Implementazione con VDS

Virtual Desktop Service

NetApp
May 24, 2023

Sommario

Implementazione con VDS

Azure

Desktop virtuale Azure

Guida all'implementazione di AVD

Panoramica

Questa guida fornirà le istruzioni dettagliate per creare un'implementazione di Azure Virtual Desktop (AVD) utilizzando NetApp Virtual Desktop Service (VDS) in Azure.

La guida inizia da: https://cwasetup.cloudworkspace.com/

Questa guida POC (Proof of of concept) è progettata per aiutarti a implementare e configurare rapidamente AVD nel tuo abbonamento Azure di prova. Questa guida presuppone un'implementazione green-field in un tenant Azure Active Directory pulito e non in produzione.

Le implementazioni in produzione, in particolare negli ambienti ad o Azure ad esistenti, sono molto comuni, tuttavia questo processo non viene considerato in questa guida POC. I POC complessi e le implementazioni di produzione devono essere avviati con i team di vendita/servizi VDS di NetApp e non eseguiti in modo self-service.

Questo documento POC ti illustrerà l'intera implementazione di AVD e ti fornirà una breve panoramica delle principali aree della configurazione post-implementazione disponibili nella piattaforma VDS. Una volta completato, avrai un ambiente AVD completamente implementato e funzionale, completo di pool di host, gruppi di applicazioni e utenti. In alternativa, avrai la possibilità di configurare la distribuzione automatica delle applicazioni, i gruppi di sicurezza, le autorizzazioni di condivisione file, Azure Cloud Backup, l'ottimizzazione intelligente dei costi. VDS implementa una serie di impostazioni di Best practice tramite GPO. Sono inoltre incluse istruzioni su come disattivare facoltativamente questi controlli, nel caso in cui il POC non necessiti di alcun controllo di sicurezza, in modo simile a un ambiente di dispositivi locali non gestito.

Nozioni di base su AVD

Azure Virtual Desktop è un servizio completo di virtualizzazione di applicazioni e desktop eseguito nel cloud. Ecco un rapido elenco di alcune delle funzionalità principali:

- Servizi della piattaforma, tra cui gateway, brokering, licenze e accesso, inclusi come servizio da Microsoft. Questa infrastruttura ha ridotto al minimo la necessità di hosting e gestione.
- Azure Active Directory può essere utilizzato come provider di identità, consentendo la stratificazione di servizi di sicurezza aggiuntivi di Azure come l'accesso condizionale.
- Gli utenti sperimentano un'esperienza di single sign-on per i servizi Microsoft.
- Le sessioni utente si connettono all'host di sessione tramite una tecnologia proprietaria di connessione inversa. Ciò significa che non è necessario aprire porte in entrata, ma che un agente crea una connessione in uscita al piano di gestione AVD che a sua volta si connette al dispositivo dell'utente finale.
- La connessione inversa consente anche l'esecuzione delle macchine virtuali senza essere esposte a Internet pubblico, consentendo carichi di lavoro isolati anche mantenendo la connettività remota.
- AVD include l'accesso a Windows 10 Multi Session, consentendo un'esperienza Windows 10 Enterprise con l'efficienza delle sessioni utente ad alta densità.

- La tecnologia di containerizzazione del profilo FSLogix include, migliorando le performance delle sessioni utente, l'efficienza dello storage e l'esperienza di Office in ambienti non persistenti.
- AVD supporta l'accesso completo a desktop e RemoteApp. Esperienze sia persistenti che non persistenti, sia dedicate che multisessione.
- Le organizzazioni possono risparmiare sulle licenze Windows perché AVD può sfruttare "Windows 10 Enterprise E3 per utente", che sostituisce la necessità di CAL RDS e riduce significativamente il costo orario delle VM host di sessione in Azure.

Scopo della guida

Questa guida illustra l'implementazione di AVD utilizzando la tecnologia NetApp VDS dal punto di vista di un amministratore di Azure e VDS. Il tenant e l'abbonamento Azure sono disponibili senza preconfigurazione e questa guida consente di configurare AVD end-to-end

Questa guida illustra i seguenti passaggi:

1. Confermare i prerequisiti per le autorizzazioni del tenant Azure, dell'abbonamento Azure e dell'account amministratore Azure
2. Raccogliere i dettagli di rilevamento richiesti
3. Crea l'ambiente Azure utilizzando la procedura guidata VDS per Azure
4. Creare il primo pool di host con un'immagine EVD standard di Windows 10
5. Assegnazione di desktop virtuali agli utenti di Azure ad
6. Aggiungere utenti al gruppo di applicazioni predefinito per fornire l'ambiente desktop agli utenti. Facoltativamente, Creare pool di host aggiuntivi per l'erogazione dei servizi RemoteApp
7. Connettersi come utente finale tramite software client e/o client Web
8. Connettersi alla piattaforma e ai servizi client come amministratore locale e di dominio
9. <<Autenticazione multifattore (MFA),Facoltativamente, abilitare l'autenticazione a più fattori di VDS per gli amministratori VDS utenti finali AVD
10. Se lo si desidera, esaminare l'intero flusso di lavoro relativo ai diritti dell'applicazione, inclusi il popolamento della libreria delle applicazioni, l'automazione dell'installazione delle applicazioni, il mascheramento delle applicazioni da parte degli utenti e dei gruppi di sicurezza
11. Facoltativamente, è possibile creare e gestire gruppi di sicurezza, permessi delle cartelle e diritti delle applicazioni di Active Directory per gruppo.
12. Facoltativamente, è possibile configurare le tecnologie di ottimizzazione dei costi, tra cui Workload Scheduling e Live Scaling
13. Facoltativamente, creare, aggiornare e Sysprep un'immagine della macchina virtuale per implementazioni future
14. Configurazione facoltativa di Azure Cloud Backup
15. Se si desidera, disattivare i criteri predefiniti dei gruppi di controllo della protezione

Prerequisiti di Azure

VDS utilizza il contesto di sicurezza nativo di Azure per implementare l'istanza di AVD. Prima di avviare l'installazione guidata di VDS, è necessario stabilire alcuni prerequisiti di Azure.

Durante l'implementazione, gli account di servizio e le autorizzazioni vengono concessi a VDS tramite l'autenticazione di un account amministratore esistente all'interno del tenant Azure.

Rapida lista di controllo dei prerequisiti

- Azure Tenant con istanza di Azure ad (può essere un'istanza di Microsoft 365)
- Abbonamento Azure
- Quota Azure disponibile per le macchine virtuali Azure
- Azure Admin account con ruoli di amministrazione globale e di proprietà dell'abbonamento

I prerequisiti dettagliati sono documentati a. "Questo PDF"

Amministratore di Azure in Azure ad

Questo amministratore Azure esistente deve essere un account Azure ad nel tenant di destinazione. Gli account Windows Server ad possono essere implementati con VDS Setup, ma sono necessari ulteriori passaggi per configurare una sincronizzazione con Azure ad (fuori dall'ambito di questa guida)

Questa operazione può essere confermata trovando l'account utente nel portale di gestione Azure in utenti > tutti gli utenti.[]

Ruolo di amministratore globale

All'amministratore di Azure deve essere assegnato il ruolo di amministratore globale nel tenant di Azure.

Per verificare il tuo ruolo in Azure ad, segui questa procedura:

1. Accedere al portale Azure all'indirizzo https://portal.azure.com/
2. Cercare e selezionare Azure Active Directory
3. Nel riquadro successivo a destra, fare clic sull'opzione Users (utenti) nella sezione Manage (Gestione)
4. Fare clic sul nome dell'utente amministratore che si sta controllando
5. Fare clic su Directory role (ruolo directory). Nel riquadro all'estrema destra dovrebbe essere elencato il ruolo di amministratore globale[]

Se questo utente non ha il ruolo di amministratore globale, è possibile eseguire i seguenti passaggi per aggiungerlo (si noti che l'account connesso deve essere un amministratore globale per eseguire questi passaggi):

1. Dalla pagina User Directory role detail (Dettagli ruolo directory utente) del passaggio 5, fare clic sul pulsante Add Assignment (Aggiungi assegnazione) nella parte superiore della pagina Detail (Dettagli).
2. Fare clic su Global Administrator nell'elenco dei ruoli. Fare clic sul pulsante Add (Aggiungi).[]

Proprietà dell'abbonamento Azure

Azure Administrator deve essere anche un Subscription Owner nell'abbonamento che conterrà l'implementazione.

Per verificare che l'amministratore sia un proprietario dell'abbonamento, attenersi alla seguente procedura:

1. Accedere al portale Azure all'indirizzo https://portal.azure.com/
2. Cercare e selezionare Abbonamenti
3. Nel riquadro successivo a destra, fare clic sul nome dell'abbonamento per visualizzare i dettagli dell'abbonamento
4. Fare clic sulla voce di menu Access Control (IAM) nel riquadro, quindi da sinistra

5. Fare clic sulla scheda assegnazioni ruoli. L'amministratore di Azure deve essere elencato nella sezione Owner (Proprietario).[]

Se Azure Administrator non è presente nell'elenco, è possibile aggiungere l'account come proprietario dell'abbonamento seguendo questa procedura:

1. Fare clic sul pulsante Add (Aggiungi) nella parte superiore della pagina e selezionare l'opzione Add role Assignment (Aggiungi assegnazione ruolo)
2. Viene visualizzata una finestra di dialogo a destra. Scegliere "Proprietario" nell'elenco a discesa ruolo, quindi digitare il nome utente dell'amministratore nella casella Seleziona. Quando viene visualizzato il nome completo dell'amministratore, selezionarlo
3. Fare clic sul pulsante Save (Salva) nella parte inferiore della finestra di dialogo[]

Quota core di calcolo di Azure

L'installazione guidata CWA e il portale VDS creeranno nuove macchine virtuali e l'abbonamento Azure deve disporre di una quota disponibile per poter eseguire correttamente .

Per controllare la quota, attenersi alla seguente procedura:

1. Accedere al modulo Abbonamenti e fare clic su "utilizzo + quote"
2. Selezionare tutti i provider nell'elenco a discesa "provider", quindi "Microsoft.Compute" nell'elenco a discesa "Provider"
3. Selezionare la regione di destinazione nell'elenco a discesa "sedi"
4. Viene visualizzato un elenco delle quote disponibili per famiglia di macchine virtuali[]Se è necessario aumentare la quota, fare clic su Richiedi aumento e seguire le istruzioni per aggiungere ulteriore capacità. Per l'implementazione iniziale, richiedere un preventivo più elevato per la "Standard DSv3 Family vCPU"

Raccogliere i dettagli del rilevamento

Una volta eseguita l'installazione guidata di CWA, è necessario rispondere a diverse domande. NetApp VDS ha fornito un PDF collegato che può essere utilizzato per registrare queste selezioni prima dell'implementazione. L'elemento include:

Elemento	Descrizione
Credenziali di amministrazione VDS	Raccogliere le credenziali di amministratore VDS esistenti, se già presenti. In caso contrario, durante l'implementazione verrà creato un nuovo account admin.
Regione di Azure	Determinare la regione Azure di destinazione in base alle performance e alla disponibilità dei servizi. Questo "Tool Microsoft" può stimare l'esperienza dell'utente finale in base alla regione.
Tipo di Active Directory	Le macchine virtuali dovranno unirsi a un dominio, ma non possono entrare direttamente in Azure ad. L'implementazione di VDS può creare una nuova macchina virtuale o utilizzare un controller di dominio esistente.

Elemento	Descrizione
Gestione dei file	Le performance dipendono in larga misura dalla velocità del disco, in particolare per quanto riguarda lo storage del profilo utente. L'installazione guidata di VDS può implementare un semplice file server o configurare Azure NetApp Files (ANF). Per quasi tutti gli ambienti di produzione, si consiglia l'utilizzo di ANF, tuttavia per un POC l'opzione del file server fornisce performance sufficienti. Le opzioni di storage possono essere riviste dopo l'implementazione, anche utilizzando le risorse di storage esistenti in Azure. Consulta i prezzi ANF per i dettagli: https://azure.microsoft.com/en-us/pricing/details/netapp/
Ambito della rete virtuale	Per l'implementazione è necessario un intervallo di rete routable /20. L'installazione guidata VDS consente di definire questo intervallo. È importante che questo intervallo non si sovrapponga a nessun vNet esistente in Azure o on-premise (se le due reti saranno connesse tramite VPN o ExpressRoute).

Sezioni di configurazione VDS

Accedere a. https://cwasetup.cloudworkspace.com/ Con le credenziali di amministratore di Azure trovate nella sezione dei prerequisiti.

IaaS e piattaforma

[]

Nome di dominio Azure ad

Il nome di dominio Azure ad viene ereditato dal tenant selezionato.

Posizione

Selezionare una **Regione Azure** appropriata. Questo "Tool Microsoft" può stimare l'esperienza dell'utente finale in base alla regione.

Tipo di Active Directory

È possibile eseguire il provisioning di VDS con una nuova macchina virtuale** per la funzione del controller di dominio o impostare un controller di dominio esistente. In questa guida selezioneremo New Windows Server Active Directory, che creerà una o due macchine virtuali (in base alle scelte effettuate durante questo processo) sotto l'abbonamento.

È disponibile un articolo dettagliato relativo a una distribuzione ad esistente "qui".

Nome di dominio di Active Directory

Immettere un nome di dominio **. Si consiglia di eseguire il mirroring del nome di dominio ad Azure riportato sopra.

Gestione dei file

VDS può eseguire il provisioning di una semplice macchina virtuale di file server o configurare Azure NetApp Files. In produzione, Microsoft consiglia di allocare 30 gb per utente e abbiamo osservato che per ottenere performance ottimali è necessario allocare 5-15 IOPS per utente.

In un ambiente POC (non in produzione), il file server è un'opzione di implementazione semplice e a basso costo, tuttavia le performance disponibili dei dischi gestiti Azure possono essere sopraffatte dal consumo di IOPS anche di una piccola implementazione in produzione.

Ad esempio, un disco SSD standard da 4 TB in Azure supporta fino a 500 IOPS, che potrebbero supportare solo un massimo di 100 utenti totali a 5 IOPS/utente. Con ANF Premium, la configurazione dello storage delle stesse dimensioni supporterebbe 16,000 IOPS con un numero di IOPS di 32 volte superiore.

Per le implementazioni AVD in produzione, **Azure NetApp Files è consigliato da Microsoft**.

Azure NetApp Files deve essere reso disponibile per l'abbonamento in cui si desidera implementare. Contattare il responsabile del proprio account NetApp o utilizzare questo xref:{relative_path} https://aka.ms/azurenetappfiles

È inoltre necessario registrare NetApp come provider per l'abbonamento. Per eseguire questa operazione, procedere come segue:

- Accedere a Subscriptions (Abbonamenti) nel portale Azure
  - Fare clic su Provider di risorse
  - Filtro per NetApp
  - Selezionare il provider e fare clic su Register (Registra)

Numero di licenza RDS

NetApp VDS può essere utilizzato per implementare ambienti RDS e/o AVD. Durante l'implementazione di AVD, questo campo può **rimanere vuoto**.

ThinPrint

NetApp VDS può essere utilizzato per implementare ambienti RDS e/o AVD. Durante l'implementazione di AVD, questo interruttore può rimanere **spento** (alternato a sinistra).

E-mail di notifica

VDS invierà le notifiche di implementazione e i report sullo stato di salute in corso all'e-mail fornita**. Questa operazione può essere modificata in seguito.

Macchine virtuali e rete

Per supportare un ambiente VDS, è necessario eseguire una serie di servizi, denominati collettivamente "piattaforma VDS". A seconda della configurazione, questi possono includere CWMGR, uno o due gateway RDS, uno o due gateway HTML5, un server FTPS e una o due macchine virtuali Active Directory.

La maggior parte delle implementazioni AVD sfrutta l'opzione di macchina virtuale singola, poiché Microsoft gestisce i gateway AVD come servizio PaaS.

Per ambienti più piccoli e semplici che includano casi di utilizzo RDS, tutti questi servizi possono essere condensati nell'opzione di macchina virtuale singola per ridurre i costi delle macchine virtuali (con scalabilità limitata). Per i casi di utilizzo RDS con più di 100 utenti, si consiglia di utilizzare più macchine virtuali per facilitare la scalabilità del gateway RDS e/o HTML5[]

Configurazione delle macchine virtuali della piattaforma

NetApp VDS può essere utilizzato per implementare ambienti RDS e/o AVD. Quando si implementa AVD, si consiglia di selezionare una singola macchina virtuale. Per le implementazioni RDS è necessario implementare e gestire componenti aggiuntivi come Brokers e Gateway, in produzione questi servizi devono essere eseguiti su macchine virtuali dedicate e ridondanti. Per AVD, tutti questi servizi sono forniti da Azure come servizio incluso e pertanto si consiglia la configurazione **singola macchina virtuale**.

Singola macchina virtuale

Si tratta della scelta consigliata per le implementazioni che utilizzeranno esclusivamente AVD (e non RDS o una combinazione delle due). In un'implementazione di una singola macchina virtuale, i seguenti ruoli sono tutti ospitati su una singola macchina virtuale in Azure:

- Gestore CW
- Gateway HTML5
- Gateway RDS
- Applicazione remota
- Server FTPS (opzionale)
- Ruolo del controller di dominio

Il numero massimo di utenti consigliato per i casi di utilizzo RDS in questa configurazione è di 100 utenti. I gateway RDS/HTML5 con bilanciamento del carico non sono un'opzione in questa configurazione, limitando la ridondanza e le opzioni per aumentare la scalabilità in futuro. Anche in questo caso, questo limite non si applica alle implementazioni AVD, poiché Microsoft gestisce i gateway come servizio PaaS.

Se questo ambiente è progettato per la multi-tenancy, la configurazione di una singola macchina virtuale non è supportata, né AVD né ad Connect.

Più macchine virtuali

Quando si suddivide la piattaforma VDS in più macchine virtuali, i seguenti ruoli vengono ospitati su macchine virtuali dedicate in Azure:

- Remote Desktop Gateway

  VDS Setup può essere utilizzato per implementare e configurare uno o due gateway RDS. Questi gateway ritrasmettono la sessione utente RDS da Internet aperta alle macchine virtuali host della sessione all'interno dell'implementazione. I gateway RDS gestiscono una funzione importante, proteggendo RDS dagli attacchi diretti da Internet aperto e crittografando tutto il traffico RDS in entrata e in uscita dall'ambiente. Quando vengono selezionati due Remote Desktop Gateway, VDS Setup implementa 2 VM e le configura in modo da bilanciare il carico delle sessioni utente RDS in entrata.

- Gateway HTML5

  VDS Setup può essere utilizzato per implementare e configurare uno o due gateway HTML5. Questi gateway ospitano i servizi HTML5 utilizzati dalla funzione *Connect to Server* in VDS e dal client VDS basato su Web (H5 Portal). Quando vengono selezionati due portali HTML5, VDS Setup implementa 2 VM e le configura in modo da bilanciare il carico delle sessioni utente HTML5 in entrata.

Quando si utilizza un'opzione con più server (anche se gli utenti si connettono solo tramite il client VDS installato), si consiglia di utilizzare almeno un gateway HTML5 per abilitare la funzionalità *Connect to Server* da VDS.

- Note sulla scalabilità del gateway

  Per i casi di utilizzo RDS, è possibile scalare le dimensioni massime dell'ambiente con macchine virtuali gateway aggiuntive, con ciascun gateway RDS o HTML5 che supporta circa 500 utenti. È possibile aggiungere altri gateway in un secondo momento con un'assistenza dei servizi professionali NetApp minima

Se questo ambiente è progettato per la multi-tenancy, è necessario selezionare più macchine virtuali.

Fuso orario

Sebbene l'esperienza degli utenti finali rifletta il fuso orario locale, è necessario selezionare un fuso orario predefinito. Selezionare il fuso orario da cui eseguire la **amministrazione primaria** dell'ambiente.

Ambito della rete virtuale

Si consiglia di isolare le macchine virtuali in sottoreti diverse in base al loro scopo. In primo luogo, definire l'ambito di rete e aggiungere un intervallo /20.

VDS Setup rileva e suggerisce un intervallo che dovrebbe avere successo. In base alle Best practice, gli indirizzi IP della subnet devono rientrare in un intervallo di indirizzi IP privati.

Questi intervalli sono:

- da 192.168.0.0 a 192.168.255.255
- da 172.16.0.0 a 172.31.255.255
- da 10.0.0.0 a 10.255.255.255

Esaminare e regolare se necessario, quindi fare clic su Validate (convalida) per identificare le subnet per ciascuna delle seguenti opzioni:

- Tenant (tenant): Intervallo in cui risiedono i server host di sessione e i server di database
- Servizi: Questa è la gamma in cui risiedono i servizi PaaS come Azure NetApp Files
- Platform (piattaforma): Intervallo in cui risiedono i server della piattaforma
- Directory (Directory): Intervallo in cui risiedono i server ad

Revisione

L'ultima pagina offre l'opportunità di rivedere le tue scelte. Una volta completata la revisione, fare clic sul pulsante convalida. VDS Setup esaminerà tutte le voci e verificherà che l'implementazione possa procedere con le informazioni fornite. Questa convalida può richiedere 2-10 minuti. Per seguire l'avanzamento, fare clic sul logo del registro (in alto a destra) per visualizzare l'attività di convalida.

Una volta completata la convalida, viene visualizzato il pulsante verde Provision (Provision) al posto del pulsante Validate (convalida). Fare clic su Provision (Provision) per avviare il processo di provisioning per l'implementazione.

Stato

Il processo di provisioning richiede 2-4 ore a seconda del carico di lavoro di Azure e delle scelte effettuate. È possibile seguire l'avanzamento del registro facendo clic sulla pagina Status (Stato) o attendere l'e-mail che indica il completamento del processo di implementazione. L'implementazione crea le macchine virtuali e i componenti Azure necessari per supportare sia VDS che un desktop remoto o un'implementazione AVD. Ciò include una singola macchina virtuale che può fungere sia da host di sessione di Desktop remoto che da file server. In un'implementazione AVD, questa macchina virtuale agirà solo come file server.

Installare e configurare ad Connect

Una volta completata l'installazione, è necessario installare e configurare ad Connect nel controller di dominio. In una configurazione VM con piattaforma Singe, la macchina CWMGR1 è la DC. Gli utenti di ad devono eseguire la sincronizzazione tra Azure ad e il dominio locale.

Per installare e configurare ad Connect, attenersi alla seguente procedura:

1. Connettersi al controller di dominio come amministratore di dominio.
    a. Ottenere le credenziali da Azure Key Vault (vedere "Istruzioni del vault chiave qui")
2. Installare ad Connect, effettuare l'accesso con l'amministratore di dominio (con le autorizzazioni di ruolo Enterprise Admin) e Azure ad Global Admin

Attivazione dei servizi AVD

Una volta completata l'implementazione, il passaggio successivo consiste nell'attivare la funzionalità AVD. Il processo di abilitazione di AVD richiede all'amministratore di Azure di eseguire diversi passaggi per registrare il proprio dominio Azure ad e l'abbonamento per l'accesso utilizzando i servizi Azure AVD. Allo stesso modo, Microsoft richiede che VDS richieda le stesse autorizzazioni per la nostra applicazione di automazione in Azure. I passaggi riportati di seguito illustrano il processo.

Creare un pool di host AVD

L'accesso dell'utente finale alle macchine virtuali AVD è gestito dai pool di host , che contengono le macchine virtuali e i gruppi di applicazioni, che a loro volta contengono gli utenti e il tipo di accesso dell'utente.

Per creare il primo pool di host

1. Fare clic sul pulsante Add (Aggiungi) sul lato destro dell'intestazione della sezione AVD host Pools (pool di host AVD).[]
2. Immettere un nome e una descrizione per il pool di host.
3. Scegliere un tipo di pool di host
    a. **In pool** significa che più utenti accederanno allo stesso pool di macchine virtuali con le stesse applicazioni installate.
    b. **Personale** crea un pool di host a cui gli utenti sono assegnati alla propria macchina virtuale host di sessione.
4. Selezionare il tipo di bilanciamento del carico
    a. **Depth First** riempirà la prima macchina virtuale condivisa fino al numero massimo di utenti prima di iniziare sulla seconda macchina virtuale del pool
    b. **La larghezza prima** distribuirà gli utenti a tutte le macchine virtuali del pool in modo round robin
5. Selezionare un modello di macchine virtuali Azure per la creazione delle macchine virtuali in questo pool. Sebbene VDS mostri tutti i modelli disponibili nell'abbonamento, si consiglia di selezionare la build multiutente più recente di Windows 10 per ottenere un'esperienza ottimale. L'attuale build è Windows-10-

20h1-evd. (Facoltativamente, creare un'immagine Gold utilizzando la funzionalità Provisioning Collection per creare host da un'immagine di macchina virtuale personalizzata)

6. Selezionare la dimensione della macchina Azure. A scopo di valutazione, NetApp consiglia la serie D (tipo di macchina standard per più utenti) o e (configurazione della memoria avanzata per scenari multi-utente più pesanti). Le dimensioni della macchina possono essere modificate successivamente in VDS se si desidera sperimentare serie e dimensioni diverse
7. Selezionare un tipo di storage compatibile per le istanze del disco gestito delle macchine virtuali dall'elenco a discesa
8. Selezionare il numero di macchine virtuali che si desidera creare come parte del processo di creazione del pool di host. È possibile aggiungere macchine virtuali al pool in un secondo momento, ma VDS crea il numero di macchine virtuali richieste e le aggiunge al pool di host una volta creato
9. Fare clic sul pulsante Add host pool (Aggiungi pool host) per avviare il processo di creazione. È possibile tenere traccia dei progressi nella pagina AVD oppure visualizzare i dettagli del registro del processo nella pagina Deployments/Deployment name (Nome distribuzione/distribuzione) nella sezione Tasks (attività)
10. Una volta creato, il pool di host viene visualizzato nell'elenco dei pool di host nella pagina AVD. Fare clic sul nome del pool di host per visualizzare la relativa pagina dei dettagli, che include un elenco delle macchine virtuali, dei gruppi di applicazioni e degli utenti attivi

> Gli host AVD in VDS vengono creati con un'impostazione che non consente la connessione delle sessioni utente. Questo è progettato per consentire la personalizzazione prima di accettare le connessioni dell'utente. Questa impostazione può essere modificata modificando le impostazioni dell'host di sessione. []

Abilitare i desktop VDS per gli utenti

Come indicato in precedenza, VDS crea tutti gli elementi necessari per supportare le aree di lavoro degli utenti finali durante l'implementazione. Una volta completata l'implementazione, il passaggio successivo consiste nell'abilitare l'accesso allo spazio di lavoro per ogni utente che si desidera introdurre nell'ambiente AVD. Questa fase crea la configurazione del profilo e l'accesso al livello di dati dell'utente finale che sono i valori predefiniti per un desktop virtuale. VDS riutilizza questa configurazione per collegare gli utenti finali di Azure ad ai pool di applicazioni AVD.

Per abilitare le aree di lavoro per gli utenti finali, attenersi alla seguente procedura:

1. Accedere a VDS all'indirizzo https://manage.cloudworkspace.com Utilizzando l'account amministratore primario VDS creato durante il provisioning. Se non ricordi le informazioni del tuo account, contatta NetApp VDS per assistenza nel recupero
2. Fare clic sulla voce di menu Workspace, quindi sul nome dell'area di lavoro creata automaticamente durante il provisioning
3. Fare clic sulla scheda Users and Groups (utenti e gruppi)[]
4. Per ogni utente che si desidera abilitare, scorrere il nome utente e fare clic sull'icona Gear
5. Scegliere l'opzione "Enable Cloud Workspace" (attiva area di lavoro cloud)[]
6. Il completamento del processo di abilitazione richiede circa 30-90 secondi. Si noti che lo stato dell'utente cambia da Pending (in sospeso) a Available (disponibile)

L’attivazione di Azure ad Domain Services crea un dominio gestito in Azure e ogni macchina virtuale AVD creata verrà unita a tale dominio. Affinché l’accesso tradizionale alle macchine virtuali funzioni, 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.

Abilitare le sessioni utente

Per impostazione predefinita, gli host di sessione non sono in grado di accettare le connessioni utente. Questa impostazione è comunemente chiamata "modalità drain", in quanto può essere utilizzata in produzione per impedire nuove sessioni utente, consentendo all’host di rimuovere tutte le sessioni utente. Quando sono consentite nuove sessioni utente su un host, questa azione viene comunemente definita come inserimento dell’host di sessione in rotazione.

In produzione è opportuno avviare nuovi host in modalità drain, poiché in genere è necessario completare i task di configurazione prima che l’host sia pronto per i carichi di lavoro di produzione.

Durante il test e la valutazione è possibile interrompere immediatamente la modalità drain degli host per consentire agli utenti di connettersi e confermare la funzionalità. .Per abilitare le sessioni utente sugli host di sessione, attenersi alla seguente procedura:

1. Accedere alla sezione AVD della pagina Workspace.
2. Fare clic sul nome del pool di host in "AVD host Pools" (pool di host AVD).[]
3. Fare clic sul nome degli host di sessione e selezionare la casella "Allow New Sessions" (Consenti nuove sessioni), quindi fare clic su "Update Session host" (Aggiorna host di sessione). Ripetere la procedura per tutti gli host che devono essere posizionati in rotazione.[]
4. Le statistiche correnti di "Allow New Session" (Consenti nuova sessione) vengono visualizzate anche nella pagina AVD principale per ogni voce della linea host.

Gruppo di applicazioni predefinito

Si noti che il Desktop Application Group viene creato per impostazione predefinita come parte del processo di creazione del pool di host. Questo gruppo fornisce l’accesso interattivo al desktop a tutti i membri del gruppo. .Per aggiungere membri al gruppo:

1. Fare clic sul nome dell’App Group[]
2. Fare clic sul collegamento che mostra il numero di utenti aggiunti[]
3. Selezionare gli utenti che si desidera aggiungere al gruppo di applicazioni selezionando la casella accanto al nome
4. Fare clic sul pulsante Select Users (Seleziona utenti)
5. Fare clic sul pulsante Update app group (Aggiorna gruppo di applicazioni)

Creazione di gruppi di applicazioni AVD aggiuntivi

È possibile aggiungere ulteriori gruppi di applicazioni al pool di host. Questi gruppi di applicazioni pubblicheranno applicazioni specifiche dalle macchine virtuali del pool di host agli utenti dell’App Group utilizzando RemoteApp.

AVD consente solo agli utenti finali di essere assegnati al tipo di Desktop App Group o al tipo di RemoteApp App Group, ma non a entrambi nello stesso pool di host, quindi assicurarsi di separare gli utenti di conseguenza. Se gli utenti hanno bisogno di accedere a un desktop e ad applicazioni in streaming, è necessario un secondo pool di host per ospitare le applicazioni.

Per creare un nuovo gruppo di applicazioni:

1. Fare clic sul pulsante Add (Aggiungi) nell'intestazione della sezione app groups (gruppi di applicazioni)[]
2. Immettere un nome e una descrizione per l'App Group
3. Selezionare gli utenti da aggiungere al gruppo facendo clic sul collegamento Add Users (Aggiungi utenti). Selezionare ciascun utente facendo clic sulla casella di controllo accanto al nome, quindi fare clic sul pulsante Select Users (Seleziona utenti)[]
4. Fare clic sul collegamento Add RemoteApps (Aggiungi applicazioni RemoteApps) per aggiungere applicazioni a questo gruppo di applicazioni. AVD genera automaticamente l'elenco delle applicazioni possibili eseguendo la scansione dell'elenco delle applicazioni installate sulla macchina virtuale . Selezionare l'applicazione facendo clic sulla casella di controllo accanto al nome dell'applicazione, quindi fare clic sul pulsante Select RemoteApps (Seleziona applicazioni RemoteApps).[]
5. Fare clic sul pulsante Add App Group (Aggiungi gruppo di applicazioni) per creare l'App Group

Accesso AVD dell'utente finale

Gli utenti finali possono accedere agli ambienti AVD utilizzando il client Web o un client installato su una vasta gamma di piattaforme

- Client Web: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web
- URL di accesso al client Web: http://aka.ms/AVDweb
- Client Windows: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10
- Client Android: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android
- Client MacOS: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos
- Client iOS: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios
- Thin client IGEL: https://www.igel.com/igel-solution-family/windows-virtual-desktop/

Accedere utilizzando il nome utente e la password dell'utente finale. Tenere presente che le connessioni RADC (Remote App and Desktop Connections), mstsc (Remote Desktop Connection) e CloudWorksapce Client per Windows non supportano attualmente la possibilità di accedere alle istanze di AVD.

Monitorare gli accessi degli utenti

La pagina dei dettagli del pool di host visualizza anche un elenco di utenti attivi quando accedono a una sessione AVD.

Opzioni di connessione Admin

Gli amministratori VDS sono in grado di connettersi alle macchine virtuali dell'ambiente in diversi modi.

Connettersi al server

Nel portale, gli amministratori VDS troveranno l'opzione "Connect to Server" (Connetti al server). Per impostazione predefinita, questa funzione connette l'amministratore alla macchina virtuale generando dinamicamente le credenziali di amministratore locale e inserendole in una connessione client Web. Per

connettersi, l'amministratore non deve conoscere (e non viene mai fornito) le credenziali.

Questo comportamento predefinito può essere disattivato in base all'amministratore, come descritto nella sezione successiva.

Account admin .TECH/livello 3

Nel processo di installazione di CWA è stato creato un account amministratore di livello III. Il nome utente è formattato come username.tech@domain.xyz

Questi account, comunemente denominati account ".tech", sono denominati account amministratore a livello di dominio. Gli amministratori VDS possono utilizzare il proprio account .TECH per la connessione a un server CWMGR1 (piattaforma) e, facoltativamente, per la connessione a tutte le altre macchine virtuali dell'ambiente.

Per disattivare la funzione di accesso amministratore locale automatico e forzare l'utilizzo dell'account di livello III, modificare questa impostazione. Accedere a VDS > Admins > Admin Name > Check "Tech account Enabled" (VDS > amministratori > Nome amministratore > selezionare "Tech account Enabled". Se questa casella è selezionata, l'amministratore di VDS non verrà automaticamente connesso alle macchine virtuali come amministratore locale e verrà richiesto di inserire le proprie credenziali .TECH.

Queste credenziali e altre credenziali rilevanti vengono memorizzate automaticamente nel *Azure Key Vault* ed è possibile accedervi dal portale di gestione Azure all'indirizzo https://portal.azure.com/.

Azioni post-implementazione opzionali

Autenticazione a più fattori (MFA)

NetApp VDS include SMS/Email MFA gratuitamente. Questa funzione può essere utilizzata per proteggere gli account VDS Admin e/o gli account dell'utente finale."Articolo MFA"

Workflow dei diritti dell'applicazione

VDS fornisce un meccanismo per assegnare agli utenti finali l'accesso alle applicazioni da un elenco predefinito di applicazioni chiamato catalogo applicazioni. Il catalogo di applicazioni copre tutte le implementazioni gestite.

> Il server TSD1 implementato automaticamente deve rimanere così com'è per supportare i diritti dell'applicazione. In particolare, non eseguire la funzione "Converti in dati" su questa macchina virtuale.

La gestione delle applicazioni è descritta in dettaglio nel presente articolo: ""

Gruppi di sicurezza Azure ad

VDS include funzionalità per creare, popolare ed eliminare gruppi di utenti supportati da Azure ad Security Groups. Questi gruppi possono essere utilizzati al di fuori di VDS come qualsiasi altro gruppo di sicurezza. In VDS questi gruppi possono essere utilizzati per assegnare permessi di cartella e diritti di applicazione.

Creare gruppi di utenti

La creazione di gruppi di utenti viene eseguita nella scheda Users & Groups (utenti e gruppi) all'interno di un'area di lavoro.

Assegnare permessi di cartella per gruppo

Le autorizzazioni per visualizzare e modificare le cartelle nella condivisione aziendale possono essere assegnate a utenti o gruppi.

""

Assegnare le applicazioni per gruppo

Oltre ad assegnare applicazioni agli utenti singolarmente, è possibile eseguire il provisioning delle applicazioni ai gruppi.

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.[]

Configurare le opzioni di ottimizzazione dei costi

La gestione dello spazio di lavoro si estende anche alla gestione delle risorse Azure che supportano l'implementazione di AVD. VDS consente di configurare le pianificazioni dei workload e la scalabilità in tempo reale per attivare e disattivare le macchine virtuali Azure in base alle attività dell'utente finale. Queste funzionalità consentono di abbinare l'utilizzo e la spesa delle risorse di Azure al modello di utilizzo effettivo degli utenti finali. Inoltre, se è stata configurata un'implementazione AVD Proof of Concept, è possibile trasformare l'intera implementazione dall'interfaccia VDS.

Pianificazione del carico di lavoro

Workload Scheduling è una funzionalità che consente all'amministratore di creare una pianificazione impostata per le macchine virtuali Workspace da attivare per supportare le sessioni dell'utente finale. Quando viene raggiunta la fine del periodo di tempo pianificato per un giorno specifico della settimana, VDS arresta/disalloca le macchine virtuali in Azure in modo che le spese orarie si interrompano.

Per attivare la pianificazione del carico di lavoro:

1. Accedere a VDS all'indirizzo https://manage.cloudworkspace.com Utilizzando le credenziali VDS.
2. Fare clic sulla voce di menu Workspace (Area di lavoro), quindi sul nome dell'area di lavoro nell'elenco. []
3. Fare clic sulla scheda Workload Schedule (Pianificazione del carico di lavoro). []
4. Fare clic sul collegamento Manage (Gestisci) nell'intestazione Workload Schedule (Pianificazione workload). []
5. Scegliere uno stato predefinito dall'elenco a discesa Stato: Sempre attivo (impostazione predefinita), sempre disattivato o pianificato.
6. Se si sceglie pianificato, le opzioni di pianificazione includono:
    a. Esegui ogni giorno all'intervallo assegnato. Questa opzione consente di impostare la pianificazione in modo che sia la stessa ora di inizio e di fine per tutti e sette i giorni della settimana. []
    b. Eseguito all'intervallo assegnato per giorni specificati. Questa opzione consente di impostare la pianificazione sullo stesso orario di inizio e fine solo per i giorni selezionati della settimana. I giorni non selezionati della settimana indicheranno a VDS di non attivare le macchine virtuali per quei giorni. []
    c. Eseguire a intervalli di tempo e giorni variabili. Questa opzione consente di impostare la pianificazione su orari di inizio e fine diversi per ciascun giorno selezionato. []
    d. Al termine dell'impostazione della pianificazione, fare clic sul pulsante Update schedule (Aggiorna

pianificazione). []

Scalabilità in tempo reale

Live Scaling attiva e disattiva automaticamente le macchine virtuali in un pool di host condiviso in base al carico dell'utente simultaneo. Quando ciascun server si riempie, viene attivato un server aggiuntivo in modo che sia pronto quando il bilanciamento del carico del pool di host invia le richieste di sessione dell'utente. Per un utilizzo efficace di Live Scaling, scegliere "Depth First" come tipo di bilanciamento del carico.

Per attivare Live Scaling:

1. Accedere a VDS all'indirizzo https://manage.cloudworkspace.com Utilizzando le credenziali VDS.
2. Fare clic sulla voce di menu Workspace (Area di lavoro), quindi sul nome dell'area di lavoro nell'elenco. []
3. Fare clic sulla scheda Workload Schedule (Pianificazione del carico di lavoro). []
4. Fare clic sul pulsante di opzione Enabled (attivato) nella sezione Live Scaling (scalabilità in tempo reale). []
5. Fare clic sul numero massimo di utenti per server e immettere il numero massimo. A seconda delle dimensioni della macchina virtuale, questo numero è generalmente compreso tra 4 e 20. []
6. FACOLTATIVO – fare clic su Extra Powered on Servers Enabled (Server aggiuntivi attivati) e immettere un numero di server aggiuntivi che si desidera attivare per il pool di host. Questa impostazione attiva il numero specificato di server oltre al server che esegue il riempimento attivo, in modo da fungere da buffer per grandi gruppi di utenti che accedono alla stessa finestra temporale. []

Live Scaling si applica attualmente a tutti i pool di risorse condivisi. Nel prossimo futuro, ciascun pool disporrà di opzioni indipendenti di Live Scaling.

Spegnere l'intera implementazione

Se si prevede di utilizzare la distribuzione di valutazione solo su base sporadica e non in produzione, è possibile disattivare tutte le macchine virtuali nella distribuzione quando non vengono utilizzate.

Per attivare o disattivare la distribuzione (ad esempio, spegnere le macchine virtuali durante l'implementazione), attenersi alla seguente procedura:

1. Accedere a VDS all'indirizzo https://manage.cloudworkspace.com Utilizzando le credenziali VDS.
2. Fare clic sulla voce di menu Deployments (implementazioni). []Scorrere il cursore sulla riga corrispondente all'implementazione di destinazione per visualizzare l'icona ingranaggio di configurazione. []
3. Fare clic sull'ingranaggio, quindi scegliere Stop. []
4. Per riavviare o avviare, seguire i passaggi 1-3 e scegliere Start. []

L'interruzione o l'avvio di tutte le macchine virtuali durante l'implementazione potrebbe richiedere alcuni minuti.

Creare e gestire immagini VM

VDS contiene funzionalità per la creazione e la gestione di immagini di macchine virtuali per implementazioni future. Per accedere a questa funzionalità, accedere a: VDS > Deployments > Deployment Name > Provisioning Collections. Le funzionalità di raccolta immagini VDI sono documentate qui: ""

Configurare Azure Cloud Backup Service

VDS può configurare e gestire in modo nativo Azure Cloud Backup, un servizio Azure PaaS per il backup delle

macchine virtuali. I criteri di backup possono essere assegnati a singoli computer o gruppi di computer in base al tipo o al pool di host. I dettagli sono disponibili qui: ""

Selezionare la modalità di gestione/policy dell'applicazione

Per impostazione predefinita, VDS implementa una serie di oggetti Criteri di gruppo (GPO) che bloccano lo spazio di lavoro dell'utente finale. Questi criteri impediscono l'accesso a entrambe le posizioni principali dei livelli di dati (ad esempio, c:) e la possibilità di eseguire le installazioni delle applicazioni come utente finale.

Questa valutazione ha lo scopo di dimostrare le funzionalità di Windows Virtual Desktop, in modo da poter rimuovere gli oggetti Criteri di gruppo in modo da poter implementare un "spazio di lavoro di base" che offra le stesse funzionalità e gli stessi accessi di un'area di lavoro fisica. A tale scopo, seguire la procedura descritta nell'opzione "Basic Workspace" (Area di lavoro di base).

È inoltre possibile scegliere di utilizzare il set completo di funzionalità di gestione di Virtual Desktop per implementare un'area di lavoro controllata. Questi passaggi includono la creazione e la gestione di un catalogo di applicazioni per i diritti dell'utente finale e l'utilizzo delle autorizzazioni a livello di amministratore per gestire l'accesso alle applicazioni e alle cartelle di dati. Seguire i passaggi della sezione "Area di lavoro controllata" per implementare questo tipo di area di lavoro nei pool di host AVD.

Area di lavoro AVD controllata (policy predefinite)

L'utilizzo di uno spazio di lavoro controllato è la modalità predefinita per le implementazioni VDS. I criteri vengono applicati automaticamente. Questa modalità richiede agli amministratori VDS di installare le applicazioni e agli utenti finali viene concesso l'accesso all'applicazione tramite un collegamento sul desktop della sessione. In modo simile, l'accesso alle cartelle di dati viene assegnato agli utenti finali creando cartelle condivise mappate e impostando le autorizzazioni per visualizzare solo le lettere di unità mappate anziché le unità di avvio e/o dati standard. Per gestire questo ambiente, seguire la procedura riportata di seguito per installare le applicazioni e fornire l'accesso dell'utente finale.

Ripristino dello spazio di lavoro AVD di base

La creazione di un'area di lavoro di base richiede la disattivazione dei criteri GPO predefiniti creati per impostazione predefinita.

A tale scopo, seguire questa procedura unica:

1. Accedere a VDS all'indirizzo https://manage.cloudworkspace.com utilizzando le credenziali di amministratore principali.
2. Fare clic sulla voce di menu Deployments (implementazioni) a sinistra. []
3. Fare clic sul nome dell'implementazione. []
4. Nella sezione Platform Servers (Server piattaforma) (pagina centrale a destra), scorrere a destra della riga per CWMGR1 fino a visualizzare l'ingranaggio. []
5. Fare clic sull'ingranaggio e scegliere Connetti. []
6. Immettere le credenziali "Tech" create durante il provisioning per accedere al server CWMGR1 utilizzando l'accesso HTML5. []
7. Fare clic sul menu Start (Windows) e scegliere Strumenti di amministrazione di Windows. []
8. Fare clic sull'icona Gestione criteri di gruppo. []
9. Fare clic sulla voce AADDC Users (utenti AADDC) nell'elenco nel riquadro di sinistra. []
10. Fare clic con il pulsante destro del mouse sul criterio "Cloud Workspace Users" (utenti Cloud Workspace) nell'elenco nel riquadro a destra, quindi deselezionare l'opzione "link Enabled" (collegamento abilitato).

Fare clic su OK per confermare questa azione. [] []

11. Selezionare azione, aggiornamento criteri di gruppo dal menu, quindi confermare che si desidera forzare l'aggiornamento dei criteri su tali computer. []
12. Ripetere i passaggi 9 e 10 ma selezionare "utenti AADDC" e "Società Cloud Workspace" come criterio per disattivare il collegamento. Non è necessario forzare un aggiornamento dei criteri di gruppo dopo questo passaggio. [] []
13. Chiudere l'editor di gestione dei criteri di gruppo e le finestre Strumenti di amministrazione, quindi disconnettersi. []Questi passaggi forniranno un ambiente di lavoro di base per gli utenti finali. Per confermare, effettuare l'accesso come account utente finale: L'ambiente di sessione non deve avere alcuna restrizione dell'area di lavoro controllata, ad esempio il menu Start nascosto, l'accesso bloccato all'unità C: E il pannello di controllo nascosto.

> L'account .TECH creato durante l'implementazione dispone dell'accesso completo per installare le applicazioni e modificare la sicurezza delle cartelle indipendentemente da VDS. Tuttavia, se si desidera che gli utenti finali del dominio Azure ad abbiano un accesso completo simile, è necessario aggiungerli al gruppo Local Administrators di ciascuna macchina virtuale.

Guida all'implementazione di AVD - supplemento ad esistente

Panoramica

VDS Setup consente di connettere una nuova implementazione a una struttura ad esistente. Queste istruzioni illustrano in dettaglio questa opzione. Questo articolo non è autonomo, ma è una spiegazione dettagliata di un'alternativa all'opzione New ad descritta in "Guida all'implementazione di AVD"

Tipo di Active Directory

La sezione successiva definisce il tipo di implementazione di Active Directory per l'implementazione di VDS. In questa guida verrà selezionata la Active Directory di Windows Server esistente, che utilizzerà una struttura ad già esistente.

Rete ad esistente

VDS Setup visualizza un elenco di vNets che potrebbero rappresentare la connessione tra la struttura ad esistente e Azure ad. Il VNET selezionato deve disporre di un controller di dominio con hosting Azure configurato in Azure. Inoltre, VNET disporrà di impostazioni DNS personalizzate che puntano al controller di dominio ospitato da Azure.

[]

Nome di dominio Active Directory esistente

Inserire il nome di dominio esistente che verrà utilizzato. Nota: Non si desidera utilizzare il dominio che si trova in Azure Portal nel modulo Active Directory, in quanto può causare problemi DNS. L'esempio principale è che gli utenti non potranno accedere al sito Web (ad esempio, <yourdomain>.com) dall'interno del desktop.

Nome utente e password ad esistenti

Esistono tre modi per fornire le credenziali necessarie per facilitare un'implementazione utilizzando una struttura ad esistente.

1. Specificare il nome utente e la password dell'amministratore di dominio Active Directory

Questo è il metodo più semplice: Fornire credenziali di amministratore di dominio utilizzate per facilitare l'implementazione.

> Questo account può essere creato una sola volta e cancellato una volta completato il processo di implementazione.

2. Crea account corrispondente alle autorizzazioni richieste

   Questo metodo richiede agli amministratori dei clienti di creare manualmente la struttura delle autorizzazioni, quindi inserire qui le credenziali per l'account CloudWorkspaceSVC e continuare.

3. Processo di implementazione manuale

   Contattare il supporto NetApp VDS per assistenza nella configurazione dell'accesso ad con account principal con privilegi minimi.

Passi successivi

In questo articolo vengono descritte le procedure specifiche per la distribuzione in un ambiente ad esistente. Una volta completata questa procedura, è possibile tornare alla guida di implementazione standard "qui".

Componenti e autorizzazioni VDS

Entità e servizi di sicurezza AVD e VDS

Azure Virtual Desktop (AVD) richiede account e componenti di sicurezza in Azure ad e Active Directory locale per eseguire azioni automatizzate. Virtual Desktop Service (VDS) di NetApp crea componenti e impostazioni di sicurezza durante il processo di implementazione che consentono agli amministratori di controllare l'ambiente AVD. Questo documento descrive gli account, i componenti e le impostazioni di sicurezza VDS rilevanti in entrambi gli ambienti.

I componenti e le autorizzazioni del processo di automazione dell'implementazione sono principalmente distinti dai componenti dell'ambiente finale implementato. Pertanto, questo articolo è costituito da due sezioni principali, la sezione relativa all'automazione della distribuzione e la sezione relativa all'ambiente distribuito.

[larghezza=75%]

Componenti e autorizzazioni per l'automazione dell'implementazione AVD

L'implementazione di VDS sfrutta più componenti Azure e NetApp e le autorizzazioni di sicurezza per implementare implementazioni e spazi di lavoro.

Servizi di implementazione VDS

Applicazioni aziendali

VDS sfrutta le applicazioni aziendali e le registrazioni delle applicazioni nel dominio Azure ad di un tenant. Le applicazioni Enterprise sono il conduttore per le chiamate verso gli endpoint Azure Resource Manager, Azure Graph e (se si utilizza AVD Fall Release) API AVD dal contesto di sicurezza dell'istanza di Azure ad utilizzando i ruoli delegati e le autorizzazioni concesse al Service Principal associato. Le registrazioni delle applicazioni possono essere create in base allo stato di inizializzazione dei servizi AVD per il tenant tramite VDS.

Per consentire la creazione e la gestione di queste macchine virtuali, VDS crea diversi componenti di supporto nell'abbonamento Azure:

Cloud Workspace

Questo è il consenso iniziale degli amministratori delle applicazioni aziendali e viene utilizzato durante il processo di installazione guidata VDS.

L'applicazione Cloud Workspace Enterprise richiede un set specifico di autorizzazioni durante il processo di installazione di VDS. Queste autorizzazioni sono:

- Access Directory as the signed in User (delegata) (accesso alla directory come utente registrato)
- Lettura e scrittura dei dati della directory (delegata)
- Profilo utente di accesso e lettura (delegato)
- Accesso utenti (delegato)
- Visualizza profilo di base degli utenti (delegato)
- Accesso a Azure Service Management come utenti dell'organizzazione (delegati)

API Cloud Workspace

Gestisce le chiamate di gestione generali per le funzioni PaaS di Azure. Esempi di funzioni PaaS di Azure sono Azure Compute, Azure Backup, Azure Files e così via Il presente Service Principal richiede i diritti del proprietario per l'abbonamento Azure di destinazione durante l'implementazione iniziale e i diritti del collaboratore per la gestione continua (nota: L'utilizzo dei file Azure richiede i diritti del proprietario dell'abbonamento per impostare le autorizzazioni per utente su Azure file Objects).

L'applicazione Enterprise API Cloud Workspace richiede un set specifico di autorizzazioni durante il processo di installazione VDS. Queste autorizzazioni sono:

- Subscription Contributor (o Subscription Owner se vengono utilizzati i file Azure)
- Grafico ad Azure
  - Lettura e scrittura di tutte le applicazioni (applicazione)
  - Gestire le applicazioni create o possedete da questa applicazione (applicazione)
  - Dispositivi di lettura e scrittura (applicazione)
  - Accesso alla directory come utente registrato (delegato)
  - Lettura dei dati della directory (applicazione)
  - Read Directory Data (delegata)
  - Lettura e scrittura dei dati della directory (applicazione)
  - Lettura e scrittura dei dati della directory (delegata)
  - Domini di lettura e scrittura (applicazione)
  - Lettura di tutti i gruppi (delegati)
  - Lettura e scrittura di tutti i gruppi (delegati)
  - Read All Hidden Memberships (applicazioni) (Leggi tutte le appartenenze nascoste
  - Lettura delle appartenenze nascoste (delegate)
  - Profilo utente di accesso e lettura (delegato)
  - Leggi profili completi di tutti gli utenti (delegati)
  - Leggi i profili di base di tutti gli utenti (delegati)

- Gestione dei servizi Azure
    - Accesso a Azure Service Management come utenti dell'organizzazione (delegati)

NetApp VDS

I componenti NetApp VDS vengono utilizzati tramite il piano di controllo VDS per automatizzare l'implementazione e la configurazione di ruoli, servizi e risorse AVD.

Ruolo personalizzato

Il ruolo di Automation Contributor è stato creato per facilitare le implementazioni attraverso metodologie meno privilegiate. Questo ruolo consente alla macchina virtuale CWMGR1 di accedere all'account di automazione Azure.

Account di automazione

Durante l'implementazione viene creato un account di automazione che è un componente necessario durante il processo di provisioning. L'account Automation contiene variabili, credenziali, moduli e configurazioni di stato desiderate e fa riferimento al vault delle chiavi.

Configurazione dello stato desiderata

Questo è il metodo utilizzato per creare la configurazione di CWMGR1. Il file di configurazione viene scaricato sulla macchina virtuale e applicato tramite Local Configuration Manager sulla macchina virtuale. Esempi di elementi di configurazione includono:

- Installazione delle funzionalità di Windows
- Installazione del software
- Applicazione delle configurazioni software
- Garantire l'applicazione dei set di autorizzazioni appropriati
- Applicazione del certificato Let's Encrypt
- Garantire che i record DNS siano corretti
- Assicurarsi che CWMGR1 sia Unito al dominio

Moduli:

- ActiveDirectoryDsc: Risorsa di configurazione dello stato desiderata per l'implementazione e la configurazione di Active Directory. Queste risorse consentono di configurare nuovi domini, domini figlio e controller di dominio ad alta disponibilità, stabilire trust tra domini e gestire utenti, gruppi e unità organizzative.
- AZ.Accounts: Modulo fornito da Microsoft utilizzato per la gestione delle credenziali e degli elementi di configurazione comuni per i moduli Azure
- AZ.Automation: Un modulo fornito da Microsoft per i commandlet di Azure Automation
- Az.Compute:A Microsoft ha fornito il modulo per i commandlet di calcolo Azure
- AZ.KeyVault: Un modulo fornito da Microsoft per i comandi di Azure Key Vault
- AZ.Resources: Un modulo fornito da Microsoft per i comandi di Azure Resource Manager
- CChoco: Risorsa di configurazione dello stato desiderata per il download e l'installazione di pacchetti utilizzando chocolatey

- CjAz: Questo modulo creato da NetApp fornisce strumenti di automazione al modulo di automazione Azure
- CjAzACS: Questo modulo creato da NetApp contiene funzioni di automazione dell'ambiente e processi PowerShell eseguiti dall'interno del contesto utente.
- CjAzBuild: Questo modulo creato da NetApp contiene l'automazione della build e della manutenzione e i processi PowerShell eseguiti dal contesto del sistema.
- CNtfsAccessControl: Risorsa di configurazione dello stato desiderata per la gestione del controllo di accesso NTFS
- ComputerManagementDsc: Risorsa di configurazione dello stato desiderata che consente attività di gestione del computer come l'Unione di un dominio e la pianificazione di attività, nonché la configurazione di elementi come memoria virtuale, registri eventi, fusi orari e impostazioni di alimentazione.
- CUserRightsAssignment: Risorsa di configurazione dello stato desiderata che consente la gestione dei diritti utente, ad esempio diritti e privilegi di accesso
- NetworkingDsc: t risorsa di configurazione dello stato desiderato per il networking
- XCertificate: Risorsa di configurazione dello stato desiderata per semplificare la gestione dei certificati su Windows Server.
- XDnsServer: Risorsa di configurazione dello stato desiderata per la configurazione e la gestione del server DNS di Windows Server
- XNetworking: Risorsa di configurazione dello stato desiderata relativa alla rete.
- "XRemoteDesktopAdmin": Questo modulo utilizza un repository che contiene le risorse di configurazione dello stato desiderate per configurare le impostazioni del desktop remoto e il firewall di Windows su un computer locale o remoto.
- XRemoteDesktopSessionHost: Risorsa di configurazione dello stato desiderata (xRDSessionDeployment, xRDSessionCollection, xRDSessionCollectionConfiguration e xRDRemoteApp) che consente la creazione e la configurazione di un'istanza di Remote Desktop Session host (RDSH)
- XSmbShare: Risorsa di configurazione dello stato desiderata per la configurazione e la gestione di una condivisione SMB
- XSystemSecurity: Risorsa di configurazione dello stato desiderata per la gestione di UAC e IE Esc

> Azure Virtual Desktop installa anche i componenti di Azure, incluse le applicazioni Enterprise e le registrazioni delle applicazioni per Azure Virtual Desktop e Azure Virtual Desktop Client, AVD Tenant, AVD host Pools, AVD App Groups e AVD Registered Virtual Machine. Mentre i componenti di automazione VDS gestiscono questi componenti, AVD controlla la configurazione predefinita e il set di attributi, quindi fare riferimento alla documentazione di AVD per ulteriori dettagli.

Componenti ad ibridi

Per facilitare l'integrazione con ad esistente on-remises o in esecuzione nel cloud pubblico, sono necessari ulteriori componenti e autorizzazioni nell'ambiente ad esistente.

Controller di dominio

Il controller di dominio esistente può essere integrato in un'implementazione AVD tramite ad Connect e/o una VPN sito-sito (o Azure ExpressRoute).

AD Connect

Per facilitare l'autenticazione dell'utente tramite i servizi AVD PaaS, è possibile utilizzare ad Connect per sincronizzare il controller di dominio con Azure ad.

Gruppo di sicurezza

VDS utilizza un gruppo di sicurezza di Active Directory chiamato CW-Infrastructure per contenere le autorizzazioni necessarie per automatizzare le attività dipendenti da Active Directory, come l'Unione del dominio e l'allegato dei criteri GPO.

Account di servizio

VDS utilizza un account di servizio Active Directory chiamato CloudworkspaceSVC che viene utilizzato come identità per i servizi VDS Windows e il servizio dell'applicazione IIS. Questo account non è interattivo (non consente l'accesso RDP) ed è il membro principale dell'account CW-Infrastructure

VPN o ExpressRoute

È possibile utilizzare una VPN site-to-site o Azure ExpressRoute per collegare direttamente le macchine virtuali Azure al dominio esistente. Si tratta di una configurazione opzionale disponibile quando i requisiti di progetto lo impongono.

Delega di autorizzazioni ad locali

NetApp offre uno strumento opzionale in grado di ottimizzare il processo ad ibrido. Se si utilizza lo strumento opzionale di NetApp, deve:

- Eseguito su un sistema operativo server anziché su un sistema operativo per workstation
- Eseguire su un server che è collegato al dominio o che è un controller di dominio
- Disporre di PowerShell 5.0 o superiore sia sul server che esegue lo strumento (se non viene eseguito sul controller di dominio) che sul controller di dominio
- Essere eseguito da un utente con privilegi di amministratore di dominio O essere eseguito da un utente con autorizzazioni di amministratore locale e con la possibilità di fornire una credenziale di amministratore di dominio (per l'utilizzo con RunAs)

Sia che vengano create manualmente o applicate dallo strumento NetApp, le autorizzazioni richieste sono:

- Gruppo infrastruttura CW
  - Il gruppo di sicurezza Cloud Workspace Infrastructure (**CW-Infrastructure**) ha il pieno controllo del livello di unità organizzativa Cloud Workspace e di tutti gli oggetti discendenti
  - <deployment code>.cloudworkspace.app zona DNS: Gruppo di infrastrutture CW assegnato a CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedRight, Delete, GenericWrite
  - Server DNS: Il gruppo di infrastrutture CW ha concesso ReadProperty, GenericExecute
  - Accesso dell'amministratore locale per le VM create (CWMGR1, VM di sessione AVD) (eseguito in base ai criteri di gruppo sui sistemi AVD gestiti)
- CW-CWMGRAccess group questo gruppo fornisce diritti amministrativi locali per CWMGR1 su tutti i modelli, il singolo server, il nuovo modello nativo di Active Directory utilizza i gruppi integrati Server Operators Remote Desktop Users e Network Configuration Operators.

Componenti e permessi ambientali AVD

Una volta completato il processo di automazione dell'implementazione, l'utilizzo e l'amministrazione di implementazioni e aree di lavoro richiedono un set distinto di componenti e autorizzazioni, come definito di seguito. Molti dei componenti e delle autorizzazioni di cui sopra rimangono rilevanti, ma questa sezione si concentra sulla definizione della struttura di un distribuito.

I componenti delle implementazioni VDS e delle aree di lavoro possono essere organizzati in diverse categorie logiche:

- Client degli utenti finali
- Componenti del piano di controllo VDS
- Componenti di Microsoft Azure AVD-PaaS
- Componenti della piattaforma VDS
- Componenti dello spazio di lavoro VDS in Azure tenant
- Componenti ad ibridi

Client degli utenti finali

Gli utenti possono connettersi al desktop AVD e/o da diversi tipi di endpoint. Microsoft ha pubblicato applicazioni client per Windows, macOS, Android e iOS. Inoltre, è disponibile un client Web per l'accesso senza client.

Alcuni fornitori di thin client Linux hanno pubblicato un client endpoint per AVD. Questi sono elencati all'indirizzo https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

Componenti del piano di controllo VDS

API REST VDS

VDS si basa su API REST completamente documentate, in modo che tutte le azioni disponibili nell'applicazione Web siano disponibili anche tramite l'API. La documentazione per l'API è qui: https://api.cloudworkspace.com/5.4/swagger/ui/index#

Applicazione web VDS

Gli amministratori VDS possono interagire con l'applicazione ADS tramite l'applicazione web VDS. Questo portale web si trova all'indirizzo: https://manage.cloudworkspace.com

Database del piano di controllo

I dati e le impostazioni VDS sono memorizzati nel database SQL del piano di controllo, ospitato e gestito da NetApp.

Comunicazioni VDS

Componenti del tenant Azure

L'automazione dell'implementazione di VDS crea un singolo gruppo di risorse Azure per contenere gli altri componenti AVD, tra cui macchine virtuali, subnet di rete, gruppi di sicurezza di rete e container di file Azure o pool di capacità Azure NetApp Files. Nota: Il valore predefinito è un singolo gruppo di risorse, ma VDS dispone di strumenti per creare risorse in gruppi di risorse aggiuntivi, se lo si desidera.

Componenti di Microsoft Azure AVD-PaaS

API REST AVD

Microsoft AVD può essere gestito tramite API. VDS ha sfruttato ampiamente queste API per automatizzare e gestire gli ambienti AVD. La documentazione è disponibile all'indirizzo: https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/

Broker di sessione

Il broker determina le risorse autorizzate per l'utente e orchestrerà la connessione dell'utente al gateway.

Diagnostica Azure

Azure Diagnostics è stato creato appositamente per supportare le implementazioni AVD.

Client web AVD

Microsoft ha fornito un client Web per consentire agli utenti di connettersi alle proprie risorse AVD senza un client installato localmente.

Gateway di sessione

Il client RD installato localmente si connette al gateway per comunicare in modo sicuro nell'ambiente AVD.

Componenti della piattaforma VDS

CWMGR1

CMWGR1 è la VM di controllo VDS per ogni implementazione. Per impostazione predefinita, viene creato come macchina virtuale Windows 2019 Server nell'abbonamento Azure di destinazione. Consultare la sezione distribuzione locale per l'elenco dei componenti VDS e di terze parti installati su CWMGR1.

AVD richiede che le VM AVD siano unite a un dominio Active Directory. Per facilitare questo processo e fornire gli strumenti di automazione per la gestione dell'ambiente VDS, sulla macchina virtuale CWMGR1 vengono installati diversi componenti e all'istanza di ad vengono aggiunti diversi componenti. I componenti includono:

- **Servizi Windows** - VDS utilizza i servizi Windows per eseguire azioni di automazione e gestione dall'interno di un'implementazione:
  - **CW Automation Service** è un servizio Windows implementato su CWMGR1 in ogni implementazione AVD che esegue molte delle attività di automazione rivolte all'utente nell'ambiente. Questo servizio viene eseguito sotto l'account ad **CloudWorkspaceSVC**.
  - **CW VM Automation Service** è un servizio Windows implementato su CWMGR1 in ogni implementazione AVD che esegue le funzioni di gestione delle macchine virtuali. Questo servizio viene eseguito sotto l'account ad **CloudWorkspaceSVC**.
  - **CW Agent Service** è un servizio Windows implementato su ciascuna macchina virtuale sotto la gestione di VDS, incluso CWMGR1. Questo servizio viene eseguito nel contesto **LocalSystem** sulla macchina virtuale.
  - **CWManagerX API** è un listener basato su pool di applicazioni IIS installato su CWMGR1 in ogni implementazione AVD. In questo modo vengono gestite le richieste in entrata provenienti dal piano di controllo globale e vengono eseguite con l'account **CloudWorkspaceSVC** ad.
- **SQL Server 2017 Express** – VDS crea un'istanza di SQL Server Express sulla macchina virtuale

CWMGR1 per gestire i metadati generati dai componenti di automazione.

- **Internet Information Services (IIS)** – IIS è abilitato su CWMGR1 per ospitare l'applicazione IIS CWManagerX e CWApps (solo se la funzionalità RDS RemoteApp è attivata). VDS richiede IIS versione 7.5 o successiva.
- **HTML5 Portal (opzionale)** – VDS installa il servizio Spark Gateway per fornire l'accesso HTML5 alle macchine virtuali nell'implementazione e dall'applicazione web VDS. Si tratta di un'applicazione basata su Java e può essere disattivata e rimossa se non si desidera utilizzare questo metodo di accesso.
- **RD Gateway (opzionale)** – VDS abilita il ruolo RD Gateway su CWMGR1 per fornire l'accesso RDP ai pool di risorse basati su RDS Collection. Questo ruolo può essere disattivato/disinstallato se si desidera solo l'accesso a AVD Reverse Connect.
- **RD Web (opzionale)** – VDS abilita il ruolo RD Web e crea l'applicazione Web CWApps IIS. Questo ruolo può essere disattivato se si desidera solo l'accesso AVD.
- **DC Config** – un'applicazione Windows utilizzata per eseguire attività di configurazione avanzata e configurazione specifica del sito VDS e di implementazione.
- **Test VDC Tools** – un'applicazione Windows che supporta l'esecuzione diretta delle attività per le modifiche di configurazione a livello di macchina virtuale e client, utilizzata nei rari casi in cui le attività API o dell'applicazione Web devono essere modificate per la risoluzione dei problemi.
- **Crittografiamo certificato jolly (opzionale)** – creato e gestito da VDS – tutte le macchine virtuali che richiedono traffico HTTPS su TLS vengono aggiornate con il certificato ogni notte. Il rinnovo è gestito anche da attività automatizzate (i certificati sono 90 giorni, quindi il rinnovo inizia poco prima). Se lo si desidera, il cliente può fornire il proprio certificato jolly. VDS richiede inoltre diversi componenti di Active Directory per supportare le attività di automazione. L'intento di progettazione è quello di utilizzare un numero minimo di aggiunte di autorizzazioni e componenti ad, pur continuando a supportare l'ambiente per la gestione automatica. Questi componenti includono:
- **Cloud Workspace Organizational Unit (OU)** – questa unità organizzativa fungerà da container ad primario per i componenti figlio richiesti. Le autorizzazioni per i gruppi CW-Infrastructure e Client DHP Access verranno impostate a questo livello e ai relativi componenti figlio. Vedere l'Appendice A per le sottounità organizzative create in questa unità organizzativa.
- **Cloud Workspace Infrastructure Group (CW-Infrastructure)** è un gruppo di sicurezza creato nell'ad locale per consentire l'assegnazione delle autorizzazioni delegate richieste all'account del servizio VDS (**CloudWorkspaceSVC**)
- **Client DHP Access Group (ClientDHPAccess)** è un gruppo di sicurezza creato nell'annuncio locale per consentire a VDS di gestire la posizione in cui risiedono i dati della società condivisa, della home page dell'utente e del profilo.
- Account del servizio **CloudWorkspaceSVC** (membro del Cloud Workspace Infrastructure Group)
- **Zona DNS per il dominio <deployment code>.cloudworkspace.app** (questo dominio gestisce i nomi DNS creati automaticamente per le macchine virtuali host di sessione), creata dalla configurazione di implementazione.
- **GPO specifici di NetApp** collegati a varie OU figlio dell'unità organizzativa Cloud Workspace. Questi GPO sono:
  - **GPO Cloud Workspace (collegato all'unità organizzativa Cloud Workspace)** – definisce i protocolli di accesso e i metodi per i membri del gruppo CW-Infrastructure. Aggiunge inoltre il gruppo al gruppo Administrators locale sugli host di sessione AVD.
  - **Cloud Workspace Firewall GPO** (collegato a server dei clienti dedicati, desktop remoto e OU di gestione temporanea) - Crea una policy che garantisce e isola le connessioni agli host delle sessioni dai server della piattaforma.
  - **Cloud Workspace RDS** (Dedicated Customers Servers, Remote Desktop e Staging OU) - limiti

impostati per la qualità della sessione, l'affidabilità e i limiti di timeout di disconnessione. Per le sessioni RDS viene definito il valore del server di licenza TS.

- **Cloud Workspace Companies** (NON COLLEGATO per impostazione predefinita) – GPO opzionale per "bloccare" una sessione utente/area di lavoro impedendo l'accesso a strumenti e aree di amministrazione. Può essere collegato/abilitato per fornire un'area di lavoro con attività limitate.

Le configurazioni predefinite delle impostazioni di Criteri di gruppo possono essere fornite su richiesta.

Componenti dello spazio di lavoro VDS

Livello di dati

Azure NetApp Files

Un pool di capacità Azure NetApp Files e i volumi associati verranno creati se si sceglie Azure NetApp Files come opzione di livello dati nella configurazione VDS. Il volume ospita lo storage archiviato condiviso per i profili utente (tramite container FSLogix), le cartelle personali dell'utente e la cartella di condivisione dei dati aziendali.

File Azure

Se si sceglie Azure Files come opzione Data Layer in CWS Setup, verrà creata una condivisione file Azure e il relativo account di storage Azure associato. Azure file Share ospita lo storage archiviato condiviso per i profili utente (tramite container FSLogix), le cartelle personali dell'utente e la cartella di condivisione dei dati aziendali.

File server con disco gestito

Una macchina virtuale Windows Server viene creata con un disco gestito se si sceglie file Server come opzione Data Layer in VDS Setup. Il file server ospita lo storage archiviato condiviso per i profili utente (tramite container FSLogix), le cartelle personali dell'utente e la cartella di condivisione dei dati aziendali.

Networking Azure

Rete virtuale Azure

VDS crea una rete virtuale Azure e supporta le subnet. VDS richiede una subnet separata per i controller di dominio CWMGR1, AVD e Azure e il peering tra le subnet. Tenere presente che la subnet del controller ad esiste già, pertanto le subnet VDS implementate dovranno essere peering con la subnet esistente.

Gruppi di sicurezza di rete

Viene creato un gruppo di sicurezza di rete per controllare l'accesso alla macchina virtuale CWMGR1.

- Tenant: Contiene gli indirizzi IP per l'utilizzo da parte dell'host di sessione e delle VM di dati
- Servizi: Contiene indirizzi IP per l'utilizzo da parte dei servizi PaaS (ad esempio, Azure NetApp Files)
- Piattaforma: Contiene indirizzi IP da utilizzare come macchine virtuali della piattaforma NetApp (CWMGR1 e qualsiasi server gateway)
- Directory: Contiene gli indirizzi IP da utilizzare come macchine virtuali Active Directory

Azure ad

L'automazione e l'orchestrazione di VDS implementa le macchine virtuali in un'istanza di Active Directory di destinazione e quindi unisce le macchine al pool di host designato. Le macchine virtuali AVD sono gestite a livello di computer sia dalla struttura ad (unità organizzative, policy di gruppo, permessi di amministratore del computer locale, ecc.) che dall'appartenenza alla struttura AVD (pool di host, appartenenza al gruppo di applicazioni dell'area di lavoro), che sono regolate dalle entità e dalle autorizzazioni di Azure ad. VDS gestisce questo ambiente di "doppio controllo" utilizzando l'applicazione VDS Enterprise/Azure Service Principal per le azioni AVD e l'account di servizio ad locale (CloudWorkspaceSVC) per le azioni ad locali e del computer locale.

I passaggi specifici per creare una macchina virtuale AVD e aggiungerla al pool di host AVD includono:

- Creazione di una macchina virtuale da un modello Azure visibile all'abbonamento Azure associato ad AVD (utilizza le autorizzazioni Azure Service Principal)
- Check/Configure DNS address for new Virtual Machine using the Azure VNET designed during VDS Deployment (requires local ad permissions (Everything delegated to CW-Infrastructure above) (verifica/Configurazione indirizzo DNS per la nuova macchina virtuale utilizzando lo schema di denominazione VDS standard ***{companycode}TS{sequencenumber}***). Esempio: XYZTS3. (Richiede autorizzazioni ad locali (inserite nella struttura OU creata on-premise (desktop remoto/companycode/shared) (stessa autorizzazione/descrizione del gruppo di cui sopra)
- Posiziona la macchina virtuale nell'Active Directory Organizational Unit (ad) designata (richiede le autorizzazioni delegate alla struttura di unità organizzative (indicate durante il processo manuale sopra))
- Aggiornare la directory DNS ad interna con il nuovo nome del computer/indirizzo IP (richiede autorizzazioni ad locali)
- Aggiunta di una nuova macchina virtuale al dominio ad locale (richiede autorizzazioni ad locali)
- Aggiornare il database locale VDS con nuove informazioni sul server (non richiede autorizzazioni aggiuntive)
- Aggiungere la macchina virtuale al pool di host AVD designato (richiede le autorizzazioni AVD Service Principal)
- Installare i componenti chocolatey sulla nuova macchina virtuale (richiede il privilegio di amministratore del computer locale per l'account **CloudWorkspaceSVC**)
- Installare i componenti FSLogix per l'istanza AVD (richiede autorizzazioni amministrative del computer locale per l'unità organizzativa AVD nell'ad locale)
- Aggiornare l'oggetto Criteri di gruppo di ad Windows Firewall per consentire il traffico verso la nuova macchina virtuale (richiede la creazione/modifica dell'oggetto Criteri di gruppo ad per i criteri associati all'unità organizzativa AVD e alle macchine virtuali associate. Richiede la creazione/modifica del criterio GPO ad sull'unità organizzativa AVD nell'ad locale. Può essere disattivato dopo l'installazione se non si gestiscono le macchine virtuali tramite VDS).
- Impostare il flag "Allow New Connections" (Consenti nuove connessioni) sulla nuova macchina virtuale (richiede autorizzazioni Azure Service Principal)

Aggiungere le macchine virtuali ad Azure ad

Le macchine virtuali nel tenant Azure devono essere unite al dominio, tuttavia le macchine virtuali non possono unirsi direttamente ad Azure ad. Pertanto, VDS implementa il ruolo di controller di dominio nella piattaforma VDS e quindi sincronizza il controller di dominio con Azure ad utilizzando ad Connect. Le opzioni di configurazione alternative includono l'utilizzo di Azure ad Domain Services (AADDS), la sincronizzazione con un DC ibrido (una VM on-premise o altrove) utilizzando ad Connect o l'Unione diretta delle VM a un DC ibrido attraverso una VPN sito-sito o Azure ExpressRoute.

Pool di host AVD

I pool di host sono una raccolta di una o più macchine virtuali (VM) identiche all'interno degli ambienti di desktop virtuale Azure. Ogni pool di host può contenere un gruppo di applicazioni con cui gli utenti possono interagire come su un desktop fisico.

Host di sessione

All'interno di qualsiasi pool di host sono presenti una o più macchine virtuali identiche. Queste sessioni utente che si connettono a questo pool di host sono bilanciate dal carico dal servizio di bilanciamento del carico AVD.

Gruppi di applicazioni

Per impostazione predefinita, il gruppo di applicazioni *Desktop Users* viene creato al momento dell'implementazione. A tutti gli utenti di questo gruppo di applicazioni viene offerta un'esperienza desktop Windows completa. Inoltre, è possibile creare gruppi di app per fornire servizi di app streaming.

Spazio di lavoro per l'analisi dei log

Viene creato uno spazio di lavoro Log Analytics per memorizzare i log dei processi di implementazione e DSC e di altri servizi. Questa operazione può essere eliminata dopo l'implementazione, ma questa operazione non è consigliata in quanto abilita altre funzionalità. Per impostazione predefinita, i registri vengono conservati per 30 giorni, senza costi di conservazione.

Set di disponibilità

Un set di disponibilità viene impostato come parte del processo di implementazione per consentire la separazione delle macchine virtuali condivise (pool di host AVD condivisi, pool di risorse RDS) nei domini di errore. Se lo si desidera, è possibile eliminarla dopo l'implementazione, ma disattiverebbe l'opzione per fornire ulteriore tolleranza agli errori per le macchine virtuali condivise.

Vault di ripristino Azure

Durante l'implementazione, VDS Automation crea un Recovery Service Vault. Questa opzione è attualmente attivata per impostazione predefinita, poiché Azure Backup viene applicato a CWMGR1 durante il processo di implementazione. Questa opzione può essere disattivata e rimossa, se lo si desidera, ma viene ricreata se Azure Backup è attivato nell'ambiente.

Vault delle chiavi Azure

Un Azure Key Vault viene creato durante il processo di implementazione e viene utilizzato per memorizzare certificati, chiavi API e credenziali utilizzati dagli account di automazione Azure durante l'implementazione.

Appendice A – struttura predefinita dell'unità organizzativa Cloud Workspace

- Cloud Workspace
  - Cloud Workspace Companies
  - Server Cloud Workspace
    - Server dedicati per i clienti
    - Infrastruttura
- Server CWMGR
- Server gateway

- Server FTP
- Macchine virtuali modello
  - Desktop remoto
  - Staging
    - Account del servizio Cloud Workspace
  - Account del servizio client
  - Account dei servizi dell'infrastruttura
    - Utenti tecnici di Cloud Workspace
  - Gruppi
  - Tecnici TECH 3

Prerequisiti di AVD e VDS v5.4

Requisiti e note di AVD e VDS

Questo documento descrive gli elementi necessari per l'implementazione di Azure Virtual Desktop (AVD) utilizzando NetApp Virtual Desktop Service (VDS). La "lista di controllo rapido" fornisce un breve elenco dei componenti necessari e delle fasi di pre-implementazione da intraprendere per garantire un'implementazione efficiente. Il resto della guida fornisce maggiori dettagli per ciascun elemento, a seconda delle scelte di configurazione effettuate.

Checklist rapida

Requisiti di Azure

- Tenant Azure ad
- Microsoft 365 Licensing per il supporto di AVD
- Abbonamento Azure
- Quota Azure disponibile per le macchine virtuali Azure
- Azure Admin account con ruoli di amministrazione globale e di proprietà dell'abbonamento
- Account admin di dominio con ruolo 'Enterprise Admin' per la configurazione di ad Connect

Informazioni di pre-implementazione

- Determinare il numero totale di utenti
- Determinare la regione di Azure
- Determinare il tipo di Active Directory
- Determinare il tipo di storage
- Identificare l'immagine o i requisiti della VM host della sessione
- Valutare la configurazione di rete esistente di Azure e on-premise

Requisiti dettagliati per l'implementazione di VDS

Requisiti di connessione per l'utente finale

I seguenti client di desktop remoto supportano Azure Virtual Desktop:

- Desktop di Windows
- Web
- MacOS
- IOS
- IGEL Think Client (Linux)
- Android (anteprima)

Azure Virtual Desktop non supporta il client RemoteApp and Desktop Connections (RADC) o il client Remote Desktop Connection (MSTSC).

Azure Virtual Desktop attualmente non supporta il client Desktop remoto da Windows Store. Il supporto per questo client verrà aggiunto in una release futura.

I client di Desktop remoto devono avere accesso ai seguenti URL:

Indirizzo	Porta TCP in uscita	Scopo	Client
*.AVD.microsoft.com	443	Traffico di servizio	Tutto
*.servicebus.windows.net 443 risoluzione dei problemi	Tutto	go.microsoft.com	443
Microsoft FWLinks	Tutto	aka.ms.	443
Shortener URL Microsoft	Tutto	docs.microsoft.com	443
Documentazione	Tutto	privacy.microsoft.com	443
Dichiarazione sulla privacy	Tutto	query.prod.cms.rt.microsoft.com	443

L'apertura di questi URL è essenziale per un'esperienza client affidabile. Il blocco dell'accesso a questi URL non è supportato e influisce sulla funzionalità del servizio. Questi URL corrispondono solo ai siti e alle risorse client e non includono URL per altri servizi come Azure Active Directory.

Punto di partenza dell'installazione guidata VDS

L'installazione guidata di VDS è in grado di gestire gran parte della configurazione dei prerequisiti necessaria per una corretta implementazione di AVD. L'installazione guidata ("") crea o utilizza i seguenti componenti.

Tenant Azure

Obbligatorio: tenant Azure e Active Directory Azure

L'attivazione AVD in Azure è un'impostazione a livello di tenant. VDS supporta l'esecuzione di un'istanza AVD per tenant.

Iscrizione Azure

Obbligatorio: un abbonamento Azure (annotare l'ID dell'abbonamento che si desidera utilizzare)

Tutte le risorse Azure implementate devono essere configurate in un'unica sottoscrizione dedicata. In questo modo, il monitoraggio dei costi per AVD è molto più semplice e il processo di implementazione è semplificato. NOTA: Le versioni di prova gratuite di Azure non sono supportate in quanto non dispongono di crediti sufficienti per implementare un'implementazione AVD funzionale.

Quota core di Azure

Quota sufficiente per le famiglie di macchine virtuali che utilizzerai, in particolare almeno 10 core della famiglia DS v3 per l'implementazione iniziale della piattaforma (è possibile utilizzare solo 2 core, ma 10 copre ogni possibilità di implementazione iniziale).

Account amministratore di Azure

Obbligatorio: account amministratore globale Azure.

L'installazione guidata di VDS richiede all'amministratore di Azure di concedere autorizzazioni delegate all'entità del servizio VDS e di installare l'applicazione VDS Azure Enterprise. L'amministratore deve avere i seguenti ruoli Azure assegnati:

- Amministratore globale del tenant
- Ruolo del proprietario nell'abbonamento

Immagine della macchina virtuale

Obbligatorio: immagine Azure che supporta Windows 10 multisessione.

Azure Marketplace fornisce le versioni più recenti dell'immagine di base di Windows 10 e tutte le sottoscrizioni Azure possono accedervi automaticamente. Se desideri utilizzare un'immagine diversa o personalizzata, vuoi che il team VDS fornisca consigli sulla creazione o la modifica di altre immagini o abbia domande generali sulle immagini Azure, facci sapere e possiamo pianificare una conversazione.

Active Directory

AVD richiede che l'identità dell'utente faccia parte di Azure ad e che le macchine virtuali siano unite a un dominio Active Directory sincronizzato con la stessa istanza di Azure ad. Le VM non possono essere collegate direttamente all'istanza di Azure ad, pertanto è necessario configurare un controller di dominio e sincronizzarlo con Azure ad.

Queste opzioni supportate includono:

- La creazione automatica di un'istanza di Active Directory all'interno dell'abbonamento. L'istanza di ad viene in genere creata da VDS sulla VM di controllo VDS (CWMGR1) per le implementazioni di Azure Virtual Desktop che utilizzano questa opzione. AD Connect deve essere configurato e configurato per la sincronizzazione con Azure ad come parte del processo di installazione.

  []

- Integrazione in un dominio Active Directory esistente accessibile dall'abbonamento Azure (in genere tramite Azure VPN o Express Route) e con il relativo elenco utenti sincronizzato con Azure ad utilizzando ad Connect o un prodotto di terze parti.

[]

Layer di storage

In AVD, la strategia di storage è progettata in modo che non risiedano dati utente/aziendali persistenti sulle macchine virtuali della sessione AVD. I dati persistenti per i profili utente, i file utente e le cartelle e i dati aziendali/applicativi sono ospitati su uno o più volumi di dati ospitati su un livello di dati indipendente.

FSLogix è una tecnologia di containerizzazione dei profili che risolve molti problemi relativi ai profili utente (come la crescita dei dati e gli accessi lenti) montando un container di profili utente (formato VHD o VHDX) sull'host della sessione all'inizializzazione della sessione.

Grazie a questa architettura è necessaria una funzione di storage dei dati. Questa funzione deve essere in grado di gestire il trasferimento dei dati richiesto ogni mattina/pomeriggio quando una parte significativa degli utenti effettua l'accesso/disconnessione contemporaneamente. Anche gli ambienti di medie dimensioni possono avere requisiti significativi di trasferimento dei dati. Le prestazioni del disco del layer di storage dei dati sono una delle principali variabili di performance dell'utente finale e occorre prestare particolare attenzione a dimensionare in modo appropriato le performance di questo storage, non solo la quantità di storage. In genere, il livello di storage deve essere dimensionato in modo da supportare 5-15 IOPS per utente.

L'installazione guidata VDS supporta le seguenti configurazioni:

- Configurazione e configurazione di Azure NetApp Files (ANF) (consigliata). *Il livello di servizio standard ANF supporta fino a 150 utenti, mentre gli ambienti di 150-500 utenti sono consigliati ANF Premium. Per oltre 500 utenti si consiglia ANF Ultra.*

  []

- Installazione e configurazione di una macchina virtuale file server

  []

Networking

Obbligatorio: un inventario di tutte le subnet di rete esistenti, incluse le subnet visibili all'abbonamento Azure tramite un percorso Azure Express o una VPN. L'implementazione deve evitare la sovrapposizione delle subnet.

L'installazione guidata di VDS consente di definire l'ambito della rete nel caso in cui sia necessario o debba essere evitato un intervallo come parte dell'integrazione pianificata con le reti esistenti.

Determinare un intervallo IP per l'utente durante l'implementazione. Secondo le Best practice di Azure, sono supportati solo gli indirizzi IP in un intervallo privato.

Le opzioni supportate includono i seguenti valori, ma il valore predefinito è /20:

- da 192.168.0.0 a 192.168.255.255
- da 172.16.0.0 a 172.31.255.255
- da 10.0.0.0 a 10.255.255.255

CWMGR1

Alcune delle funzionalità esclusive di VDS, come la pianificazione del carico di lavoro per il risparmio dei costi e la funzionalità Live Scaling, richiedono una presenza amministrativa all'interno del tenant e dell'abbonamento. Pertanto, una macchina virtuale amministrativa denominata CWMGR1 viene implementata

come parte dell'automazione della procedura guidata di installazione VDS. Oltre alle attività di automazione VDS, questa macchina virtuale contiene anche la configurazione VDS in un database SQL Express, file di log locali e un'utility di configurazione avanzata chiamata DCConfig.

A seconda delle selezioni effettuate nell'installazione guidata VDS, questa macchina virtuale può essere utilizzata per ospitare funzionalità aggiuntive, tra cui:

- Un gateway RDS (utilizzato solo nelle implementazioni RDS)
- Un gateway HTML 5 (utilizzato solo nelle implementazioni RDS)
- Un server di licenza RDS (utilizzato solo nelle implementazioni RDS)
- Un controller di dominio (se scelto)

Albero decisionale nella procedura guidata di implementazione

Nell'ambito dell'implementazione iniziale, viene fornita una serie di domande per personalizzare le impostazioni del nuovo ambiente. Di seguito è riportata una descrizione delle principali decisioni da prendere.

Regione di Azure

Decidere quale regione o quali regioni Azure ospiteranno le macchine virtuali AVD. Tenere presente che Azure NetApp Files e alcune famiglie di macchine virtuali (ad esempio, le macchine virtuali abilitate alla GPU) dispongono di un elenco di supporto delle regioni Azure definito, mentre AVD è disponibile nella maggior parte delle regioni.

- Questo link può essere utilizzato per identificare "Disponibilità dei prodotti Azure per regione"

Tipo di Active Directory

Scegliere il tipo di Active Directory che si desidera utilizzare:

- Active Directory esistente on-premise
- Fare riferimento a. "Componenti e autorizzazioni di AVD VDS" Documento per una spiegazione delle autorizzazioni e dei componenti richiesti in Azure e nell'ambiente Active Directory locale
- Nuova istanza di Active Directory basata su abbonamento Azure
- Servizi di dominio Active Directory di Azure

Storage dei dati

Decidere dove collocare i dati per i profili utente, i singoli file e le condivisioni aziendali. Le scelte includono:

- Azure NetApp Files
- File Azure
- File server tradizionale (Azure VM con disco gestito)

Requisiti di implementazione di NetApp VDS per i componenti esistenti

Implementazione di NetApp VDS con i controller di dominio Active Directory esistenti

Questo tipo di configurazione estende un dominio Active Directory esistente per supportare l'istanza di AVD. In questo caso, VDS implementa un set limitato di componenti nel dominio per supportare attività di provisioning e gestione automatizzate per i componenti AVD.

Questa configurazione richiede:

- Un controller di dominio Active Directory esistente a cui possono accedere le macchine virtuali su Azure VNET, in genere tramite Azure VPN o Express Route O un controller di dominio creato in Azure.
- Aggiunta di componenti VDS e autorizzazioni necessarie per la gestione VDS dei pool di host AVD e dei volumi di dati quando vengono Uniti al dominio. La guida relativa ai componenti e alle autorizzazioni di AVD VDS definisce i componenti e le autorizzazioni richiesti e il processo di implementazione richiede che un utente di dominio con privilegi di dominio esegua lo script che creerà gli elementi necessari.
- Si noti che l'implementazione VDS crea un VNET per impostazione predefinita per le VM create da VDS. È possibile eseguire il peering di VNET con reti VNet di rete Azure esistenti oppure spostare la macchina virtuale CWMGR1 in una rete VNET esistente con le subnet richieste predefinite.

Tool per la preparazione delle credenziali e dei domini

Gli amministratori devono fornire una credenziale Domain Administrator a un certo punto del processo di implementazione. È possibile creare, utilizzare ed eliminare una credenziale temporanea di Domain Administrator in un secondo momento (una volta completato il processo di implementazione). In alternativa, i clienti che necessitano di assistenza per la creazione dei prerequisiti possono sfruttare il Domain Preparation Tool.

Implementazione di NetApp VDS con file system esistente

VDS crea condivisioni Windows che consentono di accedere al profilo utente, alle cartelle personali e ai dati aziendali dalle VM di sessione AVD. VDS implementerà le opzioni file Server o Azure NetApp file per impostazione predefinita, ma se si dispone di un componente di file storage esistente, VDS può puntare le condivisioni a tale componente una volta completata l'implementazione di VDS.

I requisiti per l'utilizzo e il componente di storage esistente:

- Il componente deve supportare SMB v3
- Il componente deve essere Unito allo stesso dominio Active Directory degli host di sessione AVD
- Il componente deve essere in grado di esporre un percorso UNC per l'utilizzo nella configurazione VDS: È possibile utilizzare un percorso per tutte e tre le condivisioni oppure specificare percorsi separati per ciascuna. Si noti che VDS imposterà le autorizzazioni a livello utente per queste condivisioni, quindi fare riferimento al documento componenti e permessi di VDS AVD per assicurarsi che siano state concesse le autorizzazioni appropriate ai VDS Automation Services.

Implementazione di NetApp VDS con servizi di dominio ad Azure esistenti

Questa configurazione richiede un processo per identificare gli attributi dell'istanza esistente dei servizi di dominio Active Directory di Azure. Contatta il tuo account manager per richiedere un'implementazione di questo tipo. Implementazione di NetApp VDS con implementazione di AVD esistente questo tipo di configurazione presuppone che esistano già i componenti Azure VNET, Active Directory e AVD necessari. L'implementazione di VDS viene eseguita allo stesso modo della configurazione "NetApp VDS Deployment with Existing ad" (implementazione di NetApp VDS con ad esistente), ma aggiunge i seguenti requisiti:

- RD il ruolo di proprietario del tenant AVD deve essere assegnato alle applicazioni VDS Enterprise in Azure
- Le VM AVD host Pool e AVD host Pool devono essere importate in VDS utilizzando la funzione di importazione VDS nell'applicazione Web VDS. Questo processo raccoglie i metadati del pool di host AVD e della VM di sessione e li memorizza in IT VDS in modo che questi elementi possano essere gestiti da VDS
- I dati AVD User devono essere importati nella sezione VDS User (utente VDS) utilizzando lo strumento CRA. Questo processo inserisce i metadati relativi a ciascun utente nel piano di controllo VDS in modo che

le informazioni sulla sessione e l'appartenenza a AVD App Group possano essere gestite da VDS

APPENDICE A: URL del piano di controllo VDS e indirizzi IP

I componenti VDS nell'abbonamento Azure comunicano con i componenti del piano di controllo globale VDS, come l'applicazione Web VDS e gli endpoint API VDS. Per l'accesso, è necessario mettere in sicurezza i seguenti indirizzi URI di base per l'accesso bidirezionale sulla porta 443:

"" "" "" "" ""

Se il dispositivo di controllo degli accessi può elencare solo in base all'indirizzo IP, è necessario che il seguente elenco di indirizzi IP sia protetto. Si noti che VDS utilizza il servizio Azure Traffic Manager, pertanto questo elenco potrebbe cambiare nel tempo:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239 52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

APPENDICE B: Requisiti di Microsoft AVD

Questa sezione sui requisiti di Microsoft AVD è un riepilogo dei requisiti di AVD di Microsoft. I requisiti AVD completi e attuali sono disponibili qui:

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Licenze host sessione di Azure Virtual Desktop

Azure Virtual Desktop supporta i seguenti sistemi operativi, quindi assicurati di disporre delle licenze appropriate per gli utenti in base al desktop e alle applicazioni che intendi implementare:

SISTEMA OPERATIVO	Licenza richiesta
Windows 10 Enterprise multisessione o Windows 10 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows 7 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows Server 2012 R2, 2016, 2019	RDS Client Access License (CAL) con Software Assurance

Accesso URL per macchine AVD

Le macchine virtuali Azure create per Azure Virtual Desktop devono avere accesso ai seguenti URL:

Indirizzo	Porta TCP in uscita	Scopo	Codice di matricola
*.AVD.microsoft.com	443	Traffico di servizio	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Aggiornamenti dello stack SXS e Agent	AzureCloud
*.core.windows.net	443	Traffico dell'agente	AzureCloud
*.servicebus.windows.net	443	Traffico dell'agente	AzureCloud

Indirizzo	Porta TCP in uscita	Scopo	Codice di matricola
prod.warmpath.msftcloudes.com	443	Traffico dell'agente	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Attivazione di Windows	Internet
AVDportalstorageblob.blob.core.windows.net	443	Supporto del portale Azure	AzureCloud

La seguente tabella elenca gli URL opzionali a cui le macchine virtuali Azure possono accedere:

Indirizzo	Porta TCP in uscita	Scopo	Codice di matricola
*.microsoftonline.com	443	Autenticazione ai servizi MS Online	Nessuno
*.events.data.microsoft.com	443	Servizio di telemetria	Nessuno
www.msftconnecttest.com	443	Rileva se il sistema operativo è connesso a Internet	Nessuno
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	Nessuno
login.windows.net	443	Accedere a MS Online Services, Office 365	Nessuno
*.sfx.ms.	443	Aggiornamenti per il software client OneDrive	Nessuno
*.digicert.com	443	Verifica della revoca del certificato	Nessuno

Fattori di performance ottimali

Per ottenere prestazioni ottimali, assicurarsi che la rete soddisfi i seguenti requisiti:

- La latenza di andata e ritorno (RTT) dalla rete del client alla regione Azure in cui sono stati implementati i pool di host deve essere inferiore a 150 ms.
- Il traffico di rete può fluire al di fuori dei confini del paese/regione quando le macchine virtuali che ospitano desktop e applicazioni si connettono al servizio di gestione.
- Per ottimizzare le performance di rete, si consiglia di allocare le VM dell'host di sessione nella stessa regione Azure del servizio di gestione.

Immagini del sistema operativo delle macchine virtuali supportate

Azure Virtual Desktop supporta le seguenti immagini del sistema operativo x64:

- Windows 10 Enterprise multisessione, versione 1809 o successiva
- Windows 10 Enterprise, versione 1809 o successiva

- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop non supporta le immagini dei sistemi operativi x86 (32 bit), Windows 10 Enterprise N o Windows 10 Enterprise KN. Windows 7 non supporta inoltre soluzioni di profili basate su VHD o VHDX ospitate su Azure Storage gestito a causa di una limitazione delle dimensioni del settore.

Le opzioni di automazione e implementazione disponibili dipendono dal sistema operativo e dalla versione scelti, come mostrato nella tabella seguente:

Sistema operativo	Galleria di immagini Azure	Implementazione manuale delle macchine virtuali	Integrazione dei modelli ARM	Provisioning dei pool di host su Azure Marketplace
Windows 10 multisessione, versione 1903	Sì	Sì	Sì	Sì
Windows 10 multisessione, versione 1809	Sì	Sì	No	No
Windows 10 Enterprise, versione 1903	Sì	Sì	Sì	Sì
Windows 10 Enterprise, versione 1809	Sì	Sì	No	No
Windows 7 Enterprise	Sì	Sì	No	No
Windows Server 2019	Sì	Sì	No	No
Windows Server 2016	Sì	Sì	Sì	Sì
Windows Server 2012 R2	Sì	Sì	No	No

Prerequisiti di AVD e VDS v6.0

Requisiti e note di AVD e VDS

Questo documento descrive gli elementi necessari per l'implementazione di Azure Virtual Desktop (AVD) utilizzando NetApp Virtual Desktop Service (VDS). La "lista di controllo rapido" fornisce un breve elenco dei componenti necessari e delle fasi di pre-implementazione da intraprendere per garantire un'implementazione efficiente. Il resto della guida fornisce maggiori dettagli per ciascun elemento, a seconda delle scelte di configurazione effettuate.

Checklist rapida

Requisiti di Azure

- Tenant Azure ad
- Microsoft 365 Licensing per il supporto di AVD
- Abbonamento Azure
- Quota Azure disponibile per le macchine virtuali Azure
- Azure Admin account con ruoli di amministrazione globale e di proprietà dell'abbonamento

- Account admin di dominio con ruolo 'Enterprise Admin' per la configurazione di ad Connect

Informazioni di pre-implementazione

- Determinare il numero totale di utenti
- Determinare la regione di Azure
- Determinare il tipo di Active Directory
- Determinare il tipo di storage
- Identificare l'immagine o i requisiti della VM host della sessione
- Valutare la configurazione di rete esistente di Azure e on-premise

Requisiti dettagliati per l'implementazione di VDS

Requisiti di connessione per l'utente finale

I seguenti client di desktop remoto supportano Azure Virtual Desktop:

- Desktop di Windows
- Web
- MacOS
- IOS
- IGEL Think Client (Linux)
- Android (anteprima)

> Azure Virtual Desktop non supporta il client RemoteApp and Desktop Connections (RADC) o il client Remote Desktop Connection (MSTSC).

> Azure Virtual Desktop attualmente non supporta il client Desktop remoto da Windows Store. Il supporto per questo client verrà aggiunto in una release futura.

I client di Desktop remoto devono avere accesso ai seguenti URL:

Indirizzo	Porta TCP in uscita	Scopo	Client
*.wvd.microsoft.com	443	Traffico di servizio	Tutto
*.servicebus.windows.net	443	Risoluzione dei problemi relativi ai dati	Tutto
go.microsoft.com	443	Microsoft FWLinks	Tutto
aka.ms.	443	Shortener URL Microsoft	Tutto
docs.microsoft.com	443	Documentazione	Tutto
privacy.microsoft.com	443	Dichiarazione sulla privacy	Tutto
query.prod.cms.rt.microsoft.com	443	Aggiornamenti del client	Desktop di Windows

L’apertura di questi URL è essenziale per un’esperienza client affidabile. Il blocco dell’accesso a questi URL non è supportato e influisce sulla funzionalità del servizio. Questi URL corrispondono solo ai siti e alle risorse client e non includono URL per altri servizi come Azure Active Directory.

Punto di partenza dell’installazione guidata VDS

L’installazione guidata di VDS è in grado di gestire gran parte della configurazione dei prerequisiti necessaria per una corretta implementazione di AVD. L’installazione guidata ("") crea o utilizza i seguenti componenti.

Tenant Azure

Obbligatorio: tenant Azure e Active Directory Azure

L’attivazione AVD in Azure è un’impostazione a livello di tenant. VDS supporta l’esecuzione di un’istanza AVD per tenant.

Iscrizione Azure

Obbligatorio: un abbonamento Azure (annotare l’ID dell’abbonamento che si desidera utilizzare)

Tutte le risorse Azure implementate devono essere configurate in un’unica sottoscrizione dedicata. In questo modo, il monitoraggio dei costi per AVD è molto più semplice e il processo di implementazione è semplificato. NOTA: Le versioni di prova gratuite di Azure non sono supportate in quanto non dispongono di crediti sufficienti per implementare un’implementazione AVD funzionale.

Quota core di Azure

Quota sufficiente per le famiglie di macchine virtuali che utilizzerai, in particolare almeno 10 core della famiglia DS v3 per l’implementazione iniziale della piattaforma (è possibile utilizzare solo 2 core, ma 10 copre ogni possibilità di implementazione iniziale).

Account amministratore di Azure

Obbligatorio: account amministratore globale Azure.

L’installazione guidata di VDS richiede all’amministratore di Azure di concedere autorizzazioni delegate all’entità del servizio VDS e di installare l’applicazione VDS Azure Enterprise. L’amministratore deve avere i seguenti ruoli Azure assegnati:

- Amministratore globale del tenant
- Ruolo del proprietario nell’abbonamento

Immagine della macchina virtuale

Obbligatorio: immagine Azure che supporta Windows 10 multisessione.

Azure Marketplace fornisce le versioni più recenti dell’immagine di base di Windows 10 e tutte le sottoscrizioni Azure possono accedervi automaticamente. Se desideri utilizzare un’immagine diversa o personalizzata, vuoi che il team VDS fornisca consigli sulla creazione o la modifica di altre immagini o abbia domande generali sulle immagini Azure, facci sapere e possiamo pianificare una conversazione.

Active Directory

AVD richiede che l'identità dell'utente faccia parte di Azure ad e che le macchine virtuali siano unite a un dominio Active Directory sincronizzato con la stessa istanza di Azure ad. Le VM non possono essere collegate direttamente all'istanza di Azure ad, pertanto è necessario configurare un controller di dominio e sincronizzarlo con Azure ad.

Queste opzioni supportate includono:

- La creazione automatica di un'istanza di Active Directory all'interno dell'abbonamento. L'istanza di ad viene in genere creata da VDS sulla VM di controllo VDS (CWMGR1) per le implementazioni di Azure Virtual Desktop che utilizzano questa opzione. AD Connect deve essere configurato e configurato per la sincronizzazione con Azure ad come parte del processo di installazione.

  []

- Integrazione in un dominio Active Directory esistente accessibile dall'abbonamento Azure (in genere tramite Azure VPN o Express Route) e con il relativo elenco utenti sincronizzato con Azure ad utilizzando ad Connect o un prodotto di terze parti.

  []

Layer di storage

In AVD, la strategia di storage è progettata in modo che non risiedano dati utente/aziendali persistenti sulle macchine virtuali della sessione AVD. I dati persistenti per i profili utente, i file utente e le cartelle e i dati aziendali/applicativi sono ospitati su uno o più volumi di dati ospitati su un livello di dati indipendente.

FSLogix è una tecnologia di containerizzazione dei profili che risolve molti problemi relativi ai profili utente (come la crescita dei dati e gli accessi lenti) montando un container di profili utente (formato VHD o VHDX) sull'host della sessione all'inizializzazione della sessione.

Grazie a questa architettura è necessaria una funzione di storage dei dati. Questa funzione deve essere in grado di gestire il trasferimento dei dati richiesto ogni mattina/pomeriggio quando una parte significativa degli utenti effettua l'accesso/disconnessione contemporaneamente. Anche gli ambienti di medie dimensioni possono avere requisiti significativi di trasferimento dei dati. Le prestazioni del disco del layer di storage dei dati sono una delle principali variabili di performance dell'utente finale e occorre prestare particolare attenzione a dimensionare in modo appropriato le performance di questo storage, non solo la quantità di storage. In genere, il livello di storage deve essere dimensionato in modo da supportare 5-15 IOPS per utente.

L'installazione guidata VDS supporta le seguenti configurazioni:

- Configurazione e configurazione di Azure NetApp Files (ANF) (consigliata). *Il livello di servizio standard ANF supporta fino a 150 utenti, mentre gli ambienti di 150-500 utenti sono consigliati ANF Premium. Per oltre 500 utenti si consiglia ANF Ultra.*

  []

- Installazione e configurazione di una macchina virtuale file server

  []

Networking

Obbligatorio: un inventario di tutte le subnet di rete esistenti, incluse le subnet visibili all'abbonamento Azure tramite un percorso Azure Express o una VPN. L'implementazione deve evitare la sovrapposizione delle

subnet.

L'installazione guidata di VDS consente di definire l'ambito della rete nel caso in cui sia necessario o debba essere evitato un intervallo come parte dell'integrazione pianificata con le reti esistenti.

Determinare un intervallo IP per l'utente durante l'implementazione. Secondo le Best practice di Azure, sono supportati solo gli indirizzi IP in un intervallo privato.

Le opzioni supportate includono i seguenti valori, ma il valore predefinito è /20:

- da 192.168.0.0 a 192.168.255.255
- da 172.16.0.0 a 172.31.255.255
- da 10.0.0.0 a 10.255.255.255

CWMGR1

Alcune delle funzionalità esclusive di VDS, come la pianificazione del carico di lavoro per il risparmio dei costi e la funzionalità Live Scaling, richiedono una presenza amministrativa all'interno del tenant e dell'abbonamento. Pertanto, una macchina virtuale amministrativa denominata CWMGR1 viene implementata come parte dell'automazione della procedura guidata di installazione VDS. Oltre alle attività di automazione VDS, questa macchina virtuale contiene anche la configurazione VDS in un database SQL Express, file di log locali e un'utility di configurazione avanzata chiamata DCConfig.

A seconda delle selezioni effettuate nell'installazione guidata VDS, questa macchina virtuale può essere utilizzata per ospitare funzionalità aggiuntive, tra cui:

- Un gateway RDS (utilizzato solo nelle implementazioni RDS)
- Un gateway HTML 5 (utilizzato solo nelle implementazioni RDS)
- Un server di licenza RDS (utilizzato solo nelle implementazioni RDS)
- Un controller di dominio (se scelto)

Albero decisionale nella procedura guidata di implementazione

Nell'ambito dell'implementazione iniziale, viene fornita una serie di domande per personalizzare le impostazioni del nuovo ambiente. Di seguito è riportata una descrizione delle principali decisioni da prendere.

Regione di Azure

Decidere quale regione o quali regioni Azure ospiteranno le macchine virtuali AVD. Tenere presente che Azure NetApp Files e alcune famiglie di macchine virtuali (ad esempio, le macchine virtuali abilitate alla GPU) dispongono di un elenco di supporto delle regioni Azure definito, mentre AVD è disponibile nella maggior parte delle regioni.

- Questo link può essere utilizzato per identificare "Disponibilità dei prodotti Azure per regione"

Tipo di Active Directory

Scegliere il tipo di Active Directory che si desidera utilizzare:

- Active Directory esistente on-premise
- Fare riferimento a. "Componenti e autorizzazioni di AVD VDS" Documento per una spiegazione delle autorizzazioni e dei componenti richiesti in Azure e nell'ambiente Active Directory locale
- Nuova istanza di Active Directory basata su abbonamento Azure

- Servizi di dominio Active Directory di Azure

Storage dei dati

Decidere dove collocare i dati per i profili utente, i singoli file e le condivisioni aziendali. Le scelte includono:

- Azure NetApp Files
- File Azure
- File server tradizionale (Azure VM con disco gestito)

Requisiti di implementazione di NetApp VDS per i componenti esistenti

Implementazione di NetApp VDS con i controller di dominio Active Directory esistenti

Questo tipo di configurazione estende un dominio Active Directory esistente per supportare l'istanza di AVD. In questo caso, VDS implementa un set limitato di componenti nel dominio per supportare attività di provisioning e gestione automatizzate per i componenti AVD.

Questa configurazione richiede:

- Un controller di dominio Active Directory esistente a cui possono accedere le macchine virtuali su Azure VNET, in genere tramite Azure VPN o Express Route O un controller di dominio creato in Azure.
- Aggiunta di componenti VDS e autorizzazioni necessarie per la gestione VDS dei pool di host AVD e dei volumi di dati quando vengono Uniti al dominio. La guida relativa ai componenti e alle autorizzazioni di AVD VDS definisce i componenti e le autorizzazioni richiesti e il processo di implementazione richiede che un utente di dominio con privilegi di dominio esegua lo script che creerà gli elementi necessari.
- Si noti che l'implementazione VDS crea un VNET per impostazione predefinita per le VM create da VDS. È possibile eseguire il peering di VNET con reti VNet di rete Azure esistenti oppure spostare la macchina virtuale CWMGR1 in una rete VNET esistente con le subnet richieste predefinite.

Tool per la preparazione delle credenziali e dei domini

Gli amministratori devono fornire una credenziale Domain Administrator a un certo punto del processo di implementazione. È possibile creare, utilizzare ed eliminare una credenziale temporanea di Domain Administrator in un secondo momento (una volta completato il processo di implementazione). In alternativa, i clienti che necessitano di assistenza per la creazione dei prerequisiti possono sfruttare il Domain Preparation Tool.

Implementazione di NetApp VDS con file system esistente

VDS crea condivisioni Windows che consentono di accedere al profilo utente, alle cartelle personali e ai dati aziendali dalle VM di sessione AVD. VDS implementerà le opzioni file Server o Azure NetApp file per impostazione predefinita, ma se si dispone di un componente di file storage esistente, VDS può puntare le condivisioni a tale componente una volta completata l'implementazione di VDS.

I requisiti per l'utilizzo e il componente di storage esistente:

- Il componente deve supportare SMB v3
- Il componente deve essere Unito allo stesso dominio Active Directory degli host di sessione AVD
- Il componente deve essere in grado di esporre un percorso UNC per l'utilizzo nella configurazione VDS: È possibile utilizzare un percorso per tutte e tre le condivisioni oppure specificare percorsi separati per ciascuna. Si noti che VDS imposterà le autorizzazioni a livello utente per queste condivisioni, quindi fare riferimento al documento componenti e permessi di VDS AVD per assicurarsi che siano state concesse le

autorizzazioni appropriate ai VDS Automation Services.

Implementazione di NetApp VDS con servizi di dominio ad Azure esistenti

Questa configurazione richiede un processo per identificare gli attributi dell'istanza esistente dei servizi di dominio Active Directory di Azure. Contatta il tuo account manager per richiedere un'implementazione di questo tipo. Implementazione di NetApp VDS con implementazione di AVD esistente questo tipo di configurazione presuppone che esistano già i componenti Azure VNET, Active Directory e AVD necessari. L'implementazione di VDS viene eseguita allo stesso modo della configurazione "NetApp VDS Deployment with Existing ad" (implementazione di NetApp VDS con ad esistente), ma aggiunge i seguenti requisiti:

- RD il ruolo di proprietario del tenant AVD deve essere assegnato alle applicazioni VDS Enterprise in Azure
- Le VM AVD host Pool e AVD host Pool devono essere importate in VDS utilizzando la funzione di importazione VDS nell'applicazione Web VDS. Questo processo raccoglie i metadati del pool di host AVD e della VM di sessione e li memorizza in IT VDS in modo che questi elementi possano essere gestiti da VDS
- I dati AVD User devono essere importati nella sezione VDS User (utente VDS) utilizzando lo strumento CRA. Questo processo inserisce i metadati relativi a ciascun utente nel piano di controllo VDS in modo che le informazioni sulla sessione e l'appartenenza a AVD App Group possano essere gestite da VDS

APPENDICE A: URL del piano di controllo VDS e indirizzi IP

I componenti VDS nell'abbonamento Azure comunicano con i componenti del piano di controllo globale VDS, come l'applicazione Web VDS e gli endpoint API VDS. Per l'accesso, è necessario mettere in sicurezza i seguenti indirizzi URI di base per l'accesso bidirezionale sulla porta 443:

"" "" "" "" ""

Se il dispositivo di controllo degli accessi può elencare solo in base all'indirizzo IP, è necessario che il seguente elenco di indirizzi IP sia protetto. Si noti che VDS utilizza il servizio Azure Traffic Manager, pertanto questo elenco potrebbe cambiare nel tempo:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239 52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

APPENDICE B: Requisiti di Microsoft AVD

Questa sezione sui requisiti di Microsoft AVD è un riepilogo dei requisiti di AVD di Microsoft. I requisiti AVD completi e attuali sono disponibili qui:

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Licenze host sessione di Azure Virtual Desktop

Azure Virtual Desktop supporta i seguenti sistemi operativi, quindi assicurati di disporre delle licenze appropriate per gli utenti in base al desktop e alle applicazioni che intendi implementare:

SISTEMA OPERATIVO	Licenza richiesta
Windows 10 Enterprise multisessione o Windows 10 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5

SISTEMA OPERATIVO	Licenza richiesta
Windows 7 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows Server 2012 R2, 2016, 2019	RDS Client Access License (CAL) con Software Assurance

Accesso URL per macchine AVD

Le macchine virtuali Azure create per Azure Virtual Desktop devono avere accesso ai seguenti URL:

Indirizzo	Porta TCP in uscita	Scopo	Codice di matricola
*.AVD.microsoft.com	443	Traffico di servizio	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Aggiornamenti dello stack SXS e Agent	AzureCloud
*.core.windows.net	443	Traffico dell'agente	AzureCloud
*.servicebus.windows.net	443	Traffico dell'agente	AzureCloud
prod.warmpath.msftcloudes.com	443	Traffico dell'agente	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Attivazione di Windows	Internet
AVDportalstorageblob.blob.core.windows.net	443	Supporto del portale Azure	AzureCloud

La seguente tabella elenca gli URL opzionali a cui le macchine virtuali Azure possono accedere:

Indirizzo	Porta TCP in uscita	Scopo	Codice di matricola
*.microsoftonline.com	443	Autenticazione ai servizi MS Online	Nessuno
*.events.data.microsoft.com	443	Servizio di telemetria	Nessuno
www.msftconnecttest.com	443	Rileva se il sistema operativo è connesso a Internet	Nessuno
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	Nessuno
login.windows.net	443	Accedere a MS Online Services, Office 365	Nessuno
*.sfx.ms.	443	Aggiornamenti per il software client OneDrive	Nessuno
*.digicert.com	443	Verifica della revoca del certificato	Nessuno

Fattori di performance ottimali

Per ottenere prestazioni ottimali, assicurarsi che la rete soddisfi i seguenti requisiti:

- La latenza di andata e ritorno (RTT) dalla rete del client alla regione Azure in cui sono stati implementati i pool di host deve essere inferiore a 150 ms.
- Il traffico di rete può fluire al di fuori dei confini del paese/regione quando le macchine virtuali che ospitano desktop e applicazioni si connettono al servizio di gestione.
- Per ottimizzare le performance di rete, si consiglia di allocare le VM dell'host di sessione nella stessa regione Azure del servizio di gestione.

Immagini del sistema operativo delle macchine virtuali supportate

Azure Virtual Desktop supporta le seguenti immagini del sistema operativo x64:

- Windows 10 Enterprise multisessione, versione 1809 o successiva
- Windows 10 Enterprise, versione 1809 o successiva
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop non supporta le immagini dei sistemi operativi x86 (32 bit), Windows 10 Enterprise N o Windows 10 Enterprise KN. Windows 7 non supporta inoltre soluzioni di profili basate su VHD o VHDX ospitate su Azure Storage gestito a causa di una limitazione delle dimensioni del settore.

Le opzioni di automazione e implementazione disponibili dipendono dal sistema operativo e dalla versione scelti, come mostrato nella tabella seguente:

Sistema operativo	Galleria di immagini Azure	Implementazione manuale delle macchine virtuali	Integrazione dei modelli ARM	Provisioning dei pool di host su Azure Marketplace
Windows 10 multisessione, versione 1903	Sì	Sì	Sì	Sì
Windows 10 multisessione, versione 1809	Sì	Sì	No	No
Windows 10 Enterprise, versione 1903	Sì	Sì	Sì	Sì
Windows 10 Enterprise, versione 1809	Sì	Sì	No	No
Windows 7 Enterprise	Sì	Sì	No	No
Windows Server 2019	Sì	Sì	No	No
Windows Server 2016	Sì	Sì	Sì	Sì
Windows Server 2012 R2	Sì	Sì	No	No

Google

Guida all’implementazione di RDS per Google Cloud (GCP)

Panoramica

Questa guida fornisce le istruzioni dettagliate per creare un’implementazione RDS (Remote Desktop Service) utilizzando NetApp Virtual Desktop Service (VDS) in Google Cloud.

Questa guida POC (Proof of of concept) è progettata per aiutarti a implementare e configurare rapidamente RDS nel tuo progetto GCP di prova.

Le implementazioni in produzione, in particolare negli ambienti ad esistenti, sono molto comuni, tuttavia questo processo non viene considerato in questa guida POC. I POC complessi e le implementazioni di produzione devono essere avviati con i team di vendita/servizi VDS di NetApp e non eseguiti in modo self-service.

Il presente documento POC illustra l’intera implementazione RDS e fornisce una breve panoramica delle principali aree di configurazione post-implementazione disponibili nella piattaforma VDS. Una volta completato, avrai un ambiente RDS completamente implementato e funzionale, completo di host di sessione, applicazioni e utenti. In alternativa, avrai la possibilità di configurare la distribuzione automatica delle applicazioni, i gruppi di sicurezza, le autorizzazioni di condivisione file, Cloud Backup, ottimizzazione intelligente dei costi. VDS implementa una serie di impostazioni di Best practice tramite GPO. Sono inoltre incluse istruzioni su come disattivare facoltativamente questi controlli, nel caso in cui il POC non necessiti di alcun controllo di sicurezza, in modo simile a un ambiente di dispositivi locali non gestito.

Architettura di implementazione

[larghezza=75%]

Nozioni di base su RDS

VDS implementa un ambiente RDS completamente funzionale, con tutti i servizi di supporto necessari da zero. Questa funzionalità può includere:

- Server gateway RDS
- Server di accesso client Web
- Server controller di dominio
- Servizio di licenza RDS
- Servizio di licenza ThinPrint
- Servizio del server FTPS di FileZilla

Scopo della guida

Questa guida illustra l’implementazione di RDS utilizzando la tecnologia NetApp VDS dal punto di vista di un amministratore GCP e VDS. Il progetto GCP non prevede alcuna preconfigurazione e questa guida ti aiuta a configurare RDS end-to-end

Creare un account di servizio

1. In GCP, selezionare (o cercare) *IAM & Admin > Service Accounts*

   []

2. FARE CLIC SU + *CREATE SERVICE ACCOUNT*

   []

3. Inserire un nome account di servizio univoco e fare clic su *CREATE*. Annotare l'indirizzo e-mail dell'account di servizio che verrà utilizzato in un passaggio successivo.

   []

4. Selezionare il ruolo *Owner* per l'account del servizio, quindi fare clic su *CONTINUE*

   []

5. Nella pagina successiva non sono necessarie modifiche (*Consenti agli utenti di accedere a questo account di servizio (opzionale)*), fare clic su *DONE*

   []

6. Dalla pagina *account servizio*, fare clic sul menu delle azioni e selezionare *Crea chiave*

   []

7. Selezionare *P12* e fare clic su *CREATE*

   []

8. Scaricare il file .P12 e salvarlo sul computer. La *password della chiave privata* è rimasta invariata.

   []

   []

Abilitare Google compute API

1. In GCP, selezionare (o cercare) *API & servizi* > *Libreria*

   []

2. Nella libreria API GCP, selezionare (o cercare) *Compute Engine API*, quindi fare clic su *ENABLE*

   []

Creare una nuova implementazione VDS

1. In VDS, accedere a *Deployments* e fare clic su + *New Deployment*

   []

2. Immettere un nome per l'implementazione

   []

3. Selezionare *Google Cloud Platform*

   []

Piattaforma di infrastruttura

1. Immettere l' *ID progetto* e l'indirizzo e-mail OAuth. Caricare il file .P12 dalle pagine precedenti di questa guida e selezionare la zona appropriata per questa implementazione. Fare clic su *Test* per verificare che le voci siano corrette e che siano state impostate le autorizzazioni appropriate.

   L'indirizzo e-mail OAuth è l'indirizzo dell'account di servizio creato in precedenza in questa guida.

   []

2. Una volta confermata, fare clic su *Continue* (continua)

   []

Account

Account VM locali

1. Inserire una password per l'account Administrator locale. Documentare questa password per un utilizzo successivo.
2. Inserire una password per l'account SA SQL. Documentare questa password per un utilizzo successivo.

La complessità della password richiede un minimo di 8 caratteri con 3 dei 4 seguenti tipi di caratteri: Maiuscolo, minuscolo, numero, carattere speciale

Account SMTP

VDS può inviare notifiche e-mail tramite impostazioni SMTP personalizzate oppure è possibile utilizzare il servizio SMTP incorporato selezionando *automatico*.

1. Inserire un indirizzo e-mail da utilizzare come indirizzo *from* quando VDS invia la notifica via e-mail. *no-reply@<your-domain>.com* è un formato comune.
2. Inserire un indirizzo e-mail in cui indirizzare i report di successo.
3. Inserire un indirizzo e-mail in cui indirizzare i report dei guasti.

[]

Tecnici di livello 3

Account tecnici di livello 3 (alias *.TECH accounts*) sono account a livello di dominio che gli amministratori VDS devono utilizzare quando eseguono attività amministrative sulle macchine virtuali nell'ambiente VDS. È possibile creare account aggiuntivi in questa fase e/o in un secondo momento.

1. Immettere il nome utente e la password per gli account admin di livello 3. ".tech" verrà aggiunto al nome utente immesso per consentire la differenziazione tra utenti finali e account tecnici. Documentare queste credenziali per un utilizzo successivo.

La procedura consigliata consiste nel definire gli account denominati per tutti gli amministratori VDS che devono disporre di credenziali a livello di dominio per l'ambiente. Gli amministratori VDS che non dispongono di questo tipo di account possono comunque disporre dell'accesso admin a livello di macchina virtuale tramite la funzionalità *Connect to server* integrata in VDS.

[]

Domini

Active directory

Immettere il nome di dominio ad desiderato.

Di dominio pubblico

L'accesso esterno è protetto da un certificato SSL. Può essere personalizzato con il proprio dominio e un certificato SSL autogestiti. In alternativa, selezionando *Automatic*, VDS può gestire il certificato SSL, incluso un aggiornamento automatico del certificato di 90 giorni. Quando si utilizza la modalità automatica, ogni implementazione utilizza un sottodominio univoco di *cloudworkspace.app*.

[]

Macchine virtuali

Per le implementazioni RDS, i componenti richiesti, come domain controller, broker RDS e gateway RDS, devono essere installati sui server della piattaforma. In produzione, questi servizi devono essere eseguiti su macchine virtuali dedicate e ridondanti. Per le implementazioni proof of of concept, è possibile utilizzare una singola macchina virtuale per ospitare tutti questi servizi.

Configurazione delle macchine virtuali della piattaforma

Singola macchina virtuale

Questa è la scelta consigliata per le implementazioni POC. In un'implementazione di una singola macchina virtuale, i seguenti ruoli sono tutti ospitati su una singola macchina virtuale:

- Gestore CW
- Gateway HTML5
- Gateway RDS
- Applicazione remota
- Server FTPS (opzionale)
- Controller di dominio

Il numero massimo di utenti consigliato per i casi di utilizzo RDS in questa configurazione è di 100 utenti. I gateway RDS/HTML5 con bilanciamento del carico non sono un'opzione in questa configurazione, limitando la ridondanza e le opzioni per aumentare la scalabilità in futuro.

Se questo ambiente è progettato per la multi-tenancy, la configurazione di una singola macchina virtuale non è supportata.

Server multipli

Quando si suddivide la piattaforma VDS in più macchine virtuali, i seguenti ruoli vengono ospitati su macchine virtuali dedicate:

- Remote Desktop Gateway

  VDS Setup può essere utilizzato per implementare e configurare uno o due gateway RDS. Questi gateway ritrasmettono la sessione utente RDS da Internet aperta alle macchine virtuali host della sessione all'interno dell'implementazione. I gateway RDS gestiscono una funzione importante, proteggendo RDS dagli attacchi diretti da Internet aperto e crittografando tutto il traffico RDS in entrata e in uscita dall'ambiente. Quando vengono selezionati due Remote Desktop Gateway, VDS Setup implementa 2 VM e le configura in modo da bilanciare il carico delle sessioni utente RDS in entrata.

- Gateway HTML5

  VDS Setup può essere utilizzato per implementare e configurare uno o due gateway HTML5. Questi gateway ospitano i servizi HTML5 utilizzati dalla funzione *Connect to Server* in VDS e dal client VDS basato su Web (H5 Portal). Quando vengono selezionati due portali HTML5, VDS Setup implementa 2 VM e le configura in modo da bilanciare il carico delle sessioni utente HTML5 in entrata.

  

  Quando si utilizza un'opzione con più server (anche se gli utenti si connettono solo tramite il client VDS installato), si consiglia di utilizzare almeno un gateway HTML5 per abilitare la funzionalità *Connect to Server* da VDS.

- Note sulla scalabilità del gateway

  Per i casi di utilizzo RDS, è possibile scalare le dimensioni massime dell'ambiente con macchine virtuali gateway aggiuntive, con ciascun gateway RDS o HTML5 che supporta circa 500 utenti. È possibile aggiungere altri gateway in un secondo momento con un'assistenza dei servizi professionali NetApp minima

Se questo ambiente è progettato per la multi-tenancy, è necessaria la selezione di *server multipli*.

Ruoli del servizio

- Cwmgr1

  Questa macchina virtuale è la macchina virtuale amministrativa NetApp VDS. Esegue il database SQL Express, le utility di supporto e altri servizi amministrativi. In un'implementazione di *server singolo*, questa macchina virtuale può ospitare anche gli altri servizi, ma in una configurazione di *server multipli* tali servizi vengono spostati in macchine virtuali diverse.

- CWPortal1(2)

  Il primo gateway HTML5 è denominato *CWPortal1*, il secondo è *CWPortal2*. È possibile creare uno o due elementi al momento dell'implementazione. È possibile aggiungere server aggiuntivi dopo l'implementazione per aumentare la capacità (~500 connessioni per server).

- CWRDSGateway1(2)

  Il primo gateway RDS è denominato *CWRDSGateway1*, il secondo è *CWRDSGateway2*. È possibile creare uno o due elementi al momento dell'implementazione. È possibile aggiungere server aggiuntivi dopo l'implementazione per aumentare la capacità (~500 connessioni per server).

- Applicazione remota

  App Service è una raccolta dedicata per l'hosting delle applicazioni RemotApp, ma utilizza i gateway RDS e i relativi ruoli RDWeb per l'instradamento delle richieste di sessione dell'utente finale e l'hosting dell'elenco di abbonamento dell'applicazione RDWeb. Nessuna vm dedicata viene implementata per questo ruolo di servizio.

- Controller di dominio

  Al momento dell'implementazione, è possibile creare e configurare automaticamente uno o due domain controller per il funzionamento con VDS.

[]

Sistema operativo

Selezionare il sistema operativo del server desiderato da implementare per i server della piattaforma.

Fuso orario

Selezionare il fuso orario desiderato. I server della piattaforma verranno configurati in base all'ora e i file di log rifletteranno questo fuso orario. La sessione dell'utente finale rifletterà comunque il proprio fuso orario, indipendentemente da questa impostazione.

Servizi aggiuntivi

FTP

VDS può installare e configurare Filezilla in modo che venga eseguito un server FTPS per lo spostamento dei dati all'interno e all'esterno dell'ambiente. Si tratta di una tecnologia meno recente e si consigliano metodi di trasferimento dei dati più moderni (come Google Drive).

[]

Rete

Si consiglia di isolare le macchine virtuali in sottoreti diverse in base al loro scopo.

Definire l'ambito di rete e aggiungere un intervallo /20.

VDS Setup rileva e suggerisce un intervallo che dovrebbe avere successo. In base alle Best practice, gli indirizzi IP della subnet devono rientrare in un intervallo di indirizzi IP privati.

Questi intervalli sono:

- da 192.168.0.0 a 192.168.255.255
- da 172.16.0.0 a 172.31.255.255
- da 10.0.0.0 a 10.255.255.255

Esaminare e regolare se necessario, quindi fare clic su Validate (convalida) per identificare le subnet per ciascuna delle seguenti opzioni:

- Tenant (tenant): Intervallo di residenza dei server host di sessione e dei server di database

- Servizi: Questa è la gamma in cui risiedono i servizi PaaS come Cloud Volumes Service
- Platform (piattaforma): Intervallo in cui risiedono i server della piattaforma
- Directory (Directory): Intervallo in cui risiedono i server ad

[]

Licensing

N. SPLA

Inserire il numero SPLA in modo che VDS possa configurare il servizio di licenza RDS per semplificare la creazione di report SPLA RDS CAL. È possibile inserire un numero temporaneo (ad esempio 12345) per un'implementazione POC, ma dopo un periodo di prova (~120 giorni) le sessioni RDS smetteranno di connettersi.

Prodotti SPLA

Inserire i codici di licenza MAK per qualsiasi prodotto Office concesso in licenza tramite SPLA per consentire la creazione di report SPLA semplificati dall'interno dei report VDS.

ThinPrint

Scegliere di installare il server di licenza e la licenza ThinPrint inclusi per semplificare il reindirizzamento della stampante per l'utente finale.

[]

Revisione e provisioning

Una volta completate tutte le fasi, esaminare le selezioni, quindi convalidare e fornire l'ambiente.[]

Passi successivi

Il processo di automazione dell'implementazione ora implementerà un nuovo ambiente RDS con le opzioni selezionate durante la procedura guidata di implementazione.

Riceverai più e-mail al termine dell'implementazione. Una volta completato, avrai un ambiente pronto per il tuo primo spazio di lavoro. Un'area di lavoro conterrà gli host di sessione e i server di dati necessari per supportare gli utenti finali. Torna a questa guida per seguire i passaggi successivi una volta completata l'automazione dell'implementazione in 1-2 ore.

Creare una nuova raccolta di provisioning

Il provisioning delle raccolte è una funzionalità in VDS che consente la creazione, la personalizzazione e SysPrep delle immagini delle macchine virtuali. Una volta entrati nell'implementazione dell'ambiente di lavoro, è necessaria un'immagine da implementare e i seguenti passaggi ti guideranno nella creazione di un'immagine della macchina virtuale.

Per creare un'immagine di base per l'implementazione, procedere come segue:

1. Accedere a *Deployments* > *Provisioning Collections* e fare clic su *Add*

   []

2. Immettere un Nome e una Descrizione. Scegliere *Type: Shared*.

> È possibile scegliere Shared (condivisa) o VDI. Shared supporterà un server di sessione e (facoltativamente) un server di business per applicazioni come un database. VDI è una singola immagine VM per le macchine virtuali che sarà dedicata ai singoli utenti.

3. Fare clic su *Add* per definire il tipo di immagine del server da creare.

   []

4. Selezionare TSData come *ruolo server*, l'immagine VM appropriata (in questo caso Server 2016) e il tipo di storage desiderato. Fare clic su *Aggiungi server*

   []

5. Se si desidera, selezionare le applicazioni che verranno installate su questa immagine.
   a. L'elenco delle applicazioni disponibili viene compilato dalla libreria delle applicazioni a cui è possibile accedere facendo clic sul menu admin name (Nome amministratore) nell'angolo in alto a destra, sotto la pagina *Settings > App Catalog*.

      []

6. Fare clic su *Add Collection* e attendere la creazione della VM. VDS costruirà una macchina virtuale accessibile e personalizzabile.
7. Una volta completata la creazione della macchina virtuale, connettersi al server e apportare le modifiche desiderate.
   a. Una volta visualizzato lo stato *Collection Validation*, fare clic sul nome della raccolta.

      []

   b. Quindi, fare clic sul *nome modello server*

      []

   c. Infine, fare clic sul pulsante *Connetti al server* per connettersi e accedere automaticamente alla macchina virtuale con le credenziali di amministratore locale.

      []

   []

8. Una volta completate tutte le personalizzazioni, fare clic su *Validate Collection* in modo che VDS possa eseguire la sysprep e finalizzare l'immagine. Una volta completata l'operazione, la macchina virtuale verrà eliminata e l'immagine sarà disponibile per il modulo di implementazione nelle procedure guidate di implementazione VDS.

   []5

Creare un nuovo spazio di lavoro

Uno spazio di lavoro è un insieme di host di sessione e server di dati che supportano un gruppo di utenti. Un'implementazione può contenere un'area di lavoro singola (tenant singolo) o più aree di lavoro (multi-tenant).

Le aree di lavoro definiscono la raccolta di server RDS per un gruppo specifico. In questo esempio, implementeremo una singola raccolta per dimostrare la funzionalità del desktop virtuale. Tuttavia, il modello può essere esteso a più aree di lavoro/raccolte RDS per supportare gruppi diversi e posizioni diverse all'interno dello stesso spazio di dominio di Active Directory. Facoltativamente, gli amministratori possono limitare l'accesso tra le aree di lavoro/raccolte per supportare i casi di utilizzo che richiedono un accesso limitato alle applicazioni e ai dati.

Client e impostazioni

1. In NetApp VDS, accedere a *Workspaces* e fare clic su + *New Workspace*

   []

2. Fare clic su *Add* per creare un nuovo client. I dettagli del cliente in genere rappresentano le informazioni aziendali o le informazioni relative a un'ubicazione/reparto specifico.

   []

   a. Inserire i dettagli dell'azienda e selezionare l'implementazione in cui verrà implementato questo spazio di lavoro.
   b. **Unità dati:** definire la lettera dell'unità da utilizzare per l'unità condivisa mappata dell'azienda.
   c. **User Home Drive:** definisce la lettera del disco da utilizzare per il disco mappato dell'utente.
   d. **Impostazioni aggiuntive**

      Le seguenti impostazioni possono essere definite al momento dell'implementazione e/o selezionate dopo l'implementazione.

      i. *Enable Remote App:* l'applicazione Remote presenta le applicazioni come applicazioni di streaming invece di (o in aggiunta) presentare una sessione desktop remota completa.
      ii. *Enable App Locker:* VDS contiene la funzionalità di implementazione e autorizzazione delle applicazioni, per impostazione predefinita il sistema mostra/nasconde le applicazioni agli utenti finali. L'abilitazione di App Locker impone l'accesso alle applicazioni tramite un safelist GPO.
      iii. *Enable Workspace User Data Storage:* determinare se gli utenti finali hanno la necessità di avere accesso allo storage dei dati nel proprio desktop virtuale. Per le implementazioni RDS, questa impostazione deve essere sempre selezionata per abilitare l'accesso ai dati per i profili utente.
      iv. *Disable Printer Access:* VDS può bloccare l'accesso alle stampanti locali.
      v. *Permit Access to Task Manager:* VDS può abilitare/disabilitare l'accesso dell'utente finale a Task Manager in Windows.
      vi. *Richiedi password utente complessa:* la richiesta di password complesse abilita le regole native per le password complesse di Windows Server. Disattiva inoltre lo sblocco automatico ritardato degli account utente bloccati. Pertanto, se attivato, l'intervento dell'amministratore è necessario quando gli utenti finali bloccano i propri account con più tentativi di password non riusciti.
      vii. *Enable MFA for All Users:* VDS include un servizio gratuito di email/SMS MFA che può essere utilizzato per proteggere l'accesso dell'utente finale e/o dell'account amministratore VDS. L'attivazione di questa opzione richiede a tutti gli utenti finali in questo spazio di lavoro di autenticare con MFA per accedere al proprio desktop e/o alle applicazioni.

Scegliere applicazioni

Selezionare la versione del sistema operativo Windows e la raccolta Provisioning creata in precedenza in questa guida.

A questo punto è possibile aggiungere altre applicazioni, ma per questo POC si tratteremo dei diritti dell'applicazione post-implementazione.

[]

Aggiungi utenti

Gli utenti possono essere aggiunti selezionando un gruppo di sicurezza ad esistente o singoli utenti. In questa guida POC aggiungeremo gli utenti dopo l'implementazione.

[]

Revisione e provisioning

Nella pagina finale, esaminare le opzioni scelte e fare clic su *Provision* per avviare la creazione automatica delle risorse RDS.

[]

Durante il processo di implementazione, i log vengono creati ed è possibile accedervi in *Cronologia attività* nella parte inferiore della pagina dei dettagli di implementazione. Accessibile da *VDS > Deployments > Deployment Name*

Passi successivi

Il processo di automazione dell'ambiente di lavoro ora implementerà nuove risorse RDS con le opzioni selezionate durante la procedura guidata di implementazione.

Una volta completato, è possibile seguire diversi flussi di lavoro comuni per personalizzare l'implementazione RDS tipica.

- "Aggiungi utenti"
- "Accesso dell'utente finale"
- "Diritti dell'applicazione"
- "Ottimizzazione dei costi"

Prerequisiti di Google Compute Platform (GCP) e VDS

Requisiti e note di GCP e VDS

Questo documento descrive gli elementi necessari per l'implementazione dei servizi di desktop remoto (RDS) utilizzando NetApp Virtual Desktop Service (VDS). La "lista di controllo rapido" fornisce un breve elenco dei componenti necessari e delle fasi di pre-implementazione da intraprendere per garantire un'implementazione efficiente. Il resto della guida fornisce maggiori dettagli per ciascun elemento, a seconda delle scelte di configurazione effettuate.

[larghezza=75%]

Checklist rapida

Requisiti GCP

- Tenant GCP
- Progetto GCP
- Account di servizio con ruolo di proprietario assegnato

Informazioni di pre-implementazione

- Determinare il numero totale di utenti
- Determinare la regione e la zona del GCP
- Determinare il tipo di Active Directory
- Determinare il tipo di storage
- Identificare l'immagine o i requisiti della VM host della sessione
- Valutare la configurazione di rete GCP e on-premise esistente

Requisiti dettagliati per l'implementazione di VDS

Requisiti di connessione per l'utente finale

I seguenti client di desktop remoto supportano RDS in GCP:

- "NetApp VDS Client per Windows"
  - Requisiti di sicurezza dell'url in uscita di NetApp VDS Client per Windows
    - api.cloudworkspace.com
    - vdsclient.app
    - api.vdsclient.app
    - bin.vdsclient.app
  - Funzionalità avanzate:
    - Wake on Demand di VDS
    - Client ThinPrint e lice nsing
    - Reimpostazione self-service della password
    - Negoziazione automatica degli indirizzi di server e gateway
    - Supporto completo per desktop e applicazioni in streaming
    - Branding personalizzato disponibile
    - Switch del programma di installazione per l'implementazione e la configurazione automatizzate
    - Strumenti integrati per la risoluzione dei problemi
- "Client Web NetApp VDS"
- "Client Microsoft RD"
  - Windows
  - MacOS
  - ISO
  - Android

- software e/o thin client di terze parti
    - Requisito: Supporto della configurazione del gateway RD

Layer di storage

In RDS implementato da VDS, la strategia di storage è progettata in modo che non risiedano dati utente/aziendali persistenti sulle macchine virtuali della sessione AVD. I dati persistenti per i profili utente, i file utente e le cartelle e i dati aziendali/applicativi sono ospitati su uno o più volumi di dati ospitati su un livello di dati indipendente.

FSLogix è una tecnologia di containerizzazione dei profili che risolve molti problemi relativi ai profili utente (come la crescita dei dati e gli accessi lenti) montando un container di profili utente (formato VHD o VHDX) sull'host della sessione all'inizializzazione della sessione.

Grazie a questa architettura è necessaria una funzione di storage dei dati. Questa funzione deve essere in grado di gestire il trasferimento dei dati richiesto ogni mattina/pomeriggio quando una parte significativa degli utenti effettua l'accesso/disconnessione contemporaneamente. Anche gli ambienti di medie dimensioni possono avere requisiti significativi di trasferimento dei dati. Le prestazioni del disco del layer di storage dei dati sono una delle principali variabili di performance dell'utente finale e occorre prestare particolare attenzione a dimensionare in modo appropriato le performance di questo storage, non solo la quantità di storage. In genere, il livello di storage deve essere dimensionato in modo da supportare 5-15 IOPS per utente.

Networking

Obbligatorio: un inventario di tutte le subnet di rete esistenti, incluse le subnet visibili al progetto GCP tramite una VPN. L'implementazione deve evitare la sovrapposizione delle subnet.

L'installazione guidata di VDS consente di definire l'ambito della rete nel caso in cui sia necessario o debba essere evitato un intervallo come parte dell'integrazione pianificata con le reti esistenti.

Determinare un intervallo IP per l'utente durante l'implementazione. In base alle Best practice, sono supportati solo gli indirizzi IP in un intervallo privato.

Le opzioni supportate includono i seguenti valori, ma il valore predefinito è /20:

- da 192.168.0.0 a 192.168.255.255
- da 172.16.0.0 a 172.31.255.255
- da 10.0.0.0 a 10.255.255.255

CWMGR1

Alcune delle funzionalità esclusive di VDS, come la pianificazione del carico di lavoro per il risparmio dei costi e la funzionalità Live Scaling, richiedono una presenza amministrativa all'interno dell'organizzazione e del progetto. Pertanto, una macchina virtuale amministrativa denominata CWMGR1 viene implementata come parte dell'automazione della procedura guidata di installazione VDS. Oltre alle attività di automazione VDS, questa macchina virtuale contiene anche la configurazione VDS in un database SQL Express, file di log locali e un'utility di configurazione avanzata chiamata DCConfig.

A seconda delle selezioni effettuate nell'installazione guidata VDS, questa macchina virtuale può essere utilizzata per ospitare funzionalità aggiuntive, tra cui:

- Un gateway RDS
- Un gateway HTML 5
- Un server di licenza RDS

- Un controller di dominio

Albero decisionale nella procedura guidata di implementazione

Nell'ambito dell'implementazione iniziale, viene fornita una serie di domande per personalizzare le impostazioni del nuovo ambiente. Di seguito è riportata una descrizione delle principali decisioni da prendere.

Regione GCP

Decidere quale regione o quali regioni GCP ospiteranno le macchine virtuali VDS. Si noti che la regione deve essere selezionata in base alla vicinanza agli utenti finali e ai servizi disponibili.

Storage dei dati

Decidere dove collocare i dati per i profili utente, i singoli file e le condivisioni aziendali. Le scelte includono:

- Cloud Volumes Service per GCP
- File server tradizionale

Requisiti di implementazione di NetApp VDS per i componenti esistenti

Implementazione di NetApp VDS con i controller di dominio Active Directory esistenti

Questo tipo di configurazione estende un dominio Active Directory esistente per supportare l'istanza RDS. In questo caso, VDS implementa un set limitato di componenti nel dominio per supportare attività di provisioning e gestione automatizzate per i componenti RDS.

Questa configurazione richiede:

- Un controller di dominio Active Directory esistente a cui possono accedere le macchine virtuali sulla rete VPC GCP, in genere tramite VPN o un controller di dominio creato in GCP.
- Aggiunta di componenti VDS e autorizzazioni necessarie per la gestione VDS degli host RDS e dei volumi di dati quando vengono Uniti al dominio. Il processo di implementazione richiede che un utente di dominio con privilegi di dominio esegua lo script che creerà gli elementi necessari.
- Si noti che l'implementazione VDS crea una rete VPC per impostazione predefinita per le VM create da VDS. È possibile eseguire il peering della rete VPC con le reti VPC esistenti oppure spostare la macchina virtuale CWMGR1 in una rete VPC esistente con le subnet richieste predefinite.

Tool per la preparazione delle credenziali e dei domini

Gli amministratori devono fornire una credenziale Domain Administrator a un certo punto del processo di implementazione. È possibile creare, utilizzare ed eliminare una credenziale temporanea di Domain Administrator in un secondo momento (una volta completato il processo di implementazione). In alternativa, i clienti che necessitano di assistenza per la creazione dei prerequisiti possono sfruttare il Domain Preparation Tool.

Implementazione di NetApp VDS con file system esistente

VDS crea condivisioni Windows che consentono di accedere al profilo utente, alle cartelle personali e ai dati aziendali dagli host di sessione RDS. VDS implementerà il file server per impostazione predefinita, ma se si dispone di un componente di file storage esistente, VDS può puntare le condivisioni a tale componente una volta completata l'implementazione di VDS.

I requisiti per l'utilizzo e il componente di storage esistente:

- Il componente deve supportare SMB v3
- Il componente deve essere Unito allo stesso dominio Active Directory degli host di sessione RDS
- Il componente deve essere in grado di esporre un percorso UNC per l'utilizzo nella configurazione VDS: È possibile utilizzare un percorso per tutte e tre le condivisioni oppure specificare percorsi separati per ciascuna. Tenere presente che VDS imposterà le autorizzazioni a livello di utente per queste condivisioni, assicurandosi che siano state concesse le autorizzazioni appropriate ai VDS Automation Services.

APPENDICE A: URL del piano di controllo VDS e indirizzi IP

I componenti VDS del progetto GCP comunicano con i componenti del piano di controllo globale VDS ospitati in Azure, tra cui l'applicazione Web VDS e gli endpoint API VDS. Per l'accesso, è necessario mettere in sicurezza i seguenti indirizzi URI di base per l'accesso bidirezionale sulla porta 443:

"" "" "" ""

Se il dispositivo di controllo degli accessi può elencare solo in base all'indirizzo IP, è necessario che il seguente elenco di indirizzi IP sia protetto. Si noti che VDS utilizza un bilanciamento del carico con indirizzi IP pubblici ridondanti, pertanto questo elenco potrebbe cambiare nel tempo:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239 52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

Fattori di performance ottimali

Per ottenere prestazioni ottimali, assicurarsi che la rete soddisfi i seguenti requisiti:

- La latenza di andata e ritorno (RTT) dalla rete del client alla regione GCP in cui sono stati implementati gli host di sessione deve essere inferiore a 150 ms.
- Il traffico di rete può fluire al di fuori dei confini del paese/regione quando le macchine virtuali che ospitano desktop e applicazioni si connettono al servizio di gestione.
- Per ottimizzare le performance di rete, si consiglia di allocare le VM dell'host di sessione nella stessa regione del servizio di gestione.

Immagini del sistema operativo delle macchine virtuali supportate

Gli hsot di sessione RDS, implementati da VDS, supportano le seguenti immagini del sistema operativo x64:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Informazioni sul copyright

Informazioni sul marchio commerciale