recuperarla in seguito.
- **Data di scadenza del segreto.** Inserisci la data di scadenza del segreto dell'applicazione. Riceverai un avviso sulla console prima che la chiave segreta scada. Tuttavia, se la chiave segreta scade, si verificano degli errori.

Nota:

Per motivi di sicurezza, il periodo di scadenza non può essere superiore a due anni.

- **URL di autenticazione.** Questo campo viene compilato automaticamente e non è modificabile.
- **URL di gestione.** Questo campo viene compilato automaticamente e non è modificabile.
- **Suffisso di archiviazione.** Questo campo viene compilato automaticamente e non è modificabile.

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

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

5. Dopo aver selezionato **Salva**, tornerai alla pagina **Dettagli connessione**. Selezionare **Avanti** per passare alla pagina successiva.
6. Configurare le risorse per la connessione. Le risorse comprendono la regione e la rete.
 - Nella pagina **Regione**, seleziona una regione.
 - Nella pagina **Rete**, procedi come segue:
 - Digitare un nome di risorsa di 1–64 caratteri per facilitare 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 hai più di una rete virtuale con lo stesso nome, l'associazione del nome della rete al gruppo di risorse fornisce

combinazioni univoche.) Se la regione selezionata nella pagina precedente non ha reti virtuali, torna a quella pagina e seleziona una regione che abbia reti virtuali.

7. Nella pagina **Riepilogo** , visualizza un riepilogo delle impostazioni e seleziona **Fine** per completare la configurazione.

Gestire i principali servizi e le connessioni

Questa sezione descrive in dettaglio come gestire i principali servizi e le connessioni:

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

Configurare le impostazioni di limitazione di Azure

Azure Resource Manager limita le richieste di sottoscrizioni e tenant, instradando il traffico in base a limiti definiti, personalizzati in base alle esigenze specifiche del provider. Per ulteriori informazioni, vedere [Limitazione delle richieste di Resource Manager](#) sul sito Microsoft. Esistono limiti per gli abbonamenti e gli inquilini, per cui la gestione di molte macchine può diventare problematica. Ad esempio, un abbonamento contenente molte macchine potrebbe presentare problemi di prestazioni relativi alle operazioni di alimentazione.

Mancia:

Per ulteriori informazioni, vedere [Miglioramento delle prestazioni di Azure con i servizi di creazione macchine](#).

Per attenuare questi problemi, puoi rimuovere la limitazione interna di MCS per utilizzare una quota maggiore di richieste disponibile da Azure.

Si consigliano le seguenti impostazioni ottimali quando si accendono o spengono le VM in abbonamenti di grandi dimensioni, ad esempio quelli contenenti 1.000 VM:

- Operazioni simultanee assolute: 500
- Numero massimo di nuove operazioni al minuto: 2000
- Concorrenza massima delle operazioni: 500

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

1. In Web Studio, seleziona **Hosting** nel riquadro di sinistra.

2. Selezionare la connessione.
3. Nella procedura guidata **Modifica connessione** , seleziona **Avanzate**.
4. Nella pagina **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.

Edit Connection ×

Azure-08

Connection Properties

Advanced

Scopes

Advanced

Use these settings to specify a maximum number of simultaneous actions (or concurrent machines) per hosting connection. For simultaneous actions, specify both settings. The lower value overrides the higher value. [Learn more](#)

	Absolute	Percentage (%)
Simultaneous actions (all types): ?	<input type="text" value="500"/>	<input type="text" value="100"/>
Maximum new actions per minute:	<input type="text" value="2000"/>	

Connection options:

Use this setting only when Citrix Technical Support or the product documentation makes the recommendation.

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

Utilizzare la proprietà **PowerShell** , `MaximumConcurrentProvisioningOperations`, per specificare il numero massimo di operazioni di provisioning di Azure simultanee. 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 delle immagini in Azure

Durante la creazione o l'aggiornamento dei cataloghi delle macchine, è possibile selezionare immagini condivise da diversi tenant e sottoscrizioni di Azure (condivise tramite Azure Compute Gallery).

Per abilitare la condivisione delle immagini all'interno o tra i tenant, è necessario effettuare le impostazioni necessarie in Azure:

- Condividere immagini all'interno di un tenant (tra gli abbonamenti)
- Condividi le immagini tra i tenant

Condividere immagini all'interno di un tenant (tra gli abbonamenti) Per selezionare un'immagine in Azure Compute Gallery che appartiene a una sottoscrizione diversa, l'immagine deve essere condivisa con l'entità servizio (SPN) di tale sottoscrizione.

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

Principale del servizio: SPN 1

Abbonamento: abbonamento 1

Inquilino: inquilino 1

L'immagine è in un abbonamento diverso, configurato in Studio come:

Abbonamento: abbonamento 2

Inquilino: inquilino 1

Se si desidera condividere l'immagine nell'abbonamento 2 con l'abbonamento 1 (SPN 1), andare all'abbonamento 2 e condividere il gruppo di risorse con SPN1.

L'immagine deve essere condivisa con un altro SPN tramite il controllo degli accessi basato sui ruoli di Azure (RBAC). Azure RBAC è il sistema di autorizzazione utilizzato 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 \(Azure RBAC\)](#). Per concedere l'accesso, assegnare ruoli ai principali servizi nell'ambito del gruppo di risorse con il ruolo di Collaboratore. Per assegnare ruoli di Azure, è necessario disporre dell'autorizzazione `Microsoft.Authorization/roleAssignments/write`, ad esempio Amministratore accesso utente o Proprietario. Per ulteriori informazioni sulla condivisione di immagini con un altro SPN, vedere il documento Microsoft [Assegnare ruoli di Azure tramite il portale di Azure](#).

Per informazioni sulla selezione di un'immagine da un abbonamento diverso tramite comandi di PowerShell, Seleziona un'immagine da un abbonamento diverso.

Condividi le immagini tra i tenant Per condividere immagini tra tenant con Azure Compute Gallery, creare una registrazione dell'applicazione.

Ad esempio, se ci sono due inquilini (Inquilino 1 e Inquilino 2) e desideri condividere la tua galleria di immagini con l'Inquilino 1, allora:

1. Creare una registrazione dell'applicazione per il Tenant 1. Per ulteriori informazioni, vedere [Creare la registrazione dell'app](#).
2. Concedere all'Inquilino 2 l'accesso all'applicazione richiedendo l'accesso tramite un browser. Sostituisci `ID Tenant2` con l'ID tenant del Tenant 1. Sostituisci `ID applicazione (client)` con l'ID applicazione della registrazione dell'applicazione che hai creato. Una volta completate le sostituzioni, incolla l'URL in un browser e segui le istruzioni di accesso per accedere al Tenant 2. Per esempio:

```
1 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 all'inquilino 2 l'accesso](#).

3. Concedere all'applicazione l'accesso al gruppo di risorse Tenant 2. Accedi come Tenant 2 e consenti all'applicazione di accedere al gruppo di risorse contenente l'immagine della galleria. Per ulteriori informazioni, vedere [Autenticare le richieste tra i tenant](#).

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

1. Aggiorna le proprietà personalizzate della connessione di hosting con ID tenant condivisi.
2. Seleziona un'immagine da un tenant diverso.

Aggiungere tenant condivisi a una connessione tramite Web Studio

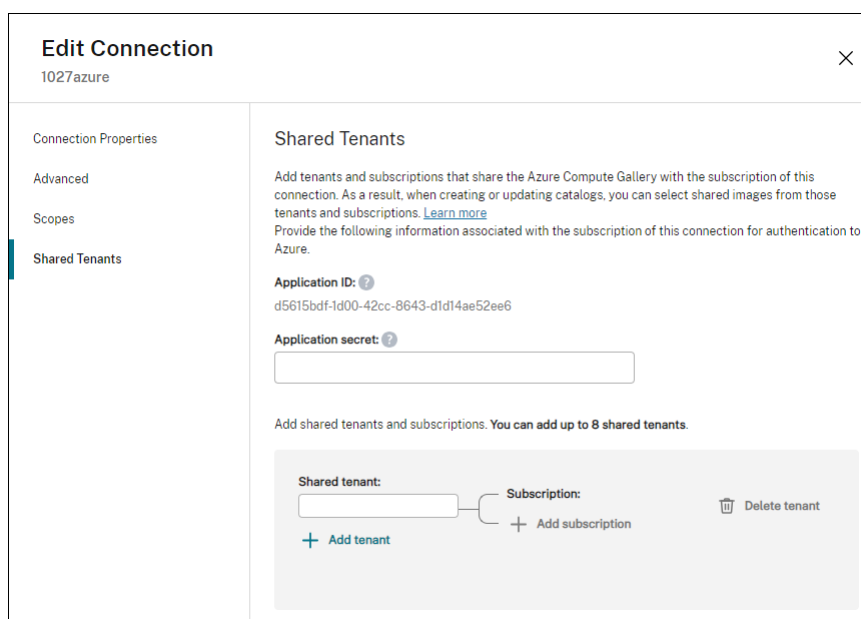
Quando si creano o si aggiornano cataloghi di macchine in Web Studio, è possibile selezionare immagini condivise da diversi tenant e sottoscrizioni di Azure (condivise tramite Azure Compute Gallery). Per questa funzionalità è necessario fornire informazioni condivise sul tenant e sull'abbonamento per le connessioni host associate.

Nota:

Assicurati di aver configurato le impostazioni necessarie in Azure per abilitare la condivisione delle immagini tra i tenant. Per ulteriori informazioni, vedere [Condividere immagini tra tenant](#).

Per effettuare una connessione, completare i seguenti passaggi:

1. In Web Studio, seleziona **Hosting** nel riquadro di sinistra.
2. Selezionare la connessione, quindi selezionare **Modifica connessione** nella barra delle azioni.



3. In **Shared Tenants**, 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 ad Azure AD.
- Aggiungere tenant e sottoscrizioni che condividono Azure Compute Gallery con la sottoscrizione della connessione. È possibile aggiungere fino a 8 tenant condivisi e 8 abbonamenti per ciascun tenant.

4. Una volta terminato, seleziona **Applica** per applicare le modifiche apportate e mantenere la finestra aperta, oppure seleziona **OK** per applicare le modifiche e chiudere la finestra.

Implementare la condivisione delle immagini tramite PowerShell

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

- Seleziona un'immagine da un abbonamento diverso
- Aggiorna le proprietà personalizzate della connessione di hosting con ID tenant condivisi
- Seleziona un'immagine da un tenant diverso

Seleziona un'immagine da un abbonamento diverso È possibile selezionare un'immagine in Azure Compute Gallery che appartiene a una sottoscrizione condivisa diversa nello stesso tenant di Azure per creare e aggiornare i cataloghi MCS utilizzando i comandi di PowerShell.

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

2. Elenca tutti gli abbonamenti condivisi in un tenant.

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

3. Selezionare una sottoscrizione condivisa, quindi elencare tutti i gruppi di risorse condivise di tale sottoscrizione condivisa.

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

4. Seleziona un gruppo di risorse, quindi elenca tutte le gallerie di quel gruppo di risorse.

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

5. Seleziona una galleria, quindi elenca tutte le definizioni delle immagini presenti in quella galleria.

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

6. Seleziona una definizione dell'immagine, quindi elenca tutte le versioni dell'immagine di quella definizione.

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

7. Crea e aggiorna un catalogo MCS utilizzando i seguenti elementi:

- Gruppo di risorse
- Galleria
- Definizione dell'immagine della galleria
- Versione immagine galleria

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

Aggiorna 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 condivisi e ID di sottoscrizione. Aggiungere una proprietà `SharedTenants` in `CustomProperties`. Il formato di `Shared Tenant` è:

```
1 [ {
```

```

2  "Tenant": "94367291-119e-457c-bc10-25337231f7bd", "Subscriptions": [ "7
    bb42f40-8d7f-4230-a920-be2781f6d5d9" ] }
3  , {
4  "Tenant": "50e83564-c4e5-4209-b43d-815c45659564", "Subscriptions": [ "06
    ab8944-6a88-47ee-a975-43dd491a37d0" ] }
5  ]

```

Per esempio:

```

1  Set-Item -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='SubscriptionId' Value='
    123' />
3  <Property xsi:type='StringProperty' Name='ManagementEndpoint'
    Value='https://management.azure.com/' />
4  <Property xsi:type='StringProperty' Name='AuthenticationAuthority'
    Value='https://login.microsoftonline.com/' />
5  <Property xsi:type='StringProperty' Name='StorageSuffix' Value='
    core.windows.net' />
6  <Property xsi:type='StringProperty' Name='TenantId' Value='123
    abc' />
7  <Property xsi:type='StringProperty' Name='SharedTenants' Value='
    [ {
8  'Tenant': '123abc', 'Subscriptions': ['345', '567'] }
9  ]' />
10 </CustomProperties>
11 -LiteralPath @("XDHyp:\Connections\azure") -PassThru -UserName "
    advc345" -SecurePassword
12 $psd

```

Nota:

È possibile aggiungere più di un inquilino. Ogni tenant può avere più di un abbonamento.

Seleziona un'immagine da un tenant diverso È possibile selezionare un'immagine nella Galleria di Azure Compute che appartiene a un tenant di Azure diverso per creare e aggiornare i cataloghi MCS utilizzando i comandi di PowerShell.

1. Nella cartella radice dell'unità di hosting, Citrix crea una nuova cartella di sottoscrizione condivisa denominata `sharedsubscription`.
2. Elenca tutti gli abbonamenti condivisi.

```

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

```

3. Selezionare una sottoscrizione condivisa, quindi elencare tutti i gruppi di risorse condivise di tale sottoscrizione condivisa.

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

4. Seleziona un gruppo di risorse, quindi elenca tutte le gallerie di quel gruppo di risorse.

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

5. Seleziona una galleria, quindi elenca tutte le definizioni delle immagini presenti in quella galleria.

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

6. Seleziona una definizione dell'immagine, quindi elenca tutte le versioni dell'immagine di quella definizione.

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

7. Crea e aggiorna un catalogo MCS utilizzando i seguenti elementi:

- Gruppo di risorse
- Galleria
- Definizione dell'immagine della galleria
- Versione immagine galleria

Per informazioni su come creare un catalogo utilizzando Remote PowerShell SDK, 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

Assicuratevi di modificare il segreto dell'applicazione per una connessione prima che scada. Riceverai un avviso su Web Studio prima che la chiave segreta scada.

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

1. Selezionare **Azure Active Directory**.
2. Da **Registrazioni app** in Azure AD, seleziona la tua applicazione.
3. Vai a **Certificati & segreti**.
4. Fai clic su **Segreti client > Nuovo segreto client**.

5. Fornire una descrizione del segreto e specificarne la durata. Una volta terminato, seleziona **Aggiungi**.

Nota:

Assicurati di salvare il segreto del client perché non potrai recuperarlo in seguito.

6. Copia il valore del segreto client e la data di scadenza.
7. In Web Studio, modifica la connessione corrispondente e sostituisci il contenuto nei campi **Segreto applicazione** e **Data di scadenza del segreto** con i valori copiati.

Cambia 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 **Aggiungi connessione e risorse** , fai clic con il pulsante destro del mouse su una connessione e fai clic su **Modifica connessione**.
2. Nella pagina **Proprietà connessione** , fare clic su **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.

Permessi minimi

Le autorizzazioni minime garantiscono un migliore controllo della sicurezza. Tuttavia, le nuove funzionalità che richiedono autorizzazioni aggiuntive non funzionano perché vengono utilizzate solo le autorizzazioni minime.

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

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

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

```
1 "Microsoft.Compute/virtualMachines/read",
2 "Microsoft.Resources/subscriptions/resourceGroups/read",
3 "Microsoft.Compute/virtualMachines/deallocate/action",
```

```
4 "Microsoft.Compute/virtualMachines/start/action",
5 "Microsoft.Compute/virtualMachines/restart/action",
```

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

Di seguito è riportato l'elenco delle autorizzazioni minime richieste quando l'immagine master è gestita su disco o gli snapshot si trovano nella stessa regione della connessione di hosting.

```
1 "Microsoft.Resources/subscriptions/resourceGroups/read",
2 "Microsoft.Resources/deployments/validate/action",
3 "Microsoft.Compute/virtualMachines/read",
4 "Microsoft.Compute/virtualMachines/write",
5 "Microsoft.Compute/virtualMachines/delete",
6 "Microsoft.Compute/virtualMachines/deallocate/action",
7 "Microsoft.Compute/snapshots/read",
8 "Microsoft.Compute/snapshots/write",
9 "Microsoft.Compute/snapshots/delete",
10 "Microsoft.Compute/snapshots/beginGetAccess/action",
11 "Microsoft.Compute/snapshots/endGetAccess/action",
12 "Microsoft.Compute/disks/read",
13 "Microsoft.Compute/disks/write",
14 "Microsoft.Compute/disks/delete",
15 "Microsoft.Compute/disks/beginGetAccess/action",
16 "Microsoft.Compute/disks/endGetAccess/action",
17 "Microsoft.Network/virtualNetworks/read",
18 "Microsoft.Network/virtualNetworks/subnets/join/action",
19 "Microsoft.Network/virtualNetworks/subnets/read",
20 "Microsoft.Network/networkSecurityGroups/read",
21 "Microsoft.Network/networkSecurityGroups/write",
22 "Microsoft.Network/networkSecurityGroups/delete",
23 "Microsoft.Network/networkSecurityGroups/join/action",
24 "Microsoft.Network/networkInterfaces/read",
25 "Microsoft.Network/networkInterfaces/write",
26 "Microsoft.Network/networkInterfaces/delete",
27 "Microsoft.Network/networkInterfaces/join/action",
```

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

- Se l'immagine master è un VHD in un account di archiviazione situato nella stessa regione della connessione di hosting:

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

- Se l'immagine master è un ImageVersion dalla Galleria immagini condivise:

```
1 "Microsoft.Compute/galleries/read",
2 "Microsoft.Compute/galleries/images/read",
```

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

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

```
1 "Microsoft.Storage/storageAccounts/read",
2 "Microsoft.Storage/storageAccounts/listKeys/action",
3 "Microsoft.Storage/storageAccounts/write",
4 "Microsoft.Storage/storageAccounts/delete",
```

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

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

- Se inserisci l'immagine master nella Galleria immagini condivise:

```
1 "Microsoft.Compute/galleries/write",
2 "Microsoft.Compute/galleries/images/write",
3 "Microsoft.Compute/galleries/images/versions/write",
4 "Microsoft.Compute/galleries/read",
5 "Microsoft.Compute/galleries/images/read",
6 "Microsoft.Compute/galleries/images/versions/read",
7 "Microsoft.Compute/galleries/delete",
8 "Microsoft.Compute/galleries/images/delete",
9 "Microsoft.Compute/galleries/images/versions/delete",
```

- Se utilizzi il supporto host dedicato di Azure:

```
1 "Microsoft.Compute/hostGroups/read",
2 "Microsoft.Compute/hostGroups/write",
3 "Microsoft.Compute/hostGroups/hosts/read",
```

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

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

- Se distribuisce VM utilizzando modelli ARM (profilo macchina):

```
1 "Microsoft.Resources/deployments/write",
2 "Microsoft.Resources/deployments/operationstatuses/read",
3 "Microsoft.Resources/deployments/read",
4 "Microsoft.Resources/deployments/delete",
```

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

```
1 "Microsoft.Resources/templateSpecs/read",
2 "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 VHD e utilizza il

gruppo di risorse fornito dall'amministratore:

```
1 "Microsoft.Resources/subscriptions/resourceGroups/read",
2 "Microsoft.Storage/storageAccounts/delete",
3 "Microsoft.Storage/storageAccounts/listKeys/action",
4 "Microsoft.Storage/storageAccounts/read",
5 "Microsoft.Storage/storageAccounts/write",
6 "Microsoft.Compute/virtualMachines/deallocate/action",
7 "Microsoft.Compute/virtualMachines/delete",
8 "Microsoft.Compute/virtualMachines/read",
9 "Microsoft.Compute/virtualMachines/write",
10 "Microsoft.Resources/deployments/validate/action",
11 "Microsoft.Network/networkInterfaces/delete",
12 "Microsoft.Network/networkInterfaces/join/action",
13 "Microsoft.Network/networkInterfaces/read",
14 "Microsoft.Network/networkInterfaces/write",
15 "Microsoft.Network/networkSecurityGroups/delete",
16 "Microsoft.Network/networkSecurityGroups/join/action",
17 "Microsoft.Network/networkSecurityGroups/read",
18 "Microsoft.Network/networkSecurityGroups/write",
19 "Microsoft.Network/virtualNetworks/subnets/read",
20 "Microsoft.Network/virtualNetworks/read",
21 "Microsoft.Network/virtualNetworks/subnets/join/action"
```

Permesso generale

Il ruolo di collaboratore ha pieno accesso alla gestione di tutte le risorse. Questo set di autorizzazioni non ti impedisce di ottenere nuove funzionalità.

Il seguente set di autorizzazioni garantisce la migliore compatibilità futura, sebbene includa più autorizzazioni di quelle necessarie con l'attuale set di funzionalità:

```
1 "Microsoft.Compute/diskEncryptionSets/read",
2 "Microsoft.Compute/disks/beginGetAccess/action",
3 "Microsoft.Compute/disks/delete",
4 "Microsoft.Compute/disks/endGetAccess/action",
5 "Microsoft.Compute/disks/read",
6 "Microsoft.Compute/disks/write",
7 "Microsoft.Compute/galleries/delete",
8 "Microsoft.Compute/galleries/images/delete",
9 "Microsoft.Compute/galleries/images/read",
10 "Microsoft.Compute/galleries/images/versions/delete",
11 "Microsoft.Compute/galleries/images/versions/read",
12 "Microsoft.Compute/galleries/images/versions/write",
13 "Microsoft.Compute/galleries/images/write",
14 "Microsoft.Compute/galleries/read",
15 "Microsoft.Compute/galleries/write",
16 "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

È possibile configurare facilmente tutte le autorizzazioni minime richieste per un'entità servizio o un account utente in Azure associato 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 servizio di Azure esistente a livello di sottoscrizione.

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

Dove andare dopo

- Se ti trovi nel processo di distribuzione iniziale, consulta [Crea cataloghi macchine](#)
- Per informazioni specifiche su Azure, vedere [Creare un catalogo Microsoft Azure](#)

Ulteriori informazioni

- [Collegamenti 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.

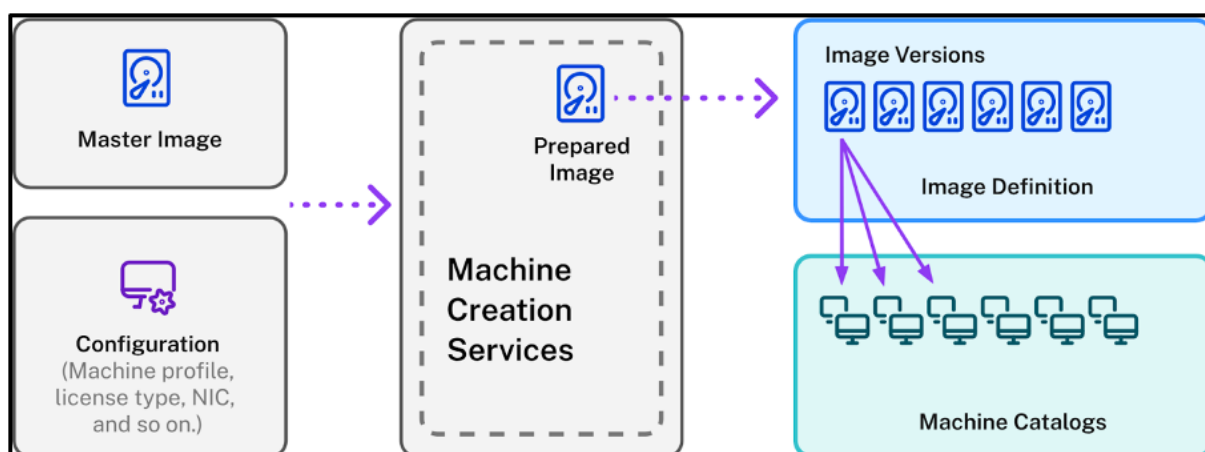
Cos'è un'immagine preparata?

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

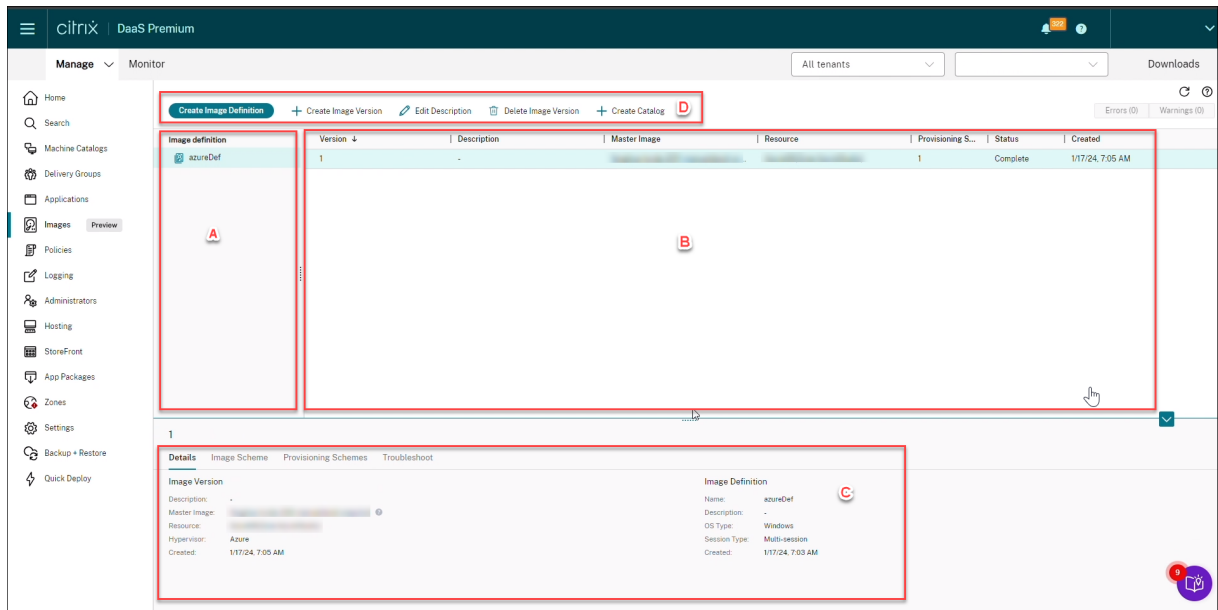
Utilizzare Web Studio

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	<ul style="list-style-type: none"> 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.
D	Barra delle azioni	<p>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).</p>

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 **storage 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**.

Create Image Version

✕

azureDef

- Introduction
- Image
- Storage and License Types
- Machine Specification
- NICs
- Disk Settings
- 7 Summary

Summary

Resources:	azure
Master image:	[REDACTED]
Machine profile:	[REDACTED]
Storage type:	Premium SSD (supports I/O-intensive workloads with significantly high throughput and low latency) [Azure Managed Disks]
License usage:	Use my Windows Server licenses
NICs:	0-Using default
Machine size:	Standard_B2s
Disk encryption set:	/subscriptions/3fd5967-[REDACTED]-2bd5d0cad70c/resourceGroups/ZRJ-MCS/providers/Microsoft.Compute/diskEncryptionSets/^[REDACTED]

Version
2

Description (optional)

Image version description

Back
Finish

Cancel

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.

Specifiche 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
- Gestire 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,

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

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

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

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

```
1 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,

```
1 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,

```
1 New-ProvImageVersionSpec
2 -SourceImageVersionSpecUid c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
3 -NetworkMapping @{
4   "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
   azureresourcegroup.resourcegroup\azure-vnet-eastus.
   virtualprivatecloud\dev.network"
5 -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:

```

1 $ImageDefintion = New-ProvImageDefinition
2 -ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
   MultiSession
3 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
   $ImageDefintion.ImageDefinitionName -Description "version 1"
4 $MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
   azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
5 $SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
   $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
   .ImageVersionNumber -HostingUnitName azure -MasterImagePath
   $MasterImagePath
6 $Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
   $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
7   "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
   azureresourcegroup.resourcegroup\azure-vnet-eastus.
   virtualprivatecloud\dev.network" }
8   -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
9 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:

```

1 $ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
   OsType Windows -VdaSessionSupport SingleSession
2 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
   $ImageDefintion.ImageDefinitionName -Description "version 1"
3 $MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
   master-snap.snapshot"
4 $SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
   $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
   .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
   $MasterImagePath
5 $Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
   $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
6   "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
7   -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
8 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,

```
1 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

```
1 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:

```
1 $Catalog = New-BrokerCatalog -AllocationType "Random" -IsRemotePC
  $False -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -
  PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
  SessionSupport "MultiSession"
2 $IdentityPool = New-AcctIdentityPool -AllowUnicode -Domain "azure.
  local" -IdentityPoolName "azurecatalog" -IdentityType "
  ActiveDirectory" -NamingScheme "azure##" -NamingSchemeType "Numeric
  " -Scope @()
3 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
  ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
  PreparationType -eq 'Mcs'"
4 $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 @{
5  "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
    azureresourcegroup.resourcegroup\azure-vnet-eastus.
    virtualprivatecloud\dev.network" }
6  -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
7  Get-ProvTask -TaskId $Task.TaskId
8  $ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
9  Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid

```

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

```

1  $Catalog = New-BrokerCatalog -AllocationType "Random" -IsRemotePC
    $False -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
2  $IdentityPool = New-AcctIdentityPool -AllowUnicode -Domain "vmware.
    local" -IdentityPoolName "vmwarecatalog" -IdentityType "
    ActiveDirectory" -NamingScheme "vmware###" -NamingSchemeType "
    Numeric" -Scope @()
3  $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
4  $Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
    -Scope @() -SecurityGroup @() -NetworkMapping @{
5  "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
6  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
7  Get-ProvTask -TaskId $Task.TaskId
8  $ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
9  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,

```

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

```

Oppure

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

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

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
   ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
   PreparationType -eq 'Mcs'"
2 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,

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
   ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
   PreparationType -eq 'Mcs'"
2 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,

```
1 $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
```

Gestire 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

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

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

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

Oppure

```
1 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:

```
1 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,

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

Oppure

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

- Per ottenere i dettagli della versione dell'immagine,

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

Oppure

```
1 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,

```
1 Get-ProvImageVersionSpec -ImageVersionId <Guid>
```

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

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

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

```
1 Get-ProvImageVersionSpec -ImageVersionId <Guid> -Filter '
  PreparationType -eq "MCS" -and SourceImageVersionSpecId -
  eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx"'
```

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

```
1 Get-ProvImageVersionSpec -ImageVersionId <Guid> -Filter '
  PreparationType -eq "MCS" -and SourceImageVersionSpecId -
  eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx" -and
  ImageVersionSpecStatus -eq "Complete"'
```

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

```
1 Get-ProvImageVersionSpec -ImageVersionSpecId <Guid>
```

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

```
1 Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
  ProvisioningSchemeId <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:

```
1 Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
  String>] [-ProvisioningSchemeId <Guid>] [-ImageVersionSpecId
  <Guid>] [-ImageVersionSpecHistoryId <Guid>] [-
  ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
  Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
  Guid>]
```

Creare cataloghi di macchine

January 24, 2025

Importante:

A partire da Citrix Virtual Apps and Desktops 7 2006, se la distribuzione corrente utilizza una delle seguenti tecnologie, è possibile aggiornare la distribuzione alla versione corrente solo dopo aver rimosso gli elementi End of Life (EOL) che utilizzano tali tecnologie.

- vDisk personali (PvD)
- AppDisk
- Tipi di host cloud pubblici: Citrix CloudPlatform, Microsoft Azure Classic

Per i dettagli, vedere [Rimuovi PVD, AppDisk e host non supportati](#).

Nota:

È possibile gestire la distribuzione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basata sul Web) e Citrix Studio (basata 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.

Se desideri utilizzare connessioni host cloud pubbliche per la tua distribuzione, ti servirà la licenza Hybrid Rights per completare la nuova installazione o l'aggiornamento alla versione corrente.

Quando il programma di installazione rileva una o più tecnologie non supportate o connessioni host senza licenza Hybrid Rights, l'aggiornamento si interrompe o si interrompe. Appare un messaggio esplicativo. I registri di installazione contengono dettagli. Per ulteriori informazioni, vedere [Aggiornare una distribuzione](#).

Introduzione

Le raccolte di macchine fisiche o virtuali vengono gestite come un'unica entità denominata catalogo macchine. Tutte le macchine in un catalogo hanno lo stesso tipo di sistema operativo: sistema operativo multisezione o sistema operativo monosezione e macchine Windows o Linux.

Web Studio ti guida nella creazione del primo catalogo macchine dopo aver creato il sito. Dopo aver creato il primo catalogo, Web Studio ti guiderà nella creazione del primo gruppo di distribuzione. Successivamente potrai modificare il catalogo creato e crearne altri.

Mancia:

L'aggiornamento di una distribuzione esistente abilita la funzionalità di ottimizzazione dell'

archiviazione (MCS I/O) di Machine Creation Services (MCS), senza che sia richiesta alcuna configurazione aggiuntiva. L'aggiornamento di MCS I/O avviene tramite Virtual Delivery Agent (VDA) e Delivery Controller.

Panoramica

Quando si crea un catalogo di VM, si specifica come effettuare il provisioning di tali VM. È possibile utilizzare Machine Creation Services (MCS). Oppure puoi utilizzare i tuoi utensili per fornire macchine.

Considerare:

- MCS supporta un singolo disco di sistema dall'immagine della macchina virtuale. Ignora il resto dei dischi dati collegati a quell'immagine.
- Se si utilizza MCS per il provisioning delle VM, è necessario fornire un'immagine master (o uno snapshot di un'immagine) per creare VM identiche nel catalogo. Prima di creare il catalogo, è necessario utilizzare gli strumenti per creare e configurare l'immagine master. Questo processo include l'installazione di un Virtual Delivery Agent (VDA) sull'immagine. Quindi si crea il catalogo delle macchine in Web Studio. Si seleziona l'immagine (o l'istantanea), si specifica il numero di VM da creare nel catalogo e si configurano informazioni aggiuntive.
- Se le tue macchine sono già disponibili, devi comunque creare uno o più cataloghi macchine per quelle macchine.
- Se si crea un catalogo utilizzando direttamente PowerShell SDK, è possibile specificare un modello di hypervisor (**VMTemplates**), anziché un'immagine o uno snapshot.
- L'utilizzo di un modello per predisporre un catalogo è considerata una funzionalità sperimentale. Utilizzando questo metodo, la preparazione della macchina virtuale potrebbe non riuscire. Di conseguenza, il catalogo non può essere pubblicato utilizzando il modello.

Quando si utilizza MCS o Citrix Provisioning per creare il primo catalogo, si utilizza la connessione host configurata durante la creazione del sito. Successivamente (dopo aver creato il primo catalogo e il primo gruppo di distribuzione), potrai modificare le informazioni relative a tale connessione o crearne altre.

Dopo aver completato la procedura guidata di creazione del catalogo, vengono eseguiti automaticamente dei test per garantire che la configurazione sia corretta. Una volta completati i test, è possibile visualizzare un report. Esegui i test in qualsiasi momento da Web Studio.

Nota:

MCS non supporta Windows 10 IoT Core e Windows 10 IoT Enterprise. Per ulteriori informazioni, fare riferimento al sito Microsoft .

Per dettagli tecnici sugli strumenti di provisioning Citrix, vedere [Gestione delle immagini di Citrix Virtual Apps and Desktops](#).

Controllo della licenza RDS

Attualmente Web Studio non esegue il controllo delle licenze Microsoft RDS valide durante la creazione di un catalogo macchine contenente macchine con sistema operativo Windows multisesione. Per visualizzare lo stato della licenza Microsoft RDS per una macchina con sistema operativo Windows **multisesione**, vai a Citrix Director. Visualizza lo stato della licenza Microsoft RDS nel pannello **Dettagli macchina**. Questo pannello si trova nella pagina **Dettagli macchina e nella pagina** Dettagli utente. Per ulteriori informazioni, vedere [Stato della licenza Microsoft RDS](#).

Registrazione VDA

Quando si avviano sessioni negoziate, un VDA deve essere registrato presso un Delivery Controller. Le VDA non registrate possono comportare il sottoutilizzo di risorse altrimenti disponibili. Esistono vari motivi per cui un VDA potrebbe non essere registrato, molti dei quali possono essere risolti da un amministratore. Web Studio fornisce informazioni sulla risoluzione dei problemi nella procedura guidata di creazione del catalogo e dopo aver aggiunto macchine da un catalogo a un gruppo di distribuzione.

Dopo aver aggiunto le macchine esistenti tramite la procedura guidata, l'elenco dei nomi degli account computer indica se ciascuna macchina è idonea per essere aggiunta al catalogo. Passando il mouse sull'icona accanto a ogni macchina verrà visualizzato un messaggio informativo sulla macchina stessa.

Se il messaggio identifica una macchina problematica, rimuovere la macchina o aggiungerla. Ad esempio, se un messaggio indica che non è possibile ottenere informazioni su una macchina, aggiungere comunque la macchina.

Per ulteriori informazioni, vedere:

- [CTX136668](#) per la guida alla risoluzione dei problemi di registrazione VDA
- Versioni VDA e livelli funzionali
- [Metodi di registrazione VDA](#)

Riepilogo della creazione del catalogo MCS

Ecco una breve panoramica delle azioni MCS predefinite dopo aver immesso informazioni nella procedura guidata di creazione del catalogo.

- Se è stata selezionata un'immagine master (anziché uno snapshot), MCS crea uno snapshot.
- MCS crea una copia completa dello snapshot e la posiziona in ogni posizione di archiviazione definita nella connessione host.
- MCS aggiunge le macchine ad Active Directory, creando identità univoche.

- MCS crea il numero di VM specificato nella procedura guidata, con due dischi definiti per ciascuna VM. Oltre ai due dischi per VM, nella stessa posizione di archiviazione viene archiviato anche un master. Se sono definite più posizioni di archiviazione, ciascuna ottiene i seguenti tipi di disco:
 - La copia completa dello snapshot, di sola lettura e condivisa tra le VM appena create.
 - Un disco di identità univoco da 16 MB che assegna a ciascuna VM un'identità univoca. Ogni macchina virtuale riceve un disco di identità.
 - Un disco diverso e univoco per memorizzare le scritture effettuate sulla VM. Questo disco è sottoposto a provisioning sottile (se supportato dall'archiviazione host) e aumenta fino alla dimensione massima dell'immagine master, se necessario. Ogni macchina virtuale riceve un disco diverso. Il disco delle differenze contiene le modifiche apportate durante le sessioni. È permanente per i desktop dedicati. Per i desktop in pool, questo viene eliminato e ne viene creato uno nuovo dopo ogni riavvio tramite il delivery controller.

In alternativa, quando si creano VM per distribuire desktop statici, è possibile specificare (nella pagina **Macchine** della procedura guidata di creazione del catalogo) cloni di VM thick (copia completa). I cloni completi non richiedono la conservazione dell'immagine master su ogni archivio dati. Ogni VM ha il suo file.

Considerazioni sullo stoccaggio MCS

Sono molti i fattori da considerare nella scelta delle soluzioni di storage, delle configurazioni e delle capacità per MCS. Le seguenti informazioni forniscono considerazioni adeguate sulla capacità di archiviazione:

Considerazioni sulla capacità:

- Dischi

I dischi Delta o Differenziazione (Diff) consumano la maggiore quantità di spazio nella maggior parte delle distribuzioni MCS per ogni VM. A ogni VM creata da MCS vengono assegnati almeno 2 dischi al momento della creazione.

- Disk0 = Diff Disk: contiene il sistema operativo quando copiato dall'immagine di base master.
- Disk1 = Disco identità: 16 MB - contiene i dati di Active Directory per ogni VM.

Con l'evoluzione del prodotto, potrebbe essere necessario aggiungere più dischi per soddisfare determinati casi d'uso e consumi di funzionalità. Per esempio:

- [L'ottimizzazione dello storage MCS](#) crea un disco in stile cache di scrittura per ogni VM.
- MCS ha aggiunto la possibilità di utilizzare [cloni completi](#) anziché lo scenario del disco Delta descritto nella sezione precedente.

Anche le funzionalità dell'hypervisor potrebbero entrare in gioco. Per esempio:

- [XenServer IntelliCache](#) crea un disco di lettura nell'archiviazione locale per ogni XenServer. Questa opzione consente di risparmiare IOPS rispetto all'immagine master che potrebbe essere conservata nella posizione di archiviazione condivisa.

- Sovraccarico dell'hypervisor

Diversi hypervisor utilizzano file specifici che generano overhead per le VM. Gli hypervisor utilizzano l'archiviazione anche per operazioni di gestione e di registrazione generali. Calcola lo spazio da includere per le spese generali:

- [File di registro](#)
- File specifici dell'hypervisor. Per esempio:
 - * VMware aggiunge altri file alla cartella **di archiviazione della VM** . Vedere [Best practice VMware](#).
 - * Calcola i requisiti di dimensione totale della tua macchina virtuale. Consideriamo una macchina virtuale contenente 20 GB per il disco virtuale, 16 GB per il file di swap e 100 MB per i file di registro, per un totale di 36,1 GB.
- [Snapshot per XenServer](#); [Snapshot per VMware](#).

- Spese generali del processo

La creazione di un catalogo, l'aggiunta di una macchina e l'aggiornamento di un catalogo hanno implicazioni uniche in termini di archiviazione. Per esempio:

- [La creazione iniziale del catalogo](#) richiede che una copia del disco di base venga copiata in ogni posizione di archiviazione.
 - * Richiede inoltre la creazione temporanea di una VM di preparazione .
- [L'aggiunta di una macchina](#) a un catalogo non richiede la copia del disco di base in ogni posizione di archiviazione. La creazione del catalogo varia in base alle funzionalità selezionate.
- [Aggiornamento del catalogo](#) per creare un disco di base extra in ogni posizione di archiviazione. Anche gli aggiornamenti del catalogo subiscono un picco di archiviazione temporaneo, in cui ogni VM nel catalogo ha 2 dischi Diff per un certo periodo di tempo.

Ulteriori considerazioni:

- **Dimensionamento RAM:** Influisce sulla dimensione di determinati file e dischi dell'hypervisor, inclusi i dischi di ottimizzazione I/O, la cache di scrittura e i file snapshot.
- **Provisioning sottile/spessore:** Si preferisce l'archiviazione NFS per le capacità di provisioning sottile.

Ottimizzazione dello storage dei Machine Creation Services (MCS)

Con la funzionalità di ottimizzazione dell'archiviazione Machine Creation Services (MCS), denominata MCS I/O:

- Il contenitore della cache di scrittura è basato su file **, la stessa funzionalità presente in Citrix Provisioning. Ad esempio, il nome del file della cache di scrittura di Citrix Provisioning è `D:\vdiskdif.vhdx` e il nome del file della cache di scrittura di MCS I/O è `D:\mcsdif.vhdx`.
- Ottieni miglioramenti diagnostici includendo il supporto per un file di dump di arresto anomalo di Windows scritto sul disco della cache di scrittura.
- MCS I/O mantiene la tecnologia *cache nella RAM con overflow sul disco rigido* per fornire la soluzione di cache di scrittura multilivello più ottimale. Questa funzionalità consente all'amministratore di bilanciare i costi di ogni livello, RAM e disco, e le prestazioni per soddisfare le aspettative relative al carico di lavoro desiderato.

L'aggiornamento del metodo di cache di scrittura da *basato su disco* a *basato su file* richiede le seguenti modifiche:

1. MCS I/O non supporta più solo la cache RAM. Specificare una dimensione del disco in Web Studio durante la creazione del catalogo macchine.
2. Il disco della cache di scrittura della VM viene creato e formattato automaticamente al primo avvio di una VM. Una volta che la VM è attiva, il file della cache di scrittura `mcsdif.vhdx` viene scritto nel volume formattato `MCSWCDisk`.
3. Il file di paging viene reindirizzato a questo volume formattato, `MCSWCDisk`. Di conseguenza, questa dimensione del disco considera la quantità totale di spazio su disco. Include la differenza tra la dimensione del disco e il carico di lavoro generato, più la dimensione del file di paging. In genere è associato alla dimensione della RAM della VM.

Abilitazione degli aggiornamenti di ottimizzazione dello storage MCS Per abilitare la funzionalità di ottimizzazione dell'archiviazione I/O MCS, aggiornare Delivery Controller e VDA all'ultima versione di Citrix Virtual Apps and Desktops.

Nota:

Se si aggiorna una distribuzione esistente in cui è abilitato MCS I/O, non è richiesta alcuna configurazione aggiuntiva. L'aggiornamento VDA e Delivery Controller gestiscono l'aggiornamento I/O MCS.

Quando si abilita l'aggiornamento dell'ottimizzazione dell'archiviazione MCS, tenere presente quanto segue:

- Durante la creazione di un catalogo macchine, l'amministratore può configurare la RAM e la dimensione del disco.

Machine Catalog Setup

Studio

- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Master Image
- Virtual Machines**
- Computer Accounts
- Summary

Virtual Machines

How many virtual machines do you want to create?

1 - +

Configure your machines.

Total memory (MB) on each machine: 4096 - +

Configure a cache for temporary data on each machine.

Memory allocated to cache (MB): 256 - +

Disk cache size (GB): 10 - +

i Caching should not be enabled if you intend to use this catalog to create AppDisks.
If you clear both check boxes, temporary data is not cached; it is written to the OS storage for each VM. (This is the provisioning action in releases earlier than 7.9.)

Back Next Cancel

- L'aggiornamento di un catalogo macchine esistente a un nuovo snapshot VM contenente un VDA configurato per la versione 1903 genera il seguente comportamento: il nuovo snapshot continua a utilizzare l'impostazione I/O MCS del catalogo esistente per RAM e dimensioni del disco. Il disco raw esistente è formattato.

Importante:

L'ottimizzazione dell'archiviazione MCS è stata modificata con Citrix Virtual Apps and Desktops versione 1903. Questa versione supporta la tecnologia di cache di scrittura basata su file, garantendo migliori prestazioni e stabilità. La nuova funzionalità fornita da MCS I/O potrebbe richiedere un requisito di archiviazione della cache di scrittura più elevato rispetto alle precedenti versioni di Citrix Virtual Apps and Desktops. Citrix consiglia di rivalutare le dimensioni del disco per assicurarsi che disponga di spazio sufficiente per il flusso di lavoro allocato e di dimensioni aggiuntive per il file di paging. La dimensione del file di paging è in genere correlata alla quantità di RAM di sistema. Se la dimensione del disco catalogo esistente non è sufficiente, creare un catalogo macchina e allocare un disco cache di scrittura più grande.

Assegna una lettera di unità specifica al disco cache di write-back I/O MCS

È possibile assegnare una lettera di unità specifica al disco della cache di write-back I/O MCS. Questa implementazione consente di evitare conflitti tra la lettera dell'unità di qualsiasi applicazione utilizzata e la lettera dell'unità del disco della cache di write-back I/O MCS. Per assegnare una lettera di unità al disco cache di write-back I/O MCS, è possibile utilizzare i comandi di PowerShell. Gli hypervisor supportati sono Azure, GCP, VMware, SCVMM e XenServer.

Nota:

Questa funzionalità richiede VDA versione 2305 o successiva.

Limitazioni

- Applicabile solo al sistema operativo Windows
- Lettera di unità applicabile per il disco cache write-back: E a Z
- Non applicabile quando il disco temporaneo di Azure viene utilizzato come disco di cache write-back
- Applicabile solo quando si crea un nuovo catalogo macchine

Assegna una lettera di unità al disco di cache write-back

Per assegnare una lettera di unità a un disco cache write-back:

1. Aprire la finestra **PowerShell**.
2. Esegui `asnp citrix*`.
3. Creare un pool di identità se non è già stato creato.
4. Creare uno schema di provisioning utilizzando il comando `New-ProvScheme` con la proprietà `WriteBackCacheDriveLetter`. Per esempio:

```
1 New-ProvScheme -CleanOnBoot `
2 -HostingUnitName "<name>" `
3 -IdentityPoolName $schemeName `
4 -ProvisioningSchemeName $schemeName `
5 -InitialBatchSizeHint 1 `
6 -UseWriteBackCache -WriteBackCacheDiskSize 127 -
  WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
7 -MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
  resources.resourcegroup\
  MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa145ec77.
  manageddisk" `
8 -NetworkMapping @{
```

```

9  "0"="XDHyp:\\HostingUnits\\name\\virtualprivatecloud.folder\\East
    US.region\\virtualprivatecloud.folder\\abcd-resources.
    resourcegroup\\abcd-resources-vnet.virtualprivatecloud\\
    default.network" }
10  `
11  -ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.
    folder\\Standard_D2s_v5.serviceoffering" `
12  -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
13  <Property xsi:type="StringProperty" Name="UseManagedDisks" Value
    ="true" />
14  <Property xsi:type="StringProperty" Name="OsType" Value="Windows
    " />
15  <Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS"/>
16  <Property xsi:type="StringProperty" Name="PersistWBC" Value="
    false" />
17  <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
    false" />
18  <Property xsi:type="StringProperty" Name="PersistVm" Value="
    false" />
19  <Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="Premium_LRS" />
20  <Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
    Value="false" />
21  <Property xsi:type="StringProperty" Name="ResourceGroups" Value
    ="abcd-group1" />
22  <Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
23  <Property xsi:type="StringProperty" Name="SchemaVersion" Value
    ="2" />
24  </CustomProperties>'

```

5. Completa la creazione del catalogo. Per informazioni, vedere <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>.

Preparare un'immagine master

Per informazioni sulla creazione di connessioni host, vedere [Connessioni e risorse](#).

L'immagine master contiene il sistema operativo, le applicazioni non virtualizzate, VDA e altri software.

Buono a sapersi:

- Un'immagine master può anche essere chiamata immagine clone, immagine golden, VM di base o immagine di base. I fornitori di servizi di hosting utilizzano termini diversi.
- Assicurarsi che l'host disponga di processori, memoria e spazio di archiviazione sufficienti per ospitare il numero di macchine create.

- Configurare la quantità corretta di spazio sul disco rigido necessaria per desktop e applicazioni. Tale valore non potrà essere modificato in seguito né nel catalogo della macchina.
- I cataloghi delle macchine con accesso remoto al PC non utilizzano immagini master.

Installare e configurare il seguente software sull'immagine master:

- Strumenti di integrazione per l'hypervisor (ad esempio Citrix VM Tools, Hyper-V Integration Services o VMware Tools). Se si omette questo passaggio, le applicazioni e i desktop potrebbero non funzionare correttamente.
- Un VDA. Citrix consiglia di installare la versione più recente per poter accedere alle funzionalità più recenti. La mancata installazione di un VDA sull'immagine master determina il fallimento della creazione del catalogo.
- Strumenti di terze parti, se necessario, come software antivirus o agenti di distribuzione elettronica di software. Configurare i servizi con impostazioni adatte agli utenti e al tipo di macchina (ad esempio, l'aggiornamento delle funzionalità).
- Applicazioni di terze parti che non si desidera virtualizzare. Citrix consiglia di virtualizzare le applicazioni. La virtualizzazione riduce i costi eliminando la necessità di aggiornare l'immagine master dopo l'aggiunta o la riconfigurazione di un'applicazione. Inoltre, un minor numero di applicazioni installate riduce le dimensioni dei dischi rigidi dell'immagine master, con conseguente risparmio sui costi di archiviazione.
- Client App-V con le impostazioni consigliate, se si prevede di pubblicare applicazioni App-V. Il client App-V è disponibile da Microsoft.
- Quando si utilizza MCS, se si localizza Microsoft Windows, installare le versioni locali e i pacchetti di lingua. Durante il provisioning, quando viene creato uno snapshot, le VM provisionate utilizzano le impostazioni locali e i pacchetti di lingua installati.

Importante:

Se si utilizza MCS, non eseguire Sysprep sulle immagini master.

Per preparare un'immagine master:

1. Utilizzando lo strumento di gestione dell'hypervisor, crea un'immagine master e quindi installa il sistema operativo, oltre a tutti i service pack e gli aggiornamenti. Specificare il numero di vCPU. È anche possibile specificare il valore vCPU se si crea il catalogo macchine tramite PowerShell. Non è possibile specificare il numero di vCPU quando si crea un catalogo tramite Web Studio. Configura la quantità di spazio sul disco rigido necessaria per desktop e applicazioni. Tale valore non potrà essere modificato in seguito né nel catalogo.
2. Assicurarsi che il disco rigido sia collegato alla posizione 0 del dispositivo. La maggior parte dei modelli di immagini master standard configurano questa posizione per impostazione predefinita, ma alcuni modelli personalizzati potrebbero non farlo.
3. Installare e configurare il software elencato sopra sull'immagine master.

4. Se non si utilizza MCS, unire l'immagine master al dominio di cui sono membri le applicazioni e i desktop. Assicurarsi che l'immagine master sia disponibile sull'host in cui vengono create le macchine. Se si utilizza MCS, non è necessario unire l'immagine master a un dominio. Le macchine fornite vengono aggiunte al dominio specificato nella procedura guidata di creazione del catalogo.
5. Citrix consiglia di creare e denominare uno snapshot dell'immagine master. Se durante la creazione di un catalogo si specifica un'immagine master anziché uno snapshot, Web Studio crea uno snapshot. Non puoi dargli un nome.

Attivazione delle licenze di volume

MCS supporta l'attivazione di licenze multilicenza per automatizzare e gestire l'attivazione dei sistemi operativi Windows e di Microsoft Office. I tre modelli supportati da MCS per l'attivazione delle licenze volume sono:

- Servizio di gestione delle chiavi (KMS)
- Attivazione basata su Active Directory (ADBA)
- Chiave di attivazione multipla (MAK)

È possibile modificare le impostazioni di attivazione dopo aver creato il catalogo macchine.

Servizio di gestione delle chiavi (KMS)

Il KMS è un servizio leggero che non richiede un sistema dedicato e può essere facilmente co-ospitato su un sistema che fornisce altri servizi. Questa funzionalità è supportata su tutte le versioni di Windows supportate da Citrix. Durante la preparazione delle immagini, MCS esegue il riarmo di Microsoft Windows e Microsoft Office KMS. È possibile saltare il riarmo eseguendo il comando `Set-Provserviceconfigurationdata`. Per ulteriori informazioni su Microsoft Windows KMS Rearm e Microsoft Office KMS Rearm durante la preparazione dell'immagine, vedere [Machine Creation Services: panoramica sulla preparazione dell'immagine e individuazione degli errori](#). Per ulteriori informazioni sull'attivazione KMS, vedere [Attivazione tramite Key Management Service](#).

Nota:

Tutti i cataloghi macchina creati dopo l'esecuzione del comando `Set-Provserviceconfigurationdata` hanno la stessa impostazione fornita nel comando.

Attivazione basata su Active Directory (ADBA)

ADBA consente di attivare le macchine tramite le relative connessioni di dominio. Le macchine vengono attivate immediatamente quando si uniscono al dominio. Queste macchine rimangono attive

finché rimangono collegate al dominio e in contatto con esso. Questa funzionalità è supportata su tutte le versioni di Windows supportate da Citrix. Per ulteriori informazioni sull'attivazione basata su Active Directory, vedere Attivazione tramite [Attivazione basata su Active Directory](#).

Chiave di attivazione multipla (MAK)

MAK è un modo per attivare il volume e autenticare il sistema Windows con l'aiuto del server Microsoft. È necessario acquistare la chiave MAK da Microsoft, a cui viene assegnato un numero fisso di attivazioni. Ogni volta che viene attivato un sistema Windows, il conteggio delle attivazioni diminuisce. Esistono due modi per attivare il sistema:

- Attivazione online: se il sistema Windows che si desidera attivare ha accesso a Internet, il sistema attiva automaticamente Windows durante l'installazione della chiave prodotto. Questo processo riduce di 1 il conteggio delle attivazioni per il MAK corrispondente.
- Attivazione offline: se il sistema Windows non è in grado di connettersi a Internet per effettuare l'attivazione online, MCS riceve un ID di conferma e un ID di installazione dal server Microsoft per attivare il sistema Windows. Questo metodo di attivazione è utile per i cataloghi di macchine non persistenti.

Nota:

- MCS non supporta l'attivazione di Microsoft Office tramite MAK.
- La versione VDA minima richiesta è 2303.

Requisiti chiave

- Il Delivery Controller deve avere accesso a Internet.
- Creare un nuovo catalogo se la nuova immagine da aggiornare ha una chiave MAK diversa dall'originale.
- Installare la chiave MAK sull'immagine master. Consultare [Distribuisci attivazione MAK](#) per i passaggi necessari per installare la chiave MAK su un sistema Windows.
- Se non si utilizza la preparazione delle immagini:
 1. Aggiungere il valore DWORD del registro `Manuale` in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.
 2. Imposta il valore su 1.

Conteggi di attivazione Per visualizzare il numero di attivazioni rimanenti per la chiave MAK o per verificare se una VM sta consumando due o più attivazioni, utilizzare Volume Activation Management Tool (VAMT). Vedere [Installa VAMT](#).

Attivare il sistema Windows tramite MAK Per attivare il sistema Windows tramite MAK:

1. Installare la chiave del prodotto sull'immagine master. Questo passaggio consuma un conteggio di attivazione.
2. Creare un catalogo macchine MCS.
3. Se non si utilizza la preparazione delle immagini:
 - a) Aggiungere il valore DWORD del registro `Manuale` in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.
 - b) Imposta il valore su 1.

Questo metodo disabilita l'opzione di attivazione online.

4. Aggiungere VM al catalogo macchine.
5. Accendere le VM.
6. A seconda che l'attivazione avvenga online o offline, viene attivato il sistema Windows.
 - Se l'attivazione avviene online, il sistema Windows viene attivato dopo l'installazione della chiave prodotto.
 - Se l'attivazione avviene offline, MCS comunica con le VM fornite per ottenere lo stato di attivazione del sistema Windows. MCS recupera quindi un ID di conferma e un ID installato dal server Microsoft. Questi ID vengono utilizzati per attivare il sistema Windows.

Risoluzione dei problemi Se la VM fornita non è attivata con la chiave MAK installata, eseguire il comando `Get-ProvVM` o `Get-ProvScheme` in una finestra di PowerShell.

- Comando `Get-ProvScheme` : vedere il parametro `WindowsActivationType` associato al catalogo macchine MCS dall'ultima immagine master.
- Il comando `Get-ProvVM`. Vedere i parametri `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

Puoi controllare l'errore e verificare i passaggi per risolvere il problema.

Creare un catalogo macchine utilizzando Web Studio

Prima di creare un catalogo:

- Rivedi questa sezione per saperne di più sulle scelte che fai e sulle informazioni che fornisci.
- Assicurati di aver creato una connessione all'hypervisor, al servizio cloud e ad altre risorse che ospitano i tuoi computer.

- Se hai creato un'immagine master per il provisioning delle macchine, assicurati di aver installato un VDA su tale immagine.

Per avviare la procedura guidata di creazione del catalogo:

1. Se questo è il primo catalogo creato, verrai indirizzato alla selezione corretta (ad esempio “Configura le macchine e crea cataloghi macchine per eseguire app e desktop”). Si apre la procedura guidata per la creazione del catalogo.
2. Se hai già creato un catalogo e vuoi crearne un altro, segui questi passaggi:
 - a) Accedi a Web Studio, seleziona **Cataloghi macchine** nel riquadro a sinistra, quindi seleziona **Crea catalogo macchine** nella barra delle azioni.
 - b) Per organizzare i cataloghi utilizzando le cartelle, creare cartelle nella cartella predefinita **Machine Catalogs** . Per ulteriori informazioni, vedere [Creare una cartella catalogo](#).
 - c) Seleziona la cartella in cui vuoi creare il catalogo, quindi fai clic su **Crea catalogo macchina**. Si apre la procedura guidata per la creazione del catalogo.

La procedura guidata ti guiderà attraverso le seguenti voci. Le pagine della procedura guidata visualizzate variano a seconda delle selezioni effettuate.

Sistema operativo

Ogni catalogo contiene macchine di un solo tipo. Selezionane una.

- **Sistema operativo multisessione:** Un catalogo di sistemi operativi multisessione fornisce desktop condivisi ospitati. Le macchine possono eseguire versioni supportate dei sistemi operativi Windows o Linux, ma il catalogo non può contenerli entrambi. (Per maggiori dettagli su questo sistema operativo, consultare la documentazione Linux VDA.)
- **Sistema operativo a sessione singola:** Un catalogo di sistemi operativi a sessione singola fornisce desktop VDI che è possibile assegnare a vari utenti diversi.
- **Accesso PC remoto:** Un catalogo di accesso PC remoto fornisce agli utenti l'accesso remoto ai loro computer desktop fisici in ufficio. L'accesso remoto al PC non richiede una VPN per garantire la sicurezza.

Gestione delle macchine

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso PC remoto.

La pagina **Gestione macchine** indica come vengono gestite le macchine e quali strumenti utilizzare per distribuirle.

Scegliere se l'alimentazione delle macchine nel catalogo debba essere gestita tramite Web Studio.

- L'alimentazione delle macchine avviene tramite Web Studio, ad esempio macchine virtuali o PC blade. Questa opzione è disponibile solo se hai già configurato una connessione a un host.
- Le macchine, ad esempio le macchine fisiche, non sono gestite elettricamente tramite Web Studio.

Se hai indicato che l'alimentazione delle macchine è gestita tramite Web Studio, scegli quale strumento utilizzare per creare le VM.

- **Tecnologia di provisioning Citrix**

- **Citrix Machine Creation Services (MCS)** Crea un catalogo di VM fornite e di cui è stata creata l'immagine tramite MCS. MCS copia le immagini clonate da un'immagine master su quelle VM.
- **Citrix Provisioning Services (PVS)** Crea un catalogo di VM fornite tramite MCS e di cui è stata creata l'immagine tramite PVS. Tali VM fungono da dispositivi di destinazione PVS e il server PVS può trasmettere in streaming su di esse un'unica immagine disco condivisa.

Nota:

Questa opzione è disponibile solo per i siti PVS registrati con Citrix Cloud e attualmente è limitata alle risorse di Azure.

- **Altro servizio o tecnologia** Uno strumento che gestisce le macchine già presenti nel data center. Citrix consiglia di utilizzare Microsoft System Center Configuration Manager o un'altra applicazione di terze parti per garantire la coerenza delle macchine nel catalogo.

Tipi di desktop (esperienza desktop)

Questa pagina viene visualizzata solo quando si crea un catalogo contenente macchine con sistema operativo a sessione singola.

La pagina **Esperienza desktop** determina cosa accade ogni volta che un utente effettua l'accesso. Seleziona uno dei:

- Ogni volta che effettuano l'accesso, gli utenti si collegano a un nuovo desktop (casuale).
- Ogni volta che accedono, gli utenti si collegano allo stesso desktop (statico).

Immagine e profilo macchina

Questa pagina viene visualizzata solo quando si utilizza MCS per creare VM.

1. Selezionare un tipo di immagine per il catalogo macchine, quindi selezionare un'immagine. Sono disponibili due tipi di immagine:

- **Immagine principale.** Un'immagine che non ha ancora superato il processo di preparazione. Il processo di preparazione delle immagini viene avviato automaticamente quando inizia la creazione del catalogo.

Nota:

- Quando si utilizza MCS, non eseguire Sysprep sulle immagini master.
- Se si specifica un'immagine master anziché uno snapshot, Web Studio crea uno snapshot, ma non è possibile assegnargli un nome.

- **Prepared image.** An image that has gone through the image preparation process and can be used for VM creation directly. Opting for prepared images rather than master images during catalog creation ensures faster and more reliable machine catalog creation, along with streamlined image lifecycle management.

```

1 > **Note:**
2 >
3 > - VMs created using prepared images don't support
  hibernation.
4 > - Currently, creating catalogs using prepared images are
  available only in Azure and VMware environments.
```

Per maggiori informazioni su come creare immagini preparate, vedere [Gestione delle immagini \(anteprima\)](#).

Quando selezioni un'immagine, se necessario puoi aggiungere una nota all'immagine selezionata.

Per consentire l'utilizzo delle funzionalità più recenti del prodotto, assicurarsi che nell'immagine master sia installata la versione VDA più recente. Non modificare la selezione VDA minima predefinita. Tuttavia, se è necessario utilizzare una versione VDA precedente, vedere Versioni VDA e livelli funzionali.

Se si seleziona uno snapshot o una VM non compatibile con la tecnologia di gestione delle macchine selezionata in precedenza nella procedura guidata, viene visualizzato un messaggio di errore.

2. Per utilizzare una VM esistente come profilo macchina, selezionare **Usa un profilo macchina**, quindi selezionare la VM.

Nota:

Attualmente, l'utilizzo dei profili macchina è limitato alle VM di Azure, AWS, GCP e VMware.

Per le distribuzioni VMware, quando si crea un catalogo macchine utilizzando un profilo macchina, è necessario specificare la cartella in cui si desidera conservare le macchine virtuali.

Per specificare il percorso della cartella della macchina virtuale, nella procedura guidata di creazione del catalogo, vai alla pagina **Macchine virtuali**, quindi vai alla sezione **Seleziona una cartella in cui posizionare le macchine** e seleziona il percorso della cartella della macchina virtuale. Se non specificato, il sistema considera come posizione predefinita la cartella del profilo macchina selezionato.

3. Selezionare il livello funzionale minimo per il catalogo. Per consentire l'utilizzo delle funzionalità più recenti del prodotto, assicurarsi che nell'immagine master sia installata la versione VDA più recente.

Macchine

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso PC remoto.

Il titolo di questa pagina dipende da cosa hai selezionato nella pagina **Gestione macchine: Macchine, Macchine virtuali o VM e utenti**.

Quando si utilizza MCS:

- Specificare quante macchine virtuali creare. Inserisci **0** (zero) se non vuoi crearne nessuno. Successivamente, puoi creare VM per un catalogo vuoto eseguendo **Aggiungi macchine**.
- Seleziona la quantità di memoria (in MB) di cui dispone ogni VM.
- Ogni VM creata ha un disco rigido. La sua dimensione è impostata nell'immagine master. Non è possibile modificare la dimensione del disco rigido nel catalogo.
- Se la distribuzione contiene più di una zona, è possibile selezionarne una per il catalogo.
- Se si creano VM desktop statiche, selezionare una modalità di copia della macchina virtuale. Vedere Modalità di copia della macchina virtuale.
- Se si creano VM desktop casuali che non utilizzano vDisk, è possibile configurare una cache da utilizzare per i dati temporanei su ciascuna macchina. Vedere Configurare la cache per i dati temporanei.

Quando si utilizzano altri strumenti:

Aggiungere (o importare un elenco di) nomi di account macchina Active Directory. È possibile modificare il nome dell'account Active Directory per una VM dopo averla aggiunta/importata. Se hai specificato macchine statiche nella pagina **Esperienza desktop**, puoi facoltativamente specificare il nome utente di Active Directory per ogni VM aggiunta.

Dopo aver aggiunto o importato i nomi, puoi utilizzare il pulsante **Rimuovi** per eliminare i nomi dall'elenco, mentre sei ancora su questa pagina.

Quando si utilizzano altri strumenti (ma non MCS):

Un'icona e una descrizione comandi per ogni macchina aggiunta (o importata) aiutano a identificare le macchine che potrebbero non essere idonee per l'aggiunta al catalogo o che non possono essere

registrate con un Delivery Controller. Per i dettagli, vedere versioni VDA e livelli funzionali.

Aggiungere SID durante la creazione di macchine virtuali

Ora puoi aggiungere il parametro `ADAccountSid` per identificare in modo univoco le macchine durante la creazione di nuove macchine virtuali.

Per fare questo:

1. Creare un catalogo con il tipo di identità supportato.
2. Aggiungere macchine al catalogo utilizzando `NewProvVM`. Per esempio:

```
1 New-ProvVM -ProvisioningSchemeName "name" -ADAccountSid @"SID") -RunAsynchronously
```

Tuttavia, non è possibile predisporre una macchina con:

- Un account AD che non è nel pool di identità del catalogo
- Un account AD che non è disponibile

Modalità di copia della macchina virtuale

La modalità di copia specificata nella pagina **Macchine** determina se MCS crea cloni sottili (copia veloce) o spessi (copia completa) dall'immagine master. (Default = cloni sottili)

- Utilizza cloni di copia rapida per un utilizzo più efficiente dello storage e una creazione più rapida delle macchine.
- Utilizzare cloni di copie complete per un migliore supporto al recupero e alla migrazione dei dati, con IOPS potenzialmente ridotti dopo la creazione delle macchine.

Versioni VDA e livelli funzionali

Il livello funzionale di un catalogo controlla quali caratteristiche del prodotto sono disponibili per le macchine nel catalogo. Per utilizzare le funzionalità introdotte nelle nuove versioni del prodotto è necessario un nuovo VDA. Impostando un livello funzionale, tutte le funzionalità introdotte in quella versione (e in quelle successive, se il livello funzionale non cambia) diventano disponibili per le macchine presenti nel catalogo. Tuttavia, le macchine presenti in quel catalogo con una versione VDA precedente non possono registrarsi.

Un menu nella parte inferiore della pagina **Macchine** (o **Dispositivi**) consente di selezionare il livello VDA minimo. Imposta il livello funzionale minimo del catalogo. Per impostazione predefinita, per le

distribuzioni on-premise viene selezionato il livello funzionale più aggiornato. Se si segue la raccomandazione di Citrix di installare e aggiornare sempre i VDA e i componenti principali alla versione più recente, non è necessario modificare questa selezione. Tuttavia, se è necessario continuare a utilizzare versioni VDA precedenti, selezionare il valore corretto.

Una versione di Citrix Virtual Apps and Desktops potrebbe non includere una nuova versione VDA oppure la nuova VDA potrebbe non influire sul livello funzionale. In questi casi, il livello funzionale potrebbe indicare una versione VDA precedente ai componenti installati o aggiornati. L'articolo [Novità](#) di ogni versione indica eventuali modifiche al livello funzionale predefinito.

Il livello funzionale selezionato influisce sull'elenco delle macchine superiori. Nell'elenco, una descrizione comandi accanto a ciascuna voce indica se il VDA della macchina è compatibile con il catalogo a quel livello funzionale.

Se il VDA su ogni macchina non soddisfa o supera il livello funzionale minimo selezionato, vengono pubblicati dei messaggi sulla pagina. Puoi continuare con la procedura guidata. Probabilmente in seguito tali macchine non saranno più in grado di registrarsi con un Controller. In alternativa, puoi:

- Rimuovere dall'elenco le macchine contenenti VDA più vecchie, aggiornare i loro VDA e quindi aggiungerle nuovamente al catalogo.
- Scegliere un livello funzionale inferiore che impedisca l'accesso alle funzionalità più recenti del prodotto.

Viene inoltre visualizzato un messaggio se una macchina non è stata aggiunta al catalogo perché è del tipo sbagliato. Esempi di ciò includono il tentativo di aggiungere un server a un catalogo di sistemi operativi a sessione singola o l'aggiunta di una macchina con sistema operativo a sessione singola creata originariamente per l'allocazione casuale a un catalogo di macchine statiche.

Importante:

Nella versione 1811 è stato aggiunto un livello funzionale extra: **1811 (o più recente)**. Questo livello è destinato all'uso con le future funzionalità di Citrix Virtual Apps and Desktops. La selezione **7.9 (o più recente)** rimane quella predefinita. Ora questa impostazione predefinita è valida per tutte le distribuzioni.

Se si seleziona **1811 (o più recente)**, tutte le versioni VDA precedenti in quel catalogo non potranno registrarsi con un Controller. Tuttavia, se il catalogo contiene solo VDA con versione 1811 o versioni successive supportate, è possibile registrarli tutti. Sono inclusi i cataloghi contenenti VDA configurati per le versioni successive di Citrix Virtual Apps and Desktops, tra cui la versione 1903 e altre versioni 19XX precedenti alla versione corrente.

Configurare la cache per i dati temporanei

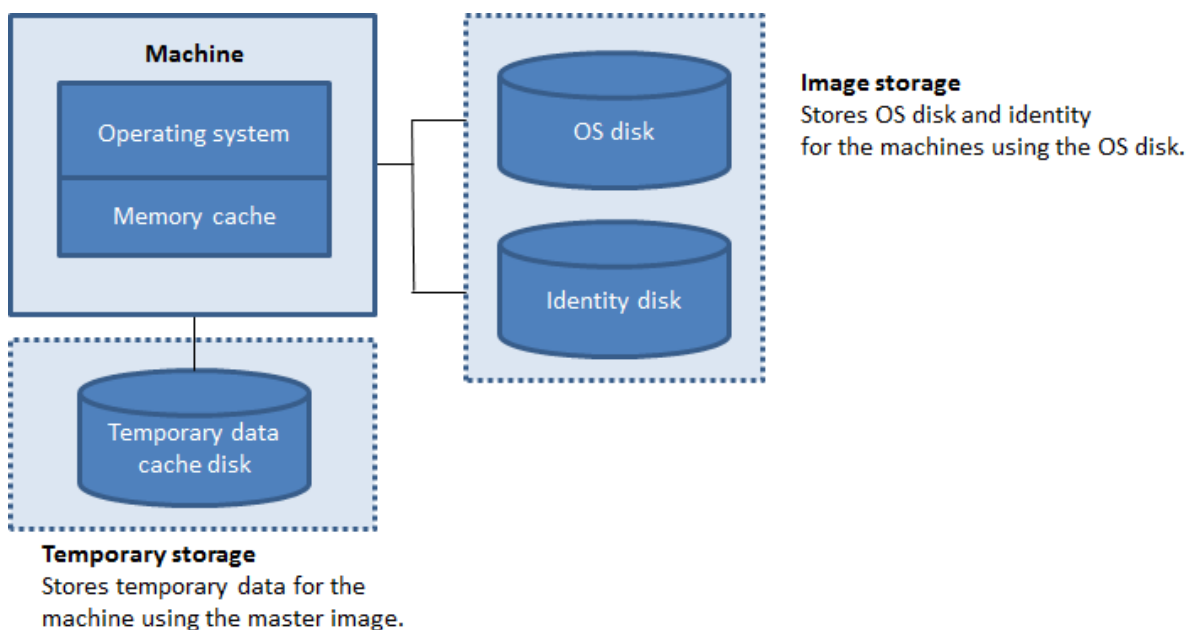
La memorizzazione nella cache locale dei dati temporanei sulla VM è facoltativa. È possibile abilitare l'utilizzo della cache dati temporanea sulla macchina quando si utilizza MCS per gestire macchine in pool (non dedicate) in un catalogo. Se il catalogo utilizza una connessione che specifica l'archiviazione per i dati temporanei, è possibile abilitare e configurare le informazioni sulla cache dei dati temporanei quando si crea il catalogo.

Importante:

Questa funzionalità richiede un driver MCS I/O aggiornato. L'installazione di questo driver è un'opzione quando si installa o si aggiorna un VDA. Per impostazione predefinita, quel driver non è installato.

Quando si crea la connessione utilizzata dal catalogo, è possibile specificare se i dati temporanei utilizzano un archivio condiviso o locale. Per ulteriori informazioni, vedere [Connessioni e risorse](#). Per configurare una cache per i dati temporanei su ogni macchina, puoi utilizzare le due opzioni seguenti: **Memoria allocata alla cache (MB)** e **Dimensione della cache del disco (GB)**. Per impostazione predefinita, le due opzioni sono deselezionate. Per abilitare l'opzione Memoria allocata nella cache (MB), selezionare la casella di controllo Dimensione cache disco (GB). Se la casella di controllo **Dimensione cache disco** non è selezionata, l'opzione **Memoria allocata alla cache** è disattivata. A seconda del tipo di connessione, i valori predefiniti per queste opzioni potrebbero variare. In genere, i valori predefiniti sono sufficienti per la maggior parte dei casi. Tuttavia, bisogna tenere conto dello spazio necessario per:

- File di dati temporanei creati da Windows stesso, incluso il file di paging di Windows.
- Dati del profilo utente.
- Dati ShareFile sincronizzati con le sessioni degli utenti.
- Dati che potrebbero essere creati o copiati da un utente di sessione o da qualsiasi applicazione che gli utenti potrebbero installare all'interno della sessione.



Per configurare una cache per i dati temporanei su ogni macchina, tenere presente i tre scenari seguenti:

- Se non si selezionano le caselle di controllo Dimensione cache disco e Memoria allocata alla cache, i dati temporanei non verranno memorizzati nella cache. Viene scritto direttamente sul disco differente (ubicato nell'archiviazione del sistema operativo) per ogni VM. (Questa è l'azione di provisioning nella versione 7.8 e precedenti.)
- Se si selezionano le caselle di controllo Dimensione cache disco e Memoria allocata alla cache, i dati temporanei vengono inizialmente scritti nella cache di memoria. Quando la cache di memoria raggiunge il limite configurato (il valore Memoria allocata alla cache), i dati più vecchi vengono spostati sul disco della cache dati temporanea.

Importante:

- Se la cache del disco esaurisce lo spazio, la sessione dell'utente diventa inutilizzabile.
- Questa funzionalità non è disponibile quando si utilizza una connessione host Nutanix.
- Non è possibile modificare i valori della cache in un catalogo macchine dopo la creazione della macchina.

Nota:

- La configurazione della cache write-back con solo una cache su disco e nessuna cache di memoria è diventata obsoleta. Per abilitare una cache per i dati temporanei, consigliamo di selezionare sia **Dimensione cache disco (GB)** che **Memoria allocata alla cache (MB)** e di specificare una dimensione maggiore di 0 per la cache di memoria.

- La cache di memoria è una parte della quantità totale di memoria presente su ogni macchina. Pertanto, se si abilita l'opzione Memoria allocata nella cache, si consiglia di aumentare la quantità totale di memoria su ciascuna macchina.
- La modifica della dimensione della cache del disco rispetto al valore predefinito può influire sulle prestazioni. Le dimensioni devono essere adatte alle esigenze dell'utente e al carico che grava sulla macchina.

NIC

Questa pagina non viene visualizzata quando si creano cataloghi di Accesso PC remoto.

Nella pagina **Schede di interfaccia di rete**, se si prevede di utilizzare più NIC, associare una rete virtuale a ciascuna scheda. Ad esempio, è possibile assegnare una scheda per accedere a una specifica rete protetta e un'altra scheda per accedere a una rete utilizzata più comunemente. Da questa pagina è anche possibile aggiungere o rimuovere NIC.

Conti macchina

Questa pagina viene visualizzata solo quando si creano cataloghi di Accesso PC remoto.

Nella pagina **Account macchina**, specificare gli account macchina Active Directory o le unità organizzative (OU) da aggiungere che corrispondono agli utenti o ai gruppi di utenti. Non utilizzare una barra (/) nel nome di una OU.

Quando aggiungi OU, puoi fare quanto segue se il dominio non è visualizzato nell'elenco:

- Cercalo utilizzando una corrispondenza esatta.
- Esplora tutti i domini per trovarlo.

È possibile scegliere una connessione di gestione dell'alimentazione configurata in precedenza oppure scegliere di non utilizzare la gestione dell'alimentazione. Se si desidera utilizzare la gestione dell'alimentazione ma non è ancora stata configurata una connessione idonea, è possibile creare tale connessione in un secondo momento e quindi modificare il catalogo delle macchine per aggiornare le impostazioni di gestione dell'alimentazione.

Identità delle macchine

Questa pagina viene visualizzata solo quando si utilizza MCS per creare VM.

Ogni macchina nel catalogo deve avere un'identità univoca. Questa pagina consente di configurare le identità per le macchine nel catalogo. Le macchine vengono aggiunte all'identità dopo essere state fornite. Non è possibile modificare il tipo di identità dopo aver creato il catalogo.

Di seguito è riportato un flusso di lavoro generale per configurare le impostazioni in questa pagina:

1. Seleziona un'identità dall'elenco.
2. Indica se creare account o utilizzare quelli esistenti e la posizione (dominio) per tali account.

Puoi selezionare una delle seguenti opzioni:

- **Active Directory locale.** Macchine di proprietà di un'organizzazione e a cui è stato effettuato l'accesso tramite un account Active Directory appartenente a tale organizzazione. Sono presenti in sede.
- **Azure Active Directory ibrido unito a.** Macchine di proprietà di un'organizzazione e a cui è stato effettuato l'accesso tramite un account Active Directory Domain Services appartenente a tale organizzazione. Sono disponibili nel cloud e in locale. Per informazioni sui requisiti, le limitazioni e le considerazioni, vedere [Azure Active Directory ibrido unito a](#).

Nota:

- Prima di poter utilizzare l'aggiunta ibrida ad Azure Active Directory, assicurati che l'ambiente Azure soddisfi i prerequisiti. Vedere <https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains>.
- Questa opzione richiede che l'immagine master soddisfi i prerequisiti del sistema operativo. Per ulteriori informazioni, consultare la documentazione Microsoft: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid>.

Importante:

- Se si seleziona **Active Directory locale** o **Azure Active Directory ibrido unito a** come tipo di identità, ogni computer nel catalogo deve avere un account computer Active Directory corrispondente.

Se si creano account, è necessario disporre dell'autorizzazione per creare account computer nell'OU in cui risiedono i computer. Ogni macchina nel catalogo deve avere un nome univoco. Specificare lo schema di denominazione degli account per le macchine che si desidera creare. Per ulteriori informazioni, vedere Schema di denominazione degli account macchina.

Nota:

Assicurarsi che i nomi delle OU non utilizzino barre (/).

Se utilizzi account esistenti, accedi agli account o fai clic su **Importa** e specifica un file .csv contenente i nomi degli account. Il contenuto del file importato deve utilizzare il formato:

- [ADComputerAccount] NomeaccountcomputerAD.dominio

Assicurati che ci siano abbastanza account per tutte le macchine che vuoi aggiungere. L'interfaccia di Web Studio gestisce tali account. Pertanto, è opportuno consentire all'interfaccia di reimpostare le password per tutti gli account oppure specificare la password dell'account, che deve essere la stessa per tutti gli account.

Per i cataloghi contenenti macchine fisiche o esistenti, selezionare o importare account esistenti e assegnare ciascuna macchina sia a un account computer Active Directory sia a un account utente.

Schema di denominazione dell'account macchina

Ogni macchina in un catalogo deve avere un nome univoco. Quando si crea un catalogo, è necessario specificare uno schema di denominazione per l'account macchina. Utilizzare i caratteri jolly (cancelletti) come segnaposto per i numeri o le lettere sequenziali che compaiono nel nome.

Quando si specifica uno schema di denominazione, tenere presente le seguenti regole:

- Lo schema di denominazione deve contenere almeno un carattere jolly. Devi mettere insieme tutti i caratteri jolly.
- Il nome completo, inclusi i caratteri jolly, deve contenere almeno 2 e non più di 15 caratteri. Deve includere almeno un carattere non numerico e un carattere jolly #.
- Il nome non deve contenere spazi o nessuno dei seguenti caratteri: `,~!@' $%^&. ()} { \/*?"<>|=+[];:_".`
- Il nome non può terminare con un trattino (-).

Inoltre, quando si specifica lo schema di denominazione, lasciare abbastanza spazio per la crescita. Consideriamo questo esempio: se si creano 1.000 account macchina con lo schema "veryverylong#", l'ultimo nome account creato (veryverylong1000) contiene 16 caratteri. Pertanto, lo schema di denominazione determina uno o più nomi di macchina che superano il massimo di 15 caratteri.

È possibile indicare se i valori sequenziali sono numeri (0-9) o lettere (AZ):

- **0-9.** Se selezionati, i caratteri jolly specificati vengono risolti in numeri sequenziali.

Nota:

Se è presente un solo carattere jolly (#), i nomi degli account iniziano con 1. Se ce ne sono due, i nomi degli account iniziano con 01. Se sono tre, i nomi degli account iniziano con 001 e così via.

- **DA.** Se selezionati, i caratteri jolly specificati vengono risolti in lettere sequenziali.

Ad esempio, uno schema di denominazione PC-Sales-## (con **0-9** selezionato) genera account denominati PC-Sales-01, PC-Sales-02, PC-Sales-03 e così via.

Facoltativamente, puoi specificare con quale nome iniziano i nomi degli account.

- Se si seleziona **0-9**, gli account vengono denominati in sequenza, a partire dai numeri specificati. Immettere una o più cifre, a seconda del numero di caratteri jolly utilizzati nel campo precedente. Ad esempio, se si utilizzano due caratteri jolly, immettere due o più cifre.
- Se si seleziona **AZ**, gli account vengono denominati in sequenza, iniziando con le lettere specificate. Inserisci una o più lettere, a seconda del numero di caratteri jolly utilizzati nel campo precedente. Ad esempio, se si utilizzano due caratteri jolly, immettere due o più lettere.

Credenziali di dominio

Selezionare **Inserisci credenziali** e immettere le credenziali di un amministratore autorizzato a eseguire operazioni sull'account nel dominio Active Directory di destinazione.

Utilizzare l'opzione **Controlla nome** per verificare se il nome utente è valido o univoco. L'opzione è utile, ad esempio, quando:

- Lo stesso nome utente esiste in più domini. Ti verrà chiesto di selezionare l'utente desiderato.
- Non ricordi il nome del dominio. È possibile immettere il nome utente senza specificare il nome di dominio. Se il controllo viene superato, il nome di dominio viene compilato automaticamente.

Nota:

Se il tipo di identità selezionato in **Identità macchina** è **Azure Active Directory ibrido unito a**, le credenziali immesse devono avere ricevuto l'autorizzazione **Scrittura userCertificates**.

Riepilogo, nome e descrizione

Nella pagina **Riepilogo**, rivedi le impostazioni specificate. Inserisci un nome e una descrizione per il catalogo. Queste informazioni vengono visualizzate in Web Studio.

Una volta terminato, clicca su **Fine** per avviare la creazione del catalogo. Una volta terminato, seleziona **Fine** per avviare la creazione del catalogo.

In **Cataloghi macchine**, il nuovo catalogo appare con una barra di avanzamento incorporata.

Per visualizzare i dettagli dell'avanzamento della creazione:

1. Passare il mouse sul catalogo delle macchine.
2. Nella descrizione comandi che appare, clicca su **Visualizza dettagli**.

Viene visualizzato un grafico di avanzamento passo dopo passo in cui è possibile vedere quanto segue:

- Storia dei passi
- Avanzamento e tempo di esecuzione del passaggio corrente
- Passaggi rimanenti

Sincronizzazione oraria MCS

La sincronizzazione temporale è determinata dall'immagine master e dal tipo di catalogo unito all'identità della macchina. Si ottiene il seguente metodo di sincronizzazione temporale in base all'immagine master e al catalogo:

Immagine principale	Catalogare	Metodo di sincronizzazione temporale risultante
NDJ	AD o Azure AD ibrido	Per impostazione predefinita, NT5DS. È possibile disabilitare MCS dalla modifica delle impostazioni di sincronizzazione dell'ora utilizzando le impostazioni del registro nell'immagine master
NDJ	NDJ o Azure AD	Uguale all'impostazione di sincronizzazione oraria originale
AD o Azure AD ibrido	AD o Azure AD ibrido	Uguale all'impostazione di sincronizzazione oraria originale
Azure AD	Azure AD	Uguale all'impostazione di sincronizzazione oraria originale

Nota:

La sincronizzazione oraria originale è controllata dalla seguente impostazione del registro e non può essere modificata:

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Servizi\W32Time\Config

Valore: MaxAllowedPhaseOffset, MaxNegPhaseCorrection e MaxPosPhaseCorrection

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parametri`

Valore: Tipo

Per impedire a MCS di modificare l'impostazione di sincronizzazione dell'ora, impostare il valore della seguente impostazione del registro nell'immagine master:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Nome: `TimeSyncMethodKeep`
- Tipo: `DWORD`
- 0 (oppure valore `TimeSyncMethodKeep` non configurato): non mantiene l'impostazione di sincronizzazione dell'ora originale.
- 1: Mantiene le impostazioni di sincronizzazione dell'ora originali e i valori dei parametri predefiniti.

Considerazioni importanti sull'impostazione delle proprietà personalizzate

Le proprietà personalizzate devono essere impostate correttamente su `New-ProvScheme` e `Set-ProvScheme` negli ambienti GCP e Azure. Se si specificano una o più proprietà personalizzate inesistenti, viene visualizzato il seguente messaggio di errore e i comandi non vengono eseguiti.

- In Azure: `Proprietà non valida trovata: <invalid property>`. Assicurarsi che il parametro `CustomProperties` supporti la proprietà.
- In GCP: `Proprietà non valida trovata: <invalid property>`. Assicurarsi che il valore fornito per la proprietà sia supportato nell'`Hypervisor`.

Risoluzione dei problemi

Importante:

Dopo aver creato il catalogo macchine tramite Web Studio, non è più possibile utilizzare il comando PowerShell `Get-ProvTask` per recuperare le attività associate alla creazione del catalogo macchine. Questa restrizione è dovuta al fatto che Web Studio elimina tali attività dopo la creazione del catalogo macchina, indipendentemente dal fatto che la creazione del catalogo sia avvenuta correttamente.

Citrix consiglia di raccogliere i registri per aiutare il team di supporto a fornire soluzioni. Quando si utilizza Citrix Provisioning, utilizzare la seguente procedura per generare i file di registro:

1. Nell'immagine master, creare la seguente chiave di registro con il valore 1 (come valore `DWORD` (32 bit)): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.

2. Chiudere l'immagine master e creare uno snapshot.
3. Sul Delivery Controller, eseguire il seguente comando PowerShell: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Crea un catalogo basato su tale istantanea.
5. Una volta creata la VM di preparazione sull'hypervisor, effettuare l'accesso ed estrarre i seguenti file dalla radice di C:\: Image-prep.log e PvsVmAgentLog.txt.
6. Spegnerne la macchina, che a quel punto segnala il guasto.
7. Eseguire il seguente comando PowerShell per riattivare l'arresto automatico delle macchine di preparazione delle immagini: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

Problemi di preparazione delle immagini

Poiché MCS crea molte macchine da una singola immagine, vengono eseguiti alcuni passaggi per garantire che tutte le macchine siano univoche e correttamente dotate di licenza. La preparazione delle immagini fa parte del processo di creazione del catalogo. Questa preparazione garantisce che tutte le macchine fornite abbiano indirizzi IP univoci e si annuncino correttamente al server KMS come istanze univoche. In MCS, la preparazione dell'immagine avviene dopo aver selezionato l'istantanea dell'immagine master. Viene creata una copia per consentire al catalogo di isolarsi dalla macchina selezionata. Viene creata una VM di preparazione **, basata sulla VM originale, ma con la connessione di rete disconnessa. La disconnessione della connessione di rete impedisce conflitti con altre macchine e garantisce al contempo che la VM preparata venga collegata solo al disco appena copiato.

Un piccolo disco di istruzioni **, contenente i passaggi necessari per eseguire la preparazione dell'immagine, è allegato alla VM preparata. La VM preparata si avvia e inizia il processo di preparazione dell'immagine. La preparazione delle immagini comprende i seguenti processi:

- Abilita DHCP. L'abilitazione di DHCP garantisce che le macchine fornite non causino conflitti di indirizzi IP. DHCP è abilitato su tutte le schede di rete.
- Riarmo di Microsoft Windows KMS. Il riarmo del KMS garantisce che Microsoft Windows sia correttamente concesso in licenza. Il sistema operativo riarmato viene richiamato in modo da essere correttamente segnalato come una nuova istanza al server delle licenze KMS.
- Riarmo di Microsoft Office KMS (se Microsoft Office è installato). Il riarmo di Microsoft Office garantisce che qualsiasi versione di Microsoft Office (2010+) venga registrata correttamente sul server KMS. Una volta richiamato Microsoft Office, questo viene segnalato come una nuova istanza al server delle licenze KMS.

Mancia:

Una volta completato il processo di preparazione dell'immagine, il disco di istruzioni viene ottenuto dall'hypervisor. L'hypervisor contiene le informazioni ricavate dal processo di preparazione delle immagini.

Esistono diverse ragioni per cui la fase di preparazione dell'immagine può fallire. Viene visualizzato un messaggio di errore simile al seguente: Riarmo dell'ufficio preparazione immagine non riuscito.

Questi fallimenti vengono discussi nelle sezioni seguenti.

Abilita DHCP Questi casi di errore sono causati da schede di rete che non supportano indirizzi IP statici. Ad esempio, le versioni precedenti delle schede di rete Dell SonicWall. L'operazione non è riuscita perché la scheda SonicWall è una scheda di rete firewall, quindi non ha senso impostare la scheda su DHCP, in quanto supporta solo DHCP. Questo problema è stato risolto nelle versioni successive di Citrix Virtual Apps and Desktops. Tuttavia, se il problema si verifica su altri tipi di schede di rete, è necessario segnalarlo a Citrix tramite i forum o contattando il supporto tecnico.

Nota:

Negli esempi seguenti, questa impostazione di PowerShell viene applicata al sito Citrix Virtual Apps and Desktops, pertanto influisce su tutti i nuovi cataloghi e sugli aggiornamenti delle immagini eseguiti sui cataloghi esistenti.

Se riscontri questo problema con altre schede di rete, puoi risolverlo eseguendo un comando PowerShell sul Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps  
-Value EnableDHCP
```

Riarmo di Microsoft Office Possono verificarsi vari errori di riarmo del KMS durante la fase di riarmo di Microsoft Office. I principali fallimenti sono:

- Alcuni runtime di Microsoft Office, ad esempio **Access Runtime**, possono richiamare il riarmo di Office, causandone il fallimento.
- Non è installata la versione KMS di Microsoft Office.
- Superato il conteggio dei riarmi.

Se l'errore è un falso positivo, puoi risolverlo eseguendo il seguente comando di PowerShell sul Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps  
-Value OfficeRearm
```

Riarmo di Microsoft Windows Durante la fase di riarmo di Microsoft Windows possono verificarsi vari errori del KMS. I principali fallimenti sono:

- La versione di Windows installata non è attivata tramite KMS. Ad esempio, utilizza una chiave di attivazione multipla (MAK).
- Superato il conteggio dei riarmi.

Se la versione di Microsoft Windows è correttamente autorizzata, è possibile annullare il riarmo del sistema operativo eseguendo il seguente comando di PowerShell sul Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps  
-Value OsRearm
```

Casi di fallimento completo La macchina per la preparazione delle immagini non è connessa alla rete per impostazione predefinita, il che significa che a volte la fase di preparazione delle immagini può segnalare solo un guasto completo. Un esempio di questo tipo di errore è simile al seguente: Preparazione dell'immagine della VM master non riuscita. Assicurarsi che l'immagine selezionata abbia un sistema operativo supportato (ad esempio, Windows 7) e che sia installata la versione corretta del VDA (7.0 o successiva).

Le principali cause di un fallimento totale sono:

Virtual Delivery Agent (VDA) non è installato oppure è installata la versione 5.x di VDA Se VDA 7.x non è installato sull'immagine master, la preparazione dell'immagine si interrompe dopo 20 minuti e viene visualizzato l'errore sopra indicato. Ciò avviene perché sull'immagine master non è installato alcun software per eseguire la fase di preparazione dell'immagine e segnalare il successo o il fallimento. Per risolvere questo problema, assicurarsi che VDA (versione minima 7) sia installato sullo snapshot selezionato come immagine master.

DISKPART SAN Politica L'intera fase di preparazione dell'immagine può fallire a causa della policy `DISKPART SAN` impostata sull'immagine master. Se non è impostato per portare online il disco con le istruzioni di preparazione dell'immagine, la macchina viene spenta e la preparazione dell'immagine segnala un errore dopo 20 minuti. Per verificarlo sull'immagine master, eseguire i seguenti comandi:

```
1 C:\>; Diskpart.exe  
2 DISKPART>; San
```

Questo comando restituisce la policy corrente. Se non è *Online All*, modificarlo eseguendo il seguente comando:

```
DISKPART>; San policy=OnlineAll
```

Arrestare l'immagine master, creare uno snapshot della macchina e utilizzarlo come immagine MCS di base.

Se la preparazione dell'immagine fallisce per un altro motivo Se la preparazione dell'immagine non riesce e non vi è una causa chiara del problema, è possibile ignorare il processo di preparazione dell'immagine durante la creazione di un catalogo MCS. Tuttavia, ignorare questo processo può causare problemi con le licenze KMS e con la rete (DHCP) sul tuo sito. Utilizzare il seguente comando PowerShell:

```
1 Set-ProvServiceConfigurationData -Name  
ImageManagementPrep_DoImagePreparation -Value $false
```

Se possibile, raccogliere i registri per il team di supporto Citrix. Segnalare il problema a Citrix tramite i forum o tramite il proprio contatto di supporto. Per raccogliere i registri:

1. Sull'immagine master creare la seguente chiave di registro con il valore 1 (come "valore DWORD (32 bit)"): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Chiudere l'immagine master e creare uno snapshot. Sul Delivery Controller, avviare PowerShell, con gli snap-in Citrix PowerShell caricati, ed eseguire `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
3. Crea un catalogo basato su tale istantanea.
4. Quando la VM di preparazione viene creata sull'hypervisor, accedi ed estrai dalla radice di C::

```
1 Image-prep.log  
2 PvsVmAgentLog.txt
```

Spegnere la macchina. A questo punto segnala il guasto.

Eseguire il seguente comando PowerShell per riattivare l'arresto automatico delle macchine di preparazione delle immagini:

```
Rimuovi-ProvServiceConfigurationData -Nome ImageManagementPrep_NoAutoShutdown
```

Dove andare dopo

Per informazioni sulla creazione di cataloghi di servizi cloud specifici, vedere:

- [Crea un catalogo AWS](#)
- [Creare un catalogo XenServer](#)
- [Crea un catalogo di Google Cloud Platform](#)
- [Creare un catalogo Microsoft Azure](#)
- [Creare un catalogo di Microsoft System Center Virtual Machine Manager](#)

- [Crea un catalogo Nutanix](#)
- [Creare un catalogo VMware](#)

Se questo è il primo catalogo creato, Web Studio ti guiderà nella [creazione di un gruppo di distribuzione](#).

Per rivedere l'intero processo di configurazione, vedere [Installa e configura](#).

È possibile creare un catalogo Citrix Provisioning utilizzando Web Studio e PowerShell. Questa implementazione ti offre i seguenti vantaggi:

- Un'unica console unificata per gestire i cataloghi MCS e Citrix Provisioning.
- Avere nuove funzionalità per i cataloghi di Citrix Provisioning, come soluzioni di gestione delle identità, provisioning on-demand e così via.

Attualmente questa funzionalità è disponibile solo per i carichi di lavoro Azure e VMware. Tuttavia, negli ambienti VMware, attualmente è possibile creare i cataloghi utilizzando solo comandi PowerShell. Per ulteriori informazioni, vedere [Creare cataloghi Citrix Provisioning in Citrix Studio](#).

Ulteriori informazioni

- [Crea e gestisci connessioni e risorse](#)
- [Crea cataloghi di diversi tipi di join](#)
- [Gestire i cataloghi delle macchine](#)

Crea un catalogo AWS

November 8, 2024

In [Creare cataloghi di macchine](#) sono descritte le procedure guidate per la creazione di un catalogo di macchine. Le informazioni che seguono riguardano i dettagli specifici degli ambienti di virtualizzazione AWS.

Nota:

Prima di creare un catalogo di AWS, è necessario completare la creazione di una connessione ad AWS. Vedere [Connessione ad AWS](#).

Limitazione

Da Citrix Virtual Apps and Desktops 2203 LTSR e versioni successive, il plug-in MCS AWS effettua una chiamata API AWS `DescribeInstanceTypes` e, se questa ha esito positivo, MCS utilizza il nome dell'inventario creato dalla risposta API.

Pertanto, quando si esegue l'aggiornamento da CVAD 1912 a 2203 o versione successiva, disabilitare l'autorizzazione `DefineInstanceType` su AWS, quindi aggiornare il catalogo esistente utilizzando il comando `Set-ProvScheme` in modo che corrisponda allo schema di denominazione AWS. Quindi, aggiungere nuovamente le autorizzazioni `DescribeInstanceType` una volta completato l'aggiornamento del catalogo e quando l'offerta del servizio corrisponde allo schema di denominazione AWS.

Impostazioni di rete durante la preparazione dell'immagine

Durante la preparazione dell'immagine, viene creata una macchina virtuale (VM) di preparazione basata sulla macchina virtuale originale. Questa macchina virtuale di preparazione è disconnessa dalla rete. Per disconnettere la rete dalla macchina virtuale di preparazione, viene creato un gruppo di sicurezza di rete per negare tutto il traffico in entrata e in uscita. Questo gruppo di sicurezza di rete persiste e viene riutilizzato. Il nome del gruppo di sicurezza di rete è `Citrix.XenDesktop.IsolationGroup-GUID`, dove GUID viene generato casualmente.

Configurare la tenancy AWS

AWS offre le seguenti opzioni di tenancy:

- Tenancy condivisa (il tipo predefinito): più istanze di Amazon EC2 di clienti diversi potrebbero risiedere sullo stesso componente hardware fisico.
- Tenancy dedicata: le istanze di EC2 vengono eseguite solo su hardware con altre istanze distribuite. Gli altri clienti non utilizzano lo stesso hardware.

È possibile utilizzare MCS per eseguire il provisioning di host AWS dedicati utilizzando PowerShell.

Configurare la tenancy dell'host AWS dedicato utilizzando PowerShell

È possibile creare un catalogo di macchine con tenancy host definita tramite PowerShell.

Un host dedicato Amazon [EC2] è un server fisico con capacità di istanza [EC2] completamente dedicata, che consente di utilizzare licenze software esistenti per socket o per macchina virtuale.

Gli host dedicati hanno un utilizzo preimpostato in base al tipo di istanza. Ad esempio, un singolo host dedicato allocato di tipi di istanza C4 Large è limitato all'esecuzione di 16 istanze. Per ulteriori informazioni, consultare il [sito di AWS](#).

I requisiti per il provisioning sugli host AWS includono:

- Un'immagine BYOL (Bring Your Own License) importata (AMI). Con host dedicati, utilizzare e gestire le licenze esistenti.

- Un'allocazione di host dedicati con un utilizzo sufficiente per soddisfare le richieste di provisioning.
- abilitare il **posizionamento automatico**.

Per effettuare il provisioning su un host dedicato in AWS tramite PowerShell, utilizzare il cmdlet **New-ProvScheme** con il parametro `TenancyType` impostato su `Host`.

Per ulteriori informazioni, consultare la [documentazione per gli sviluppatori Citrix](#).

Acquisizione delle proprietà della macchina dalle AMI

Quando si crea un catalogo per il provisioning di macchine utilizzando Machine Creation Services (MCS) in AWS, si seleziona un'AMI per rappresentare l'immagine master/golden di quel catalogo. Da tale AMI, MCS utilizza una snapshot del disco. Nelle versioni precedenti, se si voleva avere ruoli o tag sulle macchine si utilizzava la console AWS per impostarli individualmente. Questa funzionalità è abilitata per impostazione predefinita.

Mancia:

Per utilizzare l'acquisizione delle proprietà delle istanze AWS, è necessario disporre di una macchina virtuale associata all'AMI.

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

Le proprietà acquisite includono:

- Ruoli IAM: applicati alle istanze di cui è stato eseguito il provisioning.
- Tag: applicati alle istanze di cui è stato eseguito il provisioning, il relativo disco e le NIC. Questi tag vengono applicati alle risorse Citrix transitorie, tra cui: bucket e oggetti S3, AMI, snapshot e modelli di avvio.

Mancia:

Il tagging delle risorse Citrix temporanee è facoltativo e può essere configurato tramite la proprietà personalizzata `AwsOperationalResourcesTagging`.

Acquisire la proprietà dell'istanza AWS

È possibile utilizzare questa funzionalità specificando una proprietà personalizzata, `AwsCaptureInstanceProperties`, quando si crea uno schema di provisioning per una connessione di hosting AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"  
...<parametri provscheme standard
```

Per ulteriori informazioni, consultare la [documentazione per gli sviluppatori Citrix](#).

Nota:

La proprietà `AwsCaptureInstanceProperties` è deprecata. Consigliamo invece di utilizzare i profili macchina per specificare le proprietà della macchina per le VM.

Acquisizione delle proprietà della macchina dai profili della macchina

Quando si crea un catalogo per il provisioning delle macchine AWS tramite MCS, è possibile utilizzare un profilo macchina per preimpostare determinate impostazioni delle proprietà della macchina.

A tale scopo, attenersi alla seguente procedura:

1. Memorizzare i profili macchina nella stessa zona di disponibilità delle risorse in cui si sta creando questo catalogo.
2. Nella pagina **Modello macchina** della procedura guidata di creazione catalogo, seleziona **Usa un profilo macchina**. Vengono visualizzati i profili macchina che si trovano nella stessa zona disponibile delle risorse selezionate.
3. Selezionare un profilo macchina in base alle proprie esigenze.

Nota:

Per acquisire le proprietà della macchina è possibile utilizzare un profilo macchina o un'AMI. In Web Studio, quando selezioni **Usa un profilo macchina**, l'opzione **Applica le proprietà del modello macchina alle macchine virtuali** viene automaticamente nascosta.

Applicare tag a una risorsa operativa AWS

Quando si crea un catalogo per il provisioning delle macchine in AWS utilizzando MCS, è possibile controllare se applicare il ruolo IAM e le proprietà dei tag a tali macchine. È inoltre possibile controllare se applicare tag delle macchine alle risorse operative.

Un'Amazon Machine Image (AMI) rappresenta un tipo di appliance virtuale utilizzata per creare una macchina virtuale all'interno dell'ambiente Amazon Cloud, comunemente denominato EC2. È possibile utilizzare un'AMI per distribuire servizi che utilizzano l'ambiente EC2. Quando si crea un catalogo

per eseguire il provisioning di macchine utilizzando MCS per AWS, selezionare l'**AMI** che funge da immagine golden per quel catalogo.

Importante:

La creazione di cataloghi mediante l'acquisizione di una proprietà di istanza e di un modello di avvio è necessaria per utilizzare la codifica delle risorse operative.

Per creare un catalogo di AWS, è necessario innanzitutto creare un'AMI per l'istanza in cui si desidera collocare l'immagine golden. MCS legge i tag di quell'istanza e li incorpora nel modello di avvio. I tag del modello di avvio vengono quindi applicati a tutte le risorse Citrix create nell'ambiente AWS, tra cui:

- Macchine virtuali
- Dischi delle macchine virtuali
- Interfacce di rete delle macchine virtuali
- Bucket S3
- Oggetti S3
- Modelli di lancio
- AMI

Applicare tag a una risorsa operativa

Per utilizzare PowerShell per etichettare le risorse:

1. Aprire una finestra di PowerShell dall'host DDC.
2. Eseguire il comando `asnp citrix` per caricare i moduli PowerShell specifici di Citrix.

Per contrassegnare una risorsa per una VM approvvigionata, utilizzare la nuova proprietà personalizzata `AwsOperationalResourcesTagging`. La sintassi di questa proprietà è la seguente:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;  
AwsOperationalResourcesTagging,true"...<standard provscheme parameters  
>
```

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 gestire i cataloghi, vedere [Gestire i cataloghi delle macchine](#) e [Gestire un catalogo AWS](#)

Copia i tag sulle VM

È possibile copiare i tag sulle schede di rete e sui dischi (disco di identità, disco di cache di write back e disco del sistema operativo) specificati nel profilo macchina nelle VM appena create in un catalogo macchine MCS. È possibile specificare questi tag in una qualsiasi delle origini del profilo macchina (istanza VM AWS o versione modello di avvio AWS). Questa funzionalità è applicabile ai cataloghi di macchine e alle VM persistenti e non persistenti.

Nota:

- Nella console AWS EC2, non è possibile visualizzare i valori **Tag Network Interfaces** sotto i **Launch Template Version Resource Tags**. Tuttavia, è possibile eseguire il comando PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` per visualizzare le specifiche del tag.
- Se una sorgente di profilo macchina (versione VM o modello di avvio) ha due interfacce di rete (eni-1 ed eni-2), e eni-1 ha tag t1 ed eni-2 ha tag t2, la VM ottiene entrambi i tag delle interfacce di rete.

Creare un catalogo utilizzando un profilo macchina

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

Nota:

Le proprietà del volume EBS derivano solo dal profilo di una macchina.

Considerazioni importanti

Le considerazioni importanti durante la creazione di un catalogo di macchine MCS sono:

- Se si aggiungono parametri di proprietà hardware della macchina nei comandi `New-ProvScheme` e `Set-ProvScheme`, i valori forniti nei parametri sovrascrivono i valori nel profilo della macchina.
- Se si imposta `AwsCaptureInstanceProperties` su `true` e non si imposta la proprietà `MachineProfile`, vengono acquisiti solo i ruoli e i tag IAM.

- Non è possibile impostare contemporaneamente `AwsCaptureInstanceProperties` e `MachineProfile`.

****Nota:**

La proprietà `AwsCaptureInstanceProperties` è deprecata.

- È necessario fornire esplicitamente i valori delle seguenti proprietà:
 - TenancyType
 - Gruppo di sicurezza
 - NIC o rete virtuale
- Puoi abilitare `AwsOperationalResourcesTagging` solo se abiliti `AwsCaptureInstanceProperties` o specifichi un profilo macchina.

Le considerazioni importanti dopo la creazione di un catalogo di macchine MCS sono:

- Solo le nuove macchine virtuali aggiunte al catalogo sono interessate dalla modifica.
- Non è possibile trasformare un catalogo da basato su profili di macchina in non basato su profili macchina.

Creare un catalogo macchine utilizzando un profilo macchina

Per creare un catalogo di macchine utilizzando un profilo macchina:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Creare un pool di identità se non è già stato creato. Per esempio,

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
   Domain abcdf -NamingSchemeType Numerico
```

4. Eseguire il comando `New-ProvScheme`. Per esempio:

```
1 Nuovo-ProvScheme -ProvisioningSchemeName demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
   demet-ami.0 (ami-0ca813xxxxx061ef).template'
6 -MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
   -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxx).
   vm'
```

5. Completare la creazione del catalogo. Per ulteriori informazioni, vedere [Citrix PowerShell SDK](#).

Per aggiornare il profilo macchina su un catalogo di cui inizialmente era stato effettuato il provisioning con un profilo macchina:

1. Esegui il comando `Set-ProvScheme` . Per esempio,

```
1 Set-ProvScheme `
2 -ProvisioningSchemeUid "<ID" `
3 -MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
   availabilityzone\citrix-cvad-machineprofile-instance (i-0
   xxxxxxxx).vm"
```

Creare un catalogo con la versione del modello di avvio

È possibile creare un catalogo di macchine MCS con una versione del modello di avvio come input per il profilo macchina. È inoltre possibile aggiornare l'input di un catalogo di profili di macchina da una macchina virtuale a una versione del modello di avvio e da una versione del modello di avvio a una macchina virtuale.

Sulla console AWS EC2, è possibile fornire le informazioni di configurazione dell'istanza di un modello di avvio insieme al numero di versione. Quando si specifica la versione del modello di avvio come input del profilo macchina durante la creazione o l'aggiornamento di un catalogo di macchine, le proprietà di quella versione del modello di avvio vengono copiate nelle VM dei VDA di cui è stato eseguito il provisioning.

Le seguenti proprietà possono essere fornite utilizzando l'input del profilo macchina o esplicitamente come parametri nei comandi `New-ProvScheme` o `Set-ProvScheme`. Se vengono forniti nei comandi `New-ProvScheme` o `Set-ProvScheme`, hanno la precedenza sui valori del profilo macchina di queste proprietà.

- Offerta di servizi
- Reti
- Gruppi di sicurezza
- Tipo di tenancy

Nota:

Se l'offerta del servizio non è fornita nel modello di avvio del profilo macchina o come parametro nel comando `New-ProvScheme`, viene visualizzato un errore appropriato.

Per creare un catalogo utilizzando la versione del modello di avvio come input del profilo macchina:

1. Aprire una finestra di **PowerShell**.
2. Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
3. Ottenere l'elenco delle versioni del modello di avvio di un modello di avvio. Per esempio:


```
1 XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
  ls | Seleziona FullPath
```

4. Creare un pool di identità se non è già stato creato. Per esempio:

```
1 New-AcctIdentityPool `
2 -IdentityPoolName "abc11" `
3 -NamingScheme "abc1-##" `
4 -NamingSchemeType Numerico `
5 -Domain "citrix-xxxxxx.local" `
6 -ZoneUid "xxxxxxx" `
```

5. Creare uno schema di provisioning con una versione del modello di avvio come input del profilo macchina. Per esempio:

```
1 New-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxxx" `
4 -IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxxxx" `
5 -MasterImageVM "XDHyp:\HostingUnits\xxxx-ue1a\apollo-non-
  persistent-vda-win2022 (ami-0axxxxxxxxxxxx).template" `
6 -CleanOnBoot `
7 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
  (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
  launchtemplateversion"
```

È anche possibile ignorare parametri quali offerta di servizi, gruppi di sicurezza, tenancy e reti. Per esempio:

```
1 New-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxxx" `
4 -IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxxxx" `
5 -MasterImageVM "XDHyp:\HostingUnits\xxxx-ue1a\apollo-non-
  persistent-vda-win2022 (ami-0axxxxxxxxxxxx).template" `
6 -CleanOnBoot `
7 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
  (lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion" `
8 -ServiceOffering "XDHyp:\HostingUnits\xxxx-ue1a\T3 Istanza di
  grandi dimensioni.serviceoffering"
```

6. Registrare lo schema di provisioning come catalogo del broker. Per esempio:

```
1 New-BrokerCatalog -Name "MPLT1" `
2 -AllocationType Random `
3 -Description "Catalogo profili macchina" `
4 -ProvisioningSchemeId fe7df345-244e-4xxx-xxxx-xxxxxxxx `
5 -ProvisioningType Mcs `
6 -SessionSupport MultiSession `
7 -PersistUserChanges Ignora
```

7. Completare la creazione del catalogo. Per ulteriori informazioni, vedere [Citrix PowerShell SDK](#)

È inoltre possibile aggiornare l'input di un catalogo di profili di macchina da una macchina virtuale a una versione del modello di avvio e da una versione del modello di avvio a una macchina virtuale. Per esempio:

- Per aggiornare l'input di un catalogo di profili macchina da una macchina virtuale a una versione del modello di avvio:

```
1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
2 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-0bxxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxxx (1).
   launchtemplateversion"
```

- Per aggiornare l'input di un catalogo di profili macchina da una versione del modello di avvio a una macchina virtuale:

```
1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
2 -MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxx).vm"
```

Filtrare le istanze di VM

Un'istanza AWS EC2 utilizzata come VM con profilo macchina deve essere compatibile affinché il catalogo macchine possa essere creato e funzionare correttamente. Per elencare le istanze AWS EC2 che possono essere utilizzate come VM di input del profilo macchina, è possibile utilizzare il comando `Get-HypInventoryItem`. Il comando può effettuare il paging e filtrare l'inventario delle VM disponibili su un'unità di hosting.

Paging:

`Get-HypInventoryItem` supporta due modalità di impaginazione:

- La modalità di paging utilizza i parametri `-MaxRecords` e `-Skip` per restituire set di elementi:
 - `-MaxRecords`: Il valore predefinito è **1**. Questo controlla quanti elementi restituire.
 - `-Salta`: Il valore predefinito è **0**. Questo controlla quanti elementi saltare dall'inizio assoluto (o dalla fine assoluta) dell'elenco nell'hypervisor.
- La modalità di scorrimento utilizza i parametri `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` per consentire lo scorrimento dei record:
 - `-ForwardDirection`: Il valore predefinito è **Vero**. Viene utilizzato insieme a `-MaxRecords` per restituire il set successivo di record corrispondenti o il set precedente di record corrispondenti.

- `-ContinuationToken`: Restituisce gli elementi immediatamente successivi (o precedenti se `ForwardDirection` è **false**) ma escluso l'elemento specificato in `ContinuationToken`.

Esempi di paging:

- Per restituire un singolo record del modello di macchina con il nome più basso. Il campo `AdditionalData` ha `TotalItemsCount` e `TotalFilteredItemsCount`:

```
1 Modello Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\
  ctx-test" -ResourceType
```

- Per restituire dieci record del modello di macchina con il nome più basso:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType modello -MaxRecords 10 | seleziona Nome
```

- Per restituire una matrice di record che termina con il nome più alto:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType modello -ForwardDirection $False -MaxRecords 10
  | seleziona Nome
```

- Per restituire un array di record a partire dal modello macchina associato al `ContinuationToken` specificato:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType modello -ContinuationToken "ami-07xxxxxxxxxx" -
  MaxRecords 10
```

Filtraggio:

I seguenti parametri opzionali aggiuntivi sono supportati per il filtraggio. È possibile combinare questi parametri con le opzioni di paging.

- `-ContainsName "my_name"`: Se la stringa specificata corrisponde a parte di un nome AMI, allora l'AMI viene inclusa nel risultato `Ottieni`. Per esempio:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType modello -MaxRecords 100 -ContainName 'apollo' |
  seleziona Nome
```

- `-Tag '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Se un'AMI ha almeno uno di questi tag, viene incluso nel risultato `Ottieni`. Per esempio:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType template -MaxRecords 100 -Tags '{
2 "opex owner": "Non taggato" }
3 ' | select Nome
```

Nota:

Sono supportati due valori di tag. **Non taggato il valore del tag** corrisponde agli elementi che non hanno il tag specificato nel loro elenco di tag. **Tutti i valori** il valore del tag corrisponde agli elementi che hanno il tag indipendentemente dal valore del tag. Altrimenti, la corrispondenza avviene solo se l'elemento contiene il tag e il valore è uguale a quello indicato nel filtro.

- `-Id "ami-0a2d913927e0352f3"`: Se l'AMI corrisponde all'ID specificato, viene inclusa nel risultato `Ottieni`. Per esempio:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType modello -Id ami-xxxxxxxxxxxxx
```

Filtraggio in base al parametro `AdditionalData`:

Il parametro filtro `AdditionalData` elenca modelli o VM in base alla loro capacità, all'offerta di servizi o a qualsiasi proprietà presente in `AdditionalData`. Per esempio:

```
1 (Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
   AdditionalData
```

È anche possibile aggiungere un parametro `-Warn` per indicare le VM incompatibili. Le VM sono incluse con un campo `AdditionalData` denominato **Warning**. Per esempio:

```
1 (Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-
   -015xxxxxxxxxx" -Warn $true).AdditionalData
```

Ulteriori informazioni

- [Crea e gestisci connessioni e risorse](#)
- [Connessione ad AWS](#)
- [Creare cataloghi di macchine](#)

Creare un catalogo di Microsoft Azure

November 7, 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.

Quando si crea un catalogo di macchine MCS, viene creata una VM temporanea basata sulla VM originale per eseguire attività di preparazione come l'abilitazione di DHCP e il riarmo della licenza. Questa VM temporanea è chiamata VM di preparazione. Il nome di questa VM di preparazione segue il formato **Preparati-84x9n**, dove gli ultimi cinque caratteri vengono generati casualmente per evitare

uplicazioni. La convenzione di denominazione per questa VM di preparazione è fissa e non può essere personalizzata. Una volta completate le attività di preparazione, la VM di preparazione viene distrutta.

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 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 su Azure Trusted Launch, vedi <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 MC-SIO)
- 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 au-

tomatico 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.

Machine Catalog Setup [X]

Introduction ✓
Machine Type ✓
Machine Management ✓
Desktop Experience ✓
Master Image ✓
6 Storage and License Types
7 Virtual Machines
8 NICs
9 Disk Settings
10 Resource Group
11 Machine Identities
12 Domain Credentials
13 Scopes
14 Summary

Storage and License Types

Select the type of storage to use for this machine catalog. MCS configures premium and standard disks to use Locally Redundant Storage (LRS). LRS makes multiple synchronous copies of your disk data within a single data center. The storage type you select affects the machine sizes offered later in this wizard.

Premium SSD (supports I/O-intensive workloads with significantly high throughput and low latency)
 Standard SSD
 Standard HDD

You can use Windows volume licenses to provision VMs in Azure at the base compute rate. To verify that your volume licensing agreement with Microsoft qualifies for the Azure base compute rate, consult Microsoft.

Use my Windows Client licenses
 Use my Windows Server licenses
 Use Azure Windows Server licenses

Place image in Azure Shared Image Gallery [?]

Back Next Cancel

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 VM di cui è stato eseguito il provisioning stia utilizzando il vantaggio della 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 all'indirizzo <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 all'indirizzo <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>.

In alternativa, puoi 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 su `New-ProvScheme` e `Set-ProvScheme`.

Esempio di impostazione di `LicenseType` su RHEL_BYOS su `New-provScheme`:

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

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

```

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

```

Nota:

Se il valore `LicenseType` è vuoto, i valori predefiniti sono Azure Windows Server License o Azure Linux License, a seconda del valore `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.

The screenshot shows the 'Machine Catalog Setup' dialog box with the 'Disk Settings' section selected in the left-hand navigation pane. The 'Disk Settings' section includes the following options:

- Write-back cache disk:**
 - Enable write-back cache
 - Memory allocated to cache (MB): 256
 - Disk cache size (GB): 127
- Select the storage type for the write-back cache disk:**
 - Premium SSD
 - Standard SSD
 - Standard HDD
- Select the type for the write-back cache disk:**
 - Use non-persistent write-back cache disk
 - Use persistent write-back cache disk
- System disk:**
 - Retain system disk during power cycles
 - Retain VMs across power cycles
- Customer-managed encryption key:**
 - Use the following key to encrypt data on each machine
 - Select a Disk Encryption Set (dropdown menu)

At the bottom of the dialog, there are 'Back', 'Next', and 'Cancel' buttons.

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**, è possibile 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 <code>mcsdif.vhdx</code> 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 <code>McSWCDisk</code> e su questo disco viene inserito il file WBC <code>mcsdif.vhdx</code> .
Il disco temporaneo dispone di spazio sufficiente per l'utilizzo della cache di riscrittura, ma <code>UseTempDiskForWBC</code> è impostato su false .	Viene creato un disco VHD <code>McSWCDisk</code> e su questo disco viene inserito il file WBC <code>mcsdif.vhdx</code> .

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 `DependsOn` specificato nelle specifiche del modello. Per esempio:

““

“dipendeDa”: [

“[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]]”

],
““

1. Creare **Review+Create** (Rivedi+Crea) e le specifiche del modello.
2. 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).
3. 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:

```
1 get-item XDHyp:\Unità di Hosting\Est\machineprofile.folder\abc.  
resourcegroup\bggTemplateSpec.templatespec
```

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

```
1 get-item XDHyp:\Unità di Hosting\Est\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 modificare la chiave con cui è crittografato il disco, si modifica la chiave corrente nel `DiskEncryptionSet`. Tutte le risorse associate a quel `DiskEncryptionSet` vengono 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. Per farlo, vedi <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 il tuo abbonamento, vedi <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:

```
1 PS XDHyp:\Connessioni\\east us.region\  
serviceoffering.folder>
```

```
1 PS XDHyp:\HostingUnits\\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 desideri utilizzare una specifica del modello, assegna il parametro **Encryption at Host** come **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 la crittografia delle informazioni sull'host da un profilo macchina quando si esegue il comando PowerShell con il parametro **AdditionalData** . Se il parametro

`EncryptionAtHost` è **True**, indica che la crittografia sull'host è abilitata per il profilo del computer.

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

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

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

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

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 sul profilo macchina per creare un catalogo di macchine, è possibile riutilizzare il `DiskEncryptionSetID` memorizzato.
- 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 di macchine che ha già un `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 VM dispongono di un disco temporaneo o di risorse per archiviare un disco del sistema operativo temporaneo, come [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 di PowerShell ([UseWritebackCache](#) e [UseEphemeralOSDisk](#)) hanno esito negativo con i messaggi di errore corretti se li imposti 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*: ogni immagine in una galleria di immagini condivise può avere più versioni e ogni versione può avere più repliche in diverse regioni. 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`. Per esempio:

```
1 PS C:\Utenti\nomeutente> (get-item XDHY:\HostingUnits\
    mynetwork\image.folder\nomeutente-dev-testing-rg.
    resourcegroup\nomeutente-dev-tsvda.vm).AdditionalData
```

I campi dati aggiuntivi sono:

- * `DiskSecurityType`
- * `ConfidentialVMDiskEncryptionSetId`
- * `DiskSecurityProfiles`

Per ottenere la proprietà informatica riservata delle dimensioni di una macchina, esegui il comando seguente: `(Get-Item -path «XDHY p:\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.
 - **Gestione delle chiavi**: Crittografia del disco riservata con una chiave gestita dalla piattaforma Per ulteriori informazioni sulla creazione di VM 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

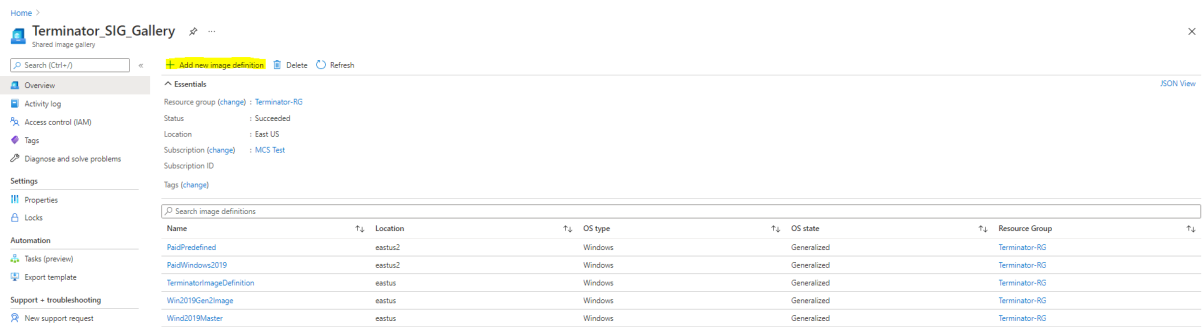
Citrix Virtual Apps and Desktops supporta l'utilizzo di un'immagine master in Azure che contiene informazioni sul piano per creare un catalogo delle macchine. Per ulteriori informazioni, vedere [Microsoft Azure Marketplace](#).

Mancia:

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.

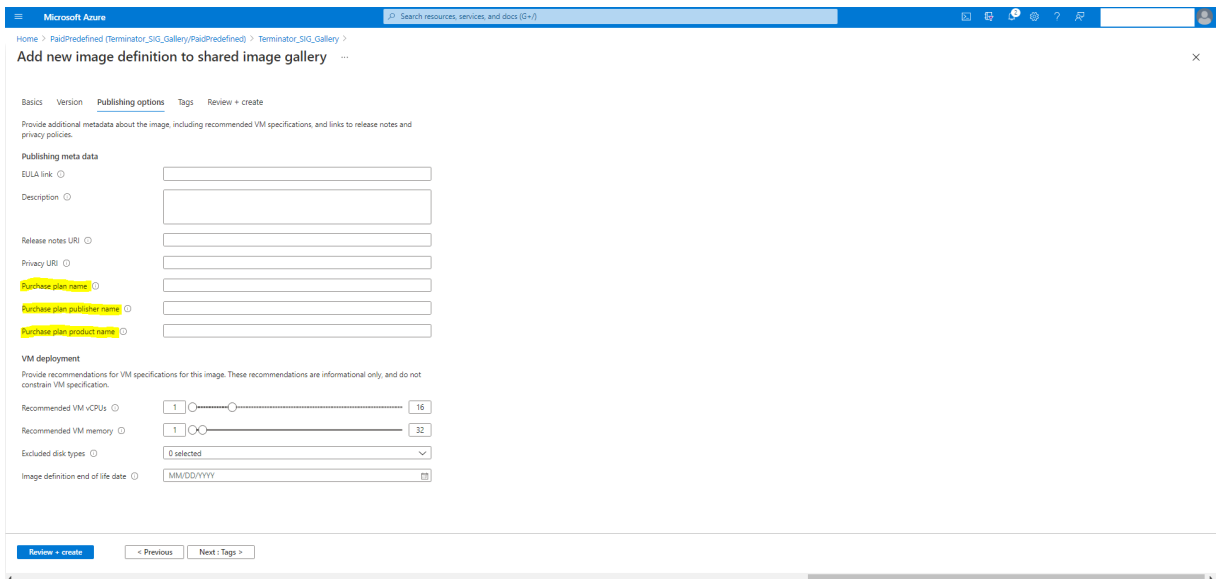
Assicurarsi che l'immagine creata nella Raccolta immagini condivise contenga informazioni sul piano di Azure

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):

Citrix Virtual Apps e Desktop 7 2402 LTSR

Home > Terminator_SIG_Gallery > PaidPredefined (Terminator_SIG_Gallery/PaidPredefined)

Image definition

Search (Ctrl+F)

+ Create VM + Create VMSS Delete Refresh

Overview

Essentials

Resource group (change) : Terminator-RG
Location (change) : East US 2
Subscription (change) : MCS Test
Subscription ID :
Status : Succeeded

Tags (change) :

Shared image gallery : Terminator_SIG_Gallery
Operating system : Windows
Operating system state : Generalized
Publisher : Offer : SKU : PaidPublisher2 : PaidOffer2 : PaidSKU2

Properties Get started Image versions

Filter by number... Showing 1 of 1 image versions

+ Add version Delete

Number	Provisioning State	Published date	Target regions	Replication status	Create VM from version
1.0.0	Succeeded	7/7/2021, 2:13:24 PM	East US	Completed	Create VM

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

Microsoft Azure Search resources, services, and docs (G+V)

Home > Terminator_SIG_Gallery > PaidPredefined (Terminator_SIG_Gallery/PaidPredefined)

Create image version

Basics Replication Encryption Tags Review + create

Create a new image that can be used to deploy virtual machines and virtual machine scale sets. With a shared image, you can easily replicate the image to Azure regions around the world and manage versions of the image. [Learn more](#)

Project details

Subscription : MCS Test
Resource group : Terminator-RG

Instance details

Region : (US) East US

Version details

Version number :
Source : Disks and/or snapshots
OS disk : https://aad-2019
LUN : 0
Data disk : Select a disk or snapshot

Exclude from latest :
End of life date : MM/DD/YYYY

Gallery details

Shared images are part of the Shared Image Gallery service. The image requires 2 additional resources: a gallery and a definition. A gallery is a repository for managing and sharing images. A definition carries information about the image and requirements for using it internally. [Learn more](#)

Target image gallery : Terminator_SIG_Gallery

Review + create < Previous Next : Replication >

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

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

```
1 -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
2 /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
3 XMLSchema-instance"> `
4 <Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
5 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
6 "/> `
7 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
8 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
9 Premium_LRS"/> `
10 <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
11 Premium_LRS"/> `
12 <Property xsi:type="StringProperty" Name="LicenseType" Value="
13 Windows_Client"/> `
14 <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
15 true"/> `
16 </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 disco cache write-back persistente, utilizzare il parametro PowerShell `New-ProvScheme CustomProperties`. Questo parametro supporta una proprietà aggiuntiva, `PersistWBC`, utilizzata per determinare in che modo il disco della cache write-back persiste per le macchine con provisioning MCS. La proprietà `PersistWBC` viene utilizzata solo quando viene specificato il parametro `UseWritebackCache` e quando il parametro `WritebackCacheDiskSize` è impostato per indicare che è stato creato un disco.

Esempi di proprietà presenti nel parametro `CustomProperties` prima di supportare `PersistWBC` includono:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="benva1dev5RG3" />
5 </CustomProperties>
```

Quando utilizzate queste proprietà, tenete presente 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 il computer tramite Web Studio.

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

Nota:

Se la proprietà `PersistWBC` viene omessa, il valore predefinito è **false** e la cache di write-back viene eliminata quando il computer viene spento tramite Web Studio.

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

```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
  benva1dev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>

```

Importante:

La proprietà `PersistWBC` può essere impostata solo utilizzando il cmdlet PowerShell `New-ProvScheme`. Il tentativo di modificare `CustomProperties` di uno schema di provisioning dopo la creazione non ha alcun impatto sul catalogo delle macchine e sulla persistenza del disco di cache write-back quando una macchina viene spenta.

Ad esempio, imposta `New-provScheme` per utilizzare la cache write-back mentre imposti la proprietà `PersistWBC` su `true`:

```

1 Nuovo-ProvScheme
2 -CleanOnBoot
3 -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=`"benva1dev5RG3`" /><Property xsi:type=`"StringProperty`" Name
  =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
  GoldImages.resourcegroup\W10MCSI0-01
  _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.cartella\
  CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
  adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
  cartella\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache

```

```
13 -WriteBackCacheDiskSize 127
14 -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 PowerShell `PersistOsDisk` nel comando `New-ProvScheme` per configurare questa funzionalità. Le opzioni associate a `New-provScheme` includono:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
   />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="Resource ` ` ` ` ` ` <!--NeedCopy
   -->
5 ` ` ` ` ` ` ` ` ` ` Gruppi" Valore="benvaldev5RG3" />
6 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
7 </CustomProperties>
```

Per abilitare questa funzionalità, imposta la proprietà personalizzata `PersistOsDisk` su **true**. Per esempio:

```
1 Nuovo-ProvScheme
2 -CleanOnBoot
3 -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>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.cartella\
   CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
   adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   cartella\Standard_D2s_v3.serviceoffering"
```

```

12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -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. Eseguì `asnp citrix*`.
3. Creare o aggiornare un catalogo.
 - Per creare un catalogo:
 - a) Utilizzate il comando `New-ProvScheme` con una specifica del modello come input del profilo macchina. Per esempio:

```

1 New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
  image.folder/fgthj.resourcegroup/nab-ws-
  vda_OsDisk_1_XXXXXXXXXX.manageddisk"
2 MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
  folder/fgthj.resourcegroup/test.templatespec/V1.
  templatespecversion"
3 -ProvisioningSchemeName <String>
4 -HostingUnitName <String>
5 -IdentityPoolName <String>
6 [-ServiceOffering <String>][-CustomProperties <String>]
7 [-LoggingId <Guid>]
8 [-BearerToken <String>][-AdminAddress <String>]
9 [<CommonParameters>]

```

- b) Completare la creazione del catalogo di macchine.

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

```

1 Italiano: Set-ProvScheme -MasterImageVm 'XDHyp://Connections/
  Azure/East Us.region/vm.folder/MasterDisk.vm'
2 MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
  folder/fgthj.resourcegroup/testing.templatespec/V1.
  templatespecversion'
3 [-ProvisioningSchemeName] <String>

```

```

4 [-CustomProperties <String>] [-ServiceOffering <String>] [-
  PassThru]
5 [-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 **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il seguente comando:

```

1 $s = (ls XDHyp:\HostingUnits\\
  cartellaserviceoffering\<"VM size".serviceoffering)

```

4. Esegui `$s | select -ExpandProperty Dati aggiuntivi`
5. Controlla il valore dell'attributo `SupportTrustedLaunch`.
 - Se `SupportTrustedLaunch` è **True**, la dimensione della VM supporta il lancio affidabile.
 - Se `SupportTrustedLaunch` è **False**, la dimensione della VM non supporta il lancio affidabile.

Come da PowerShell di Azure, è possibile usare il seguente comando per determinare le dimensioni di macchina virtuale che supportano l'avvio attendibile:

```

1 (Get-AzComputeResourceSku | dove {
2   $_.Locations.Contains($region) -e ($_ .Name -eq "<VM size>") }
3 ) [0].Capacities

```

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 seconda generazione e la funzionalità `TrustedLaunchDisabled` è **True**, la dimensione della macchina virtuale di seconda generazione non è supportata per Trusted Launch.
- *Esempio 3:* se la macchina virtuale di Azure supporta solo la seconda generazione e la funzionalità `TrustedLaunchDisabled` non viene visualizzata dopo l'esecuzione del comando PowerShell, la dimensione della macchina virtuale di seconda generazione è supportata per il lancio affidabile.

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 desideri utilizzare i comandi PowerShell, usa 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 VM come input del profilo macchina:

```

1 New-ProvScheme -CleanOnBoot -HostingUnitName "nome" -
   IdentityPoolName "nome" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
   resourcegroup/nab-ws-vda_0sDisk_1_xxxxxxxxxxa.manageddisk"

```

```

3  -MachineProfile "XDHyp:\HostingUnits\\machineprofile.
    folder\

```

Esempio di `New-provScheme` con le specifiche del modello come input del profilo macchina:

```

1  New-ProvScheme -CleanOnBoot -HostingUnitName "nome" -
    IdentityPoolName "nome" -InitialBatchSizeHint 1
2  -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxa.manageddisk"
3  MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
4  -ProvisioningSchemeName <String>
5  -HostingUnitName <String>
6  -IdentityPoolName <String>
7  [-ServiceOffering <String>][-CustomProperties <String>]
8  [<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	<code>ProfiloMacchinaNonSupportatoPerCatalogoNonGestito</code>
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	<code>SecurityTypeNonSupportatoPerUngestedDisk</code>
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	<code>MachineProfileNotFoundForTrustedLaunchMasterImage</code>
Se si seleziona un profilo macchina con un tipo di sicurezza diverso dal tipo di protezione dell'immagine master	<code>SecurityTypeConflictTraMasterImageEMachineProfile</code>

Scenario	Errore
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 `ServiceOffering` non è specificato, viene impostato dal 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` ha tutte le proprietà definite o 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 Ottieni-ProvScheme | seleziona 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 Ottieni-ProvScheme | seleziona 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 Ottieni-ProvScheme | seleziona 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:

```

1 Ottieni-ProvScheme | seleziona 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="<mpA
  -value>"/>
5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<CustomPropertiesA-value>"/>
6 <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
  value>"/>
7 </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

```

1 New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.cartella\azure.resourcegroup\mpA.vm"
2 -ServiceOffering "XDHyp:\HostingUnits\azureunit\
  serviceoffering.cartella\<explicit-machine-size>.
  serviceoffering"

```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```

1 Get-ProvScheme | seleziona ServiceOffering
2 serviceoffering.folder\<explicit-machine-size>.
  serviceoffering
3

```

```

4 Get-ProvScheme | seleziona CustomProperties
5 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
6 <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="explicit-storage-type"/>
7 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "value-from-machineprofile"/>
8 </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.cartella\azure.resourcegroup\mpA.vm"-MasterImageVM
"XDHyp:\HostingUnits\azureunit\immagine.cartella\linux-
master-image.manageddisk"

```

Il valore dell'immagine master viene scritto nelle proprietà personalizzate, in questo caso Linux.

```

1 Ottieni-ProvScheme | seleziona 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 Ottieni-ProvScheme | seleziona 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:

```

1 Ottieni-ProvScheme | seleziona CustomProperties
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="<CustomPropertiesB-value>"/>
4 <Property xsi:type="StringProperty" Name="OSType" Value="<
  CustomPropertiesB-value>"/>
5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<mp-A-value>"/>
6 </CustomProperties>

```

- 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.cartella\azure.resourcegroup\mpB.vm"
```

I seguenti valori sono impostati come proprietà personalizzate per il catalogo:

```
1 Get-ProvScheme | seleziona ServiceOffering
2 serviceoffering.folder\
```

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/estensioni/lettura
 - Microsoft.Compute/virtualMachines/estensioni/scrittura
 - Microsoft.Insights/DataCollectionRuleAssociations/Leggi
 - Microsoft.Insights/dataCollectionRuleAssociations/scrittura
 - Microsoft.Insights/DataCollectionRules/Leggi
- 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 è stata inserita nella whitelist: le estensioni `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` sono estensioni definite da Citrix nella whitelist. Per visualizzare l'elenco delle estensioni inserite nella lista bianca, usa 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:

```
1 {  
2  
3 "type": "Microsoft.Compute/virtualMachines/extensions",  
4 "apiVersion": "2022-03-01",
```

```
5 "name": "<vm-name>/AzureMonitorWindowsAgent",
6 "dependsOn": [
7   "Microsoft.Compute/virtualMachines/<vm-name>"
8 ],
9 "location": "<azure-region>",
10 "properties": {
11
12   "publisher": "Microsoft.Azure.Monitor",
13   "type": "AzureMonitorWindowsAgent", Italiano:
14   "typeHandlerVersion": "1.0",
15   "autoUpgradeMinorVersion": true,
16   "enableAutomaticUpgrade": true
17 }
18
19 }
20 ,
21 {
22
23   "type": "Microsoft.Insights/
24     dataCollectionRuleAssociations",
25   "apiVersion": "2021-11-01",
26   "name": "<associatio-name>",
27   "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
28   "dependsOn": [
29     "Microsoft.Compute/virtualMachines/<vm-name>",
30     "Microsoft.Compute/virtualMachines/<vm-name>/extensions
31       /AzureMonitorWindowsAgent"
32   ],
33   "properties": {
34     "description": "Associazione della regola di
35       raccolta dati. L'eliminazione di questa
36       associazione interromperà la raccolta dati per
37       questo server Arc.",
38     "dataCollectionRuleId": "/subscriptions/<azure-
39       subscription>/resourcegroups/<azure-resource-group>/
40       providers/microsoft.insights/datacollectionrules
41       /<azure-data-collection-rule>"
42   }
43 }
```

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:

```
1 Set-ProvScheme -ProvisioningSchemeName "nome"  
2 -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:

```
1 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. Inserisci `cd xdhyp:/`.
4. Inserisci `cd. \ HostingUnits\` (la tua unità di hosting).
5. Inserisci `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.
Per esempio:

```

1 $customProperties = "<CustomProperties xmlns='http://schemas.
  citrix.com/2014/xd/machinecreation' xmlns:xsi='http://www.w3.
  org/2001/XMLSchema-instance'">
2 <Property xsi:type='StringProperty' Name='StorageAccountType'
  Value='Standard_LRS' />
3 <Property xsi:type='StringProperty' Name='persistWBC' Value='
  False' />
4 <Property xsi:type='StringProperty' Name='PersistOsDisk' Value
  ='false' />
5 <Property xsi:type='StringProperty' Name='UseManagedDisks'
  Value='true' />
6 <Property xsi:type='StringProperty' Name='DiskEncryptionSetId'
  Value='/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxx/
  resourceGroups/abc/providers/Microsoft.Compute/
  diskEncryptionSets/abc-des' />
7 </CustomProperties>

```

9. Creare un pool di identità se non è già stato creato. Per esempio:

```

1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
  Domain def.local -NamingSchemeType Numerico

```

10. Eseguire il comando New-ProvScheme: Ad esempio:

```

1 New-ProvScheme -CleanOnBoot -HostingUnitName "nome" -
  IdentityPoolName "nome" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
  resourcegroup\def.snapshot"
3 -NetworkMapping @{
4   "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
  def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
  " }
5
6 -ProvisioningSchemeName "nome"
7 -ServiceOffering "XDHyp:\UnitàHosting\azure-res2\serviceoffering.
  cartella\Standard_DS2_v2.serviceoffering"
8 -MachineProfile "XDHyp:\UnitàHosting\<adnet>\machineprofile.
  cartella\<def.resourcegroup>\<machine profile vm.vm>"
9 -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 NomeUnitàHosting` (ad 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) Passa a **Disks>Key management** 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, sotto `properties>StorageProfile>OSDisk>ManagedDisk`, aggiungi il parametro `DiskEncryptionSet` e aggiungi 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 utilizzano i comandi di PowerShell, eseguire una delle seguenti operazioni:
 - Se non utilizzi un flusso di lavoro basato sul profilo del computer, aggiungi la proprietà personalizzata `DiskEncryptionSetId` nel comando `New-ProvScheme`. Per esempio:

```

1 New-ProvScheme -CleanOnBoot -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="
    StorageAccountType" Value="Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="
    DiskEncryptionSetId" Value="/subscriptions/12345678-
    xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
    providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
5 </CustomProperties>'
6 -HostingUnitName "Redatto"
7 -IdentityPoolName "Redatto"
8 -InitialBatchSizeHint 1
9 -MasterImageVM "Redatto"
10 -NetworkMapping @{
11 "0"="Redatto" }
12
13 -ProvisioningSchemeName "Redatto"
14 -ServiceOffering "Redatto"

```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input del profilo macchina nel comando `New-ProvScheme`. Per esempio:

```

1 Italiano: New-ProvScheme -CleanOnBoot
2 -HostingUnitName azure-east
3 -IdentityPoolName aio-ip
4 -InitialBatchSizeHint 1
5 -MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
    \abc.resourcegroup\fgb-vda-snapshot.snapshot
6 -NetworkMapping @{
7 "0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
    folder\apa-resourceGroup.resourcegroup\apa-
    resourceGroup-vnet.virtualprivatecloud\default.network"
    }
8
9 -ProvisioningSchemeName aio-test
10 -MachineProfile XDHyp:\Unità di hosting\azure-east\
    machineprofile.cartella\abc.resourcegroup\abx-mp.
    templatespec\1.0.0.templatespecversione

```

5. Completare la creazione di un catalogo utilizzando l'SDK Remote PowerShell. Per informazioni su come creare un catalogo utilizzando Remote PowerShell SDK, vedere <https://developer-do>

cs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Tutte le macchine create nel catalogo sono crittate 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 del computer, aggiungere la proprietà personalizzata `DiskEncryptionSetID` nel comando `Set-ProvScheme`. Per esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2 -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
   resourceGroups/Sample-RG/providers/Microsoft.Compute/
   diskEncryptionSets/SampleEncryptionSet" />
4 </CustomProperties>'
```

- Se si utilizza un flusso di lavoro basato sul profilo macchina, utilizzare un input del profilo macchina nel comando `Set-ProvScheme`. Per esempio:

```
1 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**.

- Eseguire il comando `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.
- Usa `Get-ProvScheme` per ottenere le informazioni del tuo catalogo macchine. Per esempio:

```
1 Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

- Recuperare la proprietà personalizzata DES Id del catalogo di macchine. Per esempio:

```
1 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
  Value="/subscriptions
  /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
  -RG/providers/Microsoft.Compute/diskEncryptionSets/
  SampleEncryptionSet" />
```

- 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 è specificato un valore, tutti i VDA sottoposti a provisioning continuano a utilizzare un disco del sistema operativo fornito.

Di seguito è riportato un esempio di set di proprietà personalizzate da utilizzare nello schema di provisioning:

```
1 "CustomProperties": [
2     {
3
4         "Nome": "UseManagedDisks",
5         "Valore": "vero"
6     }
7 ,
8     {
9
10        "Nome": "StorageType",
11        "Valore": "Standard_LRS"
12    }
13 ,
14    {
15
16        "Nome": "UseSharedImageGallery",
17        "Valore": "vero"
```

```
18     }
19   ,
20     {
21     "Nome": "SharedImageGalleryReplicaRatio",
22     "Valore": "40"
23   }
24   ,
25     {
26     "Nome": "SharedImageGalleryReplicaMaximum",
27     "Valore": "10"
28   }
29   ,
30     {
31     "Nome": "LicenseType",
32     "Valore": "Windows_Server"
33   }
34   ,
35     {
36     "Nome": "UseEphemeralOsDisk",
37     "Valore": "true"
38   }
39 ],
```

Configurare un disco temporaneo per un catalogo

Per configurare un disco del sistema operativo temporaneo di Azure per un catalogo, usa il parametro `UseEphemeralOsDisk` in `Set-ProvScheme`. Imposta il valore del parametro `UseEphemeralOsDisk` su **true**.

Nota:

Per utilizzare questa funzionalità, è necessario abilitare anche i parametri `UseManagedDisks` e `UseSharedImageGallery`.

Per esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-catalogo -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 effettuare il provisioning di dischi del sistema operativo temporanei utilizzando `New-provScheme`, considerate 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 ...altre proprietà personalizzate...
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.

```
1 Get-ChildItem -LiteralPath @"(\"XDHyp:\HostingUnits\testresource\  
image.folder\sharedImageGalleryTest.resourcegroup\"")
```

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

```
1 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.

```
1 Get-ChildItem -LiteralPath @"(\"XDHyp:\HostingUnits\testresource\  
image.folder\sharedImageGalleryTest.resourcegroup\  
sharedImageGallery.sharedimagegallery\sigstestimage.  
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 Remote PowerShell SDK, vedere <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>.

Configurare la Raccolta immagini condivise

Utilizzate il comando `New-provScheme` per creare uno schema di provisioning con il supporto di Shared Image Gallery. Utilizzate 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.

`SharedImageGalleryReplicaMassimo`

- 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.

Mancia:

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. Utilizzate il comando `Set -ProvScheme` per aggiornare le proprietà personalizzate per tutte le macchine esistenti nel catalogo e per tutte le macchine future:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-catalogo -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. Esegui `Set-ProvScheme` con il flag `UseSharedImageGallery` impostato su **True**. È possibile includere le proprietà `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Aggiornare il catalogo.
3. Spegner e riaccendere le macchine per forzare un aggiornamento.

Per esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-catalogo -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>'
```

Mancia:

I parametri `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` non sono obbligatori. Al termine del comando `Set-ProvScheme`, l'immagine della Galleria immagini condivise non è ancora stata 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. Esegui `Set-ProvScheme` con il flag `UseSharedImageGallery` impostato su **False** o non definito.
2. Aggiornare il catalogo.
3. Spegner e riaccendere le macchine per forzare un aggiornamento.

Per esempio:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-catalogo -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>'
```

Mancia:

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. Esegui il comando seguente per visualizzare le proprietà personalizzate originali di Shared Image Gallery: `Get-ProvVM -ProvisioningSchemeName catalog-name`. Al termine del comando `Set-ProvScheme`, l'istantanea dell'immagine non è ancora stata 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. Spegnendo e riaccendendo le macchine, le macchine vengono aggiornate, a quel punto i dati personalizzati della macchina vengono aggiornati per indicare 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.

Eeguire 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, puoi visualizzare gli articoli dell'inventario dell'offerta utilizzando `Get-Item`. Ad esempio, per visualizzare l'offerta di servizi `Standard_B1LS` della 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, utilizzate il parametro `AdditionalData` per l'elemento:

```
$serviceOffering.Datiaggiuntivi
```

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** 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.

Utilizzate 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.

Mancia:

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.

Mancia:

`StorageType` è configurato per un tipo di sistema operativo e un account di archiviazione. `WBCDiskStorageType` è configurato per il tipo di archiviazione cache write-back. Per un

catalogo normale, è richiesto `StorageType`. Se `WBCDiskStorageType` non è configurato, `StorageType` viene utilizzato come predefinito 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 storage per le VM, utilizza il parametro `StorageType` in `New-ProvScheme`. Impostate il valore del parametro `StorageType` su uno dei tipi di storage supportati.

Di seguito è riportato un esempio di set del parametro `CustomProperties` in uno schema di provisioning:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-catalogo -CustomProperties
  '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
  Windows_Client" />
5 </CustomProperties>'
```

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` con i parametri `-StartSnow` e `-DurationInMinutes -1` ed è possibile modificare la macchina esistente dallo storage 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 con `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 crei un nuovo catalogo in Azure usando il comando `New-ProvScheme` PowerShell, usa `Standard_ZRS` come valore nel `StorageAccountType`. Per esempio:

```
1 <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:

- `Tipo di archiviazione`
- `WBCKDiskStorageType`
- `IdentityDiskStorageType`

Nota:

Durante la creazione del catalogo, viene utilizzato il disco OS `StorageType` del profilo macchina se le proprietà personalizzate non sono impostate.

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, inserisci il resourceID completo per l'account di archiviazione come `storageAccountId`.

Una volta che le VM sono configurate per registrare i dati nell'account di storage, i dati possono essere trovati 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 | riepiloga Count=count()per ResourceId
```

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, specifica `EventHubAuthorizationRuleID` nel seguente formato: `/subscriptions/093F4C12-704B-4B1D-8339-F339E7557F60/ResourceGroups/matspo/providers/Microsoft.EventHub/Namespace/matspoeventHub/AuthorizationRules/rootManageSharedSharedChiave di accesso`
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:

```
1 az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
1 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 "ambito": "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 utilizzando il comando `New-ProvScheme`, aggiornare un catalogo macchine esistente utilizzando il comando `Set-ProvScheme` e aggiornare le VM esistenti utilizzando 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>[dimensione minima] [dimensione massima]` (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 pagina 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 eseguire questa operazione eseguendo il comando `New-ProvScheme` includendo le seguenti proprietà personalizzate:

- `PageFileDiskDriveLetterOverride`: posizione del file di pagina, lettera dell'unità disco
- `InitialPageFileSizeInMB`: dimensione del file della pagina iniziale in MB
- `MaxPageFileSizeInMB`: dimensione massima del file di pagina 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"> `
```

```

2 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
  "/> `
3 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
4 <Property xsi:type="StringProperty" Name="
  PageFileDiskDriveLetterOverride" Value="d"/> `
5 <Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
  Value="2048"/> `
6 <Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
  ="8196"/> `
7 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS"/> `
8 <Property xsi:type="StringProperty" Name="LicenseType" Value="
  Windows_Client"/> `
9 </CustomProperties>'

```

Vincoli:

- È possibile aggiornare l'impostazione del file di pagina solo quando si crea uno schema di provisioning eseguendo il comando `New-ProvScheme` e l'impostazione del file di pagina non può essere modificata in seguito.
- Specificate tutte le proprietà relative alle impostazioni del file di pagina (`PageFileDiskDriveLetterOverride`, `InitialPageFileSizeInMB` e `MaxPageFileSizeInMB`) nelle proprietà personalizzate o non specificatene nessuna.
- 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 una dimensione di VM supporta Spot VM, allora

`supportsSpotVM` è **True**.

```
1 (Ottieni elemento "XDHyp:\HostingUnits\azure-res-conn2\
  serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  Dati aggiuntivi
```

- 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 di Azure Spot, devi selezionare l'istanza di Azure Spot (se usi una macchina virtuale) o impostare la priorità " come `Spot` (se usi la specifica del modello).

Passaggi per creare un catalogo utilizzando le macchine virtuali Azure Spot

1. Creare un'origine 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, aggiungi le seguenti proprietà in **resources > type: Microsoft.compute/VirtualMachines > properties** nella specifica del modello. Per esempio:

```
“
“priority”: “Spot”,
“evictionPolicy”: “Dealloca”,
“billingProfile”: {
“maxPrice”: 0,01
```

```
}
“
```

```
1 > **Nota:**
2 >
3 > - Il criterio di sfratto può essere **Deallocate** (Rimuovi
  allocazione) o **Delete** (Elimina).
4 > - 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**.
```

```

5 > - 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.
6 > - 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](https://learn.microsoft.com/it-it/azure/virtual-machines/spot-vms#pricing)
.

```

1. 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 Azure Spot VM. Per esempio,

- Se l'origine del profilo della macchina è una VM, eseguire il comando seguente:

```

1 (Ottieni elemento "XDHyp:\HostingUnits\azure-res-conn2\
machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
delete.vm"). Dati aggiuntivi

```

- Se l'origine del profilo macchina è una specifica di modello, eseguire il comando seguente:

```

1 (Ottieni elemento "XDHyp:\HostingUnits\azure-res-conn2\
machineprofile.folder\fifthcolumn.resourcegroup\fc-ae-
templatespec.templatespec\14.0.0-spot-delete.
templatespecversion").AdditionalData

```

2. Crea 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 `Set-ProvScheme` PowerShell.
- 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, imposta una finestra temporale di aggiornamento per le VM utilizzando `Set-ProvVmUpdateTimeWindow` e avvia le VM all'interno della 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 nello schema di provisioning.

Creare un catalogo con le dimensioni delle VM di backup

Nota:

Per risolvere il problema del blocco dell'interfaccia utente di Studio, sostituisci tutte le virgolette singole con `"`; durante l'esecuzione dei comandi PowerShell.

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. Vedi [Come configurare la configurazione di backup](#).
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`. Vedi [Come configurare la configurazione di backup](#).

Aggiornare le macchine virtuali esistenti

È possibile aggiornare le VM esistenti in un catalogo utilizzando il comando `Set-ProvVmUpdateTimeWindow` PowerShell. Il comando aggiorna le VM create dallo schema di provisioning associato al catalogo alla successiva accensione entro la finestra temporale specificata. Per 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 programmata. `DurationInMinutes` è la finestra temporale della pianificazione.

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, imposta una finestra temporale di aggiornamento per le VM utilizzando `Set-ProvVmUpdateTimeWindow` e avvia le VM all'interno della finestra. Per esempio:

1. Esegui il comando `Set-ProvVM` per configurare l'elenco delle dimensioni delle VM di backup per una VM MCS esistente selezionata. Per esempio:

```

1 Set-ProvVM -ProvisioningSchemeName "nome" -VMName "Vm-001"
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"/>
8 <Property xsi:type="StringProperty" Name="BackupVmConfiguration
   " Value="{
9   &quot;ServiceOffering&quot;; &quot;Standard_D2as_v4&quot;; &quot;
   Type&quot;; &quot;Spot&quot;; }
10 , {
```

```

11  &quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;; &quot;
    Type&quot;: &quot;Regular&quot; }
12  , {
13  &quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;; &quot;
    Type&quot;: &quot;Spot&quot; }
14  ]`"/>
15 </CustomProperties>"

```

2. Esegui il comando `Set-ProvVmUpdateTimeWindow` per applicare gli aggiornamenti. Per esempio:

```

1 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.

```

“
“tag”: {
“TagC”: “Valore3”

```

```

},
“

```

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. Per esempio:

```
1 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. Per esempio:

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <  
YourCatalogName> -VMName macchina1 -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 non corrisponde il numero di NIC forniti nel profilo della macchina e il numero di NIC forniti nel 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

- [Crea e gestisci connessioni e risorse](#)
- [Connessione a Microsoft Azure Resource Manager](#)
- [Creare cataloghi di macchine](#)

Gestire i cataloghi delle macchine

January 24, 2025

Nota:

È possibile gestire la distribuzione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basata sul Web) e Citrix Studio (basata 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.

Introduzione

È possibile aggiungere o rimuovere macchine da un catalogo macchine, rinominarle, modificarne la descrizione o gestire gli account computer Active Directory di un catalogo.

La manutenzione dei cataloghi può includere anche la verifica che ogni macchina disponga degli ultimi aggiornamenti del sistema operativo. Inclusi aggiornamenti antivirus, upgrade del sistema operativo o modifiche alla configurazione.

- I cataloghi contenenti macchine casuali raggruppate, create utilizzando Machine Creation Services (MCS), gestiscono le macchine aggiornando l'immagine master utilizzata nel catalogo e quindi aggiornando le macchine stesse. Questo metodo consente di aggiornare in modo efficiente un gran numero di macchine utente.
- Per i cataloghi contenenti macchine statiche assegnate in modo permanente e per i cataloghi di macchine con accesso remoto al PC, gli aggiornamenti alle macchine degli utenti vengono

gestiti all'esterno di Web Studio. Eseguire questa attività individualmente o collettivamente utilizzando strumenti di distribuzione software di terze parti.

Per informazioni sulla creazione e la gestione delle connessioni agli hypervisor host, vedere [Connessioni e risorse](#).

Nota:

MCS non supporta Windows 10 IoT Core e Windows 10 IoT Enterprise. Per ulteriori informazioni, fare riferimento al sito Microsoft .

Informazioni sulle istanze persistenti

Quando si aggiorna un catalogo MCS creato utilizzando istanze persistenti o dedicate, tutte le nuove macchine create per il catalogo utilizzano l'immagine aggiornata. Le istanze preesistenti continuano a utilizzare l'istanza originale. Il processo di aggiornamento di un'immagine avviene nello stesso modo per qualsiasi altro tipo di catalogo. Considera quanto segue:

- Con i cataloghi di dischi persistenti, le macchine preesistenti non vengono aggiornate alla nuova immagine, ma tutte le nuove macchine aggiunte al catalogo utilizzano la nuova immagine.
- Per i cataloghi di dischi non persistenti, l'immagine della macchina viene aggiornata al successivo ripristino della macchina.
- Con i cataloghi macchine persistenti, l'aggiornamento dell'immagine aggiorna anche le istanze del catalogo che la utilizzano.
- Per i cataloghi che non persistono, se si desiderano immagini diverse per macchine diverse, le immagini devono risiedere in cataloghi separati.

Gestire i cataloghi delle macchine

È possibile gestire un catalogo macchine in due modi:

- Utilizzo di Web Studio
- Utilizzo di PowerShell

Utilizzare Web Studio

Questa sezione descrive in dettaglio come gestire i cataloghi utilizzando Web Studio:

- [Visualizza i dettagli del catalogo](#)
- [Aggiungere macchine a un catalogo](#)
- [Eliminare macchine da un catalogo](#)
- [Modificare un catalogo](#)

- Rinominare un catalogo
- [Spostare un catalogo in una zona diversa](#)
- [Eliminare un catalogo](#)
- [Gestire gli account dei computer Active Directory in un catalogo](#)
- [Aggiornare un catalogo](#)
- [Cambia il livello funzionale o annulla la modifica](#)
- [Clonare un catalogo](#)
- [Organizzare i cataloghi utilizzando le cartelle](#)

Visualizza i dettagli del catalogo

1. Utilizzare la funzione di ricerca per individuare un catalogo di macchine specifico. Per istruzioni, fare riferimento a [Cerca istanze](#).
2. Dai risultati della ricerca, seleziona un catalogo a seconda delle tue esigenze.
3. Per la descrizione delle colonne del catalogo, fare riferimento alla tabella seguente.
4. Per ulteriori informazioni su questo catalogo, fare clic su una scheda nel riquadro dei dettagli in basso.

Colonna	Descrizione
Catalogo Macchine	Il nome e il tipo di allocazione del catalogo. I tipi di allocazione includono: Casuale: le macchine nel catalogo vengono assegnate a un utente in modo casuale.
Tipo di macchina	Permanente: le macchine nel catalogo vengono assegnate a un utente in modo permanente. Tipo di sistema operativo: sistema operativo multisessione (virtuale); Dati utente: ignora. Tipo di sistema operativo: sistema operativo multisessione (virtuale); dati utente: su disco locale
Conteggio delle macchine	Tipo di sistema operativo: sistema operativo a sessione singola (virtuale) o sistema operativo a sessione singola (virtuale); dati utente: ignora
Conteggio assegnato	Il numero di macchine nel catalogo assegnate a un gruppo di consegna. Tipo di sistema operativo: sistema operativo a sessione singola (virtuale); dati utente: su disco locale

Colonna	Descrizione
Cartella	Posizione del catalogo all'interno dell'albero Cataloghi macchine . Visualizza il nome della cartella in cui si trova il catalogo (inclusa la barra rovesciata finale) oppure – se il catalogo si trova al livello radice.
Aggiornamento VDA	Stato di aggiornamento VDA. I valori possibili includono: Non configurato, Pianificato, Disponibile e Aggiornato.
Stato dell'immagine	Lo stato di aggiornamento delle immagini del catalogo. Applicabile solo ai cataloghi di macchine non persistenti. I valori possibili includono: Completamente aggiornato, Parzialmente aggiornato, Aggiornamenti in sospenso, Preparazione

Aggiungere macchine a un catalogo

Prima di iniziare:

- Assicurarsi che l'host di virtualizzazione disponga di processori, memoria e storage sufficienti per ospitare le macchine aggiuntive.
- Assicuratevi di avere un numero sufficiente di account computer Active Directory inutilizzati. Se si utilizzano account esistenti, il numero di macchine che è possibile aggiungere è limitato dal numero di account disponibili.
- Se si utilizza Web Studio per creare account computer Active Directory per i computer aggiuntivi, è necessario disporre dell'autorizzazione di amministratore di dominio appropriata.

Per aggiungere macchine a un catalogo:

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo macchine, quindi seleziona **Aggiungi macchine** nella barra delle azioni.
4. Seleziona il numero di macchine virtuali da aggiungere.
5. Se non sono presenti account Active Directory sufficienti per il numero di VM che si desidera aggiungere, selezionare il dominio e la posizione in cui vengono creati gli account. Specificare uno schema di denominazione dell'account, utilizzando caratteri cancellato per indicare dove compaiono numeri o lettere sequenziali. Non utilizzare una barra (/) nel nome di una OU. Un nome non può iniziare con un numero. Ad esempio, uno schema di denominazione PC-Sales-##

(con 0-9 selezionato) genera account computer denominati PC-Sales-01, PC-Sales-02, PC-Sales-03 e così via.

6. Se si utilizzano account Active Directory esistenti, accedere agli account oppure fare clic su **Importa** e specificare un file .csv contenente i nomi degli account. Assicurati che ci siano abbastanza account per tutte le macchine che vuoi aggiungere. Web Studio gestisce questi account. Consentire a Web Studio di reimpostare le password per tutti gli account oppure specificare la password dell'account, che deve essere la stessa per tutti gli account.

Le macchine vengono create come processo in background e, se vengono create numerose macchine, possono richiedere molto tempo. La creazione della macchina continua anche se si chiude Web Studio.

Eliminare macchine da un catalogo

Dopo aver eliminato una macchina da un catalogo macchine, gli utenti non potranno più accedervi, quindi prima di eliminare una macchina, assicurati che:

- I dati utente sono stati sottoposti a backup o non sono più necessari.
- Tutti gli utenti vengono disconnessi. L'attivazione della modalità di manutenzione impedisce che vengano stabilite nuove connessioni a una macchina.
- Le macchine sono spente.

Per eliminare macchine da un catalogo:

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo, quindi seleziona **Visualizza macchine** nella barra delle azioni.
4. Seleziona una o più macchine, quindi seleziona **Elimina** nella barra delle azioni.

Scegliere se eliminare le macchine da rimuovere. Se si sceglie di eliminare le macchine, indicare se gli account Active Directory per tali macchine vengono mantenuti, disabilitati o eliminati.

Modificare un catalogo

1. Nella pagina **Descrizione**, modifica la descrizione del catalogo.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo, quindi seleziona **Modifica catalogo macchina** nella barra delle azioni.
4. Nella pagina **Ambiti**, modifica gli ambiti.
5. A seconda del tipo di catalogo, potresti visualizzare altre pagine.

Per i cataloghi creati utilizzando un'immagine di Azure Resource Manager, sono visibili le pagine seguenti. Tieni presente che le modifiche apportate verranno applicate solo alle macchine che aggiungerai al catalogo in un secondo momento. Le macchine esistenti rimangono invariate.

- Nella pagina **Macchine virtuali**, modifica le dimensioni della macchina e le zone di disponibilità in cui desideri creare le macchine.

Nota:

- Vengono mostrate solo le dimensioni delle macchine supportate dal catalogo.
- Se necessario, selezionare **Mostra solo le dimensioni macchina utilizzate in altri cataloghi macchina** per filtrare l'elenco delle dimensioni macchina.

- On the **Machine Profile** page, choose whether to use or change a machine profile.
- (Visible only when the catalog is configured with a dedicated group host) On the **Dedicated host group** page, choose whether to change a host group.
- On the **Storage and License Types** page, choose whether to change the storage type, license type, and Azure Computer Gallery settings (available only when **Place prepared image in Azure Gallery** is in use).

Nota:

Se la nuova impostazione selezionata non supporta le dimensioni correnti della macchina, viene visualizzata una finestra di dialogo di avviso che informa che la modifica dell'impostazione comporta il ripristino delle impostazioni relative alle dimensioni della macchina. Se scegli di continuare, accanto al menu **Macchine virtuali** apparirà un punto rosso che ti chiederà di selezionare una nuova dimensione della macchina.

- On the **License Type** page, choose whether to change the Windows license or Linux license setting.

Per i cataloghi di Accesso PC remoto sono visibili le seguenti pagine:

- On the **Power Management** page, change the power management settings and select a power management connection.
- Nella pagina **Unità organizzative**, aggiungi o rimuovi le OU di Active Directory.

6. Fai clic su **Applica** per applicare le modifiche apportate e fai clic su **Salva** per uscire.

Rinominare un catalogo

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo, quindi seleziona **Rinomina catalogo macchina** nella barra delle azioni.
4. Inserisci il nuovo nome.

Spostare un catalogo in una zona diversa

Se la distribuzione ha più di una zona, è possibile spostare un catalogo da una zona all'altra.

Lo spostamento di un catalogo in una zona diversa dall'hypervisor contenente le VM in quel catalogo influisce sulle prestazioni.

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo, quindi seleziona **Sposta** nella barra delle azioni.
4. Seleziona la zona in cui desideri spostare il catalogo.

Eliminare un catalogo

Prima di eliminare un catalogo, assicurati che:

- Tutti gli utenti vengono disconnessi e non è possibile eseguire sessioni disconnesse.
- La modalità di manutenzione è attivata per tutte le macchine nel catalogo, in modo che non sia possibile effettuare nuove connessioni.
- Tutte le macchine presenti nel catalogo sono spente.
- Il catalogo non è associato ad alcun gruppo di consegna. In altre parole, il gruppo di consegna non contiene macchine dal catalogo.

Per eliminare un catalogo:

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo, quindi seleziona **Elimina catalogo macchina** nella barra delle azioni.
4. Indica se le macchine nel catalogo vengono eliminate. Se si sceglie di eliminare le macchine, indicare se gli account computer Active Directory per tali macchine vengono mantenuti, disabilitati o eliminati.

Gestire gli account dei computer Active Directory in un catalogo

Per gestire gli account di Active Directory in un catalogo macchine, è possibile:

- Liberare gli account macchina inutilizzati rimuovendo gli account computer Active Directory dai cataloghi dei sistemi operativi a sessione singola e multisezione. Tali account potranno poi essere utilizzati per altre macchine.
- Aggiungere account in modo che, quando si aggiungono più macchine al catalogo, gli account dei computer siano già attivi. Non utilizzare una barra (/) nel nome di una OU.

Per gestire gli account di Active Directory:

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo, quindi seleziona **Gestisci account AD** nella barra delle azioni.
4. Scegli se aggiungere o eliminare account computer. Se aggiungi account, specifica cosa fare con le password degli account: reimpostarli tutti o immettere una password valida per tutti gli account.

È possibile reimpostare le password se non si conoscono le password dell'account corrente; per eseguire una reimpostazione della password è necessario disporre dell'autorizzazione. Quando si immette una password, la password viene modificata negli account durante l'importazione. Quando elimini un account, scegli se mantenerlo, disabilitarlo o eliminarlo in Active Directory.

Indica se gli account di Active Directory vengono mantenuti, disabilitati o eliminati quando si rimuovono macchine da un catalogo o si elimina un catalogo.

Aggiornare un catalogo

Si consiglia di salvare copie o snapshot delle immagini master prima di aggiornare le macchine nel catalogo. Il database conserva una registrazione storica delle immagini master utilizzate con ciascun catalogo macchina. Ripristinare o ripristinare le macchine in un catalogo in modo che utilizzino la versione precedente dell'immagine master. Esegui questa attività se gli utenti riscontrano problemi con gli aggiornamenti distribuiti sui loro desktop. Ciò riduce al minimo i tempi di inattività dell'utente. Non eliminare, spostare o rinominare le immagini master. Non è possibile ripristinare un catalogo per utilizzarli.

Dopo l'aggiornamento, la macchina si riavvia automaticamente.

Aggiorna o crea un'immagine master

Prima di aggiornare il catalogo delle macchine, aggiorna un'immagine master esistente o creane una sull'hypervisor host.

1. Sull'hypervisor, esegui uno snapshot della VM corrente e assegnagli un nome significativo. Se necessario, questo snapshot può essere utilizzato per ripristinare (rollback) le macchine nel catalogo.
2. Se necessario, accendere l'immagine master ed effettuare l'accesso.
3. Installare gli aggiornamenti o apportare le modifiche necessarie all'immagine master.
4. Spegnerla la macchina virtuale.
5. Scattare uno snapshot della VM. Assegnargli un nome significativo che venga riconosciuto quando il catalogo viene aggiornato in Web Studio. Sebbene Web Studio possa creare uno

snapshot, Citrix consiglia di crearlo tramite la console di gestione dell'hypervisor. Quindi seleziona lo snapshot in Web Studio. Questo processo consente di fornire un nome e una descrizione significativi anziché un nome generato automaticamente. Per le immagini master GPU, è possibile modificare l'immagine master solo tramite la console XenServer.

Cambia l'immagine principale

Per preparare e distribuire l'aggiornamento su tutte le macchine in un catalogo:

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona un catalogo, quindi seleziona **Cambia immagine master** nella barra delle azioni.
4. Nella pagina **Immagine**, seleziona l'host e l'immagine che vuoi distribuire. > **Suggerimento:** >> Per un catalogo creato da MCS, è possibile annotare l'immagine aggiungendo una nota. Una nota può contenere fino a 500 caratteri. Ogni volta che si modifica l'immagine master, viene creata una voce relativa alla nota, indipendentemente dal fatto che si aggiunga una nota. Se si aggiorna un catalogo senza aggiungere una nota, la voce appare come null (-). Per visualizzare la cronologia delle note per l'immagine, seleziona il catalogo, clicca su **Proprietà modello** nel riquadro in basso, quindi clicca su **Visualizza cronologia note**.
5. Nella pagina **Strategia di distribuzione**, scegli quando le macchine nel catalogo macchine verranno aggiornate con la nuova immagine master: al successivo arresto o immediatamente. > **Nota:** >> La pagina **Strategia di distribuzione** non è disponibile per le VM persistenti perché il rollout è applicabile solo alle VM non persistenti.
6. Verificare le informazioni nella pagina **Riepilogo** e quindi fare clic su **Fine**. Ogni macchina si riavvia automaticamente dopo l'aggiornamento.

Per monitorare l'avanzamento dell'aggiornamento, individuare il catalogo in **Cataloghi macchine** per visualizzare la barra di avanzamento in linea e il grafico di avanzamento passo dopo passo.

Quando si aggiorna un catalogo utilizzando direttamente PowerShell SDK anziché Web Studio, specificare un modello di hypervisor (**VMTemplates**). Utilizzalo come alternativa a un'immagine o a un'istantanea di un'immagine.

Strategia di lancio:

L'aggiornamento delle immagini al successivo arresto avrà effetto immediato su tutte le macchine non in uso, ovvero quelle che non dispongono di una sessione utente attiva. Un sistema in uso riceve l'aggiornamento al termine della sessione attiva corrente. Considera quanto segue:

- Non sarà possibile avviare nuove sessioni finché l'aggiornamento non sarà completato sui computer interessati.
- Per le macchine con sistema operativo a sessione singola, l'aggiornamento avviene immediatamente quando non sono in uso o quando gli utenti non hanno effettuato l'accesso.

- Per un sistema operativo multisessione con macchine secondarie, i riavvii non avvengono automaticamente. Per applicare l'immagine master aggiornata, riavviare i computer tramite Studio, PowerShell o Workspace. Il riavvio dalle macchine o dall'hypervisor non applica l'aggiornamento.

Mancia:

Limitare il numero di macchine riavviate utilizzando le impostazioni avanzate per una connessione host. Utilizzare queste impostazioni per modificare le azioni intraprese per un determinato catalogo; le impostazioni avanzate variano a seconda dell'hypervisor.

Ripristina l'immagine master

Dopo aver distribuito un'immagine master nuova o aggiornata, è possibile ripristinarla. Questo processo potrebbe essere necessario se si verificano problemi con le macchine appena aggiornate. Quando si esegue il rollback, le macchine nel catalogo vengono riportate all'ultima immagine funzionante. Tutte le nuove funzionalità che richiedono l'immagine più recente non saranno più disponibili. Come per il rollout, anche il rollback di una macchina comporta un riavvio.

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Selezionare il catalogo, quindi selezionare **Ripristina immagine master** nella barra delle azioni.
4. Specificare quando applicare l'immagine master precedente alle macchine, come descritto nella sezione precedente per l'operazione di rollout.

Il rollback viene applicato solo alle macchine che devono essere ripristinate. Le macchine che non vengono aggiornate con la nuova immagine master o con quella aggiornata non ricevono messaggi di notifica e non sono costrette a disconnettersi.

Per monitorare l'avanzamento del rollback, individuare il catalogo in **Cataloghi macchine** per visualizzare la barra di avanzamento in linea e il grafico di avanzamento passo dopo passo.

Cambia il livello funzionale o annulla la modifica

Modificare il livello funzionale del catalogo macchine dopo aver aggiornato i VDA sulle macchine a una versione più recente. Citrix consiglia di aggiornare tutti i VDA alla versione più recente per consentire l'accesso a tutte le funzionalità più recenti.

Prima di modificare il livello funzionale di un catalogo macchine:

- Avviare le macchine aggiornate in modo che si registrino con il Controller. Questo processo consente a Web Studio di determinare se le macchine nel catalogo necessitano di un aggiornamento.

Per modificare il livello funzionale di un catalogo:

1. Accedi a Web Studio.
2. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
3. Seleziona il catalogo. La scheda **Dettagli** nel riquadro inferiore mostra le informazioni sulla versione.
4. Seleziona **Modifica livello funzionale**. Se Web Studio rileva che il catalogo necessita di un aggiornamento, visualizza un messaggio. Segui le istruzioni. Se una o più macchine non possono essere aggiornate, un messaggio ne spiega il motivo. Per garantire il corretto funzionamento di tutte le macchine, Citrix consiglia di risolvere i problemi delle macchine prima di fare clic su **Modifica** per procedere.

Una volta completata la modifica del catalogo, è possibile ripristinare le versioni VDA precedenti delle macchine selezionando il catalogo e quindi selezionando **Annulla modifica del livello funzionale** nella barra delle azioni.

Clonare un catalogo

Prima di clonare un catalogo, tieni presente le seguenti considerazioni:

- Non è possibile modificare le impostazioni associate al sistema operativo e alla gestione della macchina. Il catalogo clonato eredita tali impostazioni dall'originale.
- La clonazione di un catalogo può richiedere del tempo. Se necessario, seleziona **Nascondi avanzamento** per eseguire la clonazione in background.
- Il catalogo clonato eredita il nome dell'originale e ha il suffisso **Copia**. Puoi cambiare il nome. Vedere Rinominare un catalogo.
- Una volta completata la clonazione, assicurarsi di assegnare il catalogo clonato a un gruppo di distribuzione.

1. Accedi a Web Studio, quindi seleziona **Cataloghi macchine** nel riquadro a sinistra.
2. Seleziona un catalogo, quindi seleziona **Clona** nella barra delle azioni.
3. Nella finestra **Clona catalogo macchine selezionato**, visualizza le impostazioni per il catalogo clonato e configura le impostazioni come applicabile. Selezionare **Avanti** per procedere alla pagina successiva.
4. Nella pagina **Riepilogo**, visualizza un riepilogo delle impostazioni e seleziona **Fine** per avviare la clonazione.
5. Se necessario, seleziona **Nascondi avanzamento** per eseguire la clonazione in background.

Organizzare i cataloghi utilizzando le cartelle

È possibile creare cartelle per organizzare i cataloghi e facilitarne l'accesso. Ad esempio, è possibile organizzare i cataloghi in base al tipo di immagine o alla struttura organizzativa.

Crea una cartella catalogo

Prima di iniziare, pianifica come organizzare i tuoi cataloghi. Considera quanto segue:

- È possibile nidificare cartelle fino a cinque livelli di profondità (esclusa la cartella radice predefinita).
- Una cartella catalogo può contenere cataloghi e sottocartelle.
- Tutti i nodi in Web Studio (ad esempio i nodi **Cataloghi macchine** e i nodi **Applicazioni**) condividono un albero di cartelle nel backend. Per evitare conflitti di nomi con altri nodi durante la ridenominazione o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in nodi diversi.

Per creare una cartella catalogo, segui questi passaggi:

1. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
2. Nella gerarchia delle cartelle, seleziona una cartella e poi seleziona **Crea cartella** nella barra **Azione**.
3. Inserisci un nome per la nuova cartella, quindi fai clic su **Fatto**.

Mancia:

Se si crea una cartella in una posizione non desiderata, è possibile trascinarla nella posizione corretta.

Spostare un catalogo

È possibile spostare un catalogo tra le cartelle. I passaggi dettagliati sono i seguenti:

1. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
2. Visualizza i cataloghi per cartella. Puoi anche attivare **Visualizza tutto** sopra la gerarchia delle cartelle per visualizzare tutti i cataloghi contemporaneamente.
3. Fare clic con il pulsante destro del mouse su un catalogo e quindi selezionare **Sposta catalogo macchina**.
4. Seleziona la cartella in cui vuoi spostare il catalogo, quindi fai clic su **Fatto**.

Mancia:

È possibile trascinare un catalogo in una cartella.

Gestisci cartelle catalogo

È possibile eliminare, rinominare e spostare le cartelle del catalogo.

È possibile eliminare una cartella solo se essa e le sue sottocartelle non contengono cataloghi.

Per gestire una cartella, seguire i passaggi seguenti:

1. Selezionare **Cataloghi macchine** nel riquadro di sinistra.
2. Nella gerarchia delle cartelle, seleziona una cartella, quindi seleziona un'azione nella barra **Azione** in base alle tue esigenze:
 - Per rinominare la cartella, seleziona **Rinomina cartella**.
 - Per eliminare la cartella, seleziona **Elimina cartella**.
 - Per spostare la cartella, seleziona **Sposta cartella**.
3. Seguire le istruzioni sullo schermo per completare i passaggi rimanenti.

Utilizzare PowerShell

Questa sezione descrive in dettaglio come gestire i cataloghi utilizzando PowerShell:

- [Recupera avvisi ed errori associati a un catalogo](#)
- [Aggiungere descrizioni a un'immagine](#)
- [Reimpostare il disco del sistema operativo](#)
- [Modificare l'impostazione di rete per uno schema di provisioning esistente](#)
- [Gestire le versioni di un catalogo macchine](#)
- [Convertire un catalogo macchine non basato su profili macchina in un catalogo macchine basato su profili macchina](#)
- [Riparare le informazioni di identità degli account di computer attivi](#)
- [Modificare la configurazione della cache su un catalogo di macchine esistente](#)
- [Supporto per l'aggiornamento VDA tramite accesso alla condivisione file locale](#)

Recupera avvisi ed errori associati a un catalogo

È possibile ottenere errori e avvisi storici per comprendere i problemi del catalogo macchine MCS e risolverli.

Utilizzando i comandi di PowerShell è possibile:

- Ottieni un elenco di errori o avvisi

- Cambia lo stato di avviso da **Nuovo** a **Riconosciuto**
- Elimina gli errori o gli avvisi

Per eseguire i comandi di PowerShell:

1. Aprire una finestra di PowerShell.
2. Eseguire `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.

Per ottenere un elenco di errori e avvisi:

Esegui il comando `Get-ProvOperationEvent`.

- Senza parametri: Ottiene tutti gli errori e gli avvisi
- Con i parametri `LinkedObjectType` e `LinkedObjectId`: Ottiene tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con il parametro `EventId`: ottiene un errore o un avviso specifico che corrisponde a questo ID evento
- Con il parametro `Filtro`: Ottiene errori o avvisi tramite filtro personalizzato

Per modificare lo stato degli errori o degli avvisi da **Nuovo** a **Riconosciuto**:

Esegui il comando `Confirm-ProvOperationEvent`.

- Con il parametro `EventId`: imposta lo stato di un errore o di un avviso specifico che corrisponde a questo ID evento. È possibile ottenere l'EventId " di un errore o avviso specifico come output dal comando `Get-ProvOperationEvent`
- Con i parametri `LinkedObjectType` e `LinkedObjectId`: imposta lo stato di tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con **Tutti i parametri**: Imposta lo stato di tutti gli errori e gli avvisi come **Riconosciuto**

Per eliminare gli errori o gli avvisi:

Esegui il comando `Remove-ProvOperationEvent`.

- Con il parametro `EventId`: rimuove un errore o un avviso specifico che corrisponde a questo ID evento. È possibile ottenere l'EventId " di un errore o avviso specifico come output dal comando `Get-ProvOperationEvent`
- Con i parametri `LinkedObjectType` e `LinkedObjectId`: rimuove tutti gli errori e gli avvisi associati a uno schema di provisioning specifico
- Con **Tutti i parametri**: rimuove tutti gli errori e gli avvisi

Per ulteriori informazioni, vedere [Citrix PowerShell SDK](#).

Aggiungere descrizioni a un'immagine

È possibile aggiungere descrizioni informative sulle modifiche relative agli aggiornamenti delle immagini per i cataloghi delle macchine. Utilizzare questa funzione per aggiungere una descrizione du-

rante la creazione di un catalogo o quando si aggiorna un'immagine master esistente per un catalogo. È anche possibile visualizzare informazioni per ciascuna immagine master nel catalogo. Utilizzare i seguenti comandi per aggiungere o visualizzare le descrizioni delle immagini:

- Per aggiungere una nota durante la creazione di un catalogo macchine con un'immagine master, utilizzare il parametro `MasterImageNote` nel comando `NewProvScheme`. Per esempio:

```
1 C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
   HostingUnitName <name> -IdentityPoolName <name> -
   MasterImageVM
2 XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.
   snapshot -MasterImageNote "Note"
```

- Per aggiornare l'immagine master associata a un catalogo macchine, utilizzare il parametro `MasterImageNote` nel comando `Publish-ProvMasterVMImage`. Per esempio:

```
1 C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
   -MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
   name>.vm\base.snapshot -MasterImageNote "Note"
```

- Per visualizzare le informazioni per ciascuna immagine, utilizzare il comando `Get-ProvSchemeMasterVMImageHistory`. Per esempio:

```
1 C:\PS>Get-ProvSchemeMasterVMImageHistory -
   ProvisioningSchemeName MyScheme -Showall
```

Per monitorare l'avanzamento del rollback, individuare il catalogo in **Cataloghi macchine** per visualizzare la barra di avanzamento in linea e il grafico di avanzamento passo dopo passo.

Non è possibile effettuare il rollback in determinati scenari, tra cui quelli riportati di seguito. (L'opzione **Ripristina immagine master** non è visibile).

- Non hai l'autorizzazione per effettuare il rollback.
- Il catalogo non è stato creato utilizzando MCS.
- Il catalogo è stato creato utilizzando un'immagine del disco del sistema operativo.
- Lo snapshot utilizzato per creare il catalogo è danneggiato.
- Le modifiche apportate dall'utente alle macchine nel catalogo non vengono mantenute.
- Le macchine presenti nel catalogo sono in funzione.

Reimpostare il disco del sistema operativo

Utilizzare il comando PowerShell `Reset-ProvVMDisk` per reimpostare il disco del sistema operativo di una VM persistente in un catalogo macchine creato da MCS. Attualmente questa funzionalità è applicabile ad AWS, Azure, XenServer, Google Cloud. Ambienti di virtualizzazione SCVMM e VMware.

Per eseguire correttamente il comando PowerShell, assicurarsi che:

- Le VM di destinazione si trovano in un catalogo MCS persistente.
- Il catalogo delle macchine MCS funziona correttamente.
- Ciò implica che lo schema di provisioning e l'host esistono e che lo schema di provisioning contiene voci corrette.
- L'hypervisor non è in modalità di manutenzione.
- Le VM di destinazione sono spente e in modalità di manutenzione.

Per reimpostare il disco del sistema operativo, procedere come segue:

1. Aprire una finestra di PowerShell.
2. Eseguire **asnp citrix*** per caricare i moduli PowerShell specifici di Citrix.
3. Eseguire il comando PowerShell `Reset-ProvVMDisk` in uno dei seguenti modi:
 - Specificare l'elenco delle VM come elenco separato da virgole ed eseguire il ripristino su ciascuna VM:

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc", "def") -OS
```

- Specificare l'elenco delle VM come output dal comando `Get-ProvVM` ed eseguire il ripristino su ciascuna VM:

```
1 (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc" -OS
```

- Specificare una singola VM per nome:

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- Creare attività di ripristino separate per ciascuna delle VM restituite dal comando `Get-ProvVM`. Questa soluzione è meno efficiente perché ogni attività eseguirà gli stessi controlli ridondanti, come il controllo della capacità dell'hypervisor e il controllo della connessione per ogni VM.

```
1 Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -OS
```

4. Viene visualizzata una richiesta di conferma in cui sono elencate le VM da reimpostare, insieme a un messaggio di avviso che indica che si tratta di un'operazione non recuperabile. Se non si fornisce una risposta e si preme **Invio**, non verrà eseguita alcuna ulteriore azione.

Nota:

Non togliere le VM dalla modalità di manutenzione né accenderle prima del completamento del processo di ripristino.

È possibile eseguire il comando PowerShell `-WhatIf` per stampare l'azione che verrebbe intrapresa e uscire senza eseguirla.

È anche possibile ignorare la richiesta di conferma utilizzando uno dei seguenti metodi:

- Fornire il parametro `-Force` :

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
   -OS -Force
```

- Fornire il parametro `-Conferma:$false` :

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
   -OS -Confirm:$false
```

- Prima di eseguire `Reset-ProvVMDisk`, modificare `$ConfirmPreference` in **None**:

```
1 PS C:\Windows\system32> $ConfirmPreference='None'
2 PS C:\Windows\system32> $ConfirmPreference
3 None
4 PS C:\Windows\system32> Reset-ProvVMDisk -
   ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

5. Eseguire `Get-ProvTask` per ottenere lo stato delle attività restituite dal comando `Reset-ProvVMDisk`.

Modificare l'impostazione di rete per uno schema di provisioning esistente

È possibile modificare le impostazioni di rete per uno schema di provisioning esistente in modo che le nuove VM vengano create sulla nuova sottorete. Utilizzare il parametro `-NetworkMapping` nel comando `Set-ProvScheme` per modificare le impostazioni di rete.

Nota:

Questa funzionalità è supportata su Citrix Virtual Apps and Desktops 2203 LTSR CU3 e versioni successive.

Per modificare le impostazioni di rete per uno schema di provisioning esistente, procedere come segue:

1. Nella finestra di PowerShell, eseguire il comando `asnp citrix*` per caricare i moduli di PowerShell.
2. Esegui `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` per arrivare al percorso di rete che vuoi modificare.

3. Assegna una variabile alla nuova impostazione di rete. Per esempio:

```
1 $NewNetworkMap = @{
2   "0" = "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }
```

4. Esegui `Set-ProvScheme -ProvisioningSchemeName "nome"-NetworkMapping $NewNetworkMap`.

5. Eseguire `(Get-ProvScheme -ProvisioningSchemeName "name").NetworkMaps` per verificare la nuova impostazione di rete per lo schema di provisioning esistente.

Gestire le versioni di un catalogo macchine

Quando un catalogo di macchine MCS viene aggiornato con il comando `Set-ProvScheme`, la configurazione corrente viene salvata come versione. È quindi possibile gestire le varie versioni del catalogo macchine utilizzando i comandi di PowerShell. Puoi:

- Visualizza l'elenco delle versioni di un catalogo di macchine
- Utilizzare qualsiasi versione precedente per aggiornare il catalogo delle macchine
- Elimina manualmente una versione se non è utilizzata da una VM di quel catalogo macchine
- Modifica il numero massimo di versioni da conservare nel catalogo della macchina (il valore predefinito è 99)

Una versione include le seguenti informazioni di un catalogo macchine:

- Conteggio VM CPU
- Memoria VMM
- Proprietà personalizzate
- Servizio Offerta
- Profilo della macchina
- Mappatura della rete
- Gruppo di sicurezza

Eseguire i seguenti comandi (forniti come esempi) per gestire le varie versioni di un catalogo macchine.

- Per visualizzare i dettagli di configurazione delle varie versioni di un catalogo macchine:

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- Per visualizzare i dettagli di configurazione di una particolare versione di un catalogo macchine:

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
   Version 2
```

- Per visualizzare il numero totale di versioni associate a un catalogo macchine:

```
1 (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).  
Count
```

- Per utilizzare una qualsiasi versione precedente per aggiornare il catalogo macchine:

```
1 Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- Per eliminare manualmente una versione se non è utilizzata da una VM di quel catalogo macchine:

```
1 Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -  
Version 3
```

- Per impostare il numero massimo di versioni da conservare nel catalogo della macchina (il valore predefinito è 99). Questa impostazione viene applicata a tutti i cataloghi. Ad esempio, in questo caso, verranno conservate al massimo 15 versioni per tutti i cataloghi forniti da MCS.

```
1 Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions"  
-Value 15
```

Se il numero di versioni raggiunge il numero massimo di versioni, non sarà possibile creare una nuova versione se una qualsiasi delle VM nel catalogo delle macchine utilizza versioni precedenti. In tal caso, procedere in uno dei seguenti modi:

- Aumentare il limite del numero massimo di versioni da conservare nel catalogo macchine.
- Aggiornare alcune VM che si trovano su versioni precedenti in modo che tali versioni precedenti non siano più referenziate da alcuna VM e possano essere eliminate.

Convertire un catalogo macchine non basato su profili macchina in un catalogo macchine basato su profili macchina

È possibile utilizzare una VM, una specifica modello (nel caso di Azure) o un modello di avvio (nel caso di AWS) come input del profilo macchina per convertire un catalogo macchine basato su un profilo non macchina in un catalogo macchine basato su un profilo macchina. Le nuove VM aggiunte al catalogo prendono i valori delle proprietà dal profilo della macchina, a meno che non vengano sovrascritti da una proprietà personalizzata esplicita.

Nota:

Un catalogo macchine esistente basato sul profilo macchina non può essere modificato in un catalogo macchine non basato sul profilo macchina.

Per fare questo:

1. Creare un catalogo macchine persistente o non persistente con VM e senza un profilo macchina.

2. Aprire la finestra **PowerShell**.
3. Eseguire il comando `Set-ProvScheme` per applicare i valori delle proprietà dal profilo macchina alle nuove VM aggiunte al catalogo macchine. Per esempio:

- Nel caso di Azure:

```
1 Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName
   xxxx -MachineProfile XDHyp:\HostingUnits\  

   HostingUnitName>\machineprofile.folder\  

   ResourceGroupName>\<TemplateSpecName>\<VersionName>
```

- Nel caso di AWS:

```
1 Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName
   xxxx -MachineProfile "XDHyp:\HostingUnits\<hosting-unit  

   >\<launch-template>.launchtemplate\<launch-template-  

   version>.launchtemplateversion"
```

Riparare le informazioni di identità degli account di computer attivi

È possibile reimpostare le informazioni di identità degli account computer attivi che presentano problemi di identità. È possibile scegliere di reimpostare solo la password della macchina e le chiavi di attendibilità oppure di reimpostare tutta la configurazione del disco di identità. Questa implementazione è applicabile sia ai cataloghi di macchine MCS persistenti che a quelli non persistenti.

Nota:

Attualmente, la funzionalità è supportata solo per gli ambienti di virtualizzazione Azure e VMware.

Condizioni

Per reimpostare correttamente il disco di identità, assicurarsi di quanto segue:

- Spegner e impostare la VM in modalità manutenzione
- Non includere il parametro `-OS` nel comando PowerShell

Reimposta disco identità

Per reimpostare il disco di identità:

1. Aprire la finestra **PowerShell**.
2. Eseguire `asnp citrix*` per caricare i moduli PowerShell specifici di Citrix.

3. Reimposta le informazioni di identità.

- Per reimpostare solo la password della macchina e le chiavi di attendibilità, eseguire il seguente comando:

```
1 Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
$password -Target IdentityInfo
```

La descrizione dei parametri utilizzati nel comando è la seguente:

- IdentityAccountName: Nome dell'account di identità che deve essere riparato.
 - PrivilegedUserName: account utente che dispone dell'autorizzazione di scrittura sul provider di identità (AD o AzureAD).
 - PrivilegedUserPassword: Password per PrivilegedUserName.
 - Obiettivo: Obiettivo dell'azione di riparazione. Può essere IdentityInfo per riparare la password/chiave di attendibilità dell'account e UserCertificate per riparare gli attributi del certificato utente delle identità delle macchine unite ad AzureAD ibrido.
- Per reimpostare tutta la configurazione del disco di identità, eseguire i seguenti comandi nell'ordine seguente:

```
1 Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
$password -Target IdentityInfo
```

```
1 Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <
name> -Identity
```

- Per ricreare completamente il disco di identità:

```
1 Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <
name> -Identity -Recreate
```

- ### 4. Digitare **y** per confermare l'azione. È anche possibile saltare la richiesta di conferma utilizzando il parametro `-Force`. Per esempio:

```
1 Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
Identity -Force
```

- ### 5. Eseguire `Get-ProvVM -ProvisioningSchemeName <name> -VMName <name>` per verificare l'impostazione aggiornata del disco di identità. Gli attributi del disco di identità (ad esempio, `IdentityDiskId`) devono essere aggiornati. `StorageID` e `IdentityDiskIndex` non devono cambiare.

Modificare la configurazione della cache su un catalogo di macchine esistente

Dopo aver creato un catalogo non persistente con MCSIO abilitato, è possibile utilizzare il comando `Set-ProvScheme` per modificare i seguenti parametri:

- `WriteBackCacheMemorySize`
- `WriteBackCacheDiskSize`

Questa funzionalità è attualmente applicabile a:

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

Requisiti

I requisiti per modificare la configurazione della cache sono:

- Aggiornare all'ultima versione di VDA (2308 o successiva).
- Abilitare il parametro `UseWriteBackCache` per il catalogo macchine esistente. Utilizzare `New-ProvScheme` per creare un catalogo macchine con `UseWriteBackCache` abilitato.

Per esempio:

```

1 New-ProvScheme -ProvisioningSchemeName $CatalogName -
   HostingUnitUid $HostingUnitUid `
2 -IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
3 -MasterImageVM $MasterImage `
4 -ServiceOffering $ServiceOffering `
5 -NetworkMap $NetworkMap `
6 -SecurityGroup $SecurityGroup `
7 -UseWriteBackCache -WriteBackCacheDiskSize 8

```

Cambia la configurazione della cache

Eseguire il comando `Set-ProvScheme`. Per esempio:

```

1 Set-ProvScheme -ProvisioningSchemeName $provScheme.
   ProvisioningSchemeName -WriteBackCacheDisk32 -
   WriteBackCacheMemorySize 128

```

Nota:

- Il valore di `WriteBackCacheDiskSize` deve essere maggiore di zero perché è richiesto almeno 1 GB di spazio di archiviazione su disco della cache.
- Il valore di `WriteBackCacheMemorySize` deve essere inferiore alla dimensione della memoria del catalogo macchina.

- Queste modifiche riguardano solo le nuove VM aggiunte al catalogo dopo che la modifica è stata apportata. Le VM esistenti non sono interessate da queste modifiche.

Supporto per l'aggiornamento VDA tramite accesso alla condivisione file locale

Specificare il percorso del programma di installazione VDA tramite cmdlet di PowerShell, riducendo così lo sforzo necessario per specificare regole di rete per consentire a ogni VDA di andare a recuperare il nuovo programma di installazione VDA dalla CDN di Citrix Managed Azure.

Cmdlet di PowerShell

Due nuovi parametri facoltativi aggiunti ai cmdlet **New-VusCatalogSchedule** e **New-VusMachineUpgrade** che consentono di utilizzare programmi di installazione da una condivisione file locale

- **VdaWorkstationPackageUri** - per specificare il percorso UNC per il programma di installazione VDA del sistema operativo della workstation
- **VdaServerPackageUri** - per specificare il percorso UNC per il programma di installazione VDA del sistema operativo del server

Prerequisiti

- VUS Agent Installer fornito con VDA 2311
- VDA Upgrade Agent alla versione 7.40.0.35 o successiva (utilizzando il programma di installazione VDA versione 2311 o successiva)
- Virtual Apps and Desktops Remote PowerShell SDK versione 7.40 o successiva (rilasciata il 10 gennaio 2024 o successiva)

Come impostare le autorizzazioni di condivisione file

Le condivisioni di rete contenenti i pacchetti di installazione VDA devono disporre di accesso in lettura per il servizio VDA Upgrade Agent, che viene eseguito come sistema locale (principale NT AUTHORITY\SYSTEM).

- **Autorizzazione di condivisione file unita al dominio**

Quando la macchina VDA è aggiunta a un dominio, l'account **Local System** (VUA viene eseguito come Local System) utilizza le credenziali del computer quando accede alle condivisioni di rete.

Il permesso con privilegi minimi può essere impostato concedendo l'accesso **Lettura** ai computer del dominio.

1. Seleziona le persone sulla tua rete con cui desideri condividere il file.
2. Fare clic su **Impostazioni di condivisione avanzate** e attivare **Condivisione file e stampanti**.

- **Autorizzazione di condivisione file non associata al dominio**

Quando la macchina VDA non è unita a un dominio, l'account **Sistema locale** (VUA viene eseguito come Sistema locale), utilizza **ACCESSO ANONIMO** quando accede alle condivisioni di rete.

1. Seleziona una cartella condivisa.
2. Disattivare la protezione tramite password.
 - a) Vai alla cartella **Proprietà**.
 - b) Seleziona **Centro connessioni di rete e condivisione**.
 - c) Disattiva **Condivisione protetta da password**.
3. Fare clic su **Condivisione avanzata** per concedere un'autorizzazione di condivisione.
 - a) Seleziona **Permessi**.
 - b) Concedi un permesso di condivisione **Lettura** a **ACCESSO ANONIMO**.
4. Selezionare la scheda Sicurezza ** per concedere i permessi alla cartella
 - a) Fare clic su **Modifica** per aggiungere autorizzazioni alla cartella condivisa
 - b) Seleziona la cartella condivisa a cui concedere i permessi di accesso **ACCESSO ANONIMO**.
5. Fare clic su **Avanzate** per attivare **Condivisione file e stampanti**.
6. Aggiungere il nome della cartella condivisa a **Criterio di sicurezza dell'accesso alla rete**.

Nota:

Riavvia il computer affinché la modifica abbia effetto immediato.

Aggiornamenti VDA da una condivisione file locale

1. Scaricare il programma di installazione VDA e inserirlo nel file condiviso.

Nota:

Con il servizio di aggiornamento virtuale puoi scegliere tra il percorso Current Release o il percorso LTSR.

Ad esempio: Se il catalogo della macchina è impostato sulla versione corrente, ovvero 2311, e la versione VDA è 2305, è necessario aggiornare la versione VDA alla versione 2311.

- a) Vai alla pagina **Download** sul [nostro sito web](#).
- b) Selezionare **Citrix Virtual Apps and Desktops** come prodotto.

- c) Seleziona **Citrix Virtual Apps and Desktops 7 2311, tutte le edizioni.**
 - d) Selezionare il programma di installazione VDA dai componenti **presenti nell'ISO del prodotto ma anche confezionati separatamente** espandibili.
2. Selezionare il programma di installazione VDA appropriato in base al tipo di catalogo.
- Scarica il programma di installazione VDA multi-sessione del sistema operativo **** se il tipo di catalogo è **multi-sessione**
 - Scarica il programma di installazione VDA del sistema operativo a sessione singola **** se il tipo di catalogo è **sessione singola**
 - Scarica il programma di installazione VDA dei servizi core del sistema operativo a sessione singola **** se il tipo di catalogo è **Accesso PC remoto**

Nota:

La versione del programma di installazione della condivisione file deve corrispondere esattamente a ** la versione dell'ultima versione del programma di installazione pubblicata da VUS sul cloud.

Risoluzione dei problemi

- Per le macchine con stato “Power State Unknown”, vedere [CTX131267](#) per istruzioni.
- Per risolvere il problema delle VM che mostrano continuamente uno stato di alimentazione sconosciuto, vedere [Come risolvere il problema delle VM che mostrano continuamente uno stato di alimentazione sconosciuto.](#)

Dove andare dopo

Per informazioni sulla gestione di cataloghi specifici di servizi cloud, vedere:

- [Gestire un catalogo AWS](#)
- [Gestire un catalogo XenServer](#)
- [Gestisci un catalogo di Google Cloud Platform](#)
- [Gestire un catalogo Microsoft Azure](#)
- [Gestire un catalogo di Microsoft System Center Virtual Machine Manager](#)
- [Gestire un catalogo VMware](#)

Gestire i gruppi di consegna

January 24, 2025

Nota:

È possibile gestire la distribuzione di Citrix Virtual Apps and Desktops utilizzando due console di gestione: Web Studio (basata sul Web) e Citrix Studio (basata 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.

Introduzione

In questo articolo vengono descritte le procedure per la gestione dei gruppi di distribuzione dalla console di gestione. Oltre a modificare le impostazioni specificate durante la creazione del gruppo, è possibile configurare altre impostazioni che non sono disponibili quando si crea un gruppo di recapito.

Le categorie di procedure includono: generale, utenti, macchine e sessioni. Alcune attività rientrano in più categorie. Ad esempio, "Impedisci agli utenti di connettersi ai computer" è descritto nella categoria Computer, ma riguarda anche gli utenti. Se non riesci a trovare un'attività in una categoria, controlla una categoria correlata.

Altri articoli contengono informazioni correlate:

- [Le applicazioni](#) contengono informazioni sulla gestione delle applicazioni nei gruppi di distribuzione.
- Per gestire i gruppi di consegna sono necessarie le autorizzazioni predefinite del ruolo Amministratore del gruppo di consegna. Per i dettagli, vedere [Amministrazione delegata](#).

Generale

- Visualizza i dettagli del gruppo
- Cambia il tipo di consegna
- Cambia gli indirizzi StoreFront
- Cambia il livello funzionale
- Gestisci i gruppi di distribuzione dell'accesso remoto al PC
- Organizzare i gruppi di consegna utilizzando le cartelle
- Gestisci la protezione delle app

Visualizza i dettagli del gruppo

1. Utilizzare la funzione di ricerca per individuare uno specifico gruppo di consegna. Per istruzioni, fare riferimento a [Cerca istanze](#).
2. Dai risultati della ricerca, seleziona un gruppo in base alle tue esigenze.

3. Per le descrizioni delle colonne del gruppo, fare riferimento alla tabella seguente.
4. Per ulteriori informazioni su questo gruppo, fare clic su una scheda nel riquadro dei dettagli in basso.

Colonna	Descrizione
Gruppo di consegna	Il nome del gruppo e il tipo di sessione. I tipi di sessione includono il sistema operativo a sessione singola e il sistema operativo multisessione.
Consegna	Il tipo di risorse fornite da questo gruppo. I valori possibili includono Applicazioni, Desktop e Applicazioni e Desktop. “Assegnazione macchina statica” viene visualizzato se il gruppo di consegna è composto da macchine dedicate.
Sessione in uso	Numero di macchine configurate e numero di macchine in stato Disconnesso.
Conteggio assegnato	Numero di macchine nel catalogo assegnate a un gruppo di consegna.
Cartella	Posizione del gruppo all'interno dell'albero Gruppi di consegna . Visualizza il nome della cartella in cui si trova il gruppo (inclusa la barra rovesciata finale) oppure – se il gruppo si trova al livello radice.

Modificare il tipo di consegna di un gruppo di consegna

Il tipo di consegna indica cosa il gruppo può consegnare: applicazioni, desktop o entrambi.

Prima di modificare il tipo di applicazione **solo per desktop** o **il tipo di applicazione** nel tipo di applicazione **solo per desktop**, elimina tutte le applicazioni dal gruppo.

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Tipo di consegna**, seleziona il tipo di consegna desiderato.
4. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Cambia gli indirizzi StoreFront

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.

2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **StoreFront**, seleziona o aggiungi gli URL StoreFront. Questi URL vengono utilizzati dall'app Citrix Workspace, installata su ogni macchina del gruppo di distribuzione.
4. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

È anche possibile specificare gli indirizzi del server StoreFront selezionando **StoreFront** nel riquadro di sinistra.

Cambia il livello funzionale

Modificare il livello funzionale per il gruppo di distribuzione dopo aver aggiornato i VDA sulle relative macchine e i cataloghi macchine contenenti le macchine utilizzate nel gruppo di distribuzione.

Prima di iniziare:

- Se si utilizza Citrix Provisioning (in precedenza Provisioning Services), aggiornare la versione VDA nella console Citrix Provisioning.
- Avviare le macchine contenenti il VDA aggiornato in modo che possano registrarsi con un Delivery Controller. Questo processo indica alla console cosa deve essere aggiornato nel gruppo di distribuzione.
- Se è necessario continuare a utilizzare le versioni VDA precedenti, le funzionalità più recenti del prodotto non saranno disponibili. Per ulteriori informazioni, consultare la documentazione relativa all'aggiornamento.

Per modificare il livello funzionale di un gruppo di distribuzione:

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Cambia livello funzionale** nella barra delle azioni. L'azione **Modifica livello funzionale** viene visualizzata solo se vengono rilevati VDA aggiornati.
3. Fai clic su **Modifica**.

Il display indica quali macchine, se presenti, non possono essere modificate al livello funzionale e il motivo. È quindi possibile annullare l'azione di modifica, risolvere i problemi della macchina e quindi eseguire nuovamente l'azione di modifica.

Una volta completata la modifica, è possibile ripristinare lo stato precedente delle macchine. Selezionare il gruppo di consegna, quindi selezionare **Annulla modifica livello funzionale** nella barra delle azioni.

Gestisci i gruppi di distribuzione dell'accesso remoto al PC

Se una macchina presente in un catalogo di macchine di Remote PC Access non è assegnata, la macchina viene temporaneamente assegnata a un gruppo di distribuzione associato a tale catalogo. Questa assegnazione temporanea consente di assegnare la macchina a un utente in un secondo momento.

L'associazione tra il gruppo di consegna e il catalogo della macchina ha un valore di priorità. La priorità determina il gruppo di consegna assegnato alla macchina quando questa si registra nel sistema o quando un utente necessita dell'assegnazione di una macchina. Più basso è il valore, maggiore è la priorità. Se un catalogo di macchine con accesso remoto al PC ha più assegnazioni di gruppi di distribuzione, il software seleziona la corrispondenza con la priorità più alta. Utilizzare PowerShell SDK per impostare questo valore di priorità.

Al momento della creazione, i cataloghi delle macchine di Remote PC Access sono associati a un gruppo di distribuzione. Gli account macchina o le unità organizzative aggiunti al catalogo in un secondo momento possono essere aggiunti al gruppo di distribuzione. Questa associazione può essere attivata o disattivata.

Per aggiungere o rimuovere un'associazione al catalogo macchine di Remote PC Access con un gruppo di distribuzione:

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.
2. Selezionare un gruppo di accesso PC remoto.
3. Nella sezione **Dettagli**, fare clic sulla scheda **Cataloghi macchine** e quindi selezionare un catalogo di Accesso PC remoto.
4. Per aggiungere o ripristinare un'associazione, fare clic su **Aggiungi desktop**. Per rimuovere un'associazione, fare clic su **Rimuovi associazione**.

Organizzare i gruppi di consegna utilizzando le cartelle

È possibile creare cartelle per organizzare i gruppi di consegna e facilitarne l'accesso.

Ruoli richiesti Per impostazione predefinita, per creare e gestire le cartelle del gruppo di recapito è necessario disporre del seguente ruolo integrato: Amministratore cloud, Amministratore completo o Amministratore del gruppo di recapito. Se necessario, è possibile personalizzare i ruoli per la creazione e la gestione delle cartelle dei gruppi di recapito. Per ulteriori informazioni, vedere Autorizzazioni richieste.

Crea una cartella del gruppo di consegna Prima di iniziare, pianifica come organizzare i tuoi gruppi di consegna. Considera quanto segue:

- È possibile nidificare le cartelle fino a cinque livelli (esclusa la cartella radice predefinita).
- Una cartella può contenere gruppi di recapito e sottocartelle.
- Tutti i nodi (ad esempio i nodi **Cataloghi macchine, Applicazioni e Gruppi di distribuzione**) condividono un albero di cartelle nel back-end. Per evitare conflitti di nomi con altri nodi durante la ridenominazione o lo spostamento di cartelle, si consiglia di assegnare nomi diversi alle cartelle di primo livello in nodi diversi.

Per creare una cartella del gruppo di consegna, segui questi passaggi:

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, seleziona una cartella e poi seleziona **Crea cartella** nella barra **Azione**.
3. Inserisci un nome per la nuova cartella, quindi fai clic su **Fatto**.

Mancia:

Se si crea una cartella in una posizione non desiderata, è possibile trascinarla nella posizione corretta.

Sposta un gruppo di consegna

È possibile spostare un gruppo di recapito tra le cartelle. I passaggi dettagliati sono i seguenti:

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Visualizza i gruppi per cartella. Puoi anche attivare **Visualizza tutto** sopra la gerarchia delle cartelle per visualizzare tutti i gruppi contemporaneamente.
3. Fare clic con il pulsante destro del mouse su un gruppo e quindi selezionare **Sposta gruppo di consegna**.
4. Seleziona la cartella in cui vuoi spostare il gruppo, quindi fai clic su **Fatto**.

Mancia:

È possibile trascinare un gruppo in una cartella.

Gestisci le cartelle del gruppo di consegna

È possibile eliminare, rinominare e spostare le cartelle del gruppo di consegna.

Tieni presente che puoi eliminare una cartella solo se essa e le sue sottocartelle non contengono gruppi di recapito.

Per gestire una cartella, segui questi passaggi:

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Nella gerarchia delle cartelle, seleziona una cartella, quindi seleziona un'azione nella barra **Azione** in base alle tue esigenze:
 - Per rinominare la cartella, seleziona **Rinomina cartella**.
 - Per eliminare la cartella, seleziona **Elimina cartella**.
 - Per spostare la cartella, seleziona **Sposta cartella**.
3. Seguire le istruzioni sullo schermo per completare i passaggi rimanenti.

Autorizzazioni richieste Nella tabella seguente sono elencate le autorizzazioni necessarie per eseguire azioni sulle cartelle del gruppo di recapito.

Azione	Autorizzazioni richieste
Crea cartelle di gruppo di consegna	Crea cartella gruppo di consegna
Elimina le cartelle del gruppo di consegna	Rimuovi cartella gruppo di consegna
Sposta le cartelle del gruppo di consegna	Sposta cartella gruppo di consegna
Rinomina le cartelle del gruppo di consegna	Modifica cartella gruppo di consegna
Sposta i gruppi di consegna nelle cartelle	Modifica cartella gruppo di consegna e modifica proprietà gruppo di consegna

Gestisci la protezione delle app

Le seguenti informazioni sono integrative di [Protezione app](#). Tieni presente i seguenti dettagli:

- Devi disporre di un diritto valido di Protezione app. Per acquistare la funzionalità App Protection, contatta il tuo rappresentante commerciale Citrix.
- App Protection richiede attendibilità XML. Per abilitare l'attendibilità XML, vai su **Impostazioni > Abilita l'attendibilità XML**.
- Per quanto riguarda l'anti-cattura dello schermo:
 - Su Windows e macOS, solo la finestra del contenuto protetto è vuota. La protezione delle app è attiva quando una finestra protetta non è ridotta a icona.
 - Su Linux, l'intera cattura è vuota. La protezione delle app è attiva indipendentemente dal fatto che una finestra protetta sia ridotta a icona o meno.

Per scegliere un metodo di protezione delle app per un gruppo di distribuzione, attenersi alla seguente procedura:

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi seleziona **Modifica** nella barra delle azioni.
3. Nella pagina **Protezione app** puoi abilitare **Anti-keylogging** e **Anti-cattura schermo**.

Utenti

- Modificare le impostazioni utente
- Aggiungere o rimuovere utenti

Modificare le impostazioni utente in un gruppo di consegna

Il nome di questa pagina appare come **Impostazioni utente** o **Impostazioni di base**.

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Impostazioni utente** (o **Impostazioni di base**), modifica una qualsiasi delle impostazioni nella tabella seguente.
4. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Collocamento	Descrizione
Descrizione	Il testo utilizzato da Citrix Workspace (o StoreFront) e visualizzato dagli utenti.
Abilita gruppo di consegna	Se il gruppo di recapito è abilitato.
Fuso orario	Fuso orario in cui devono risiedere le macchine di questo gruppo di consegna. L'opzione elenca i fusi orari supportati dal sito. Nota: La modifica del fuso orario su un gruppo di distribuzione potrebbe comportare il riavvio delle macchine in quel gruppo di distribuzione. Per evitare ciò, assicurarsi di modificare le impostazioni del fuso orario al di fuori dell'orario di produzione.

Collocamento	Descrizione
Abilita ICA sicuro	Protegge le comunicazioni da e verso le macchine nel gruppo di consegna utilizzando SecureICA, che crittografa il protocollo ICA. Il livello predefinito è 128 bit. Il livello può essere modificato tramite l'SDK. Citrix consiglia di utilizzare più metodi di crittografia, come la crittografia TLS, quando si attraversano reti pubbliche. Inoltre, SecureICA non verifica l'integrità dei dati.

Aggiungere o rimuovere utenti in un gruppo di consegna

Per informazioni dettagliate sugli utenti, vedere [Utenti](#).

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Utenti** :
 - Per aggiungere utenti, fare clic su **Aggiungi**, quindi specificare gli utenti che si desidera aggiungere.
 - Per rimuovere utenti, seleziona uno o più utenti e poi clicca su **Rimuovi**.
 - Selezionare o deselezionare la casella di controllo per consentire l'accesso agli utenti non autenticati.
4. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Importare o esportare elenchi di utenti Per i gruppi di distribuzione contenenti macchine fisiche con sistema operativo a sessione singola, è possibile importare le informazioni utente da un file .csv dopo aver creato il gruppo di distribuzione. È anche possibile esportare le informazioni utente in un file .csv. Il file .csv può contenere dati di una versione precedente del prodotto.

La prima riga del file CSV deve contenere due intestazioni di colonna, separate da una virgola. Assicurati che la prima intestazione sia **Account macchina** e che la seconda intestazione sia **Nomi utente**. (È possibile includere intestazioni aggiuntive, ma non sono supportate.) Le righe successive nel file contengono dati separati da virgole. Le voci dell'account macchina “ possono essere SID del computer, FQDN o coppie di nomi di dominio e computer.

Per importare o esportare le informazioni utente:

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Allocazione macchina** , seleziona **Importa elenco** o **Esporta elenco** , quindi vai al percorso del file.
4. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Macchine

- Cambiare le assegnazioni delle macchine agli utenti
- Modificare il numero massimo di macchine per utente
- Aggiornare una macchina
- Aggiungere, modificare o rimuovere una restrizione di tag per un desktop
- Rimuovi una macchina
- Limitare l'accesso alle macchine
- Impedire agli utenti di connettersi a una macchina (modalità di manutenzione)
- Spegnerne e riavviare le macchine
- Crea e gestisci pianificazioni di riavvio per le macchine
- Abilita la pianificazione di riavvio una tantum
- Macchine gestite dal carico
- Macchine gestite dall'energia

Modificare le assegnazioni delle macchine agli utenti in un gruppo di consegna

È possibile modificare le assegnazioni delle macchine con sistema operativo a sessione singola fornite con MCS. Non è possibile modificare le assegnazioni per macchine con sistema operativo multi-sessione o macchine fornite con Citrix Provisioning.

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Desktop** o **Regole di assegnazione desktop** (il titolo della pagina dipende dal tipo di catalogo macchine utilizzato dal gruppo di distribuzione), specificare i nuovi utenti.
4. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Modificare il numero massimo di macchine per utente in un gruppo di consegna

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.

3. Nella pagina **Regole di assegnazione desktop** , imposta il valore massimo di desktop per utente.
4. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Aggiorna una macchina in un gruppo di consegna

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Visualizza macchine** nella barra delle azioni.
3. Seleziona una macchina e poi clicca su **Aggiorna macchine** nella barra delle azioni.

Per scegliere un'immagine diversa, seleziona **Immagine** e poi seleziona un'istantanea.

Per applicare le modifiche e notificare gli utenti della macchina, selezionare **Notifica di distribuzione agli utenti finali**. Quindi specificare:

- Quando aggiornare l'immagine master: ora o al prossimo riavvio
- Tempo di distribuzione del riavvio (tempo totale per iniziare ad aggiornare tutte le macchine nel gruppo)
- Se gli utenti vengono avvisati del riavvio
- Il messaggio che gli utenti ricevono

Aggiungere, modificare o rimuovere una restrizione di tag per un desktop

L'aggiunta, la modifica e la rimozione delle restrizioni dei tag possono avere effetti imprevedibili sui desktop presi in considerazione per l'avvio. Rivedere le considerazioni e le cautele nei tag .

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Desktop** , seleziona il desktop e fai clic su **Modifica**.
4. Per aggiungere una restrizione tramite tag, seleziona **Limita gli avvii alle macchine con il tag** , quindi seleziona il tag.
5. Per modificare o rimuovere una restrizione di tag:
 - Seleziona un tag diverso.
 - Rimuovere la restrizione del tag deselegionando **Limita gli avvii alle macchine con questo tag**.
6. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Rimuovere una macchina da un gruppo di consegna

La rimozione di una macchina la elimina dal gruppo di distribuzione. Non lo elimina dal catalogo macchine utilizzato dal gruppo di consegna. Pertanto, la macchina è disponibile per l'assegnazione a un altro gruppo di consegna.

Prima di poter rimuovere le macchine, è necessario spegnerle. Per impedire temporaneamente agli utenti di connettersi a una macchina mentre la stai rimuovendo, metti la macchina in modalità di manutenzione prima di spegnerla.

Le macchine potrebbero contenere dati personali, quindi prestare attenzione prima di assegnarle a un altro utente. Si potrebbe prendere in considerazione la possibilità di riprogettare la macchina.

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Visualizza macchine** nella barra delle azioni.
3. Assicurarsi che la macchina sia spenta.
4. Selezionare la macchina e quindi fare clic su **Rimuovi dal gruppo di distribuzione** nella barra delle azioni.

È anche possibile rimuovere una macchina da un gruppo di distribuzione tramite la connessione utilizzata dalla macchina.

Limitare l'accesso alle macchine in un gruppo di consegna

Tutte le modifiche apportate per limitare l'accesso alle macchine in un gruppo di distribuzione sostituiscono le impostazioni precedenti, indipendentemente dal metodo utilizzato. Puoi:

- **Limita l'accesso per gli amministratori utilizzando ambiti di amministrazione delegati:** Crea e assegna un ambito che consenta agli amministratori di accedere a tutte le applicazioni e un altro ambito che fornisca l'accesso solo a determinate applicazioni. Per i dettagli, vedere [Amministrazione delegata](#).
- **Limita l'accesso degli utenti tramite espressioni di policy SmartAccess:** Utilizza espressioni di policy per filtrare le connessioni utente effettuate tramite Citrix Gateway.
 1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
 2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
 3. Nella pagina **Criteri di accesso**, seleziona **Connessioni tramite NetScaler Gateway**.
 4. Per scegliere un sottoinsieme di tali connessioni, selezionare **Connessioni che soddisfano uno dei seguenti filtri**. Quindi definire il sito Citrix Gateway e aggiungere, modificare o rimuovere le espressioni di policy SmartAccess per gli scenari di accesso utente consentiti. Per maggiori dettagli, consultare la documentazione di Citrix Gateway.
 5. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

- **Limita l'accesso degli utenti tramite filtri di esclusione:** Utilizza filtri di esclusione sui criteri di accesso impostati nell'SDK. I criteri di accesso vengono applicati ai gruppi di distribuzione per perfezionare le connessioni. Ad esempio, è possibile limitare l'accesso alla macchina a un sottoinsieme di utenti e specificare i dispositivi utente consentiti. I filtri di esclusione perfezionano ulteriormente i criteri di accesso. Ad esempio, per motivi di sicurezza, è possibile negare l'accesso a un sottoinsieme di utenti o dispositivi. Per impostazione predefinita, i filtri di esclusione sono disabilitati.

Ad esempio, un laboratorio didattico su una sottorete di rete aziendale che impedisce l'accesso da quel laboratorio a un particolare gruppo di consegna. Indipendentemente da chi utilizza le macchine nel laboratorio, utilizzare il comando: `Set-BrokerAccessPolicy -Name VPPesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

Utilizzare il carattere jolly asterisco (*) per trovare la corrispondenza con tutti i tag che iniziano con la stessa espressione di policy. Ad esempio, se si aggiunge il tag `VPDesktops_Direct` a una macchina e `VPDesktops_Test` a un'altra, impostando il tag nello script `Set-BrokerAccessPolicy` su `VPDesktops_*` si applica il filtro a entrambe le macchine.

Se sei connesso tramite un browser web o con la funzionalità di esperienza utente dell'app Citrix Workspace abilitata nello store, non puoi utilizzare un filtro di esclusione del nome client.

Impedire agli utenti di connettersi a una macchina (modalità di manutenzione) in un gruppo di distribuzione

Quando è necessario interrompere temporaneamente le nuove connessioni alle macchine, è possibile attivare la modalità di manutenzione per una o tutte le macchine in un gruppo di distribuzione. È possibile farlo prima di applicare patch o di utilizzare strumenti di gestione.

- Quando un computer con sistema operativo multisessione è in modalità di manutenzione, gli utenti possono connettersi alle sessioni esistenti, ma non possono avviarne di nuove.
- Quando un computer con sistema operativo a sessione singola (o un PC che utilizza Remote PC Access) è in modalità di manutenzione, gli utenti non possono connettersi o riconnettersi. Le connessioni correnti rimangono attive finché non vengono disconnesse o disconnesse.

Per attivare o disattivare la modalità di manutenzione:

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.
2. Seleziona un gruppo.
3. Per attivare la modalità di manutenzione per tutte le macchine nel gruppo di distribuzione, fare clic su **Attiva modalità di manutenzione** nella barra delle azioni.

Per attivare la modalità di manutenzione per una macchina, fare clic su **Visualizza macchine**

nella barra delle azioni. Seleziona una macchina, quindi fai clic su **Attiva modalità di manutenzione** nella barra delle azioni.

4. Per disattivare la modalità di manutenzione per una o tutte le macchine in un gruppo di distribuzione, seguire le istruzioni precedenti, ma fare clic su **Disattiva modalità di manutenzione** nella barra delle azioni.

Le impostazioni di Connessione Desktop remoto (RDC) di Windows influiscono anche sulla modalità di manutenzione di un computer con sistema operativo multisessione. La modalità di manutenzione è attiva quando si verifica una delle seguenti situazioni:

- La modalità di manutenzione è attivata, come descritto in precedenza.
- RDC è impostato su **Non consentire connessioni a questo computer**.
- RDC non è impostato su **Non consentire connessioni a questo computer**. L'impostazione **Modalità di accesso utente della configurazione host remoto** è **Consenti riconessioni, ma impedisce nuovi accessi** o **Consenti riconessioni, ma impedisce nuovi accessi finché il server non viene riavviato**.

Puoi anche attivare o disattivare la modalità di manutenzione per:

- Una connessione che influisce sulle macchine che utilizzano quella connessione.
- Un catalogo di macchine, che interessa le macchine presenti in quel catalogo.

Arrestare e riavviare le macchine in un gruppo di consegna

Questa procedura non è supportata per i computer con accesso remoto al PC.

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Visualizza macchine** nella barra delle azioni.
3. Selezionare la macchina e quindi fare clic su una delle seguenti voci nella barra delle azioni:
 - **Spegnimento forzato:** Spegne forzatamente la macchina e aggiorna l'elenco delle macchine.
 - **Riavvio:** Richiede al sistema operativo di arrestarsi e quindi riavviare la macchina. Se il sistema operativo non riesce a soddisfare le richieste, la macchina rimane nello stato attuale.
 - **Riavvio forzato:** Arresta forzatamente il sistema operativo e quindi riavvia la macchina.
 - **Sospendi:** Mette in pausa la macchina senza spegnerla e aggiorna l'elenco delle macchine.
 - **Spegnimento:** Richiede al sistema operativo di spegnersi.

Per le azioni non forzate, se la macchina non si spegne entro 10 minuti, viene spenta. Se Windows tenta di installare gli aggiornamenti durante l'arresto, c'è il rischio che il computer venga spento prima del completamento degli aggiornamenti.

Citrix consiglia di impedire agli utenti di macchine con sistema operativo a sessione singola di selezionare **Spegni** durante una sessione. Per maggiori dettagli, consultare la documentazione Microsoft sui criteri.

È anche possibile spegnere e riavviare i computer su una connessione .

Crea e gestisci pianificazioni di riavvio per le macchine in un gruppo di distribuzione

Nota:

- Quando si applica una pianificazione di riavvio a un gruppo di distribuzione con Autoscale abilitato, le relative macchine vengono semplicemente spente e lasciate in attesa che Autoscale le accenda.
- Quando le pianificazioni di riavvio vengono applicate a macchine con una sola sessione casuale, tali macchine vengono spente anziché riavviate, per risparmiare sui costi. Ti consigliamo di utilizzare Autoscale per accendere le macchine.
- La modifica del fuso orario in un gruppo di distribuzione potrebbe comportare il riavvio dei computer in quel gruppo di distribuzione. Per evitare ciò, assicurarsi di modificare le impostazioni del fuso orario al di fuori dell'orario di produzione.

Una pianificazione di riavvio specifica quando le macchine in un gruppo di distribuzione vengono riavviate periodicamente. È possibile creare una o più pianificazioni per un gruppo di consegne. Una pianificazione può influenzare:

- Tutte le macchine del gruppo.
- Una o più (ma non tutte) le macchine del gruppo. Le macchine sono identificate da un'etichetta che si applica alla macchina. Questa è chiamata restrizione del tag, perché il tag limita un'azione ai soli elementi che hanno il tag.

Supponiamo, ad esempio, che tutte le tue macchine facciano parte di un gruppo di consegna. Si desidera che ogni macchina venga riavviata una volta alla settimana e che le macchine utilizzate dal team contabile vengano riavviate quotidianamente. Per ottenere questo risultato, è necessario impostare una pianificazione per tutte le macchine e un'altra pianificazione solo per le macchine in contabilità.

Un programma include il giorno e l'ora di inizio del riavvio, nonché la durata.

È possibile abilitare o disabilitare una pianificazione. Disattivare una pianificazione può essere utile durante i test, durante intervalli speciali o quando si preparano pianificazioni prima di averne bisogno.

Non è possibile utilizzare le pianificazioni per l'accensione o l'arresto automatici dalla console di gestione, ma solo per il riavvio.

Sovrapposizione di programma Più pianificazioni possono sovrapporsi. Nell'esempio sopra, entrambe le pianificazioni interessano le macchine contabili. Domenica queste macchine potrebbero essere riavviate due volte. Il codice di pianificazione è progettato per evitare di riavviare la stessa macchina più spesso del previsto, ma non è possibile garantirlo.

- Se gli orari di avvio e di durata coincidono esattamente, è più probabile che le macchine vengano riavviate una sola volta.
- Quanto più gli orari di inizio e durata differiscono, tanto più è probabile che si verifichino più riavvii.
- Anche il numero di macchine interessate da una pianificazione influisce sulla probabilità di una sovrapposizione. Nell'esempio, la pianificazione settimanale che interessa tutte le macchine potrebbe avviare i riavvii più rapidamente della pianificazione giornaliera per le macchine contabili, a seconda della durata specificata per ciascuna.

Per un'analisi approfondita delle pianificazioni di riavvio, vedere [Interni della pianificazione di riavvio](#).

Visualizza i programmi di riavvio

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Selezionare la pagina **Pianificazione riavvio**.

La pagina **Pianificazione riavvio** contiene le seguenti informazioni per ogni pianificazione configurata:

- Nome della pianificazione.
- Restrizione dei tag utilizzata, se presente.
- Con quale frequenza si verifica il riavvio della macchina.
- Se gli utenti della macchina ricevono una notifica.
- Se la pianificazione è abilitata.

Aggiungi (applica) tag Quando si configura una pianificazione di riavvio che utilizza una restrizione di tag, assicurarsi che il tag sia stato aggiunto alle macchine interessate dalla pianificazione. Nell'esempio sopra, a ciascuna delle macchine utilizzate dal team contabile è stato applicato un tag. Per i dettagli, vedere [Tag](#).

Sebbene sia possibile applicare più di un tag a una macchina, una pianificazione di riavvio può specificarne solo uno.

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Selezionare il gruppo contenente le macchine controllate dalla programmazione.
3. Fare clic su **Visualizza macchine** , quindi selezionare le macchine a cui si desidera aggiungere un tag.
4. Fare clic su **Gestisci tag** nella barra delle azioni.
5. Se il tag esiste, seleziona la casella di controllo accanto al nome del tag. Se il tag non esiste, fare clic su **Crea** e quindi specificare il nome per il tag. Dopo aver creato il tag, seleziona la casella di controllo accanto al nome del tag appena creato.
6. Fare clic su **Salva** nella finestra di dialogo **Gestisci tag** .

Crea un programma di riavvio

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Pianificazione riavvio** , fare clic su **Aggiungi**.
4. Nella pagina **Aggiungi pianificazione riavvio** :
 - Per abilitare la pianificazione, seleziona **Sì**. Per disattivare la pianificazione, selezionare **No**.
 - Digitare un nome e una descrizione per la pianificazione.
 - Per **Limita al tag**, applica una restrizione al tag.
 - Per **Includi macchine in modalità manutenzione**, scegli se includere in questa pianificazione le macchine che sono in modalità manutenzione. Per utilizzare invece PowerShell, vedere Riavvii pianificati per macchine in modalità di manutenzione.
 - Per **Frequenza di riavvio**, seleziona la frequenza con cui si verifica il riavvio: giornaliera, settimanale, mensile o una volta. Se selezioni **Settimanale** o **Mensile**, puoi specificare uno o più giorni specifici.
 - Per **Ripeti ogni**, specifica la frequenza con cui desideri che venga eseguita la pianificazione.
 - Per **Data di inizio**, specificare una data di inizio per la prima occorrenza della pianificazione.
 - Per **Inizia il riavvio alle**, specifica, nel formato a 24 ore, l'ora del giorno in cui iniziare il riavvio.
 - Per **Durata del riavvio**:
 - Se non si desidera utilizzare il riavvio naturale, selezionare **Riavvia tutte le macchine contemporaneamente** o **Riavvia tutte le macchine entro un periodo di tempo**.

- Se vuoi usare il riavvio naturale, seleziona **Riavvia tutte le macchine dopo aver svuotato tutte le sessioni**.

All'avvio di una pianificazione di riavvio configurata per utilizzare il riavvio naturale:

- * Tutte le macchine inattive appartenenti al gruppo di consegna vengono riavviate immediatamente
- * Ogni macchina appartenente a un gruppo di distribuzione con una o più sessioni attive viene riavviata quando tutte le sessioni vengono disconnesse.

Nota:

È possibile utilizzare questa opzione sia per le macchine con gestione dell'alimentazione che per quelle senza.

- In **Invia notifica agli utenti**, scegli se visualizzare un messaggio di notifica sui computer interessati prima che venga avviato un riavvio. Per impostazione predefinita, non viene visualizzato alcun messaggio.
- Se si sceglie di visualizzare un messaggio 15 minuti prima dell'inizio del riavvio, è possibile scegliere (in **Frequenza di notifica**) di ripetere il messaggio ogni cinque minuti dopo il messaggio iniziale. Per impostazione predefinita, il messaggio non viene ripetuto.
- Inserisci il titolo e il testo della notifica. Non esiste alcun testo predefinito.

```
1 If you want the message to include a countdown to restart,
   include the variable **%m%***. Unless you chose to
   restart all machines at the same time, the message
   appears on each machine at the appropriate time before
   the restart.
```

5. Fare clic su **Fatto** per applicare le modifiche e chiudere la finestra **Aggiungi pianificazione di riavvio**.
6. Fare clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Riavviare dopo lo scarico Un altro valore di durata del riavvio è disponibile quando si utilizza PowerShell per creare o aggiornare una pianificazione di riavvio della macchina (`New-BrokerRebootSchedulev2` o `Set-BrokerRebootSchedulev2`).

Se si abilita la funzionalità di riavvio dopo lo svuotamento con il parametro `-UseNaturalReboot <Boolean>`, tutte le macchine vengono riavviate dopo aver svuotato tutte le sessioni. Una volta raggiunto il tempo di riavvio, le macchine vengono messe in stato di svuotamento e poi riavviate quando tutte le sessioni vengono chiuse.

Questa funzionalità è supportata per i gruppi di distribuzione contenenti macchine monosessione o multisessione. È possibile utilizzare questa opzione sia per le macchine con gestione dell'alimentazione che per quelle senza.

In un ambiente on-premise, questa funzionalità è supportata solo quando si utilizza PowerShell. La funzionalità non è disponibile in Web Studio.

Modifica, rimuovi, abilita o disabilita una pianificazione di riavvio

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi clicca su **Modifica** nella barra delle azioni.
3. Nella pagina **Riavvia pianificazione**, seleziona la casella di controllo per una pianificazione.
 - Per modificare una pianificazione, fare clic su **Modifica**. Aggiorna la configurazione della pianificazione, seguendo le istruzioni in *Crea una pianificazione di riavvio*.
 - Per abilitare o disabilitare una pianificazione, fare clic su **Modifica**. Seleziona o deseleziona la casella di controllo **Abilita pianificazione riavvio**.
 - Per rimuovere una pianificazione, fare clic su **Rimuovi**. Conferma la rimozione. La rimozione di una pianificazione non influisce sui tag applicati alle macchine nelle macchine interessate.

Riavvii programmati ritardati a causa dell'interruzione del database

Nota:

Questa funzionalità è disponibile solo in PowerShell.

Se si verifica un'interruzione del database del sito prima dell'inizio di un riavvio pianificato per le macchine (VDA) in un gruppo di distribuzione, i riavvii inizieranno al termine dell'interruzione. Ciò può avere effetti indesiderati.

Ad esempio, supponiamo che tu abbia pianificato che il riavvio di un gruppo di consegna avvenga durante le ore di non produzione (a partire dalle 03:00). Un'interruzione del database del sito si verifica un'ora prima dell'inizio del riavvio programmato (02:00). L'interruzione dura sei ore (fino alle 08:00). La pianificazione del riavvio inizia quando viene ripristinata la connessione tra Delivery Controller e il database del sito. I riavvii VDA ora iniziano cinque ore dopo la programmazione originale, con il conseguente riavvio dei VDA durante le ore di produzione.

Per evitare questa situazione, è possibile utilizzare il parametro `MaxOvertimeStartMins` per i cmdlet `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. Il valore specifica il numero massimo di minuti oltre l'orario di inizio pianificato entro cui può iniziare una pianificazione di riavvio.

- Se la connessione al database viene ripristinata entro tale intervallo di tempo (tempo pianificato + `MaxOvertimeStartMins`), il riavvio del VDA inizia.

- Se la connessione al database non viene ripristinata entro tale periodo di tempo, il riavvio del VDA non avrà luogo.
- Se questo parametro viene omesso o ha valore zero, il riavvio pianificato inizia quando viene ripristinata la connessione al database, indipendentemente dalla durata dell'interruzione.

Per ulteriori informazioni, vedere la guida del cmdlet. Questa funzionalità è disponibile solo in PowerShell. Non è possibile impostare questo valore quando si configura una pianificazione di riavvio in Web Studio.

Riavvii programmati per macchine in modalità manutenzione

Nota:

Questa funzionalità è disponibile solo in PowerShell. L'opzione `IgnoreMaintenanceMode` è supportata con Citrix Virtual Apps and Desktops 7 2006 e versioni successive.

Per indicare se una pianificazione di riavvio influisce sulle macchine in modalità di manutenzione, utilizzare l'opzione `IgnoreMaintenanceMode` con i cmdlet `BrokerRebootScheduleV2`.

Ad esempio, il cmdlet seguente crea una pianificazione che riavvia i computer che si trovano in modalità di manutenzione (oltre a quelli che non lo sono).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

Il seguente cmdlet modifica una pianificazione di riavvio esistente.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

Per ulteriori informazioni, vedere la guida del cmdlet. Questa funzionalità è disponibile solo in PowerShell.

Abilita la pianificazione di riavvio una tantum

Se si desidera abilitare la pianificazione di riavvio una tantum tramite PowerShell, utilizzare i seguenti comandi di PowerShell `BrokerCatalogRebootSchedule` per creare, modificare ed eliminare una pianificazione di riavvio:

- Ottieni-BrokerCatalogRebootSchedule
- Nuovo-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Rimuovi-BrokerCatalogRebootSchedule
- Rinomina-BrokerCatalogRebootSchedule

Limitazioni:

- Viene creata una pianificazione di riavvio del catalogo associata a un catalogo senza fuso orario configurato, ma non si avvia.
- Quando viene creata una pianificazione di riavvio del catalogo, la pianificazione di riavvio viene eseguita solo sulle VM del catalogo appartenenti a un gruppo di distribuzione.

Esempio,

- Per creare una pianificazione di riavvio delle VM nel catalogo denominato **BankTellers** con inizio il 3 febbraio 2022, tra le 2:00 e le 4:00.

```
1 C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -
    CatalogName BankTellers -StartDate "2022-02-03" -StartTime
    "02:00" -Enabled $true -RebootDuration 120
```

- Per creare una pianificazione di riavvio delle VM nel catalogo con UID 17, a partire dal 3 febbraio 2022, tra l'1:00 e le 5:00 del mattino. Dieci minuti prima del riavvio, ogni macchina virtuale è impostata per visualizzare una finestra di messaggio con il titolo **ATTENZIONE: riavvio in sospeso** e il messaggio **Salva il tuo lavoro** in ogni sessione utente.

```
1 C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -
    Enabled $true -RebootDuration 240 -WarningTitle "WARNING:
    Reboot pending" -WarningMessage "Save your work" -
    WarningDuration 10
```

- Per rinominare il catalogo riavviare la pianificazione denominata **Vecchio nome** in **Nuovo nome**.

```
1 C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -
    NewName "New Name"
```

- Per visualizzare tutte le pianificazioni di riavvio del catalogo con UID 1, quindi rinominare la pianificazione di riavvio del catalogo con UID 1 in **Nuovo nome**.

```
1 C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
    BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- Per impostare la pianificazione del riavvio del catalogo denominata **Contabilità** per visualizzare un messaggio con il titolo, **AVVISO: Riavvio in sospeso, e il messaggio, Salva il tuo lavoro**, dieci minuti prima del riavvio di ogni VM. Il messaggio appare in ogni sessione utente su quella VM.

“

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage "Save your
work"-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
```

- To display all restart schedules that are disabled, and then enable all disabled restart schedules.


```
1 C:\PS> Get-BrokerCatalogRebootSchedule -Abilitato $false | Set-BrokerCatalogRebootSchedule -Abilitato $true
```

- To set the catalog restart schedule with UID 17 to display the message **Rebooting in %m% minutes** fifteen, ten, and five minutes before the restart of each VM.

```
1 C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Riavvio in %m% minuti." -WarningDuration 15 -WarningRepeatInterval 5
```

- To configure the time zone for the catalog named **MyCatalog**.

```
C:\PS> Set-BrokerCatalog -Nome "MyCatalog"-Fuso orario <TimeZone>
```

Caricare le macchine gestite nei gruppi di consegna

È possibile caricare e gestire solo macchine con sistema operativo multisessione.

La gestione del carico misura il carico del server e determina quale server selezionare in base alle condizioni ambientali correnti. Questa selezione si basa su:

- **Stato della modalità di manutenzione del server:** Una macchina con sistema operativo multisessione viene presa in considerazione per il bilanciamento del carico solo quando la modalità di manutenzione è disattivata.
- **Indice di carico del server:** Determina la probabilità che un server che fornisce macchine con sistema operativo multisessione riceva connessioni. L'indice è una combinazione di valutatori del carico: il numero di sessioni e le impostazioni per le metriche delle prestazioni quali l'utilizzo di CPU, disco e memoria. I valutatori del carico sono specificati nelle impostazioni della policy di gestione del carico.

Un indice di carico del server pari a 10000 indica che il server è completamente carico. Se non sono disponibili altri server, gli utenti potrebbero ricevere un messaggio che indica che il desktop o l'applicazione non sono disponibili quando avviano una sessione.

È possibile monitorare l'indice di carico in Director (Monitor), nella ricerca di Web Studio (Manage) e nell'SDK.

Nelle visualizzazioni della console, per visualizzare la colonna **Server Load Index** (nascosta per impostazione predefinita), selezionare una macchina, fare clic con il pulsante destro del mouse su un'intestazione di colonna, quindi selezionare **Seleziona colonna**. Nella categoria Macchina ******, **seleziona **Indice di carico**.

Nell'SDK, utilizzare il cmdlet `Get-BrokerMachine`. Per i dettagli, vedere [CTX202150](#).

- **Impostazione della policy di tolleranza degli accessi simultanei:** Numero massimo di richieste simultanee di accesso al server. (Questa impostazione equivale alla limitazione del carico nelle versioni 6.x di XenApp.)

Quando tutti i server raggiungono o superano il valore impostato per la tolleranza degli accessi simultanei, la richiesta di accesso successiva viene assegnata al server con il minor numero di accessi in sospeso. Se più server soddisfano questi criteri, viene selezionato il server con l'indice di carico più basso.

Macchine gestite dall'alimentazione in un gruppo di consegna

È possibile gestire l'alimentazione solo delle macchine virtuali con sistema operativo a sessione singola, non delle macchine fisiche (incluse le macchine con accesso remoto al PC). I computer con sistema operativo a sessione singola e funzionalità GPU non possono essere sospesi, pertanto le operazioni di spegnimento falliscono. Per i computer con sistema operativo multisessione, è possibile creare una pianificazione di riavvio.

Nei gruppi di distribuzione contenenti macchine in pool, le macchine virtuali con sistema operativo a sessione singola possono trovarsi in uno dei seguenti stati:

- Assegnato in modo casuale e in uso
- Non assegnato e non connesso

Nei gruppi di distribuzione contenenti macchine statiche, le macchine virtuali del sistema operativo a sessione singola possono essere:

- Assegnato in modo permanente e in uso
- Assegnato in modo permanente e non connesso (ma pronto)
- Non assegnato e non connesso

Durante il normale utilizzo, i gruppi di distribuzione statici contengono in genere sia macchine allocate in modo permanente che non allocate. Inizialmente, tutte le macchine non sono assegnate, ad eccezione di quelle assegnate manualmente quando è stato creato il gruppo di consegna. Quando gli utenti si connettono, le macchine vengono assegnate in modo permanente. È possibile gestire completamente le macchine non assegnate in quei gruppi di distribuzione, ma solo parzialmente le macchine assegnate in modo permanente.

- **Pool e buffer:** Per i gruppi di distribuzione in pool e i gruppi di distribuzione statici con macchine non assegnate, un pool (in questo caso) è un set di macchine non assegnate o temporaneamente assegnate che vengono mantenute accese, pronte per la connessione degli utenti. L'utente riceve una macchina subito dopo aver effettuato l'accesso. La dimensione del pool (il numero di macchine tenute accese) è configurabile in base all'ora del giorno. Per i gruppi di distribuzione statici, utilizzare l'SDK per configurare il pool.

Un buffer è un set di macchine di standby extra non assegnate che vengono attivate quando il numero di macchine nel pool scende al di sotto di una soglia. La soglia è una percentuale della dimensione del gruppo di consegna. Per gruppi di consegna di grandi dimensioni, al superamento della soglia potrebbe essere attivato un numero significativo di macchine. Pertanto, è opportuno pianificare attentamente le dimensioni del gruppo di distribuzione oppure utilizzare l'SDK per regolare la dimensione predefinita del buffer.

- **Timer dello stato di alimentazione:** È possibile utilizzare i timer dello stato di alimentazione per sospendere i computer dopo che gli utenti si sono disconnessi per un periodo di tempo specificato. Ad esempio, le macchine si sospendono automaticamente al di fuori dell'orario d'ufficio se gli utenti rimangono disconnessi per almeno 10 minuti.

È possibile configurare i timer per i giorni feriali e i fine settimana, nonché per gli intervalli di punta e di non punta.

- **Gestione parziale dell'alimentazione delle macchine allocate in modo permanente:** Per le macchine allocate in modo permanente, è possibile impostare i timer dello stato di alimentazione, ma non i pool o i buffer. Le macchine vengono accese all'inizio di ogni periodo di punta e spente all'inizio di ogni periodo di bassa stagione. Non si ha lo stesso controllo preciso che si ha con le macchine non assegnate sul numero di macchine che diventano disponibili per compensare quelle consumate.

Gestisci l'alimentazione delle macchine virtuali con sistema operativo a sessione singola

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.
2. Seleziona un gruppo e poi fai clic su **Modifica gruppo di consegna** nella barra delle azioni.
3. Nella pagina **Gestione alimentazione**, seleziona **Giorni feriali** in **Macchine con gestione alimentazione**. Per impostazione predefinita, i giorni feriali sono dal lunedì al venerdì.
4. Per i gruppi di consegna casuali, in **Macchine da accendere**, fare clic su **Modifica** e quindi specificare la dimensione del pool durante i giorni feriali. Quindi, seleziona il numero di macchine da accendere.
5. In **Ore di punta**, imposta le ore di punta e di non punta per ogni giorno.
6. Imposta i timer dello stato di alimentazione per le ore di punta e non di punta durante i giorni feriali: In **Durante le ore di punta > Quando disconnesso**, specifica il ritardo (in minuti) prima di sospendere qualsiasi macchina disconnessa nel gruppo di distribuzione, quindi seleziona **Sospendi**. In **Durante le ore non di punta > Quando disconnesso**, specificare il ritardo prima di spegnere qualsiasi macchina disconnessa nel gruppo di distribuzione, quindi selezionare **Spegnimento**. Questo timer non è disponibile per i gruppi di consegna con macchine casuali.
7. Selezionare **Weekend** in **Macchine di gestione dell'alimentazione**, quindi configurare le ore di punta e i timer dello stato di alimentazione per i fine settimana.
8. Fai clic su **Applica** per applicare le modifiche apportate e mantenere la finestra aperta. Oppure clicca su **Salva** per applicare le modifiche e chiudere la finestra.

Utilizzare l'SDK per:

- Spegnere, anziché sospendere, i computer in risposta ai timer dello stato di alimentazione oppure se si desidera che i timer siano basati sulle disconnessioni, anziché sulle disconnessioni.
- Modifica le definizioni predefinite dei giorni feriali e dei fine settimana.
- Disattivare la gestione dell'alimentazione. Vedere [CTX217289](#).

Gestire l'alimentazione delle macchine VDI in transizione verso un periodo di tempo diverso con sessioni disconnesse

Importante:

Questo miglioramento si applica solo alle macchine VDI con sessioni disconnesse. Non si applica alle macchine VDI con sessioni disconnesse.

Nelle versioni precedenti, una macchina VDI che passava a un periodo di tempo in cui era richiesta un'azione (azione di disconnessione="Sospendi" o "Spegni") rimaneva accesa. Questo scenario si è verificato se la macchina si è disconnessa durante un periodo di tempo (orari di punta o di bassa stagione) in cui non era richiesta alcuna azione (azione di disconnessione="Niente").

A partire da Citrix Virtual Apps and Desktops 7 1909, la macchina viene sospesa o spenta allo scadere del tempo di disconnessione specificato, a seconda dell'azione di disconnessione configurata per il periodo di tempo di destinazione.

Ad esempio, è possibile configurare i seguenti criteri di alimentazione per un gruppo di distribuzione VDI:

- Imposta `PeakDisconnectAction` su "Niente"
- Imposta `OffPeakDisconnectAction` su "Arresto"
- Imposta `OffPeakDisconnectTimeout` su "10"

Per ulteriori informazioni sull'azione di disconnessione nella policy di alimentazione, vedere https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy e <https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>.

Nelle versioni precedenti, una macchina VDI con una sessione disconnessa durante gli orari di punta rimaneva accesa quando passava dall'orario di punta a quello di bassa stagione. A partire da Citrix Virtual Apps and Desktops 7 1909, le azioni di policy `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` vengono applicate alla macchina VDI durante la transizione del periodo. Di conseguenza, la macchina si spegne 10 minuti dopo il passaggio alla fascia oraria di basso consumo.

Se si desidera ripristinare il comportamento precedente (ovvero non eseguire alcuna azione sulle macchine che passano dalla modalità di punta a quella di bassa stagione o viceversa con sessioni disconnesse), procedere in uno dei seguenti modi:

- Imposta il valore del registro `LegacyPeakTransitionDisconnectedBehaviour` su 1, l'equivalente di *true* che abilita il comportamento precedente. Per impostazione predefinita, il valore è 0, oppure *false*, che attiva le azioni di disconnessione della politica di alimentazione durante la transizione del periodo.
 - Percorso: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
 - Nome: `LegacyPeakTransitionDisconnectedBehaviour`
 - Tipo: `REG_DWORD`
 - Dati: `0x00000001 (1)`
- Configurare l'impostazione utilizzando il comando PowerShell `Set-BrokerServiceConfigurationData`. Per esempio:
 - PS `C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Una macchina deve soddisfare i seguenti criteri prima che le azioni della politica energetica possano essere applicate durante la transizione del periodo:

- Avere una sessione disconnessa.
- Non avere azioni di potenza in sospeso.
- Appartenere a un gruppo di distribuzione VDI (singola sessione) che passa a un periodo di tempo diverso.
- Avere una sessione che si disconnette durante un determinato periodo di tempo (orari di punta o di bassa stagione) e passa a un periodo in cui è assegnata un'azione di potenza.

Modifica la percentuale di VDA in stato alimentato per i cataloghi

1. Regola le ore di punta per il gruppo di consegna dalla sezione **Gestione alimentazione** per il gruppo di consegna.
2. Prendi nota del nome del gruppo desktop.
3. Con privilegi di amministratore, avviare PowerShell ed eseguire i seguenti comandi. Sostituisci "Nome gruppo desktop" con il nome del gruppo desktop in cui è in esecuzione una percentuale modificata di VDA.

```
asnp Citrix*
```

```
# Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent 100
```

Un valore pari a 100 significa che il 100% dei VDA è pronto.

4. Verificare la soluzione eseguendo:

```
#Get-BrokerDesktopGroup "Desktop Group Name"
```

```

PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerDesktopGroup "win 7 pvd pol
led"

AdministratorNames           : <>
AutomaticPowerOnForAssigned  : True
ColorDepth                   : TwentyFourBit
Description                   :
DesktopKind                  : Private
DesktopsAvailable            : 0
DesktopsDisconnected         : 0
DesktopsInUse                : 0
DesktopsNeverRegistered      : 0
DesktopsPreparing           : 0
DesktopsUnregistered         : 0
Enabled                       : True
IconUid                      : 1
InMaintenanceMode           : False
Name                         : Win 7 PvD Polled
OffPeakBuffer$izePercent     : 10
OffPeakDisconnectAction      : Nothing
OffPeakDisconnectTimeout    : 0
OffPeakExtendedDisconnectAction : Nothing
OffPeakExtendedDisconnectTimeout : 0
OffPeakLogOffAction         : Nothing
OffPeakLogOffTimeout        : 0
PeakBuffer$izePercent        : 100
PeakDisconnectAction         : Nothing
PeakDisconnectTimeout       : 0
PeakExtendedDisconnectAction : Nothing
PeakExtendedDisconnectTimeout : 0
PeakLogOffAction            : Nothing
PeakLogOffTimeout           : 0
ProtocolPriority             : <>
PublishedName                : Win 7 PvD Polled
SecureIcaRequired            : False
ShutdownDesktopsAfterUse    : False
Tags                         : <>
TimeZone                    : Eastern Standard Time
TotalDesktops                : 3
UUID                        : e3854918-420e-4fab-a2b8-1dfb08416d4b
Uid                          : 3

PS C:\Program Files\Citrix\Desktop Studio>

```

Potrebbe volerci fino a un'ora prima che le modifiche diventino effettive.

Per chiudere i VDA dopo che l'utente si è disconnesso, immettere:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutdownDesktopsAfterUse
$True
```

Per riavviare i VDA durante le ore di punta, in modo che siano pronti per gli utenti dopo la disconnessione, immettere:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
$True
```

Sessioni

- Disconnettersi o disconnettere una sessione, oppure inviare un messaggio agli utenti
- Configurare il pre-avvio della sessione e il mantenimento della sessione
- Controlla la riconnessione della sessione quando disconnesso dalla macchina in modalità di manutenzione

- Configurare il roaming della sessione

Disconnettersi o disconnettere una sessione

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.
2. Seleziona un gruppo di consegna, quindi seleziona **Visualizza macchine** nella barra delle azioni.
3. Nel riquadro centrale, seleziona la macchina, seleziona **Visualizza sessioni** nella barra delle azioni, quindi seleziona una sessione.
 - In alternativa, nel riquadro centrale, seleziona la scheda **Sessione** e quindi seleziona una sessione.
4. Per disconnettersi da una sessione, selezionare **Disconnetti** nella barra delle azioni. La sessione si chiude e l'utente viene disconnesso. La macchina diventa disponibile per altri utenti, a meno che non venga assegnata a un utente specifico.
5. Per disconnettere una sessione, seleziona **Disconnetti** nella barra delle azioni. Le applicazioni continuano a essere eseguite nella sessione e la macchina rimane assegnata a quell'utente. L'utente può riconnettersi alla stessa macchina.

È possibile configurare i timer dello stato di alimentazione per i computer con sistema operativo a sessione singola, in modo da gestire automaticamente le sessioni inutilizzate. Per maggiori dettagli, vedere [Macchine con gestione dell'alimentazione](#).

Invia un messaggio a un gruppo di consegna

1. Selezionare **Gruppi di consegna** nel riquadro a sinistra.
2. Seleziona un gruppo di consegna, quindi seleziona **Visualizza macchine** nella barra delle azioni.
3. Nel riquadro centrale, seleziona la macchina a cui desideri inviare un messaggio.
4. Nella barra delle azioni, seleziona **Visualizza sessioni**.
5. Nel riquadro centrale, seleziona tutte le sessioni, quindi seleziona **Invia messaggio** nella barra delle azioni.
6. Digita il tuo messaggio e clicca su **OK**. Se necessario, è possibile specificare il livello di gravità. Le opzioni includono **Critico, Domanda, Avviso e Informazioni**.

In alternativa, è possibile inviare un messaggio tramite Citrix Director. Per ulteriori informazioni, vedere [Invia messaggi agli utenti](#).

Configurare il preavvio della sessione e la permanenza della sessione in un gruppo di distribuzione

Queste funzionalità sono supportate solo su macchine con sistema operativo multisessione.

Le funzionalità di preavvio e mantenimento della sessione aiutano determinati utenti ad accedere rapidamente alle applicazioni, avviando le sessioni prima che vengano richieste (preavvio della sessione) e mantenendo attive le sessioni delle applicazioni dopo che l'utente ha chiuso tutte le applicazioni (mantenimento della sessione).

Per impostazione predefinita, il pre-avvio della sessione e il mantenimento della sessione non vengono utilizzati. Una sessione inizia (viene avviata) quando un utente avvia un'applicazione e rimane attiva fino alla chiusura dell'ultima applicazione aperta nella sessione.

Considerazioni:

- Il gruppo di consegna deve supportare le applicazioni e le macchine devono eseguire un VDA per sistemi operativi multisessione, versione minima 7.6.
- Queste funzionalità sono supportate solo quando si utilizza l'app Citrix Workspace per Windows e richiedono inoltre una configurazione aggiuntiva dell'app Citrix Workspace. Per istruzioni, cerca il preavvio della sessione nella documentazione del prodotto per la versione dell'app Citrix Workspace per Windows.
- L'app Citrix Workspace per HTML5 non è supportata.
- Quando si utilizza il preavvio della sessione, se il computer di un utente viene messo in modalità sospensione o ibernazione, il preavvio non funziona (indipendentemente dalle impostazioni del preavvio della sessione). Gli utenti possono bloccare i propri computer/sessioni. Tuttavia, se un utente si disconnette dall'app Citrix Workspace, la sessione viene terminata e il preavvio non è più valido.
- Quando si utilizza il preavvio della sessione, i computer client fisici non possono utilizzare le funzioni di gestione dell'alimentazione di sospensione o ibernazione. Gli utenti dei computer client possono bloccare le proprie sessioni, ma non devono disconnettersi.
- Le sessioni pre-avviate e persistenti consumano una licenza simultanea, ma solo quando si è connessi. Se si utilizza una licenza utente/dispositivo, la licenza dura 90 giorni. Per impostazione predefinita, le sessioni pre-avviate e persistenti inutilizzate si disconnettono dopo 15 minuti. Questo valore può essere configurato in PowerShell (`cmdletNew/Set-BrokerSessionPreLaunch`).
- Un'attenta pianificazione e un monitoraggio dei modelli di attività dei tuoi utenti sono essenziali per adattare queste funzionalità in modo che si completino a vicenda. Una configurazione ottimale bilancia i vantaggi della disponibilità anticipata delle applicazioni per gli utenti con i costi di mantenimento delle licenze in uso e delle risorse assegnate.
- È anche possibile configurare il preavvio della sessione per un orario programmato della giornata nell'app Citrix Workspace.

Per quanto tempo le sessioni pre-lanciate e persistenti inutilizzate rimangono attive Esistono diversi modi per specificare per quanto tempo una sessione inutilizzata rimane attiva se l'utente non avvia un'applicazione: un timeout configurato e soglie di carico del server. Puoi configurarli tutti. L'evento che si verifica per primo determina la chiusura della sessione inutilizzata.

- **Timeout:** Un timeout configurato specifica il numero di minuti, ore o giorni in cui una sessione pre-avviata o persistente inutilizzata rimane attiva. Se si configura un timeout troppo breve, le sessioni pre-avviate terminano prima di poter offrire all'utente il vantaggio di un accesso più rapido alle applicazioni. Se si configura un timeout troppo lungo, le connessioni utente in arrivo potrebbero essere negate perché il server non dispone di risorse sufficienti.

È possibile abilitare questo timeout solo dall'SDK (`cmdletNew/Set-BrokerSessionPreLaunch`), non dalla console di gestione. Se si disabilita il timeout, questo non verrà visualizzato nella console per quel gruppo di recapito o nelle pagine **Modifica gruppo di recapito**.

- **Soglie:** La conclusione automatica delle sessioni pre-avviate e persistenti in base al carico del server garantisce che le sessioni restino aperte il più a lungo possibile, supponendo che le risorse del server siano disponibili. Le sessioni pre-avviate e persistenti inutilizzate non causano connessioni negate perché vengono terminate automaticamente quando sono necessarie risorse per nuove sessioni utente.

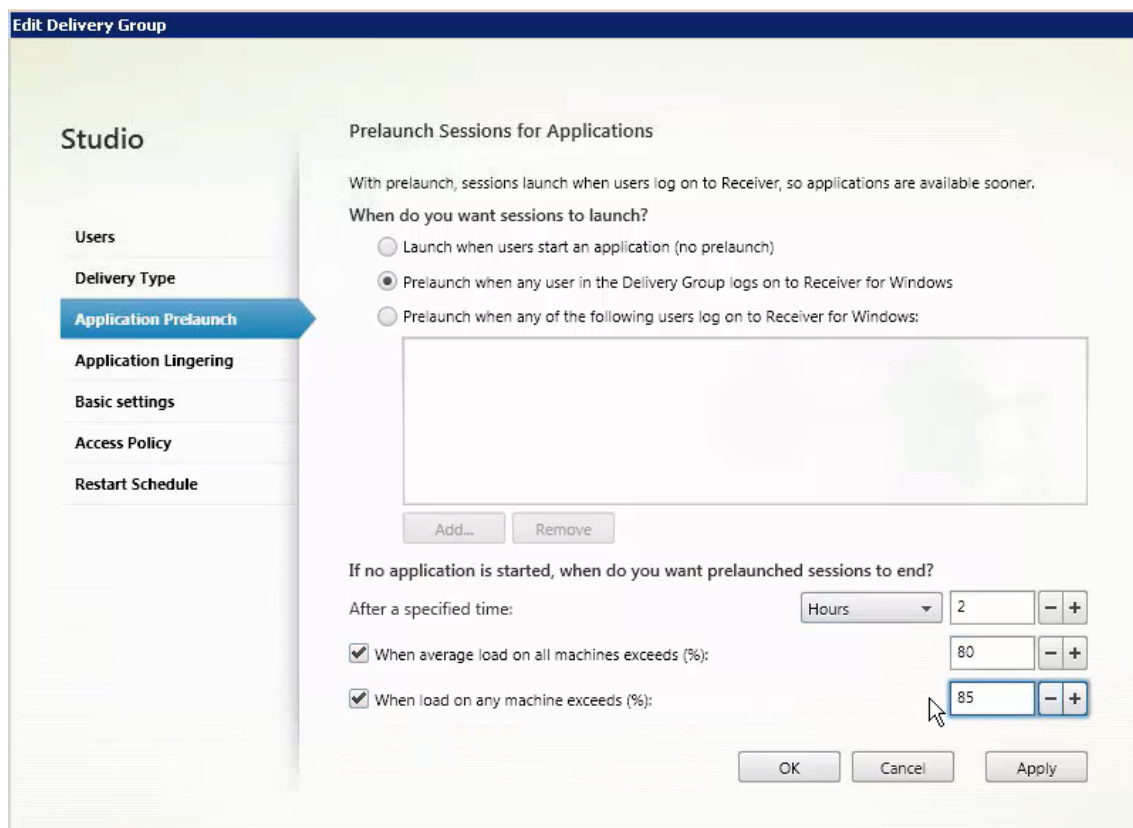
È possibile configurare due soglie: la percentuale media del carico di tutti i server nel gruppo di distribuzione e la percentuale massima del carico di un singolo server nel gruppo. Quando viene superata una soglia, le sessioni rimaste più a lungo nello stato di pre-lancio o in stato di attesa vengono terminate. Le sessioni vengono terminate una alla volta a intervalli di un minuto, finché il carico non scende sotto la soglia. Finché la soglia viene superata, non vengono avviate nuove sessioni di pre-lancio.

I server con VDA che non sono registrati presso un Controller e i server in modalità di manutenzione sono considerati completamente caricati. Un'interruzione non pianificata provoca la fine automatica delle sessioni di pre-avvio e di quelle persistenti, liberando capacità.

Per abilitare il preavvio della sessione

1. Seleziona un gruppo e poi fai clic su **Modifica gruppo di consegna** nella barra delle azioni.
2. Nella pagina **Preavvio applicazione**, abilita il preavvio della sessione scegliendo quando avviare la sessione:
 - Quando un utente avvia un'applicazione. Questa è l'impostazione predefinita. Il preavvio della sessione è disabilitato.
 - Quando un utente del gruppo di distribuzione accede all'app Citrix Workspace per Windows.

- Quando qualcuno in un elenco di utenti e gruppi di utenti accede all'app Citrix Workspace per Windows. Se si sceglie questa opzione, assicurarsi di specificare anche gli utenti o i gruppi di utenti.



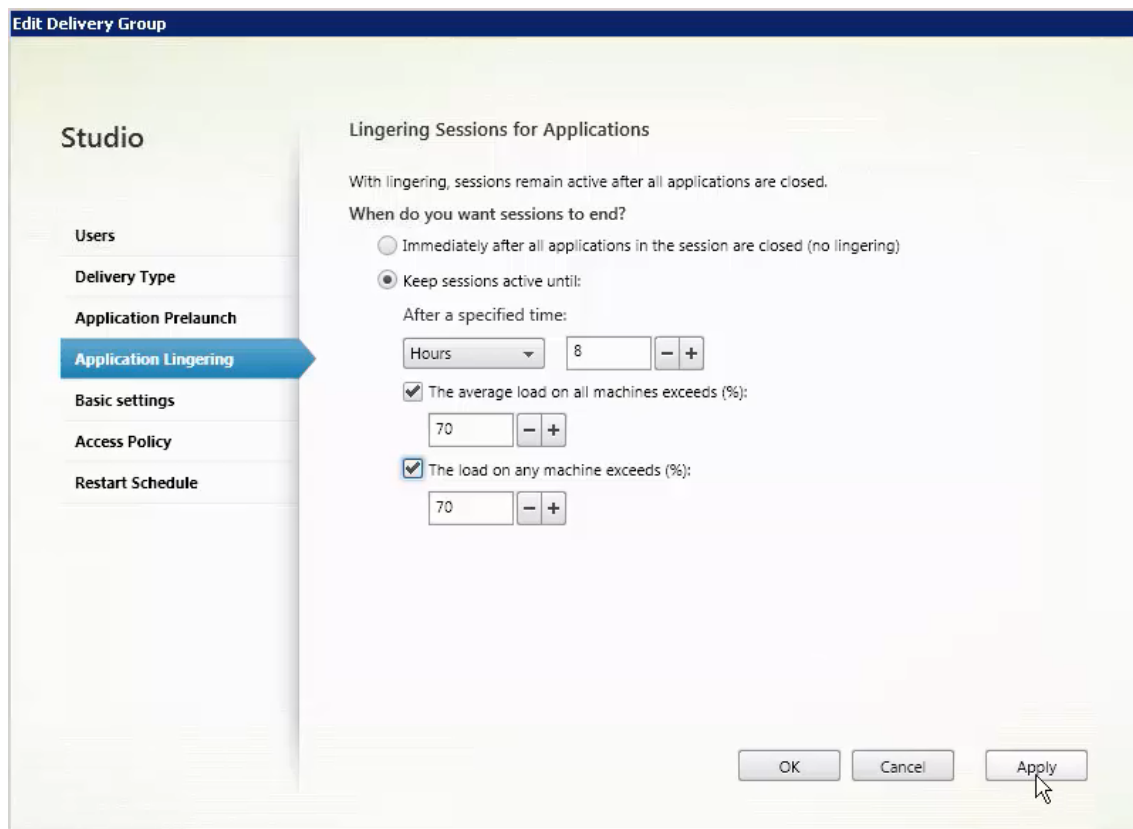
3. Una sessione pre-avviata viene sostituita da una sessione normale quando l'utente avvia un'applicazione. Se l'utente non avvia un'applicazione (la sessione pre-avviata non viene utilizzata), le seguenti impostazioni influiscono sulla durata di attività della sessione.
 - Quando trascorre un intervallo di tempo specificato. È possibile modificare l'intervallo di tempo (1–99 giorni, 1–2376 ore o 1–142.560 minuti).
 - Quando il carico medio su tutte le macchine del gruppo di consegna supera una percentuale specificata (1-99%).
 - Quando il carico su una qualsiasi macchina del gruppo di consegna supera una percentuale specificata (1-99%).

Riepilogo: una sessione pre-avviata rimane attiva finché non si verifica uno dei seguenti eventi: un utente avvia un'applicazione, scade il tempo specificato o viene superata una soglia di carico specificata.

Per abilitare la sessione linger

1. Selezionare **Gruppi di distribuzione** nel riquadro a sinistra.

2. Seleziona un gruppo e poi fai clic su **Modifica gruppo di consegna** nella barra delle azioni.
3. Nella pagina **Persistenza applicazione**, abilita la persistenza della sessione selezionando **Mantieni le sessioni attive fino a**.



4. Diverse impostazioni determinano per quanto tempo una sessione persistente rimane attiva se l'utente non avvia un'altra applicazione.
 - Quando trascorre un intervallo di tempo specificato. È possibile modificare l'intervallo di tempo: 1–99 giorni, 1–2376 ore o 1–142.560 minuti.
 - Quando il carico medio su tutte le macchine del gruppo di consegna supera una percentuale specificata: 1–99%.
 - Quando il carico su una qualsiasi macchina del gruppo di consegna supera una percentuale specificata: 1–99%.

Riepilogo: una sessione persistente rimane attiva finché non si verifica uno dei seguenti eventi: un utente avvia un'applicazione, scade il tempo specificato o viene superata una soglia di carico specificata.

Controlla la riconnessione della sessione quando disconnesso dalla macchina in modalità di manutenzione

NOTA:

Questa funzionalità è disponibile solo in PowerShell.

È possibile controllare se le sessioni disconnesse sui computer in modalità di manutenzione possono riconnettersi ai computer nel gruppo di distribuzione.

Prima della versione 2106, la riconnessione non era consentita per le sessioni desktop in pool a sessione singola che si erano disconnesse dai computer in modalità di manutenzione. A partire dalla versione 2106, è possibile configurare un gruppo di distribuzione per consentire o vietare le riconnesioni (indipendentemente dal tipo di sessione) dopo la disconnessione da una macchina in modalità di manutenzione.

Quando si crea o si modifica un gruppo di distribuzione (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), utilizzare il parametro `-AllowReconnectInMaintenanceMode <boolean>` per consentire o vietare le riconnesioni per le macchine che sono state disconnesse da una macchina in modalità di manutenzione.

- Se impostato su `true`, le sessioni possono riconnettersi alle macchine del gruppo.
- Se impostato su `false`, le sessioni non possono riconnettersi alle macchine del gruppo.

Valori predefiniti:

- Sessione singola: disabilitato
- Multi-sessione: Abilitato

Configurare il roaming della sessione

Per impostazione predefinita, il roaming di sessione è abilitato per i gruppi di distribuzione. Le sessioni si spostano tra i dispositivi client insieme all'utente. Quando l'utente avvia una sessione e poi passa a un altro dispositivo, viene utilizzata la stessa sessione e le applicazioni sono disponibili contemporaneamente su entrambi i dispositivi. È possibile visualizzare le applicazioni su più dispositivi. Le applicazioni vengono eseguite indipendentemente dal dispositivo e dall'esistenza o meno di sessioni correnti. Spesso seguono anche le stampanti e altre risorse assegnate all'applicazione. In alternativa, è possibile utilizzare PowerShell. Per ulteriori informazioni, vedere [Roaming di sessione](#).

Configurare il roaming di sessione per le applicazioni Per configurare il roaming di sessione per le applicazioni, seguire questi passaggi:

1. Nella console, seleziona **Gruppi di distribuzione** nel riquadro di sinistra.
2. Seleziona un gruppo, quindi seleziona **Modifica gruppo di consegna** nella barra delle azioni.

3. Nella pagina **Utenti** , abilita il roaming di sessione selezionando la casella di controllo **Le sessioni si muovono con gli utenti mentre si spostano tra i dispositivi** .
 - Se abilitata, se un utente avvia una sessione di un'applicazione e poi passa a un altro dispositivo, la stessa sessione viene utilizzata ed è disponibile su entrambi i dispositivi. Se disabilitata, la sessione non verrà più spostata tra i dispositivi.
4. Selezionare **OK** per applicare le modifiche e chiudere la finestra.

Configurare il roaming di sessione per i desktop Per configurare il roaming di sessione per un desktop, seguire questi passaggi:

1. Nella console, seleziona **Gruppi di distribuzione** nel riquadro di sinistra.
2. Seleziona un gruppo e poi seleziona **Modifica** nella barra delle azioni.
3. Nella pagina **Desktop** , seleziona il desktop e seleziona **Modifica**.
4. Abilitare il roaming di sessione selezionando la casella di controllo **Roaming di sessione** .
 - Se abilitata, se l'utente avvia il desktop e poi passa a un altro dispositivo, viene utilizzata la stessa sessione e le applicazioni sono disponibili su entrambi i dispositivi. Se disabilitata, la sessione non verrà più spostata tra i dispositivi.

Selezionare **OK** per applicare le modifiche e chiudere la finestra.

Risoluzione dei problemi

- I VDA che non sono registrati con un Delivery Controller non vengono presi in considerazione quando si avviano sessioni negoziate. Ciò comporta il sottoutilizzo di risorse altrimenti disponibili. Esistono vari motivi per cui un VDA potrebbe non essere registrato, molti dei quali possono essere risolti da un amministratore. La visualizzazione dei dettagli fornisce informazioni sulla risoluzione dei problemi nella procedura guidata di creazione del catalogo e dopo aver aggiunto un catalogo a un gruppo di distribuzione.

Dopo aver creato un gruppo di distribuzione, il riquadro dei dettagli per un gruppo di distribuzione indica il numero di macchine che possono essere registrate ma non lo sono. Ad esempio, una o più macchine sono accese e non in modalità di manutenzione, ma non sono attualmente registrate con un controller. Quando si visualizza una macchina “non registrata, ma dovrebbe esserlo”, consultare la scheda **Risoluzione dei problemi** nel riquadro dei dettagli per individuare possibili cause e azioni correttive consigliate.

Per messaggi sul livello funzionale, vedere [versioni VDA e livelli funzionali](#).

Per informazioni sulla risoluzione dei problemi di registrazione VDA, vedere [CTX136668](#).

- Nella visualizzazione di un gruppo di distribuzione, la versione VDA installata ** nel riquadro dei dettagli potrebbe differire dalla versione effettivamente installata sui computer. La schermata Programmi e funzionalità di Windows del computer mostra la versione VDA effettiva.
- Per le macchine con stato **Stato di alimentazione sconosciuto** , vedere [CTX131267](#) per istruzioni.

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 disattivare l'impostazione **Enable automatic assignment of multiple users for Remote PC Access** (Abilita l'assegnazione automatica di più utenti per l'accesso remoto al PC).

Citrix Virtual Apps and Desktops può gestire più casi d'uso per PC fisici utilizzando altri tipi di cataloghi di macchine. Questi casi d'uso includono:

- PC Linux fisici
- PC fisici in pool (ovvero assegnati in modo casuale, non dedicati)

Note:

Per i dettagli sulle versioni del sistema operativo supportate, vedere i requisiti di sistema per il VDA per il [sistema operativo a sessione singola](#) e [Linux VDA](#).

Per le distribuzioni locali, 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 uti-

lizzando 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: RpgaMode
- 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: RpgaTimeout
- 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 RpccaMode è 1 o il valore del Registro di sistema RpccaMode 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 RpccaMode 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 RpcMode è 1 o il valore del Registro di sistema RpcMode è 2 o il valore del Registro di sistema RpcMode 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 RpcMode 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:

```

1 # Load Citrix SnapIns
2 Add-PSSnapIn -Name "*citrix*"
3
4 # Provide the name of the Wake on LAN host connection
5 [string]$connectionName = "Remote PC Access Wake on LAN"
6
7 # Create the hypervisor connection
8 $hypHc = New-Item -Path xdhyp:\Connections `
9     -Name $connectionName `
10    -HypervisorAddress "N/A" `
11    -UserName "woluser" `
12    -Password "wolpwd" `
13    -ConnectionType Custom `
14    -PluginId VdaWOLMachineManagerFactory `
15    -CustomProperties "<CustomProperties></CustomProperties
16    >" `
17    -Persist
18 $bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
19     $hypHc.HypervisorConnectionUid
20 # Wait for the connection to be ready before trying to use it
21 while (-not $bhc.IsReady)
22 {
23
24     Start-Sleep -s 5
25     $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
26         $hypHc.HypervisorConnectionUid
27 }

```

Quando la connessione host è pronta, eseguire i seguenti comandi per recuperare l’identificatore univoco della connessione host:

```

1 $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2 $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:

```

1 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 \(Accesso remoto PC\)](#).

Aggiornare e migrare

January 24, 2025

Introduzione

L'aggiornamento modifica la distribuzione alla versione corrente (CR) di Citrix Virtual Apps and Desktops 7 ** senza dover configurare nuovi computer o siti. Questo è noto come aggiornamento sul posto.

L'aggiornamento ti dà accesso alle funzionalità e alle tecnologie più recenti per cui hai diritto. Gli aggiornamenti possono contenere anche correzioni, chiarimenti e miglioramenti rispetto alle versioni precedenti.

Panoramica dell'aggiornamento

1. Prima di iniziare l'aggiornamento, leggere l'articolo [Aggiornare una distribuzione](#) . Questa è la principale fonte di informazioni per apprendere come preparare e implementare un aggiornamento.
2. Assicurati che le date attuali dei tuoi servizi di Customer Success Services siano valide e non scadute. Per ulteriori informazioni, consultare l'articolo [Rinnovo delle licenze dei Customer Success Services](#) .
3. Completare le istruzioni per la preparazione.
4. Eseguire 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 altri componenti.

Ogni fase di preparazione e aggiornamento è descritta in dettaglio in [Aggiornare una distribuzione](#).

Versioni che puoi aggiornare

È possibile effettuare l'aggiornamento a Citrix Virtual Apps and Desktops 2402 LTSR da:

- Applicazioni e desktop virtuali 2203 LTSR con o senza CU, fino a CU5 incluso
- Applicazioni e desktop virtuali 1912 LTSR con o senza CU, fino a CU9 incluso
- Versioni CR attualmente supportate di Citrix Virtual Apps and Desktops

Nota:

- Prima di avviare il processo di aggiornamento, Citrix consiglia ai clienti di testare l'aggiornamento in un ambiente controllato e di verificare che soddisfi i loro requisiti specifici. Inoltre, consigliamo di rivedere tutta la documentazione pertinente al prodotto, incluso l'elenco dei prodotti deprecati e dei problemi noti, per garantire una transizione senza intoppi. Questo approccio aiuta ad attenuare le potenziali interruzioni dei sistemi di produzione e migliora l'esperienza di aggiornamento complessiva.
- Citrix Virtual Apps and Desktops 1912 LTSR raggiungerà presto la fase di fine ciclo di vita. Per maggiori informazioni sull'elenco delle versioni supportate, vedere [Product Matrix](#).

Domande frequenti

Questa sezione risponde ad alcune domande frequenti sull'aggiornamento di Citrix Virtual Apps and Desktops.

- **Qual è l'ordine corretto per aggiornare il mio 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 ha diversi Delivery Controller (in zone diverse). Cosa succede se ne aggiorno solo alcuni? Sono obbligato ad aggiornare tutti i controller del sito durante la stessa finestra di manutenzione?**

La procedura migliore è quella di aggiornare tutti i Delivery Controller durante la stessa finestra di manutenzione, poiché vari servizi su ciascun Controller comunicano tra loro. Mantenere versioni diverse potrebbe causare problemi. Durante una finestra di manutenzione, ti consigliamo di aggiornare metà dei controller, aggiornare il sito e quindi aggiornare i controller rimanenti. Per i dettagli, vedere la procedura di aggiornamento .

- **Posso passare direttamente alla versione più recente oppure devo effettuare aggiornamenti incrementali?**

È quasi sempre possibile eseguire l'aggiornamento all'ultima versione e saltare le release intermedie, a meno che non sia esplicitamente indicato nell'articolo **Novità** per la versione a cui si desidera effettuare l'aggiornamento.- **Un cliente può effettuare l'aggiornamento da un ambiente LTSR (Long Term Service Release) a una Current Release?**

Sì. I clienti non sono tenuti a mantenere un Long Term Service Release per un periodo prolungato. I clienti possono spostare un ambiente LTSR a una versione corrente, in base alle funzionalità e ai requisiti aziendali.

- **Sono consentite versioni miste dei componenti?**

Citrix consiglia di aggiornare tutti i componenti alla stessa versione in ogni sito. Sebbene sia possibile utilizzare versioni precedenti di alcuni componenti, alcune funzionalità della versione più recente potrebbero non essere disponibili. Per ulteriori informazioni, vedere [Considerazioni sugli ambienti misti](#).

- **Con quale frequenza è necessario aggiornare 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 la versione Current Release più recente. Le versioni correnti raggiungono la fine del ciclo di vita (EOL) 18 mesi dopo la data di rilascio.- **Cosa è consigliato: passare a LTSR o CR?**

Le versioni correnti (CR) offrono le funzionalità e le caratteristiche più recenti e innovative per la virtualizzazione di app, desktop e server. Ciò ti consente di rimanere al passo con la tecnologia e di essere un passo avanti rispetto alla concorrenza.

Le Long Term Service Release (LTSR) sono ideali per gli ambienti di produzione delle grandi aziende che preferiscono mantenere la stessa versione di base per un periodo di tempo prolungato.

- **Devo aggiornare le mie licenze?**

Assicurati che la data della licenza corrente non sia scaduta e che sia valida per la versione a cui stai effettuando l'aggiornamento. Vedere [CTX111618](#). Per informazioni sul rinnovo, vedere [Rinnovo delle licenze dei Customer Success Services](#).

- **Quanto tempo richiede un aggiornamento?**

Il tempo necessario per aggiornare una distribuzione varia a seconda dell'infrastruttura e della rete. Pertanto non possiamo fornire un orario esatto.

- **Quali sono le migliori pratiche?**

Assicurati di aver compreso e seguito le istruzioni di preparazione .

- **Quali sistemi operativi sono supportati?**

L'articolo [Requisiti di sistema](#) per la versione a cui stai effettuando 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 ai collegamenti ai problemi noti.

- **Quando la mia versione cesserà di funzionare?**

Controllare la matrice prodotto .

- **Quali sono i problemi noti dell'ultima versione?**

- [Applicazioni e desktop virtuali Citrix](#)
- [Negozio Front](#)
- [Fornitura Citrix](#)
- [Server di licenza Citrix](#)
- [Applicazione Citrix Workspace per Windows](#)

Ulteriori informazioni**Gli aggiornamenti della distribuzione Long Term Service Release (LTSR) utilizzano aggiornamenti cumulativi (CU). Una CU aggiorna i componenti di base dell'LTSR e ogni CU include il proprio metainstaller**

Ogni CU ha una documentazione dedicata. Ad esempio, per il LTSR 2203, controlla il collegamento sulla pagina **Novità** del LTSR per l'ultima CU. Ogni pagina CU include informazioni sulla versione supportata, istruzioni e un collegamento al pacchetto di download CU.

Migrare

Migrare al cloud

È possibile utilizzare lo strumento di configurazione automatizzata per Citrix Virtual Apps and Desktops per migrare la distribuzione on-premise sul cloud. Per ulteriori informazioni, vedere [Migrazione al cloud](#).

Migrazione legacy

La migrazione sposta 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 dei dati dalla vecchia farm e la successiva importazione dei dati nel nuovo sito.

Non sono disponibili strumenti o script supportati per la migrazione delle versioni di 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 precedenti alla migrazione di XenApp 6.x, vedere quanto segue. Né gli script né gli articoli sono supportati o mantenuti.

- 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 gestisce questi script di migrazione
- [Modifiche in 7.x](#)
- [Aggiornare un worker XenApp 6.5 a un nuovo VDA](#)
- [Migrare XenApp 6.x](#)

Aggiornare una distribuzione

January 24, 2025

Nota:

Questo articolo riguarda gli aggiornamenti per le distribuzioni che coinvolgono Web Studio. Per informazioni sugli aggiornamenti che coinvolgono Citrix Studio, vedere l'articolo equivalente in Citrix Virtual Apps and Desktops 7 2212 o versioni precedenti.

Introduzione

È possibile aggiornare determinate distribuzioni a versioni più recenti senza dover prima configurare nuovi computer o siti. Questo è chiamato aggiornamento sul posto.

Per sapere quali versioni di Citrix Virtual Apps and Desktops puoi aggiornare, consulta [Versioni che puoi aggiornare](#).

Prima di effettuare l'aggiornamento a una qualsiasi delle versioni di Citrix Virtual Apps and Desktops, assicurati che le date correnti dei tuoi Customer Success Services siano valide e non siano scadute. Per ulteriori informazioni, consultare l'articolo [Rinnovo delle licenze dei Customer Success Services](#).

Per avviare un aggiornamento, è necessario eseguire il programma di installazione dalla nuova versione per aggiornare i componenti principali installati in precedenza, i VDA e alcuni altri componenti. Quindi si aggiornano i database e il sito.

È possibile aggiornare qualsiasi componente installabile con il programma di installazione completo del prodotto (e con i programmi di installazione VDA autonomi), se è disponibile una versione più recente. Per altri componenti che non sono installati con il programma di installazione completo del prodotto (ad esempio Citrix Provisioning e Profile Management), consultare la documentazione del componente in questione per ulteriori informazioni. Per gli aggiornamenti dell'host, consultare la documentazione appropriata.

Prima di iniziare un aggiornamento, leggere attentamente tutte le informazioni contenute in questo articolo.

Sequenza di aggiornamento

Il diagramma seguente mostra i passaggi della sequenza di aggiornamento. La procedura di aggiornamento contiene i dettagli di ogni passaggio nel diagramma.

[Diagramma di flusso della sequenza di aggiornamento](#)

Nota:

Per evitare errori, è necessario aggiornare tutti i Delivery Controller e il database prima di eseguire qualsiasi attività correlata al provisioning e al gruppo di distribuzione, come la creazione di un nuovo catalogo macchine, l'eliminazione di un catalogo macchine, l'aggiornamento di una macchina in un gruppo di distribuzione e così via.

Licenze di diritti ibridi

Le licenze Hybrid Rights sono licenze di abbonamento a termine che vengono fornite, in aggiunta all'abbonamento al servizio cloud, quando un cliente passa da una licenza perpetua a un abbonamento

al servizio cloud. Puoi anche acquistare un componente aggiuntivo Hybrid Rights con i tuoi abbonamenti DaaS.

Se disponi di una licenza Hybrid Rights con attributo SaaS, quando esegui l'upgrade a Citrix Virtual Apps and Desktops LTSR 2203 e versioni successive, diventi idoneo ad accedere a funzionalità non disponibili con Citrix Virtual Apps and Desktops LTSR 1912. Queste funzionalità includono il provisioning e l'hosting di carichi di lavoro su cloud pubblici, come Microsoft Azure, AWS EC2 e Google Cloud. Prima di distribuire il nuovo file di licenza, aggiorna il License Server alla versione più recente.

Se hai accesso a una licenza Hybrid Rights senza attributo SaaS, segui questi passaggi per ottenere l'accesso alla nuova licenza Hybrid Rights con attributo SaaS:

Nota:

- Riceverai un'e-mail con un nuovo codice di licenza. Per ulteriori informazioni, vedere [Utilizzare il codice di accesso alla licenza](#).
- Le tue licenze esistenti sono state revocate. Le licenze revocate devono essere eliminate dai server delle licenze e poi installate nuove licenze. Per ulteriori informazioni, vedere [Eliminazione dei file di licenza](#).

1. Vai al portale citrix.com Gestisci licenze e scarica il nuovo file di licenza Hybrid Rights con i diritti di provisioning cloud abilitati (attributo SaaS). Per ulteriori informazioni, vedere [Scarica licenze](#). L'immagine seguente mostra il file di licenza Hybrid Rights con l'attributo SaaS nella sezione Incrementi.

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
VENDOR_STRING=LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS;SA=0;ODP=0;NODURMIN=2880;NODURMAX=525600;AP=ADMIN/INT/14
OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. Installare il file di licenza Hybrid Rights sul License Server. Per ulteriori informazioni, vedere [Installa licenze](#).
3. In caso di modifica delle edizioni o del modello di licenza, assicurarsi di eseguire il comando broker per impostare l'edizione e il modello, quindi avviare l'aggiornamento sul posto. Per ulteriori informazioni sui comandi Broker, vedere la sezione [Broker PowerShell SDK](#).

Per ulteriori informazioni sul supporto del cloud pubblico con le versioni correnti e le versioni di servizi a lungo termine di Citrix Virtual Apps and Desktops, vedere [CTX270373](#).

Procedura di aggiornamento

La maggior parte dei componenti principali del prodotto può essere aggiornata eseguendo il programma di installazione del prodotto sul computer che contiene il componente.

Se una macchina contiene più di un componente (ad esempio, Studio e License Server), tutti i componenti su quella macchina vengono aggiornati, se il supporto del prodotto contiene versioni più recenti del loro software.

Per utilizzare gli installatori:

- Per eseguire l'interfaccia grafica del programma di installazione completo del prodotto, accedere al computer, quindi inserire il supporto o montare l'unità ISO per la nuova versione. Fare doppio clic su **Selezione automatica**.
- Per utilizzare l'interfaccia della riga di comando, immettere il comando appropriato. Vedere [Installare tramite la riga di comando](#).

Fase 1: Preparazione

Prima di iniziare un aggiornamento, assicurati di essere pronto. Leggi e completa tutte le attività necessarie:

- Rimuovi PVD, AppDisk e host non supportati
- VDA che hanno componenti PvD o AppDisk
- Limitazioni
- Considerazioni sull'ambiente misto
- Sistemi operativi precedenti
- Preparazione
- Prove preliminari in loco
- Controllo della versione di SQL Server

Passaggio 2: Aggiorna il server delle licenze

Se l'installazione include una nuova versione del software Citrix License Server, aggiornare prima questo componente e poi tutti gli altri.

Se non hai ancora determinato se il tuo License Server è compatibile con la nuova versione, è essenziale eseguire il programma di installazione sul License Server prima di aggiornare qualsiasi altro componente principale.

Passaggio 3: Aggiorna StoreFront

Se il supporto di installazione contiene una nuova versione del software StoreFront, eseguire il programma di installazione sul computer che contiene il server StoreFront.

- Nell'interfaccia grafica, seleziona **Citrix StoreFront** dalla sezione **Estendi distribuzione**.

- Dalla riga di comando, eseguire `CitrixStoreFront-x64.exe`, disponibile nella cartella `x64` del supporto di installazione di Citrix Virtual Apps and Desktops.

Passaggio 4: Aggiorna Director

Se il supporto di installazione contiene una nuova versione del software Director, eseguire il programma di installazione sul computer che contiene Director.

Passaggio 5: aggiornare Citrix Provisioning

Il supporto di installazione di Citrix Provisioning è disponibile separatamente dal supporto di installazione di Citrix Virtual Apps and Desktops. Per informazioni su come installare e aggiornare il software del server Citrix Provisioning e del dispositivo di destinazione, consultare la [documentazione del prodotto Citrix Provisioning](#).

Fase 6: Aggiornare metà dei Delivery Controller

Ad esempio, se il tuo sito ha quattro controller, esegui il programma di installazione su due di essi.

Lasciando attivi metà dei Controller, gli utenti potranno accedere al sito. I VDA possono registrarsi presso i restanti Controllori. Potrebbero verificarsi momenti in cui la capacità del sito è ridotta perché sono disponibili meno controllori. L'aggiornamento provoca solo una breve interruzione nella creazione di nuove connessioni client durante le fasi finali di aggiornamento del database. I Controller aggiornati non potranno elaborare le richieste finché non sarà stato aggiornato l'intero sito.

Se il tuo sito ha un solo Controller, questo non sarà operativo durante l'aggiornamento.

Prima dell'avvio dell'aggiornamento vero e proprio, vengono eseguiti test preliminari sul sito sul primo Controller. Per maggiori dettagli, vedere Test preliminari del sito.

Passaggio 7: Aggiorna Studio

Se non hai ancora aggiornato Web Studio (perché si trovava sullo stesso computer di un altro componente), esegui il programma di installazione sul computer che contiene Studio.

Nota:

Dopo aver aggiornato Web Studio, le informazioni sulla versione potrebbero non aggiornarsi immediatamente. Potrebbe venirti richiesto di aggiornare Web Studio anche se è già aggiornato. Per risolvere il problema, vai al server Web Studio, apri Gestione Internet Information Services

(IIS), vai a Pagina iniziale > Siti > Sito Web predefinito e seleziona **Riavvia** nel riquadro Gestisci sito Web.

Passaggio 8: riavviare Studio

Riavviare il Web Studio aggiornato. Il processo di aggiornamento riprende automaticamente.

Passaggio 9: Aggiornare il database e il sito

Nota:

Per evitare errori, è necessario aggiornare tutti i Delivery Controller e il database prima di eseguire qualsiasi attività correlata al provisioning e al gruppo di distribuzione, come la creazione di un nuovo catalogo macchine, l'eliminazione di un catalogo macchine, l'aggiornamento di una macchina in un gruppo di distribuzione e così via.

Controllare Preparazione per le autorizzazioni necessarie per aggiornare lo schema dei database di SQL Server.

- Se si dispone dell'autorizzazione sufficiente per aggiornare lo schema del database di SQL Server, è possibile avviare un aggiornamento automatico del database. Continua con **Aggiorna automaticamente il database e il sito**.
- Se non si dispone di sufficienti autorizzazioni per il database, è possibile avviare un aggiornamento manuale tramite script e procedere con l'aiuto dell'amministratore del database (qualcuno che dispone delle autorizzazioni necessarie). Per un aggiornamento manuale, l'utente Studio genera gli script e quindi esegue gli script che abilitano e disabilitano i servizi. L'amministratore del database esegue altri script che aggiornano lo schema del database, utilizzando l'utilità SQLCMD o SQL Server Management Studio in modalità SQLCMD. Continua con **Aggiorna manualmente il database e il sito**.
- Se si dispone di una distribuzione multizona e si desidera aggiornare automaticamente il database e il sito, Citrix consiglia di eseguire l'aggiornamento di dbschema nella stessa zona che ospita i database SQL Server del sito. In caso contrario, l'aggiornamento automatico del database e del sito potrebbe non riuscire.

Citrix consiglia vivamente di eseguire il backup del database prima di effettuare l'aggiornamento. Vedere CTX135207. Durante un aggiornamento del database, i servizi del prodotto vengono disabilitati. Durante questo periodo, i controllori non possono mediare nuove connessioni per il sito, quindi occorre pianificare attentamente.

Aggiorna automaticamente il database e il sito

1. Avvia lo Studio appena aggiornato.

2. Indica che desideri avviare automaticamente l'aggiornamento del sito e conferma di essere pronto.

L'aggiornamento del database e del sito procede.

Aggiornare manualmente il database e il sito

1. Avvia lo Studio appena aggiornato.
2. Indica che desideri aggiornare il sito manualmente. La procedura guidata verifica la compatibilità del server licenze e richiede conferma.
3. Conferma di aver eseguito il backup del database.

La procedura guidata genera e visualizza gli script e un elenco di controllo dei passaggi di aggiornamento. Se lo schema di un database non è cambiato dopo l'aggiornamento della versione del prodotto, lo script non viene generato. Ad esempio, se lo schema del database di registrazione non cambia, lo script `UpgradeLoggingDatabase.sql` non viene generato.

4. Eseguire gli script seguenti nell'ordine indicato.
 - `DisableServices.ps1`: L'utente Studio esegue questo script di PowerShell su un controller per disabilitare i servizi del prodotto.
 - `UpgradeSiteDatabase.sql`: L'amministratore del database esegue questo script SQL sul server contenente il database del sito
 - `UpgradeMonitorDatabase.sql`: L'amministratore del database esegue questo script SQL sul server contenente il database Monitor.
 - `UpgradeLoggingDatabase.sql`: L'amministratore del database esegue questo script SQL sul server contenente il database di registrazione della configurazione. Eseguire questo script solo se il database cambia (ad esempio, dopo l'applicazione di un hotfix).
 - `EnableServices.ps1`: L'utente Studio esegue questo script di PowerShell su un controller per abilitare i servizi del prodotto.

Una volta completato l'aggiornamento del database e abilitati i servizi del prodotto, Studio testa automaticamente l'ambiente e la configurazione, quindi genera un report HTML. Se vengono identificati dei problemi, è possibile ripristinare il backup del database. Dopo aver risolto i problemi, puoi aggiornare nuovamente il database.

5. Dopo aver completato le attività della checklist, fare clic su **Termina aggiornamento**.

Passaggio 10: Aggiornare i Delivery Controller rimanenti

Dallo Studio appena aggiornato, seleziona **Citrix Studio nome-sito** nel riquadro di navigazione. Nella scheda **Attività comuni**, seleziona **Aggiorna i Delivery Controller rimanenti**.

Nota:

Per rendere disponibili i Delivery Controller rimanenti **Upgrade**, creare almeno un catalogo macchine e un gruppo di consegna per il sito.

Dopo aver completato l'aggiornamento e confermato il completamento, chiudere e riaprire Studio. Studio potrebbe richiedere un ulteriore aggiornamento del sito per registrare i servizi del Controller sul sito o per creare un ID di zona se non esiste.

Fase 11: Aggiornare i VDA

Importante:

Se stai aggiornando un VDA alla versione 1912 o successiva, consulta [Aggiornamento di VDA alla versione 1912 o successiva](#).

Eeguire il programma di installazione del prodotto sui computer contenenti VDA.

Se hai utilizzato Machine Creation Services e un'immagine master per creare le macchine, vai al tuo host e aggiorna il VDA sull'immagine master. È possibile utilizzare uno qualsiasi degli installatori VDA disponibili.

- Per una guida all'interfaccia grafica, vedere [Installa VDA](#).
- Per la guida alla riga di comando, vedere [Installazione tramite riga di comando](#).

Se hai utilizzato Citrix Provisioning per creare le macchine, consulta la documentazione del prodotto Citrix Provisioning per indicazioni sull'aggiornamento.

Fase 12: Aggiornare i cataloghi delle macchine e i gruppi di consegna

- [Aggiorna i cataloghi che utilizzano macchine con VDA aggiornati](#).
- [Aggiorna i cataloghi che utilizzano macchine con VDA aggiornati](#).
- [Gruppi di distribuzione degli aggiornamenti che utilizzano macchine con VDA aggiornati](#).

Fase 13: Dopo l'aggiornamento

Aggiorna gli altri componenti della tua distribuzione. Per ulteriori informazioni, consultare la seguente documentazione del prodotto:

- [Negozio Front](#)
- [AppDNA](#)
- [Stratificazione delle applicazioni Citrix](#)

- [Pacchetto di ottimizzazione in tempo reale HDX](#)
- [Gestione del profilo](#)
- [Fornitura Citrix](#)
- [Registrazione della sessione](#)
- [Gestione dell'ambiente di lavoro](#)

Se è necessario sostituire il software Microsoft SQL Server Express LocalDB con una versione successiva, vedere Sostituisci SQL Server Express LocalDB.

Aggiornamento Dbschema

Quando si aggiorna la distribuzione, è possibile aggiornare diversi schemi di database. Nella tabella seguente sono elencati gli schemi del database che vengono aggiornati durante il processo:

From/To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203 RTM	2203 CU1	2203 CU2	2203 CU3
7.15 RTM/CU	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 RTM	Config	Site; Config	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU1		Site	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU2			Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU3				Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU4					Site; Config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU5						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU6						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU7						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
2203 RTM							Config	Config	Config
2203 CU1								Config	Config
2203 CU2									Config

Definizione dei termini:

- **Sito:** Datastore del sito. L'aggiornamento Dbschema viene eseguito sul Site Datastore.
- **Monitor:** monitora l'archivio dati. L'aggiornamento Dbschema viene eseguito sul Monitor Datastore.
- **Config:** Tabella di configurazione. Nella tabella Configurazione vengono aggiornate la versione di Desktop Studio, le informazioni sulla licenza o entrambe.
- **Registrazione:** Datastore di registrazione. Viene eseguito l'aggiornamento di Dbschema nel Logging Datastore.

Aggiornare VDA a 2203 o versione successiva

Se il componente Personal vDisk (PvD) è mai stato installato su un VDA, tale VDA non può essere aggiornato alla versione 2203 o successiva. Per utilizzare il nuovo VDA, è necessario disinstallare il VDA corrente e quindi installare il nuovo VDA.

Questa istruzione è valida anche se non hai mai utilizzato PvD.

Ecco come il componente PvD potrebbe essere stato installato nelle versioni precedenti:

- Nell'interfaccia grafica del programma di installazione VDA, PvD era un'opzione nella pagina **Componenti aggiuntivi**.

- Sulla riga di comando, l'opzione `/baseimage` installava PvD. Se hai specificato questa opzione o hai utilizzato uno script che conteneva questa opzione, PvD è stato installato.

Se non sai se il tuo VDA ha installato PvD, esegui il programma di installazione per il nuovo VDA (2203 o successivo) sulla macchina o sull'immagine.

- Se PvD è installato, viene visualizzato un messaggio che indica la presenza di un componente incompatibile.
 - Dall'interfaccia grafica, fare clic su **Annulla** nella pagina contenente il messaggio, quindi confermare che si desidera chiudere il programma di installazione.
 - Dalla CLI, il comando fallisce semplicemente e viene visualizzato il messaggio.
- Se PvD non è installato, l'aggiornamento procede.

Cosa fare

Se il VDA non ha PvD installato, seguire la consueta procedura di aggiornamento.

Se il VDA ha installato PvD:

1. Disinstallare l'attuale VDA.
2. Installare il nuovo VDA.

Se desideri continuare a utilizzare PvD sui tuoi computer Windows 10 (1607 e precedenti, senza aggiornamenti), la versione più recente supportata è VDA 7.15 LTSR.

Nota:

Posso utilizzare Personal vDisk con i desktop Windows 7 in XenApp e XenDesktop 7.15 LTSR?

Citrix ha escluso Personal vDisk (PvD) da XenApp e XenDesktop 7.6 LTSR, annunciati nel gennaio 2016. Inoltre, Citrix ha annunciato l'abbandono della tecnologia PvD e consiglia ai clienti di iniziare a utilizzare Citrix App Layering in futuro. Citrix App Layering (versione 4.4 e successive) è un componente compatibile con XenApp e XenDesktop 7.15 LTSR. Tuttavia, per aiutare i clienti con distribuzioni PvD esistenti su Windows 7 a migrare alla tecnologia Citrix App Layering, Citrix ha deciso di fornire supporto a tempo limitato per le distribuzioni PvD per desktop Windows 7 tramite gli aggiornamenti cumulativi (CU) XenApp e XenDesktop 7.15 LTSR fino al 14 gennaio 2020. Il componente PvD verrà rimosso dalle CU LTSR e non sarà più supportato dopo il 14 gennaio 2020. Inoltre, l'utilizzo di PvD per Windows 7 oltre il 14 gennaio 2020 renderà i siti LTSR non conformi. Inoltre, PvD per Windows 10 continua a essere escluso da 7.15 LTSR. Pertanto, i clienti non dovrebbero utilizzarlo con i loro siti LTSR 7.15.

Rimuovi PvD, AppDisk e host non supportati

Le seguenti tecnologie e tipi di host non sono supportati nelle distribuzioni di Citrix Virtual Apps and Desktops 7 Current Release:

- **vDisk personali (PvD)** per archiviare dati accanto alle VM degli utenti nei cataloghi. La funzionalità del livello di personalizzazione dell'utente ora gestisce la persistenza dell'utente.
- **AppDisk** per la gestione delle applicazioni utilizzate nei Delivery Group.
- **Tipi di host:** Azure Classic, CloudPlatform (il prodotto Citrix originale).
 - Per i tipi di host supportati in questa versione, vedere [Requisiti di sistema](#).
 - Per informazioni su modi alternativi per continuare a utilizzare ARM e AWS, vedere [CTX270373](#).

Se la distribuzione corrente utilizza PvD o AppDisk oppure presenta connessioni a tipi di host non supportati (ad esempio, Microsoft Azure Classic), è possibile eseguire l'aggiornamento alla versione 2006 (o a versioni successive supportate) solo dopo aver rimosso gli elementi che utilizzano tali tecnologie. Se la tua distribuzione attuale utilizza connessioni host cloud pubbliche (ad esempio, AWS), assicurati di disporre della licenza Hybrid Rights prima di effettuare l'aggiornamento. Quando il programma di installazione rileva una o più tecnologie non supportate o connessioni host senza licenza Hybrid Rights, l'aggiornamento si interrompe o si arresta e viene visualizzato un messaggio esplicativo. I registri di installazione contengono dettagli.

Per garantire un aggiornamento riuscito, rivedere e seguire le linee guida applicabili per la rimozione degli elementi non supportati.

- Rimuovi PvD
- Rimuovi AppDisk
- Rimuovi gli elementi host non supportati

Anche se non hai utilizzato PvD o AppDisk nella tua distribuzione, gli MSI correlati potrebbero essere stati inclusi in una precedente installazione o aggiornamento VDA. Prima di poter aggiornare i VDA alla versione 2006 (o a una versione successiva supportata), è necessario rimuovere il software in questione, anche se non lo si è mai utilizzato. Quando si utilizza l'interfaccia grafica, la rimozione può essere effettuata automaticamente oppure è possibile includere opzioni di rimozione quando si utilizza la CLI. Per maggiori dettagli, vedere [Aggiornamento di VDA con componenti PvD o AppDisk](#).

Rimuovi PvD

Un aggiornamento della distribuzione non potrà avere successo finché non si rimuoveranno tutte le macchine configurate per utilizzare PvD. Ciò riguarda cataloghi e gruppi di consegna.

Per rimuovere PvD da gruppi e cataloghi:

1. Da Studio, se un gruppo di consegna contiene macchine da un catalogo che utilizza PvD, [rimuove tali macchine dal gruppo](#).
2. Da Studio, [elimina tutti i cataloghi](#) contenenti macchine che utilizzano PvD.

Aggiornamenti VDA: L'aggiornamento della distribuzione non rileva se i VDA hanno installati i componenti AppDisk o PvD. Tuttavia, gli installatori VDA lo fanno. Per maggiori dettagli, vedere VDA che hanno componenti PvD o AppDisks.

Se si prevede di utilizzare App Layering anziché PvD, consultare [Migrazione di PvD ad App Layering](#) per informazioni sullo spostamento dei dati.

Rimuovi AppDisk

Un aggiornamento della distribuzione non può procedere finché non si rimuovono gli AppDisk da tutti i Delivery Group che li utilizzano e quindi non si rimuovono gli AppDisk stessi.

1. Selezionare **Gruppi di distribuzione** nel riquadro di navigazione dello Studio.
2. Seleziona un gruppo e poi fai clic su **Gestisci AppDisk** nel riquadro Azione.
3. Fare clic sull'azione che rimuove l'AppDisk dal gruppo.
4. Ripetere i passaggi 2 e 3 per ogni Delivery Group che utilizza AppDisk.
5. Selezionare **AppDisks** nel riquadro di navigazione di Studio.
6. Selezionare un AppDisk e fare clic sull'azione che elimina l'AppDisk.
7. Ripetere i passaggi 5 e 6 per ogni AppDisk.

Aggiornamenti VDA: L'aggiornamento della distribuzione non rileva se i VDA hanno installati i componenti AppDisk o PvD. Tuttavia, gli installatori VDA lo fanno. Per maggiori dettagli, vedere VDA che hanno componenti PvD o AppDisks.

Rimuovi gli elementi host non supportati

L'aggiornamento della distribuzione alla versione 2006 (o a una versione successiva supportata) non può essere eseguito se il sito presenta connessioni a tipi di host non supportati, ad esempio Citrix CloudPlatform o Microsoft Azure Classic. Prima di tentare un aggiornamento, completare le seguenti attività.

Da Studio:

- [Elimina tutte le connessioni](#) verso host non supportati.
- Se un gruppo di distribuzione contiene macchine da un catalogo creato con un'immagine master da un host non supportato, [rimuove tali macchine dal gruppo](#).
- [Elimina tutti i cataloghi](#) creati utilizzando un'immagine master da un host non supportato.

VDA che hanno componenti PvD o AppDisks

Se i componenti che abilitano le tecnologie PvD e AppDisks sono installati su un VDA, tale VDA non potrà essere aggiornato finché tali componenti non verranno rimossi.

Nota:

Durante l'aggiornamento alla versione 1912, era necessario disinstallare la VDA corrente e quindi installare la nuova VDA. In questa versione, ti viene chiesto se desideri che Citrix rimuova il componente e poi continui l'aggiornamento.

I componenti AppDisk e PvD potrebbero essere stati installati in versioni precedenti di VDA, anche se non hai mai utilizzato queste tecnologie:

- Interfaccia grafica: negli installer VDA, la pagina **Componenti aggiuntivi** conteneva l'opzione **Citrix AppDisk / Personal vDisk**. La versione 7.15 LTSR e le precedenti versioni 7.x abilitavano questa opzione per impostazione predefinita. Quindi, se hai accettato le impostazioni predefinite (o hai abilitato esplicitamente l'opzione in una qualsiasi versione che la offriva), quel componente è stato installato.
- CLI: specificando l'opzione `/base image` è stato installato il componente.

Cosa fare Se il programma di installazione VDA non rileva i componenti AppDisk o PvD nel VDA attualmente installato, l'aggiornamento procede normalmente.

Se il programma di installazione rileva componenti AppDisk o PvD nel VDA attualmente installato:

- Interfaccia grafica: l'aggiornamento si interrompe. Un messaggio chiede se si desidera che i componenti non supportati vengano rimossi automaticamente. Se fai clic su **OK**, i componenti vengono rimossi automaticamente e l'aggiornamento procede.
- CLI: per evitare errori nel comando, includere le seguenti opzioni nel comando:

```
- /remove_appdisk_ack  
- /remove_pvd_ack
```

Limitazioni

Per gli aggiornamenti si applicano le seguenti limitazioni:

- **Installazione selettiva dei componenti:** Se installi o aggiorni dei componenti alla nuova versione ma scegli di non aggiornare altri componenti (su macchine diverse) che richiedono l'aggiornamento, Studio te lo ricorda. Ad esempio, supponiamo che un aggiornamento includa

nuove versioni del Controller e di Studio. Si aggiorna il Controller ma non si esegue il programma di installazione sul computer in cui è installato Studio. Studio non ti consentirà di continuare a gestire il sito finché non esegui l'aggiornamento.

Non è necessario aggiornare i VDA, ma Citrix consiglia di farlo tutti per poter utilizzare tutte le funzionalità disponibili.

- **Versioni Early Release o Technology Preview:** Non è possibile effettuare l'aggiornamento da una versione Early Release, Technology Preview o preview.
- **Componenti sui sistemi operativi precedenti:** Non è possibile installare gli attuali VDA sui sistemi operativi che non sono più supportati da Microsoft o Citrix. Per ulteriori informazioni, vedere Sistemi operativi precedenti.
- **Ambienti/siti misti:** Se devi continuare a eseguire siti di versioni precedenti e siti di versioni correnti, consulta Considerazioni sugli ambienti misti.
- **Selezione prodotto:** Quando si esegue l'aggiornamento da una versione precedente, non è necessario scegliere o specificare il prodotto (Citrix Virtual Apps o Citrix Virtual Apps and Desktops) impostato durante l'installazione.

Considerazioni sull'ambiente misto

Quando esegui l'aggiornamento, Citrix consiglia di aggiornare tutti i componenti e i VDA in modo da poter accedere a tutte le funzionalità nuove e migliorate nella tua edizione e versione.

Ad esempio, sebbene sia possibile utilizzare gli attuali VDA in distribuzioni contenenti versioni precedenti del Controller, le nuove funzionalità della versione corrente potrebbero non essere disponibili. Possono verificarsi problemi di registrazione VDA anche quando si utilizzano versioni non aggiornate.

In alcuni ambienti potrebbe non essere possibile aggiornare tutti i VDA alla versione più recente. In tal caso, quando si crea un catalogo macchine, è possibile specificare la versione VDA installata sulle macchine. (Questo è chiamato livello funzionale.) Per impostazione predefinita, questa impostazione specifica la versione VDA minima consigliata. Il valore predefinito è sufficiente per la maggior parte delle distribuzioni. Si consiglia di modificare l'impostazione con una versione precedente solo se il catalogo contiene VDA precedenti a quella predefinita. Si sconsiglia di mescolare versioni VDA in un catalogo macchine.

Se un catalogo viene creato con l'impostazione predefinita della versione minima VDA e una o più macchine hanno una versione VDA precedente a quella predefinita, tali macchine non potranno registrarsi con il Controller e non funzioneranno.

Per ulteriori informazioni, vedere [versioni VDA e livelli funzionali](#).

Più siti con diverse versioni

Se l'ambiente contiene siti con diverse versioni del prodotto (ad esempio, un sito XenDesktop 7.18 e un sito Citrix Virtual Apps and Desktops 1909), Citrix consiglia di utilizzare StoreFront per aggregare applicazioni e desktop da diverse versioni del prodotto. Per maggiori dettagli, consultare la documentazione di [StoreFront](#).

In un ambiente misto, continuare a utilizzare le versioni Studio e Director per ogni release, ma assicurarsi che le diverse versioni siano installate su computer separati.

Sistemi operativi precedenti

Supponiamo che tu abbia installato una versione precedente di un componente su un computer che esegua una versione supportata del sistema operativo (SO). Ora, vuoi utilizzare una versione più recente del componente, ma quel sistema operativo non è più supportato per la versione corrente del componente.

Supponiamo, ad esempio, di aver installato un server VDA su un computer Windows Server 2008 R2. Ora vuoi aggiornare il VDA alla versione corrente, ma Windows Server 2008 R2 non è supportato nella versione corrente a cui stai effettuando l'aggiornamento.

Se si tenta di installare o aggiornare un componente su un sistema operativo non più consentito, viene visualizzato un messaggio di errore, ad esempio "Impossibile installarlo su questo sistema operativo".

Queste considerazioni si applicano all'aggiornamento delle versioni Current Release e Long Term Service Release. (Non influisce sull'applicazione di CU a una versione LTSR.)

Segui i link per scoprire quali sistemi operativi sono supportati:

- Citrix Virtual Apps and Desktops (versione corrente):
 - [Delivery Controller, Studio, Direttore, VDA, Server di stampa universale](#)
 - [Servizio di autenticazione federata](#)
 - Per [StoreFront](#), [Self-Service Password Resete](#) [Session Recording](#), vedere l'articolo sui requisiti di sistema per la versione corrente.
- Per gli LTSR, vedere gli elenchi dei componenti per la versione LTSR e CU in uso. (Seleziona la tua versione LTSR dalla pagina principale della documentazione del prodotto [Citrix Virtual Apps and Desktops](#).)

Sistemi operativi non validi

Nella tabella seguente sono elencati i sistemi operativi precedenti che non sono validi per l'installazione/aggiornamento dei componenti nella versione corrente. Indica l'ultima versione valida del

componente supportata per ciascun sistema operativo elencato, nonché la versione del componente al momento in cui l'installazione e l'aggiornamento non sono più validi.

I sistemi operativi nella tabella includono service pack e aggiornamenti.

Sistema operativo	Componente/funzionalità	Ultima versione valida	Installazione/aggiornamento no
Windows 7 LTSR	7 componenti di Windows 7	Windows 7 LTSR	2012
Windows 8	8 componenti di Windows 8	Windows 8 LTSR	2012
Windows Server 2008 R2	Componenti di Windows Server 2008 R2	Windows Server 2008 R2 LTSR	2012
Windows Server 2012	Componenti di Windows Server 2012	Windows Server 2012 LTSR	2012
Windows Server 2012 R2	Componenti di Windows Server 2012 R2	Windows Server 2012 R2 LTSR	2012

Windows XP e Windows Vista non sono validi per alcun componente o tecnologia 7.x.

* Si applica a Delivery Controller, Studio, Director e VDA.

Cosa puoi fare

Hai delle scelte. Puoi:

- Continua con il sistema operativo corrente
- Ripristinare l'immagine o aggiornare la macchina
- Aggiungi nuove macchine e poi rimuovi quelle vecchie

Continua con il sistema operativo corrente Questi metodi sono realizzabili per le VDA. Se desideri continuare a utilizzare computer con il sistema operativo precedente, puoi scegliere una delle seguenti opzioni:

- Continua a utilizzare la versione del componente installata.
- Scarica l'ultima versione valida del componente, quindi aggiorna il componente a quella versione. (Questo presuppone che non sia già installata l'ultima versione valida del componente.)

Ad esempio, su un computer con Windows 7 SP1 è installato un VDA 7.14. L'ultima versione VDA valida sui computer con sistema operativo Windows 7 è XenApp e XenDesktop 7.15 LTSR. Puoi continuare a utilizzare la versione 7.14 oppure scaricare una versione LTSR VDA 7.15 e poi aggiornare la tua versione VDA a quella. Le versioni VDA precedenti funzionano in distribuzioni contenenti Delivery Controller con versioni più recenti. Ad esempio, un VDA LTSR 7.15 può connettersi a un controller Citrix Virtual Apps and Desktops 7 1808.

Ripristinare l'immagine o aggiornare la macchina Questi metodi sono realizzabili per VDA e altre macchine che non hanno componenti principali installati (ad esempio i Delivery Controller). Scegli una delle seguenti opzioni:

- Dopo aver messo fuori servizio la macchina (attivando la modalità di manutenzione e consentendo la chiusura di tutte le sessioni), è possibile ricrearne l'immagine con una versione supportata del sistema operativo Windows e quindi installare la versione più recente del componente.
- Per aggiornare il sistema operativo senza effettuare il reimaging, disinstallare il software Citrix prima di aggiornare il sistema operativo (ciò include gli aggiornamenti interni del sistema operativo). Ad esempio, da Windows 10 versione 1903 a Windows 10 versione 1909). In caso contrario, il software Citrix non sarà supportato. Quindi, installa il nuovo componente.
- Per aggiornare il sistema operativo in una macchina VDA senza effettuare il reimaging, è necessario prima installare la versione VDA supportata dal sistema operativo a cui si sta eseguendo l'aggiornamento oppure aggiornare VDA dopo aver aggiornato il sistema operativo. In caso contrario, il software Citrix non sarà supportato. È possibile eseguire l'aggiornamento alle seguenti versioni minime del sistema operativo quando si esegue un aggiornamento sul posto senza disinstallare VDA:
 - Windows 11 con [2023-07 aggiornamento cumulativo per Windows 11 \(KB5028185\)](#) o versione successiva installato (build 22H2.1992 o successiva).
 - Windows 10 con [2023-07 Dynamic Update per Windows 10 \(KB5028311\)](#) installato.
- Se la versione di Windows a cui si intende effettuare l'aggiornamento non è conforme alle linee guida sopra menzionate, è necessario disinstallare VDA prima di aggiornare il sistema operativo e quindi installare una versione VDA supportata una volta completato l'aggiornamento del sistema operativo.

Aggiungi nuove macchine e poi rimuovi quelle vecchie Questo metodo è fattibile se è necessario aggiornare il sistema operativo su macchine dotate di un Delivery Controller o di un altro componente principale.

Citrix consiglia che tutti i controller di un sito abbiano lo stesso sistema operativo. La seguente sequenza di aggiornamento riduce al minimo l'intervallo in cui diversi controller hanno sistemi operativi diversi.

1. Eseguire uno snapshot di tutti i Delivery Controller nel sito, quindi eseguire il backup del database del sito.
2. Installare nuovi Delivery Controller su server puliti con sistemi operativi supportati. Ad esempio, installare un controller su due macchine Windows Server 2016.
3. Aggiungere i nuovi controller al sito.
4. Rimuovere i controller in esecuzione su sistemi operativi non validi per la versione corrente. Ad esempio, rimuovere due controller su due macchine Windows Server 2008 R2. Seguire i consigli per la rimozione dei controller in [Delivery Controllers](#).

Preparazione

Prima di iniziare un aggiornamento, rivedere le seguenti informazioni e completare le attività necessarie.

Nota:

Sebbene l'aggiornamento dei VDA avvenga più avanti nella sequenza di aggiornamento, è consigliabile scegliere un programma di installazione e rivedere la procedura prima di avviare l'aggiornamento, in modo da sapere cosa aspettarsi.

Scegli un programma di installazione e un'interfaccia

Per aggiornare i componenti, utilizzare il programma di installazione completo del prodotto dall'ISO. È possibile aggiornare i VDA utilizzando il programma di installazione completo del prodotto o uno dei programmi di installazione VDA autonomi. Tutti i programmi di installazione offrono interfacce grafiche e a riga di comando.

Per ulteriori informazioni, vedere [Programmi di installazione](#).

Specifiche di installazione: Dopo aver completato il lavoro di preparazione e quando sei pronto per avviare il programma di installazione, l'articolo di installazione ti mostra cosa vedrai (se stai utilizzando l'interfaccia grafica) o cosa digitare (se stai utilizzando l'interfaccia della riga di comando).

- [Installa/aggiorna i componenti principali utilizzando l'interfaccia grafica](#)
- [Installa/aggiorna i componenti principali tramite la riga di comando](#)
- [Installa/aggiorna i VDA utilizzando l'interfaccia grafica](#)
- [Installa/aggiorna i VDA tramite la riga di comando](#)

Se in origine hai installato un VDA a sessione singola con il programma di installazione `VDAWorkstationCoreSetup.exe`, Citrix consiglia di utilizzare tale programma di installazione per aggiornarlo. Se si utilizza il programma di installazione VDA completo del prodotto o il programma di installazione `VDAWorkstationSetup.exe` per aggiornare VDA, i componenti originariamente esclusi potrebbero essere installati, a meno che non vengano espressamente omessi/esclusi dall'aggiornamento.

Quando si aggiorna un VDA alla versione corrente, durante il processo di aggiornamento si verifica un riavvio della macchina. (Questo requisito è stato introdotto con la versione 7.17.) Non è possibile evitarlo. L'aggiornamento riprende automaticamente dopo il riavvio (a meno che non si specifichi `/noresume` sulla riga di comando).

Azioni del database

Eseguire il backup dei database del sito, del monitoraggio e della registrazione della configurazione. Seguire le istruzioni in [CTX135207](#). Se dopo l'aggiornamento vengono rilevati problemi, è possibile ripristinare il backup.

Per informazioni sull'aggiornamento delle versioni di SQL Server non più supportate, vedere [Controllo della versione di SQL Server](#). (Si riferisce al server SQL utilizzato per i database di registrazione del sito, del monitor e della configurazione.)

Microsoft SQL Server Express LocalDB viene installato automaticamente, per l'utilizzo con Local Host Cache. Se è necessario sostituire una versione precedente, la nuova versione deve essere SQL Server Express LocalDB 2019. Per informazioni dettagliate sulla sostituzione di SQL Server Express LocalDB con la nuova versione dopo l'aggiornamento dei componenti e del sito, vedere [Sostituisci SQL Server Express LocalDB](#).

Assicurati che la tua licenza Citrix sia aggiornata

Per una panoramica completa sulla gestione delle licenze Citrix, vedere [Attivare, aggiornare e gestire le licenze Citrix](#).

È possibile utilizzare il programma di installazione completo del prodotto per aggiornare License Server. In alternativa, è possibile scaricare e aggiornare separatamente i componenti della licenza. Vedere [Aggiorna](#).

Prima di effettuare l'aggiornamento, assicurati che la data del tuo Customer Success Services/Software Maintenance/Subscription Advantage sia valida per la nuova versione del prodotto. La data deve essere almeno 2021.11.15.

Assicurati che il tuo Citrix License Server sia compatibile

Assicurati che il tuo Citrix License Server sia compatibile con la nuova versione. Ci sono due modi per farlo:

- Prima di aggiornare qualsiasi altro componente Citrix, eseguire il programma di installazione [XenDesktopServerSetup.exe](#) dal layout ISO sulla macchina contenente un Delivery Con-

troller. Se si verificano problemi di incompatibilità, il programma di installazione li segnala, consigliando i passaggi per risolverli.

- Dalla directory `XenDesktop Setup` sul supporto di installazione, eseguire il comando: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. Il display indica se il License Server è compatibile. Se il server delle licenze non è compatibile, aggiornarlo.

Eseguire il backup di tutte le modifiche di StoreFront

Prima di iniziare un aggiornamento, se hai apportato modifiche ai file in `C:\inetpub\wwwroot\Citrix\%StoreName%\App_Data`, come `default.ica` e `usernamepassword.tfrm`, esegui il backup per ogni archivio. Dopo l'aggiornamento potrai ripristinarli per ripristinare le modifiche.

Chiudere applicazioni e console

Prima di avviare un aggiornamento, chiudere tutti i programmi che potrebbero potenzialmente causare blocchi di file, tra cui le console di amministrazione e le sessioni di PowerShell.

Riavviando il computer si garantisce che tutti i blocchi dei file vengano rimossi e che non vi siano aggiornamenti di Windows in sospeso.

Prima di avviare un aggiornamento, arrestare e disabilitare tutti i servizi di monitoraggio di terze parti.

Assicurati di avere le autorizzazioni appropriate

Oltre a essere un utente di dominio, devi essere un amministratore locale sul computer su cui stai aggiornando i componenti del prodotto.

Il database del sito e il sito stesso possono essere aggiornati automaticamente o manualmente. Per un aggiornamento automatico del database, le autorizzazioni dell'utente Studio devono includere la possibilità di aggiornare lo schema del database SQL Server (ad esempio, il ruolo del database `db_securityadmin` o `db_owner`). Per maggiori dettagli, vedere [Database](#).

Se l'utente Studio non dispone di tali autorizzazioni, l'avvio di un aggiornamento manuale del database genera degli script. L'utente Studio esegue alcuni degli script da Studio. L'amministratore del database esegue altri script, utilizzando uno strumento come SQL Server Management Studio.

Altri compiti di preparazione

- Eseguire il backup dei modelli e aggiornare gli hypervisor, se necessario
- Completare tutte le altre attività preparatorie previste dal piano di continuità aziendale.

Prove preliminari in loco

Quando si aggiornano i Delivery Controller e un sito, vengono eseguiti test preliminari del sito prima che abbia inizio l'aggiornamento vero e proprio. Questi test verificano:

- Il database del sito è raggiungibile ed è stato sottoposto a backup
- Le connessioni ai servizi Citrix essenziali funzionano correttamente
- L'indirizzo del server di licenza Citrix è disponibile
- È possibile raggiungere il database di registrazione della configurazione
- Se vuoi aggiungere connessioni host cloud pubbliche (ad esempio, AWS), assicurati di disporre della licenza Hybrid Rights. In caso contrario, il test preliminare del sito si interrompe o si arresta e viene visualizzato un messaggio esplicativo.

Dopo aver eseguito i test, è possibile visualizzare un report dei risultati. È quindi possibile correggere eventuali problemi rilevati ed eseguire nuovamente i test. La mancata esecuzione dei test preliminari del sito e la successiva risoluzione degli eventuali problemi possono avere ripercussioni sul funzionamento del sito.

Il report contenente i risultati del test è un file HTML ([PreliminarySiteTestResult.html](#)) nella stessa directory dei log di installazione. Se il file non esiste, viene creato. Se il file esiste, il suo contenuto viene sovrascritto.

Eseguire i test

- Quando si utilizza l'interfaccia grafica del programma di installazione per l'aggiornamento, la procedura guidata include una pagina in cui è possibile avviare i test e quindi visualizzare il report. Dopo aver eseguito i test, aver visualizzato il report e risolto gli eventuali problemi rilevati, è possibile rieseguire i test. Una volta completati correttamente i test, fare clic su **Avanti** per continuare con la procedura guidata.
- Quando si utilizza l'interfaccia della riga di comando per l'aggiornamento, i test vengono eseguiti automaticamente. Per impostazione predefinita, se un test fallisce, l'aggiornamento non viene eseguito. Dopo aver visualizzato il report e risolto i problemi, eseguire nuovamente il comando.

Citrix consiglia di eseguire sempre i test preliminari del sito e di risolvere eventuali problemi prima di continuare con l'aggiornamento del controller e del sito. Il potenziale vantaggio vale ampiamente i pochi minuti dedicati all'esecuzione dei test. Tuttavia, è possibile ignorare questa azione consigliata.

- Quando si esegue l'aggiornamento tramite l'interfaccia grafica, è possibile scegliere di saltare i test e continuare con l'aggiornamento.

- Quando si esegue l'aggiornamento dalla riga di comando, non è possibile saltare i test. Per impostazione predefinita, un test del sito non riuscito determina il fallimento del programma di installazione, senza eseguire l'aggiornamento. Nella maggior parte dei casi, se si include l'opzione `/ignore_site_test_failure`, tutti gli errori dei test vengono ignorati e l'aggiornamento procede. (Vedere Controllo della versione di SQL Server per le eccezioni.)

Quando si aggiornano più controller

Quando si avvia un aggiornamento su un controller e poi si avvia un aggiornamento di un altro controller nello stesso sito (prima del completamento del primo aggiornamento):

- Se i test preliminari del sito sono stati completati sul primo Controller, la pagina dei test preliminari del sito non viene visualizzata nella procedura guidata sull'altro Controller.
- Se i test sul primo Controller sono in corso quando si avvia l'aggiornamento sull'altro Controller, la pagina dei test del sito viene visualizzata nella procedura guidata sull'altro Controller. Tuttavia, se i test sul primo Controller terminano, vengono conservati solo i risultati dei test del primo Controller.

Errori nei test non correlati allo stato del sito

- Se i test preliminari del sito falliscono a causa di memoria insufficiente, rendere disponibile più memoria e quindi eseguire nuovamente i test.
- Se si dispone dell'autorizzazione per l'aggiornamento, ma non si eseguono test del sito, i test preliminari del sito falliscono. Per risolvere questo problema, eseguire nuovamente il programma di installazione con un account utente che disponga dell'autorizzazione per eseguire i test.

Controllo della versione di SQL Server

Per una distribuzione corretta di Citrix Virtual Apps and Desktops è necessaria una versione supportata di Microsoft SQL Server per i database di registrazione del sito, del monitor e della configurazione. L'aggiornamento di una distribuzione Citrix con una versione di SQL Server non più supportata può causare problemi di funzionalità e il sito non sarà più supportato.

Per sapere quali versioni di SQL Server sono supportate dalla versione di Citrix a cui stai effettuando l'aggiornamento, consulta l'articolo [Requisiti di sistema](#) per quella versione.

Durante l'aggiornamento di un controller, il programma di installazione di Citrix controlla la versione di SQL Server attualmente installata e utilizzata per i database di registrazione del sito, del monitor e della configurazione.

- Se il controllo determina che la versione di SQL Server attualmente installata non è una versione supportata nella versione di Citrix a cui si sta eseguendo l'aggiornamento:
 - Interfaccia grafica: l'aggiornamento si interrompe con un messaggio. Fare clic su **Ho capito** e quindi fare clic su **Annulla** per chiudere il programma di installazione di Citrix. (Non è possibile continuare con l'aggiornamento.)
 - Interfaccia della riga di comando: il comando fallisce (anche se hai incluso l'opzione /`ignore_db_check_failure` con il comando).

Aggiornare la versione di SQL Server, quindi riavviare l'aggiornamento di Citrix.

- Se il controllo non riesce a determinare quale versione di SQL Server è attualmente installata, controlla se la versione attualmente installata è supportata nella versione a cui stai effettuando l'aggiornamento ([Requisiti di sistema](#)).
 - Interfaccia grafica: l'aggiornamento si interrompe con un messaggio.
 - * Se la versione di SQL Server attualmente installata è supportata, fare clic su **Ho capito** per chiudere il messaggio, quindi fare clic su **Avanti** per continuare con l'aggiornamento di Citrix.
 - * Se la versione di SQL Server attualmente installata non è supportata, fare clic su **Ho capito** per chiudere il messaggio, quindi fare clic su **Annulla** per terminare l'aggiornamento di Citrix. Aggiorna SQL Server a una versione supportata, quindi riavvia l'aggiornamento di Citrix.
 - Interfaccia della riga di comando: il comando fallisce e viene visualizzato un messaggio. Dopo aver chiuso il messaggio:
 - * Se la versione di SQL Server attualmente installata è supportata, eseguire nuovamente il comando con l'opzione /`ignore_db_check_failure`.
 - * Se la versione di SQL Server attualmente installata non è supportata, aggiornare SQL Server a una versione supportata. Eseguire nuovamente il comando per avviare l'aggiornamento di Citrix.

Aggiornamento di SQL Server

Se si attivano nuovi server SQL Server e si migra il database del sito, è necessario aggiornare le stringhe di connessione.

Se il sito utilizza attualmente SQL Server Express per il database del sito (che Citrix ha installato automaticamente durante la creazione del sito):

1. Installare la versione più recente di SQL Server Express.
2. Scollegare il database.

3. Collegare il database al nuovo SQL Server Express.
4. Migrare le stringhe di connessione.

Per ulteriori informazioni, vedere [Configurazione delle stringhe di connessione](#) e la documentazione del prodotto Microsoft SQL Server.

Sostituisci SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB è una funzionalità di SQL Server Express che Local Host Cache utilizza in modo autonomo. La cache host locale non richiede alcun componente di SQL Server Express diverso da SQL Server Express LocalDB.

Se hai installato una versione di Delivery Controller precedente alla 1912 e poi aggiorni la distribuzione alla versione 1912 o successiva, Citrix non aggiornerà automaticamente la versione di SQL Server Express LocalDB. Perché no? Perché potresti avere componenti non Citrix che si basano su SQL Server Express LocalDB. Se sono presenti componenti non Citrix che utilizzano SQL Server Express LocalDB, assicurarsi che l'aggiornamento di SQL Server Express LocalDB non interrompa tali componenti. Per aggiornare (sostituire) la versione SQL Server Express LocalDB, seguire le istruzioni riportate in questa sezione.

- **Quando si aggiornano i Delivery Controller alle versioni 2402 LTSR o successive di Citrix Virtual Apps and Desktops:** la versione supportata è SQL Server Express LocalDB 2022.

Nota:

Le versioni 2017, 2019 e 2022 di SQL Server Express LocalDB sono tutte compatibili tra loro. Pertanto, non è obbligatorio aggiornare SQL Server Express LocalDB affinché LHC funzioni.

Cosa ti serve:

- Supporto di installazione di Citrix Virtual Apps and Desktops contenente una copia di Microsoft SQL Server Express LocalDB 2022.
- Lo strumento [PsExec](#) dalla casella degli strumenti Sysinternals di Windows che puoi scaricare da Microsoft. Vedere il documento Microsoft [PsExec v2.43](#).

Procedura:

1. Completa l'aggiornamento dei componenti, dei database e del sito di Citrix Virtual Apps and Desktops. (Tali aggiornamenti del database interessano i database del sito, del monitoraggio e della registrazione della configurazione. Non influiscono sul database Local Host Cache che utilizza SQL Server Express LocalDB.)
2. Accedere al Delivery Controller utilizzato per ricreare il database LHC.
3. Su quel Delivery Controller, scarica [PsExec](#) da Microsoft e posizionalo in `C:\Temp`.

- Arrestare il servizio Citrix High Availability.
- Aprire il prompt dei comandi, andare su `C:\Temp`, quindi eseguire il seguente comando per elevare il prompt dei comandi con l'account del servizio di rete:

```
1 psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
```

- Esegui `whoami` per confermare che il prompt dei comandi è in esecuzione come account del servizio di rete. Si dovrebbe ottenere il seguente output: `nt authority\networkservice`.
- Utilizzare il prompt dei comandi per passare all'istanza SQL LocalDB:

- Se si esegue l'aggiornamento da SQL LocalDB 2014:

```
1 cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

- Se si esegue l'aggiornamento da SQL LocalDB 2017:

```
1 cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
```

- Se si esegue l'aggiornamento da SQL LocalDB 2019:

```
1 cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

- Arresta ed elimina l'istanza SQL LocalDB: `CitrixHA`.

```
1 SqlLocalDB stop CitrixHA
2
3 SqlLocalDB delete CitrixHA
```

- Rimuovere i file correlati in `C:\Windows\ServiceProfiles\NetworkService`.

```
1 HADatabaseName.*
2 HADatabaseName_log.*
3 HAImportDatabaseName.* (if exists)
4 HAImportDatabaseName_log.* (if exists)
```

- Disinstallare SQL LocalDB SQL Server Express esistente dal server utilizzando la funzionalità di Windows per la rimozione dei programmi.
- Installa SQL Server Express LocalDB 2022. Nella cartella **Support > SQLLocalDB** sul supporto di installazione di Citrix Virtual Apps and Desktops, fare doppio clic su `sqllocaldb.msi`. Potrebbe essere richiesto un riavvio per completare l'installazione. Il nuovo SQL LocalDB risiede in `C:\Programmi\Microsoft SQL Server\160\Tools\Binn`.
- Avviare il servizio Citrix High Availability sul Delivery Controller in cui è stata disinstallata la vecchia versione di SQL LocalDB.
- Nel prompt dei comandi, esegui `SqlLocalDB i` per confermare se `CitrixHA` è stato creato di nuovo oppure no.

14. Ripetere i passaggi sui Delivery Controller rimanenti.
15. Assicurarsi che il database della cache host locale venga creato su ciascun Delivery Controller. Ciò conferma che, se necessario, il servizio di alta disponibilità (broker secondario) può subentrare.
 - a) Sul server Controller, passare a `C:\Windows\ServiceProfiles\NetworkService`.
 - b) Verificare che `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` siano stati creati.

Secure HDX (anteprima)

November 5, 2024

Secure HDX è una soluzione ALE (Application Level Encryption) che impedisce a qualsiasi elemento di rete nel percorso del traffico di ispezionare il traffico HDX. Ciò è possibile grazie alla crittografia end-to-end (E2EE) a livello applicativo tra l'app Citrix Workspace (client) e il VDA (host della sessione) mediante l'uso della crittografia AES-256-GCM.

Importante:

Secure HDX è attualmente in anteprima. Questa funzionalità è fornita senza supporto e non è ancora consigliata per l'uso in ambienti di produzione. Per inviare feedback o segnalare problemi, utilizzare [questo modulo](#).

Requisiti di sistema

L'elenco seguente illustra i requisiti di sistema per l'utilizzo di Secure HDX.

- Piano di controllo
 - Citrix DaaS
 - Citrix Virtual Apps and Desktops 2402 o versioni successive
- Host della sessione
 - Sistema operativo
 - * Finestre 10 22H2
 - * Windows 11 22H2 o successivo
 - * Windows Server 2019 o versione successiva
 - Virtual Delivery Agent (VDA)

- ★ Windows: versione 2402 o successiva
- ★ Linux: versione 2407 o successiva
- App Workspace
 - Windows: versione 2402 o successiva
 - Linux: versione 2408 o successiva
 - Mac: versione 2409 o successiva
 - Chrome OS: versione 2409 o successiva
 - HTML5: versione 2408 o successiva
- Livello di accesso
 - Spazio di lavoro Citrix
 - Citrix StoreFront 2402 o successivo

Configurazione

Per impostazione predefinita, Secure HDX è disabilitato. È possibile configurare questa funzionalità utilizzando l'impostazione Secure HDX nella policy Citrix:

HDX sicuro: definisce se abilitare la funzionalità per tutte le sessioni, solo per le connessioni dirette oppure disabilitarla.

Considerazioni

Di seguito sono riportate alcune considerazioni sull'utilizzo di Secure HDX:

- Se un utente tenta di connettersi a un host di sessione con Secure HDX abilitato utilizzando un client che non supporta la funzionalità, la connessione verrà negata.
- La continuità del servizio non è attualmente supportata con Secure HDX. Se hai abilitato Service Continuity nel tuo ambiente Citrix Cloud, non potrai accedere a nessuna sessione host che abbia abilitato Secure HDX in caso di interruzione del servizio Cloud.
- Se si utilizza HDX Insight, tenere presente che l'utilizzo di Secure HDX impedisce la raccolta dei dati di HDX Insight poiché NetScaler non è in grado di ispezionare il traffico HDX crittografato. Se devi utilizzare HDX Insight, puoi impostare Secure HDX in modo che sia abilitato solo per le connessioni dirette.
- Se si utilizza SmartControl, tenere presente che l'utilizzo di Secure HDX impedisce il funzionamento di SmartControl poiché NetScaler non è in grado di ispezionare il traffico HDX crittografato. Se devi utilizzare SmartControl, puoi impostare Secure HDX in modo che sia abilitato solo per le connessioni dirette.

- Multi-Stream ICA non è supportato quando Secure HDX è abilitato.
- Se utilizzi soluzioni di terze parti che si basano sull'ispezione del traffico HDX, queste non funzioneranno più se abiliti Secure HDX, poiché il traffico HDX è crittografato.
- Se hai abilitato Secure ICA sui gruppi di distribuzione su cui desideri abilitare Secure HDX, devi prima disabilitare Secure ICA (Modifica impostazioni utente gruppo di distribuzione >).

Risoluzione dei problemi

Per confermare che Secure HDX è attivo, è possibile utilizzare l'utilità `ctxsession.exe` sulla macchina VDA.

Per utilizzare l'utilità `CtxSession.exe`, aprire un prompt dei comandi o PowerShell all'interno della sessione ed eseguire `ctxsession.exe -v`. Se è in uso Secure HDX, ICA Encryption visualizza `SecureHDX AES-256 GCM`.

```
PS C:\Users\ > ctxsession -v
Session Id 1:
Transport Protocols:  UDP -> DTLS -> CGP -> ICA
Local Address:         :55000
Remote Address:       :65469
Client Address:       :53637
Security Protocol:    DTLS 1.2
Security Cipher:      256 bit AES
Cipher Strength:      256 bits
ICA Encryption:       SecureHDX AES-256 GCM
Rendezvous Version:  None
HDX Direct State:    Connected - External
Reducer Version:     4.0

EDT Reliable Statistics:
Bandwidth 94.516 Mbps, RTT 34.538 ms, EDT MTU: 1480

EDT Unreliable Statistics:
Bandwidth 7.544 Kbps, RTT 1 us, EDT MTU: 1480

EDT Reliable Basic FEC Statistics:
Bandwidth 92.090 Mbps, RTT 7.980 ms, EDT MTU: 1480

ICA Statistics:
SentBandwidth (bps) = 4968
HDX Latency = 31
IcaBufferLength = 1436
```

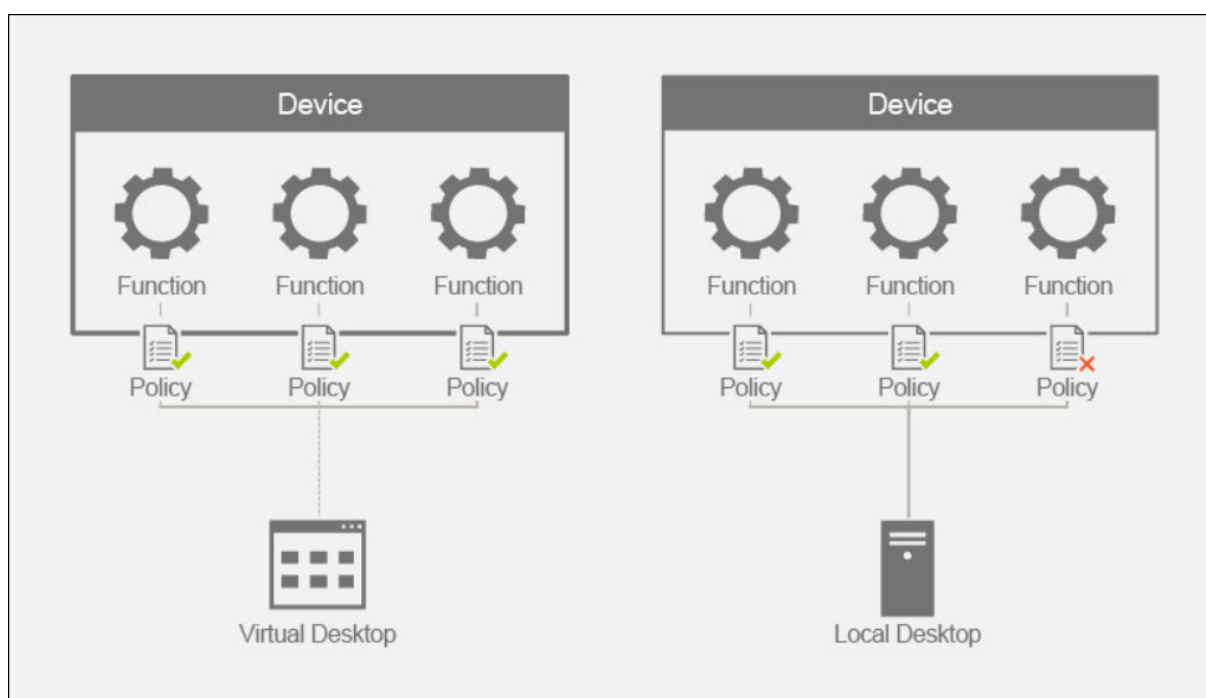
Quando Secure HDX non viene abilitato nella sessione

- Assicurarsi che la versione VDA in uso supporti la funzionalità in base ai requisiti di sistema.
- Verificare di avere applicato un criterio al VDA che abiliti Secure HDX e che non vi siano altri criteri con priorità più alta che disabilitano la funzionalità.
- Se il dispositivo client si connette tramite NetScaler Gateway o Gateway Service, assicurarsi che Secure HDX non sia impostato su “Solo connessioni dirette”.
- Se l'host della sessione era già in esecuzione quando hai configurato Secure HDX, riavvia il computer per assicurarti che le modifiche abbiano effetto.

Dispositivi compositi e divisione dei dispositivi

November 5, 2024

Un dispositivo USB composito è un singolo dispositivo che funziona come più dispositivi USB indipendenti collegati a un computer. Ha un unico connettore USB ma può esporre più interfacce al computer, ognuna con il proprio set di funzionalità. Quando un utente collega un dispositivo USB composito, il dispositivo host verifica tutte le funzioni (interfacce) rispetto a ciascuna regola dei criteri. Se la prima corrispondenza per una funzione (interfaccia) è una regola Deny, la regola viene considerata definitiva per il dispositivo composito e il dispositivo viene negato. Se la prima corrispondenza per una funzione (interfaccia) è una regola Consenti, il dispositivo host continua a far corrispondere le regole alla funzione successiva (interfaccia). Il dispositivo composito è consentito se nessuna funzione (interfaccia) è negata da una regola politica. Se la corrispondenza definitiva per il dispositivo composito è una regola di negazione, il dispositivo è disponibile solo per il desktop locale, altrimenti il dispositivo è remoto sul desktop virtuale. Se non viene trovata alcuna corrispondenza, vengono utilizzate regole predefinite.



Possiamo suddividere il dispositivo composito utilizzando le regole appropriate nella policy Device redirection rules (Versione 2) per consentire solo funzionalità specifiche di un dispositivo composito. Ad esempio, potremmo voler utilizzare solo le funzioni HID di una chiave FIDO2 ma non la funzionalità smartcard. In tal caso, stabiliremo le regole come illustrato di seguito:

1. Connessione: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 consentiva le funzioni FIDO2 HID.

2. Nega: VID=1050 PID=0407 split=01 intf=02 # Funzione smartcard Yubikey serie 5 bloccata.

Mancia:

Quando si creano nuove regole di policy, fare riferimento ai codici di classe USB , disponibili sul sito Web USB.

Configurazione di un signature pad

1. Installare il driver di dispositivo appropriato sull'host VDA.
2. Abilitare l'impostazione del criterio di reindirizzamento del dispositivo USB client in Citrix Web Studio.

1

Modifica l'impostazione della policy **Client USB Device Rules (Version 2)**.

```
1 1. Imposta le informazioni **VID** e **PID** per il signature pad che deve essere reindirizzato e fai clic su **Salva**. Ad esempio: **Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
```

1

Modificare l'impostazione dei criteri **Regole di ottimizzazione dei dispositivi USB client**.

```
1 1. Imposta la modalità insieme ad altre informazioni sul dispositivo. Ad esempio: Mode=00000004 VID=06A8 PID=0057 class=03 #Input dispositivo funzionante in modalità di acquisizione
```

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB esistenti**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB appena arrivati**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

Una volta configurate queste impostazioni, i successivi avvii delle sessioni comporteranno il reindirizzamento automatico del dispositivo e non richiederanno alcuna azione aggiuntiva da parte dell'utente finale.

Nota:

Sostituisci il VID e il PID con il VID e il PID effettivi del dispositivo da reindirizzare.

Configurazione della tastiera Bloomberg tramite reindirizzamento USB

1. Abilitare l'impostazione del criterio **Consenti la connessione automatica dei dispositivi USB esistenti** in Citrix Web Studio.

1

Le tastiere Bloomberg 5 sono impostate di default nelle regole di reindirizzamento dei dispositivi USB del client (**versione 2**) e non è necessaria alcuna azione aggiuntiva da parte dell'amministratore.

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB esistenti**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB appena arrivati**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

Una volta configurate queste impostazioni, le chiavi Bloomberg verranno presentate automaticamente nelle sessioni HDX successive e non richiederanno alcuna azione aggiuntiva da parte dell'utente finale.

Configurazione di una chiave FIDO2 tramite reindirizzamento USB

Citrix consiglia di utilizzare il reindirizzamento FIDO2 per l'utilizzo delle chiavi FIDO2 nelle sessioni HDX. Tuttavia, potrebbero esserci situazioni in cui è necessario reindirizzare le chiavi FIDO2 utilizzando invece il reindirizzamento USB. Tra questi rientrano gli scenari in cui il reindirizzamento FIDO2

non è disponibile perché la funzionalità non è supportata dal client, dal VDA o dal sistema operativo (ad esempio Windows Server 2016).

Ci possono essere anche situazioni in cui la chiave ha più modalità abilitate, ma si desidera consentire solo un sottoinsieme di quelle nelle sessioni HDX. Ad esempio, potresti voler consentire FIDO2 e OTP, ma bloccare la smart card.

I passaggi seguenti illustrano come configurare una chiave FIDO2 utilizzando il reindirizzamento USB (Yubikey vid=1050, pid=0407).

1. Abilitare l'impostazione del criterio di reindirizzamento del dispositivo USB client **in Citrix Web Studio**.

1

Modifica l'impostazione dei criteri per le regole di reindirizzamento dei dispositivi USB del client (versione 2).

```
1 1. Imposta le informazioni **VID** e **PID** , nonché la
   configurazione del dispositivo diviso per la chiave FIDO2 da
   reindirizzare nella sessione e fai clic su **Salva**.
2
3 1. **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #
   Yubikey series 5 consentiva le funzioni FIDO2 HID.
4
5 1. **Nega**: VID=1050 PID=0407 split=01 intf=02 # Funzione smartcard
   Yubikey serie 5 bloccata.
```

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB esistenti**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB appena arrivati**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

Una volta configurate queste impostazioni, le tastiere FIDO2 verranno presentate automaticamente nelle sessioni HDX successive e non richiederanno alcuna azione aggiuntiva da parte dell'utente finale.

Configurazione di un mouse 3D tramite reindirizzamento USB

Oggi, i driver 3DConnexion Space Mouse sono supportati solo sui sistemi operativi delle workstation (Win 10 e Win11). Non funzionano su sistemi operativi server. Di seguito sono riportati i passaggi per configurare uno SpaceMouse Enterprise su un sistema operativo workstation (vid=046D, PID=C016).

1. Installare l'ultimo driver [per Windows](#) sull'host VDA.
2. Abilitare l'impostazione del criterio di reindirizzamento del dispositivo USB client **in Citrix Web Studio**.

1

Modifica l'impostazione dei criteri per le regole di reindirizzamento dei dispositivi USB del client (versione 2).

```
1 1. Imposta le informazioni **VID** e **PID** per il signature pad che deve essere reindirizzato e fai clic su **Salva**. Ad esempio: **Connect**: VID=046D PID=C016 #SpaceMouse Enterprise
```

1

Modificare l'impostazione dei criteri **Regole di ottimizzazione dei dispositivi USB client**.

```
1 1. Imposta la modalità insieme ad altre informazioni sul dispositivo. Ad esempio: Mode=00000004 VID=046D PID=C016 class=03 Dispositivo # Input funzionante in modalità di acquisizione
```

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB esistenti**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB appena arrivati**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

Configurazione di due o più dispositivi tramite reindirizzamento USB con regole di dispositivo diverse

È possibile reindirizzare più dispositivi all'interno della sessione HDX con regole del dispositivo diverse. Un amministratore potrebbe voler reindirizzare automaticamente un dispositivo fornendo al contempo un'opzione all'utente finale per reindirizzare l'altro dispositivo. Di seguito sono riportati i passaggi per configurare due dispositivi con regole diverse.

1. Abilitare l'impostazione del criterio **di reindirizzamento del dispositivo USB client in Citrix Web Studio**.

1

Modifica l'impostazione della policy **Client USB Device Rules (Version 2)**.

```
1 1. Aggiungi le informazioni VID e PID dei due dispositivi da
   reindirizzare con la regola del dispositivo appropriata nella
   sessione e fai clic su Salva.
2
3 1. Consenti: VID=0911 PID=0C1C #Phillips microfono vocale.
4
5 1. Connect: VID=06A8 PID=0043 class=03 # Tampone per firme HSB
   Topaz
```

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB esistenti**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

1

Modifica l'impostazione dei criteri **Consenti la connessione automatica dei dispositivi USB appena arrivati**.

1

Deseleziona la casella di controllo **Usa il valore predefinito** e seleziona **Reindirizza automaticamente i dispositivi USB disponibili** dal menu a discesa e fai clic su **Salva**.

Una volta configurate queste impostazioni, il signature pad Topaz HSB verrà presentato automaticamente nelle sessioni HDX successive e non richiederà alcuna azione aggiuntiva da parte dell'utente finale. Il microfono vocale Phillips, invece, richiederà all'utente finale di abilitare il reindirizzamento in Connection Center o nella scheda Dispositivi di CDViewer.

Configurazione del reindirizzamento USB legacy

November 5, 2024

Se stai usando componenti precedenti alla versione 2212 o se stai usando CWA per Linux, segui questa guida per configurare il reindirizzamento USB nel tuo ambiente.

Abilitazione del reindirizzamento USB generico

1. Aprite **Citrix Web Studio policies** e fate clic sulla scheda **Policies**.
2. Fai clic su **Crea policy** ed espandi le policy **ICA > USB Devices**.
3. Modifica la politica di reindirizzamento del dispositivo USB del client **.
4. Seleziona **Allowed** e fai clic su **Save**.

Creazione di regole di policy di reindirizzamento USB

Quando l'utente tenta di reindirizzare un dispositivo USB a Virtual Desktop, viene confrontato a turno con ciascuna regola della politica USB fino a quando non viene trovata una corrispondenza. La prima partita per qualsiasi dispositivo è considerata definitiva. Se la prima corrispondenza è una regola Consenti, il dispositivo corrispondente può essere reindirizzato al desktop virtuale. Se la prima corrispondenza è una regola Nega, il dispositivo corrispondente è disponibile solo nel desktop locale. Se non viene trovata alcuna corrispondenza, vengono utilizzate regole predefinite.

Impostazione della politica sul DDC:

1. Aprite **Citrix Web Studio policies** e fate clic sulla scheda **Policies**.
2. Fai clic su **Crea policy** ed espandi le policy **ICA > USB Devices**.
3. Modifica le regole di reindirizzamento del dispositivo USB del client **.
4. Imposta il valore in base agli esempi forniti nella descrizione per ogni dispositivo USB che deve essere reindirizzato e fai clic su Salva. Ad esempio: Consenti: VID=056A PID=00A4 #STU-430
Nega: Classe=08 sottoclasse=05 # Archiviazione di massa

Nota:

Se un amministratore Citrix seleziona Usa valore predefinito e fa clic su Salva, le regole predefinite si trovano nel seguente registro del VDA.

Attenzione!:

Fai riferimento al Disclaimer alla fine di questo articolo prima di utilizzare l'Editor del Registro di sistema. `HKLM\ SOFTWARE\ Wow6432 Node\ Citrix\ Portica\`

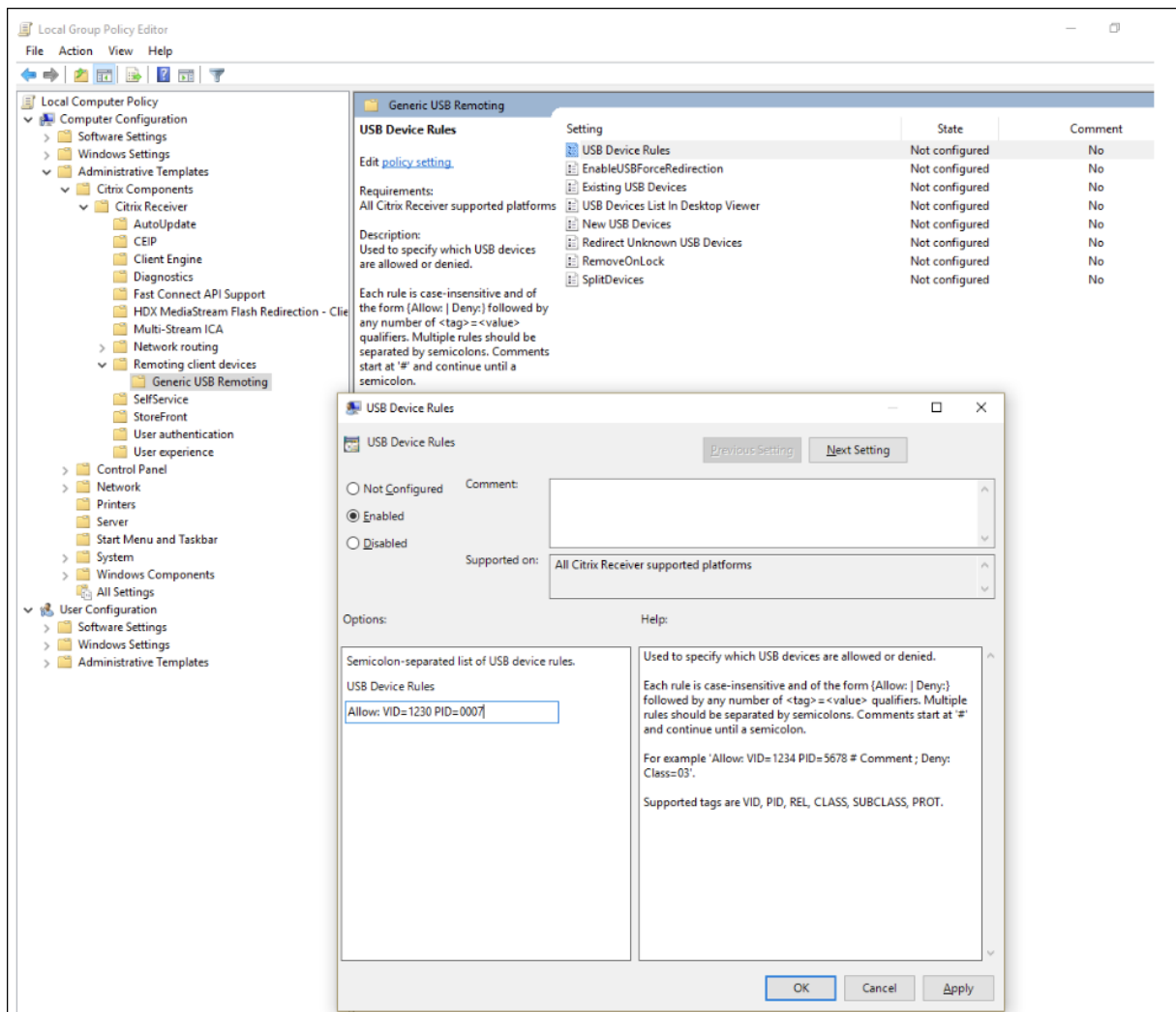
GenericUSB\ DeviceRules

Utilizzo dei GPO sul client:

1. Aprire **Local Group Policy Editor** e accedere a **Modelli amministrativi > Citrix Components > Citrix Receiver > Dispositivi client remoti > Generic USB Remoting**.
2. Apri l'impostazione **USB Device Rules** e abilita l'impostazione. Aggiungere la regola Dispositivo USB come in questo esempio, La regola Consenti: VID=1230 PID=0007 consente il dispositivo con ID fornitore 1230 e ID prodotto 0007.

Nota:

Usa la regola Allow: vid=XXXX PID=XXXX quando un dispositivo specifico deve essere in cima all'elenco delle regole del dispositivo.



Nota:

Uno strumento come USBView o anche la barra degli strumenti Connection può essere utilizzato per determinare i dettagli del dispositivo come VID e PID (includi SS qui).

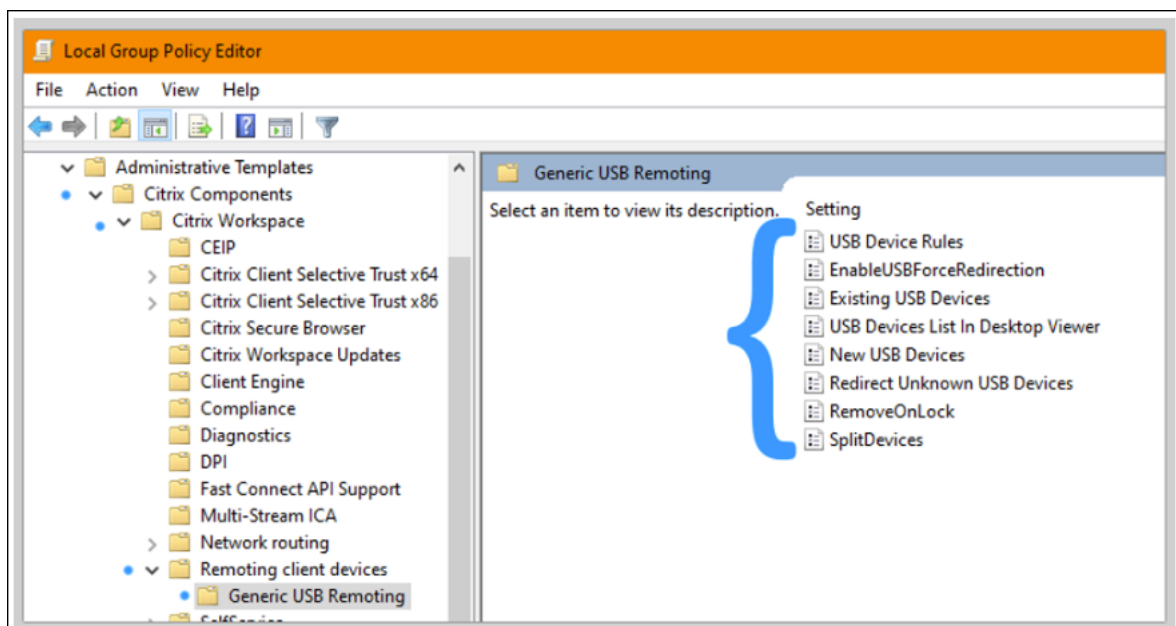
Configurare il reindirizzamento automatico dei dispositivi USB

I dispositivi USB vengono reindirizzati automaticamente quando è abilitato il supporto USB. Inoltre, le impostazioni delle preferenze utente USB sono impostate per connettere automaticamente i dispositivi USB. Reindirizzare tutti i dispositivi USB non è sempre la scelta migliore. Gli utenti possono reindirizzare esplicitamente i dispositivi dall'elenco dei dispositivi USB che non vengono reindirizzati automaticamente. Per impedire che i dispositivi USB vengano elencati o reindirizzati, utilizzare l'impostazione del criterio DeviceRules sull'endpoint client.

Questa policy può essere impostata sul client tramite un GPO, un registro lato client, tramite le Preferenze di Citrix Workspace o la scheda Connessioni in CDViewer. Tutti questi metodi sono descritti di seguito:

Utilizzo dei GPO sul client:

1. Apri **Local Group Policy Editor** e vai a **Modelli amministrativi > Citrix Components > Citrix Receiver > Dispositivi client remoti > Remoting USB generico**.
2. Aprire **New USB Devices** (Nuovi dispositivi USB), selezionare **Enabled** (Abilitati) e fare clic su **OK**.
3. Aprire **Existing USB Devices** (Dispositivi USB esistenti), selezionare **Enabled** (Abilitati) e fare clic su **OK**.

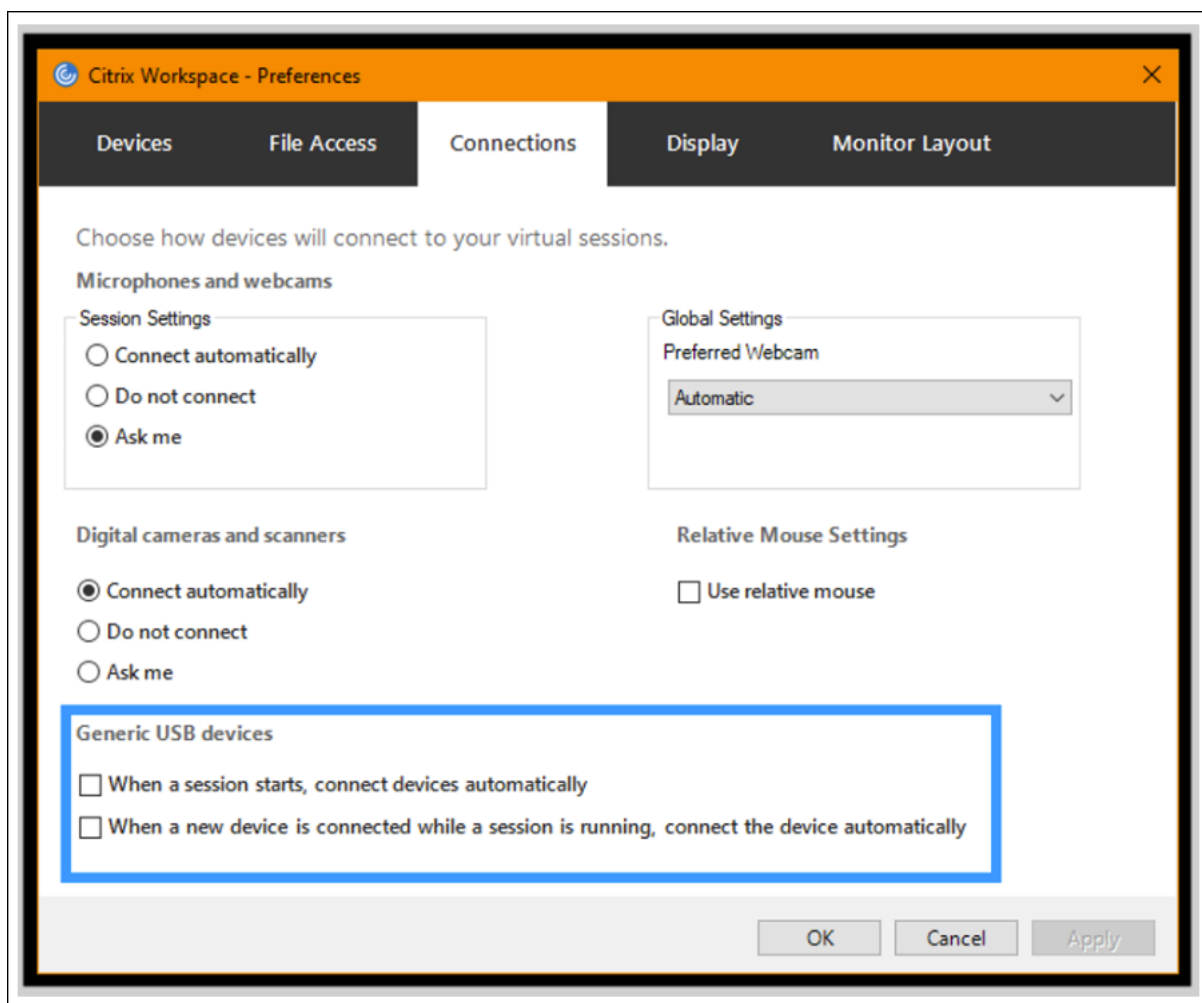


Utilizzo di Citrix Connection Center:

1. Andate a **Citrix Workspace Preferences > Connections**.
2. Assicurarvi che siano selezionate le seguenti opzioni:
 - a) When a session starts, connect devices automatically (All'avvio di una sessione, collegare automaticamente i dispositivi)
 - b) When a new device is connected while a session is running, connect the device automatically (Quando un nuovo dispositivo viene collegato mentre una sessione è in esecuzione, collegarlo automaticamente)
3. Fare clic su **OK**.

Utilizzando la barra degli strumenti CDViewer Connection:

1. Dopo l'avvio di una sessione, fate clic sul menu a discesa **CDViewer** e selezionate la scheda **Citrix Workspace Preferences > Connections**.
2. Assicurarvi che siano selezionate le seguenti opzioni:
 - a) When a session starts, connect devices automatically (All'avvio di una sessione, collegare automaticamente i dispositivi)
 - b) When a new device is connected while a session is running, connect the device automatically (Quando un nuovo dispositivo viene collegato mentre una sessione è in esecuzione, collegarlo automaticamente)
3. Fai clic su **Applica** e **OK** per salvare la politica.



Per le configurazioni basate sul client, le chiavi di registro sono impostate sul dispositivo client nella seguente posizione:

Attenzione!:

Fai riferimento al Disclaimer alla fine di questo articolo prima di utilizzare l'Editor del Registro di sistema. `HKLM\ SOFTWARE\ Wow6432Node\ Citrix\ ICA Client\ GenericUSB`

Configurazione di due o più dispositivi tramite reindirizzamento USB con regole di dispositivo diverse

È possibile reindirizzare più dispositivi all'interno della sessione HDX con regole del dispositivo diverse. Un amministratore potrebbe voler reindirizzare automaticamente un dispositivo fornendo al contempo un'opzione all'utente finale per reindirizzare l'altro dispositivo. Di seguito sono riportati i passaggi per configurare due dispositivi con regole diverse.

1. Abilitare l'impostazione del criterio di reindirizzamento del dispositivo USB client

in Citrix Web Studio.

1

Modifica l'impostazione **delle regole del dispositivo USB** nel GPO lato client.

- 1 1. Aprire **Local Group Policy Editor** e accedere a **Modelli amministrativi > Citrix Components > Citrix Receiver > Dispositivi client remoti > Generic USB Remoting**.
- 2
- 3 1. Apri l'impostazione **USB Device Rules** e abilita l'impostazione. Aggiungi la regola Dispositivo USB come in questo esempio, la regola **Allow: VID=0911 PID=0C1C** consente il dispositivo con **Vendor ID 0911** e **Product ID 0c1c** ma non verrà reindirizzato automaticamente. La regola **Connect: VID=06A8 PID=0043** reindirizzerà automaticamente il dispositivo con **Vendor ID 06A8** e **Product ID 0043** a condizione che siano impostate le politiche di reindirizzamento automatico menzionate nel passaggio 3.
- 4
- 5 1. **Consenti**: VID=0911 PID=0C1C #Phillips microfono vocale.
- 6
- 7 1. **Connect**: VID=06A8 PID=0043 **class=03** # Tampone per firme HSB Topaz

1

Apri **Local Group Policy Editor** e vai a **Modelli amministrativi > Citrix Components > Citrix Receiver > Dispositivi client remoti > Remoting USB generico**.

1

Aprire **New USB Devices** (Nuovi dispositivi USB), selezionare **Enabled** (Abilitati) e fare clic su **OK**.

1

Aprire **Existing USB Devices** (Dispositivi USB esistenti), selezionare **Enabled** (Abilitati) e fare clic su **OK**.

Una volta configurate queste impostazioni, il signature pad Topaz verrà reindirizzato automaticamente all'interno della sessione HDX e sarà necessaria un'ulteriore azione da parte dell'utente finale (selezionare l'opzione Reindirizza nel Centro connessioni o nella scheda Dispositivi visualizzatore CD) per reindirizzare il microfono vocale Phillips nella sessione.

Nota:

Le impostazioni precedenti nei passaggi 2 e 3 possono essere applicate direttamente nel valore di registro lato client **DeviceRules** nella chiave GenericUSB (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB) ma questo non è il modo consigliato.

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 nuovo Teams e offre informazioni essenziali per la transizione all'ottimizzazione Microsoft SlimCore.

Terminologia e transizione

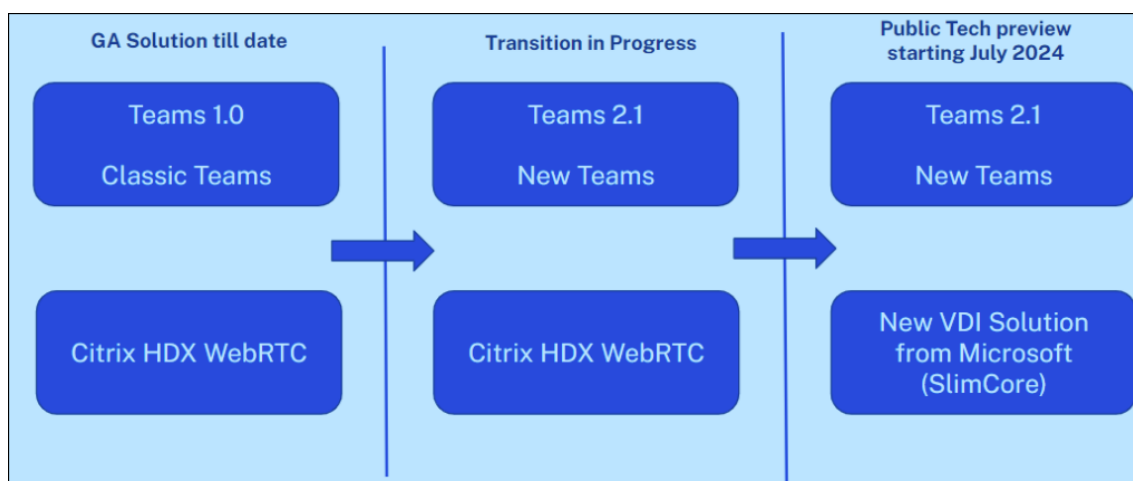
Transizione in Microsoft Teams

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

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.

Non sono necessari componenti aggiuntivi sull'endpoint tranne l'installazione dell'app Citrix Workspace.

Disponibile su piattaforme endpoint: Windows, macOS, Linux e ChromeOS.

Le nuove funzionalità vengono gestite in collaborazione da Citrix e Microsoft.

Ottimizzazione Microsoft SlimCore

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.

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 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

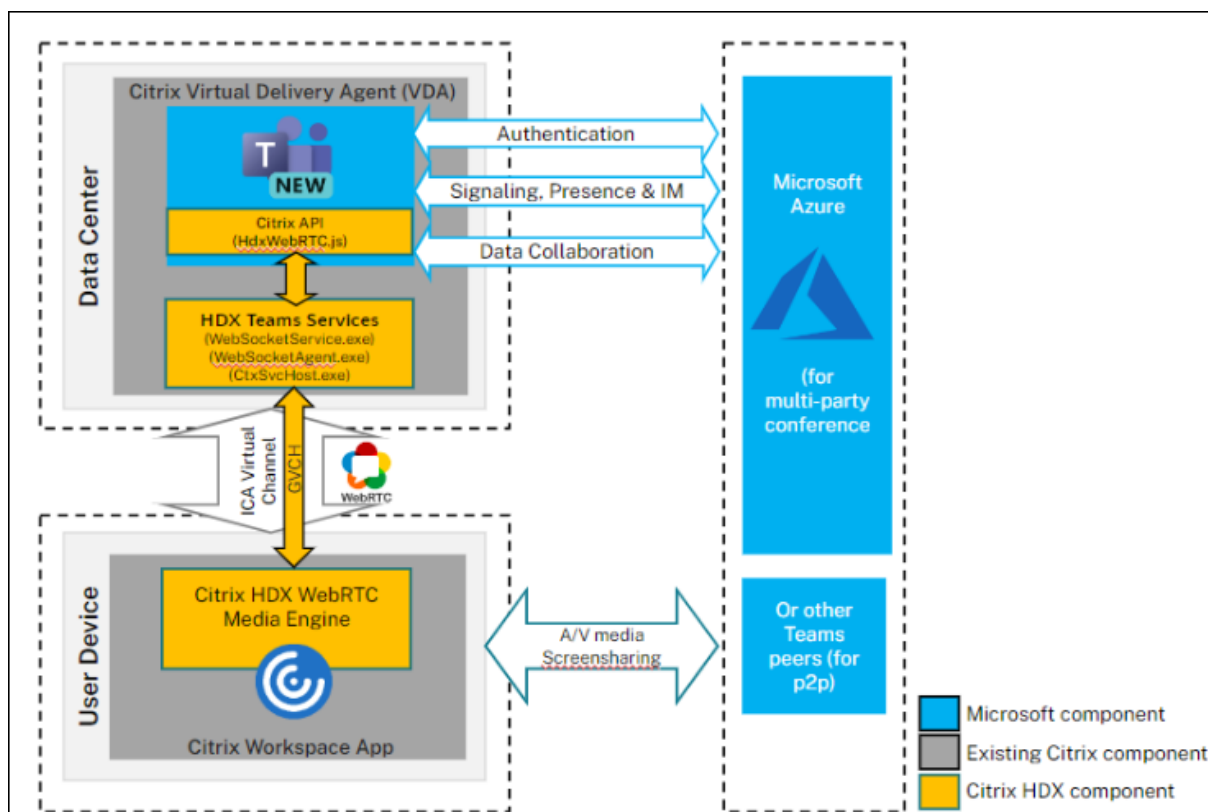
L'ottimizzazione Citrix HDX (WebRTC) e l'ottimizzazione Microsoft SlimCore possono esistere in parallelo, tuttavia il nuovo client Teams può essere ottimizzato con un solo una delle due alla volta.

- 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 registro `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 minime 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
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

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)
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
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

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)
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.

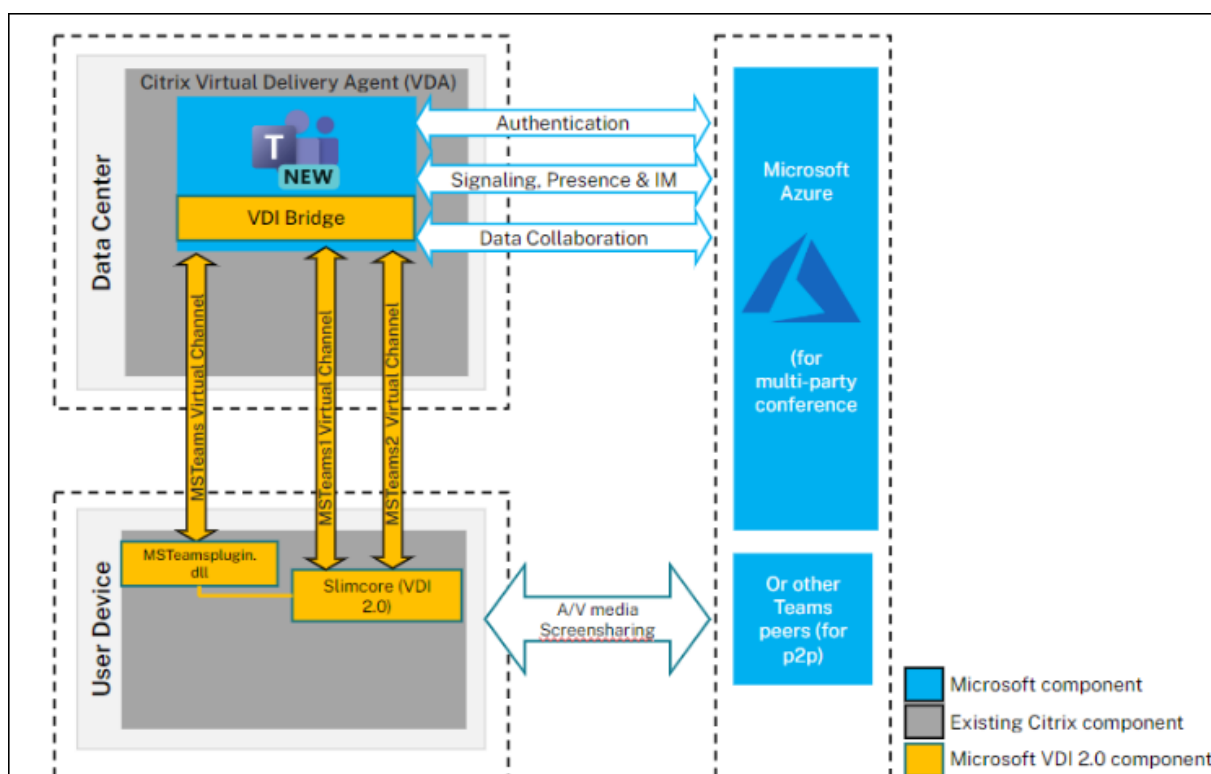
Per maggiori dettagli sulle limitazioni, vedere la pagina Microsoft [Funzionalità non supportate in VDI](#).

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

2203 LTSR CU3; 2305 CR

Versioni consigliate

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:

- ```
1 MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
2 MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
3 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

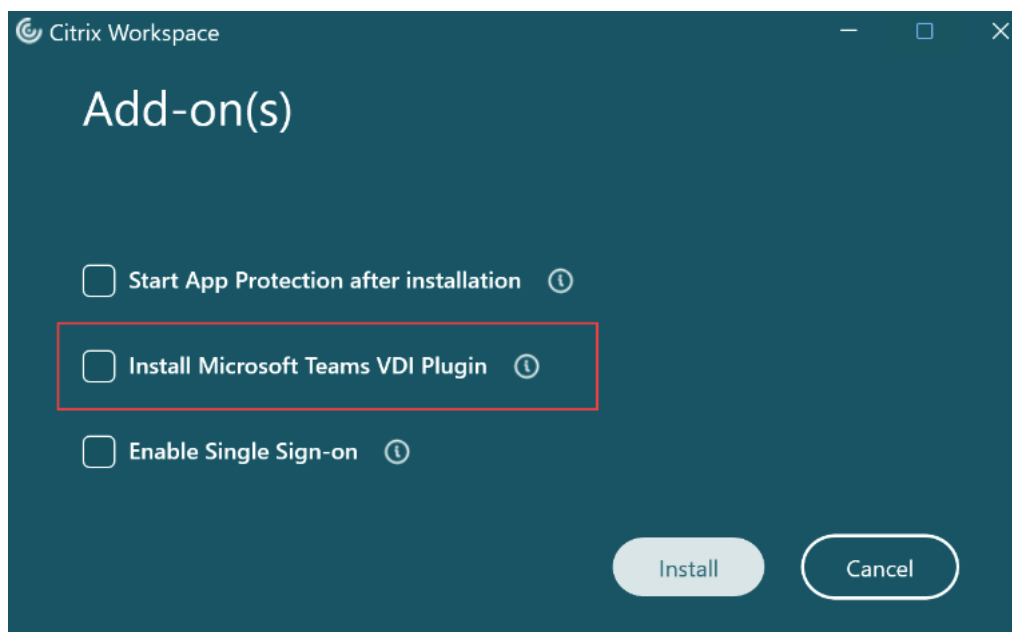
**Nota:**

- 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)

September 11, 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

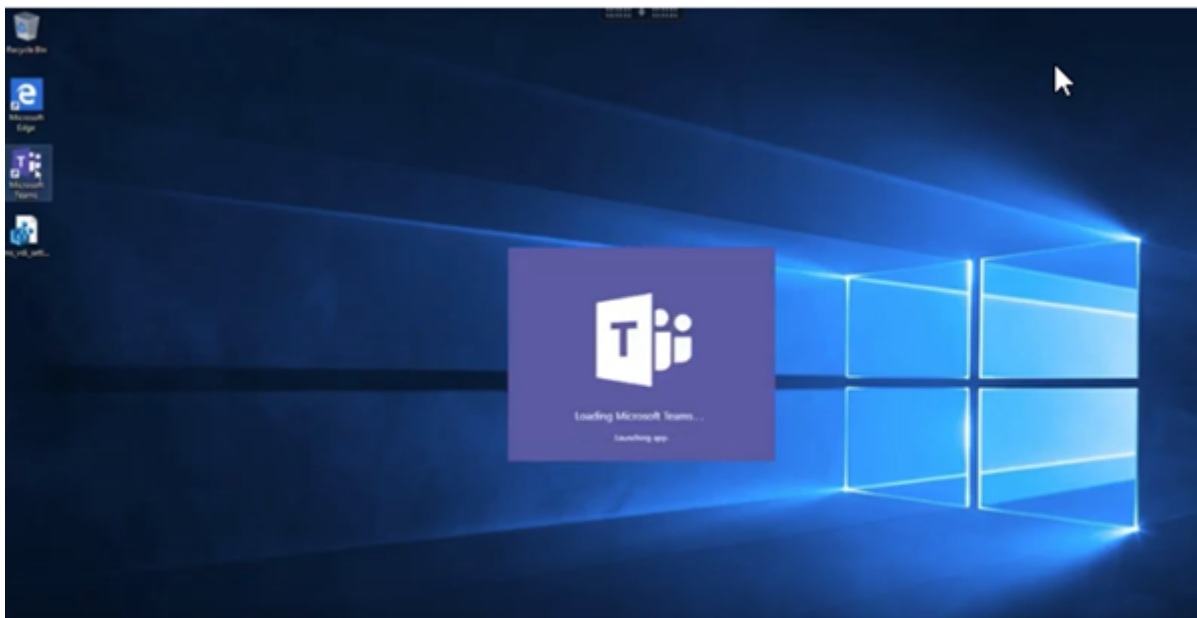
virtuale di controllo (CTXMTOP) verso il motore multimediale sul lato dell'app Citrix Workspace. L'endpoint decodifica i contenuti multimediali e ne esegue il provisioning localmente, spostando nuovamente la finestra dell'app Citrix Workspace nell'app Microsoft Teams ospitata.

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\\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\\AppData\Local\Microsoft\Teams`
- `C:\Users\\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\\AppData\Local\SquirrelTemp`
- `C:\Users\\AppData\Roaming\Microsoft\Teams`

*Collegamento sul desktop:*

```
C:\Users\\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\\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\\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

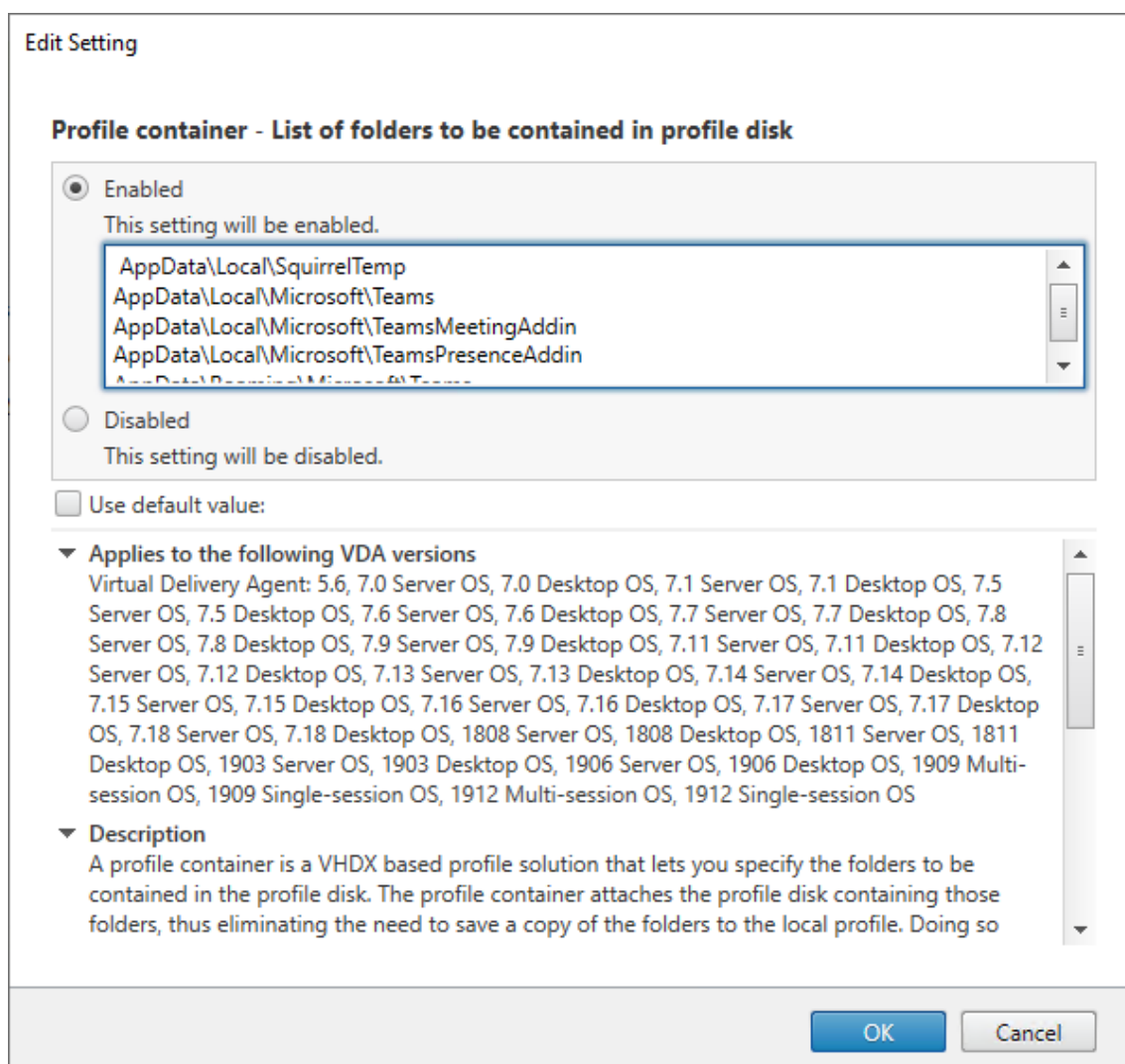
le dimensioni della memorizzazione nella cache dell'utente per ottimizzare ulteriormente la configurazione non persistente.

**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 LTSC (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'acquisizione 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.

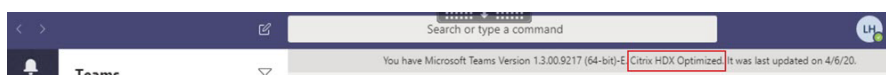
**Abilitare l'ottimizzazione di Microsoft Teams**

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\MSTeamsR** viene impostato automaticamente su **1** sul VDA. Microsoft Teams legge la chiave per caricarsi in modalità VDI.

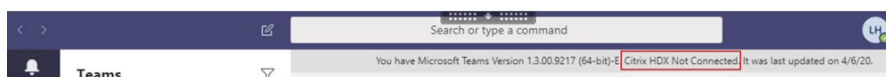
**Nota:**

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.

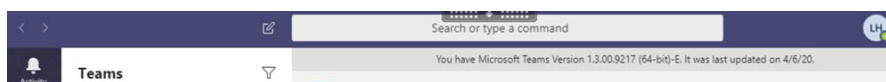
Se si fa clic su **About (Informazioni) > Version (Versione)**, viene visualizzata la legenda **Citrix HDX Optimized (Ottimizzato per Citrix HDX)**:



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: riconessioni 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 tunneling 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 (negoziato 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,<br>52.112.0.0/14,<br>52.122.0.0/15 | <b>UDP:</b> 3478, 3479, 3480, 3481, <b>TCP:</b> 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.

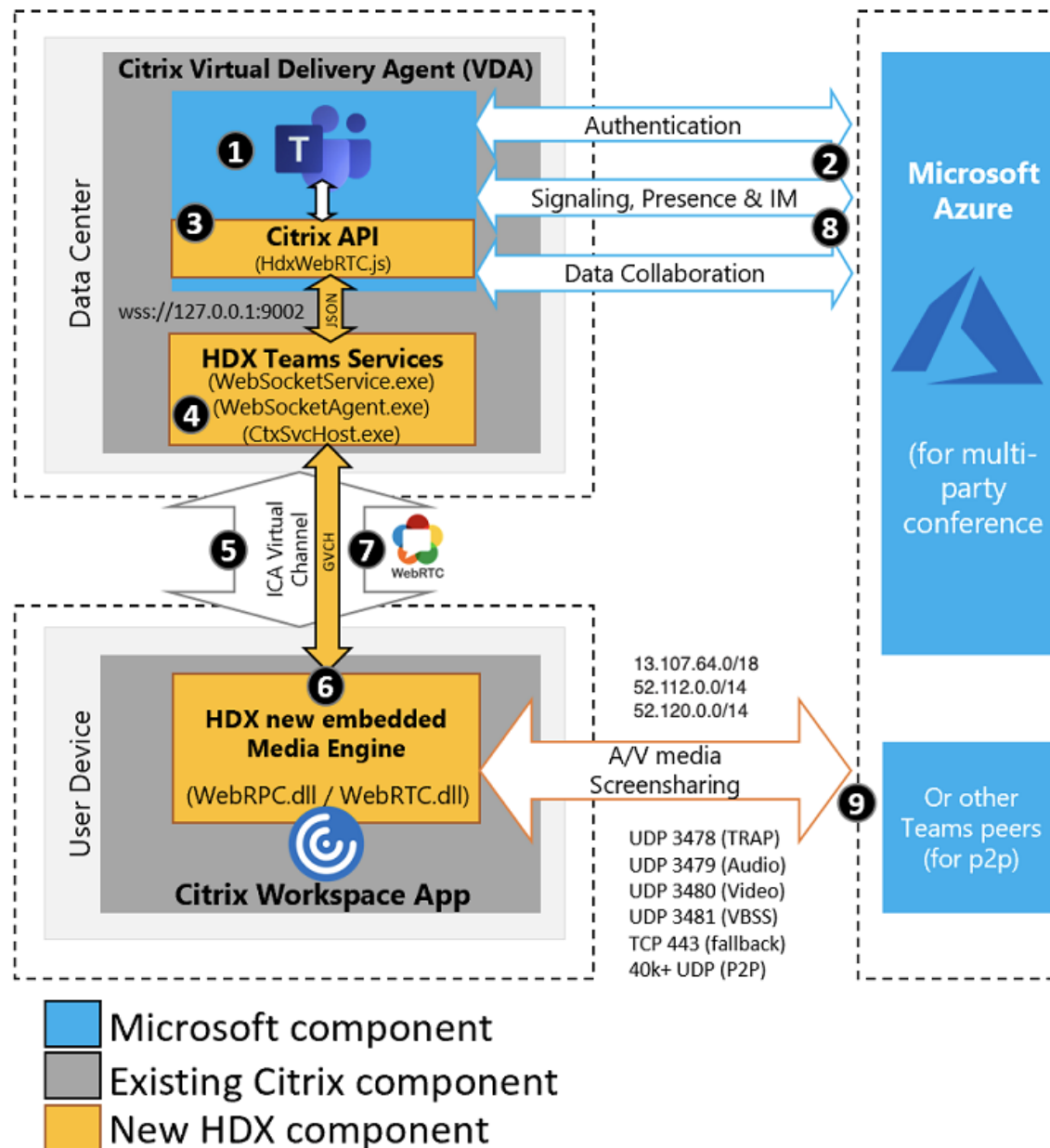
Se Microsoft Teams è stato caricato in modalità ottimizzata e HdxRtcEngine.exe è in esecuzione sull'endpoint, gli errori ICE potrebbero causare un errore di configurazione delle chiamate o audio/video monodirezionale. Quando una chiamata non può essere completata o i flussi multimediali non sono full 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, inoltramento, 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](#).

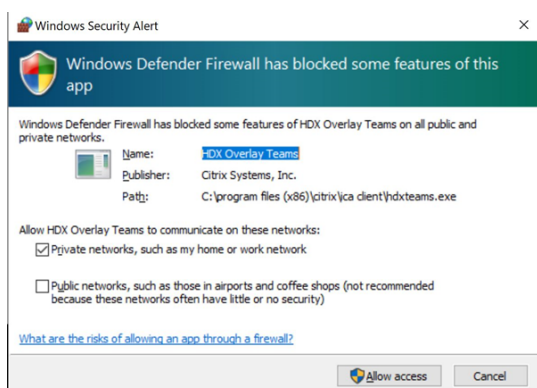
Le informazioni sulla posizione inviabili che l'app Citrix Workspace inoltra a Microsoft Teams sono:

- 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](http://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.

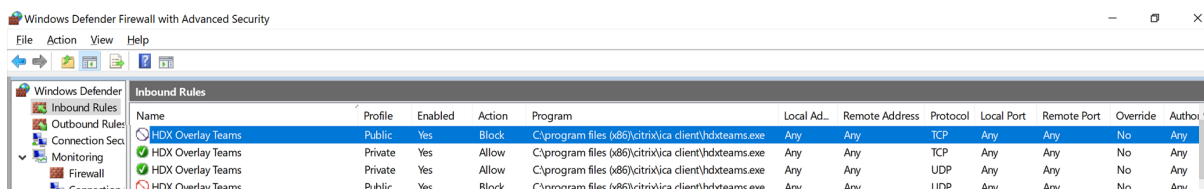
- WLAN BSSID e {IPv4-IPv6; Subnet; MAC Address} dell'endpoint in cui è installata l'app Citrix Workspace.
  - Le posizioni basate su subnet e WiFi sono supportate nell'app Workspace per Windows, Linux e Mac.
- Latitude e Longitude, se l'autorizzazione dell'utente è concessa a livello di sistema operativo 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.



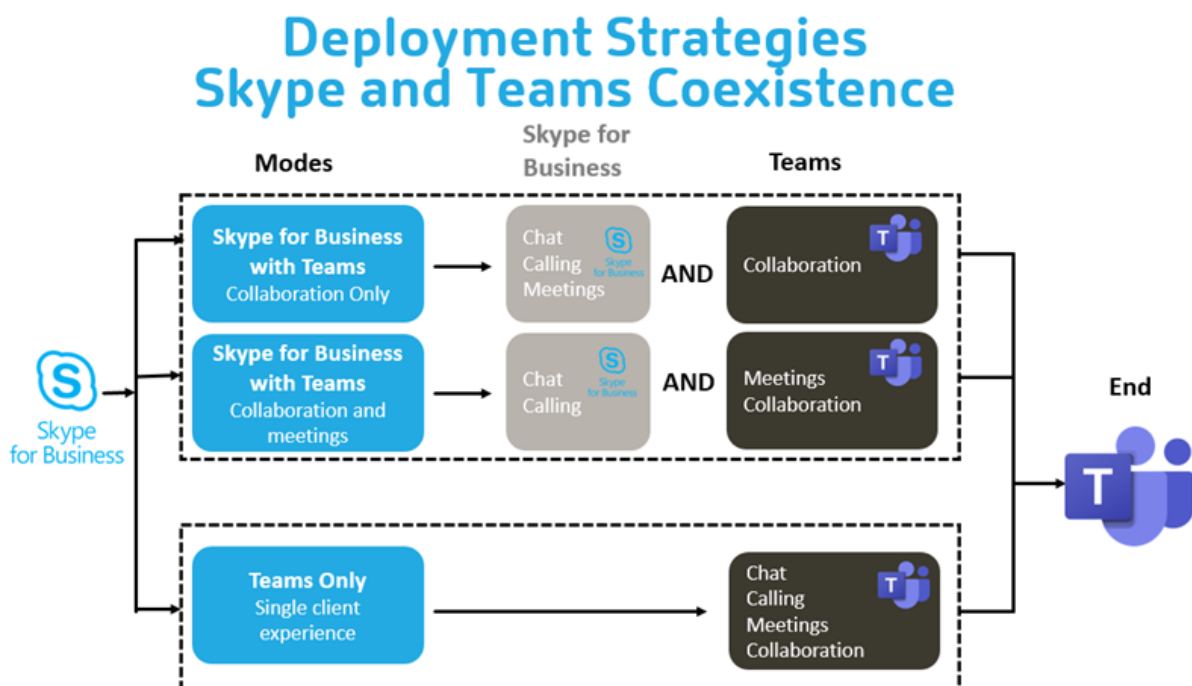
## Coesistenza di Microsoft Teams e Skype for Business

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

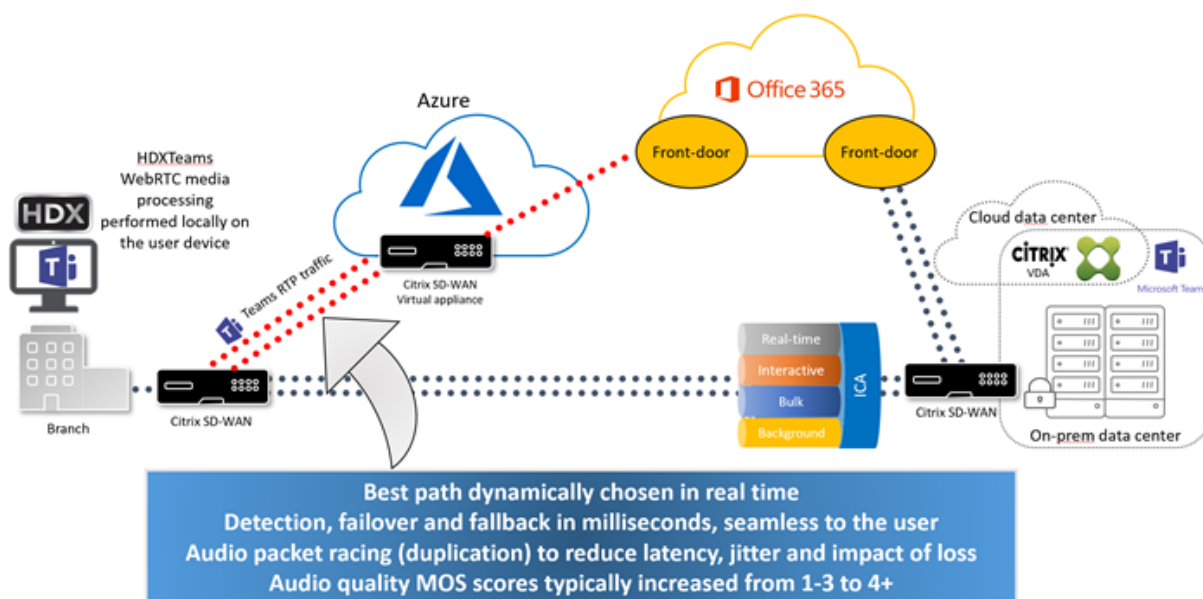
La qualità audio e video ottimale richiede una connessione di rete al cloud di Microsoft 365 con bassa latenza, basso jitter e bassa perdita di pacchetti. Il backhauling del traffico RTP audio-video di Microsoft Teams dagli utenti dell'app Citrix Workspace nelle sedi delle filiali a un centro dati prima 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,

```
1 {
2
3
4 "VideoBackgroundEffect":2,
5
6 "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).

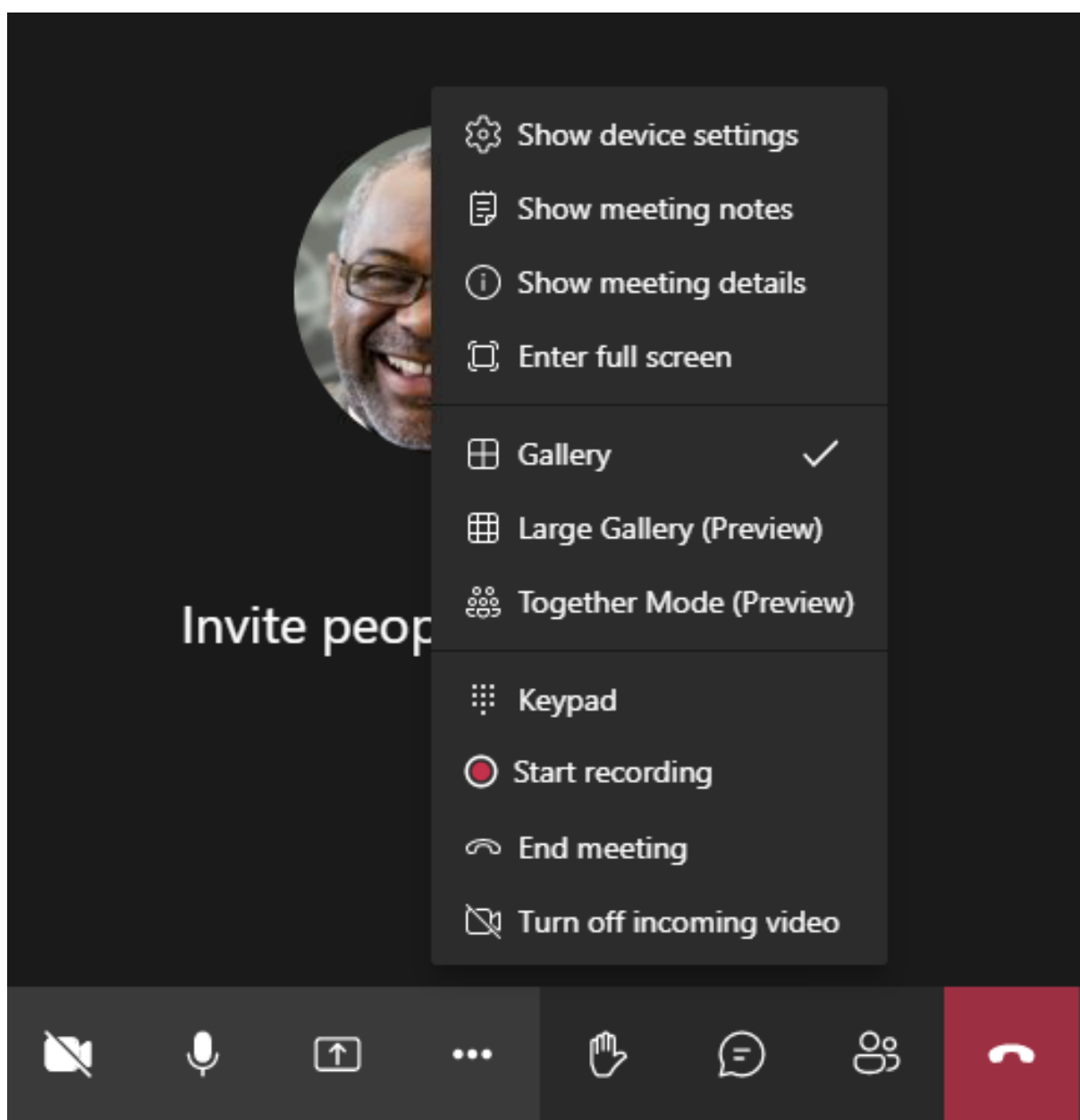
Microsoft Teams visualizza una griglia 2x2 con flussi video di quattro partecipanti (nota come **Gallery** [Galleria]). In questo caso, Microsoft Teams invia quattro flussi video al dispositivo client per la decodifica. Quando più di quattro partecipanti condividono un video, sullo schermo appaiono solo 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.                                   |

|                                            | Vista Gallery (Galleria) 2x2<br>(impostazione predefinita)                                                                                                                                                                                                                                                                                                                       | Vista Large Gallery (Galleria<br>ampia)                                                                                                                                                                                                      |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Decodifica in corrispondenza dell'endpoint | Ogni partecipante riceve fino a quattro flussi multimediali individuali. Ciò aumenta il consumo di CPU nell'endpoint di HdxRtcEngine.exe (per decodifica/rendering).                                                                                                                                                                                                             | Ogni partecipante riceve un solo flusso per audio e video. Questa impostazione riduce il consumo di CPU nell'endpoint.                                                                                                                       |
| Risoluzione massima                        | 720p. Quando quattro partecipanti condividono video, la risoluzione massima è di 360p per feed video. Se meno di quattro partecipanti condividono video, la risoluzione per feed video potrebbe essere più alta.                                                                                                                                                                 | 720p per il layout composito o il mixaggio. Non è necessario un flusso video di alta qualità per partecipante in un layout composito. A causa di questa condizione, ogni mittente riduce la risoluzione o la velocità in bit di caricamento. |
| Problema di "utente lento"                 | Il mittente modifica la qualità di ciascuna modalità (audio/video/condivisione dello schermo) sulla qualità di rete più bassa comune tra i partecipanti. Questo flusso multimediale viene quindi inoltrato a tutti gli altri partecipanti. Di conseguenza, un partecipante con cattive condizioni di rete influisce sulla qualità di tutti gli altri partecipanti alla chiamata. | Meno suscettibile allo scenario di qualità della rete più bassa comune. Il server per conferenze offre qualità diverse in base alle condizioni di rete dei singoli partecipanti.                                                             |
| Anteprima automatica                       | L'utente viene visualizzato in una piccola miniatura in tempo reale.                                                                                                                                                                                                                                                                                                             | L'utente viene visualizzato in una miniatura e mescolato con il resto dei feed video. Di conseguenza, l'utente potrebbe vedersi incluso nel layout del video principale con un ritardo aggiuntivo.                                           |

## Condivisione dello schermo in Microsoft Teams

Microsoft Teams si basa sulla condivisione dello schermo basata su video (VBSS), codificando essenzialmente il desktop condiviso con codec video come H264 e creando un flusso ad alta definizione. Con l'ottimizzazione HDX, la condivisione dello schermo in entrata viene considerata come un flusso video.

A partire dall'app Citrix Workspace 2109 o versione successiva per Windows, Linux, Mac e dall'app Citrix Workspace 2303 per ChromeOS, gli utenti possono condividere gli schermi e la videocamera contemporaneamente.

Con le versioni precedenti, se ci si trova nel mezzo di una videochiamata e l'altro peer inizia a condividere il desktop, il feed video della videocamera originale viene sospeso. Viene invece visualizzato il feed video per la condivisione dello schermo. Il peer deve quindi riprendere manualmente la condivisione della videocamera.

### Nota per PowerPoint Live

Questa limitazione non esiste se si condividono contenuti da PowerPoint Live. In tal caso, gli altri colleghi possono ancora vedere la webcam e i contenuti e navigare avanti e indietro per esaminare altre diapositive. In questo scenario, le diapositive vengono renderizzate sul VDA. Per accedere a una presentazione PowerPoint Live, fare clic sul pulsante del pannello di condivisione e selezionare una delle diapositive di PowerPoint suggerite, oppure fare clic su "Sfogliare" 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 (CD-Viewer.exe), con un bordo rosso disegnato all'intorno. Qualsiasi applicazione locale che si sovrappone a Desktop Viewer non viene acquisita.

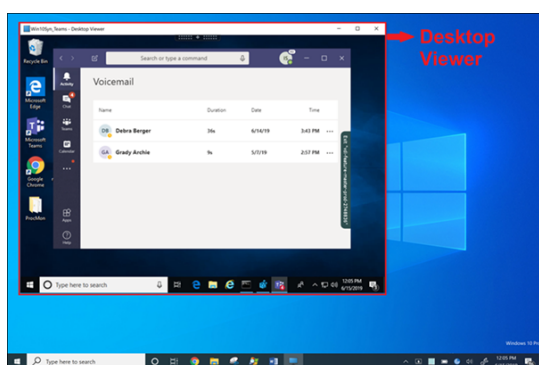
### Nota

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 composta.
- 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`:

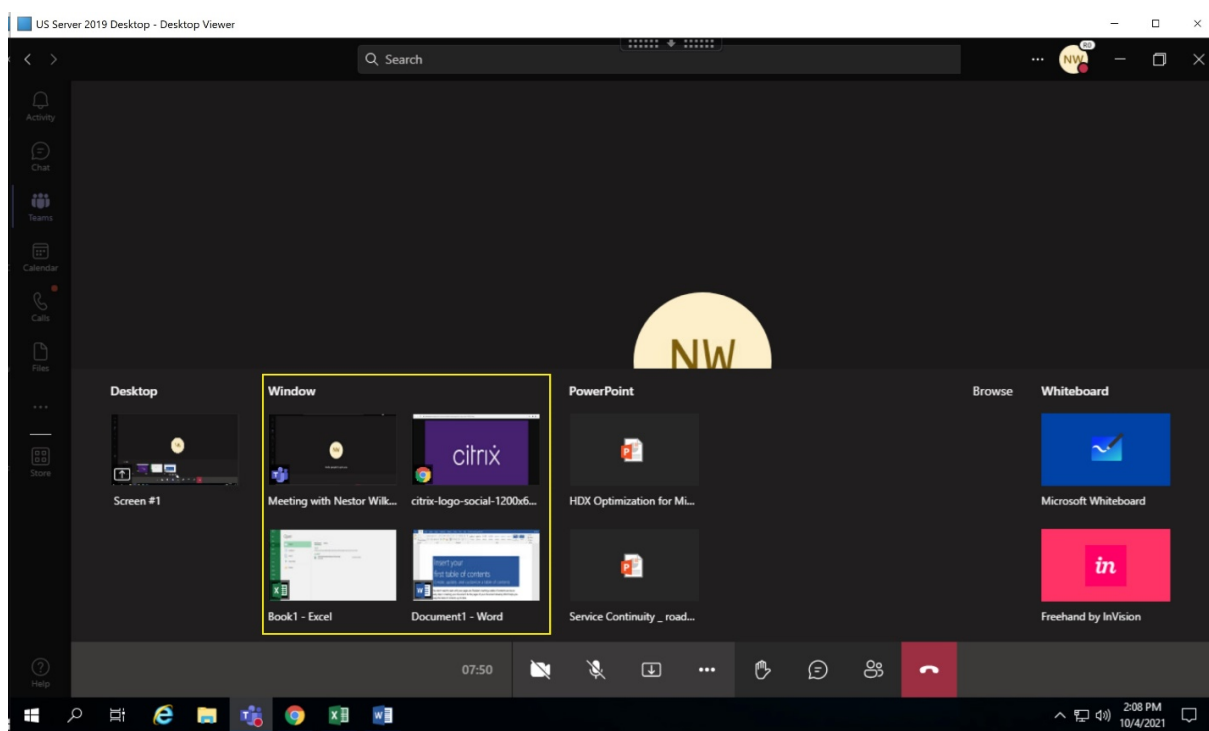
Nome: `UseWsProvider`

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.

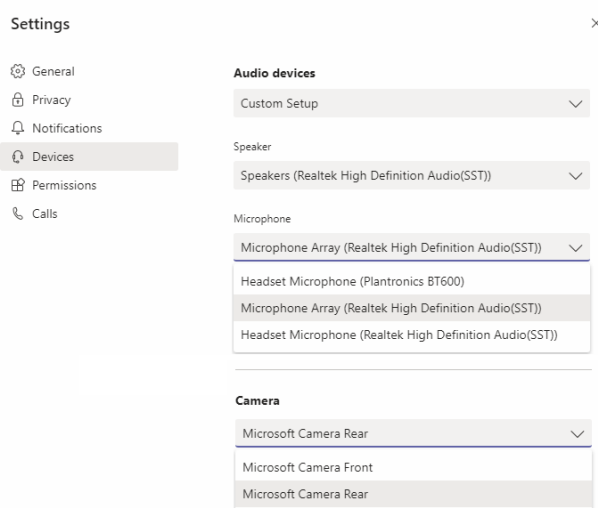
Mentre si dispone del controllo, è possibile effettuare selezioni, modifiche e altre alterazioni nello schermo condiviso. Per queste azioni, è possibile usare sia la tastiera che il mouse. Al termine fare clic su **Richiedi controllo**.

**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](http://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 webcam che eseguono la codifica H.264 on-board UVC 1.1 e 1.5.

#### **Nota:**

L'app Workspace 2009.6 per Windows è ora in grado di acquisire periferiche con formati audio a 24 bit o con frequenze superiori a 96 kHz.

HdxTeams.exe (nell'app Citrix Workspace per Windows 2009 o versioni precedenti) supporta solo questi formati specifici dei dispositivi audio (canali, profondità di bit e frequenza di campionamento):

- Dispositivi di riproduzione: fino a 2 canali, 16 bit, frequenze fino a 96.000 Hz
- Dispositivi di registrazione: fino a 4 canali, 16 bit, frequenze fino a 96.000 Hz

Anche se un solo altoparlante o microfono non corrisponde alle impostazioni previste, l'enumerazione dei dispositivi in Microsoft Teams non va a buon fine e viene visualizzato **Nessuno** in **Impostazioni > Dispositivi**.

Il 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 tec-



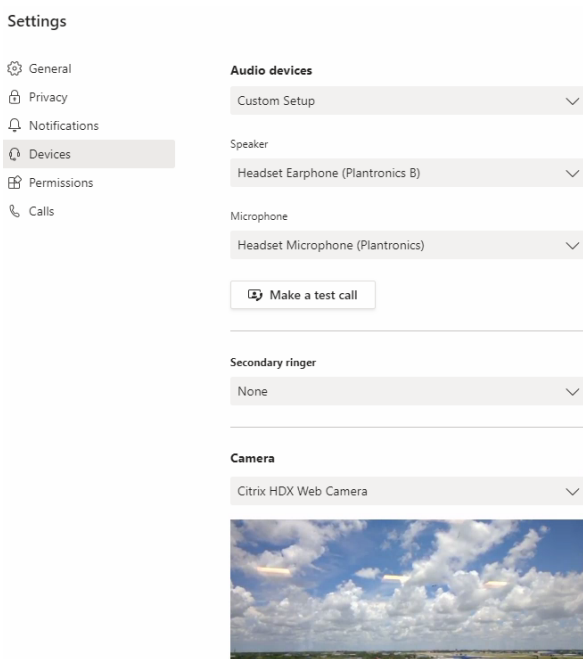
nologie HDX legacy. Le tecnologie HDX legacy potrebbero essere il reindirizzamento della webcam e il reindirizzamento del microfono e dell'audio del client. Se si utilizza una versione dell'app Workspace/un sistema operativo della piattaforma che non supporta l'ottimizzazione di Microsoft Teams, le chiavi 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 doc-

umentazione.

### 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](#)

## Timeout dinamici delle sessioni

November 5, 2024

Questa funzione consente di configurare timeout di sessione disconnessa e inattiva per le ore di utilizzo di punta e non di punta per ottenere uno svuotamento della macchina più rapido e risparmi sui costi. Questa funzionalità si applica a:

- Macchine con sistema operativo mono-sessione e multi-sessione.
- Tutte le macchine nel Delivery Group, indipendentemente dal fatto che siano contrassegnate per il ridimensionamento automatico.

Un VDA segnala i tempi di inattività per le sessioni rimaste inattive per più di 10 minuti, pertanto i timeout dinamici delle sessioni non sono in grado di disconnettere le sessioni inattive entro 10 minuti dall'inattività. Un valore inferiore rimuove prima le sessioni persistenti, riducendo così i costi.

## Manage Autoscale

Enabled

CYAZinfo1027

✕

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Force User Logoff

Autoscaling Tagged Machines

### Dynamic Session Timeout

Configure dynamic timeouts for your peak and off-peak usage times to achieve faster VM draining and cost savings. Larger values can improve user experience and smaller values can achieve faster draining.

[Learn more](#)

|                                                                        | During peak times                                |                                              | During off-peak times                                                                   |
|------------------------------------------------------------------------|--------------------------------------------------|----------------------------------------------|-----------------------------------------------------------------------------------------|
| Idle session timeout: <span style="font-size: 0.8em;">?</span>         | Disable <span style="font-size: 0.8em;">▼</span> | min <span style="font-size: 0.8em;">▼</span> | 3 <span style="font-size: 0.8em;">▼</span> min <span style="font-size: 0.8em;">▼</span> |
| Disconnected session timeout: <span style="font-size: 0.8em;">?</span> | 4 <span style="font-size: 0.8em;">▼</span>       | min <span style="font-size: 0.8em;">▼</span> | 5 <span style="font-size: 0.8em;">▼</span> min <span style="font-size: 0.8em;">▼</span> |

▲ Autoscale dynamic timeouts are for cost savings. If used for security purposes, the configured timeouts might conflict with your GPO or Studio policies. When a conflict occurs, the shorter timeout prevails. [↗](#)

Save

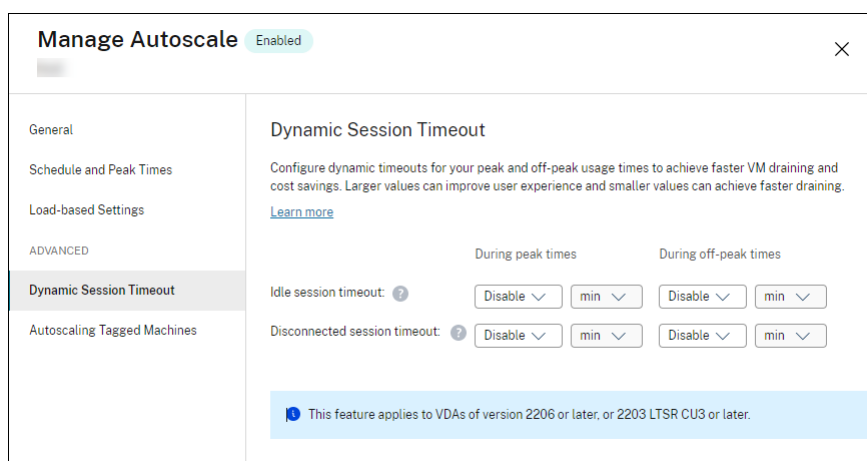
Apply

Cancel

↶

**Nota:**

- Questa funzionalità è sempre disponibile per i gruppi di consegna con sistema operativo multisessione.
- Per i gruppi di consegna di sistemi operativi a sessione singola, questa funzionalità si applica ai VDA della versione 2206 CR o successiva o 2203 LTSR CU3 o successiva. Verificare che i VDA siano stati registrati su Citrix Cloud almeno una volta. Quando non è disponibile, viene visualizzata la seguente interfaccia utente:



- I timeout dinamici di Autoscale consentono di risparmiare sui costi. Se utilizzati per scopi di sicurezza, i timeout configurati potrebbero entrare in conflitto con l'oggetto Criteri di gruppo o i criteri della console Manage. Quando si verifica un conflitto, prevale il timeout più breve.

**Timeout della sessione inattiva.** Abilita o disabilita un timer che specifica per quanto tempo viene mantenuta ininterrotta una connessione utente in assenza di input da parte dell'utente. Allo scadere del timer, la sessione viene posta nello stato disconnesso e si applica il timeout di sessione disconnessa \*\*. **Se il timeout della sessione disconnessa\*\* è disabilitato, la sessione non viene disconnessa.**

**Importante:**

- Se si specifica un valore inferiore o uguale a 10 minuti (600 secondi), Autoscale disconnette le sessioni pertinenti dopo che sono rimaste inattive per 10 minuti. Questo perché Autoscale si basa sui tempi di inattività delle sessioni riportati dai VDA. I VDA segnalano i tempi di inattività solo per le sessioni che sono rimaste inattive per più di 10 minuti.
- Una sessione inattiva può comunque essere posta in stato disconnesso se l'utente interagisce con essa entro gli ultimi 5 minuti dal raggiungimento del timeout della sessione inattiva.

**Timeout della sessione disconnessa.** Abilita o disabilita un timer che specifica per quanto tempo un desktop disconnesso debba rimanere bloccato prima che la sessione venga terminata. Se è abilitato, la sessione disconnessa viene terminata alla scadenza del timer.



## Domande frequenti

### **La funzionalità di timeout dinamico della sessione si applica solo alle macchine contrassegnate per l'Autoscaling?**

La funzionalità di timeout dinamico della sessione si applica a tutte le macchine nel gruppo Delivery, indipendentemente dal fatto che siano contrassegnate per il ridimensionamento automatico.

### **Quando una sessione viene chiusa a causa del timeout dinamico della sessione, anche le macchine non taggate vengono incluse nell'obiettivo di scalabilità automatica delle macchine taggate?**

La funzionalità di timeout dinamico della sessione non è correlata alla funzionalità di tagging Autoscale. Se i timeout dinamici delle sessioni determinano la chiusura delle sessioni, anche le macchine non contrassegnate potrebbero essere spente durante il processo, a condizione che le macchine siano in fase di esaurimento fino allo spegnimento.

## Impostazioni

September 11, 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.

È possibile usare Web Studio per gestire queste impostazioni:

- Gestire l'autenticazione
- [Programma di miglioramento dell'esperienza cliente Citrix](#)
- [Rimuovere i Delivery Controller](#)
- [Modificare il database di registrazione](#)
- Impostare data e ora
- Centralizzare la gestione del sito
- [Abilitare l'assegnazione automatica di più utenti per l'accesso remoto al PC](#)

- Abilitare la risoluzione DNS
- [Abilitare l'attendibilità XML](#)
- [Gestire la chiave di sicurezza](#)
- Impostare il timeout di inattività per la console Studio

## Gestire l'autenticazione

Per impostazione predefinita, gli utenti accedono a Web Studio utilizzando il nome utente e la password del dominio. È inoltre possibile scegliere un metodo di autenticazione diverso per gli utenti, ad esempio l'autenticazione con smart card o l'autenticazione integrata di Windows.

Per scegliere un metodo di autenticazione per gli utenti, seguire questi passaggi:

1. Accedere a Web Studio e selezionare Settings nel riquadro a sinistra.
2. Individuare il riquadro Authentication (Autenticazione) e fare clic su Edit (Modifica) per selezionare un'opzione:
  - Credenziali di dominio
  - Credenziali di dominio o autenticazione Windows integrata

Con l'autenticazione Windows integrata abilitata, gli utenti possono accedere a Web Studio utilizzando le proprie credenziali Windows (Kerberos/NTLM) o un certificato client.

Quando Web Studio e Delivery Controller sono installati su macchine diverse, affinché l'autenticazione integrata di Windows funzioni, abilitare l'opzione Allow cross-origin access (Consenti l'accesso multiorigine) e aggiungere l'URL del server Web Studio all'elenco degli indirizzi consentiti.

### Importante

L'autenticazione integrata di Windows non funziona quando Web Studio è configurato come proxy per i Delivery Controller.

- Autenticazione con smart card.
- Credenziali di dominio o autenticazione con smart card

L'attivazione dell'autenticazione tramite smart card richiede una configurazione aggiuntiva. Per ulteriori informazioni, vedere [Configurare l'autenticazione con smart card per Web Studio](#).

Dopo aver abilitato l'opzione **Integrated Windows authentication** (Autenticazione Windows integrata), al successivo accesso gli utenti accedono automaticamente. Come utente, se non si riesce ad accedere automaticamente, seguire questi passaggi per configurare il browser Web in modo da consentire l'autenticazione Windows integrata.

Per Google Chrome:

1. Dal Pannello di controllo, selezionare Opzioni Internet.
2. Selezionare la scheda **Avanzate**.
3. Selezionare **Abilita l'autenticazione Windows integrata**.
4. Selezionare la scheda **Sicurezza**.
5. Selezionare **Intranet locale > Siti > Avanzate**.
6. Nella casella **Aggiungi questo sito Web all'area**:
  - Se Web Studio e Delivery Controller risiedono sullo stesso server, digitare l'URL dell'host che esegue Web Studio.
  - In caso contrario, digitare un dominio jolly. Esempio: se il Delivery Controller è in `ddc.domain.com`, digitare `*.domain.com`.
7. Fare clic su **Aggiungi > Chiudi**

Per Mozilla Firefox:

1. Dal browser, digitare `about:config` nella casella dell'URL.
2. Nella casella **Cerca**, digitare `network negotiate`.
3. Fare clic con il pulsante destro del mouse su **network.negotiate-auth.trusted-uris** e selezionare **Modifica**.
4. Nella casella **Inserisci il valore della stringa**:
  - Se Web Studio e il Delivery Controller risiedono sullo stesso server, aggiungere un elenco separato da virgole di URL e/o alias che fanno riferimento al nome del server che ospita Web Studio.
  - In caso contrario, aggiungere gli URL in questo modo. Esempio: se il Delivery Controller è in `ddc.domain.com`, digitare `*.domain.com`.

Dopo aver configurato il browser, è possibile fare clic su **Windows integrated sign-in** (Accesso integrato di Windows) nella pagina di accesso per riprovare.

Quando Web Studio e Delivery Controller sono installati su macchine diverse, affinché l'autenticazione integrata di Windows funzioni, è necessario abilitare l'opzione **Allow cross-origin access** (Consenti l'accesso multiorigine).

Seguire questi passaggi per **abilitare l'accesso multiorigine**:

1. Selezionare la casella di controllo **Allow cross-origin access**.
2. Aggiungere l'URL del server Web Studio all'elenco degli indirizzi consentiti.

3. Nel campo **Enter URL** (Inserisci URL), inserire l'URL. Fare clic su **Add** (Aggiungi) per aggiungerne altri, se necessario.

#### Nota

- L'URL deve essere nel formato corretto: <scheme>://<hostname>. Assicurarsi che non contenga percorsi o barre finali.
- Sono supportati indirizzi IP e FQDNS. Quando si aggiunge un URL, assicurarsi che corrisponda al modo in cui si accede a Web Studio. Ad esempio, se si accede a Web Studio utilizzando un indirizzo IP, aggiungere l'URL basato sull'indirizzo IP all'elenco.
- Se si utilizza una porta non predefinita, assicurarsi di includere il numero di porta.

4. Fare clic su **Add** (Aggiungi) per aggiungerne altri, se necessario.
5. Al termine, fare clic su **Done** (Fine) per salvare e uscire.

## Impostare il fuso orario

Per personalizzare il formato di data e ora in base alle proprie preferenze, seguire questi passaggi:

1. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra.
2. Individuare il riquadro **Date and time** (Data e ora) e fare clic su **Edit** per configurare le seguenti opzioni:
  - **Time format** (Formato ora):
    - Selezionare questa opzione per visualizzare l'ora utilizzando un orologio a 12 ore (09:00 pm, ad esempio) o un orologio a 24 ore (21:00, ad esempio).
  - **Date format** (Formato data):
    - Configurare il formato della data in base alle proprie preferenze, ad esempio gg/M-M/aaaa.
  - **Time zone** (Fuso orario):
    - **UTC**: visualizza la data e l'ora in UTC in tutta l'interfaccia utente. Passando il mouse sulla data e l'ora vengono visualizzate le informazioni nel fuso orario locale.
    - **Local time zone** (Fuso orario locale): consente di visualizzare la data e l'ora nel fuso orario locale in tutta l'interfaccia utente. Passando il mouse sulla data e l'ora vengono visualizzate le informazioni in UTC.

#### Nota:

Queste impostazioni sono specifiche per ogni account utente.

## Abilitare la risoluzione DNS

Per presentare i nomi DNS anziché gli indirizzi IP nel file ICA, seguire questi passaggi:

1. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra.
2. Attivare l'impostazione **Enable DNS resolution** (Abilita risoluzione DNS).

## Impostare il timeout di inattività per la console Studio

È possibile impostare il tempo di inattività dopo il quale gli amministratori si disconnettono automaticamente dalla console Studio.

1. Accedere a Web Studio e selezionare **Settings** nel riquadro a sinistra.
2. Digitare una durata compresa tra 10 minuti e 24 ore.
3. Per applicare questa impostazione, aggiornare la pagina o uscire e quindi accedere nuovamente.

## Centralizzare la gestione del sito

Questa funzionalità consente di utilizzare una console Web Studio per gestire più siti di Citrix Virtual Apps and Desktops. Per ulteriori informazioni, vedere [Enable multiple site management](#) (Abilitare la gestione di più siti).

## Distribuzione sicura di Director

November 5, 2024

Questo articolo evidenzia le aree che potrebbero avere un impatto sulla sicurezza del sistema durante la distribuzione e la configurazione di Director.

## Configurare Microsoft Internet Information Services (IIS)

È possibile configurare Director con una configurazione IIS limitata.

## Limiti di riciclaggio del pool di applicazioni

È possibile impostare i seguenti limiti di riciclaggio del pool di applicazioni:

- Limite di memoria virtuale: 4.294.967.295

- Limite di memoria privata: la dimensione della memoria fisica del server StoreFront
- Limite richieste: 4.000.000.000

### **Estensioni dei nomi file**

È possibile non consentire le estensioni dei nomi di file non elencate.

Director richiede queste estensioni dei nomi di file in Request Filtering (Richiedi filtraggio):

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .png
- .json
- .woff
- .woff2
- .ttf

Director richiede i seguenti verbi HTTP in Request Filtering (Richiedi filtraggio). È possibile non consentire i verbi non elencati.

- GET
- POST
- HEAD

Director non richiede:

- Filtri ISAPI
- Estensioni ISAPI
- Programmi CGI
- Programmi FastCGI

#### **Importante:**

- Director richiede Full Trust (Attendibilità totale). Non impostare il livello globale di attendibilità di .NET su High (Alto) o su un valore inferiore.
- Director mantiene un pool di applicazioni separato. Per modificare le impostazioni di Director, selezionare il sito di Director e modificarlo.

## Configurare i diritti utente

Quando Director è installato, ai relativi pool di applicazioni viene concesso quanto segue:

- Diritto di accesso **Log on as a service** (Accedi come servizio)
- Privilegi **Adjust memory quotas for a process** (Regola le quote di memoria per un processo), **Generate security audits** (Genera audit di sicurezza) e **Replace a process level token** (Sostituisci un token a livello di processo)

I diritti e i privilegi menzionati sono normali comportamenti di installazione quando vengono creati pool di applicazioni.

Non è necessario modificare questi diritti utente. Questi privilegi non vengono utilizzati da Director e vengono automaticamente disabilitati.

## Comunicazioni di Director

In un ambiente di produzione, utilizzare i protocolli IPsec (Internet Protocol Security) o HTTPS per proteggere i dati che vengono trasferiti tra Director e i server.

IPsec è un insieme di estensioni standard del protocollo Internet che fornisce comunicazioni autenticate e crittografate con integrità dei dati e protezione della riproduzione. Poiché IPsec è un insieme di protocolli a livello di rete, i protocolli di livello superiore possono utilizzarlo senza modifiche. HTTPS utilizza i protocolli TLS (Transport Layer Security) per fornire una crittografia avanzata dei dati.

### Nota:

- Citrix consiglia vivamente di limitare l'accesso alla console di Director all'interno della rete intranet.
- Citrix consiglia vivamente di non abilitare connessioni non protette a Director in un ambiente di produzione.
- Le comunicazioni sicure da Director richiedono una configurazione separata per ciascuna connessione.
- Il protocollo SSL non è consigliato. Utilizzare invece il protocollo TLS, che è più sicuro.
- Proteggere le comunicazioni con Citrix ADC utilizzando TLS, non IPsec.

Per proteggere le comunicazioni tra i server di Director e Citrix Virtual Apps and Desktops (per il monitoraggio e i report), vedere [Sicurezza dell'accesso ai dati](#).

Per proteggere le comunicazioni tra Director e Citrix ADC (per Citrix Insight), fare riferimento a [Configura analisi di rete](#).

Per proteggere le comunicazioni tra Director e il server delle licenze, vedere [Proteggere la console di amministrazione delle licenze](#).

## Separazione della sicurezza di Director

È possibile distribuire qualsiasi applicazione Web nello stesso dominio Web (nome di dominio e porta) di Director. Tuttavia, qualsiasi rischio per la sicurezza in tali applicazioni Web può potenzialmente ridurre la sicurezza della distribuzione di Director. Laddove è richiesto un maggiore grado di separazione della sicurezza, Citrix consiglia di distribuire Director in un dominio Web separato.

## Matrice di compatibilità delle funzionalità

November 5, 2024

Citrix Director 7 2402 è compatibile con:

- Citrix Virtual Apps and Desktops 7 2112 e versioni successive
- Citrix Virtual Apps and Desktops 7 1912 LTSR

All'interno di ciascun sito, sebbene sia possibile utilizzare Director con versioni precedenti di Delivery Controller, tutte le funzionalità dell'ultima versione di Director potrebbero non essere disponibili. Citrix consiglia di utilizzare la stessa versione per Director, Delivery Controller e VDA.

### Nota:

Dopo aver aggiornato un Delivery Controller, viene richiesto di aggiornare il sito all'apertura di Studio. Per ulteriori informazioni, consulta la sezione **Upgrade Sequence** in [Aggiornare una distribuzione](#).

La prima volta che si effettua l'accesso dopo un aggiornamento di Director, viene eseguito un controllo della versione sui siti configurati. Se un sito sta eseguendo una versione del Controller precedente a quella di Director, viene visualizzato un messaggio sulla console di Director, che consiglia l'aggiornamento del sito. Inoltre, finché la versione del sito è più vecchia di quella di Director, rimane visualizzata una nota nella dashboard di Director che indica questa mancata corrispondenza.

### Nota:

Le versioni precedenti di Citrix Director non visualizzano i criteri applicati alle sessioni utente in esecuzione su versioni dei VDA recenti. Citrix Director 1912 e versioni precedenti non visualizzano i criteri applicati alle sessioni utente in esecuzione su VDA versioni 2003 e successive. Utilizzare Citrix Director versioni 2003 e successive per visualizzare tali criteri.

Nella tabella seguente sono elencate le funzionalità specifiche di Director con la versione minima di Delivery Controller (DC), VDA e altri componenti dipendenti richiesti insieme alla License Edition:



| <b>Versione di Director</b> | <b>Funzione</b>                                                               | <b>Dipendenze -<br/>versione minima<br/>richiesta</b> | <b>Versione</b> |
|-----------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------|-----------------|
| 2311                        | Riproduci sessioni live e registrate                                          | VDA 2308 e DDC 2311                                   | Tutte           |
| 2311                        | Topologia della sessione                                                      | Nessuna                                               | Tutte           |
| 2311                        | Risoluzione dello schermo ottimale                                            | Nessuna                                               | Tutte           |
| 2311                        | Ottimizzazione MS Teams                                                       | VDA 2311 e DDC più recenti                            | Tutte           |
| 2311                        | Miglioramenti alla panoramica delle sonde                                     | Nessuna                                               | Tutte           |
| 2311                        | Visualizzazione rinnovata della durata dell'accesso alla sessione             | Nessuna                                               | Tutte           |
| 2308                        | Riepilogo dei probe e drill-down                                              | Nessuna                                               | Tutte           |
| 2308                        | Supporto Citrix Probe Agent per l'autenticazione a più fattori Citrix Gateway | Citrix Gateway                                        | Tutte           |
| 2308                        | Disattivare gli avvisi dell'Hypervisor                                        | Nessuna                                               | Tutte           |
| 2308                        | Tendenze per le metriche relative all'esperienza di sessione                  | Nessuna                                               | Tutte           |
| 2305                        | Supporta l'autenticazione tramite Citrix Gateway                              | Nessuna                                               | Tutte           |
| 2305                        | Gestione di Autoscale in Director                                             | Nessuna                                               | Tutte           |

| <b>Versione di Director</b> | <b>Funzione</b>                                                    | <b>Dipendenze -<br/>versione minima<br/>richiesta</b>          | <b>Versione</b> |
|-----------------------------|--------------------------------------------------------------------|----------------------------------------------------------------|-----------------|
| 2303                        | Avviso di macchine con errori                                      | DC 7 2303                                                      | Premium         |
| 2203                        | Supporto TLS 1.3                                                   | -                                                              | Tutte           |
| 2212                        | Utilizzo della GPU in tempo reale disponibile per le GPU AMD       | DC 7.14 e VDA 7.14 con Windows a 64 bit e HDX 3D Pro abilitati | Tutte           |
| 2212                        | Pianificazione avanzata del probe                                  | DC 7 1906 e Citrix Probe Agent 2209                            | Premium         |
| 1909                        | Configurazione di siti locali con Citrix Analytics for Performance | DC 7 1906 e VDA 1906                                           | Tutte           |
| 1906                        | Riconnessione automatica della sessione                            | DC 7 1906 e VDA 1906                                           | Tutte           |
| 1906                        | Durata dell'avvio della sessione                                   | DC 7 1906 e VDA 1903                                           | Tutte           |
| 1906                        | Probe dei desktop                                                  | DC 7 1906 e Citrix Probe Agent 1903                            | Premium         |
| 7.9 e versioni successive   | Durata di Profile Management Citrix nel caricamento del profilo    | VDA 1903                                                       | Tutte           |
| 1811                        | Drill-down del profilo                                             | DC 7 1811 e VDA 1811                                           | Tutte           |
| 1811                        | Monitoraggio degli avvisi dell'hypervisor                          | DC 7 1811                                                      | Premium         |
| 1811                        | Probe delle applicazioni                                           | DC 7 1811 e Citrix Application Probe Agent 1811                | Premium         |
| 1811                        | Stato licenza Servizi Desktop remoto Microsoft                     | DC 7 1811 e VDA 7.16                                           | Tutte           |

| <b>Versione di Director</b> | <b>Funzione</b>                                                     | <b>Dipendenze -<br/>versione minima<br/>richiesta</b> | <b>Versione</b>                       |
|-----------------------------|---------------------------------------------------------------------|-------------------------------------------------------|---------------------------------------|
| 1811                        | Visualizzazione dei dati RTOP chiave                                | DC 7 1811 e VDA 1808                                  | Premium                               |
| 1808                        | Esportazione dei dati dei filtri                                    | DC 7 1808                                             | Tutte                                 |
| 1808                        | Drill-down della sessione interattiva                               | DC 7 1808 e VDA 1808                                  | Tutte                                 |
| 1808                        | Drill-down dell'oggetto Criteri di gruppo                           | DC 7 1808 e VDA 1808                                  | Tutte                                 |
| 1808                        | Dati cronologici della macchina disponibili utilizzando l'API OData | DC 7 1808                                             | Tutte                                 |
| 7.18                        | Probe delle applicazioni                                            | DC 7.18                                               | Premium<br>(precedentemente Platinum) |
| 7.18                        | Criteri intelligenti per gli avvisi                                 | DC 7.18                                               | Premium<br>(precedentemente Platinum) |
| 7.18                        | Link Health Assistant                                               | Nessuna                                               | Tutte                                 |
| 7.18                        | Drill-down della sessione interattiva                               | Nessuna                                               | Tutte                                 |
| 7.17                        | Autenticazione smart card PIV                                       | Nessuna                                               | Tutte                                 |
| 7.16                        | Analisi delle applicazioni                                          | DC 7.16 e VDA 7.15                                    | Tutte                                 |
| 7.16                        | API OData V.4                                                       | DC 7.16                                               | Tutte                                 |
| 7.16                        | Shadowing degli utenti di VDA Linux                                 | VDA 7.16                                              | Tutte                                 |
| 7.16                        | Supporto dei gruppi locali di dominio                               | Nessuna                                               | Tutte                                 |
| 7.16                        | Accesso alla console della macchina                                 | DC 7.16                                               | Tutte                                 |

| <b>Versione di Director</b> | <b>Funzione</b>                                                                    | <b>Dipendenze -<br/>versione minima<br/>richiesta</b> | <b>Versione</b>                          |
|-----------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------|------------------------------------------|
| 7,15                        | Monitoraggio degli errori delle applicazioni                                       | DC 7.15 e VDA 7.15                                    | Tutte                                    |
| 7,14                        | Risoluzione dei problemi incentrata sulle applicazioni                             | DC 7.13 e VDA 7.13                                    | Tutte                                    |
| 7,14                        | Monitoraggio disco                                                                 | DC 7.14 e VDA 7.14                                    | Tutte                                    |
| 7,14                        | Monitoraggio GPU                                                                   | DC 7.14 e VDA 7.14                                    | Tutte                                    |
| 7.13                        | Protocollo di trasporto nel riquadro Session Details (Dettagli sessione)           | DC 7.x e VDA 7.13                                     | Tutte                                    |
| 7,12                        | Descrizioni in linguaggio accessibile degli errori di connessione e delle macchine | DC 7.12 e VDA 7.x                                     | Tutte                                    |
| 7,12                        | Maggiore disponibilità dei dati storici nella versione Enterprise                  | DC 7.12 e VDA 7.x                                     | Enterprise                               |
| 7,12                        | Reporting personalizzato                                                           | DC 7.12 e VDA 7.x                                     | Premium<br>(precedentemente<br>Platinum) |
| 7.11                        | Report sull'utilizzo delle risorse                                                 | DC 7.11 e VDA 7.11                                    | Tutte                                    |
| 7.11                        | Avvisi estesi per condizioni legate a CPU, memoria e tempo di round trip ICA       | DC 7.11 e VDA 7.11                                    | Premium<br>(precedentemente<br>Platinum) |
| 7.11                        | Miglioramenti dell'esportazione di report                                          | DC 7.11 e VDA 7.x                                     | Tutte                                    |

| <b>Versione di Director</b> | <b>Funzione</b>                                                                   | <b>Dipendenze -<br/>versione minima<br/>richiesta</b> | <b>Versione</b>                       |
|-----------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------|---------------------------------------|
| 7.11                        | <a href="#">Integrazione con Citrix ADM</a>                                       | DC 7.11, VDA 7.x e MAS versione 11.1 Build 49.16      | Premium<br>(precedentemente Platinum) |
| 7.9                         | <a href="#">Suddivisione della durata dell'accesso</a>                            | DC 7.9 e VDA 7.x                                      | Tutte                                 |
| 7.7                         | <a href="#">Monitoraggio e avvisi proattivi</a>                                   | DC 7.7 e VDA 7.x                                      | Premium<br>(precedentemente Platinum) |
| 7.7                         | <a href="#">Integrazione con autenticazione Windows</a>                           | DC 7.x e VDA 7.x                                      | Tutte                                 |
| 7.7                         | <a href="#">Utilizzo del sistema operativo a sessione singola e multisessione</a> | DC 7.7 e VDA 7.x                                      | Premium<br>(precedentemente Platinum) |
| 7.6.300                     | <a href="#">Supporto del canale virtuale Framehawk</a>                            | DC 7.6 e VDA 7.6                                      | Tutte                                 |
| 7.6.200                     | <a href="#">Integrazione della registrazione della sessione</a>                   | DC 7.6 e VDA 7.x                                      | Premium<br>(precedentemente Platinum) |
| 7                           | <a href="#">Integrazione di HDX Insight</a>                                       | DC 7.6, VDA 7.x e Citrix ADM                          | Premium<br>(precedentemente Platinum) |

## Cause di errori e risoluzione dei problemi di Citrix Director

November 5, 2024

Le tabelle seguenti descrivono le varie categorie di errori, i motivi e le azioni da intraprendere per risolvere i problemi. Per ulteriori informazioni, vedere [Enumerazioni, codici di errore e descrizioni](#).

## Errori di connessione

| Categoria          | Motivo                                              | Problema                                                                                                                                                                                                                                                                                                                                                 | Azione                                                                                                                                                                                                                                                                                                                                            |
|--------------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N/A                | [0] Unknown. Questo codice di errore non è mappato. | Il servizio di monitoraggio non è in grado di determinare il motivo dell'errore di avvio o connessione segnalato dalle informazioni condivise dal servizio Broker.                                                                                                                                                                                       | Raccogliere i log CDF sul controller e contattare il supporto Citrix.                                                                                                                                                                                                                                                                             |
| [0] None           | [1] None                                            | Nessuna                                                                                                                                                                                                                                                                                                                                                  | N/A                                                                                                                                                                                                                                                                                                                                               |
| [2] MachineFailure | [2] SessionPreparation                              | Richiesta di preparazione della sessione dal Delivery Controller al VDA non riuscita. Possibili cause: problemi di comunicazione tra il controller e il VDA, problemi riscontrati dal servizio Broker durante la creazione di una richiesta di preparazione o problemi di rete che determinano la mancata accettazione della richiesta da parte del VDA. | Per problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, <a href="#">Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops</a> . |
| [2] MachineFailure | [3] RegistrationTimeout                             | Il VDA era acceso, ma si è verificato un timeout durante il tentativo di registrazione con il Delivery Controller.                                                                                                                                                                                                                                       | Verificare che il servizio Broker Citrix sia in esecuzione sul Delivery Controller e che il servizio Desktop sia in esecuzione sul VDA. Se sono stati interrotti, avviarli.                                                                                                                                                                       |

| Categoria                    | Motivo                | Problema                                                                                                                                                                                                                                                                                                                                                                | Azione                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1] ClientConnection-Failure | [4] ConnectionTimeout | Il client non si è connesso al VDA dopo che il VDA è stato preparato per l'avvio della sessione. Il brokering della sessione è stato eseguito correttamente, ma si è verificato un timeout durante l'attesa che il client si connettesse al VDA. Possibili cause: impostazioni del firewall, interruzioni di rete o impostazioni che impediscono le connessioni remote. | Controllare la console di Director per verificare se il client ha attualmente una connessione attiva, il che significa che nessun utente ha subito conseguenze. Se non è presente alcuna sessione, esaminare i log eventi sul client e sul VDA per verificare la presenza di eventuali errori. Risolvere eventuali problemi di connettività di rete tra il client e il VDA. |
| [4] NoLicensesAvailable      | [5] Licensing         | La richiesta di licenza non è riuscita. Possibili cause: numero insufficiente di licenze o il server delle licenze è rimasto inattivo per più di 30 giorni.                                                                                                                                                                                                             | Verificare che il server delle licenze sia online e raggiungibile. Risolvere eventuali problemi relativi alla connettività di rete del server delle licenze o riavviare il server delle licenze in caso di errato funzionamento. Verificare che ci siano licenze sufficienti nell'ambiente e assegnarne altre se necessario.                                                |

| Categoria                    | Motivo        | Problema                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1] ClientConnection-Failure | [6] Ticketing | Si è verificato un errore durante la creazione di ticket, il che indica che la connessione client al VDA non corrisponde alla richiesta di cui è stato eseguito il brokering. Un ticket di richiesta di avvio viene preparato dal Broker e consegnato nel file ICA. Quando l'utente tenta di avviare una sessione, il VDA convalida il ticket di avvio nel file ICA con il Broker. Possibili cause: il file ICA è danneggiato o l'utente sta tentando di stabilire una connessione non autorizzata. | Verificare che l'utente abbia accesso all'applicazione o al desktop in base ai gruppi di utenti definiti nei gruppi di consegna. Chiedere all'utente di riavviare l'applicazione o il desktop per determinare se si tratta di un problema temporaneo. Se il problema si verifica di nuovo, esaminare i log eventi del dispositivo client per rilevare eventuali errori. Verificare che il VDA a cui l'utente sta tentando di connettersi sia registrato. Se non è registrato, rivedere i log eventi sul VDA e risolvere eventuali problemi di registrazione. |
| [1] ClientConnection-Failure | [7] Other     | Una sessione è stata segnalata come terminata dal VDA dopo che il client ha inizialmente contattato il VDA ma prima che completasse la sequenza di connessione.                                                                                                                                                                                                                                                                                                                                     | Verificare se la sessione non è stata terminata dall'utente prima dell'avvio. Provare a riavviare la sessione, se il problema persiste, raccogliere i log CDF e contattare il supporto Citrix.                                                                                                                                                                                                                                                                                                                                                               |



| Categoria                    | Motivo                   | Problema                                                                                                                                                                                                                                                         | Azione                                                                                                                                                                                                                        |
|------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1] ClientConnection-Failure | [8] GeneralFail          | La sessione non è stata avviata. Possibili cause: è stato richiesto un avvio di cui è stato eseguito il brokering mentre il Broker si stava ancora avviando o inizializzando, oppure si è verificato un errore interno durante la fase di brokering di un avvio. | Verificare che il servizio Broker Citrix sia in esecuzione e riprovare ad avviare la sessione.                                                                                                                                |
| [5] Configuration            | [9] MaintenanceMode      | Il VDA, o il gruppo di consegna a cui appartiene il VDA, è configurato in modalità di manutenzione.                                                                                                                                                              | Determinare se la modalità di manutenzione è necessaria. Disabilitare la modalità di manutenzione sul gruppo di consegna o sulla macchina in questione se non è necessaria e chiedere all'utente di tentare di riconnettersi. |
| [5] Configuration            | [10] ApplicationDisabled | Gli utenti finali non possono accedere all'applicazione perché è stata disabilitata dall'amministratore.                                                                                                                                                         | Se l'applicazione è destinata a essere disponibile per l'uso in produzione, abilitarla e chiedere all'utente di riconnettersi.                                                                                                |

| Categoria                  | Motivo                         | Problema                                                                                                                                                                                                                                                                                                                            | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [4]<br>NoLicensesAvailable | [11] LicenseFeature<br>Refused | La funzionalità utilizzata non è coperta dalle licenze esistenti.                                                                                                                                                                                                                                                                   | Contattare un rappresentante commerciale Citrix per confermare le funzionalità coperte dalla versione e dal tipo di licenza Citrix Virtual Apps and Desktops esistenti.                                                                                                                                                                                                                                                                                                                                                                 |
| [3]<br>NoCapacityAvailable | [13]<br>SessionLimitReached    | Tutti i VDA sono in uso e non è disponibile capacità per ospitare altre sessioni. Possibili cause: tutti i VDA sono in uso (per i VDA con sistema operativo a sessione singola) oppure tutti i VDA hanno raggiunto il numero massimo di sessioni simultanee configurate consentito (per i VDA con sistema operativo multisessione). | Verificare se sono presenti VDA in modalità di manutenzione. Disabilitare la modalità di manutenzione se non è necessaria, per liberare più capacità. È consigliabile aumentare il valore di <b>Maximum Number of Sessions</b> (Numero massimo di sessioni) nell'impostazione dei criteri Citrix per consentire più sessioni per i VDA del server. Prendere in considerazione l'aggiunta di altri VDA con sistema operativo multisessione. Prendere in considerazione l'aggiunta di altri VDA con sistema operativo a sessione singola. |

| Categoria         | Motivo                      | Problema                                                                                                                                                                                                                                                                                                                                                                                                                            | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [5] Configuration | [14]<br>DisallowedProtocol  | I protocolli ICA e RDP non sono consentiti.                                                                                                                                                                                                                                                                                                                                                                                         | Eseguire il comando PowerShell <b>Get-BrokerAccessPolicyRule</b> sul Delivery Controller e verificare che il valore <b>AllowedProtocols</b> (Protocolli consentiti) disponga di tutti i protocolli desiderati. Questo problema si verifica solo in caso di errata configurazione.                                                                                                                                                                                                        |
| [5] Configuration | [15]<br>ResourceUnavailable | L'applicazione o il desktop a cui l'utente sta tentando di connettersi non è disponibile. L'applicazione o il desktop potrebbe non esistere o non sono disponibili VDA per l'esecuzione. Possibili cause: l'applicazione o il desktop non sono stati pubblicati o i VDA che ospitano l'applicazione o il desktop hanno raggiunto il carico massimo oppure l'applicazione o il desktop sono configurati in modalità di manutenzione. | Verificare che l'applicazione o il desktop siano ancora pubblicati e che i VDA non siano in modalità di manutenzione. Determinare se i VDA con sistema operativo multisessione sono a pieno carico. In tal caso, eseguire il provisioning di più VDA con sistema operativo multisessione. Verificare che siano disponibili VDA con sistema operativo a sessione singola per le connessioni. Se necessario, eseguire il provisioning di più VDA con sistema operativo a sessione singola. |

---

| Categoria          | Motivo                              | Problema                                                                                                                                                                                                                           | Azione                                                                                                                                                                                                                                                                                        |
|--------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [5] Configuration  | [16] ActiveSessionReconnectDisabled | La sessione ICA è attiva e connessa a un endpoint diverso. Tuttavia, poiché l'opzione <b>Active Session Reconnection</b> (Riconnessione della sessione attiva) è disabilitata, il client non può connettersi alla sessione attiva. | Sul Delivery Controller, verificare che l'opzione <b>Active Session Reconnection</b> (Riconnessione della sessione attiva) sia abilitata. Verificare che il valore di <b>DisableActiveSessionReconnect</b> nel Registro di sistema, in <b>HKEY_LOCAL_MACHINE\Software</b> sia impostato su 0. |
| [2] MachineFailure | [17] NoSessionToReconnect           | Il client ha tentato di riconnettersi a una sessione specifica, ma la sessione è stata terminata.                                                                                                                                  | Riprovare la riconnessione del controllo dell'area di lavoro.                                                                                                                                                                                                                                 |

| Categoria          | Motivo            | Problema                                                                                                                                                         | Azione                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [2] MachineFailure | [18] SpinUpFailed | Il VDA non può essere acceso per l'avvio della sessione. Si tratta di un problema segnalato dall'hypervisor.                                                     | Se la macchina è ancora spenta, provare ad avviarla da Citrix Studio. Se l'operazione non riesce, esaminare la connettività e le autorizzazioni dell'hypervisor. Se il VDA è una macchina con provisioning PVS, verificare nella console PVS che la macchina sia in esecuzione. In caso contrario, verificare che alla macchina sia assegnato un Personal vDisk, accedere all'hypervisor per reimpostare la VM. |
| [2] MachineFailure | [19] Refused      | Il Delivery Controller invia una richiesta al VDA per prepararsi a una connessione da parte di un utente finale, ma il VDA rifiuta attivamente questa richiesta. | Verificare tramite ping che il Delivery Controller e il VDA possano comunicare correttamente. In caso contrario, risolvere eventuali problemi di firewall o di routing di rete.                                                                                                                                                                                                                                 |

| Categoria               | Motivo                         | Problema                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Azione                                                                                                                                                                                                                                                     |
|-------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [2] MachineFailure      | [20] ConfigurationSet Failure  | Il Delivery Controller non ha inviato al VDA i dati di configurazione richiesti, come le impostazioni dei criteri e le informazioni sulla sessione, durante l'avvio della sessione.<br>Possibili cause:<br>problemi di comunicazione tra il controller e il VDA, problemi riscontrati dal servizio Broker durante la creazione di una richiesta di impostazione della configurazione o problemi di rete che determinano la mancata accettazione della richiesta da parte del VDA. | -                                                                                                                                                                                                                                                          |
| [3] NoCapacityAvailable | [21] MaxTotalInstancesExceeded | È stato raggiunto il numero massimo di istanze di un'applicazione. Non è possibile aprire istanze aggiuntive dell'applicazione sul VDA. Questo problema è correlato alla funzionalità dei limiti dell'applicazione.                                                                                                                                                                                                                                                               | Prendere in considerazione l'aumento dell'impostazione dell'applicazione <b>Limit the number of instances running at the same time</b> (Limita il numero di istanze in esecuzione contemporaneamente) su un valore più elevato, se la licenza lo consente. |

| Categoria                    | Motivo                           | Problema                                                                                                                                                                                                                                               | Azione                                                                                                                                                                                                                                                                                                                     |
|------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [3]<br>NoCapacityAvailable   | [22] MaxPerUserInstancesExceeded | L'utente sta tentando di aprire più istanze di un'applicazione, ma l'applicazione è configurata per consentire solo una singola istanza dell'applicazione per utente. Questo problema è correlato alla funzionalità dei limiti dell'applicazione.      | Per impostazione predefinita, è consentita solo un'istanza dell'applicazione per utente. Se sono necessarie più istanze per utente, prendere in considerazione la possibilità di deselezionare l'impostazione <b>Limit to one instance per user</b> (Limita a un'istanza per utente) nelle impostazioni dell'applicazione. |
| [1] ClientConnection-Failure | [23] Communication error         | Il Delivery Controller ha tentato di inviare informazioni al VDA, ad esempio una richiesta di preparazione per una connessione, ma si è verificato un errore durante il tentativo di comunicazione. Ciò può essere causato da interruzioni della rete. | Se è già avviato, riavviare il servizio Desktop sul VDA per riavviare il processo di registrazione e verificare che il VDA si registri correttamente. Verificare che i Delivery Controller configurati per il VDA siano accurati tramite i dettagli nel log eventi dell'applicazione.                                      |

---

| Categoria                  | Motivo                                                                                                                  | Problema                                                                                                                                                                                                                                                                                                                                                                                                         | Azione                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [3]<br>NoCapacityAvailable | [100]<br>NoMachineAvailable Il servizio di monitoraggio converte [12]<br>NoDesktopAvailable in questo codice di errore. | Il VDA assegnato per avviare la sessione è in uno stato non valido o non è disponibile. Possibili cause: lo stato di alimentazione del VDA è sconosciuto o non disponibile, il VDA non è stato riavviato dall'ultima sessione dell'utente, la condivisione della sessione è disabilitata mentre la sessione corrente richiede che sia abilitata oppure il VDA è stato rimosso dal gruppo di consegna o dal sito. | Verificare che il VDA si trovi in un gruppo di consegna. In caso contrario, aggiungerlo al gruppo di consegna appropriato. Verificare che vi siano sufficienti VDA registrati e pronti per poter avviare il desktop condiviso pubblicato o l'applicazione richiesta dall'utente. Verificare che l'hypervisor che ospita il VDA non sia in modalità di manutenzione. |



| Categoria          | Motivo                                                                                                               | Problema                                                                                                                                                                                                         | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [2] MachineFailure | [101] MachineNotFunctional. Il servizio di monitoraggio converte [12] NoDesktopAvailable in questo codice di errore. | Il VDA non è operativo. Possibili cause: il VDA è stato rimosso dal gruppo di consegna, il VDA non è registrato, lo stato di alimentazione del VDA non è disponibile o il VDA sta riscontrando problemi interni. | Verificare che il VDA si trovi in un gruppo di consegna. In caso contrario, aggiungerlo al gruppo di consegna appropriato. Verificare che il VDA venga visualizzato come acceso in Citrix Studio. Se lo stato di alimentazione è sconosciuto per più macchine, risolvere eventuali problemi relativi alla connettività all' hypervisor o agli errori dell' host. Verificare che l' hypervisor che ospita il VDA non sia in modalità di manutenzione. Riavviare il VDA una volta risolti questi problemi. |

### Tipo di guasto della macchina

| Codice di errore              | ID codice di errore | Problema | Azione |
|-------------------------------|---------------------|----------|--------|
| Unknown (Sconosciuto)         | -                   | -        | -      |
| Unregistered (Non registrato) | 3                   | -        | -      |

| Codice di errore                                            | ID codice di errore | Problema                                                                                 | Azione                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------|---------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MaxCapacity<br>(rappresentato come<br>Max Load su Director) | 4                   | La macchina segnala se stessa alla massima capacità, ad esempio Indice di carico massimo | Assicurarsi che tutti gli hypervisor siano accesi. Aggiungere altre macchine ai Delivery Group interessati aggiungendo più capacità all'hypervisor o aggiungendo altri hypervisor.                                                                                                             |
| StuckOnBoot (Blocco all'avvio)                              | 2                   | La VM non ha completato la sequenza di avvio e non comunica con l'hypervisor.            | Assicurarsi che la VM sia stata avviata correttamente sull'hypervisor. Controllare la presenza di altri messaggi sulla VM, ad esempio problemi del sistema operativo. Assicurarsi che gli strumenti dell'hypervisor siano installati sulla VM. Assicurarsi che il VDA sia installato sulla VM. |
| FailedToStart<br>(Impossibile avviare)                      | 1                   | La VM ha riscontrato problemi durante il tentativo di avviare l'hypervisor.              | Controllare i log dell'hypervisor.                                                                                                                                                                                                                                                             |
| Nessuna                                                     | 0                   | -                                                                                        | -                                                                                                                                                                                                                                                                                              |

**Motivo della cancellazione della registrazione della macchina (applicabile quando il tipo di errore è Unregistered [Non registrato] o Unknown [Sconosciuto])**

---

| Codice di errore                                | ID codice di errore | Problema                                                                                                                         | Azione                                                                                                                                                                                               |
|-------------------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AgentShutdown<br>(Spegnimento dell'agente)      | 0                   | Il VDA ha sperimentato un arresto normale.                                                                                       | Accendere il VDA se non si prevede che sia spento, in base ai criteri di gestione dell'alimentazione esistenti. Esaminare eventuali errori nei log eventi.                                           |
| AgentSuspended<br>(Agente sospeso)              | 1                   | Il VDA è in modalità di ibernazione o sospensione.                                                                               | Far uscire il VDA dalla modalità di ibernazione. Prendere in considerazione la disabilitazione dell'ibernazione per i VDA Citrix Virtual Apps and Desktops tramite le impostazioni di alimentazione. |
| IncompatibleVersion<br>(Versione incompatibile) | 100                 | Il VDA non può comunicare con il Delivery Controller a causa di una mancata corrispondenza nelle versioni del protocollo Citrix. | Allineare le versioni del VDA e del Delivery Controller.                                                                                                                                             |

| Codice di errore                                                                 | ID codice di errore | Problema                                                                         | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------|---------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AgentAddressResolutionFailed<br>(Risoluzione dell'indirizzo agente non riuscita) | 101                 | Il Delivery Controller non è stato in grado di risolvere l'indirizzo IP del VDA. | Verificare che l'account della macchina VDA esista in AD. In caso contrario, crearlo. Verificare che il nome e l'indirizzo IP del VDA nel DNS siano accurati. In caso contrario, correggerli. Se il problema è diffuso, convalidare le impostazioni DNS sui Delivery Controller. Verificare la risoluzione DNS dal controller eseguendo il comando <code>nslookup</code> .<br>Verificare che l'account della macchina VDA esista in AD. In caso contrario, crearlo. Verificare che il nome e l'indirizzo IP del VDA nel DNS siano accurati. In caso contrario, correggerli. |

---

| Codice di errore                                 | ID codice di errore | Problema                                                                          | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------|---------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AgentNotContactable<br>(Agente non contattabile) | 102                 | Si è verificato un problema di comunicazione tra il Delivery Controller e il VDA. | Utilizzare un comando ping per verificare che il Delivery Controller e il VDA siano in grado di comunicare correttamente. In caso contrario, risolvere eventuali problemi del firewall o di rete. Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, <a href="#">Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668)</a> . |

| Codice di errore                                                         | ID codice di errore | Problema                                                                                                                                                                                                                                                           | Azione                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                          | 102                 | Si è verificato un problema di comunicazione tra il Delivery Controller e il VDA.                                                                                                                                                                                  | Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, <a href="#">Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668)</a> . Contattare il supporto Citrix. |
| AgentWrongActiveDirectory<br>(UO di Active Directory dell'agente errata) | 103U                | Si è verificato un errore di configurazione del rilevamento di Active Directory. L'unità organizzativa specifica del sito (dove le informazioni del controller del sito sono memorizzate in AD) configurata nel Registro di sistema del VDA è per un sito diverso. | Assicurarsi che la configurazione di Active Directory sia corretta o controllare le impostazioni del Registro di sistema.                                                                                                                                                                                                                                                                      |
| EmptyRegistrationRequest<br>(Richiesta di registrazione vuota)           | 104                 | La richiesta di registrazione inviata dal VDA al Directory Controller era vuota. Ciò può essere dovuto a un'installazione del software VDA corrotta.                                                                                                               | Riavviare il servizio Desktop sul VDA per riavviare il processo di registrazione e verificare che il VDA si registri correttamente tramite il log eventi dell'applicazione.                                                                                                                                                                                                                    |

| Codice di errore                                                                                    | ID codice di errore | Problema                                                                                                                                                                                                                                                                                                            | Azione                                                                                       |
|-----------------------------------------------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| MissingRegistrationCapabilities<br>(Funzionalità di registrazione mancanti)                         | 105                 | La versione del VDA non è compatibile con il Delivery Controller.                                                                                                                                                                                                                                                   | Aggiornare il VDA o rimuovere il VDA e quindi reinstallarlo.                                 |
| MissingAgentVersion<br>(Versione agente mancante)                                                   | 106                 | La versione del VDA non è compatibile con il Delivery Controller.                                                                                                                                                                                                                                                   | Reinstallare il software VDA se il problema riguarda tutte le macchine.                      |
| InconsistentRegistrationCapabilities<br>(Funzionalità di registrazione incoerenti)                  | 107                 | Il VDA non è in grado di comunicare le proprie funzionalità al Broker. Ciò può essere dovuto all'incompatibilità tra le versioni del VDA e del Delivery Controller. Le funzionalità di registrazione, che cambiano con ogni versione, sono espresse in un modo che non corrisponde alla richiesta di registrazione. | Allineare le versioni del VDA e del Delivery Controller.                                     |
| NotLicensedForFeature<br>(Funzionalità non concessa in licenza)                                     | 108                 | La funzionalità che si sta cercando di utilizzare non è concessa in licenza.                                                                                                                                                                                                                                        | Controllare la versione delle licenze Citrix oppure rimuovere il VDA e quindi reinstallarlo. |
|                                                                                                     | 108                 | La funzionalità che si sta cercando di utilizzare non è concessa in licenza.                                                                                                                                                                                                                                        | Contattare il supporto Citrix.                                                               |
| UnsupportedCredentialSecurityVersion<br>(Versione della sicurezza delle credenziali non supportata) | 109                 | Il VDA e il Delivery Controller non utilizzano lo stesso meccanismo di crittografia.                                                                                                                                                                                                                                | Allineare le versioni del VDA e del Delivery Controller.                                     |

| Codice di errore                                                                     | ID codice di errore | Problema                                                                                                                  | Azione                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InvalidRegistrationRequest<br>(Richiesta di registrazione non valida)                | 110                 | Il VDA ha inviato una richiesta di registrazione al Broker, ma il contenuto della richiesta è danneggiato o non è valido. | Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, <a href="#">Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668)</a> . |
| SingleMultiSessionMismatch<br>(Mancata corrispondenza multisessione singola)         | 111                 | Il tipo di sistema operativo del VDA non è compatibile con il catalogo delle macchine o il gruppo di consegna.            | Aggiungere il VDA al tipo di catalogo delle macchine o al gruppo di consegna corretto contenente macchine con lo stesso sistema operativo.                                                                                                                                                                                                                      |
| FunctionalLevelTooLowForCatalog<br>(Livello funzionale troppo basso per il catalogo) | 112                 | Il catalogo delle macchine è impostato su un livello funzionale VDA superiore rispetto alla versione di VDA installata.   | Verificare che il livello funzionale del catalogo delle macchine del VDA corrisponda a quello del VDA. Aggiornare il catalogo delle macchine o eseguirne il downgrade in modo che corrisponda a quello del VDA.                                                                                                                                                 |



| Codice di errore                                                                                | ID codice di errore | Problema                                                                                                                                                                                                                                     | Azione                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FunctionalLevelTooLowForDesktopGroup<br>(Livello funzionale troppo basso per il gruppo desktop) | 110                 | Il gruppo di consegna è impostato su un livello funzionale del VDA superiore rispetto alla versione di VDA installata.                                                                                                                       | Verificare che il livello funzionale del gruppo di consegna del VDA corrisponda a quello del VDA. Aggiornare il catalogo delle macchine o eseguirne il downgrade in modo che corrisponda a quello del VDA.                                                                                                          |
| PowerOff<br>(Spegnimento)                                                                       | 200                 | Il VDA non si è chiuso correttamente.                                                                                                                                                                                                        | Se il VDA deve essere acceso, provare ad avviare il VDA da Citrix Studio e verificare che si avvii e si registri correttamente.<br>Risolvere gli eventuali problemi di avvio o registrazione.<br>Esaminare i log eventi sul VDA una volta eseguito il backup per determinare la causa principale dello spegnimento. |
| AgentRejectedSettingsUpdate<br>(Aggiornamento delle impostazioni rifiutato dall'agente)         | 201                 | Impostazioni come i criteri Citrix sono state modificate o aggiornate, ma si è verificato un errore nell'invio degli aggiornamenti al VDA. Ciò può verificarsi se gli aggiornamenti non sono compatibili con la versione del VDA installata. | Se necessario, aggiornare il VDA. Controllare se gli aggiornamenti applicati sono supportati con la versione del VDA.                                                                                                                                                                                               |

| Codice di errore                                                 | ID codice di errore | Problema                                                                                                   | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SessionPrepareFailure<br>(Errore di preparazione della sessione) | 206                 | Il Broker non ha completato un controllo delle sessioni in esecuzione sul VDA.                             | Se il problema è diffuso, riavviare il servizio Broker Citrix sul Delivery Controller.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                                                  | 206                 | Il Broker non ha completato un controllo delle sessioni in esecuzione sul VDA.                             | Contattare il supporto Citrix.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ContactLost (Perdita di contatto)                                | 207                 | Il Delivery Controller ha perso la connessione con il VDA. Ciò può essere causato da interruzioni di rete. | Verificare che il servizio Broker Citrix sia in esecuzione sul Delivery Controller e che il servizio Desktop sia in esecuzione sul VDA. Se sono stati interrotti, avviarli. Se è già avviato, riavviare il servizio Desktop sul VDA per riavviare il processo di registrazione e verificare che il VDA si registri correttamente. Verificare che i Delivery Controller configurati per il VDA siano accurati tramite i dettagli nel log eventi dell'applicazione. Utilizzare un comando ping per verificare che il Delivery Controller e il VDA siano in grado di comunicare correttamente. In caso contrario, risolvere eventuali problemi del firewall o di rete. |

| Codice di errore                                                                 | ID codice di errore | Problema                                                                                                                                                                                                                          | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                  | 207                 | Il Delivery Controller ha perso la connessione con il VDA. Ciò può essere causato da interruzioni di rete.                                                                                                                        | Verificare che il servizio Desktop sia in esecuzione sul VDA. Se è interrotto, avviarlo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| BrokerRegistrationLimitReached<br>(Limite di registrazione del Broker raggiunto) | 201                 | Il Delivery Controller ha raggiunto il numero massimo configurato di VDA a cui è consentito di registrarsi contemporaneamente. Per impostazione predefinita, il Delivery Controller consente 10.000 registrazioni VDA simultanee. | Prendere in considerazione l'aggiunta di Delivery Controller al sito o la creazione di un sito. È inoltre possibile aumentare il numero di VDA autorizzati a registrarsi contemporaneamente con il Delivery Controller tramite la chiave del Registro di sistema <b>HKEY_LOCAL_MACHINE\Software</b> .<br>Per ulteriori informazioni, vedere l'articolo del Knowledge Center <a href="#">Chiavi del Registro di sistema utilizzate da Citrix Virtual Apps and Desktops (CTX117446)</a> .<br>L'aumento di questo numero potrebbe richiedere più risorse di CPU e memoria per il controller. |

| Codice di errore                                                       | ID codice di errore | Problema                                                                                                                                                                                            | Azione                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SettingsCreationFailure<br>(Errore di creazione<br>delle impostazioni) | 208                 | Il Broker non ha creato una serie di impostazioni e configurazioni da inviare al VDA. Se il Broker non è in grado di raccogliere i dati, la registrazione non riesce e il VDA non viene registrato. | Controllare i log eventi sul Delivery Controller per verificare la presenza di eventuali errori. Riavviare il servizio Broker se i log non indicano un problema specifico. Una volta riavviato il servizio Broker, riavviare il servizio Desktop sui VDA interessati e verificare che si registrino correttamente. |
|                                                                        | 208                 | Il Broker non ha creato una serie di impostazioni e configurazioni da inviare al VDA. Se il Broker non è in grado di raccogliere i dati, la registrazione non riesce e il VDA non viene registrato. | Riavviare il servizio Desktop sui VDA interessati e verificare che si registrino correttamente. Contattare il supporto Citrix.                                                                                                                                                                                     |

| Codice di errore                                            | ID codice di errore | Problema                                                                                                                                                                         | Azione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SendSettingsFailure<br>(Errore di invio delle impostazioni) | 204                 | Il Broker non ha inviato impostazioni e dati di configurazione al VDA. Se il Broker è in grado di raccogliere i dati ma non è in grado di inviarli, la registrazione non riesce. | Se è limitato a un singolo VDA, riavviare il servizio Desktop sul VDA per forzare una nuova registrazione e verificare che il VDA si registri correttamente tramite il log eventi dell'applicazione. Risolvere eventuali errori riscontrati. Per i problemi comuni che causano problemi di comunicazione tra il controller e il VDA, vedere la procedura di risoluzione dei problemi elencati nell'articolo del Knowledge Center, <a href="#">Risoluzione dei problemi relativi alla registrazione di Virtual Delivery Agent con i Delivery Controller in Citrix Virtual Apps and Desktops (CTX136668)</a> . |
| AgentRequested<br>(Agente richiesto)                        | 2                   | Si è verificato un errore sconosciuto.                                                                                                                                           | Contattare il supporto Citrix.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| DesktopRestart<br>(Riavvio del desktop)                     | 201                 | Si è verificato un errore sconosciuto.                                                                                                                                           | Contattare il supporto Citrix.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| DesktopRemoved<br>(Desktop rimosso)                         | 202                 | Si è verificato un errore sconosciuto.                                                                                                                                           | Contattare il supporto Citrix.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SessionAuditFailure<br>(Errore di controllo della sessione) | 205                 | Si è verificato un errore sconosciuto.                                                                                                                                           | Contattare il supporto Citrix.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| UnknownError (Errore sconosciuto)                           | 300                 | Si è verificato un errore sconosciuto.                                                                                                                                           | Contattare il supporto Citrix.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Codice di errore                                                                   | ID codice di errore | Problema                               | Azione                         |
|------------------------------------------------------------------------------------|---------------------|----------------------------------------|--------------------------------|
| RegistrationStateMismatch<br>(Mancata corrispondenza dello stato di registrazione) | 102                 | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |
| Unknown<br>(Sconosciuto)                                                           | -                   | Si è verificato un errore sconosciuto. | Contattare il supporto Citrix. |

## SDK e API

November 5, 2024

Con questa versione sono disponibili diversi SDK e API. Per accedere agli SDK e alle API, andare a [Creare qualsiasi cosa con Citrix](#). Da lì, selezionare **Citrix Workspace** per accedere alle informazioni di programmazione per Citrix Virtual Apps and Desktops e ai relativi componenti.

### Nota:

Citrix Virtual Apps and Desktops SDK e Citrix Group Policy SDK possono essere installati come modulo o snap-in. Diversi SDK componenti (come Citrix Licensing, Citrix Provisioning e Store-Front) vengono installati utilizzando solo uno snap-in.

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

## Citrix Virtual Apps and Desktops SDK

Questo SDK viene installato automaticamente come modulo PowerShell quando si installa un Delivery Controller o Studio. Ciò consente di utilizzare i cmdlet di questo SDK senza dover aggiungere snap-in. Se si sceglie di installare questo SDK come snap-in, le istruzioni sono fornite di seguito.

## Autorizzazioni

È necessario eseguire la shell o lo script utilizzando un'identità con diritti di amministrazione Citrix. Sebbene i membri del gruppo di amministratori locali sul controller abbiano automaticamente privilegi amministrativi completi per consentire l'installazione di Citrix Virtual Apps o Citrix Virtual Desktops, Citrix consiglia di creare amministratori Citrix con i diritti appropriati per le normali attività, anziché utilizzare l'account degli amministratori locali.

## Accedere ai cmdlet ed eseguirli

1. Avviare una shell in PowerShell: aprire Studio, selezionare la scheda **PowerShell** e quindi fare clic su **Launch PowerShell** (Avvia PowerShell).
2. Per utilizzare i cmdlet SDK all'interno degli script, impostare il criterio di esecuzione in PowerShell. Per ulteriori informazioni sui criteri di esecuzione di PowerShell, vedere la documentazione Microsoft.
3. Se si desidera utilizzare lo snap-in (anziché il modulo), aggiungere lo snap-in utilizzando il cmdlet `Add-PSSnapin` (o `asnp`).

V1 e V2 indicano la versione dello snap-in. Gli snap-in di XenDesktop 5 corrispondono alla versione 1. Citrix Virtual Apps and Desktops e le versioni precedenti di XenDesktop 7 corrispondono alla versione 2. Ad esempio, per installare lo snap-in Citrix Virtual Apps and Desktops, digitare `Add-PSSnapin Citrix.ADIIdentity.Admin.V2`. Per importare tutti i cmdlet, digitare: `Add-PSSnapin Citrix.*.Admin.V*`

È ora possibile utilizzare i cmdlet e i file della guida.

- Per accedere ai file della guida per questo SDK, selezionare il prodotto o il componente nell'elenco [Categories](#) (Categorie), quindi selezionare **Citrix Virtual Apps and Desktops SDK** (SDK Citrix Virtual Apps and Desktops).
- Per informazioni su PowerShell, vedere [Ambiente di script integrato di Windows PowerShell \(ISE\)](#).

## SDK Group Policy

L'SDK Citrix Group Policy consente di visualizzare e configurare le impostazioni e i filtri dei Criteri di gruppo. Questa SDK utilizza un provider PowerShell per creare un'unità virtuale corrispondente alle impostazioni e ai filtri della macchina e dell'utente. Il provider appare come un'estensione di [New-PSDrive](#).

Per utilizzare l'SDK Group Policy, è necessario installare l'SDK di Studio o Citrix Virtual Apps and Desktops.

Il provider Citrix Group Policy PowerShell è disponibile come modulo o come snap-in.

- Per utilizzare il modulo, non è necessaria alcuna operazione aggiuntiva.
- Per aggiungere lo snap-in, digitare `Add-PSSnapin citrix.common.grouppolicy`.

Per accedere alla guida, digitare: `help New-PSDrive -path localgpo:/.`

Per creare un'unità virtuale e caricarla con le impostazioni, digitare `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` dove la

stringa Controller è il nome di dominio completo di un Controller nel sito a cui si desidera connettersi e da cui caricare le impostazioni.

## **API REST di Citrix Virtual Apps and Desktops**

Con le API REST di Citrix Virtual Apps and Desktops, è possibile automatizzare la gestione delle risorse all'interno di una distribuzione di Citrix Virtual Apps and Desktops.

Le API REST di Citrix Virtual Apps and Desktops sono disponibili all'indirizzo <https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>. Le API non applicabili a Citrix Virtual Apps and Desktops sono contrassegnate di conseguenza. Seguire le indicazioni riportate qui per configurare l'accesso al servizio API e utilizzare le API per gestire e ottimizzare le risorse.

## **Monitor Service OData**

L'API Monitor consente l'accesso ai dati del servizio di monitoraggio utilizzando la versione 3 o 4 dell'API OData. È possibile creare dashboard di monitoraggio e reportistica personalizzate in base ai dati interrogati dai dati del servizio di monitoraggio. OData V.4 si basa sull'[API Web ASP.NET](#) e supporta le query di aggregazione.

Per ulteriori informazioni, vedere l'[API Monitor Service OData](#).





© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.