



Gestione

Virtual Desktop Service

NetApp
May 24, 2023

This PDF was generated from https://docs.netapp.com/it-it/virtual-desktop-service/Management.Deployments.provisioning_collections.html on May 24, 2023. Always check docs.netapp.com for the latest.

Sommario

- Gestione 1
 - Implementazioni 1
 - Applicazioni 16
 - Eventi con script 29
 - Command Center 37
 - Ottimizzazione delle risorse 45
 - User Administration (Amministrazione utente) 48
 - Amministrazione del sistema 59

Gestione

Implementazioni

Raccolte di provisioning

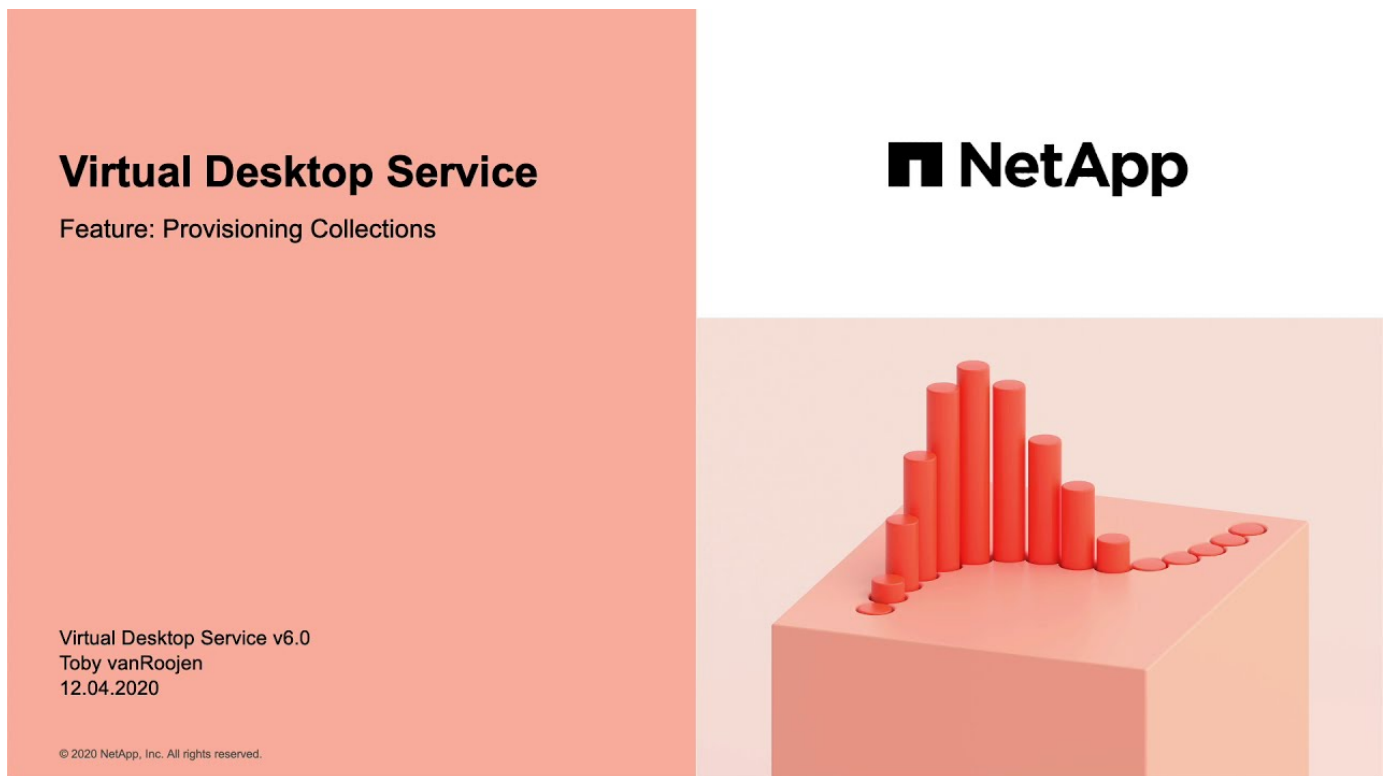
Panoramica

Provisioning Collections è una funzione di VDS correlata alla creazione e alla gestione delle immagini delle macchine virtuali.

A livello generale, il flusso di lavoro di Provisioning Collection è il seguente:

1. Una macchina virtuale temporanea (ad esempio "CWT1") viene creata in base a un'immagine esistente (un'immagine stock o una raccolta di provisioning precedentemente salvata).
2. L'amministratore VDS personalizza la macchina virtuale temporanea in base ai requisiti utilizzando ["Eventi con script"](#), ["Connettersi al server"](#) e/o strumenti di gestione di terze parti.
3. Una volta personalizzata, l'amministratore VDS fa clic su **Validate** e avvia un processo di convalida che automatizza la finalizzazione dell'immagine, esegue SysPrep, elimina la macchina virtuale temporanea e rende l'immagine disponibile per l'implementazione in VDS.

Video Demo - Gestione delle immagini delle macchine virtuali per gli host di sessione VDI



Tipi di raccolta provisioning

Esistono due tipi distinti di raccolta con casi di utilizzo specifici, **Shared** e **VDI**.

Condiviso

Il tipo **Shared** è una raccolta di immagini di macchine virtuali progettate per implementare un intero ambiente con più immagini di macchine virtuali e ruoli di macchine virtuali distinti.

VDI

Il tipo **VDI** è una singola immagine della macchina virtuale progettata per essere utilizzata e riutilizzata per implementare più macchine virtuali identiche, generalmente utilizzate per l'hosting di sessioni utente. Per tutti i tipi di host di sessione AVD, è necessario selezionare il tipo **VDI**, anche per gli host che eseguono più sessioni per macchina virtuale.

Creazione di una nuova raccolta di provisioning

Le raccolte di provisioning si trovano nell'interfaccia VDS all'interno di ogni implementazione, nella sottoscheda **Provisioning Collections**.

[larghezza=75%]

Per creare una nuova raccolta

1. Fare clic sul pulsante **+ Aggiungi raccolta**.
2. Compilare i seguenti campi:
 - a. **Nome**
 - b. **Descrizione**(opzionale)
 - c. **Type** - Shared o VDI
 - d. **Sistema operativo**
 - e. **Share Drive** - se questa macchina virtuale verrà utilizzata per ospitare i profili degli utenti o i dati di condivisione dell'azienda, scegliere la lettera dell'unità su cui verrà ospitata. In caso contrario, lasciare il campo "C"
 - f. **Minimum cache** (cache minima) - SE si desidera creare macchine virtuali da conservare per l'implementazione istantanea, specificare il numero minimo di macchine virtuali memorizzate nella cache da mantenere. Se l'implementazione di nuove macchine virtuali può attendere fino a quando l'hypervisor richiede la creazione di una macchina virtuale, è possibile impostarla su "0" per risparmiare sui costi.
 - g. **Aggiungi server**
 - i. **Role** (se è selezionato il tipo "Shared")
 - A. **TS** - questa macchina virtuale agirà solo come host di sessione
 - B. **Dati** - questa macchina virtuale non ospiterà sessioni utente
 - C. **TSDData** - questa VM sarà sia l'host di sessione che l'host di storage (massimo: Un TSDData per spazio di lavoro)
 - ii. **VM Template** (modello VM): Selezionare dall'elenco Available (disponibili), sia le immagini dell'hypervisor di stock che le raccolte di provisioning salvate in precedenza.
 - A. NOTA: Le immagini di Windows 7 da Azure Marketplace non hanno PowerShell Remoting attivato. Per utilizzare un'immagine di Windows 7, è necessario fornire un'immagine personalizzata nella galleria di immagini condivisa con PowerShell Remoting attivato.
 - B. NOTA: Utilizzando una Provisioning Collection esistente, è possibile aggiornare e ridistribuire le immagini esistenti come parte di un processo di aggiornamento dell'immagine pianificato.

- iii. **Storage Type** (tipo di storage): Consente di selezionare la velocità del disco del sistema operativo in base a costi e performance
- iv. **Unità dati** - facoltativamente, abilitare un secondo disco collegato a questa immagine, in genere per il livello di storage dei dati di cui sopra al punto 2.e.
 - A. **Data Drive Type** (tipo di unità dati) - consente di selezionare la velocità del secondo disco (dati) in base a costi e prestazioni
 - B. **Data Drive Size (GB)** (dimensione unità dati): Consente di definire le dimensioni del secondo disco (dati) in base a capacità, costi e performance
- h. **Add Applications** (Aggiungi applicazioni) - selezionare qualsiasi applicazione dalla libreria applicazioni che verrà (1) installata su questa immagine e (2) gestita dai diritti dell'applicazione VDS. (Valido solo per implementazioni RDS. Deve rimanere vuoto per le aree di lavoro AVD)

Personalizzazione della macchina virtuale temporanea

VDS include funzionalità che consentono di rimuovere l'accesso alle macchine virtuali dall'interfaccia Web di VDS. Per impostazione predefinita, viene creato un account amministratore locale di Windows con una password rotante e trasmesso alla macchina virtuale, consentendo all'amministratore locale di VDS di accedere senza la necessità di conoscere le credenziali di amministratore locale.



La funzione Connect to Server (connessione al server) dispone di un'impostazione alternativa in cui all'amministratore VDS verrà richiesto di immettere le credenziali per ogni connessione. Questa impostazione può essere attivata/disattivata modificando l'account admin VDS dalla sezione "Admin" di VDS. La funzionalità è denominata *Tech account* e selezionando la casella sarà necessario immettere le credenziali quando si utilizza Connect to Server; deselezionando questa casella si attiva l'inserimento automatico delle credenziali amministrative di Windows locali a ogni connessione.

L'amministratore VDS deve semplicemente connettersi alla macchina virtuale temporanea utilizzando Connect to Server (connessione al server) o un altro processo e apportare le modifiche necessarie per soddisfare i propri requisiti.

Convalida della raccolta

Una volta completata la personalizzazione, l'amministratore VDS può chiudere l'immagine e SysPrep facendo clic su **Validate** dall'icona Actions (azioni).

[Management.Deployments.provisioning collezioni ed97e] |

Utilizzo della raccolta

Una volta completata la convalida, lo stato della raccolta di provisioning diventerà **disponibile**. Dall'interno di Provisioning Collection, l'amministratore VDS può identificare il nome **VM Template** utilizzato per identificare questa raccolta di provisioning in VDS.

[Management.Deployments.provisioning collezioni f5a49] |

Nuovo server

Dalla pagina Workspace > Servers (Area di lavoro > Server), è possibile creare un nuovo server e la finestra di dialogo richiederà di specificare il modello di macchina virtuale. Il nome del modello riportato sopra si trova in questo elenco:

[larghezza=75%]



VDS offre un modo semplice per aggiornare gli host di sessione in un ambiente RDS utilizzando Provisioning Collections e la funzionalità **Add Server**. Questo processo può essere eseguito senza impatto sugli utenti finali e ripetuto più volte con i successivi aggiornamenti delle immagini, basandosi sulle iterazioni delle immagini precedenti. Per un flusso di lavoro dettagliato su questo processo, vedere "[Processo di aggiornamento dell'host di sessione RDS](#)" di seguito.

Nuovo pool di host AVD

Dalla pagina Workspace > AVD > host Pools (Area di lavoro > AVD > Pool host), è possibile creare un nuovo pool di host AVD facendo clic su **+ Add host Pool** (Aggiungi pool host) e la finestra di dialogo richiederà il modello di macchina virtuale. Il nome del modello riportato sopra si trova in questo elenco:

[Management.Deployments.provisioning collezioni ba2f5] |

Nuovi host di sessione AVD

Dalla pagina Workspace > AVD > host Pool > Session hosts (Area di lavoro > AVD > Pool host di sessione > host di sessione), è possibile creare nuovi host di sessione AVD facendo clic su **+ Add Session host** (Aggiungi host di sessione) e la finestra di dialogo richiederà il modello di macchina virtuale. Il nome del modello riportato sopra si trova in questo elenco:

[Management.Deployments.provisioning collezioni ba5e9] |



VDS offre un modo semplice per aggiornare gli host di sessione in un pool di host AVD utilizzando Provisioning Collections e la funzionalità **Add Session host**. Questo processo può essere eseguito senza impatto sugli utenti finali e ripetuto più volte con i successivi aggiornamenti delle immagini, basandosi sulle iterazioni delle immagini precedenti. Per un flusso di lavoro dettagliato su questo processo, vedere "[Processo di aggiornamento dell'host di sessione AVD](#)" di seguito.

Nuova area di lavoro

Dalla pagina Workspaces, è possibile creare una nuova area di lavoro facendo clic su **+ New Workspace** (Nuova area di lavoro) e la finestra di dialogo richiederà la raccolta di provisioning. Il nome della Shared Provisioning Collection si trova in questo elenco.

[Management.Deployments.provisioning collezioni 5c941] |

Nuova raccolta di provisioning

Dalla pagina Deployment > Provisioning Collection (implementazione > raccolta provisioning), è possibile creare una nuova raccolta di provisioning facendo clic su **+ Add Collection (Aggiungi raccolta)**. Quando si aggiungono server a questa raccolta, la finestra di dialogo richiede di specificare il modello di macchina virtuale. Il nome del modello riportato sopra si trova in questo elenco:

[Management.Deployments.provisioning collezioni 9eac4] |

Addendum 1 - host di sessione RDS

Processo di aggiornamento dell'host di sessione RDS

VDS offre un modo semplice per aggiornare gli host di sessione in un ambiente RDS utilizzando Provisioning Collections e la funzionalità **Add Server**. Questo processo può essere eseguito senza impatto sugli utenti finali e ripetuto più volte con i successivi aggiornamenti delle immagini, basandosi sulle iterazioni delle immagini precedenti.

Il processo di aggiornamento dell'host di sessione RDS è il seguente:

1. Creare una nuova raccolta di provisioning VDI, personalizzare e convalidare la raccolta seguendo le istruzioni riportate sopra.
 - a. In genere, questa raccolta di provisioning verrà costruita sul modello di macchina virtuale precedente, emulando un processo "Apri, Salva con nome".
2. Una volta convalidata la Provisioning Collection, accedere alla pagina *Workspace* > *Servers*, quindi fare clic su **+ Add Server** (Aggiungi server)

[Management.Deployments.provisioning_collections.rds session ospita e8204] |

3. Selezionare **TS** come **ruolo server**
4. Selezionare l'ultimo **modello di macchina virtuale**. Effettuare le selezioni appropriate **Machine Size** (dimensioni macchina) e **Storage Type** (tipo di storage) in base alle proprie esigenze. Lasciare deselezionato **Data Drive**.
5. Ripetere questa operazione per il numero totale di host di sessione richiesti per l'ambiente.
6. Fare clic su **Add Server** (Aggiungi server) per creare gli host di sessione in base al modello di macchina virtuale selezionato e iniziare a essere online entro 10-15 minuti (a seconda dell'hypervisor).
 - a. Tenere presente che gli host di sessione attualmente presenti nell'ambiente verranno infine dismessi dopo che questi nuovi host saranno stati messi in linea. Pianificare la creazione di un numero sufficiente di nuovi host per supportare l'intero carico di lavoro in questo ambiente.
7. Quando un nuovo host viene online, l'impostazione predefinita è rimanere in **non consentire nuove sessioni**. Per ciascun host di sessione, è possibile utilizzare il pulsante di attivazione **Allow New Sessions** (Consenti nuove sessioni) per gestire gli host che possono ricevere nuove sessioni utente. È possibile accedere a questa impostazione modificando le impostazioni di ogni singolo server host di sessione. Una volta creato un numero sufficiente di nuovi host e confermata la funzionalità, questa impostazione può essere gestita sia sul nuovo host che su quello precedente per instradare tutte le nuove sessioni ai nuovi host. I vecchi host, con l'opzione **Allow New Sessions** (Consenti nuove sessioni) impostata su **Disabled**, possono continuare a eseguire e ospitare le sessioni utente esistenti.

[Management.Deployments.provisioning_collections.rds_session_hosts 726d1] |

8. Man mano che gli utenti si disconnetteranno dai vecchi host e senza nuove sessioni utente che si uniranno ai vecchi host, è possibile eliminare i vecchi host in cui **sessioni = 0** facendo clic sull'icona **azioni** e selezionando **elimina**.

[Management.Deployments.provisioning_collections.rds_session_hosts 45d32] |

Addendum 2 - host di sessione AVD

Processo di aggiornamento dell'host di sessione AVD

VDS offre un modo semplice per aggiornare gli host di sessione in un pool di host AVD utilizzando Provisioning Collections e la funzionalità **Add Session host**. Questo processo può essere eseguito senza impatto sugli utenti finali e ripetuto più volte con i successivi aggiornamenti delle immagini, basandosi sulle iterazioni delle immagini precedenti.

Il processo di aggiornamento di AVD Session host è il seguente:

1. Creare una nuova raccolta di provisioning VDI, personalizzare e convalidare la raccolta seguendo le istruzioni riportate sopra.
 - a. In genere, questa raccolta di provisioning verrà costruita sul modello di macchina virtuale precedente, emulando un processo "Apri, Salva con nome".
2. Una volta convalidata la Provisioning Collection, accedere alla pagina *Workspace > AVD > host Pools* e fare clic sul nome del pool di host
3. Dalla pagina *host Pool > Session hosts*, fare clic su **+ Add Session host** (Aggiungi host sessione)

[Management.Deployments.provisioning collezioni 9ed95] |

4. Selezionare l'ultimo **modello di macchina virtuale**. Effettuare le selezioni appropriate **Machine Size** (dimensioni macchina) e **Storage Type** (tipo di storage) in base alle proprie esigenze.
5. Inserire il **numero di istanze** corrispondente al numero totale di host di sessione richiesti. In genere, questo numero corrisponde a quello attualmente presente nel pool di host, ma può essere qualsiasi numero.
 - a. Tenere presente che gli host di sessione attualmente presenti nel pool di host verranno infine dismessi dopo che il nuovo host sarà stato messo in linea. Pianificare che il **numero di istanze** immesso sia sufficiente a supportare l'intero carico di lavoro in questo pool di host.
6. Fare clic su **Save** (Salva) per creare gli host di sessione in base al modello di macchina virtuale selezionato e iniziare a essere online entro 10-15 minuti (a seconda dell'hypervisor).
7. Quando un nuovo host viene online, l'impostazione predefinita è rimanere in **non consentire nuove sessioni**. Per ciascun host di sessione, è possibile utilizzare il pulsante di attivazione **Allow New Sessions** (Consenti nuove sessioni) per gestire gli host che possono ricevere nuove sessioni utente. Una volta creato un numero sufficiente di nuovi host e confermata la funzionalità, questa impostazione può essere gestita sia sul nuovo host che su quello precedente per instradare tutte le nuove sessioni ai nuovi host. I vecchi host, con l'opzione **Allow New Sessions** (Consenti nuove sessioni) impostata su **Disabled**, possono continuare a eseguire e ospitare le sessioni utente esistenti.

[Management.Deployments.provisioning collezioni be47e] |

8. Man mano che gli utenti si disconnetteranno dai vecchi host e senza nuove sessioni utente che si uniranno ai vecchi host, è possibile eliminare i vecchi host in cui **sessioni = 0** facendo clic sull'icona **azioni** e selezionando **elimina**.

[Management.Deployments.provisioning collezioni cefb9] |

Panoramica della gerarchia logica VDS

Panoramica

VDS organizza i concetti in vari livelli di una gerarchia logica. Questo articolo aiuta a delineare il modo in cui si combinano.

Schema organizzativo VDS

Il portale di gestione VDS si trova all'indirizzo <https://manage.vds.netapp.com>. Questa interfaccia Web è un singolo pannello di controllo per la gestione di tutti gli oggetti correlati a VDS. All'interno dell'interfaccia utente Web VDS, esiste la seguente gerarchia di componenti e contenitori logici.

Implementazione VDS

Il concetto di *implementazione* è un VDS che ha organizzato e contiene *aree di lavoro VDS*. In alcune architetture di implementazione, un'implementazione può contenere più spazi di lavoro VDS.



L'esecuzione di più aree di lavoro VDS in una singola implementazione è chiamata "multi-tenancy" ed è solo un'opzione nelle implementazioni RDS, le implementazioni AVD non supportano questo approccio.

Un'implementazione viene definita dal relativo dominio Active Directory e esiste una relazione 1:1 tra il dominio ad e un'implementazione.

Alcune risorse di macchine virtuali vengono implementate per supportare un'implementazione condivisa in tutte le aree di lavoro VDS nell'implementazione. Ad esempio, ogni implementazione contiene una macchina virtuale denominata "CWMGR1" che è un server che esegue applicazioni VDS, un database SQL Express e facilita la gestione delle aree di lavoro VDS (e delle risorse contenute) all'interno dell'implementazione.

Area di lavoro VDS



Esiste una differenza tra un "**VDS** Workspace" e un "**AVD** Workspace".

Un'area di lavoro VDS è un contenitore logico all'interno dell'implementazione per le risorse del client (utente finale). Queste risorse includono macchine virtuali (per host di sessione, server di applicazioni, server di database, file server ecc.), reti virtuali, storage e altra infrastruttura hypervisor.

VDS Workspace contiene inoltre funzionalità di gestione per gestire utenti, gruppi di sicurezza, workload Scheduling, applicazioni, automazione, VM e configurazione AVD.

In genere, un'area di lavoro VDS è allineata a una singola azienda o (nelle implementazioni aziendali) a una business unit.

Siti VDS

All'interno di un'implementazione, è possibile creare più siti per rappresentare diversi provider di infrastruttura, tutti gestiti all'interno di un'unica implementazione.

Ciò è utile quando una singola azienda o business unit deve ospitare utenti e applicazioni in più sedi fisiche (ad esempio Nord America e EMEA), abbonamenti hypervisor (per allineare i costi alle business unit) e persino

hypervisor (ad esempio utenti di Azure, Google Compute e HCI on-premise su vSphere).

Aree di lavoro AVD



Esiste una differenza tra un **"VDS Workspace"** e un **"AVD Workspace"**.

Un'area di lavoro AVD è un contenitore logico che si trova all'interno di un'area di lavoro VDS e di un sito VDS. Può essere utilizzato in modo simile a un sito VDS per segmentare le policy di gestione e operative nella stessa implementazione.

Pool di host AVD

I pool di host AVD sono contenitori logici che si trovano all'interno di un'area di lavoro AVD e tengono in attesa gli utenti degli host di sessione e dei gruppi di applicazioni per gestire le sessioni dell'utente e controllare l'accesso alle singole risorse.

Gruppi di applicazioni AVD

Ogni pool di host AVD inizia con un singolo gruppo di applicazioni "Desktop". Gli utenti e/o i gruppi possono essere assegnati a questo (o altro) App Group per consentire l'accesso alle risorse dell'App Group agli utenti assegnati.

È possibile creare ulteriori gruppi di applicazioni all'interno di un pool di host in VDS. Tutti gli altri gruppi di applicazioni sono gruppi di applicazioni "RemoteApp" e offrono risorse RemoteApp invece di un'esperienza desktop Windows completa.

Applicazioni

Diritti dell'applicazione

Panoramica

VDS dispone di un'efficace funzionalità integrata di autorizzazione e automazione delle applicazioni. Questa funzionalità consente agli utenti di accedere a diverse applicazioni durante la connessione agli stessi host di sessione. Ciò è possibile grazie ad alcuni oggetti Criteri di gruppo personalizzati che nascondono i collegamenti insieme all'automazione che posiziona i collegamenti in modo selettivo sui desktop degli utenti.



Questo flusso di lavoro si applica solo alle implementazioni RDS. Per la documentazione relativa ai diritti dell'applicazione AVD, vedere ["Application Entitlement Workflow per AVD"](#)

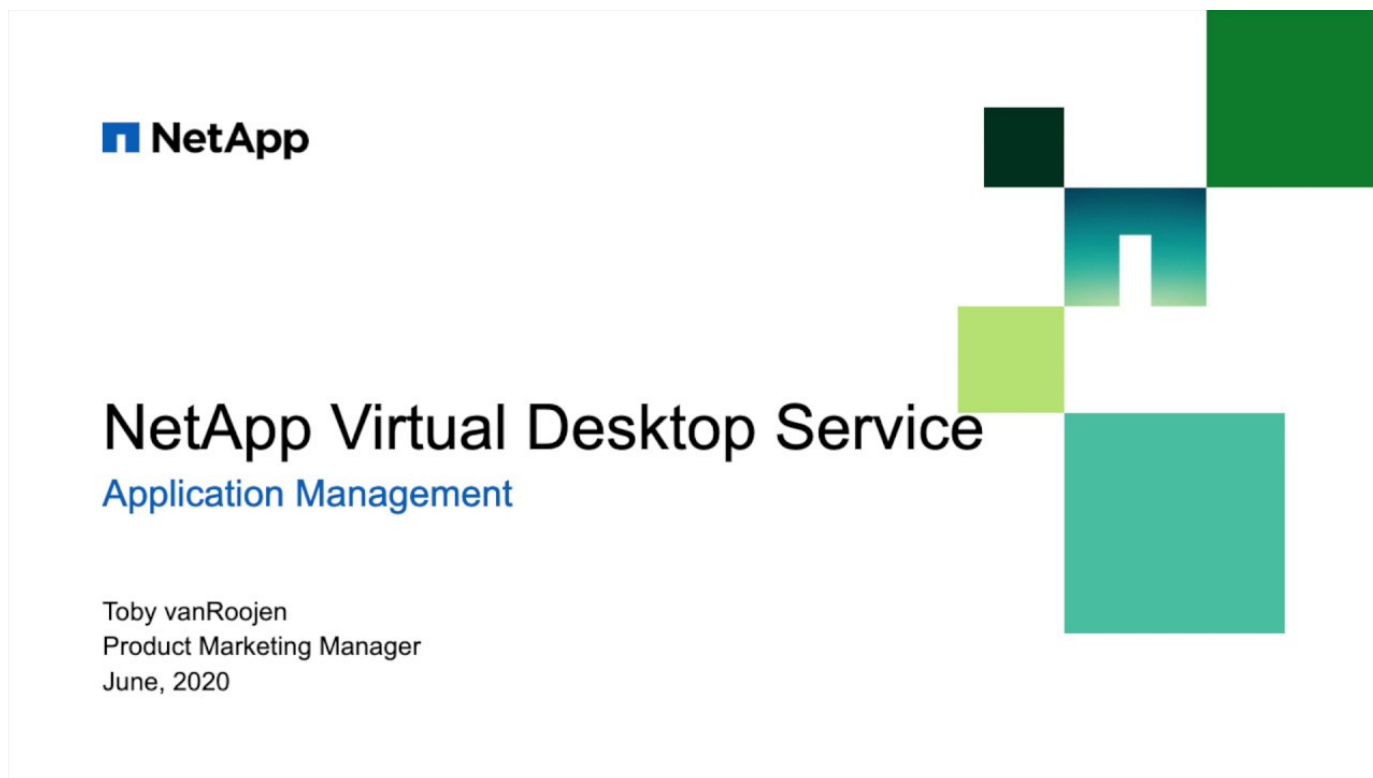
Le applicazioni possono essere assegnate agli utenti direttamente o tramite gruppi di sicurezza gestiti in VDS.

Ad alto livello, il processo di provisioning dell'applicazione segue questi passaggi.

1. Aggiungi app all'App Catalog
2. Aggiungi app all'area di lavoro
3. Installare l'applicazione su tutti gli host di sessione
4. Selezionare il percorso di scelta rapida
5. Assegnare le applicazioni a utenti e/o gruppi



I passaggi 3 e 4 possono essere completamente automatizzati con gli eventi con script, come illustrato di seguito



Video - Panoramica

Aggiungere applicazioni all'App Catalog

VDS Application Entitlement inizia con App Catalog, un elenco di tutte le applicazioni disponibili per l'implementazione negli ambienti degli utenti finali.

Per aggiungere applicazioni al catalogo, procedere come segue

1. Accedere a VDS all'indirizzo <https://manage.cloudworkspace.com> utilizzando le credenziali di amministratore principali.
2. In alto a destra, fare clic sull'icona a forma di freccia accanto al nome utente e selezionare Impostazioni.
3. Fare clic sulla scheda App Catalog.
4. Fare clic sull'opzione Add App (Aggiungi applicazione) nella barra del titolo del catalogo applicazioni.
5. Per aggiungere un gruppo di applicazioni, selezionare l'opzione Importa applicazioni.
 - a. Viene visualizzata una finestra di dialogo che fornisce un modello Excel da scaricare che crea il formato corretto per l'elenco delle applicazioni.
 - b. Per questa valutazione, NetApp VDS ha creato un elenco di applicazioni di esempio per l'importazione, disponibile qui.
 - c. Fare clic sull'area Upload (carica) e scegliere il file di modello dell'applicazione, quindi fare clic sul pulsante Import (Importa).
6. Per aggiungere singole applicazioni, selezionare il pulsante Add App (Aggiungi applicazione) per visualizzare una finestra di dialogo.
 - a. Inserire il nome dell'applicazione.

- b. L'ID esterno può essere utilizzato per inserire un identificativo di tracciamento interno, ad esempio una SKU di prodotto o un codice di tracciamento della fatturazione (opzionale).
- c. Selezionare la casella di controllo Subscription (abbonamento) se si desidera creare un report sulle applicazioni come prodotto in abbonamento (opzionale).
- d. Se il prodotto non viene installato in base alla versione (ad esempio Chrome), selezionare la casella di controllo versione non richiesta. In questo modo è possibile installare i prodotti con aggiornamenti continui senza tenere traccia delle loro versioni.
- e. Al contrario, se un prodotto supporta più versioni con nome (ad esempio QuickBooks), selezionare questa casella per installare più versioni e avere VDS specifico per ciascuna versione disponibile nell'elenco delle applicazioni che possono avere diritto e per l'utente finale.
- f. Selezionare l'opzione "Nessuna icona di desktop utente" se non si desidera che VDS provi un'icona di desktop per questo prodotto. Viene utilizzato per prodotti "back-end" come SQL Server, poiché gli utenti finali non dispongono di un'applicazione a cui accedere.
- g. "L'app deve essere associata" impone la necessità di installare un'app associata. Ad esempio, un'applicazione client server potrebbe richiedere l'installazione di SQL Server o MySQL.
- h. Selezionando la casella licenza richiesta, VDS deve richiedere il caricamento di un file di licenza per un'installazione dell'applicazione prima di impostare lo stato dell'applicazione su attivo. Questa fase viene eseguita nella pagina Application Detail di VDS.
- i. Visibile a tutti: I diritti dell'applicazione possono essere limitati a specifici partner secondari in una gerarchia multicanale. A scopo di valutazione, fare clic sulla casella di controllo in modo che tutti gli utenti possano visualizzarla nell'elenco delle applicazioni disponibili.

Aggiungere l'applicazione all'area di lavoro

Per avviare il processo di implementazione, aggiungerai l'applicazione allo spazio di lavoro.

Per eseguire questa operazione, attenersi alla seguente procedura

1. Fare clic su aree di lavoro
2. Scorrere verso il basso fino ad applicazioni
3. Fare clic su Aggiungi
4. Selezionare le applicazioni, inserire le informazioni richieste, fare clic su Add Application (Aggiungi applicazione), quindi su Add Apps (Aggiungi applicazioni).

Installare manualmente l'applicazione

Una volta aggiunta l'applicazione all'area di lavoro, è necessario installarla su tutti gli host di sessione. Questa operazione può essere eseguita manualmente e/o può essere automatizzata.

Per installare manualmente le applicazioni sugli host di sessione, attenersi alla seguente procedura

1. Accedere a Service Board (scheda di servizio).
2. Fare clic sull'attività del Service Board.
3. Fare clic sui nomi dei server per connettersi come amministratore locale.
4. Installare le applicazioni, verificare che il collegamento a questa applicazione si trovi nel percorso del menu Start.
 - a. Per Server 2016 e Windows 10: C: ProgramData/Microsoft/Windows/Menu Start/programmi.
5. Tornare all'attività del Service Board, fare clic su Browse (Sfoglia) e scegliere il collegamento o una cartella contenente i collegamenti.

6. Qualsiasi opzione selezionata viene visualizzata sul desktop dell'utente finale quando viene assegnata l'applicazione.
7. Le cartelle sono eccezionali quando un'applicazione è in realtà costituita da più applicazioni. Ad esempio, "Microsoft Office" è più semplice da implementare come cartella con ogni applicazione come collegamento all'interno della cartella.
8. Fare clic su completa installazione.
9. Se necessario, aprire l'icona creata Add Service Board Task (Aggiungi attività Service Board) e confermare che l'icona è stata aggiunta.

Assegnare le applicazioni agli utenti

Il diritto all'applicazione viene gestito da VDS e l'applicazione può essere assegnata agli utenti in tre modi

Assegnare le applicazioni agli utenti

1. Accedere alla pagina User Detail (Dettagli utente).
2. Accedere alla sezione applicazioni.
3. Selezionare la casella accanto a tutte le applicazioni richieste dall'utente.

Assegnare gli utenti a un'applicazione

1. Accedere alla sezione applicazioni della pagina Dettagli area di lavoro.
2. Fare clic sul nome dell'applicazione.
3. Selezionare la casella accanto agli utenti dell'applicazione.

Assegnare applicazioni e utenti ai gruppi di utenti

1. Accedere ai dettagli di utenti e gruppi.
2. Aggiungere un nuovo gruppo o modificare un gruppo esistente.
3. Assegnare utenti e applicazioni al gruppo.

Application Entitlement Workflow per AVD

Panoramica

In un ambiente Azure Virtual Desktop (AVD), l'accesso alle applicazioni viene gestito dall'appartenenza al gruppo di applicazioni.



Questo flusso di lavoro si applica solo alle implementazioni AVD. Per la documentazione relativa ai diritti dell'applicazione RDS, vedere ["Application Entitlement Workflow per RDS"](#)



AVD è un servizio ben documentato e CE ne sono molti ["risorse pubbliche per l'informazione"](#). VDS non esegue il sovrareseed del modo di funzionamento standard di AVD. Piuttosto, questo articolo è stato progettato per illustrare come VDS si avvicina al concetto standard presente in tutte le implementazioni AVD.



Analisi di ["Panoramica della gerarchia logica VDS"](#) articolo può essere utile prima o durante la revisione di questo articolo.

Visualizzazione per l'utente finale

In Azure Virtual Desktop, a ciascun utente finale viene assegnato l'accesso a RemoteApp e/o Desktop dal proprio amministratore AVD. Questa operazione viene eseguita tramite l'assegnazione di App Group in VDS.

RemoteApp si riferisce a un'applicazione che viene eseguita in remoto sull'host di sessione ma viene presentata sul dispositivo locale senza il contesto del desktop. Comunemente chiamata "applicazione per lo streaming", queste applicazioni assommano a un'applicazione locale sul dispositivo locale, ma vengono eseguite nel contesto di sicurezza e sul livello di storage e calcolo dell'host di sessione.

Desktop si riferisce all'esperienza Windows completa in esecuzione sull'host di sessione e presentata sul dispositivo locale, in genere in una finestra a schermo intero. Comunemente chiamato "desktop remoto", questo desktop contiene tutte le applicazioni installate su tale host di sessione che possono essere avviate dall'utente dalla finestra della sessione del desktop.

Al momento dell'accesso, all'utente finale vengono visualizzate le risorse assegnate dall'amministratore. Di seguito è riportato un esempio della vista che un utente finale potrebbe visualizzare quando accede al proprio client AVD. Si tratta di un esempio più complesso, spesso un utente finale dispone solo di un desktop dingle o RemoteApp assegnati. L'utente finale può fare doppio clic su una di queste risorse per avviare l'applicazione o il desktop.

[Management.Deployments.vds Sites 0e49c] | *Management.Deployments.vds_sites-0e49c.png*

In questo esempio più complesso, questo utente ha accesso a due sessioni desktop diverse e a 4 diverse applicazioni di streaming:

- **Desktop disponibili**
 - Desktop NVIDIA GPU
 - Desktop condiviso AVD Pool
 - Desktop Pool Operation 2
- **RemoteApp disponibili**
 - AutoCAD 2021
 - Revit 2021
 - Microsoft Edge
 - Blocco note

Dietro le quinte, queste applicazioni e desktop sono ospitati in una vasta gamma di host di sessione e aree di lavoro AVD e possono persino essere ospitati in diverse regioni di Azure.

Di seguito è riportato un diagramma che illustra la posizione di hosting di ciascuna di queste risorse e il modo in cui sono state assegnate a questo utente finale.

[Management.Deployments.vds Sites 0e880] | *Management.Deployments.vds_sites-0e880.png*

Come illustrato in precedenza, le varie risorse disponibili per questo utente finale sono ospitate in diversi host di sessione, in diversi pool di host e potenzialmente gestite da diverse organizzazioni IT in diversi spazi di lavoro AVD. Anche se non viene mostrato in questo esempio, queste risorse potrebbero essere ospitate in diverse aree Azure e/o sottoscrizioni utilizzando la funzione Siti VDS.

Accesso al desktop

Per impostazione predefinita, ogni pool di host inizia con un singolo gruppo di applicazioni, utilizzato per assegnare l'accesso all'esperienza desktop di Windows. Tutte le applicazioni installate su questi host di sessione saranno accessibili agli utenti finali assegnati a questo gruppo di applicazioni.

Per abilitare la risorsa Desktop per gli utenti in VDS:

1. Accedere alla pagina Workspaces > AVD > host Pool > App Groups (aree di lavoro > AVD > Pool host > gruppi di applicazioni) e fare clic sul gruppo di applicazioni per la risorsa "Desktop".

[Management.Applications.avd application titlement workflow 349fe] |

Management.Applications.avd_application_entitlement_workflow-349fe.png

2. Una volta all'interno dell'App Group, fare clic su Edit (Modifica)

[Management.Applications.avd application entitlement workflow 3bcfc] |

Management.Applications.avd_application_entitlement_workflow-3bcfc.png

3. Dalla finestra di dialogo di modifica, è possibile aggiungere o rimuovere utenti a questo gruppo di applicazioni per utente e/o per gruppo.

[Management.Applications.avd application entitlement workflow 07ff0] |

Accesso RemoteApp

Per eseguire il provisioning dell'accesso a RemoteApps, è necessario creare un nuovo gruppo di applicazioni all'interno del pool di host. Una volta create, le applicazioni appropriate devono essere assegnate a questo gruppo di applicazioni.



Tutte le applicazioni su questi host di sessione saranno già disponibili per tutti gli utenti assegnati all'appgroup "Desktop" di questo pool di host. Non è necessario fornire l'accesso anche tramite un gruppo di applicazioni RemoteApp semplicemente per fornire l'accesso alle applicazioni. Un gruppo di applicazioni RemoteApp è necessario solo per consentire l'accesso alle applicazioni che vengono eseguite come se sul dispositivo locale come un'applicazione di streaming.

Creare un nuovo gruppo di applicazioni

1. Accedere alla pagina Workspace > AVD > host Pool > App Groups (aree di lavoro > AVD > Pool host > gruppi di applicazioni) e fare clic sul pulsante + *Add App Group* (Aggiungi gruppo di applicazioni)

[Management.Applications.avd application entitlement workflow d33da] |

Management.Applications.avd_application_entitlement_workflow-d33da.png

2. Immettere il nome, l'area di lavoro e il nome descrittivo per questo gruppo di applicazioni. Selezionare gli utenti e/o i gruppi da assegnare e fare clic su *Save* (Salva)

[Management.Applications.avd application entitlement workflow 242eb] |

Aggiungere applicazioni all'App Group

1. Accedere alla pagina Workspace > AVD > host Pool > App Groups (aree di lavoro > AVD > Pool host > gruppi di applicazioni) e fare clic sul gruppo di applicazioni per la risorsa "RemoteApp".

[Gestione.applicazioni.avd application entitlement workflow 3dcde] |

Management.Applications.avd_application_entitlement_workflow-3dcde.png

2. Una volta all'interno dell'App Group, fare clic su Edit (Modifica)

[Management.Applications.avd application entitlement workflow 27a41] |

Management.Applications.avd_application_entitlement_workflow-27a41.png

3. Scorrere verso il basso fino alla sezione "Remote Apps" (applicazioni remote). La compilazione di questa sezione potrebbe richiedere qualche istante, poiché VDS sta eseguendo direttamente una query agli host di sessione per mostrare le applicazioni disponibili per lo streaming.

[Management.Applications.avd_application_titlement_workflow 1e9f2] |

4. Cercare e selezionare le applicazioni a cui gli utenti di questo gruppo di applicazioni devono accedere come risorsa RemoteApp.

Eventi con script

Eventi con script

Panoramica

Gli eventi con script forniscono all'amministratore avanzato un meccanismo per creare un'automazione personalizzata per la manutenzione del sistema, gli avvisi degli utenti, la gestione dei criteri di gruppo o altri eventi. Gli script possono essere progettati per essere eseguiti come un processo eseguibile con argomenti o possono essere utilizzati come argomenti per un programma eseguibile diverso. Questa funzionalità consente di combinare e nidificare gli script per supportare complesse esigenze di personalizzazione e integrazione.

Un esempio dettagliato di eventi con script in azione è disponibile in ["Guida ai diritti dell'applicazione"](#).

Inoltre, Scripted Events consente la creazione di un'automazione che non richiede l'elaborazione di uno script, ma il flusso di automazione viene avviato da un trigger di sistema ed esegue un programma o un'utilità di sistema esistente con argomenti opzionali.

Script Eventi contiene sia un **repository** di script che **attività**. Gli script contengono le istruzioni su **cosa** fare mentre le attività collegano gli script con il trigger e la destinazione appropriati (**quando e dove**) per lo script.

Repository

La scheda Repository mostra un elenco di tutti gli script disponibili per la distribuzione dall'account VDS. Si tratta di un repository personalizzato condiviso da tutti gli amministratori dell'istanza VDS. L'accesso agli eventi con script può essere gestito nella pagina *VDS > Admins > Permissions*.

[Sub.Management.Scripted Events.Scripted events 1ce76] |

Filtro cliente

Ogni organizzazione di amministratori VDS dispone di una libreria privata di script creati e/o personalizzati dalla propria organizzazione. Questi script sono definiti come tipo di script "cliente". Gli script dei clienti possono essere cancellati e modificati da qualsiasi amministratore VDS con autorizzazioni amministrative appropriate per la sezione Scripted Events.

Filtro globale

NetApp pubblica e gestisce anche una libreria di script "globali" che è la stessa per tutte le organizzazioni di amministratori VDS. Questi script sono definiti come tipo di script "Globale". Gli script globali non possono essere modificati o cancellati da alcun amministratore VDS. Piuttosto, gli script globali possono essere "clonati" e lo script risultante è uno script "cliente" che può essere modificato e utilizzato.

Scarica script

La possibilità di scaricare il file di script associato a un evento con script consente all'amministratore VDS di rivedere e modificare il file di script sottostante prima dell'implementazione. Non è mai consigliabile eseguire uno script che non si comprende appieno.

[Sub.Management.Scripted Events.Scripted events 02a9b] |

sub.Management.Scripted_Events.scripted_events-02a9b.png

Aggiungi script

Facendo clic sul pulsante + *Add script* si apre una nuova pagina per creare uno script e salvarlo nell'archivio.

[Management.Scripted Events.Scripted events a53fa] | *Management.Scripted_Events.scripted_events-*

Per creare un nuovo script, è necessario completare i seguenti campi:

- **Nome**
- **Include script file**
 - Sì - consente di caricare ed eseguire un file script (ad esempio un file .ps1) dall'eseguibile "Esegui con".
 - No - rimuove il campo "file script" (qui sotto) ed esegue semplicemente il comando "Esegui con" e "argomenti"
- **File script**
 - Se *include script file* = Yes questo campo è visibile e consente il caricamento di un file di script.
- **Esegui con**
 - Definisce il percorso dell'eseguibile utilizzato per eseguire il file di script o il comando eseguito.
 - Ad esempio, per eseguire PowerShell il valore "Execute with" (Esegui con) dovrebbe essere `C:/Windows/system32/WindowsPowerShell/v1.0/powershell.exe`
- **Argomenti**
 - Definisce eventuali argomenti aggiuntivi eseguiti con il comando "esegue con".
 - VDS offre alcune variabili che possono essere utilizzate in funzione del contesto, tra cui:
 - %Companycode% - Codice società in fase di runtime
 - %Servername% - Nome della macchina virtuale in fase di runtime
 - %samaccountname% - <username>.<companycode>
 - %applicationname% - Nome dell'applicazione richiesto in fase di runtime
 - %Scriptname% - Nome script in fase di runtime
 - %username% - nome utente@loginidentifier in fase di runtime
- **URL della documentazione**
 - Questo campo consente al writer dello script di collegarlo alla documentazione trovata al di fuori di VDS, ad esempio un sistema della Knowledge base utilizzato dall'organizzazione degli amministratori VDS.

Modifica script

Facendo clic sul nome di uno script nel repository si apre una nuova pagina con i dettagli sullo script e un pulsante di azione per **modificare**.

Quando si modifica uno script, gli stessi campi sono modificabili come descritto in precedenza in ["Aggiungi script"](#) sezione.

In questa pagina dei dettagli dello script, è possibile anche **eliminare** lo script e **scaricare** qualsiasi file di script caricato.

[Management.Scripted Events.Scripted Events 3e756] | *Management.Scripted_Events.scripted_events-*

3e756.png

Attività

Le attività collegano uno script dal repository a un'implementazione, un sottoinsieme di macchine virtuali e un evento trigger.

[Management.Scripted Events.Scripted events f971c] | *Management.Scripted_Events.scripted_events-*

f971c.png

Aggiungi attività

Facendo clic sul pulsante + *Add Activity* viene aperta una nuova pagina per la creazione di un'attività.

[Management.Scripted Events.Scripted events 02ef8] | *Management.Scripted_Events.scripted_events-*

Per creare una nuova attività, è necessario completare i seguenti campi:

- **Nome**
- **Descrizione** (opzionale)
- **Implementazione**
- **Script**
- **Argomenti**
- Casella di controllo **Enabled**
- **Impostazioni evento**

Trigger di attività

[Sub.Management.Scripted Events.Scripted events cdfcd] |

- **Installazione dell'applicazione**

- Questo viene attivato quando l'amministratore VDS fa clic su "+ Aggiungi..." Dalla pagina *Workspace > applicazioni*.
- Questa selezione consente di selezionare un'applicazione dalla Libreria applicazioni e di pre-definire il collegamento dell'applicazione.
- Le istruzioni dettagliate per questo trigger sono evidenziate nella ["Installare la documentazione dello script Adobe Reader DC"](#).

- **Disinstallazione dell'applicazione**

- Questo viene attivato quando l'amministratore VDS fa clic su **azioni > Disinstalla** dalla pagina *Workspace > applicazioni*.
- Questa selezione consente di selezionare un'applicazione dalla Libreria applicazioni e di pre-definire il collegamento dell'applicazione.
- Le istruzioni dettagliate per questo trigger sono evidenziate nella ["Disinstalla la documentazione dello script Adobe Reader DC"](#).

- **Clone Server**

- Questo viene attivato quando la funzione Clone viene eseguita su una macchina virtuale esistente

- **Crea cache**

- Questo viene attivato ogni volta che VDS costruisce una nuova macchina virtuale per una cache di raccolta del provisioning

- **Crea client**

- Questo viene attivato ogni volta che una nuova organizzazione client viene aggiunta a VDS

- **Crea server**

- Questo viene attivato ogni volta che VDS costruisce una nuova macchina virtuale

- **Crea utente**

- Questo viene attivato ogni volta che viene aggiunto un nuovo utente tramite VDS

- **Elimina utente**

- Questo viene attivato ogni volta che un nuovo utente viene cancellato tramite VDS

- **Manuale**

- Questo viene attivato manualmente da un amministratore VDS dalla pagina **Scripted Events > Activity** (Eventi script > attività)

- **Aggiornamento manuale dell'applicazione**

- **Pianificato**

- Questo viene attivato quando viene raggiunta la data/ora definita

- **Avvia server**

- Questo viene attivato su una macchina virtuale ogni volta che si avvia

Facendo clic su *Name* si apre una finestra di dialogo in cui è possibile modificare l'attività.

Command Center

Command Center Command: Panoramica

Panoramica

Command Center è un eseguibile che viene eseguito sul server della piattaforma CWMGR1 nella distribuzione. È possibile accedervi connettendosi alla macchina virtuale CWMGR1 ed eseguendola localmente sulla macchina virtuale.

Questa applicazione è stata progettata per la risoluzione dei problemi, la diagnostica e le funzioni di gestione avanzate. Questa applicazione viene utilizzata principalmente dai team di sviluppo e supporto interni di NetApp, tuttavia alcune funzioni vengono occasionalmente utilizzate dagli amministratori dei clienti. Questa documentazione è fornita a supporto dell'utilizzo delle funzioni di selezione. L'utilizzo di questi comandi deve essere eseguito con cura e in collaborazione con il team di supporto NetApp.

Esecuzione di Command Center

Per eseguire l'applicazione Command Center:

1. Connettersi al server dalla pagina *VDS > Deployment > Platform Servers* fare clic sull'icona *Actions* e selezionare "Connect"

[Management.command Panoramica del centro 68087] | *Management.command_center_overview-*

2. Quando vengono richieste le credenziali, immettere le credenziali di amministratore del dominio
 - a. L'utente deve essere membro del gruppo di protezione "infrastruttura CW". Per motivi di coerenza, consigliamo di aggiungere questa iscrizione facendo dell'utente un membro del gruppo "tecnici di livello 3" in *ad > Cloud Workspace > Cloud Workspace Tech Users > Groups*

[Management.command panoramica del centro 1c42d] | *Management.command_center_overview-*

1c42d.png

3. Individuare l'icona sul desktop di *Command Center* ed eseguirla

[Panoramica del centro Management.command 3c860] | *Management.command_center_overview-*

- a. Per attivare la scheda Advanced (Avanzate), avviare l'applicazione con l'opzione "-showadvancedtab".

Scheda Operations (operazioni)

[Management.command panoramica del centro b614e] | *Management.command_center_overview-b614e.png*

Dal menu **comando** è possibile selezionare una delle azioni elencate di seguito.

Una volta selezionato un comando, i dati possono essere popolati con i dati di implementazione dal pulsante **Load Data** (carica dati). Il pulsante Load Data (carica dati) viene utilizzato anche per eseguire query sull'hypervisor per i dati una volta effettuate le selezioni precedenti (ad esempio, caricare un elenco di date di backup disponibili dopo aver selezionato una macchina virtuale specifica da un menu a discesa)

[Management.command Panoramica del centro 85417] | *Management.command_center_overview-85417.png*

Dopo aver selezionato un comando, fare clic su **Esegui comando** per eseguire il processo selezionato.

Per rivedere i registri, fare clic sul pulsante **View All Logs** (Visualizza tutti i registri). Viene aperto il file di testo raw, con le voci più recenti in basso.

Elenco dei comandi

- ["Copia modello nella Gallery"](#)

Operazioni

Command Center Command: Copia modello nella Gallery

Avviso del Command Center



Command Center è un'applicazione che viene eseguita sul server della piattaforma CWMGR1 nella distribuzione. Questa applicazione è stata progettata per la risoluzione dei problemi, la diagnostica e le funzioni di gestione avanzate. Questa applicazione viene utilizzata principalmente dai team di sviluppo e supporto interni di NetApp, tuttavia alcune funzioni vengono occasionalmente utilizzate dagli amministratori dei clienti. Questa documentazione è fornita a supporto dell'utilizzo delle funzioni di selezione. L'utilizzo di questi comandi deve essere eseguito con cura e in collaborazione con il team di supporto NetApp. Per ulteriori informazioni, consultare ["Panoramica del Command Center"](#) articolo.

Copia modello nella galleria Panoramica

[Management.command center.Operations.copy template to gallery 67ea4] |

Quando viene finalizzata una raccolta di provisioning VDI, l'immagine viene memorizzata in Azure come immagine e può essere implementata nello stesso sito VDS. Per rendere l'immagine disponibile per la distribuzione in un'altra regione Azure all'interno dello stesso abbonamento, viene utilizzata la funzione "Copia modello nella galleria". Questa azione copia l'immagine della macchina virtuale nella galleria condivisa e la replica in tutte le regioni selezionate.

[Management.command center.Operations.copy template to gallery ed821] |

Management.command_center.operations.copy_template_to_gallery-ed821.png

Disponibilità dei modelli di macchine virtuali nel menu a discesa VDS

Una volta completata la replica, l'immagine viene visualizzata in VDS nel menu a discesa per la selezione dei modelli di macchine virtuali durante l'implementazione di nuove macchine virtuali. L'immagine condivisa sarà disponibile per l'implementazione in qualsiasi regione selezionata durante la copia.

[Management.command center.Operations.copy template to gallery 04bd8] |

Management.command_center.operations.copy_template_to_gallery-04bd8.png

Le immagini delle macchine virtuali memorizzate nella galleria condivisa vengono aggiunte con la relativa versione sotto forma di "-x.x.x", dove la versione corrisponde alla versione dell'immagine all'interno di Azure Portal.

[Management.command center.Operations.copy template to gallery e598] |



La replica dell'immagine può richiedere qualche istante (a seconda delle dimensioni dell'immagine) e lo stato può essere visualizzato facendo clic sulla versione (ad esempio n. 1.0) nella colonna "Nome" come evidenziato nella schermata precedente.

Disponibilità regionale

Le implementazioni possono essere eseguite solo nelle regioni in cui l'immagine è stata replicata. È possibile effettuare il check-in nel portale Azure facendo clic sul numero 1.x.x e quindi su *Update Replication*, come illustrato di seguito:

[Management.command center.Operations.copy template to gallery 9b63a] |

Ottimizzazione delle risorse

Pianificazione del carico di lavoro

Workload Scheduling è una funzionalità che consente di pianificare l'intervallo di tempo in cui l'ambiente è attivo.

La pianificazione del carico di lavoro può essere impostata su "Always on", "Always Off" o "Scheduled". Se impostata su "Scheduled" (pianificato), gli orari di accensione e spegnimento possono essere impostati in modo granulare come una finestra temporale diversa per ogni giorno della settimana.

[]

Quando si prevede di disattivarsi, tramite "Always Off" o "Scheduled", tutte le macchine virtuali del tenant si spegneranno. I server della piattaforma (come CWMGR1) rimarranno attivi per facilitare funzionalità come la riattivazione su richiesta.

Workload Schedule funziona in combinazione con altre funzionalità di ottimizzazione delle risorse, tra cui Live Scaling e Wake on Demand.

Attivazione su richiesta

Wake on Demand (WOD) è una tecnologia in attesa di brevetto in grado di attivare le risorse VM appropriate per un utente finale per facilitare l'accesso automatico 24 ore su 24, 7 giorni su 7, anche quando le risorse sono pianificate per essere inattive.

WOD per i servizi di desktop remoto

In RDS, il client Windows VDS dispone dell'integrazione Wake on Demand integrata e può attivare le risorse appropriate senza ulteriori azioni da parte dell'utente finale. È sufficiente avviare il normale login e il client notificherà loro un breve ritardo nell'attivazione delle macchine virtuali. Questo client (e quindi questa funzionalità automatizza la riattivazione su richiesta) è disponibile solo quando ci si connette da un dispositivo Windows a un ambiente RDS.

Funzionalità simili sono integrate nel client Web VDS per le implementazioni RDS. Il client Web VDS si trova all'indirizzo: ""

La funzionalità Wake on Demand non è integrata nel client Microsoft RD (per Windows o qualsiasi altra piattaforma) né in altri client RD di terze parti.

Attiva su richiesta per Azure Virtual Desktop

In AVD, gli unici client che possono essere utilizzati per la connessione sono forniti da Microsoft e quindi non contengono la funzionalità Wake on Demand.

VDS include una funzione self-service Wake on Demand per AVD tramite VDS Web Client. Il client Web può essere utilizzato per attivare le risorse appropriate, quindi la connessione può essere avviata tramite il client AVD standard.

Per attivare le risorse VM in AVD:

1. Connettersi al client Web VDS all'indirizzo ""

2. Accedere con le credenziali AVD dell'utente

- Viene visualizzato un messaggio di avviso "*i servizi AVD di Microsoft sono disponibili. Fare clic QUI per visualizzare lo stato e avviare i pool di host offline.*"

3. Dopo aver fatto clic su "**HERE**", nella colonna di stato viene visualizzato un elenco dei pool di host disponibili insieme al collegamento "Click to Start"



4. Fare clic per avviare il collegamento e attendere 1-5 minuti per passare allo stato "Online" e visualizzare un'icona di stato verde

5. Connettersi ad AVD utilizzando la normale procedura

Scalabilità in tempo reale

Live Scaling funziona in combinazione con Workload Scheduling gestendo il numero di host di sessione online durante l'orario attivo pianificato, come configurato in Workload Scheduling. Se pianificato per essere offline, Live Scaling non controlla la disponibilità degli host di sessione. La scalabilità in tempo reale influisce solo sugli utenti condivisi e sui server condivisi negli ambienti RDS e AVD, gli utenti VDI e le macchine virtuali VDI sono esclusi da questi calcoli. Tutti gli altri tipi di macchine virtuali non sono interessati.



L'impostazione *load balancer type* di AVD interagisce con questa configurazione, pertanto occorre prestare attenzione anche alla scelta di tale impostazione. I risparmi sui costi sono massimizzati con un tipo "depth-first", mentre le performance dell'utente finale sono massimizzate con un tipo "breadth-first".

Abilitazione della scalabilità in tempo reale senza l'opzione selezionata, il motore di automazione selezionerà automaticamente i valori per il numero di server con alimentazione extra, gli utenti condivisi per server e il numero massimo di utenti condivisi per server.

- Il valore predefinito del *numero di server extra-accesi* è 0, ovvero 1 server esegue 24 ore su 24, 7 giorni su 7.
- L'impostazione predefinita di *Shared Users per Server* indica il numero di utenti dell'azienda diviso per il numero di server.
- Il valore predefinito di *Max Shared Users per Server* è infinito.

Live Scaling attiva i server quando gli utenti si connettono e li disattiva quando gli utenti si disconnettono.

L'accensione di un server aggiuntivo viene attivata automaticamente quando il numero totale di utenti attivi raggiunge il numero di utenti condivisi per server moltiplicato per il numero totale di server attivati.

e.g. With 5 Shared Users per Server set (this is the default # we'll use for all examples in this article) and 2 servers running, a 3rd server won't be powered up until server 1 & 2 both have 5 or more active users. Until that 3rd server is available, new connections will be load balanced all available servers. In RDS and AVD Breadth mode, Load balancing sends users to the server with the fewest active users (like water flowing to the lowest point). In AVD Depth mode, Load balancing sends users to servers in a sequential order, incrementing when the Max Shared Users number is reached.

Live Scaling disattiva anche i server per risparmiare sui costi. Quando un server ha 0 utenti attivi e un altro server ha una capacità disponibile inferiore a `_utenti condivisi per server_`, il server vuoto viene spento.

L'accensione del server successivo può richiedere alcuni minuti. In alcune situazioni, la velocità di accesso può superare la disponibilità dei nuovi server. Ad esempio, se 15 persone accedono in 5 minuti, si atterreranno sul primo server (o verrà negata una sessione) mentre si accenderanno un secondo e un terzo server. In questo scenario è possibile utilizzare due strategie per ridurre l'overload di un singolo server:

1. Abilitare *Number of Extra Powered on Servers* in modo che i server aggiuntivi siano accesi e disponibili per accettare le connessioni e consentire alla piattaforma di accelerare ulteriori server.
 - a. Una volta attivato, il numero viene aggiunto alla necessità calcolata. Ad esempio, se impostato su 1 server aggiuntivo (e con 6 utenti connessi), due server sarebbero attivi a causa del numero di utenti, più un terzo a causa dell'impostazione *Extra Powered on Servers*.
2. Abilitare *Max Shared Users per Server* per porre un limite massimo al numero di utenti consentiti per server. Le nuove connessioni che superano questo limite verranno rifiutate, l'utente finale riceverà un messaggio di errore e dovrà riprovare tra qualche minuto una volta che il server aggiuntivo sarà disponibile. Se impostato, questo numero definisce anche la profondità dei server condivisi AVD.
 - a. Supponendo che il delta tra *utenti condivisi per server* e *utenti condivisi max per server* sia appropriato, i nuovi server dovrebbero diventare disponibili prima che venga raggiunto il massimo in tutte le situazioni eccetto quelle più estreme (insolitamente grandi tempeste di login).

Scalabilità delle risorse delle macchine virtuali

La scalabilità delle risorse delle macchine virtuali è una funzionalità opzionale che consente di modificare le dimensioni e la quantità delle macchine virtuali host di sessione in un ambiente.

Una volta attivato, VDS calcola le dimensioni e la quantità appropriate delle VM host di sessione in base ai criteri selezionati. Queste opzioni includono: Active Users (utenti attivi), Named Users (utenti denominati), Server Load (carico server) e Fixed (fisso)

□

Le dimensioni delle macchine virtuali sono contenute con la famiglia di macchine virtuali selezionata nell'interfaccia utente, che può essere modificata dal menu a discesa. (Ad es. *Standard DV3 Family* in Azure)

□

Scalabilità in base agli utenti



La funzione riportata di seguito si comporta allo stesso modo per "utenti attivi" o "Conteggio utenti". User Count è un semplice numero di utenti attivati con un desktop VDS. Active Users è una variabile calcolata in base alle 2 settimane precedenti di dati della sessione utente.

Durante il calcolo in base agli utenti, le dimensioni (e la quantità) delle VM host della sessione vengono calcolate in base ai requisiti di RAM e CPU definiti. L'amministratore può definire il GB di RAM e il numero di core vCPU per utente insieme a risorse aggiuntive non variabili.

Nella schermata riportata di seguito, a ciascun utente sono allocati 2 GB di RAM e 1/2 di un core vCPU. Inoltre, il server inizia con 2 core vCPU e 8 GB di RAM.

□

Inoltre, l'amministratore può definire le dimensioni massime che una macchina virtuale può raggiungere. Una volta raggiunti, gli ambienti si scaleranno orizzontalmente aggiungendo altri host di sessione VM.

Nella schermata seguente, ogni macchina virtuale è limitata a 32 GB di RAM e 8 core vCPU.

□

Con tutte queste variabili definite, VDS può calcolare la dimensione e la quantità appropriate delle VM host di sessione, semplificando notevolmente il processo di mantenimento dell'assegnazione delle risorse appropriate, anche quando gli utenti vengono aggiunti e rimossi.

Scalabilità in base al carico del server

Durante il calcolo in base al carico del server, le dimensioni (e la quantità) delle VM host di sessione vengono calcolate in base ai tassi medi di utilizzo di CPU/RAM osservati da VDS nel periodo di 2 settimane precedente.

Una volta superata la soglia massima, il VDS aumenterà la dimensione o la quantità per riportare l'utilizzo medio all'interno dell'intervallo.

Come per la scalabilità basata sull'utente, è possibile definire la famiglia di macchine virtuali e la dimensione massima delle macchine virtuali.

□

Altre risorse attive

Workload Scheduling non controlla i server della piattaforma, come CWMGR1, in quanto sono necessari per attivare la funzionalità Wake on Demand e facilitare altre attività della piattaforma e dovrebbero eseguire 24/7 per il normale funzionamento ambientale.

È possibile ottenere un ulteriore risparmio disattivando l'intero ambiente, ma è consigliato solo per gli ambienti non di produzione. Si tratta di un'azione manuale che può essere eseguita nella sezione implementazioni di VDS. Il ripristino dello stato normale dell'ambiente richiede anche un passaggio manuale sulla stessa pagina.

□ □

User Administration (Amministrazione utente)

Gestione degli account utente

Crea nuovi utenti

Gli amministratori possono aggiungere utenti facendo clic su aree di lavoro > utenti e gruppi > Aggiungi/importa

Gli utenti possono essere aggiunti singolarmente o con un'importazione in blocco.

[larghezza=25%]



L'accuratezza dell'e-mail e del numero di telefono cellulare in questa fase migliora notevolmente il processo di abilitazione dell'MFA in un secondo momento.

Una volta creati gli utenti, puoi fare clic sul loro nome per visualizzare dettagli come quando sono stati creati, il loro stato di connessione (sia che siano attualmente connessi o meno) e le relative impostazioni specifiche.

Attivazione di Virtual Desktop per gli utenti ad esistenti

Se gli utenti sono già presenti in ad, è possibile attivare il Virtual Desktop degli utenti facendo clic sull'ingranaggio accanto al nome e attivando il desktop.[larghezza=50%]



Solo per Azure ad Domain Service: Affinché gli accessi funzionino, l'hash della password per gli utenti di Azure ad deve essere sincronizzato per supportare l'autenticazione NTLM e Kerberos. Il modo più semplice per eseguire questa operazione consiste nel modificare la password utente in Office.com o nel portale Azure, che forzerà la sincronizzazione dell'hash della password. Il ciclo di sincronizzazione per i server Domain Service può richiedere fino a 20 minuti, pertanto le modifiche alle password in Azure ad richiedono in genere 20 minuti per essere riflesse in AADDS e quindi nell'ambiente VDS.

Elimina account utente

Modificare le informazioni dell'utente

Nella pagina dei dettagli dell'utente è possibile modificare i dettagli dell'utente, ad esempio il nome utente e i dettagli di contatto. I valori di e-mail e telefono vengono utilizzati per il processo di reimpostazione self-service della password (SSPR).

□

Modificare le impostazioni di sicurezza dell'utente

- VDI User Enabled (utente VDI abilitato) - impostazione RDS che, se attivata, crea un host di sessione VM dedicato e assegna a questo utente l'unico utente a cui si connette. Durante l'attivazione di questa casella di controllo, all'amministratore di CWMS viene richiesto di selezionare immagine, dimensione e tipo di storage della macchina virtuale.
 - Gli utenti AVD VDI devono essere gestiti nella pagina AVD come pool di host VDI.
- Scadenza account attivata: Consente all'amministratore di CWMS di impostare una data di scadenza sull'account dell'utente finale.
- Imponi reimpostazione password al prossimo accesso: Richiede all'utente finale di modificare la password al successivo accesso.

- **Multi-Factor Auth Enabled** (autenticazione multifattore abilitata): Attiva l'autenticazione MFA per l'utente finale e richiede di configurare l'autenticazione MFA al successivo accesso.
- **Mobile Drive Enabled** (disco mobile abilitato): Una funzione legacy non utilizzata nelle implementazioni correnti di RDS o AVD.
- **Local Drive Access Enabled** (accesso al disco locale abilitato): Consente all'utente finale di accedere allo storage del dispositivo locale dall'ambiente cloud, tra cui Copy/Paste, USB Mass Storage e dischi di sistema.
- **Wake on Demand Enabled** (attiva su richiesta attivata): Per gli utenti RDS che si connettono tramite il client CW per Windows, l'abilitazione di questa opzione consente all'utente finale di portare il proprio ambiente quando si effettua la connessione al di fuori del normale orario di lavoro, come definito dalla pianificazione del carico di lavoro.

Account bloccato

Per impostazione predefinita, cinque tentativi di accesso non riusciti bloccano l'account utente. L'account utente si sbloccherà dopo 30 minuti, a meno che l'opzione *Enable Password complessità* non sia attivata. Se la complessità della password è attivata, l'account non viene sbloccato automaticamente. In entrambi i casi, l'amministratore VDS può sbloccare manualmente l'account utente dalla pagina utenti/gruppi in VDS.

Reimpostare la password dell'utente

Ripristina la password utente.

Nota: Quando si reimpostano le password degli utenti di Azure ad (o si sblocca un account), può verificarsi un ritardo fino a 20 minuti poiché la reimpostazione si propaga attraverso Azure ad.

Accesso amministratore

Abilitando questa opzione, l'utente finale ha accesso limitato al portale di gestione per il tenant. Gli usi più comuni includono la possibilità di fornire a un dipendente on-site l'accesso per reimpostare le password dei peer, assegnare l'applicazione o consentire l'accesso manuale all'attivazione del server. Vengono impostate anche le autorizzazioni che controllano le aree della console.

Disconnettersi dagli utenti

Gli utenti connessi possono essere disconnessi dall'amministratore VDS dalla pagina utenti/gruppi in VDS.

Applicazioni

Visualizza l'applicazione implementata in questo spazio di lavoro. La casella di controllo fornisce le applicazioni a questo utente specifico. La documentazione completa sulla gestione delle applicazioni è disponibile qui. L'accesso alle applicazioni può essere concesso anche dall'interfaccia App o ai gruppi di sicurezza.

Visualizzare/eliminare i processi degli utenti

Visualizza i processi attualmente in esecuzione nella sessione dell'utente. I processi possono essere terminati anche da questa interfaccia.

Gestione delle autorizzazioni per i dati

Prospettiva dell'utente finale

Gli utenti finali di Virtual Desktop possono accedere a diversi dischi mappati. Questi dischi includono una condivisione di team accessibile ai FTP, una condivisione file aziendale e il disco principale (per documenti, desktop, ecc....) . Tutte queste unità mappate fanno riferimento a un livello di storage centrale su un servizio di storage (come Azure NetApp Files) o su una macchina virtuale del file server.

A seconda della configurazione di cui l'utente potrebbe non avere le unità H: O F: Esposte, potrebbero vedere solo il proprio desktop, documenti, ecc.... cartelle. Inoltre, l'amministratore del VDS può impostare lettere di unità diverse al momento dell'implementazione.[]

[]

Gestione delle autorizzazioni

VDS consente agli amministratori di modificare i gruppi di sicurezza e le autorizzazioni delle cartelle, tutto dal portale VDS.

Gruppi di sicurezza

I gruppi di sicurezza vengono gestiti facendo clic su Workspace > Nome tenant > utenti e gruppi > nella sezione gruppi

In questa sezione è possibile:

1. Creare nuovi gruppi di sicurezza
2. Aggiungere/rimuovere utenti ai gruppi
3. Assegnare le applicazioni ai gruppi
4. Attiva/disattiva l'accesso al disco locale ai gruppi

[]

Permessi della cartella

Per gestire le autorizzazioni delle cartelle, fare clic su Workspace > Nome tenant > Gestisci (nella sezione cartelle).

In questa sezione è possibile:

1. Aggiungi/Elimina cartelle
2. Assegnare autorizzazioni a utenti o gruppi
3. Personalizzare le autorizzazioni per sola lettura, controllo completo e Nessuna

[]

Diritti dell'applicazione

Panoramica

VDS dispone di un'efficace funzionalità integrata di autorizzazione e automazione delle applicazioni. Questa funzionalità consente agli utenti di accedere a diverse applicazioni durante la connessione agli stessi host di sessione. Ciò è possibile grazie ad alcuni oggetti Criteri di gruppo personalizzati che nascondono i collegamenti insieme all'automazione che posiziona i collegamenti in modo selettivo sui desktop degli utenti.



Questo flusso di lavoro si applica solo alle implementazioni RDS. Per la documentazione relativa ai diritti dell'applicazione AVD, vedere "[Application Entitlement Workflow per AVD](#)"

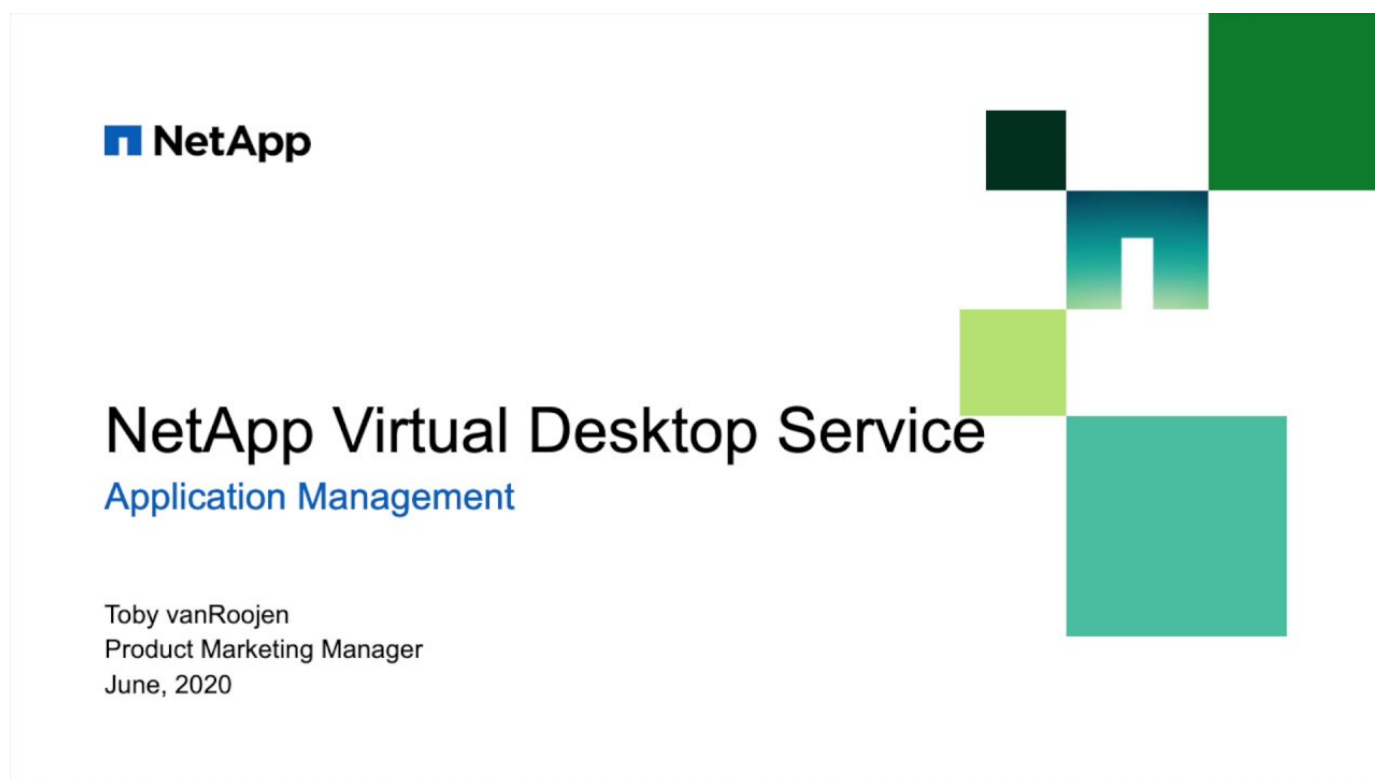
Le applicazioni possono essere assegnate agli utenti direttamente o tramite gruppi di sicurezza gestiti in VDS.

Ad alto livello, il processo di provisioning dell'applicazione segue questi passaggi.

1. Aggiungi app all'App Catalog
2. Aggiungi app all'area di lavoro
3. Installare l'applicazione su tutti gli host di sessione
4. Selezionare il percorso di scelta rapida
5. Assegnare le applicazioni a utenti e/o gruppi



I passaggi 3 e 4 possono essere completamente automatizzati con gli eventi con script, come illustrato di seguito



Video - Panoramica

Aggiungere applicazioni all'App Catalog

VDS Application Entitlement inizia con App Catalog, un elenco di tutte le applicazioni disponibili per l'implementazione negli ambienti degli utenti finali.

Per aggiungere applicazioni al catalogo, procedere come segue

1. Accedere a VDS all'indirizzo <https://manage.cloudworkspace.com> utilizzando le credenziali di amministratore principali.
2. In alto a destra, fare clic sull'icona a forma di freccia accanto al nome utente e selezionare Impostazioni.
3. Fare clic sulla scheda App Catalog.

4. Fare clic sull'opzione Add App (Aggiungi applicazione) nella barra del titolo del catalogo applicazioni.
5. Per aggiungere un gruppo di applicazioni, selezionare l'opzione Importa applicazioni.
 - a. Viene visualizzata una finestra di dialogo che fornisce un modello Excel da scaricare che crea il formato corretto per l'elenco delle applicazioni.
 - b. Per questa valutazione, NetApp VDS ha creato un elenco di applicazioni di esempio per l'importazione, disponibile qui.
 - c. Fare clic sull'area Upload (carica) e scegliere il file di modello dell'applicazione, quindi fare clic sul pulsante Import (Importa).
6. Per aggiungere singole applicazioni, selezionare il pulsante Add App (Aggiungi applicazione) per visualizzare una finestra di dialogo.
 - a. Inserire il nome dell'applicazione.
 - b. L'ID esterno può essere utilizzato per inserire un identificativo di tracciamento interno, ad esempio una SKU di prodotto o un codice di tracciamento della fatturazione (opzionale).
 - c. Selezionare la casella di controllo Subscription (abbonamento) se si desidera creare un report sulle applicazioni come prodotto in abbonamento (opzionale).
 - d. Se il prodotto non viene installato in base alla versione (ad esempio Chrome), selezionare la casella di controllo versione non richiesta. In questo modo è possibile installare i prodotti con aggiornamenti continui senza tenere traccia delle loro versioni.
 - e. Al contrario, se un prodotto supporta più versioni con nome (ad esempio QuickBooks), selezionare questa casella per installare più versioni e avere VDS specifico per ciascuna versione disponibile nell'elenco delle applicazioni che possono avere diritto e per l'utente finale.
 - f. Selezionare l'opzione "Nessuna icona di desktop utente" se non si desidera che VDS provi un'icona di desktop per questo prodotto. Viene utilizzato per prodotti "back-end" come SQL Server, poiché gli utenti finali non dispongono di un'applicazione a cui accedere.
 - g. "L'app deve essere associata" impone la necessità di installare un'app associata. Ad esempio, un'applicazione client server potrebbe richiedere l'installazione di SQL Server o MySQL.
 - h. Selezionando la casella licenza richiesta, VDS deve richiedere il caricamento di un file di licenza per un'installazione dell'applicazione prima di impostare lo stato dell'applicazione su attivo. Questa fase viene eseguita nella pagina Application Detail di VDS.
 - i. Visibile a tutti: I diritti dell'applicazione possono essere limitati a specifici partner secondari in una gerarchia multicanale. A scopo di valutazione, fare clic sulla casella di controllo in modo che tutti gli utenti possano visualizzarla nell'elenco delle applicazioni disponibili.

Aggiungere l'applicazione all'area di lavoro

Per avviare il processo di implementazione, aggiungerai l'applicazione allo spazio di lavoro.

Per eseguire questa operazione, attenersi alla seguente procedura

1. Fare clic su aree di lavoro
2. Scorrere verso il basso fino ad applicazioni
3. Fare clic su Aggiungi
4. Selezionare le applicazioni, inserire le informazioni richieste, fare clic su Add Application (Aggiungi applicazione), quindi su Add Apps (Aggiungi applicazioni).

Installare manualmente l'applicazione

Una volta aggiunta l'applicazione all'area di lavoro, è necessario installarla su tutti gli host di sessione. Questa operazione può essere eseguita manualmente e/o può essere automatizzata.

Per installare manualmente le applicazioni sugli host di sessione, attenersi alla seguente procedura

1. Accedere a Service Board (scheda di servizio).
2. Fare clic sull'attività del Service Board.
3. Fare clic sui nomi dei server per connettersi come amministratore locale.
4. Installare le applicazioni, verificare che il collegamento a questa applicazione si trovi nel percorso del menu Start.
 - a. Per Server 2016 e Windows 10: C: ProgramData/Microsoft/Windows/Menu Start/programmi.
5. Tornare all'attività del Service Board, fare clic su Browse (Sfoglia) e scegliere il collegamento o una cartella contenente i collegamenti.
6. Qualsiasi opzione selezionata viene visualizzata sul desktop dell'utente finale quando viene assegnata l'applicazione.
7. Le cartelle sono eccezionali quando un'applicazione è in realtà costituita da più applicazioni. Ad esempio, "Microsoft Office" è più semplice da implementare come cartella con ogni applicazione come collegamento all'interno della cartella.
8. Fare clic su completa installazione.
9. Se necessario, aprire l'icona creata Add Service Board Task (Aggiungi attività Service Board) e confermare che l'icona è stata aggiunta.

Assegnare le applicazioni agli utenti

Il diritto all'applicazione viene gestito da VDS e l'applicazione può essere assegnata agli utenti in tre modi

Assegnare le applicazioni agli utenti

1. Accedere alla pagina User Detail (Dettagli utente).
2. Accedere alla sezione applicazioni.
3. Selezionare la casella accanto a tutte le applicazioni richieste dall'utente.

Assegnare gli utenti a un'applicazione

1. Accedere alla sezione applicazioni della pagina Dettagli area di lavoro.
2. Fare clic sul nome dell'applicazione.
3. Selezionare la casella accanto agli utenti dell'applicazione.

Assegnare applicazioni e utenti ai gruppi di utenti

1. Accedere ai dettagli di utenti e gruppi.
2. Aggiungere un nuovo gruppo o modificare un gruppo esistente.
3. Assegnare utenti e applicazioni al gruppo.

Reimposta password utente

Procedura di reimpostazione della password utente

1. Accedere alla pagina dei dettagli utilizzati in VDS



2. Individuare la sezione Password, inserire due volte la nuova PW e fare clic su



È il momento di prendere effetto

- Per gli ambienti che eseguono un annuncio "interno" sulle macchine virtuali nell'ambiente, la modifica della password dovrebbe avere effetto immediato.
- Per gli ambienti che eseguono Azure ad Domain Services (AADDs), la modifica della password dovrebbe richiedere circa 20 minuti.
- Il tipo di ad può essere determinato nella pagina Deployment Details:



Reimpostazione self-service della password (SSRP)

Il client NetApp VDS Windows e il client Web NetApp VDS forniscono una richiesta agli utenti che inseriscono una password errata quando accedono a un'implementazione di desktop virtuale v5.2 (o successiva). Nel caso in cui l'utente abbia bloccato l'account, questa procedura sbloccherà anche l'account dell'utente.

Nota: Gli utenti devono aver già inserito un numero di telefono cellulare o un indirizzo e-mail per poter eseguire questa procedura.

SSPR è supportato con:

- NetApp VDS Window Client
- Client Web NetApp VDS

In questa serie di istruzioni, verrà descritto il processo di utilizzo di SSPR come semplice mezzo per consentire agli utenti di reimpostare le password e sbloccare i propri account.

Client NetApp VDS Windows

1. In qualità di utente finale, fare clic sul collegamento Forgot Password (Password dimenticata) per continuare.



2. Consente di selezionare se ricevere il codice tramite telefono cellulare o e-mail.



3. Se un utente finale ha fornito solo uno di questi metodi di contatto, questo sarà l'unico metodo visualizzato.



4. Al termine di questa fase, agli utenti viene visualizzato un campo Code (Codice) in cui inserire il valore numerico ricevuto sul dispositivo mobile o nella posta in arrivo (a seconda della selezione). Inserire il codice seguito dalla nuova password e fare clic su Reset (Ripristina) per continuare.

[]

5. Gli utenti visualizzeranno un messaggio che informa che la reimpostazione della password è stata completata correttamente. Fare clic su Done (fine) per completare il processo di accesso.



Se la distribuzione utilizza Azure Active Directory Domain Services, esiste un periodo di sincronizzazione delle password definito da Microsoft, ogni 20 minuti. Anche in questo caso, questo è controllato da Microsoft e non può essere modificato. Tenendo presente questo aspetto, VDS visualizza che l'utente deve attendere fino a 20 minuti per rendere effettiva la nuova password. Se la distribuzione non utilizza Azure Active Directory Domain Services, l'utente potrà effettuare nuovamente l'accesso in pochi secondi.

[]

Portale HTML5

1. Se l'utente non riesce a inserire la password corretta quando tenta di effettuare l'accesso tramite HTML5, viene visualizzata un'opzione per reimpostare la password:

[]

2. Dopo aver fatto clic sull'opzione per reimpostare la password, verranno visualizzate le opzioni di ripristino:

[]

3. Il pulsante 'Richiedi' invia un codice generato all'opzione selezionata (in questo caso l'email dell'utente). Il codice è valido per 15 minuti.

[]

4. La password è stata reimpostata. È importante ricordare che Windows Active Directory spesso richiede qualche istante per propagare la modifica, quindi se la nuova password non funziona immediatamente, attendere qualche minuto e riprovare. Ciò è particolarmente importante per gli utenti che risiedono in un'implementazione di servizi di dominio Active Directory di Azure, in cui la reimpostazione della password potrebbe richiedere fino a 20 minuti per la propagazione.

[]

Abilitazione della reimpostazione self-service della password (SSPR) per gli utenti

Per utilizzare la funzione di reimpostazione automatica della password (SSPR), gli amministratori devono prima inserire un numero di telefono cellulare e/o un account e-mail per un utente finale esistono due modi per inserire un numero di cellulare e gli indirizzi e-mail per un utente di desktop virtuale, come descritto di seguito.

In questa serie di istruzioni, verrà descritto il processo di configurazione di SSPR come un semplice mezzo per consentire agli utenti finali di reimpostare le password.

Importazione in blocco di utenti tramite VDS

Accedere al modulo Workspaces, quindi a Users & Groups e fare clic su Add/Import (Aggiungi/Importa).

È possibile inserire questi valori per gli utenti quando li creano uno alla volta:[]

In alternativa, è possibile includere questi elementi quando si importano in blocco utenti che scaricano e caricano il file XLSX Excel preconfigurato con questo contenuto completo:[]

Fornire i dati tramite l'API VDS

API NetApp VDS – in particolare questa chiamata https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – consente di aggiornare queste informazioni.

Aggiornamento del telefono utente esistente

Aggiornare il numero di telefono dell'utente nella pagina User Detail Overview (Panoramica dettagli utente) di VDS.

[]

Utilizzo di altre console

Nota: Al momento non è possibile fornire un numero di telefono per un utente tramite Azure Console, Partner Center o dalla console di amministrazione di Office 365.

Personalizzare l'indirizzo di invio di SSPR

NetApp VDS può essere configurato per inviare l'email di conferma *from* a un indirizzo personalizzato. Si tratta di un servizio fornito ai partner dei provider di servizi che desiderano che i loro utenti finali ricevano l'e-mail di reimpostazione della password da inviare dal proprio dominio e-mail personalizzato.

Questa personalizzazione richiede alcuni passaggi aggiuntivi per verificare l'indirizzo di invio. Per avviare questo processo, aprire un caso di supporto con il supporto VDS richiedendo un "Self Service Password Reset Source Address" personalizzato. Definire quanto segue:

- Il tuo codice partner (puoi trovarlo facendo clic su *settings* sotto il menu con la freccia in alto a destra in basso). Vedere la schermata riportata di seguito)

[]

- Indirizzo "da" desiderato (che deve essere valido)
- A quali client applicare l'impostazione (o tutti)

Per aprire un caso di supporto, inviare un'e-mail all'indirizzo support@spotpc.netapp.com

Una volta ricevuto, il supporto VDS funzionerà per convalidare l'indirizzo con il nostro servizio SMTP e attivare questa impostazione. Idealmente, avrai la possibilità di aggiornare i record DNS pubblici nel dominio degli indirizzi di origine per massimizzare la deliverability della posta elettronica.

Complessità delle password

VDS può essere configurato per imporre la complessità delle password. L'impostazione per questa operazione si trova nella pagina dei dettagli dell'area di lavoro nella sezione Impostazioni dell'area di lavoro cloud.

[]

[]

Complessità della password: Disattivata

Policy	Linee guida
Lunghezza minima della password	8 caratteri
Validità massima password	110 giorni
Validità minima password	0 giorni
Imponi cronologia password	24 password memorizzate
Blocco password	Il blocco automatico si verifica dopo 5 immissioni errate
Durata blocco	30 minuti

Complessità della password: Attivata

Policy	Linee guida
Lunghezza minima della password	8 caratteri non contengono il nome dell'account dell'utente o parti del nome completo dell'utente che superano i due caratteri consecutivi contengono tre delle seguenti quattro categorie: Caratteri maiuscoli inglesi (Dalla A alla Z) caratteri minuscoli inglesi (dalla a alla z) 10 cifre di base (da 0 a 9) caratteri non alfabetici (ad esempio, !, €, n., %) i requisiti di complessità vengono applicati quando le password vengono modificate o create.
Validità massima password	110 giorni
Validità minima password	0 giorni
Imponi cronologia password	24 password memorizzate
Blocco password	Il blocco automatico si verifica dopo 5 immissioni errate
Durata blocco	Rimane bloccato fino a quando l'amministratore non si sblocca

Autenticazione multifattore (MFA)

Panoramica

NetApp Virtual Desktop Service (VDS) include un servizio MFA basato su SMS/e-mail senza costi aggiuntivi. Questo servizio è indipendente da qualsiasi altro servizio (ad esempio Azure Conditional Access) e può essere utilizzato per proteggere gli accessi degli amministratori a VDS e gli accessi degli utenti ai desktop virtuali.

Nozioni di base su MFA

- VDS MFA può essere assegnato a utenti admin, singoli utenti finali o applicato a tutti gli utenti finali
- VDS MFA può inviare notifiche via SMS o e-mail
- VDS MFA dispone di una funzione di configurazione e ripristino iniziali self-service

Scopo della guida

Questa guida illustra la configurazione di MFA insieme a un'illustrazione dell'esperienza dell'utente finale

Questa guida tratta i seguenti argomenti:

1. [Abilitazione di MFA per singoli utenti](#)
2. [Richiede MFA per tutti gli utenti](#)
3. [Abilitazione di MFA per singoli amministratori](#)
4. [Configurazione iniziale dell'utente finale](#)

Abilitazione di MFA per singoli utenti

L'autenticazione MFA può essere attivata per singoli utenti nella pagina dei dettagli dell'utente facendo clic su *Multi-Factor Auth Enabled*

Aree di lavoro > Nome area di lavoro > utenti e gruppi > Nome utente > autenticazione a più fattori attivata > Aggiorna

L'MFA può anche essere assegnato a tutti gli utenti; se questa impostazione è attiva, la casella di controllo viene selezionata e (*via Client Settings*) viene aggiunto all'etichetta della casella di controllo.

Richiede MFA per tutti gli utenti

L'MFA può essere attivato e applicato a tutti gli utenti nella pagina dei dettagli dell'area di lavoro facendo clic su *MFA for All Users Enabled*

Aree di lavoro > Nome area di lavoro > MFA per tutti gli utenti attivato > Aggiorna

Abilitazione di MFA per singoli amministratori

MFA è disponibile anche per gli account amministratore che accedono al portale VDS. Questa opzione può essere attivata per amministratore nella pagina dei dettagli dell'amministratore. Amministratori > Nome amministratore > autenticazione multifattore richiesta > Aggiorna

Configurazione iniziale

Al primo accesso dopo aver attivato MFA, all'utente o all'amministratore verrà richiesto di inserire un indirizzo e-mail o un numero di telefono cellulare. Riceveranno un codice di conferma per partecipare e confermare l'avvenuta registrazione.

Amministrazione del sistema

Creare un account Domain Admin ("livello 3")

Panoramica

Occasionalmente, gli amministratori VDS avranno bisogno di credenziali a livello di dominio per gestire l'ambiente. In VDS questi account sono denominati "livello 3" o ".TECH".

Queste istruzioni mostrano come è possibile creare questi account con le autorizzazioni appropriate.

Controller di dominio Windows Server

Quando si esegue un controller di dominio ospitato internamente (o un controller di dominio locale collegato ad Azure tramite un percorso VPN/Express), è possibile gestire gli account .TECH direttamente in Active Directory Manager.

1. Connettersi al controller di dominio (CWMGR1, DC01 o alla macchina virtuale esistente) con un account admin di dominio (.TECH).
2. Creare un nuovo utente (se necessario).
3. Aggiungere l'utente al gruppo di sicurezza "tecnici livello 3"

[Management.System Administration.creare un account admin di dominio 9ee17] |

Management.System_Administration.create_domain_admin_account-9ee17.png

- a. Se il gruppo di sicurezza "tecnici livello 3" non è presente, crearlo e renderlo membro del gruppo di sicurezza "infrastruttura CW".

[Management.System Administration.create account admin di dominio 0fc27] |



L'aggiunta di ".tech" alla fine del nome utente è una procedura consigliata per delineare gli account amministratore dagli account utente finali.

Servizi di dominio ad Azure

Se vengono eseguiti in Azure ad Domain Services o se si gestisce un utente in Azure ad, questi account possono essere gestiti (ad esempio, la modifica della password) nel portale di gestione Azure come un normale utente Azure ad.

È possibile creare nuovi account, aggiungendoli a questi ruoli per ottenere le autorizzazioni necessarie:

1. Amministratori di AAD DC
2. ClientDHPAccess
3. Amministratore globale nella directory.



L'aggiunta di ".tech" alla fine del nome utente è una procedura consigliata per delineare gli account amministratore dagli account utente finali.



Accesso temporaneo a terze parti

Panoramica

Fornire l'accesso a terze parti è una pratica comune quando si esegue la migrazione a qualsiasi soluzione cloud.

Gli amministratori VDS spesso scelgono di non concedere a queste terze parti lo stesso livello di accesso di cui dispongono, per seguire una policy di accesso di sicurezza "meno richiesta".

Per impostare l'accesso admin per terze parti, accedere a VDS e accedere al modulo Organizations (organizzazioni), fare clic sull'organizzazione e fare clic su Users & Groups (utenti e gruppi).

Quindi, creare un nuovo account utente per la terza parte e scorrere verso il basso fino a visualizzare la sezione accesso amministratore e selezionare la casella per abilitare i diritti di amministratore.



VDS Admin viene quindi visualizzata la schermata di configurazione di Admin Access. Non è necessario modificare il nome utente, l'accesso o la password: Basta aggiungere un numero di telefono e/o un'e-mail se si desidera applicare l'autenticazione multifattore e selezionare il livello di accesso da concedere.

Per gli amministratori di database come un VAR o un ISV, *Server* è generalmente l'unico modulo di accesso richiesto.



Una volta salvato, l'utente finale ottiene l'accesso alle funzioni di gestione automatica accedendo a VDS con le proprie credenziali utente standard di Virtual Desktop.

Quando l'utente appena creato effettua l'accesso, vedrà solo i moduli assegnati. Possono selezionare

l'organizzazione, scorrere verso il basso fino alla sezione Server e connettersi al nome del server indicato (ad esempio, <XYZ> D1, dove XYZ è il codice della società e D1 indica che il server è un server dati. Nell'esempio riportato di seguito, viene indicato di connettersi al server TSD1 per eseguire le assegnazioni.

[]

Configurare la pianificazione del backup

Panoramica

VDS è in grado di configurare e gestire i servizi di backup nativi in alcuni provider di infrastrutture, tra cui Azure.

Azure

In Azure, VDS è in grado di configurare automaticamente i backup utilizzando i backup nativi ["Backup cloud Azure"](#) Con storage ridondante in locale (LRS). Se necessario, lo storage geodundant (GRS) può essere configurato nel portale di gestione Azure.

- È possibile definire singole policy di backup per ciascun tipo di server (con raccomandazioni predefinite). Inoltre, è possibile assegnare a singoli computer una pianificazione indipendente (dal tipo di server) dall'interfaccia utente VDS. Questa impostazione può essere applicata accedendo alla vista dettagli server facendo clic sul nome del server nella pagina Workspace (vedere il video seguente: Impostazione di criteri di backup individuali)
 - Dati
 - Backup con 7 backup giornalieri, 5 settimanali e 2 mensili. Aumentare i periodi di conservazione in base ai requisiti di business.
 - Ciò vale sia per un server dati dedicato che per le VM VPS add-on per applicazioni e database.
 - Infrastruttura
 - CWMGR1 – Backup giornaliero e conservazione 7 giorni su 7, 5 settimane, 2 mesi.
 - Gateway RDS: Backup settimanale e conservazione 4 alla settimana.
 - Gateway HTML5: Backup settimanale e conservazione 4 settimanale.
 - PowerUser (noto anche come utente VDI)
 - Non eseguire il backup della macchina virtuale poiché i dati devono essere memorizzati su un server D1 o TSD1.
 - Tenere presente che alcune applicazioni memorizzano i dati in locale e, in tal caso, è necessario prendere speciali considerazioni.
 - In caso di guasto di una macchina virtuale, è possibile creare una nuova macchina virtuale tramite la clonazione di un'altra. Nel caso in cui sia presente una sola VM VDI (o una build di VM univoca), si consiglia di eseguirne il backup in modo che non sia necessaria una ricostruzione completa della VM.
 - Se necessario, anziché eseguire il backup di tutti i server VDI, è possibile ridurre al minimo i costi configurando manualmente una singola macchina virtuale per il backup direttamente nel portale Azure Management.
 - TS
 - Non eseguire il backup della macchina virtuale poiché i dati devono essere memorizzati su un server D1 o TSD1.

- Tenere presente che alcune applicazioni memorizzano i dati in locale e, in tal caso, è necessario prendere speciali considerazioni.
- In caso di guasto di una macchina virtuale, è possibile creare una nuova macchina virtuale tramite la clonazione di un'altra. Nel caso in cui sia presente una sola VM TS, si consiglia di eseguirne il backup in modo che non sia necessaria una ricostruzione completa della VM.
- Se necessario, anziché eseguire il backup di tutti i server TS, è possibile ridurre al minimo i costi configurando manualmente una singola macchina virtuale per il backup direttamente nel portale Azure Management.

- TSDData

- Backup con 7 backup giornalieri, 5 settimanali e 2 mensili. Aumentare i periodi di conservazione in base ai requisiti di business.
- Le policy possono essere impostate per eseguire backup giornalieri o settimanali, Azure non supporta pianificazioni più frequenti.
- Per le pianificazioni giornaliere, inserire l'ora preferita per eseguire il backup. Per le pianificazioni settimanali, inserire il giorno e l'ora preferiti per eseguire il backup. Nota: Se si imposta l'ora esattamente alle 12:00, si possono verificare problemi in Azure Backup, quindi si consiglia di eseguire le 12:01.
- Definire il numero di backup giornalieri, settimanali, mensili e annuali da conservare.

Impostazione delle impostazioni predefinite di implementazione



Per configurare il backup di Azure per l'intera implementazione, attenersi alla seguente procedura:

1. Accedere alla pagina Deployments Detail (Dettagli implementazioni) e selezionare Backup Defaults (Backup predefiniti)
2. Selezionare un tipo di server dal menu a discesa. I tipi di server sono:

```
Data: these are for LOB/database server types
Infrastructure: these are platform servers
Power User: these are for Users with a TS server dedicated solely to them
TS: these are terminal servers that Users launch sessions on
TSDData: these are servers doubling as terminal and data servers.
```

- In questo modo verranno definite le impostazioni di backup generali per l'intera implementazione. Questi possono essere ignorati e impostati in un secondo momento a un livello specifico del server, se lo si desidera.

3. Fare clic sulla rotella delle impostazioni, quindi sulla finestra a comparsa Edit (Modifica) che viene visualizzata.
4. Selezionare le seguenti impostazioni di backup:

```
On or off
Daily or weekly
What time of day backups take place
How long each backup type (daily, weekly, etc.) should be retained
```

5. Infine, fare clic su Create (o Edit) Schedule (Crea (o Modifica) pianificazione) per attivare queste impostazioni.

Impostazione di singoli criteri di backup

Per applicare le impostazioni di backup integrato specifiche del server, accedere alla pagina dei dettagli dell'area di lavoro.

1. Scorrere verso il basso fino alla sezione Server e fare clic sul nome di un server
2. Fare clic su Aggiungi pianificazione
3. Applicare le impostazioni di backup desiderate e fare clic su Create Schedule (Crea pianificazione)

Ripristino dal backup

Per ripristinare i backup di una determinata macchina virtuale, accedere alla pagina dei dettagli dell'area di lavoro.

1. Scorrere verso il basso fino alla sezione Server e fare clic sul nome di un server
2. Scorrere verso il basso fino alla sezione Backup e fare clic sulla manopola per espandere le opzioni, quindi selezionare una delle due opzioni
3. Restore to Server (Ripristina su server) o Restore to Disk (Ripristina su disco) (collegare un disco dal backup in modo da poter copiare i dati dal backup alla versione esistente della macchina virtuale).
4. Procedere con il ripristino da questo punto in poi come in qualsiasi altro scenario di ripristino.



I costi dipendono dalla pianificazione che si desidera mantenere e sono interamente determinati dai costi di backup di Azure. I prezzi di backup per le macchine virtuali sono disponibili in Azure Cost Calculator: <https://azure.microsoft.com/en-us/pricing/calculator/>

Clonazione di macchine virtuali

Panoramica

Virtual Desktop Service (VDS) consente di clonare una macchina virtuale (VM) esistente. Questa funzionalità è progettata per aumentare automaticamente la disponibilità del numero di unità server in base all'aumento del numero di utenti definiti o per aggiungere server ai pool di risorse disponibili.

Gli amministratori utilizzano la clonazione in VDS in due modi:

1. Creazione automatica on-demand di nuovo server da un server client esistente
2. Creazione automatica proattiva di nuovi server client per la scalabilità automatica delle risorse in base alle regole definite e controllate dai partner

Cloning per aggiungere altri server condivisi

Un clone è una copia di una macchina virtuale esistente. La funzionalità di cloning consente di risparmiare tempo e di scalare gli amministratori, poiché l'installazione di un sistema operativo guest e di applicazioni può richiedere molto tempo. Con i cloni, è possibile eseguire molte copie di una macchina virtuale da un singolo processo di installazione e configurazione. Questo aspetto in genere è simile a:

1. Installare tutte le applicazioni e le impostazioni desiderate su un server TS o TSD
2. Accedere a: Aree di lavoro > Sezione Server > icona ingranaggio per il server di origine > fare clic su Clone (Clona)

3. Consentire l'esecuzione del processo di clonazione (in genere 45-90 minuti)
4. La fase finale attiva il server clonato, inserendolo nel pool RDS per accettare nuove connessioni. I server clonati potrebbero richiedere una singola configurazione dopo essere stati clonati, in modo che VDS aspetti che l'amministratore metta manualmente in rotazione il server.

Ripetere tutte le volte necessarie.[]

Per aumentare la capacità degli utenti in un ambiente host di sessione condivisa, la clonazione di un host di sessione è un processo semplice che richiede solo pochi passaggi.

1. Selezionare un host di sessione da clonare e verificare che nessun utente sia attualmente connesso alla macchina.
2. In VDS, accedere all'area di lavoro del client di destinazione. Scorrere fino alla sezione Server, fare clic sull'icona ingranaggio e selezionare Clone (Clona). Questo processo richiede molto tempo e porta il computer di origine offline. Sono previsti oltre 30 minuti per il completamento.

[] []

3. Il processo arresta il server, clonerà il server in un'altra immagine e preparerà l'immagine al successivo numero di servizio per il cliente. Il server viene visualizzato come *Type=Staged* e *Status=Activation Required* nell'elenco Servers (Server).

[]

4. Accedere al server e verificare che il server sia pronto per la produzione.

[]

5. Quando si è pronti, fare clic su Activate (attiva) per aggiungere il server al pool di host di sessione e iniziare ad accettare le connessioni utente.

[]

Definizione del processo di cloning VDS

Il processo passo per passo è descritto in dettaglio in VDS > Deployment > Task History (VDS > implementazione > Cronologia attività) in qualsiasi operazione di Clone Server. Il processo prevede oltre 20 passaggi, che iniziano con l'accesso all'hypervisor per avviare il processo di clonazione e terminano con l'attivazione del server clonato. Il processo di cloning include passaggi chiave come:

- Configurare il DNS e impostare il nome del server
- Assegnare StaticIP
- Aggiungere al dominio
- Aggiornare Active Directory
- Aggiorna database VDS (istanza SQL su CWMGR1)
- Creare regole firewall per il clone

Oltre a Cronologia attività, i passaggi dettagliati per qualsiasi processo di cloning possono essere visualizzati nel log CwVmAutomationService su CWMGR1 in Virtual Desktop Deployment di ciascun partner. La revisione di questi file di log è documentata ["qui"](#).

Creazione automatica di nuovi server

Questa funzionalità VDS è progettata per aumentare automaticamente la disponibilità del numero di unità server in base all'aumento del numero di utenti definito.

Il partner definisce e gestisce tramite VDS ("") > Client > Panoramica – risorse VM > scalabilità automatica. Sono esposti diversi controlli per consentire ai partner di attivare/disattivare la scalabilità automatica e creare regole personalizzate per ciascun client, ad esempio: Numero/utenti/server, RAM aggiuntiva per utente e numero di utenti per CPU.



In precedenza, si presuppone che la clonazione automatica sia abilitata per l'intera implementazione di Virtual Desktop. Ad esempio, per interrompere tutti i cloning automatici, utilizzare DCConfig, nella finestra Advanced (Avanzate), deselezionare Server Creation (creazione server)→Automated Cloning enabled (clonazione automatica abilitata).

Quando viene eseguito il processo di clonazione automatica?

Il processo automatizzato di clonazione viene eseguito quando la manutenzione giornaliera è configurata per l'esecuzione. L'impostazione predefinita è mezzanotte, ma è possibile modificarla. Parte della manutenzione giornaliera consiste nell'eseguire il thread Change Resources per ogni pool di risorse. Il thread Change Resources determina il numero di server condivisi richiesti in base al numero di utenti della configurazione del pool (personalizzabile; può essere 10, 21, 30, ecc. utenti per server).

Creazione automatica "on-demand" di nuovi server

Questa funzionalità VDS consente la clonazione automatica "on-demand" di server aggiuntivi nei pool di risorse disponibili.

L'amministratore VDS accede a VDS e, sotto i moduli Organizations (organizzazioni) o Workspaces (aree di lavoro), individua il client specifico e apre la scheda Overview (Panoramica). La sezione Server elenca tutti i server (TSD1, TS1, D1, ecc.). Per clonare un singolo server, fare clic sul simbolo all'estrema destra del nome del server e selezionare l'opzione Clone (Clona).

In genere, il processo dovrebbe richiedere circa un'ora. Tuttavia, la durata dipende dalle dimensioni della macchina virtuale e dalle risorse disponibili dell'hypervisor sottostante. Tenere presente che il server clonato dovrà essere riavviato, in modo che i partner eseguano in genere dopo l'orario di lavoro o durante una finestra di manutenzione pianificata.

Durante la clonazione di un server TSData, uno dei passaggi consiste nell'eliminare le cartelle c: Home, c: Dati e c: Pro in modo che non siano file duplicati. In questo caso, il processo di clonazione non è riuscito. Si sono verificati problemi durante l'eliminazione di questi file. Questo errore è vago. In genere, questo significa che l'evento clone non è riuscito a causa di un file o processo aperto. Tentativo successivo, disattivare qualsiasi AV (perché questo potrebbe spiegare questo errore).

Funzione di aumento automatico dello spazio su disco

Panoramica

NetApp riconosce la necessità di offrire agli amministratori un modo semplice per garantire che gli utenti abbiano sempre spazio per accedere e salvare i documenti. In questo modo, le macchine virtuali dispongono anche di spazio libero sufficiente per completare correttamente i backup, consentendo agli amministratori e ai piani di disaster recovery e business continuity. Tenendo presente questo aspetto, abbiamo creato una funzionalità che espande automaticamente il disco gestito in uso al livello successivo quando un disco sta funzionando in poco spazio.

Si tratta di un'impostazione che viene applicata per impostazione predefinita a tutte le nuove implementazioni VDS in Azure, garantendo che tutte le implementazioni proteggano gli utenti e i backup del tenant per impostazione predefinita.

Gli amministratori possono verificare che sia stata eseguita questa operazione accedendo alla scheda Deployments (implementazioni), selezionando un'implementazione e quindi connettendosi al server CWMGR1. Quindi, aprire il collegamento DCConfig sul desktop, fare clic su Advanced (Avanzate) e scorrere verso il basso.

[]

Gli amministratori possono modificare la quantità di spazio libero desiderata in GB liberi o in percentuale del disco che deve essere libero prima di passare al successivo Tier di dischi gestiti nella stessa sezione Advanced di DCConfig.

[]

Alcuni esempi pratici di applicazione:

- Se si desidera assicurarsi che sul disco siano disponibili almeno 50 GB, impostare MinFreeSpaceGB su 50
- Se si desidera assicurarsi che almeno il 15% del disco sia libero, impostare MinFreeSpacePercent da 10 a 15.

Questa azione si svolge a mezzanotte del fuso orario del server.

Accesso alle credenziali VDS in Azure Key Vault

Panoramica

CWASetup 5.4 è una deviazione dai precedenti metodi di implementazione di Azure. Il processo di configurazione e convalida è ottimizzato per ridurre la quantità di informazioni necessarie per iniziare un'implementazione. Molti di questi prompt rimossi riguardano credenziali o account come Local VM Admin, SMTP account, Tech account, SQL SA, ecc. Questi account vengono ora generati automaticamente e memorizzati in un archivio chiavi Azure. Per impostazione predefinita, l'accesso a questi account generati automaticamente richiede un passaggio aggiuntivo, descritto di seguito.

- Individuare la risorsa "vault delle chiavi" e fare clic su di essa:

[larghezza=75%]

- In 'Impostazioni', fare clic su 'Screts'. Viene visualizzato un messaggio che indica che non si è autorizzati a visualizzare:

[larghezza=75%]

- Aggiungere una 'policy di accesso' per concedere a un account Azure ad (come un amministratore globale o un amministratore di sistema) l'accesso a queste chiavi sensibili:

[larghezza=75%]

- In questo esempio viene utilizzato un amministratore globale. Dopo aver selezionato l'entità, fare clic su 'Select' (Seleziona), quindi su 'Add' (Aggiungi):

[larghezza=75%]

- Fare clic su 'S'Save' (Salva):

[larghezza=75%]

- Policy di accesso aggiunta correttamente:

[larghezza=75%]

- Rivisitare i 'Ssegreti' per verificare che l'account disponga ora dell'accesso agli account di implementazione:

[larghezza=75%]

- Ad esempio, se è stata richiesta la credenziale Domain Administrator per accedere a CWMGR1 e aggiornare i criteri di gruppo, controllare le stringhe in `cjDomainAdministratorName` e `cjDomainAdministratorPassword` facendo clic su ciascuna voce:

[larghezza=75%]

[larghezza=75%]

- Mostra o copia il valore:

[larghezza=75%]

Applicare Monitoring and Antivirus

Panoramica

Gli amministratori di Virtual Desktop Service (VDS) sono responsabili del monitoraggio dell'infrastruttura della piattaforma (che sarà costituita da CWMGR1 al minimo) e di tutte le altre infrastrutture e macchine virtuali (VM). Nella maggior parte dei casi, gli amministratori organizzano il monitoraggio dell'infrastruttura (hypervisor/SAN) direttamente con il proprio data center/provider IaaS. Gli amministratori sono responsabili del monitoraggio di server terminal e dati, in genere implementando la soluzione RMM (Remote Management and Monitoring) preferita.

L'antivirus è responsabilità dell'amministratore (sia per l'infrastruttura della piattaforma che per le macchine virtuali dei server di dati/terminali). Per semplificare questo processo, i server VDS per Azure utilizzano Windows Defender per impostazione predefinita.



Quando si installano soluzioni di terze parti, assicurarsi di non includere firewall o altri componenti che potrebbero interferire con l'automazione VDS.

In particolare, quando per impostazione predefinita sono in vigore policy antivirus molto specifiche, ciò può causare effetti negativi quando questi agenti antivirus vengono installati su un server gestito da Virtual Desktop Service.

La nostra guida generale è che, sebbene l'automazione della piattaforma VDS non sia generalmente influenzata dai prodotti antivirus o anti-malware, è consigliabile aggiungere eccezioni/esclusioni per i seguenti processi su tutti i server della piattaforma (CWMGR1, RDGateway, HTML5Gateway, FTP, ecc.):

```
*\paexec.exe
*\paexec_1_25.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CW Automation
Service\cw.automation.service.exe
C:\Program
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Printer.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Services.exe
```

Inoltre, si consiglia di elencare in modo sicuro i seguenti processi sui server client:

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe
C:\Program Files\CloudWorkspace\Pen\Pen.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

Aggiunta e spostamento di unità mappate

Panoramica

Per impostazione predefinita, sono presenti tre cartelle condivise esposte alle sessioni dell'utente finale. Queste cartelle si trovano nel layer di storage definito. Potrebbe trattarsi di un file server (TSD1 o D1) o di un servizio di storage come Azure Files, Azure NetApp Files, NetApp CVO e NetApp CVS.

Per maggiore chiarezza, in questo articolo verrà utilizzato un cliente di esempio con il codice aziendale "NECA". Questo esempio presuppone che sia stato implementato un singolo server TDS1, denominato NECATSD1. Lavoreremo attraverso il processo di spostamento di una cartella in un'altra macchina virtuale (chiamata "NECAD1"). Questa strategia può essere utilizzata per passare da una partizione all'altra sullo stesso computer o su un'altra macchina, come illustrato nell'esempio seguente...

Percorso iniziale cartelle:

- Dati: NECATSD1 (TSD1 significa che è il primo Terminal Server e funziona anche come Data Server)
- FTP: NECATSD1
- Home: NECATSD1

Posizione finale cartelle:

- Data: NECAD1/G: Data (il D1significa che è il primo server dati)
- FTP: Lo stesso processo si applica, non è necessario descriverlo per 3 volte
- Home: Lo stesso processo si applica, non è necessario descriverlo per 3 volte

Add disk for G (Aggiungi disco per G): Su NECAD1

1. Per inserire la cartella condivisa nell'unità e: È necessario aggiungerne una tramite l'hypervisor (ad esempio Azure Management Portal), quindi inicializzarla e formattarla

[]

2. Copiare il percorso della cartella esistente (su NECATSD1, C:) nella nuova posizione (su NECAD1, G:)
3. Copiare le cartelle dalla posizione originale alla nuova posizione.

[]

Raccolta di informazioni dalla condivisione della cartella originale (NECATSD1, C: Data)

1. Condividere la nuova cartella utilizzando lo stesso percorso della cartella nella posizione originale.
2. Aprire la nuova cartella NECAD1, G: E nell'esempio viene visualizzata una cartella denominata codice società, "NECA".

[]

3. Nota: Le autorizzazioni di sicurezza della condivisione della cartella originale:

[]

4. Di seguito viene riportato il setup tipico, tuttavia è importante copiare le impostazioni originali nel caso in cui siano presenti personalizzazioni da conservare. Tutte le altre autorizzazioni utente/gruppo devono essere rimosse dalla nuova condivisione della cartella
 - SISTEMA:autorizzazioni consentite
 - LocalClientDHPAccess (sul computer locale):autorizzazioni consentite
 - ClientDHPAccess (sul dominio): Sono consentite tutte le autorizzazioni
 - NECA-All users (sul dominio): Sono consentite tutte le autorizzazioni, ad eccezione di "controllo completo"

Replicare il percorso di condivisione e le autorizzazioni di sicurezza nella nuova cartella condivisa

1. Tornare alla nuova posizione (NECAD1, G: Data) e condividere la cartella NECA con lo stesso percorso di rete (escluso il computer), nel nostro esempio "neca-data"

[]

2. Per la sicurezza degli utenti, aggiungere tutti gli utenti e impostare le relative autorizzazioni in modo che corrispondano.

[]

3. Rimuovere qualsiasi altra autorizzazione utente/gruppo che potrebbe già esistere.

[]

Modifica criteri di gruppo (solo se la cartella viene spostata su una nuova macchina)

1. Quindi, modificare Drive Maps (Mappe dischi) in Group Policy Management Editor (Editor di gestione dei criteri di gruppo). Per Azure ad Domain Services, la mappatura si trova in:

```
"Cloud Workspace Users > User Configuration > Preferences > Windows Settings > Drive Maps"
```

[]

2. Una volta aggiornati i criteri di gruppo, alla successiva connessione di ciascun utente, verranno visualizzati i dischi mappati che vengono riportati alla nuova posizione.
3. A questo punto è possibile eliminare le cartelle originali su NECATSD1, C:.

Risoluzione dei problemi

Se l'utente finale visualizza le unità mappate con una X rossa, fare clic con il pulsante destro del mouse sull'unità e selezionare Disconnect (Disconnetti). La disconnessione e la riconnessione dell'unità saranno presenti correttamente.[]

Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.