Déploiement avec VDS

Virtual Desktop Service

NetApp
November 18, 2022

This PDF was generated from https://docs.netapp.com/fr-fr/virtual-desktop-service/Deploying.Azure.AVD.Deploying_AVD_in_Azure.html on November 18, 2022. Always check docs.netapp.com for the latest.

Table des matières

Déploiement avec VDS

Azure

Azure Virtual Desktop

Guide de déploiement AVD

Présentation

Ce guide fournit des instructions détaillées pour créer un déploiement Azure Virtual Desktop (AVD) à l'aide de NetApp Virtual Desktop Service (VDS) dans Azure.

Le guide commence à : https://cwasetup.cloudworkspace.com/

Ce guide de démonstration de faisabilité (POC) est conçu pour vous aider à déployer et configurer rapidement AVD dans votre propre abonnement Azure test. Ce guide suppose un déploiement sur site vert dans un locataire Azure Active Directory propre et non productif.

Les déploiements de production, en particulier dans les environnements AD ou Azure AD existants, sont très fréquents, mais ce processus n'est pas pris en compte dans ce guide de démonstration de faisabilité. Les démonstrations de faisabilité et les déploiements de production complexes doivent être lancées avec les équipes commerciales/services VDS NetApp et ne sont pas exécutées en libre-service.

Ce document POC vous fera découvrir l'ensemble du déploiement AVD et présente brièvement les principaux domaines de la configuration post-déploiement disponible sur la plate-forme VDS. Une fois l'opération terminée, vous aurez un environnement AVD entièrement déployé et fonctionnel, avec des pools d'hôtes, des groupes d'applications et des utilisateurs. Vous aurez également la possibilité de configurer la distribution automatisée des applications, les groupes de sécurité, les autorisations de partage de fichiers, Azure Cloud Backup, l'optimisation intelligente des coûts. VDS déploie un ensemble de paramètres des meilleures pratiques via GPO. Des instructions sur la désactivation facultative de ces contrôles sont également incluses, dans le cas où votre POC ne nécessite aucun contrôle de sécurité, similaire à un environnement de périphériques locaux non gérés.

Principes de base de l'AVD

Azure Virtual Desktop est un poste de travail complet et un service de virtualisation des applications qui s'exécute dans le cloud. Voici une liste rapide de certaines fonctionnalités clés :

- Services de plateforme incluant des passerelles, des courtage, des licences et des connexions, et inclus en tant que service de Microsoft. Cette infrastructure réduite requiert des solutions d'hébergement et de gestion.
- Azure Active Directory peut être utilisé comme fournisseur d'identités, ce qui permet de superposer des services de sécurité Azure supplémentaires tels que l'accès conditionnel.
- Les utilisateurs bénéficient d'une seule expérience de connexion pour les services Microsoft.
- Les sessions utilisateur se connectent à l'hôte de session via une technologie propriétaire de connexion inverse. Cela signifie qu'aucun port entrant ne doit être ouvert, au lieu de cela, un agent crée une connexion sortante au plan de gestion AVD qui, à son tour, se connecte au périphérique de l'utilisateur final.
- La connexion inverse permet même à l'exécution des machines virtuelles sans être exposées à Internet public, ce qui permet d'isoler les charges de travail, même tout en maintenant la connectivité à distance.

- AVD inclut l'accès à Windows 10 Multi-session, permettant une expérience Windows 10 Enterprise avec l'efficacité des sessions utilisateur haute densité.
- La technologie de conteneurisation des profils FSLogix inclut le développement des performances des sessions utilisateur, de l'efficacité du stockage et de l'expérience Office dans des environnements non persistants.
- AVD prend en charge l'accès complet au bureau et à l'application RemoteApp. Des expériences persistantes ou non persistantes, ainsi que des expériences dédiées et multi-sessions.
- Les entreprises peuvent réaliser des économies sur les licences Windows car AVD peut exploiter Windows 10 Enterprise E3 par utilisateur, ce qui remplace les licences CAL RDS et réduit considérablement le coût horaire des machines virtuelles hôtes de session dans Azure.

Portée du guide

Ce guide vous présente le déploiement d'AVD à l'aide de la technologie VDS NetApp du point de vue de l'administrateur Azure et VDS. Vous bénéficiez de l'abonnement et du locataire Azure sans préconfiguration. Ce guide vous aide à configurer AVD de bout en bout

Ce guide aborde les étapes suivantes :

1. Prerequisites,Vérifiez les prérequis du locataire Azure, de l'abonnement Azure et des autorisations de compte d'administrateur Azure
2. Discovery Details,Rassembler les informations requises pour la découverte
3. Setup Sections,Créez l'environnement Azure à l'aide de l'assistant d'installation VDS pour Azure spécialement conçu
4. AVD Host Pool,Créez le premier pool hôte avec une image Windows 10 EVD standard
5. VDS desktops to users,Attribution de postes de travail virtuels aux utilisateurs Azure AD
6. app group,Ajoutez des utilisateurs au groupe d'applications par défaut pour fournir l'environnement de bureau aux utilisateurs. En option, Additional AVD App Group(s),Créez un ou plusieurs pools d'hôtes supplémentaires pour la fourniture des services RemoteApp
7. User AVD Access,Connectez-vous en tant qu'utilisateur final via un logiciel client et/ou un client Web
8. connection options,Connectez-vous à la plate-forme et aux services client en tant qu'administrateur local et de domaine
9. Authentication (MFA),Activez en option l'authentification multi-facteurs VDS pour les administrateurs VDS et les utilisateurs finaux AVD
10. Entitlement Workflow,Vous pouvez également parcourir l'intégralité du workflow de droits d'application, y compris le remplissage de la bibliothèque d'applications, l'automatisation de l'installation des applications, le masquage des applications par les utilisateurs et les groupes de sécurité
11. AD Security Groups,Vous avez la possibilité de créer et de gérer des groupes de sécurité Active Directory, des autorisations de dossier et des droits d'application par groupe.
12. Cost Optimization Options,Vous pouvez également configurer des technologies d'optimisation des coûts, notamment la planification de la charge de travail et l'évolutivité dynamique
13. and Manage VM Images,Vous pouvez créer, mettre à jour et Sysprep une image de machine virtuelle pour les futurs déploiements
14. Azure Cloud Backup Service,Configurez en option Azure Cloud Backup
15. App Management/Policy Mode,Vous pouvez éventuellement désactiver les stratégies de groupe de contrôle de sécurité par défaut

Conditions préalables à Azure

VDS utilise le contexte de sécurité Azure natif pour déployer l'instance AVD. Avant de démarrer l'assistant de configuration VDS, il y a quelques prérequis Azure qui doivent être établis.

Lors du déploiement, les comptes de service et les autorisations sont accordés à VDS via l'authentification d'un compte d'administration existant à partir du locataire Azure.

Liste de contrôle des prérequis rapides

- Locataire Azure avec instance AD Azure (peut être une instance Microsoft 365)
- Abonnement Azure
- Il existe un quota Azure disponible pour les machines virtuelles Azure
- Compte d'administrateur Azure avec rôles de propriété d'administrateur global et d'abonnement

Les prérequis détaillés sont documentés le "Ce PDF"

Administrateur Azure dans Azure AD

Cet administrateur Azure existant doit être un compte Azure AD dans le locataire cible. Les comptes AD Windows Server peuvent être déployés avec la configuration VDS mais des étapes supplémentaires sont nécessaires à la configuration d'une synchronisation avec Azure AD (hors périmètre pour ce guide)

Ceci peut être confirmé en recherchant le compte utilisateur dans le portail de gestion Azure sous utilisateurs > tous les utilisateurs.[]

Rôle d'administrateur global

L'administrateur Azure doit se voir attribuer le rôle d'administrateur global dans le locataire Azure.

Pour vérifier votre rôle dans Azure AD, procédez comme suit :

1. Connectez-vous au portail Azure à l'adresse https://portal.azure.com/
2. Recherchez et sélectionnez Azure Active Directory
3. Dans le volet suivant à droite, cliquez sur l'option utilisateurs dans la section gérer
4. Cliquez sur le nom de l'utilisateur Administrateur que vous vérifiez
5. Cliquez sur rôle de répertoire. Dans le volet d'extrême droite, le rôle d'administrateur global doit être répertorié[]

Si cet utilisateur ne dispose pas du rôle d'administrateur global, vous pouvez effectuer les opérations suivantes pour l'ajouter (notez que le compte connecté doit être un administrateur global pour effectuer les opérations suivantes) :

1. Dans la page de détails sur le rôle de l'annuaire des utilisateurs de l'étape 5 ci-dessus, cliquez sur le bouton Ajouter une affectation en haut de la page de détails.
2. Cliquez sur Administrateur global dans la liste des rôles. Cliquez sur le bouton Ajouter.[]

Propriété de l'abonnement Azure

L'administrateur Azure doit également être propriétaire de l'abonnement qui contiendra le déploiement.

Pour vérifier que l'administrateur est un propriétaire de l'abonnement, procédez comme suit :

1. Connectez-vous au portail Azure à l'adresse https://portal.azure.com/
2. Recherchez et sélectionnez abonnements
3. Dans le volet suivant à droite, cliquez sur le nom de l'abonnement pour afficher les détails de l'abonnement
4. Cliquez sur l'option de menu contrôle d'accès (IAM) dans le volet secondaire à gauche
5. Cliquez sur l'onglet affectations de rôles. L'administrateur Azure doit être répertorié dans la section propriétaire.[]

Si l'administrateur Azure ne figure pas dans la liste, vous pouvez ajouter le compte en tant que propriétaire de l'abonnement en procédant comme suit :

1. Cliquez sur le bouton Ajouter en haut de la page et choisissez l'option Ajouter une affectation de rôle
2. Une boîte de dialogue apparaît à droite. Sélectionnez propriétaire dans la liste déroulante rôle, puis commencez à saisir le nom d'utilisateur de l'administrateur dans la zone Sélectionner. Lorsque le nom complet de l'administrateur s'affiche, sélectionnez-le
3. Cliquez sur le bouton Enregistrer en bas de la boîte de dialogue[]

Quota du cœur de calcul Azure

L'assistant de configuration CWA et le portail VDS créent de nouvelles machines virtuelles et l'abonnement Azure doit disposer d'un quota disponible pour s'exécuter correctement .

Pour vérifier les quotas, procédez comme suit :

1. Accédez au module abonnements et cliquez sur « utilisation + quotas ».
2. Sélectionnez tous les fournisseurs dans la liste déroulante "fournisseurs", sélectionnez "Microsoft.Compute" dans la liste déroulante "fournisseurs"
3. Sélectionnez la région cible dans la liste déroulante « emplacements »
4. Une liste des quotas disponibles par famille de machines virtuelles doit être affichée[]Si vous devez augmenter vos quotas, cliquez sur Request augmentez et suivez les invites pour ajouter de la capacité. Pour le déploiement initial, demander spécifiquement un devis plus élevé pour le « CPU virtuels de la famille DSv3 standard »

Collecte des informations de découverte

Après avoir travaillé avec l'assistant CWA Setup, plusieurs questions doivent être résolues. NetApp VDS a fourni un PDF lié qui peut être utilisé pour enregistrer ces sélections avant le déploiement. Voici les éléments suivants :

Élément	Description
Identifiants admin VDS	Collectez les informations d'identification administrateur VDS existantes si vous les avez déjà. Dans le cas contraire, un nouveau compte administrateur sera créé pendant le déploiement.
Région Azure	Déterminez la région Azure cible en fonction des performances et de la disponibilité des services. C'est ça "Outil Microsoft" permet d'estimer l'expérience utilisateur en fonction de sa région.
Type Active Directory	Les VM doivent se connecter à un domaine, mais ne peuvent pas rejoindre directement Azure AD. Le déploiement VDS peut créer une nouvelle machine virtuelle ou utiliser un contrôleur de domaine existant.

Élément	Description
Gestion de fichiers	Les performances dépendent fortement de la vitesse des disques, en particulier en ce qui concerne le stockage des profils d'utilisateurs. L'assistant d'installation VDS peut déployer un serveur de fichiers simple ou configurer Azure NetApp Files (ANF). Pour la quasi-totalité des environnements de production, ANF est recommandé. Cependant, pour un POC, l'option de serveur de fichiers offre des performances suffisantes. Les options de stockage peuvent être révisées après le déploiement, notamment l'utilisation des ressources de stockage existantes dans Azure. Consultez la page tarifaire d'ANF pour plus d'informations : https://azure.microsoft.com/en-us/pricing/details/netapp/
Portée du réseau virtuel	Une plage de réseau routable /20 est requise pour le déploiement. L'assistant de configuration VDS vous permettra de définir cette plage. Il est important que cette plage ne se chevauchent pas avec les systèmes vNets existants dans Azure ou sur site (si les deux réseaux sont connectés via un VPN ou ExpressRoute).

Sections de positionnement VDS

Connectez-vous à https://cwasetup.cloudworkspace.com/ Avec vos identifiants d'administrateur Azure trouvés dans la section conditions préalables.

IaaS et plateforme

[]

Nom du domaine Azure AD

Le nom de domaine Azure AD est hérité du locataire sélectionné.

Emplacement

Sélectionnez une région Azure ** appropriée. C'est ça "Outil Microsoft" permet d'estimer l'expérience utilisateur en fonction de sa région.

Type Active Directory

VDS peut être configurée avec une nouvelle machine virtuelle **pour la fonction ou la configuration du contrôleur de domaine afin de tirer parti d'un contrôleur de domaine existant. Dans ce guide, nous sélectionnerons Nouveau Windows Server Active Directory, qui créera une ou deux machines virtuelles (en fonction des choix effectués pendant ce processus) dans le cadre de l'abonnement.

Un article détaillé couvrant un déploiement AD existant est trouvé "ici".

Nom de domaine Active Directory

Saisissez un nom de domaine **. La mise en miroir du nom de domaine Azure AD de ci-dessus est recommandée.

Gestion de fichiers

VDS peut provisionner une machine virtuelle simple serveur de fichiers ou configurer Azure NetApp Files. En production, Microsoft recommande d'allouer 30 go par utilisateur et nous avons observé qu'il est nécessaire

d'allouer 5-15 IOPS par utilisateur pour des performances optimales.

Dans un environnement POC (non de production), le serveur de fichiers est une option de déploiement simple et économique. Cependant, les performances disponibles d'Azure Managed Disks peuvent être dépassées par la consommation d'IOPS, même lors d'un déploiement en production petit.

Par exemple, un disque SSD standard de 4 To dans Azure prend en charge jusqu'à 500 000 IOPS, ce qui ne pouvait prendre en charge que 100 utilisateurs au maximum à 5 000 IOPS/utilisateur. Avec ANF Premium, la même taille de stockage peut prendre en charge 16,000 000 IOPS et ainsi augmenter de 32 000 IOPS.

Pour les déploiements AVD en production, **Azure NetApp Files est la recommandation de Microsoft**.

> Vous devez mettre Azure NetApp Files à votre disposition pour l'abonnement que vous souhaitez déployer. Contactez votre ingénieur commercial NetApp ou utilisez le lien suivant : https://aka.ms/azurenetappfiles

Vous devez également enregistrer NetApp comme fournisseur dans votre abonnement. Pour ce faire, procédez comme suit :

- Accédez aux abonnements via le portail Azure
  - Cliquez sur fournisseurs de ressources
  - Filtre pour NetApp
  - Sélectionnez le fournisseur et cliquez sur Enregistrer

Numéro de licence RDS

Vous pouvez utiliser NetApp VDS pour déployer des environnements RDS et/ou AVD. Lors du déploiement d'AVD, ce champ peut **rester vide**.

RéplicationFine

Vous pouvez utiliser NetApp VDS pour déployer des environnements RDS et/ou AVD. Lors du déploiement d'AVD, cette bascule peut rester **désactivée** (bascule vers la gauche).

E-mail de notification

VDS enverra des notifications de déploiement et des rapports d'état de santé en cours au **e-mail fourni**. Ceci peut être modifié ultérieurement.

Les VM et le réseau

Il existe une variété de services devant être exécutés pour prendre en charge un environnement VDS ; ils sont collectivement appelés « plate-forme VDS ». Selon la configuration, ces passerelles peuvent inclure CWMGR, une ou deux passerelles RDS, une ou deux passerelles HTML5, un serveur FTPS et une ou deux VM Active Directory.

La plupart des déploiements AVD exploitent l'option de machine virtuelle unique, car Microsoft gère les passerelles AVD comme un service PaaS.

Pour les environnements plus petits et plus simples qui incluent les cas d'utilisation de RDS, tous ces services peuvent être condensés en option d'une machine virtuelle unique pour réduire les coûts des machines virtuelles (avec évolutivité limitée). Dans le cas d'utilisations RDS comptant plus de 100 utilisateurs, l'option de machines virtuelles multiples est conseillée pour faciliter l'évolutivité de la passerelle RDS et/ou HTML5[]

Configuration des machines virtuelles de la plateforme

Vous pouvez utiliser NetApp VDS pour déployer des environnements RDS et/ou AVD. Lors du déploiement d'AVD, il est recommandé de sélectionner une seule machine virtuelle. Dans le cas des déploiements RDS, vous devez déployer et gérer des composants supplémentaires, tels que Brokers et passerelles, en production, ces services doivent s'exécuter sur des machines virtuelles dédiées et redondantes. Pour AVD, tous ces services sont fournis par Azure en tant que service inclus et donc, la configuration **machine virtuelle unique** est recommandée.

Une seule machine virtuelle

Il s'agit de la sélection recommandée pour les déploiements qui utilisent exclusivement AVD (et non RDS ou une combinaison des deux). Dans un déploiement à une seule machine virtuelle, les rôles suivants sont tous hébergés sur une seule machine virtuelle dans Azure :

- Gestionnaire CW
- Passerelle HTML5
- Passerelle RDS
- Application distante
- Serveur FTPS (en option)
- Rôle de contrôleur de domaine

Dans cette configuration, le nombre maximal d'utilisateurs conseillé pour les cas d'utilisation de RDS est de 100 utilisateurs. Les passerelles RDS/HTML5 à équilibrage de charge ne sont pas une option proposée dans cette configuration, limitant ainsi la redondance et les options d'augmentation de l'évolutivité future. Encore une fois, cette limite ne s'applique pas aux déploiements AVD puisque Microsoft gère les passerelles comme un service PaaS.

Si cet environnement est conçu pour la colocation, la configuration d'une machine virtuelle unique n'est pas prise en charge, ni AVD ni AD Connect.

Plusieurs machines virtuelles

Lors de la répartition de la plateforme VDS en plusieurs machines virtuelles, les rôles suivants sont hébergés sur des machines virtuelles dédiées sur Azure :

- Passerelle Bureau à distance

  Le réglage VDS peut être utilisé pour déployer et configurer une ou deux passerelles RDS. Ces passerelles relaient la session utilisateur RDS depuis l'Internet ouvert vers les machines virtuelles hôte de session au sein du déploiement. Les passerelles RDS gèrent une fonction importante, protégeant ainsi RDS des attaques directes sur Internet et cryptant l'ensemble du trafic RDS dans/hors de l'environnement. Lorsque deux passerelles Remote Desktop sont sélectionnées, VDS Setup déploie 2 machines virtuelles et les configure pour équilibrer la charge des sessions utilisateur RDS entrantes.

- Passerelle HTML5

  L'installation VDS peut être utilisée pour déployer et configurer une ou deux passerelles HTML5. Ces passerelles hébergent les services HTML5 utilisés par la fonction *Connect to Server* dans VDS et le client VDS basé sur le Web (H5 Portal). Lorsque deux portails HTML5 sont sélectionnés, le programme d'installation VDS déploie 2 machines virtuelles et les configure pour équilibrer la charge des sessions utilisateur HTML5 entrantes.

Lors de l'utilisation de l'option de serveur multiple (même si les utilisateurs se connectent uniquement via le client VDS installé), il est fortement recommandé d'activer la fonctionnalité *Connect to Server* de VDS au moins une passerelle HTML5.

- Notes relatives à l'évolutivité des passerelles

  Dans le cas d'une solution RDS, la taille maximale de l'environnement peut être mise à l'échelle avec d'autres VM de passerelle, chaque passerelle RDS ou HTML5 prenant en charge environ 500 utilisateurs. Des passerelles supplémentaires peuvent être ajoutées ultérieurement avec une assistance minimale aux services professionnels NetApp

Si cet environnement est conçu pour la colocation, la sélection de plusieurs machines virtuelles est requise.

Fuseau horaire

Bien que l'expérience des utilisateurs finaux reflète leur fuseau horaire local, un fuseau horaire par défaut doit être sélectionné. Sélectionnez le fuseau horaire dans lequel la **administration principale** de l'environnement sera exécutée.

Portée du réseau virtuel

Il est recommandé d'isoler les machines virtuelles dans différents sous-réseaux en fonction de leur usage. Tout d'abord, définissez la portée du réseau et ajoutez une plage /20.

Le programme d'installation VDS détecte et suggère une plage qui devrait s'avérer efficace. Conformément aux bonnes pratiques, les adresses IP du sous-réseau doivent être comprises dans une plage d'adresses IP privées.

Ces plages sont :

- 192.168.0.0 à 192.168.255.255
- 172.16.0.0 à 172.31.255.255
- 10.0.0.0 à 10.255.255.255

Vérifiez et ajustez si nécessaire, puis cliquez sur Valider pour identifier les sous-réseaux pour chacun des éléments suivants :

- Tenant : il s'agit de la plage dans laquelle les serveurs hôtes de session et les serveurs de base de données résident
- Services : il s'agit de la gamme dans laquelle résideront les services PaaS comme Azure NetApp Files
- Plate-forme : il s'agit de la gamme dans laquelle les serveurs de plate-forme seront hébergés
- Répertoire : il s'agit de la plage dans laquelle les serveurs AD résident

Révision

La dernière page vous permet de passer en revue vos choix. Une fois l'évaluation terminée, cliquez sur le bouton Valider. Le programme d'installation VDS examinera toutes les entrées et vérifie que le déploiement peut continuer avec les informations fournies. Cette validation peut prendre 2-10 minutes. Pour suivre la progression, vous pouvez cliquer sur le logo du journal (en haut à droite) pour afficher l'activité de validation.

Une fois la validation terminée, le bouton vert d'approvisionnement s'affiche à la place du bouton Valider. Cliquez sur Provision pour lancer le processus de provisionnement de votre déploiement.

État

Le processus de provisionnement prend entre 2-4 heures en fonction de la charge de travail Azure et des choix que vous faites. Vous pouvez suivre la progression dans le journal en cliquant sur la page État ou attendre l'e-mail qui vous indiquera que le processus de déploiement est terminé. Le déploiement crée les machines virtuelles et les composants Azure nécessaires pour prendre en charge VDS et une implémentation Remote Desktop ou AVD. Il s'agit d'une seule machine virtuelle pouvant agir à la fois comme hôte de session Bureau à distance et serveur de fichiers. Dans une implémentation AVD, cette machine virtuelle agit uniquement comme un serveur de fichiers.

Installer et configurer AD Connect

Une fois l'installation réussie, AD Connect doit être installé et configuré sur le contrôleur de domaine. Dans une configuration VM de plate-forme unique, la machine CWMGR1 est le DC. Les utilisateurs d'AD doivent synchroniser entre Azure AD et le domaine local.

Pour installer et configurer AD Connect, procédez comme suit :

1. Connectez-vous au contrôleur de domaine en tant qu'administrateur de domaine.
    a. Obtention des informations d'identification à partir du coffre-fort de clés Azure (voir "Instructions clés du coffre-fort ici")
2. Installez AD Connect, connectez-vous avec l'administrateur de domaine (avec les autorisations de rôle d'administrateur d'entreprise) et l'administrateur global Azure AD.

Activation des services AVD

Une fois le déploiement terminé, l'étape suivante consiste à activer la fonctionnalité AVD. Le processus d'activation AVD exige que l'administrateur Azure effectue plusieurs étapes pour enregistrer son domaine Azure AD et son abonnement à l'aide des services AVD Azure. De même, Microsoft nécessite VDS pour demander les mêmes autorisations pour notre application d'automatisation dans Azure. Les étapes ci-dessous vous permettent de suivre ce processus.

Créer un pool hôte AVD

L'accès de l'utilisateur final aux machines virtuelles AVD est géré par des pools hôtes , qui contiennent les machines virtuelles et les groupes d'applications, qui contiennent à leur tour les utilisateurs et le type d'accès des utilisateurs.

Pour créer votre premier pool d'hôtes

1. Cliquez sur le bouton Ajouter dans la partie droite de l'en-tête de la section pools hôtes AVD.[]
2. Entrez un nom et une description pour votre pool d'hôtes.
3. Choisissez un type de pool d'hôtes
    a. **Pooled** signifie que plusieurs utilisateurs accèdent au même pool de machines virtuelles avec les mêmes applications installées.
    b. **Personal** crée un pool hôte dans lequel les utilisateurs sont affectés à leur propre VM hôte de session.
4. Sélectionnez le type Load Balancer
    a. **Depth First** remplit la première machine virtuelle partagée au nombre maximal d'utilisateurs avant de démarrer sur la seconde machine virtuelle du pool
    b. **Large First** distribuera les utilisateurs à toutes les machines virtuelles du pool en mode round-Robin
5. Sélectionnez un modèle de machines virtuelles Azure pour la création des machines virtuelles dans ce pool. Alors que VDS affichera tous les modèles disponibles dans l'abonnement, nous recommandons de

sélectionner la version multi-utilisateur Windows 10 la plus récente pour une expérience optimale. Le build actuel est Windows-10-20h1-evd. (Possibilité de créer une image Gold à l'aide de la fonctionnalité Provisioning Collection pour créer des hôtes à partir d'une image de machine virtuelle personnalisée)

6. Sélectionnez la taille de la machine Azure. Pour l'évaluation, NetApp recommande les séries D (type de machine standard pour multi-utilisateurs) ou E (configuration de mémoire optimisée pour les scénarios multi-utilisateurs plus lourds). La taille de la machine peut être modifiée ultérieurement dans VDS si vous souhaitez expérimenter avec différentes séries et tailles
7. Sélectionnez un type de stockage compatible pour les instances de disque géré des machines virtuelles dans la liste déroulante
8. Sélectionnez le nombre de machines virtuelles que vous souhaitez créer dans le cadre du processus de création du pool hôte. Vous pouvez ajouter des machines virtuelles au pool ultérieurement, mais VDS va générer le nombre de machines virtuelles que vous demandez et les ajouter au pool hôte une fois qu'il a été créé
9. Cliquez sur le bouton Ajouter un pool d'hôtes pour lancer le processus de création. Vous pouvez suivre la progression sur la page AVD ou consulter les détails du journal des processus sur la page déploiements/Nom du déploiement de la section tâches
10. Une fois le pool hôte créé, il apparaît dans la liste des pools hôtes de la page AVD. Cliquez sur le nom du pool d'hôtes pour afficher sa page de détails, qui comprend une liste de ses machines virtuelles , groupes d'applications et utilisateurs actifs

> Les hôtes AVD dans VDS sont créés avec un paramètre qui supprime la connexion des sessions utilisateur. Ceci est par conception pour permettre la personnalisation avant d'accepter les connexions utilisateur. Ce paramètre peut être modifié en modifiant les paramètres de l'hôte de session. []

Activer les bureaux VDS pour les utilisateurs

Comme indiqué ci-dessus, VDS crée tous les éléments nécessaires à la prise en charge des espaces de travail des utilisateurs finaux lors du déploiement. Une fois le déploiement terminé, l'étape suivante consiste à activer l'accès à l'espace de travail pour chaque utilisateur que vous souhaitez introduire dans l'environnement AVD. Cette étape permet de créer la configuration du profil et l'accès à la couche de données utilisateur final, c'est-à-dire l'accès par défaut pour un poste de travail virtuel. VDS réutilise cette configuration pour lier les utilisateurs finaux d'Azure AD aux pools d'applications AVD.

Pour activer les espaces de travail pour les utilisateurs finaux, procédez comme suit :

1. Connectez-vous à VDS at https://manage.cloudworkspace.com Utilisation du compte administrateur principal VDS que vous avez créé pendant le provisionnement. Si vous ne vous souvenez plus des informations de votre compte, contactez NetApp VDS pour obtenir de l'aide lors de leur récupération
2. Cliquez sur l'élément de menu espaces de travail, puis cliquez sur le nom de l'espace de travail créé automatiquement lors du provisionnement
3. Cliquez sur l'onglet utilisateurs et groupes[]
4. Pour chaque utilisateur que vous souhaitez activer, faites défiler le nom d'utilisateur et cliquez sur l'icône engrenage
5. Choisissez l'option "Activer le Cloud Workspace"[]
6. Le processus d'accompagnement prend environ 30-90 secondes. Notez que l'état de l'utilisateur passe de en attente à disponible

L'activation d'Azure AD Domain Services crée un domaine géré dans Azure, et chaque machine virtuelle AVD créée sera associée à ce domaine. Pour que la connexion classique aux machines virtuelles fonctionne, le hachage du mot de passe pour les utilisateurs d'Azure AD doit être synchronisé afin de prendre en charge l'authentification NTLM et Kerberos. La façon la plus simple d'effectuer cette tâche est de modifier le mot de passe de l'utilisateur dans Office.com ou sur le portail Azure, ce qui force la synchronisation du hachage de mot de passe à se produire. Le cycle de synchronisation des serveurs de service de domaine peut prendre jusqu'à 20 minutes.

Activer les sessions utilisateur

Par défaut, les hôtes de session ne peuvent pas accepter les connexions utilisateur. Ce paramètre est généralement appelé « mode vidange » car il peut être utilisé en production pour empêcher les nouvelles sessions utilisateur, permettant ainsi à l'hôte de supprimer toutes les sessions utilisateur. Lorsque de nouvelles sessions utilisateur sont autorisées sur un hôte, cette action est communément appelée « rotation » de l'hôte de session.

En production, il est judicieux de démarrer de nouveaux hôtes en mode vidange, car des tâches de configuration doivent généralement être effectuées avant que l'hôte ne soit prêt pour les charges de travail de production.

Lors du test et de l'évaluation, vous pouvez immédiatement retirer les hôtes du mode de vidange pour permettre aux utilisateurs de se connecter et confirmer leur fonctionnalité. .Pour activer les sessions utilisateur sur le ou les hôtes de session, procédez comme suit :

1. Accédez à la section AVD de la page de l'espace de travail.
2. Cliquez sur le nom du pool d'hôtes sous "pools d'hôtes AVD".[]
3. Cliquez sur le nom du ou des hôtes de session et cochez la case Autoriser les nouvelles sessions, cliquez sur mettre à jour l'hôte de session. Répétez l'opération pour tous les hôtes qui doivent être placés en rotation.[]
4. Les statistiques actuelles de « Autoriser une nouvelle session » sont également affichées sur la page AVD principale pour chaque élément de ligne hôte.

Groupe d'applications par défaut

Notez que le groupe d'applications de bureau est créé par défaut dans le cadre du processus de création du pool d'hôtes. Ce groupe fournit un accès interactif au bureau à tous les membres du groupe. .Pour ajouter des membres au groupe :

1. Cliquez sur le nom du groupe d'applications[]
2. Cliquez sur le lien indiquant le nombre d'utilisateurs ajoutés[]
3. Sélectionnez les utilisateurs que vous souhaitez ajouter au groupe d'applications en cochant la case en regard de leur nom
4. Cliquez sur le bouton Sélectionner utilisateurs
5. Cliquez sur le bouton mettre à jour le groupe d'applications

Créer des groupes d'applications AVD supplémentaires

Des groupes d'applications supplémentaires peuvent être ajoutés au pool hôte. Ces groupes d'applications publient des applications spécifiques à partir des machines virtuelles du pool hôte vers les utilisateurs du groupe d'applications à l'aide de RemoteApp.

AVD ne permet d'attribuer aux utilisateurs finaux qu'au type de groupe d'applications de bureau ou au type de groupe d'applications RemoteApp, mais pas aux deux dans le même pool d'hôtes. Veillez donc à isoler les utilisateurs en conséquence. Si les utilisateurs ont besoin d'accéder à un poste de travail et à des applications de diffusion en continu, un second pool hôte est nécessaire pour héberger les applications.

Pour créer un nouveau groupe d'applications :

1. Cliquez sur le bouton Ajouter dans l'en-tête de la section groupes d'applications[]
2. Entrez un nom et une description pour le groupe d'applications
3. Sélectionnez les utilisateurs à ajouter au groupe en cliquant sur le lien Ajouter des utilisateurs. Sélectionnez chaque utilisateur en cochant la case en regard de son nom, puis cliquez sur le bouton Sélectionner utilisateurs[]
4. Cliquez sur le lien Ajouter RemoteApps pour ajouter des applications à ce groupe d'applications. AVD génère automatiquement la liste des applications possibles en analysant la liste des applications installées sur la machine virtuelle . Sélectionnez l'application en cochant la case en regard du nom de l'application, puis cliquez sur le bouton Sélectionner les applications RemoteApps.[]
5. Cliquez sur le bouton Ajouter un groupe d'applications pour créer le groupe d'applications

Accès AVD de l'utilisateur final

Les utilisateurs finaux peuvent accéder aux environnements AVD à l'aide du client Web ou d'un client installé sur différentes plates-formes

- Client Web : https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web
- URL de connexion au client Web : http://aka.ms/AVDweb
- Client Windows : https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10
- Android client : https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android
- Mac OS client : https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos
- Client iOS : https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios
- Client léger IGEL : https://www.igel.com/igel-solution-family/windows-virtual-desktop/

Connectez-vous à l'aide du nom d'utilisateur et du mot de passe. Notez que Remote App and Desktop Connections (RADC), Remote Desktop Connection (msc) et l'application CloudWorksapce client pour Windows ne prennent actuellement pas en charge la possibilité de se connecter aux instances AVD.

Surveiller les connexions des utilisateurs

La page de détails du pool d'hôtes affiche également une liste des utilisateurs actifs lorsqu'ils se connectent à une session AVD.

Options de connexion Admin

Les administrateurs VDS peuvent se connecter aux machines virtuelles de l'environnement de différentes manières.

Connectez-vous au serveur

Dans tout le portail, les administrateurs VDS trouveront l'option « connexion au serveur ». Par défaut, cette fonction connecte l'administrateur à la machine virtuelle en générant dynamiquement des informations

d'identification d'administrateur local et en les injectant dans une connexion client Web. L'administrateur n'a pas besoin de connaître (et n'est jamais fourni) les informations d'identification pour se connecter.

Ce comportement par défaut peut être désactivé par administrateur, comme décrit dans la section suivante.

Comptes d'administration .tech/niveau 3

Un compte admin de "niveau III" est créé dans le processus d'installation de CWA. Le nom d'utilisateur est formaté en username.tech@domain.xyz

Ces comptes, communément appelés comptes «.tech », sont nommés comptes d'administrateur au niveau du domaine. Les administrateurs VDS peuvent utiliser leur compte .tech lors de la connexion à un serveur CWMGR1 (plate-forme) et éventuellement lors de la connexion à toutes les autres machines virtuelles de l'environnement.

Pour désactiver la fonction de connexion automatique d'administrateur local et forcer l'utilisation du compte de niveau III, modifiez ce paramètre. Accédez à VDS > Admins > Nom d'administrateur > cochez « compte technique activé ». Lorsque cette case est cochée, l'administrateur VDS ne sera pas automatiquement connecté aux machines virtuelles en tant qu'administrateur local et sera plutôt invité à entrer leurs informations d'identification .tech.

Ces informations d'identification, ainsi que d'autres informations d'identification pertinentes, sont automatiquement stockées dans le *Azure Key Vault* et sont accessibles depuis le portail de gestion Azure à l'adresse https://portal.azure.com/.

Actions facultatives post-déploiement

Authentification multifacteur (MFA)

VDS NetApp incluant gratuitement des SMS/e-mails MFA. Cette fonction peut être utilisée pour sécuriser les comptes administrateur VDS et/ou les comptes utilisateur final."Article MFA"

Workflow du droit aux applications

VDS fournit un mécanisme permettant d'affecter aux utilisateurs finaux l'accès aux applications à partir d'une liste prédéfinie d'applications appelée catalogue d'applications. Le catalogue des applications couvre tous les déploiements gérés.

> Le serveur TSD1 automatiquement déployé doit rester en l'état pour prendre en charge les droits d'application. Plus précisément, n'exécutez pas la fonction "convertir en données" sur cette machine virtuelle.

La gestion des applications est détaillée dans cet article : ""

Groupes de sécurité Azure AD

VDS inclut la fonctionnalité permettant de créer, de remplir et de supprimer des groupes d'utilisateurs qui sont sauvegardés par les groupes de sécurité Azure AD. Ces groupes peuvent être utilisés en dehors de VDS comme tout autre groupe de sécurité. Dans VDS, ces groupes peuvent être utilisés pour attribuer des autorisations de dossier et des droits d'application.

Créer des groupes d'utilisateurs

La création de groupes d'utilisateurs s'effectue dans l'onglet utilisateurs et groupes d'un espace de travail.

Attribuez des autorisations de dossier par groupe

Les autorisations d'affichage et de modification des dossiers dans le partage d'entreprise peuvent être attribuées à des utilisateurs ou à des groupes.

""

Affecter des applications par groupe

Outre l'affectation individuelle d'applications à des utilisateurs, les applications peuvent être provisionnées à des groupes.

1. Accédez au détail des utilisateurs et des groupes.[]
2. Ajouter un nouveau groupe ou modifier un groupe existant.[]
3. Attribuez un ou plusieurs utilisateurs et applications au groupe.[]

Configurez les options d'optimisation des coûts

La gestion de l'espace de travail s'étend également à la gestion des ressources Azure qui prennent en charge l'implémentation AVD. VDS vous permet de configurer à la fois les plannings de charge de travail et Live Scaling afin d'activer et de désactiver les machines virtuelles Azure en fonction des activités des utilisateurs finaux. Ces fonctionnalités permettent d'associer l'utilisation des ressources Azure et la dépense au modèle d'utilisation réel des utilisateurs finaux. En outre, si vous avez configuré une mise en œuvre AVD Proof of concept, vous pouvez faire pivoter le déploiement complet à partir de l'interface VDS.

Planification des charges de travail

La planification des charges de travail est une fonctionnalité qui permet à l'administrateur de créer un programme défini pour les machines virtuelles Workspace à utiliser pour prendre en charge les sessions utilisateur. Lorsque la fin de la période programmée est atteinte pour un jour donné de la semaine, VDS arrête/déalloue les machines virtuelles dans Azure afin que les frais horaires cessent.

Pour activer la planification de la charge de travail :

1. Connectez-vous à VDS at https://manage.cloudworkspace.com Utilisation de vos identifiants VDS.
2. Cliquez sur l'élément de menu espace de travail, puis cliquez sur le nom de l'espace de travail dans la liste. []
3. Cliquez sur l'onglet planification de la charge de travail. []
4. Cliquez sur le lien gérer dans l'en-tête planification de la charge de travail. []
5. Choisissez un état par défaut dans le menu déroulant État : toujours activé (par défaut), toujours désactivé ou planifié.
6. Si vous choisissez programmé, les options de planification sont les suivantes :
    a. Exécuter à l'intervalle assigné tous les jours. Cette option définit l'horaire comme étant la même heure de début et de fin pour les sept jours de la semaine. []
    b. Exécuter à l'intervalle attribué pour les jours spécifiés. Cette option définit l'horaire sur la même période de début et de fin que pour certains jours de la semaine. Les jours non sélectionnés de la semaine ne permettent pas à VDS de mettre les machines virtuelles sous tension pendant ces jours. []
    c. Exécuter à des intervalles de temps et des jours variables. Cette option définit l'horaire sur différentes heures de début et de fin pour chaque jour sélectionné. []
    d. Cliquez sur le bouton mettre à jour le planning lorsque vous avez terminé de définir le planning. []

Mise à l'échelle dynamique

Live Scaling active et désactive automatiquement les machines virtuelles dans un pool d'hôtes partagé en fonction de la charge des utilisateurs simultanés. Au fur et à mesure que chaque serveur se remplit, un serveur supplémentaire est activé de sorte que son prêt lorsque l'équilibreur de charge du pool hôte envoie des demandes de session utilisateur. Pour une utilisation efficace de Live Scaling, choisissez "Depth First" comme type d'équilibreur de charge.

Pour activer la mise à l'échelle dynamique :

1. Connectez-vous à VDS at https://manage.cloudworkspace.com Utilisation de vos identifiants VDS.
2. Cliquez sur l'élément de menu espace de travail, puis cliquez sur le nom de l'espace de travail dans la liste. []
3. Cliquez sur l'onglet planification de la charge de travail. []
4. Cliquez sur le bouton radio activé dans la section mise à l'échelle directe. []
5. Cliquez sur le nombre max. D'utilisateurs par serveur et saisissez le nombre max. Selon la taille de l'ordinateur virtuel, ce nombre est généralement compris entre 4 et 20. []
6. FACULTATIF : cliquez sur l'option serveurs alimentés supplémentaires activés et entrez un certain nombre de serveurs supplémentaires que vous souhaitez utiliser pour le pool d'hôtes. Ce paramètre active le nombre spécifié de serveurs en plus du serveur qui remplit activement pour agir comme tampon pour de grands groupes d'utilisateurs se connectant dans la même fenêtre de temps. []

> Mise à l'échelle dynamique s'applique actuellement à tous les pools de ressources partagées. Dans un proche avenir, chaque pool aura des options de mise à l'échelle dynamique indépendantes.

Arrêter l'ensemble du déploiement

Si vous prévoyez d'utiliser votre déploiement d'évaluation uniquement en dehors de la production, vous pouvez désactiver toutes les machines virtuelles du déploiement lorsque vous ne les utilisez pas.

Pour activer ou désactiver le déploiement (c'est-à-dire désactiver les machines virtuelles dans le déploiement), procédez comme suit :

1. Connectez-vous à VDS at https://manage.cloudworkspace.com Utilisation de vos identifiants VDS.
2. Cliquez sur l'élément de menu déploiements. []Faites défiler le curseur sur la ligne du déploiement cible pour afficher l'icône de la vitesse de configuration. []
3. Cliquez sur le rapport, puis choisissez Arrêter. []
4. Pour redémarrer ou démarrer, suivez les étapes 1-3 et choisissez Démarrer. []

> L'arrêt ou le démarrage de toutes les machines virtuelles du déploiement peut prendre plusieurs minutes.

Créez et gérez des images de machine virtuelle

VDS contient des fonctionnalités de création et de gestion des images de machines virtuelles pour les déploiements futurs. Pour accéder à cette fonctionnalité, accédez à : VDS > déploiements > Nom du déploiement > Collections de provisionnement. Les fonctions de la « collection d'images VDI » sont décrites ci-dessous : ""

Configurez Azure Cloud Backup Service

VDS peut configurer et gérer en mode natif Azure Cloud Backup, un service PaaS Azure pour la sauvegarde de machines virtuelles. Les stratégies de sauvegarde peuvent être attribuées à des machines ou groupes individuels de machines par type ou pool hôte. Pour plus de détails, cliquez ici : ""

Sélectionnez le mode gestion/stratégie des applications

Par défaut, VDS implémente un certain nombre d'objets de stratégie de groupe (GPO, Group Policy Objects) qui verrouillent l'espace de travail de l'utilisateur final. Ces règles empêchent l'accès aux emplacements des couches de données centrales (ex. c:\) et la possibilité d'effectuer des installations d'applications en tant qu'utilisateur final.

Cette évaluation a pour but de démontrer les fonctionnalités de Windows Virtual Desktop. Vous avez donc la possibilité de supprimer les GPO afin de mettre en œuvre un « espace de travail de base » qui fournit la même fonctionnalité et le même accès qu'un espace de travail physique. Pour ce faire, suivez les étapes de l'option "espace de travail de base".

Vous pouvez également choisir d'utiliser l'ensemble complet de fonctions de gestion de Virtual Desktop pour implémenter un « espace de travail contrôlé ». Ces étapes comprennent la création et la gestion d'un catalogue d'applications pour les droits d'application utilisateur final et l'utilisation d'autorisations de niveau administrateur pour gérer l'accès aux applications et aux dossiers de données. Suivez les étapes de la section « espace de travail contrôlé » pour implémenter ce type d'espace de travail sur vos pools hôtes AVD.

Espace de travail AVD contrôlé (stratégies par défaut)

L'utilisation d'un espace de travail contrôlé est le mode par défaut pour les déploiements VDS. Les règles sont appliquées automatiquement. Ce mode nécessite que les administrateurs VDS installent des applications, puis les utilisateurs finaux ont accès à l'application via un raccourci sur le bureau de session. De la même manière, l'accès aux dossiers de données est affecté aux utilisateurs finaux en créant des dossiers partagés mappés et en configurant des autorisations pour ne voir que les lettres de lecteur mappées au lieu de l'amorçage standard et/ou des lecteurs de données. Pour gérer cet environnement, suivez les étapes ci-dessous pour installer des applications et fournir un accès à l'utilisateur final.

Retour à l'espace de travail AVD de base

La création d'un espace de travail de base nécessite la désactivation des stratégies de GPO par défaut créées par défaut.

Pour ce faire, suivez cette procédure unique :

1. Connectez-vous à VDS at https://manage.cloudworkspace.com à l'aide de vos informations d'identification d'administrateur principales.
2. Cliquez sur l'élément de menu déploiements à gauche. []
3. Cliquez sur le nom de votre déploiement. []
4. Sous la section serveurs de plate-forme (page médiane à droite), faites défiler la ligne vers la droite pour CWMGR1 jusqu'à ce que l'engrenage apparaisse. []
5. Cliquez sur l'engrenage et choisissez connecter. []
6. Saisissez les informations d'identification « Tech » que vous avez créées lors de l'approvisionnement pour vous connecter au serveur CWMGR1 à l'aide de l'accès HTML5. []
7. Cliquez sur le menu Démarrer (Windows), choisissez Outils d'administration Windows. []
8. Cliquez sur l'icône gestion des stratégies de groupe. []

9. Cliquez sur l'élément AADDC Users dans la liste du volet gauche. []
10. Cliquez avec le bouton droit de la souris sur la stratégie "utilisateurs de Cloud Workspace" dans la liste du volet droit, puis désélectionnez l'option "liaison activée". Cliquez sur OK pour confirmer cette action. [] []
11. Sélectionnez action, mise à jour de stratégie de groupe dans le menu, puis confirmez que vous souhaitez forcer une mise à jour de stratégie sur ces ordinateurs. []
12. Répétez les étapes 9 et 10, mais sélectionnez "utilisateurs AADDC" et "sociétés Cloud Workspace" comme stratégie pour désactiver le lien. Une fois cette étape terminée, vous n'avez pas besoin de forcer la mise à jour de la stratégie de groupe. [] []
13. Fermez l'éditeur de gestion de stratégies de groupe et les fenêtres Outils d'administration, puis fermez la session. []Ces étapes fournissent un environnement d'espace de travail de base pour les utilisateurs finaux. Pour confirmer votre connexion, connectez-vous en tant que compte d'utilisateur final : l'environnement de session ne doit pas comporter de restrictions d'espace de travail contrôlées telles que le menu Démarrer masqué, l'accès verrouillé au lecteur C:\ et le panneau de configuration masqué.

> Le compte .tech créé pendant le déploiement dispose d'un accès complet pour installer des applications et modifier la sécurité sur des dossiers indépendants de VDS. Cependant, si vous souhaitez que les utilisateurs finaux du domaine Azure AD disposent d'un accès complet similaire, vous devez les ajouter au groupe administrateurs locaux sur chaque machine virtuelle.

Guide de déploiement AVD - AD supplémentaire existant

Présentation

La configuration VDS a la possibilité de connecter un nouveau déploiement à une structure AD existante. Ces instructions couvrent cette option en détail. Cet article ne se comporte pas seul, mais il s'agit plutôt d'une explication détaillée d'une alternative à l'option Nouvelle AD couverte par le "Guide de déploiement AVD"

Type Active Directory

La section suivante définit le type de déploiement Active Directory pour le déploiement VDS. Dans ce guide, nous allons sélectionner Windows Server Active Directory existant, qui va tirer parti d'une structure AD qui existe déjà.

Réseau AD existant

Le programme d'installation VDS affiche la liste des vNets susceptibles de représenter la connexion entre la structure AD existante et Azure AD. Le vnet que vous sélectionnez doit avoir un data Center hébergé par Azure que vous avez configuré dans Azure. De plus, les paramètres DNS personnalisés seront pointés sur le DC hébergé par Azure.

[]

Nom de domaine Active Directory existant

Saisissez le nom de domaine existant qui sera utilisé. Remarque : vous ne souhaitez pas utiliser le domaine qui se trouve dans le portail Azure sous le module Active Directory, car il peut causer des problèmes DNS. C'est dans cet exemple que les utilisateurs ne pourront pas accéder à ce site Web (<votredomain>.com, par exemple) depuis leur poste de travail.

Nom d'utilisateur et mot de passe AD existants

Il existe trois façons de fournir les informations d'identification nécessaires pour faciliter un déploiement à l'aide

d’une structure AD existante.

1. Indiquez le nom d’utilisateur et le mot de passe de l’administrateur du domaine Active Directory

   Il s’agit de la méthode la plus simple – fournissant des informations d’identification d’administrateur de domaine utilisées pour faciliter le déploiement.

   Ce compte peut être créé pour un usage unique et être supprimé une fois le processus de déploiement terminé.

2. Créer des autorisations requises pour la mise en correspondance de comptes

   Cette méthode implique que les administrateurs du client créent manuellement la structure des autorisations ici, puis entrent les informations d’identification du compte CloudWorkspaceSVC ici et continuer.

3. Processus de déploiement manuel

   Contactez le support NetApp VDS pour obtenir de l’aide lors de la configuration de l’accès AD avec les principes de compte les moins privilégiés.

Étapes suivantes

Cet article présente les étapes uniques du déploiement dans un environnement AD existant. Une fois ces étapes terminées, vous pouvez revenir au guide de déploiement standard "ici".

Composants et autorisations VDS

Entités et services de sécurité AVD et VDS

Pour exécuter des actions automatisées, Azure Virtual Desktop (AVD) requiert des comptes et des composants de sécurité dans Azure AD et Active Directory local. Virtual Desktop Service (VDS) de NetApp crée des composants et des paramètres de sécurité lors du processus de déploiement. Ils permettent aux administrateurs de contrôler l’environnement AVD. Ce document décrit les comptes VDS, les composants et les paramètres de sécurité appropriés dans les deux environnements.

Les composants et les autorisations du processus d’automatisation du déploiement sont la plupart du temps différents des composants de l’environnement final déployé. Cet article est donc constitué de deux sections majeures, à savoir la section automatisation du déploiement et la section sur l’environnement déployé.

[largeur=75 %]

Composants et autorisations d’automatisation de déploiement AVD

Le déploiement VDS exploite plusieurs composants Azure et NetApp ainsi que les autorisations de sécurité afin de mettre en œuvre des déploiements et des espaces de travail.

Services de déploiement VDS

Les applications d’entreprise

VDS exploite les applications d’entreprise et les enregistrements d’applications dans le domaine Azure AD d’un locataire. Les applications d’entreprise sont le conduit des appels contre Azure Resource Manager, Azure Graph et (si vous utilisez AVD Fall Release) les points de terminaison de l’API AVD du contexte de sécurité de

l'instance Azure AD à l'aide des rôles et autorisations délégués accordés au Service principal associé. Les enregistrements d'app peuvent être créés selon l'état d'initialisation des services AVD pour le locataire via VDS.

Pour permettre la création et la gestion de ces machines virtuelles, VDS crée plusieurs composants pris en charge dans l'abonnement Azure :

Espace de travail cloud

Il s'agit de l'autorisation accordée par les administrateurs d'applications entreprise initiaux à et est utilisé pendant le processus de déploiement de l'Assistant d'installation VDS.

L'application Cloud Workspace Enterprise demande un ensemble spécifique d'autorisations pendant le processus d'installation VDS. Ces autorisations sont les suivantes :

- Accès au répertoire en tant qu'utilisateur connecté (délégué)
- Lecture et écriture de données de répertoire (déléguée)
- Se connecter et lire le profil utilisateur (délégué)
- Connexion des utilisateurs (déléguée)
- Afficher le profil de base des utilisateurs (délégué)
- Accès à la gestion des services Azure en tant qu'utilisateurs de l'entreprise (délégués)

API Cloud Workspace

Gestion des appels de gestion généraux pour les fonctions PaaS d'Azure. Les fonctions PaaS d'Azure sont notamment les suivantes : Azure Compute, Azure Backup, Azure Files, etc. Ce Service principal requiert des droits de propriétaire pour l'abonnement Azure cible lors du déploiement initial, et des droits de Contributor pour la gestion continue (remarque : L'utilisation d'Azure Files nécessite des droits de propriétaire d'abonnement pour définir les autorisations par utilisateur sur les objets Azure File).

L'API Cloud Workspace Enterprise application demande un ensemble spécifique d'autorisations pendant le processus d'installation VDS. Ces autorisations sont les suivantes :

- Contributeur d'abonnement (ou propriétaire de l'abonnement si des fichiers Azure sont utilisés)
- Graphique AD Azure
  - Lecture et écriture de toutes les applications (application)
  - Gérer les applications que cette application crée ou possède (application)
  - Périphériques de lecture et d'écriture (application)
  - Accéder au répertoire en tant qu'utilisateur connecté (délégué)
  - Lire les données d'annuaire (application)
  - Lecture des données du répertoire (déléguée)
  - Lecture et écriture de données de répertoire (application)
  - Lecture et écriture de données de répertoire (déléguée)
  - Domaines de lecture et d'écriture (application)
  - Lire tous les groupes (délégués)
  - Lecture et écriture de tous les groupes (délégués)

    - Lire toutes les adhésions masquées (application)
    - Lire les adhésions masquées (déléguée)
    - Se connecter et lire le profil utilisateur (délégué)
    - Lire tous les profils des utilisateurs (délégués)
    - Lecture des profils de base de tous les utilisateurs (délégués)
- Gestion de services Azure
    - Accès à la gestion des services Azure en tant qu'utilisateurs de l'entreprise (délégués)

VDS NetApp

Les composants VDS NetApp sont utilisés via le plan de contrôle VDS pour automatiser le déploiement et la configuration des rôles, services et ressources AVD.

Rôle personnalisé

Le rôle Automation Contributor est créé pour faciliter les déploiements par le biais de méthodologies les moins privilégiées. Ce rôle permet à la machine virtuelle CWMGR1 d'accéder au compte d'automatisation Azure.

Compte d'automatisation

Un compte Automation est créé lors du déploiement et il est un composant requis lors du processus de provisionnement. Le compte Automation contient des variables, des informations d'identification, des modules et des configurations d'état souhaitées et fait référence au coffre-fort de clés.

Configuration de l'état souhaité

Il s'agit de la méthode utilisée pour générer la configuration de CWMGR1. Le fichier de configuration est téléchargé sur la machine virtuelle et appliqué via local Configuration Manager sur la machine virtuelle. Voici des exemples d'éléments de configuration :

- Installation des fonctionnalités Windows
- Installation du logiciel
- Application de configurations logicielles
- S'assurer que les ensembles d'autorisations appropriés sont appliqués
- Application du certificat Let's Encrypt
- S'assurer que les enregistrements DNS sont corrects
- S'assurer que CWMGR1 est joint au domaine

Modules :

- ActiveDirectoryDsc : ressource de configuration de l'état souhaitée pour le déploiement et la configuration d'Active Directory. Ces ressources vous permettent de configurer de nouveaux domaines, domaines enfants et contrôleurs de domaine haute disponibilité, d'établir des approbations inter-domaines et de gérer les utilisateurs, les groupes et les UO.
- AZ.Accounts : module fourni par Microsoft utilisé pour gérer les identifiants et les éléments de configuration communs pour les modules Azure
- AZ.Automation : module fourni par Microsoft pour les applets de commande Azure Automation

- Az.Compute:A module fourni par Microsoft pour les applets de commande Azure Compute
- AZ.KeyVault : module fourni par Microsoft pour les applets de commande Azure Key Vault
- AZ.Resources : module fourni par Microsoft pour les applets de commande Azure Resource Manager
- CChoco : ressource de configuration de l'état souhaité pour le téléchargement et l'installation de packages à l'aide de Chocolatey
- CjAz : ce module créé par NetApp fournit des outils d'automatisation au module d'automatisation Azure
- CjAzACS : ce module créé par NetApp contient les fonctions d'automatisation de l'environnement et les processus PowerShell s'exécutant depuis le contexte utilisateur.
- CjAzBuild : ce module créé par NetApp contient les processus de création et d'automatisation de la maintenance et des processus PowerShell exécutés à partir du contexte système.
- CNtfsAccessControl : ressource de configuration de l'état souhaitée pour la gestion du contrôle d'accès NTFS
- ComputerManagementDsc : ressource de configuration de l'état souhaitée qui permet des tâches de gestion de l'ordinateur telles que l'ajout d'un domaine et la planification de tâches, ainsi que la configuration d'éléments tels que la mémoire virtuelle, les journaux d'événements, les fuseaux horaires et les paramètres d'alimentation.
- CUserRightsAssignment : ressource de configuration d'état souhaitée permettant la gestion des droits d'utilisateur tels que les droits et privilèges d'ouverture de session
- NetworkingDsc : t ressource de configuration de l'état souhaitée pour le réseau
- XCertificate : ressource de configuration de l'état souhaitée pour simplifier la gestion des certificats sur Windows Server.
- XDnsServer : ressource de configuration de l'état souhaité pour la configuration et la gestion de Windows Server DNS Server
- XNetworking : ressource de configuration de l'état souhaitée associée à la mise en réseau.
- "XRemoteDesktopAdmin": Ce module utilise un référentiel qui contient les ressources de configuration de l'état souhaitées pour configurer les paramètres de bureau à distance et le pare-feu Windows sur un ordinateur local ou distant.
- XRemoteDesktopSessionHost : ressource de configuration de l'état souhaité (xRDSessionDeployment, xRDSessionCollection, xRDSessionCollectionConfiguration et xRRemoteApp) permettant la création et la configuration d'une instance Remote Desktop session Host (RDSH)
- XSmbShare : ressource de configuration de l'état souhaitée pour la configuration et la gestion d'un partage SMB
- XSystemSecurity : ressource de configuration de l'état souhaitée pour la gestion des UAC et IE Esc

> Azure Virtual Desktop installe également les composants Azure, notamment les applications d'entreprise et les enregistrements d'applications pour Azure Virtual Desktop et Azure Virtual Desktop client, le locataire AVD, les pools d'hôtes AVD, les groupes d'applications AVD et les machines virtuelles enregistrées AVD. Alors que les composants VDS Automation gèrent ces composants, AVD contrôle leur configuration par défaut et leur jeu d'attributs. Consultez donc la documentation AVD pour plus de détails.

Composants AD hybrides

Pour faciliter l'intégration avec l'infrastructure AD existante sur site ou exécutée dans le cloud public, d'autres composants et autorisations sont requis dans l'environnement AD existant.

Contrôleur de domaine

Le contrôleur de domaine existant peut être intégré à un déploiement AVD via AD Connect et/ou un VPN site à site (ou Azure ExpressRoute).

AD Connect

Pour faciliter l'authentification des utilisateurs via les services PaaS AVD, AD Connect peut être utilisé pour synchroniser le contrôleur de domaine avec Azure AD.

Groupe de sécurité

VDS utilise un groupe de sécurité Active Directory appelé CW-Infrastructure pour contenir les autorisations nécessaires à l'automatisation des tâches dépendantes d'Active Directory telles que la jointure de domaine et la pièce jointe de stratégie GPO.

Compte de service

VDS utilise un compte de service Active Directory appelé CloudworkspaceSVC utilisé comme identité pour les services Windows VDS et le service d'application IIS. Ce compte n'est pas interactif (ne permet pas la connexion RDP) et est le membre principal du compte CW-Infrastructure

VPN ou ExpressRoute

Un VPN site à site ou Azure ExpressRoute peut être utilisé pour relier directement les machines virtuelles Azure au domaine existant. Il s'agit d'une configuration facultative disponible lorsque les exigences du projet le requièrent.

Délégation d'autorisation AD locale

NetApp propose un outil en option permettant de rationaliser le processus AD hybride. Si vous utilisez l'outil en option de NetApp, il doit :

- Exécutez sur un système d'exploitation de serveur plutôt que sur un système d'exploitation de poste de travail
- Exécutez sur un serveur qui est joint au domaine ou qui est un contrôleur de domaine
- Disposez de PowerShell 5.0 ou supérieur sur le serveur exécutant l'outil (s'il n'est pas exécuté sur le contrôleur de domaine) et sur le contrôleur de domaine
- Être exécuté par un utilisateur avec des privilèges d'administrateur de domaine OU être exécuté par un utilisateur avec des autorisations d'administrateur local et la capacité de fournir des informations d'identification d'administrateur de domaine (pour une utilisation avec des RunAs)

Qu'elles soient créées manuellement ou appliquées par l'outil NetApp, les autorisations requises sont les suivantes :

- Groupe CW-Infrastructure
  - Le groupe de sécurité Infrastructure de l'espace de travail de Cloud (**CW-Infrastructure**) bénéficie d'un contrôle total du niveau ou de l'espace de travail de Cloud et de tous les objets descendants
  - <code de déploiement>.cloudWorkspace.app DNS zone – CW-Infrastructure group EntitCreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedRight, Delete, GenericWrite
  - Serveur DNS – Groupe CW-Infrastructure, ReadProperty, GenericExecute

    - Accès administrateur local pour les VM créées (CWMGR1, VM de session AVD) (effectué par stratégie de groupe sur les systèmes AVD gérés)
- Groupe CW-CWMGRAccess ce groupe fournit des droits d'administration locaux à CWMGR1 sur tous les modèles, le serveur unique, le nouveau modèle Active Directory natif utilise les groupes intégrés opérateurs de serveur utilisateurs de bureau à distance et opérateurs de configuration réseau.

Composants environnementaux AVD et autorisations

Une fois le processus d'automatisation du déploiement terminé, l'utilisation et l'administration continues des déploiements et des espaces de travail nécessitent l'installation d'un ensemble distinct de composants et d'autorisations, tel que défini ci-après. Bon nombre des composants et autorisations ci-dessus restent pertinents, mais cette section a pour objectif de définir la structure d'un déploiement.

Les composants des déploiements VDS et des espaces de travail peuvent être organisés en plusieurs catégories logiques :

- Clients utilisateur final
- Composants du plan de contrôle VDS
- Composants de Microsoft Azure AVD-PaaS
- Composants de la plate-forme VDS
- Composants de l'espace de travail VDS dans le locataire Azure
- Composants AD hybrides

Clients utilisateur final

Les utilisateurs peuvent se connecter à leur bureau AVD et/ou à partir de divers types de points de terminaison. Microsoft a publié des applications client pour Windows, MacOS, Android et iOS. En outre, un client Web est disponible pour un accès sans client.

Il existe des fournisseurs de clients légers Linux qui ont publié un client de noeuds finaux pour AVD. Ils sont répertoriés à l'adresse https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

Composants du plan de contrôle VDS

API REST VDS

VDS est basée sur des API REST entièrement documentées afin que toutes les actions disponibles dans l'application Web soient également disponibles via l'API. La documentation de l'API est ici : https://api.cloudworkspace.com/5.4/swagger/ui/index#

Application web VDS

Les administrateurs VDS peuvent interagir avec l'application ADS via l'application web VDS. Ce portail Web est à : https://manage.cloudworkspace.com

Base de données du plan de contrôle

Les données et paramètres VDS sont stockés dans la base de données SQL du plan de contrôle, hébergée et gérée par NetApp.

Communications VDS

Composants des locataires Azure

L'automatisation du déploiement VDS crée un groupe de ressources Azure unique contenant les autres composants AVD, notamment les VM, les sous-réseaux, les groupes de sécurité du réseau et les conteneurs Azure Files ou les pools de capacité Azure NetApp Files. Remarque – la valeur par défaut est un groupe de ressources unique, mais VDS dispose d'outils permettant de créer des ressources dans des groupes de ressources supplémentaires si nécessaire.

Composants de Microsoft Azure AVD-PaaS

API REST AVD

Microsoft AVD peut être géré via API. VDS a largement utilisé ces API pour automatiser et gérer les environnements AVD. La documentation se trouve à l'adresse suivante : https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/

Courtier de session

Le courtier détermine les ressources autorisées pour l'utilisateur et orchestre la connexion de l'utilisateur à la passerelle.

Diagnostics Azure

Azure Diagnostics a été spécialement conçu pour prendre en charge les déploiements AVD.

Client web AVD

Microsoft a fourni un client Web pour permettre aux utilisateurs de se connecter à leurs ressources AVD sans avoir installé un client local.

Passerelle de session

Le client RD installé localement se connecte à la passerelle pour communiquer en toute sécurité dans l'environnement AVD.

Composants de la plate-forme VDS

CWMGR1

CMWGR1 est la VM de contrôle VDS pour chaque déploiement. Par défaut, il est créé en tant que machine virtuelle Windows 2019 Server dans l'abonnement Azure cible. Consultez la section déploiement local pour obtenir la liste des composants VDS et tiers installés sur CWMGR1.

AVD nécessite que les machines virtuelles AVD soient jointes à un domaine Active Directory. Pour faciliter ce processus et fournir les outils d'automatisation pour la gestion de l'environnement VDS, plusieurs composants sont installés sur la machine virtuelle CWMGR1 décrite ci-dessus et plusieurs composants sont ajoutés à l'instance AD. Ses composants sont les suivants :

- **Windows Services** - VDS utilise les services Windows pour effectuer des actions d'automatisation et de gestion à partir d'un déploiement :
  - **CW Automation Service** est un service Windows déployé sur CWMGR1 dans chaque déploiement AVD qui exécute de nombreuses tâches d'automatisation en contact avec l'utilisateur dans l'environnement. Ce service s'exécute sous le compte AD **CloudWorkspaceSVC**.

    - **CW VM Automation Service** est un service Windows déployé sur CWMGR1 dans chaque déploiement AVD qui exécute les fonctions de gestion de la machine virtuelle. Ce service s'exécute sous le compte AD **CloudWorkspaceSVC**.
    - **CW Agent Service** est un service Windows déployé sur chaque machine virtuelle sous gestion VDS, y compris CWMGR1. Ce service s'exécute sous le contexte **LocalSystem** sur la machine virtuelle.
    - **CWManagerX API** est un écouteur basé sur un pool d'applications IIS installé sur CWMGR1 dans chaque déploiement AVD. Cela traite les demandes entrantes du plan de contrôle global et est exécuté sous le compte AD **CloudWorkspaceSVC**.
- **SQL Server 2017 Express** – VDS crée une instance SQL Server Express sur la machine virtuelle CWMGR1 pour gérer les métadonnées générées par les composants d'automatisation.
- **Internet information Services (IIS)** – IIS est activé sur CWMGR1 pour héberger l'application CWManagerX et CWApps IIS (uniquement si la fonctionnalité RDS RemoteApp est activée). VDS requiert la version 7.5 ou ultérieure d'IIS.
- **Portail HTML5 (facultatif)** – VDS installe le service Spark Gateway pour fournir un accès HTML5 aux machines virtuelles dans le déploiement et à partir de l'application Web VDS. Il s'agit d'une application Java qui peut être désactivée et supprimée si cette méthode d'accès n'est pas souhaitée.
- **RD Gateway (en option)** – VDS permet au rôle de passerelle RD sur CWMGR1 de fournir un accès RDP aux pools de ressources basés sur la collecte RDS. Ce rôle peut être désactivé/désinstallé si seul l'accès AVD Reverse Connect est souhaité.
- **RD Web (facultatif)** – VDS active le rôle Web RD et crée l'application Web IIS CWApps. Ce rôle peut être désactivé si seul l'accès AVD est souhaité.
- **DC Config** – application Windows utilisée pour effectuer des tâches de configuration spécifique au site VDS et déploiement et au site VDS ainsi que des tâches de configuration avancée.
- **Outils de test VDC** : application Windows prenant en charge l'exécution directe des tâches pour les changements de configuration au niveau des ordinateurs virtuels et des clients utilisés dans les rares cas où les tâches d'API ou d'application Web doivent être modifiées à des fins de dépannage.
- **Encryptons le certificat générique (facultatif)** – créé et géré par VDS – toutes les machines virtuelles nécessitant un trafic HTTPS sur TLS sont mises à jour avec le certificat chaque nuit. Le renouvellement est également géré par tâche automatisée (les certificats sont 90 jours, donc le renouvellement commence peu avant). Le client peut fournir son propre certificat de caractère générique si nécessaire. VDS nécessite également plusieurs composants Active Directory pour prendre en charge les tâches d'automatisation. L'objectif de la conception est d'utiliser un nombre minimum de composants AD et d'ajouts d'autorisations tout en continuant de prendre en charge l'environnement pour la gestion automatisée. Ces composants comprennent :
- **Unité organisationnelle (ou) de l'espace de travail Cloud** – cette unité organisationnelle agira comme conteneur AD principal pour les composants enfants requis. Les autorisations pour les groupes d'accès DHP client et CW-Infrastructure seront définies à ce niveau et pour ses composants enfants. Voir l'annexe A pour les sous-UO créés dans cette UO.
- **Cloud Workspace Infrastructure Group (CW-Infrastructure)** est un groupe de sécurité créé dans l'AD local pour permettre l'affectation des autorisations déléguées requises au compte de service VDS (**CloudWorkspaceSVC**)
- **Client DHP Access Group (ClientDHPAccess)** est un groupe de sécurité créé dans l'AD local pour permettre à VDS de gérer l'emplacement dans lequel les données de profil, de domicile utilisateur et partagées de la société résident.
- **Compte de service CloudWorkspaceSVC** (membre du groupe Cloud Workspace Infrastructure Group)
- **Zone DNS pour <code de déploiement>.cloudWorkspace.app domain** (ce domaine gère les noms DNS créés automatiquement pour les VM hôtes de session) – créé par la configuration du déploiement.

- **GPO** propres à NetApp liés à plusieurs UO enfant de l'unité organisationnelle de Cloud Workspace. Ces stratégies de groupe sont les suivantes :
  - **Cloud Workspace GPO (associé à Cloud Workspace ou)** – définit les protocoles et méthodes d'accès pour les membres du groupe CW-Infrastructure. Ajoute également le groupe au groupe d'administrateurs local sur les hôtes de session AVD.
  - **Objet GPO** du pare-feu de l'espace de travail Cloud (associé aux serveurs des clients dédiés, aux unités de bureau à distance et aux unités de stockage à distance) - crée une stratégie qui assure et isole les connexions aux hôtes des sessions à partir du ou des serveurs de plate-forme.
  - **Cloud Workspace RDS** (serveurs de clients dédiés, unités de bureau à distance et unités de stockage à distance) - la stratégie définit les limites de qualité de session, de fiabilité, de déconnexion des limites de délai d'attente. Pour les sessions RDS, la valeur TS Licensing Server est définie.
  - **Cloud Workspace Companies** (NON LIÉES par défaut) – GPO facultatif à « verrouiller » une session utilisateur/un espace de travail en empêchant l'accès aux outils et zones d'administration. Peut être lié/activé pour fournir un espace de travail d'activité restreinte.

Des configurations de paramètres de stratégie de groupe par défaut peuvent être fournies sur demande.

Composants de l'espace de travail VDS

La couche de données

Azure NetApp Files

Un pool de capacité Azure NetApp Files et un ou plusieurs volumes associés seront créés si vous choisissez Azure NetApp Files comme option de couche de données dans la configuration VDS. Le volume héberge le stockage classé partagé des profils utilisateur (via des conteneurs FSLogix), des dossiers personnels utilisateur et le dossier de partage des données d'entreprise.

Azure Files

Un partage de fichiers Azure et son compte de stockage Azure associé seront créés si vous choisissez des fichiers Azure comme option de couche de données dans CWS Setup. Le partage de fichiers Azure héberge le stockage partagé des profils utilisateur (via des conteneurs FSLogix), les dossiers personnels des utilisateurs et le dossier de partage des données d'entreprise.

Serveur de fichiers avec disque géré

Une machine virtuelle Windows Server est créée avec un disque géré si vous choisissez l'option serveur de fichiers comme couche de données dans la configuration VDS. Le serveur de fichiers héberge le stockage classé partagé pour les profils utilisateur (via les conteneurs FSLogix), les dossiers personnels utilisateur et le dossier de partage des données d'entreprise.

La mise en réseau d'Azure

Réseau virtuel Azure

VDS crée un réseau virtuel Azure et prend en charge les sous-réseaux. VDS requiert un sous-réseau séparé pour les machines hôtes CWMGR1, AVD et les contrôleurs de domaine Azure et le peering entre les sous-réseaux. Notez que le sous-réseau du contrôleur AD existe généralement déjà. Les sous-réseaux VDS déployés doivent donc être associés au sous-réseau existant.

Groupes de sécurité du réseau

Un groupe de sécurité réseau est créé pour contrôler l'accès à la machine virtuelle CWMGR1.

- Locataire : contient des adresses IP à utiliser par hôte de session et par VM de données
- Services : contient les adresses IP utilisées par les services PaaS (Azure NetApp Files, par exemple)
- Plateforme : contient des adresses IP à utiliser en tant que VM de plateforme NetApp (CWMGR1 et tous les serveurs de passerelle)
- Répertoire : contient les adresses IP à utiliser comme machines virtuelles Active Directory

Azure AD

L'automatisation et l'orchestration VDS déploient les machines virtuelles dans une instance Active Directory ciblée, puis rejoint les machines au pool hôte désigné. Les machines virtuelles AVD sont gérées au niveau de l'ordinateur par la structure AD (unités organisationnelles, stratégie de groupe, autorisations d'administrateur informatique local, etc.) et par l'appartenance à la structure AVD (pools d'hôtes, appartenance à un groupe d'applications d'espace de travail), qui sont régies par des entités et des autorisations Azure AD. VDS gère cet environnement « double contrôle » en utilisant l'application VDS Enterprise/Azure Service principal pour les actions AVD et le compte de service AD local (CloudWorkspaceSVC) pour les actions AD et informatiques locales.

Les étapes spécifiques de la création d'une machine virtuelle AVD et de son ajout au pool hôte AVD sont les suivantes :

- Création d'une machine virtuelle à partir d'un modèle Azure visible par l'abonnement Azure associé à AVD (utilise les autorisations Azure Service principal)
- Vérifier/configurer l'adresse DNS pour la nouvelle machine virtuelle à l'aide d'Azure VNet désigné pendant le déploiement VDS (nécessite des autorisations AD locales (tout délégué à CW-Infrastructure ci-dessus) définit le nom de la machine virtuelle à l'aide du schéma de nommage VDS standard ***{Code société}TS{sequencenumber}***. Exemple : XYZTS3. (Autorisations AD locales requises (placées dans la structure ou que nous avons créée sur site (poste de travail distant/code société/partagé) (même autorisation/description de groupe que ci-dessus)
- Place la machine virtuelle dans l'unité organisationnelle Active Directory désignée (AD) (nécessite les autorisations déléguées à la structure UO (désignée lors du processus manuel ci-dessus)
- Mettre à jour le répertoire DNS AD interne avec le nouveau nom de machine/adresse IP (nécessite des autorisations AD locales)
- Relier la nouvelle machine virtuelle au domaine AD local (autorisations AD locales requises)
- Mettre à jour la base de données locale VDS avec de nouvelles informations sur le serveur (ne nécessite pas d'autorisations supplémentaires)
- Associer VM au pool hôte AVD désigné (nécessite des autorisations AVD Service principal)
- Installation des composants Chocolatey sur la nouvelle machine virtuelle (nécessite un privilège d'administration informatique local pour le compte **CloudWorkspaceSVC**)
- Installer les composants FSLogix pour l'instance AVD (nécessite des autorisations administratives locales sur l'UO AVD dans l'AD local)
- Mettre à jour l'objet GPO de pare-feu AD Windows pour autoriser le trafic vers la nouvelle machine virtuelle (nécessite la création/modification de GPO AD pour les stratégies associées à l'unité d'organisation AVD et à ses machines virtuelles associées. Nécessite la création/modification de stratégie de GPO AD sur l'UO AVD dans l'AD local. Peut être désactivé après installation si vous ne gérez pas les machines virtuelles via VDS).

- Définir l'indicateur « Autoriser les nouvelles connexions » sur la nouvelle machine virtuelle (nécessite les autorisations du principal de service Azure)

Ajout de machines virtuelles à Azure AD

Les machines virtuelles du locataire Azure doivent être jointes au domaine, mais les VM ne peuvent pas se joindre directement à Azure AD. Par conséquent, VDS déploie le rôle de contrôleur de domaine dans la plateforme VDS et ensuite nous synchronisons ce DC avec Azure AD en utilisant AD Connect. Il est également possible d'utiliser Azure AD Domain Services (ADDS), de synchroniser un data Center hybride (une machine virtuelle sur site ou ailleurs) avec AD Connect, ou de joindre directement les machines virtuelles à un data Center hybride via un VPN de site à site ou Azure ExpressRoute.

Pools hôtes AVD

Les pools hôtes sont un ensemble d'une ou plusieurs machines virtuelles identiques dans les environnements Azure Virtual Desktop. Chaque pool hôte peut contenir un groupe d'applications avec lequel les utilisateurs peuvent interagir comme ils le feraient sur un poste de travail physique.

Hôtes de session

Au sein d'un pool hôte se trouve une ou plusieurs machines virtuelles identiques. Ces sessions utilisateur se connectant à ce pool hôte sont équilibrées par le service d'équilibreur de charge AVD.

Groupes d'applications

Par défaut, le groupe d'applications *Desktop Users* est créé lors du déploiement. Tous les utilisateurs de ce groupe d'applications bénéficient d'une expérience Windows complète. En outre, des groupes d'applications peuvent être créés pour servir les services d'applications en streaming.

Espace de travail d'analyse des journaux

Un espace de travail Log Analytics est créé pour stocker les journaux à partir des processus de déploiement et DSC ainsi que d'autres services. Ceci peut être supprimé après le déploiement, mais ce n'est pas recommandé car il active d'autres fonctionnalités. Les journaux sont conservés pendant 30 jours par défaut, sans frais de conservation.

Ensembles de disponibilité

Un ensemble de disponibilité fait partie du processus de déploiement afin de permettre la séparation des machines virtuelles partagées (pools hôtes AVD partagés, pools de ressources RDS) sur les domaines de pannes. Cette opération peut être supprimée après le déploiement, mais désactivez l'option pour offrir une tolérance de panne supplémentaire pour les machines virtuelles partagées.

Coffre-fort de restauration Azure

Un coffre-fort de service de récupération est créé par VDS Automation pendant le déploiement. Elle est actuellement activée par défaut, car Azure Backup est appliqué à CWMGR1 pendant le processus de déploiement. Cette option peut être désactivée et supprimée si vous le souhaitez, mais elle sera recréée si Azure Backup est activé dans l'environnement.

Coffre-fort de clés Azure

Un coffre-fort Azure Key Vault est créé pendant le processus de déploiement et utilisé pour stocker les certificats, les clés API et les identifiants utilisés par les comptes Azure Automation lors du déploiement.

Annexe A – structure d'unité organisationnelle par défaut de Cloud Workspace

- Espace de travail cloud
  - Entreprises Cloud Workspace
  - Serveurs d'espace de travail cloud
    - Serveurs client dédiés
    - Infrastructures
- Serveurs CWMGR
- Serveurs de passerelle
- Serveurs FTP
- Machines virtuelles modèles
  - Bureau à distance
  - Staging
    - Comptes de services Cloud Workspace
  - Comptes de service client
  - Comptes de services d'infrastructure
    - Utilisateurs techniques de Cloud Workspace
  - Groupes
  - Techniciens Tech 3

Conditions préalables AVD et VDS v5.4

Exigences et notes AVD et VDS

Ce document décrit les éléments requis pour déployer Azure Virtual Desktop (AVD) à l'aide de NetApp Virtual Desktop Service (VDS). La « liste de contrôle rapide » fournit une brève liste des composants requis et des étapes de pré-déploiement à suivre pour assurer un déploiement efficace. Le reste du guide fournit des détails plus détaillés sur chaque élément, en fonction des choix de configuration effectués.

Liste de contrôle rapide

Exigences d'Azure

- Locataire Azure AD
- Licence Microsoft 365 pour la prise en charge d'AVD
- Abonnement Azure
- Il existe un quota Azure disponible pour les machines virtuelles Azure
- Compte d'administrateur Azure avec rôles de propriété d'administrateur global et d'abonnement
- Compte d'administrateur de domaine avec rôle d'administrateur d'entreprise pour la configuration d'AD Connect

Informations de prédéploiement

- Déterminez le nombre total d'utilisateurs

- Déterminer la région Azure
- Déterminez le type Active Directory
- Déterminer le type de stockage
- Identifier l'image ou les besoins de la session hôte de la machine virtuelle
- Évaluer la configuration réseau Azure et sur site en place

Exigences détaillées relatives au déploiement VDS

Exigences de connexion de l'utilisateur final

Les clients Remote Desktop suivants prennent en charge Azure Virtual Desktop :

- Bureau Windows
- Web
- Mac OS
- E-S
- IGEL think client (Linux)
- Android (aperçu)

Azure Virtual Desktop ne prend pas en charge le client RemoteApp and Desktop Connections (RADC) ou le client Remote Desktop Connection (MSTSC).

Azure Virtual Desktop ne prend pas actuellement en charge le client Remote Desktop à partir du Windows Store. La prise en charge de ce client sera ajoutée dans une version ultérieure.

Les clients Bureau à distance doivent avoir accès aux URL suivantes :

Adresse	Port TCP sortant	Objectif	Client(s)
*.AVD.microsoft.com	443	Trafic de service	Tout
*.servicebus.windows.net 443 données de dépannage	Tout	go.microsoft.com	443
Microsoft FWLinks	Tout	aka.ms	443
Shortener URL Microsoft	Tout	docs.microsoft.com	443
Documentation	Tout	privacy.microsoft.com	443
Déclaration de confidentialité	Tout	query.prod.cms.rt.microsoft.com	443

L'ouverture de ces URL est essentielle pour une expérience client fiable. Le blocage de l'accès à ces URL n'est pas pris en charge et affecte la fonctionnalité de service. Ces URL correspondent uniquement aux sites et ressources client, et n'incluent pas les URL pour d'autres services tels qu'Azure Active Directory.

Point de départ de l'assistant de configuration VDS

L'assistant d'installation VDS peut gérer la plupart des configurations préalables requises pour un déploiement AVD réussi. L'assistant de configuration ("") crée ou utilise les composants suivants.

Locataire Azure

Requis : un locataire Azure et Azure Active Directory

L'activation d'AVD dans Azure est un paramètre défini pour l'ensemble du locataire. VDS prend en charge l'exécution d'une instance AVD par locataire.

Abonnement Azure

Requis : un abonnement Azure (notez l'ID d'abonnement que vous souhaitez utiliser)

Toutes les ressources Azure déployées doivent être configurées dans un abonnement dédié. Le suivi des coûts pour AVD est donc beaucoup plus facile et simplifie le processus de déploiement. REMARQUE : les essais gratuits Azure ne sont pas pris en charge car ils ne disposent pas de crédits suffisants pour déployer un déploiement AVD fonctionnel.

Le quota core Azure

Un quota suffisant pour les familles de machines virtuelles que vous utiliserez, en particulier au moins 10 cœurs de la famille DS v3 pour le déploiement initial des plateformes (2 cœurs maximum peuvent être utilisés, mais 10 couvre chaque déploiement initial).

Compte d'administrateur Azure

Requis: un compte administrateur global Azure.

L'assistant de configuration VDS demande à l'administrateur Azure d'accorder des autorisations déléguées au principal de service VDS et d'installer l'application VDS Azure Enterprise. L'administrateur doit avoir les rôles Azure suivants attribués :

- Administrateur global du locataire
- Rôle de propriétaire dans l'abonnement

Image de VM

Requis : une image Azure prenant en charge Windows 10 multi-session.

Azure Marketplace fournit les versions les plus récentes de leur image Windows 10 de base et tous les abonnements Azure y ont accès automatiquement. Si vous souhaitez utiliser une image différente ou une image personnalisée, demandez à l'équipe VDS de nous donner des conseils sur la création ou la modification d'autres images ou si des questions générales sur les images Azure nous en laissent savoir plus et nous pouvons planifier une conversation.

Active Directory

AVD nécessite que l'identité de l'utilisateur fasse partie d'Azure AD et que les VM soient joints à un domaine Active Directory synchronisé avec cette même instance AD Azure. Les machines virtuelles ne peuvent pas être directement connectées à l'instance Azure AD. Ainsi, un contrôleur de domaine doit être configuré et synchronisé avec Azure AD.

Ces options prises en charge sont les suivantes :

- Construction automatisée d'une instance Active Directory dans l'abonnement. L'instance AD est généralement créée par VDS sur la machine virtuelle de contrôle VDS (CWMGR1) pour les déploiements Azure Virtual Desktop qui utilisent cette option. AD Connect doit être configuré et configuré de manière à être synchronisé avec Azure AD dans le cadre du processus de configuration.

  []

- Intégration dans un domaine Active Directory existant accessible à partir de l'abonnement Azure (généralement via Azure VPN ou Express route) et sa liste d'utilisateurs est synchronisée avec Azure AD à l'aide d'AD Connect ou d'un produit tiers.

  []

La couche de stockage

Dans AVD, la stratégie de stockage est conçue de manière à ce qu'aucune donnée utilisateur/entreprise persistante ne réside sur les machines virtuelles de session AVD. Les données persistantes des profils utilisateur, des fichiers et des dossiers utilisateur, ainsi que les données d'entreprise/d'application sont hébergées sur un ou plusieurs volumes de données hébergés sur une couche de données indépendante.

FSLogix est une technologie de conteneurisation de profil qui résout de nombreux problèmes de profil utilisateur (comme la prolifération des données et les connexions lentes) en montant un conteneur de profil utilisateur (format VHD ou VHDX) vers l'hôte de session lors de l'initialisation de la session.

Cette architecture exige donc une fonctionnalité de stockage des données. Cette fonction doit être capable de gérer le transfert de données nécessaire chaque matin/après-midi lorsqu'une partie importante de l'utilisateur se connecte/se déconnecter en même temps. Même les environnements de taille moyenne peuvent présenter des exigences importantes en termes de transfert de données. Les performances des disques de la couche de stockage des données font partie des variables principales de performances des utilisateurs finaux et il convient de veiller à ce que ces performances soient correctement ajoutées au stockage, et pas seulement au volume de stockage. En règle générale, la couche de stockage doit être dimensionnée pour prendre en charge 5-15 IOPS par utilisateur.

L'assistant d'installation VDS prend en charge les configurations suivantes :

- Installation et configuration de Azure NetApp Files (ANF) (recommandé). Le *niveau de service standard ANF prend en charge jusqu'à 150 utilisateurs, tandis que le type d'environnement ANF Premium est recommandé pour 150-500 utilisateurs. Pour plus de 500 utilisateurs, ANF Ultra est recommandé.*

  []

- Installation et configuration d'une machine virtuelle de serveur de fichiers

  []

Mise en réseau

Requis : un inventaire de tous les sous-réseaux de réseau existants, y compris les sous-réseaux visibles par l'abonnement Azure via une route Azure Express ou un VPN. Le déploiement doit éviter le chevauchement des sous-réseaux.

L'assistant de configuration VDS vous permet de définir l'étendue du réseau au cas où une plage est requise ou doit être évitée, dans le cadre de l'intégration planifiée avec les réseaux existants.

Déterminez une plage IP pour l'utilisateur pendant votre déploiement. Conformément aux bonnes pratiques Azure, seules les adresses IP d'une plage privée sont prises en charge.

Les choix pris en charge incluent les options suivantes, mais la plage /20 par défaut :

- 192.168.0.0 à 192.168.255.255
- 172.16.0.0 à 172.31.255.255
- 10.0.0.0 à 10.255.255.255

CWMGR1

Certaines des capacités uniques de VDS, telles que la planification des coûts réduits des charges de travail et la fonctionnalité Live Scaling, requièrent une présence administrative au sein du locataire et de l'abonnement. Par conséquent, une VM administrative appelée CWMGR1 est déployée dans le cadre de l'automatisation de l'assistant d'installation VDS. Outre les tâches d'automatisation VDS, cette machine virtuelle contient également la configuration VDS dans une base de données SQL Express, les fichiers journaux locaux et un utilitaire de configuration avancée appelé DCConfig.

En fonction des sélections effectuées dans l'assistant de configuration VDS, cette machine virtuelle peut être utilisée pour héberger des fonctionnalités supplémentaires, notamment :

- Passerelle RDS (utilisée uniquement dans les déploiements RDS)
- Une passerelle HTML 5 (utilisée uniquement dans les déploiements RDS)
- Un serveur de licences RDS (utilisé uniquement dans les déploiements RDS)
- Un contrôleur de domaine (si choisi)

Arbre de décision dans l'assistant de déploiement

Dans le cadre du déploiement initial, il vous est répondu de plusieurs questions afin de personnaliser les paramètres du nouvel environnement. Vous trouverez ci-dessous un aperçu des principales décisions à prendre.

Région Azure

Choisissez la ou les régions Azure qui hébergera vos machines virtuelles AVD. Notez que Azure NetApp Files et certaines familles de VM (machines virtuelles compatibles avec les GPU, par exemple) disposent d'une liste de prise en charge de régions Azure définie, tandis que l'AVD est disponible dans la plupart des régions.

- Ce lien peut être utilisé pour identifier "Disponibilité des produits Azure par région"

Type Active Directory

Choisissez le type Active Directory que vous souhaitez utiliser :

- Active Directory déjà en place
- Reportez-vous à la "Composants et autorisations AVD VDS" Document pour obtenir une explication des autorisations et des composants requis dans l'environnement Azure et Active Directory local
- Nouvelle instance Active Directory basée sur un abonnement Azure
- Services de domaine Azure Active Directory

Stockage des données

Déterminez l'emplacement de stockage des données des profils utilisateur, des fichiers individuels et des partages de l'entreprise. Les choix possibles sont :

- Azure NetApp Files
- Azure Files
- Serveur de fichiers classique (machine virtuelle Azure avec disque géré)

Conditions de déploiement de NetApp VDS pour les composants existants

Déploiement NetApp VDS avec les contrôleurs de domaine Active Directory existants

Ce type de configuration étend un domaine Active Directory existant pour prendre en charge l'instance AVD. Dans ce cas, VDS déploie un ensemble limité de composants dans le domaine afin de prendre en charge les tâches de provisionnement et de gestion automatiques des composants AVD.

Cette configuration nécessite :

- Un contrôleur de domaine Active Directory existant accessible par les machines virtuelles sur Azure VNet, généralement via un VPN Azure ou Express route OU un contrôleur de domaine créé dans Azure.
- Ajout de composants VDS et autorisations nécessaires à la gestion VDS des pools hôtes AVD et des volumes de données lors de leur adhésion au domaine. Le guide composants et autorisations VDS AVD définit les composants et autorisations requis et le processus de déploiement requiert un utilisateur de domaine disposant de privilèges de domaine pour exécuter le script qui créera les éléments nécessaires.
- Notez que le déploiement VDS crée un vnet par défaut pour les machines virtuelles créées par VDS. Vous pouvez soit utiliser VNet avec des VNets de réseau Azure existants, soit déplacer la machine virtuelle CWMGR1 vers un VNet existant avec les sous-réseaux requis prédéfinis.

Informations d'identification et outil de préparation de domaine

Les administrateurs doivent fournir des informations d'identification d'administrateur de domaine à un moment donné du processus de déploiement. Une information d'identification temporaire de l'administrateur de domaine peut être créée, utilisée et supprimée ultérieurement (une fois le processus de déploiement terminé). Les clients qui ont besoin d'aide pour l'élaboration des prérequis peuvent également utiliser l'outil de préparation du domaine.

Déploiement NetApp VDS avec un système de fichiers existant

VDS crée des partages Windows qui permettent l'accès aux profils utilisateur, aux dossiers personnels et aux données d'entreprise à partir des machines virtuelles de session AVD. VDS déploiera les options serveur de fichiers ou Azure NetApp File par défaut, mais si vous disposez d'un composant de stockage de fichiers existant VDS peut désigner les partages sur ce composant une fois le déploiement VDS terminé.

Conditions requises pour l'utilisation de et du composant de stockage existant :

- Le composant doit prendre en charge SMB v3
- Le composant doit être joint au même domaine Active Directory que les hôtes de session AVD
- Le composant doit pouvoir exposer un chemin UNC à utiliser dans la configuration VDS ; un chemin peut être utilisé pour les trois partages ou des chemins distincts peuvent être spécifiés pour chacun. Notez que VDS définit les autorisations de niveau utilisateur sur ces partages. Il fait donc référence au document composants AVD VDS et autorisations afin de s'assurer que les autorisations appropriées ont été accordées aux services d'automatisation VDS.

Déploiement NetApp VDS avec les services de domaine Azure AD existants

Cette configuration nécessite un processus pour identifier les attributs de l'instance de services de domaine Azure Active Directory existante. Contactez votre gestionnaire de compte pour demander le déploiement de ce type. Déploiement NetApp VDS avec un déploiement AVD existant ce type de configuration suppose que les composants Azure VNet, Active Directory et AVD nécessaires existent déjà. Le déploiement VDS est effectué de la même manière que la configuration « déploiement VDS NetApp avec AD existante », mais ajoute les conditions suivantes :

- LE RÔLE de propriétaire du locataire AVD doit être accordé aux applications VDS Enterprise dans Azure
- Les machines virtuelles du pool hôte AVD et du pool hôte AVD doivent être importées dans VDS à l'aide de la fonction d'importation VDS dans l'application Web VDS Ce processus collecte les métadonnées du pool hôte AVD et de la VM de session et les stocke dans ce VDS afin que ces éléments puissent être gérés par VDS
- Les données utilisateur AVD doivent être importées dans la section utilisateur VDS à l'aide de l'outil ARC. Ce processus insère les métadonnées relatives à chaque utilisateur dans le plan de contrôle VDS afin que les informations relatives à l'adhésion au groupe d'applications AVD et à la session puissent être gérées par VDS

ANNEXE A : adresses IP et URL du plan de contrôle VDS

Les composants VDS de l'abonnement Azure communiquent avec les composants du plan de contrôle global VDS tels que l'application Web VDS et les points de terminaison de l'API VDS. Pour l'accès, les adresses URI de base suivantes doivent être safelistées pour un accès bidirectionnel sur le port 443 :

"" "" "" "" "" ""

Si votre dispositif de contrôle d'accès ne peut afficher que la liste de sécurité par adresse IP, la liste d'adresses IP suivante doit être sécurisée. Notez que VDS utilise le service Azure Traffic Manager. Cette liste peut donc changer au fil du temps :

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

ANNEXE B : configuration requise pour Microsoft AVD

Cette section de configuration requise pour Microsoft AVD récapitule les exigences AVD de Microsoft. Les exigences AVD complètes et actuelles sont disponibles ici :

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

Licence hôte pour la session Azure Virtual Desktop

Azure Virtual Desktop prend en charge les systèmes d'exploitation suivants, alors assurez-vous que vous disposez des licences appropriées pour vos utilisateurs en fonction du poste de travail et des applications que vous envisagez de déployer :

OS	Licence requise
Multi-session Windows 10 Enterprise ou Windows 10 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3 et A5

OS	Licence requise
Windows 7 entreprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3 et A5
Windows Server 2012 R2, 2016 et 2019	Licence d'accès client (CAL) RDS avec assurance logicielle

Accès à l'URL pour les machines AVD

Les machines virtuelles Azure que vous créez pour Azure Virtual Desktop doivent avoir accès aux URL suivantes :

Adresse	Port TCP sortant	Objectif	Numéro de service
*.AVD.microsoft.com	443	Trafic de service	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Mises à jour de l'agent et de la pile SXS	AzureCloud
*.core.windows.net	443	Trafic des agents	AzureCloud
*.servicebus.windows.net	443	Trafic des agents	AzureCloud
prod.warmpath.msftcloudes.com	443	Trafic des agents	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Activation de Windows	Internet
AVDportalstorageblob.blob.core.windows.net	443	Prise en charge du portail Azure	AzureCloud

Le tableau suivant répertorie les URL facultatives auxquelles vos machines virtuelles Azure peuvent accéder :

Adresse	Port TCP sortant	Objectif	Numéro de service
*.microsoftonline.com	443	Authentification aux services MS Online	Aucune
*.events.data.microsoft.com	443	Service de télémétrie	Aucune
www.msftconnecttest.com	443	Détecte si le système d'exploitation est connecté à Internet	Aucune
*.prod.do.dsp.mp.microsoft.com	443	Mise à jour Windows	Aucune
login.windows.net	443	Connectez-vous à MS Online Services, Office 365	Aucune
*.sfx.ms	443	Mises à jour du logiciel client OneDrive	Aucune

Adresse	Port TCP sortant	Objectif	Numéro de service
*.digicert.com	443	Vérification de révocation du certificat	Aucune

Facteurs de performance optimaux

Pour des performances optimales, assurez-vous que votre réseau répond aux exigences suivantes :

- La latence aller-retour du réseau du client vers la région Azure où les pools hôtes ont été déployés doit être inférieure à 150 ms.
- Le trafic réseau peut circuler en dehors des frontières du pays ou de la région lorsque les machines virtuelles hébergeant des postes de travail et des applications se connectent au service de gestion.
- Pour optimiser les performances du réseau, nous recommandons que les machines virtuelles de l'hôte de session soient situées dans la même région Azure que le service de gestion.

Images du système d'exploitation des machines virtuelles prises en charge

Azure Virtual Desktop prend en charge les images du système d'exploitation x64 suivantes :

- Multi-session Windows 10 Enterprise, version 1809 ou ultérieure
- Windows 10 Enterprise, version 1809 ou ultérieure
- Windows 7 entreprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop ne prend pas en charge les images du système d'exploitation x86 (32 bits), Windows 10 Enterprise N ou Windows 10 Enterprise KN. Windows 7 ne prend pas non plus en charge les solutions de profils VHD ou VHDX hébergées sur un stockage Azure géré en raison d'une limitation de taille de secteur.

Les options disponibles d'automatisation et de déploiement dépendent du système d'exploitation et de la version que vous sélectionnez, comme l'illustre le tableau suivant :

Système d'exploitation	Galerie d'images Azure	Déploiement manuel de VM	Intégration des modèles ARM	Provisionnement de pools hôtes sur Azure Marketplace
Windows 10 multi-session, version 1903	Oui.	Oui.	Oui.	Oui.
Windows 10 multi-session, version 1809	Oui.	Oui.	Non	Non
Windows 10 Enterprise, version 1903	Oui.	Oui.	Oui.	Oui.
Windows 10 Enterprise, version 1809	Oui.	Oui.	Non	Non
Windows 7 entreprise	Oui.	Oui.	Non	Non
Windows Server 2019	Oui.	Oui.	Non	Non
Windows Server 2016	Oui.	Oui.	Oui.	Oui.

Système d'exploitation	Galerie d'images Azure	Déploiement manuel de VM	Intégration des modèles ARM	Provisionnement de pools hôtes sur Azure Marketplace
Windows Server 2012 R2	Oui.	Oui.	Non	Non

Conditions préalables AVD et VDS v6.0

Exigences et notes AVD et VDS

Ce document décrit les éléments requis pour déployer Azure Virtual Desktop (AVD) à l'aide de NetApp Virtual Desktop Service (VDS). La « liste de contrôle rapide » fournit une brève liste des composants requis et des étapes de pré-déploiement à suivre pour assurer un déploiement efficace. Le reste du guide fournit des détails plus détaillés sur chaque élément, en fonction des choix de configuration effectués.

Liste de contrôle rapide

Exigences d'Azure

- Locataire Azure AD
- Licence Microsoft 365 pour la prise en charge d'AVD
- Abonnement Azure
- Il existe un quota Azure disponible pour les machines virtuelles Azure
- Compte d'administrateur Azure avec rôles de propriété d'administrateur global et d'abonnement
- Compte d'administrateur de domaine avec rôle d'administrateur d'entreprise pour la configuration d'AD Connect

Informations de prédéploiement

- Déterminez le nombre total d'utilisateurs
- Déterminer la région Azure
- Déterminez le type Active Directory
- Déterminer le type de stockage
- Identifier l'image ou les besoins de la session hôte de la machine virtuelle
- Évaluer la configuration réseau Azure et sur site en place

Exigences détaillées relatives au déploiement VDS

Exigences de connexion de l'utilisateur final

Les clients Remote Desktop suivants prennent en charge Azure Virtual Desktop :

- Bureau Windows
- Web
- Mac OS
- E-S

- IGEL think client (Linux)
- Android (aperçu)

Azure Virtual Desktop ne prend pas en charge le client RemoteApp and Desktop Connections (RADC) ou le client Remote Desktop Connection (MSTSC).

Azure Virtual Desktop ne prend pas actuellement en charge le client Remote Desktop à partir du Windows Store. La prise en charge de ce client sera ajoutée dans une version ultérieure.

Les clients Bureau à distance doivent avoir accès aux URL suivantes :

Adresse	Port TCP sortant	Objectif	Client(s)
*.wvd.microsoft.com	443	Trafic de service	Tout
*.servicebus.windows.net	443	Données de dépannage	Tout
go.microsoft.com	443	Microsoft FWLinks	Tout
aka.ms	443	Shortener URL Microsoft	Tout
docs.microsoft.com	443	Documentation	Tout
privacy.microsoft.com	443	Déclaration de confidentialité	Tout
query.prod.cms.rt.microsoft.com	443	Mises à jour du client	Bureau Windows

L’ouverture de ces URL est essentielle pour une expérience client fiable. Le blocage de l’accès à ces URL n’est pas pris en charge et affecte la fonctionnalité de service. Ces URL correspondent uniquement aux sites et ressources client, et n’incluent pas les URL pour d’autres services tels qu’Azure Active Directory.

Point de départ de l’assistant de configuration VDS

L’assistant d’installation VDS peut gérer la plupart des configurations préalables requises pour un déploiement AVD réussi. L’assistant de configuration ("") crée ou utilise les composants suivants.

Locataire Azure

Requis : un locataire Azure et Azure Active Directory

L’activation d’AVD dans Azure est un paramètre défini pour l’ensemble du locataire. VDS prend en charge l’exécution d’une instance AVD par locataire.

Abonnement Azure

Requis : un abonnement Azure (notez l’ID d’abonnement que vous souhaitez utiliser)

Toutes les ressources Azure déployées doivent être configurées dans un abonnement dédié. Le suivi des coûts pour AVD est donc beaucoup plus facile et simplifie le processus de déploiement. REMARQUE : les essais gratuits Azure ne sont pas pris en charge car ils ne disposent pas de crédits suffisants pour déployer un déploiement AVD fonctionnel.

Le quota core Azure

Un quota suffisant pour les familles de machines virtuelles que vous utiliserez, en particulier au moins 10 cœurs de la famille DS v3 pour le déploiement initial des plateformes (2 cœurs maximum peuvent être utilisés, mais 10 couvre chaque déploiement initial).

Compte d'administrateur Azure

Requis: un compte administrateur global Azure.

L'assistant de configuration VDS demande à l'administrateur Azure d'accorder des autorisations déléguées au principal de service VDS et d'installer l'application VDS Azure Enterprise. L'administrateur doit avoir les rôles Azure suivants attribués :

- Administrateur global du locataire
- Rôle de propriétaire dans l'abonnement

Image de VM

Requis : une image Azure prenant en charge Windows 10 multi-session.

Azure Marketplace fournit les versions les plus récentes de leur image Windows 10 de base et tous les abonnements Azure y ont accès automatiquement. Si vous souhaitez utiliser une image différente ou une image personnalisée, demandez à l'équipe VDS de nous donner des conseils sur la création ou la modification d'autres images ou si des questions générales sur les images Azure nous en laissent savoir plus et nous pouvons planifier une conversation.

Active Directory

AVD nécessite que l'identité de l'utilisateur fasse partie d'Azure AD et que les VM soient joints à un domaine Active Directory synchronisé avec cette même instance AD Azure. Les machines virtuelles ne peuvent pas être directement connectées à l'instance Azure AD. Ainsi, un contrôleur de domaine doit être configuré et synchronisé avec Azure AD.

Ces options prises en charge sont les suivantes :

- Construction automatisée d'une instance Active Directory dans l'abonnement. L'instance AD est généralement créée par VDS sur la machine virtuelle de contrôle VDS (CWMGR1) pour les déploiements Azure Virtual Desktop qui utilisent cette option. AD Connect doit être configuré et configuré de manière à être synchronisé avec Azure AD dans le cadre du processus de configuration.

  []

- Intégration dans un domaine Active Directory existant accessible à partir de l'abonnement Azure (généralement via Azure VPN ou Express route) et sa liste d'utilisateurs est synchronisée avec Azure AD à l'aide d'AD Connect ou d'un produit tiers.

  []

La couche de stockage

Dans AVD, la stratégie de stockage est conçue de manière à ce qu'aucune donnée utilisateur/entreprise persistante ne réside sur les machines virtuelles de session AVD. Les données persistantes des profils utilisateur, des fichiers et des dossiers utilisateur, ainsi que les données d'entreprise/d'application sont hébergées sur un ou plusieurs volumes de données hébergés sur une couche de données indépendante.

FSLogix est une technologie de conteneurisation de profil qui résout de nombreux problèmes de profil utilisateur (comme la prolifération des données et les connexions lentes) en montant un conteneur de profil utilisateur (format VHD ou VHDX) vers l'hôte de session lors de l'initialisation de la session.

Cette architecture exige donc une fonctionnalité de stockage des données. Cette fonction doit être capable de gérer le transfert de données nécessaire chaque matin/après-midi lorsqu'une partie importante de l'utilisateur se connecte/se déconnecter en même temps. Même les environnements de taille moyenne peuvent présenter des exigences importantes en termes de transfert de données. Les performances des disques de la couche de stockage des données font partie des variables principales de performances des utilisateurs finaux et il convient de veiller à ce que ces performances soient correctement ajoutées au stockage, et pas seulement au volume de stockage. En règle générale, la couche de stockage doit être dimensionnée pour prendre en charge 5-15 IOPS par utilisateur.

L'assistant d'installation VDS prend en charge les configurations suivantes :

- Installation et configuration de Azure NetApp Files (ANF) (recommandé). Le *niveau de service standard ANF prend en charge jusqu'à 150 utilisateurs, tandis que le type d'environnement ANF Premium est recommandé pour 150-500 utilisateurs. Pour plus de 500 utilisateurs, ANF Ultra est recommandé.*

  []

- Installation et configuration d'une machine virtuelle de serveur de fichiers

  []

Mise en réseau

Requis : un inventaire de tous les sous-réseaux de réseau existants, y compris les sous-réseaux visibles par l'abonnement Azure via une route Azure Express ou un VPN. Le déploiement doit éviter le chevauchement des sous-réseaux.

L'assistant de configuration VDS vous permet de définir l'étendue du réseau au cas où une plage est requise ou doit être évitée, dans le cadre de l'intégration planifiée avec les réseaux existants.

Déterminez une plage IP pour l'utilisateur pendant votre déploiement. Conformément aux bonnes pratiques Azure, seules les adresses IP d'une plage privée sont prises en charge.

Les choix pris en charge incluent les options suivantes, mais la plage /20 par défaut :

- 192.168.0.0 à 192.168.255.255
- 172.16.0.0 à 172.31.255.255
- 10.0.0.0 à 10.255.255.255

CWMGR1

Certaines des capacités uniques de VDS, telles que la planification des coûts réduits des charges de travail et la fonctionnalité Live Scaling, requièrent une présence administrative au sein du locataire et de l'abonnement. Par conséquent, une VM administrative appelée CWMGR1 est déployée dans le cadre de l'automatisation de l'assistant d'installation VDS. Outre les tâches d'automatisation VDS, cette machine virtuelle contient également la configuration VDS dans une base de données SQL Express, les fichiers journaux locaux et un utilitaire de configuration avancée appelé DCConfig.

En fonction des sélections effectuées dans l'assistant de configuration VDS, cette machine virtuelle peut être utilisée pour héberger des fonctionnalités supplémentaires, notamment :

- Passerelle RDS (utilisée uniquement dans les déploiements RDS)

- Une passerelle HTML 5 (utilisée uniquement dans les déploiements RDS)
- Un serveur de licences RDS (utilisé uniquement dans les déploiements RDS)
- Un contrôleur de domaine (si choisi)

Arbre de décision dans l'assistant de déploiement

Dans le cadre du déploiement initial, il vous est répondu de plusieurs questions afin de personnaliser les paramètres du nouvel environnement. Vous trouverez ci-dessous un aperçu des principales décisions à prendre.

Région Azure

Choisissez la ou les régions Azure qui hébergera vos machines virtuelles AVD. Notez que Azure NetApp Files et certaines familles de VM (machines virtuelles compatibles avec les GPU, par exemple) disposent d'une liste de prise en charge de régions Azure définie, tandis que l'AVD est disponible dans la plupart des régions.

- Ce lien peut être utilisé pour identifier "Disponibilité des produits Azure par région"

Type Active Directory

Choisissez le type Active Directory que vous souhaitez utiliser :

- Active Directory déjà en place
- Reportez-vous à la "Composants et autorisations AVD VDS" Document pour obtenir une explication des autorisations et des composants requis dans l'environnement Azure et Active Directory local
- Nouvelle instance Active Directory basée sur un abonnement Azure
- Services de domaine Azure Active Directory

Stockage des données

Déterminez l'emplacement de stockage des données des profils utilisateur, des fichiers individuels et des partages de l'entreprise. Les choix possibles sont :

- Azure NetApp Files
- Azure Files
- Serveur de fichiers classique (machine virtuelle Azure avec disque géré)

Conditions de déploiement de NetApp VDS pour les composants existants

Déploiement NetApp VDS avec les contrôleurs de domaine Active Directory existants

Ce type de configuration étend un domaine Active Directory existant pour prendre en charge l'instance AVD. Dans ce cas, VDS déploie un ensemble limité de composants dans le domaine afin de prendre en charge les tâches de provisionnement et de gestion automatiques des composants AVD.

Cette configuration nécessite :

- Un contrôleur de domaine Active Directory existant accessible par les machines virtuelles sur Azure VNet, généralement via un VPN Azure ou Express route OU un contrôleur de domaine créé dans Azure.
- Ajout de composants VDS et autorisations nécessaires à la gestion VDS des pools hôtes AVD et des volumes de données lors de leur adhésion au domaine. Le guide composants et autorisations VDS AVD définit les composants et autorisations requis et le processus de déploiement requiert un utilisateur de

domaine disposant de privilèges de domaine pour exécuter le script qui créera les éléments nécessaires.

- Notez que le déploiement VDS crée un vnet par défaut pour les machines virtuelles créées par VDS. Vous pouvez soit utiliser VNet avec des VNets de réseau Azure existants, soit déplacer la machine virtuelle CWMGR1 vers un VNet existant avec les sous-réseaux requis prédéfinis.

Informations d'identification et outil de préparation de domaine

Les administrateurs doivent fournir des informations d'identification d'administrateur de domaine à un moment donné du processus de déploiement. Une information d'identification temporaire de l'administrateur de domaine peut être créée, utilisée et supprimée ultérieurement (une fois le processus de déploiement terminé). Les clients qui ont besoin d'aide pour l'élaboration des prérequis peuvent également utiliser l'outil de préparation du domaine.

Déploiement NetApp VDS avec un système de fichiers existant

VDS crée des partages Windows qui permettent l'accès aux profils utilisateur, aux dossiers personnels et aux données d'entreprise à partir des machines virtuelles de session AVD. VDS déploiera les options serveur de fichiers ou Azure NetApp File par défaut, mais si vous disposez d'un composant de stockage de fichiers existant VDS peut désigner les partages sur ce composant une fois le déploiement VDS terminé.

Conditions requises pour l'utilisation de et du composant de stockage existant :

- Le composant doit prendre en charge SMB v3
- Le composant doit être joint au même domaine Active Directory que les hôtes de session AVD
- Le composant doit pouvoir exposer un chemin UNC à utiliser dans la configuration VDS ; un chemin peut être utilisé pour les trois partages ou des chemins distincts peuvent être spécifiés pour chacun. Notez que VDS définit les autorisations de niveau utilisateur sur ces partages. Il fait donc référence au document composants AVD VDS et autorisations afin de s'assurer que les autorisations appropriées ont été accordées aux services d'automatisation VDS.

Déploiement NetApp VDS avec les services de domaine Azure AD existants

Cette configuration nécessite un processus pour identifier les attributs de l'instance de services de domaine Azure Active Directory existante. Contactez votre gestionnaire de compte pour demander le déploiement de ce type. Déploiement NetApp VDS avec un déploiement AVD existant ce type de configuration suppose que les composants Azure VNet, Active Directory et AVD nécessaires existent déjà. Le déploiement VDS est effectué de la même manière que la configuration « déploiement VDS NetApp avec AD existante », mais ajoute les conditions suivantes :

- LE RÔLE de propriétaire du locataire AVD doit être accordé aux applications VDS Enterprise dans Azure
- Les machines virtuelles du pool hôte AVD et du pool hôte AVD doivent être importées dans VDS à l'aide de la fonction d'importation VDS dans l'application Web VDS Ce processus collecte les métadonnées du pool hôte AVD et de la VM de session et les stocke dans ce VDS afin que ces éléments puissent être gérés par VDS
- Les données utilisateur AVD doivent être importées dans la section utilisateur VDS à l'aide de l'outil ARC. Ce processus insère les métadonnées relatives à chaque utilisateur dans le plan de contrôle VDS afin que les informations relatives à l'adhésion au groupe d'applications AVD et à la session puissent être gérées par VDS

ANNEXE A : adresses IP et URL du plan de contrôle VDS

Les composants VDS de l'abonnement Azure communiquent avec les composants du plan de contrôle global VDS tels que l'application Web VDS et les points de terminaison de l'API VDS. Pour l'accès, les adresses URI

de base suivantes doivent être safelistées pour un accès bidirectionnel sur le port 443 :

"" "" "" "" ""

Si votre dispositif de contrôle d'accès ne peut afficher que la liste de sécurité par adresse IP, la liste d'adresses IP suivante doit être sécurisée. Notez que VDS utilise le service Azure Traffic Manager. Cette liste peut donc changer au fil du temps :

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

ANNEXE B : configuration requise pour Microsoft AVD

Cette section de configuration requise pour Microsoft AVD récapitule les exigences AVD de Microsoft. Les exigences AVD complètes et actuelles sont disponibles ici :

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

Licence hôte pour la session Azure Virtual Desktop

Azure Virtual Desktop prend en charge les systèmes d'exploitation suivants, alors assurez-vous que vous disposez des licences appropriées pour vos utilisateurs en fonction du poste de travail et des applications que vous envisagez de déployer :

OS	Licence requise
Multi-session Windows 10 Enterprise ou Windows 10 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3 et A5
Windows 7 entreprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3 et A5
Windows Server 2012 R2, 2016 et 2019	Licence d'accès client (CAL) RDS avec assurance logicielle

Accès à l'URL pour les machines AVD

Les machines virtuelles Azure que vous créez pour Azure Virtual Desktop doivent avoir accès aux URL suivantes :

Adresse	Port TCP sortant	Objectif	Numéro de service
*.AVD.microsoft.com	443	Trafic de service	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Mises à jour de l'agent et de la pile SXS	AzureCloud
*.core.windows.net	443	Trafic des agents	AzureCloud
*.servicebus.windows.net	443	Trafic des agents	AzureCloud
prod.warmpath.msftcloudes.com	443	Trafic des agents	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud

Adresse	Port TCP sortant	Objectif	Numéro de service
kms.core.windows.net	1688	Activation de Windows	Internet
AVDportalstorageblob.blob.core.windows.net	443	Prise en charge du portail Azure	AzureCloud

Le tableau suivant répertorie les URL facultatives auxquelles vos machines virtuelles Azure peuvent accéder :

Adresse	Port TCP sortant	Objectif	Numéro de service
*.microsoftonline.com	443	Authentification aux services MS Online	Aucune
*.events.data.microsoft.com	443	Service de télémétrie	Aucune
www.msftconnecttest.com	443	Détecte si le système d'exploitation est connecté à Internet	Aucune
*.prod.do.dsp.mp.microsoft.com	443	Mise à jour Windows	Aucune
login.windows.net	443	Connectez-vous à MS Online Services, Office 365	Aucune
*.sfx.ms	443	Mises à jour du logiciel client OneDrive	Aucune
*.digicert.com	443	Vérification de révocation du certificat	Aucune

Facteurs de performance optimaux

Pour des performances optimales, assurez-vous que votre réseau répond aux exigences suivantes :

- La latence aller-retour du réseau du client vers la région Azure où les pools hôtes ont été déployés doit être inférieure à 150 ms.
- Le trafic réseau peut circuler en dehors des frontières du pays ou de la région lorsque les machines virtuelles hébergeant des postes de travail et des applications se connectent au service de gestion.
- Pour optimiser les performances du réseau, nous recommandons que les machines virtuelles de l'hôte de session soient situées dans la même région Azure que le service de gestion.

Images du système d'exploitation des machines virtuelles prises en charge

Azure Virtual Desktop prend en charge les images du système d'exploitation x64 suivantes :

- Multi-session Windows 10 Enterprise, version 1809 ou ultérieure
- Windows 10 Enterprise, version 1809 ou ultérieure
- Windows 7 entreprise
- Windows Server 2019
- Windows Server 2016

- Windows Server 2012 R2

Azure Virtual Desktop ne prend pas en charge les images du système d'exploitation x86 (32 bits), Windows 10 Enterprise N ou Windows 10 Enterprise KN. Windows 7 ne prend pas non plus en charge les solutions de profils VHD ou VHDX hébergées sur un stockage Azure géré en raison d'une limitation de taille de secteur.

Les options disponibles d'automatisation et de déploiement dépendent du système d'exploitation et de la version que vous sélectionnez, comme l'illustre le tableau suivant :

Système d'exploitation	Galerie d'images Azure	Déploiement manuel de VM	Intégration des modèles ARM	Provisionnement de pools hôtes sur Azure Marketplace
Windows 10 multi-session, version 1903	Oui.	Oui.	Oui.	Oui.
Windows 10 multi-session, version 1809	Oui.	Oui.	Non	Non
Windows 10 Enterprise, version 1903	Oui.	Oui.	Oui.	Oui.
Windows 10 Enterprise, version 1809	Oui.	Oui.	Non	Non
Windows 7 entreprise	Oui.	Oui.	Non	Non
Windows Server 2019	Oui.	Oui.	Non	Non
Windows Server 2016	Oui.	Oui.	Oui.	Oui.
Windows Server 2012 R2	Oui.	Oui.	Non	Non

Google

Guide de déploiement RDS pour Google Cloud (GCP)

Présentation

Ce guide fournit des instructions détaillées pour créer un déploiement RDS (Remote Desktop Service) à l'aide de NetApp Virtual Desktop Service (VDS) dans Google Cloud.

Ce guide de démonstration de faisabilité a été conçu pour vous aider à déployer et configurer rapidement RDS dans votre propre projet GCP.

Les déploiements de production, en particulier dans les environnements AD existants, sont très courants cependant que le processus n'est pas pris en compte dans ce guide POC. Les démonstrations de faisabilité et les déploiements de production complexes doivent être lancées avec les équipes commerciales/services VDS NetApp et ne sont pas exécutées en libre-service.

Ce document POC présente toute la durée du déploiement RDS et décrit brièvement les principaux éléments de la configuration post-déploiement disponible dans la plateforme VDS. Une fois terminé, vous aurez un environnement RDS entièrement déployé et fonctionnel, avec des hôtes de session, des applications et des utilisateurs. Vous aurez éventuellement la possibilité de configurer la distribution automatisée des applications, les groupes de sécurité, les autorisations de partage de fichiers, Cloud Backup, l'optimisation intelligente des coûts. VDS déploie un ensemble de paramètres des meilleures pratiques via GPO. Des instructions sur la désactivation facultative de ces contrôles sont également incluses, dans le cas où votre POC ne nécessite aucun contrôle de sécurité, similaire à un environnement de périphériques locaux non gérés.

Architecture de déploiement

[largeur=75 %]

Notions de base sur RDS

VDS déploie un environnement RDS entièrement fonctionnel et tous les services de prise en charge nécessaires depuis zéro. Elle peut inclure :

- Serveur(s) passerelle RDS
- Serveur(s) d'accès client Web
- Serveur(s) de contrôleur de domaine
- Service de licences RDS
- Service de licence ThinPrint
- Service serveur FitPS FileZilla

Portée du guide

Ce guide vous présente le déploiement de RDS à l'aide de la technologie NetApp VDS du point de vue de l'administrateur GCP et VDS. Ce guide vous aide à configurer le projet GCP sans aucune préconfiguration, et vous aide à configurer le service RDS de bout en bout

Créer un compte de service

1. Dans GCP, accédez à (ou recherchez) *IAM & Admin > comptes de service*

   []

2. CLIQUEZ SUR + *CRÉER UN COMPTE DE SERVICE*

   []

3. Entrez un nom de compte de service unique, puis cliquez sur *CREATE*. Notez l'adresse e-mail du compte de service qui sera utilisée ultérieurement.

   []

4. Sélectionnez le rôle *Owner* du compte de service, puis cliquez sur *CONTINUER*

   []

5. Aucune modification n'est nécessaire sur la page suivante (*accordez aux utilisateurs l'accès à ce compte de service(facultatif)*), cliquez sur *DONE*

   []

6. Dans la page *Service Accounts*, cliquez sur le menu d'action et sélectionnez *Create key*

   []

7. Sélectionnez *P12*, puis cliquez sur *CREATE*

   []

8. Téléchargez le fichier .P12 et enregistrez-le sur votre ordinateur. Le mot de passe de la clé privée est calé.

   []

   []

Activez l'API de calcul Google

1. Dans GCP, accédez à (ou recherchez) *API & Services > Library*

   []

2. Dans la bibliothèque API GCP, accédez à (ou recherchez) *Compute Engine API*, puis cliquez sur *ENABLE*

   []

Créer un nouveau déploiement VDS

1. Dans VDS, accédez à *déploiements* et cliquez sur + *New Deployment*

   []

2. Entrez un nom pour le déploiement

   []

3. Sélectionnez *Google Cloud Platform*

   []

La plateforme de l'infrastructure cloud

1. Saisissez l'ID de projet_ et l'adresse e-mail OAuth. Téléchargez le fichier .P12 à partir de la section précédente de ce guide et sélectionnez la zone appropriée pour ce déploiement. Cliquez sur *Test* pour confirmer que les entrées sont correctes et que les autorisations appropriées ont été définies.

   L'e-mail OAuth est l'adresse du compte de service créé précédemment dans ce guide.

   []

2. Une fois la confirmation terminée, cliquez sur *Continuer*

   []

Comptes

Comptes de VM locaux

1. Saisissez un mot de passe pour le compte administrateur local. Documentez ce mot de passe pour une utilisation ultérieure.
2. Saisissez un mot de passe pour le compte SQL sa. Documentez ce mot de passe pour une utilisation ultérieure.

La complexité du mot de passe nécessite un minimum de 8 caractères avec 3 des 4 types de caractères suivants : majuscules, minuscules, nombre, caractère spécial

Compte SMTP

VDS peut envoyer des notifications par e-mail via des paramètres SMTP personnalisés ou le service SMTP intégré peut être utilisé en sélectionnant *Automatic*.

1. Entrez une adresse e-mail à utiliser comme adresse *de* lorsque la notification par e-mail est envoyée par VDS. *no-réponse@<votre-domaine>.com* est un format commun.
2. Entrez une adresse e-mail à laquelle les rapports de réussite doivent être dirigés.
3. Entrez une adresse e-mail à laquelle les rapports d'échec doivent être dirigés.

[]

Techniciens de niveau 3

Comptes de technicien de niveau 3 (alias *.TECH Accounts*) sont des comptes au niveau domaine que les administrateurs VDS peuvent utiliser lors de l'exécution de tâches administratives sur les VM dans l'environnement VDS. Des comptes supplémentaires peuvent être créés pour cette étape et/ou ultérieure.

1. Saisissez le nom d'utilisateur et le mot de passe des comptes d'administrateur de niveau 3. «.tech » sera ajouté au nom d'utilisateur que vous entrez pour vous aider à différencier des utilisateurs finaux et des comptes techniques. Documentez ces informations d'identification pour une utilisation ultérieure.

   La meilleure pratique consiste à définir des comptes nommés pour tous les administrateurs VDS devant disposer d'identifiants au niveau du domaine dans l'environnement. Les administrateurs VDS sans ce type de compte peuvent toujours disposer d'un accès administrateur au niveau des VM via la fonctionnalité *Connect to Server* intégrée dans VDS.

   []

Domaines

Répertoire actif

Entrez le nom de domaine AD souhaité.

Domaine public

L'accès externe est sécurisé par le biais d'un certificat SSL. Ceci peut être personnalisé avec votre propre domaine et un certificat SSL auto-géré. Vous pouvez également sélectionner *Automatic* pour permettre à VDS de gérer le certificat SSL, y compris une actualisation automatique de 90 jours du certificat. Lors de l'utilisation automatique, chaque déploiement utilise un sous-domaine unique de *cloudWorkspace.app*.

[]

Ordinateurs virtuels

Pour les déploiements RDS, les composants requis, tels que les contrôleurs de domaine, les courtiers RDS et les passerelles RDS, doivent être installés sur le ou les serveurs de plateforme. En production, ces services doivent être exécutés sur des machines virtuelles dédiées et redondantes. Pour les déploiements de

démonstration de faisabilité, une seule machine virtuelle peut être utilisée pour héberger l'ensemble de ces services.

Configuration des machines virtuelles de la plateforme

Une seule machine virtuelle

C'est ce choix recommandé pour les déploiements POC. Dans un déploiement à une seule machine virtuelle, les rôles suivants sont tous hébergés sur une seule machine virtuelle :

- Gestionnaire CW
- Passerelle HTML5
- Passerelle RDS
- Application distante
- Serveur FTPS (en option)
- Contrôleur de domaine

Dans cette configuration, le nombre maximal d'utilisateurs conseillé pour les cas d'utilisation de RDS est de 100 utilisateurs. Les passerelles RDS/HTML5 à équilibrage de charge ne sont pas une option proposée dans cette configuration, limitant ainsi la redondance et les options d'augmentation de l'évolutivité future.

Si cet environnement est conçu pour la colocation, une configuration de serveur virtuel unique n'est pas prise en charge.

Serveurs multiples

Lors du fractionnement de la plateforme VDS en plusieurs machines virtuelles, les rôles suivants sont hébergés sur des machines virtuelles dédiées :

- Passerelle Bureau à distance

  Le réglage VDS peut être utilisé pour déployer et configurer une ou deux passerelles RDS. Ces passerelles relaient la session utilisateur RDS depuis l'Internet ouvert vers les machines virtuelles hôte de session au sein du déploiement. Les passerelles RDS gèrent une fonction importante, protégeant ainsi RDS des attaques directes sur Internet et cryptant l'ensemble du trafic RDS dans/hors de l'environnement. Lorsque deux passerelles Remote Desktop sont sélectionnées, VDS Setup déploie 2 machines virtuelles et les configure pour équilibrer la charge des sessions utilisateur RDS entrantes.

- Passerelle HTML5

  L'installation VDS peut être utilisée pour déployer et configurer une ou deux passerelles HTML5. Ces passerelles hébergent les services HTML5 utilisés par la fonction *Connect to Server* dans VDS et le client VDS basé sur le Web (H5 Portal). Lorsque deux portails HTML5 sont sélectionnés, le programme d'installation VDS déploie 2 machines virtuelles et les configure pour équilibrer la charge des sessions utilisateur HTML5 entrantes.

  

  Lors de l'utilisation de l'option de serveur multiple (même si les utilisateurs se connectent uniquement via le client VDS installé), il est fortement recommandé d'activer la fonctionnalité *Connect to Server* de VDS au moins une passerelle HTML5.

- Notes relatives à l'évolutivité des passerelles

Dans le cas d'une solution RDS, la taille maximale de l'environnement peut être mise à l'échelle avec d'autres VM de passerelle, chaque passerelle RDS ou HTML5 prenant en charge environ 500 utilisateurs. Des passerelles supplémentaires peuvent être ajoutées ultérieurement avec une assistance minimale aux services professionnels NetApp

Si cet environnement est conçu pour la colocation, la sélection de *plusieurs serveurs* est requise.

Rôles de service

- Cwmgr1

  Ce VM correspond à la machine virtuelle d'administration VDS NetApp. Il exécute la base de données SQL Express, les utilitaires d'aide et d'autres services administratifs. Dans un *déploiement serveur* unique, cette machine virtuelle peut également héberger les autres services, mais dans une *configuration serveur* multiple, ces services sont déplacés vers différentes machines virtuelles.

- CWPortal1 (2)

  La première passerelle HTML5 s'appelle *CWPortal1*, la seconde est *CWPortal2*. Un ou deux peuvent être créés au moment du déploiement. Des serveurs supplémentaires peuvent être ajoutés après déploiement pour augmenter la capacité (environ 500 connexions par serveur).

- CWRDSGateway1(2)

  La première passerelle RDS est nommée *CWRDSGateway1*, la seconde est *CWRDSGateway2*. Un ou deux peuvent être créés au moment du déploiement. Des serveurs supplémentaires peuvent être ajoutés après déploiement pour augmenter la capacité (environ 500 connexions par serveur).

- Application distante

  App Service est une collection dédiée pour l'hébergement d'applications RemotApp, mais utilise les passerelles RDS et leurs rôles RDWeb pour le routage des demandes de session utilisateur final et l'hébergement de la liste d'abonnement aux applications RDWeb. Aucune vm dédiée n'est déployée pour ce rôle de service.

- Contrôleurs de domaine

  Au déploiement, un ou deux contrôleurs de domaine peuvent être automatiquement créés et configurés pour fonctionner avec VDS.

[]

Système d'exploitation

Sélectionnez le système d'exploitation de serveur à déployer pour les serveurs de plate-forme.

Fuseau horaire

Sélectionnez le fuseau horaire souhaité. Les serveurs de plate-forme seront configurés pour cette heure et les fichiers journaux refléteront ce fuseau horaire. La session de l'utilisateur final reflètera toujours son propre fuseau horaire, indépendamment de ce paramètre.

Services supplémentaires

FTP

VDS peut installer et configurer Filezilla en option afin d'exécuter un serveur FTPS pour déplacer des données dans et hors de l'environnement. Cette technologie est plus ancienne et des méthodes de transfert de données plus modernes (comme Google Drive) sont recommandées.

[]

Le réseau

Il est recommandé d'isoler les machines virtuelles dans différents sous-réseaux en fonction de leur usage.

Définissez la portée du réseau et ajoutez une plage /20.

Le programme d'installation VDS détecte et suggère une plage qui devrait s'avérer efficace. Conformément aux bonnes pratiques, les adresses IP du sous-réseau doivent être comprises dans une plage d'adresses IP privées.

Ces plages sont :

- 192.168.0.0 à 192.168.255.255
- 172.16.0.0 à 172.31.255.255
- 10.0.0.0 à 10.255.255.255

Vérifiez et ajustez si nécessaire, puis cliquez sur Valider pour identifier les sous-réseaux pour chacun des éléments suivants :

- Tenant : il s'agit de la plage dans laquelle les serveurs hôtes de session et les serveurs de base de données résident
- Services : il s'agit de la plage dans laquelle les services PaaS comme Cloud Volumes Service résideront
- Plate-forme : il s'agit de la plage dans laquelle les serveurs de plate-forme seront hébergés
- Répertoire : il s'agit de la plage dans laquelle les serveurs AD résident

[]

Licences

NO SPLA

Saisissez votre numéro SPLA afin que VDS puisse configurer le service de licence RDS pour faciliter le reporting SPLA RDS CAL. Vous pouvez saisir un nombre temporaire (par exemple 12345) pour un déploiement POC, mais après une période d'essai (~120 jours), les sessions RDS cessent de se connecter.

Produits SPLA

Saisissez les codes de licence MAK pour tous les produits Office concédés sous licence par SPLA pour permettre la création simplifiée de rapports SPLA à partir des rapports VDS.

RéplicationFine

Choisissez d'installer le serveur de licences ThinPrint inclus et la licence pour simplifier la redirection des imprimantes des utilisateurs finaux.

[]

Révision et mise en service

Une fois toutes les étapes effectuées, examinez les sélections, puis validez et provisionnez l'environnement.[]

Étapes suivantes

Le processus d'automatisation du déploiement déploiera un nouvel environnement RDS avec les options que vous avez sélectionnées tout au long de l'assistant de déploiement.

Vous recevrez plusieurs e-mails à la fin du déploiement. Une fois terminé, vous aurez un environnement prêt pour votre premier espace de travail. Un espace de travail contiendra les hôtes de session et les serveurs de données nécessaires pour prendre en charge les utilisateurs finaux. Revenez à ce guide pour suivre les étapes suivantes une fois le déploiement automatisé terminé en 1-2 heures.

Créer une nouvelle collection d'approvisionnement

Les collections de provisionnement sont des fonctionnalités dans VDS qui permettent la création, la personnalisation et la représentation Sysprep des images de VM. Une fois le déploiement en milieu de travail effectué, une image est nécessaire. Les étapes suivantes vous guideront dans la création d'une image VM.

Pour créer une image de base pour le déploiement, procédez comme suit :

1. Accédez à *déploiements* > *Provisioning Collections*, puis cliquez sur *Add*

   []

2. Entrez un nom et une description. Choisissez *Type: Shared*.

   Vous pouvez choisir Shared ou VDI. Partagé prendra en charge un serveur de session plus (éventuellement) un serveur d'entreprise pour des applications telles qu'une base de données. L'infrastructure VDI est une image VM unique pour les machines virtuelles qui seront dédiées aux utilisateurs individuels.

3. Cliquez sur *Add* pour définir le type d'image du serveur à construire.

   []

4. Sélectionnez TSData comme le *Server role*, l'image VM appropriée (Server 2016 dans ce cas) et le type de stockage souhaité. Cliquez sur *Add Server*

   []

5. Sélectionnez éventuellement les applications qui seront installées sur cette image.
   a. La liste des applications disponibles est remplie à partir de la bibliothèque d'applications accessible en cliquant sur le menu du nom d'administrateur dans le coin supérieur droit, sous la page *Settings* > *App Catalog*.

      []

6. Cliquez sur *Add Collection* et attendez que la machine virtuelle soit créée. VDS crée une machine virtuelle accessible et personnalisée.
7. Une fois la compilation VM terminée, connectez-vous au serveur et apportez les modifications souhaitées.

    a. Une fois que l'état affiche *Collection validation*, cliquez sur le nom de la collection.

    []

    b. Cliquez ensuite sur le nom du modèle *Server*

    []

    c. Enfin, cliquez sur le bouton *Connect to Server* pour être connecté et automatiquement connecté à la machine virtuelle avec des informations d'identification d'administrateur local.

    []

    []

8. Une fois toutes les personnalisations terminées, cliquez sur *Validate Collection* pour que VDS puisse sysprep et finaliser l'image. Une fois cette opération terminée, la machine virtuelle sera supprimée et l'image sera disponible dans les assistants de déploiement VDS.

    []5

Créer un nouvel espace de travail

Un espace de travail est un ensemble d'hôtes de session et de serveurs de données qui prennent en charge un groupe d'utilisateurs. Ce déploiement peut contenir un seul espace de travail (un seul locataire) ou plusieurs espaces de travail (colocation).

Les espaces de travail définissent la collection du serveur RDS pour un groupe spécifique. Dans cet exemple, nous allons déployer une seule collection pour démontrer la fonctionnalité des postes de travail virtuels. Toutefois, le modèle peut être étendu à plusieurs espaces de travail/collections RDS afin de prendre en charge différents groupes et emplacements dans le même espace de domaine Active Directory. Les administrateurs peuvent éventuellement restreindre l'accès entre les espaces de travail/collections pour prendre en charge les cas d'utilisation exigeant un accès limité aux applications et aux données.

Client et paramètres

1. Dans NetApp VDS, accédez à *Workspaces* et cliquez sur *+ New Workspace*

    []

2. Cliquez sur *Ajouter* pour créer un nouveau client. Les détails du client représentent généralement les informations de l'entreprise ou les informations d'un emplacement ou d'un service spécifique.

    []

    a. Entrez les détails de l'entreprise et sélectionnez le déploiement dans lequel cet espace de travail sera déployé.

    b. **Lecteur de données :** définissez la lettre de lecteur à utiliser pour le lecteur mappé de partage de l'entreprise.

c. **User Home Drive:** définissez la lettre de lecteur à utiliser pour le lecteur mappé de l'individu.

d. **Paramètres supplémentaires**

Les paramètres suivants peuvent être définis au moment du déploiement et/ou sélectionnés après le déploiement.

i. *Activer l'application distante:* l'application distante présente les applications comme des applications de streaming au lieu (ou en plus) de présenter une session de bureau à distance complète.

ii. *Activer App Locker:* VDS contient les fonctionnalités de déploiement et d'attribution d'applications, le système affichera/masquera les applications aux utilisateurs finaux. L'activation d'App Locker force l'accès aux applications via une liste de sécurité GPO.

iii. *Activer le stockage des données utilisateur de l'espace de travail:* déterminer si les utilisateurs ont besoin d'un accès au stockage de données dans leur poste de travail virtuel. Pour les déploiements RDS, ce paramètre doit toujours être vérifié afin d'activer l'accès aux données pour les profils utilisateur.

iv. *Désactiver l'accès à l'imprimante:* VDS peut bloquer l'accès aux imprimantes locales.

v. *Autoriser l'accès au Gestionnaire des tâches :* VDS peut activer/désactiver l'accès de l'utilisateur final au Gestionnaire des tâches dans Windows.

vi. *Exiger un mot de passe d'utilisateur complexe :* la nécessité de mots de passe complexes active les règles de mot de passe complexes de Windows Server natives. Il désactive également le déverrouillage automatique différé des comptes utilisateur verrouillés. Par conséquent, lorsque cette option est activée, une intervention d'administrateur est requise lorsque les utilisateurs verrouillent leurs comptes avec plusieurs tentatives de mot de passe ayant échoué.

vii. *Activer MFA pour tous les utilisateurs :* VDS comprend un service MFA SMS/e-mail gratuit qui peut être utilisé pour sécuriser l'accès aux comptes utilisateur final et/ou administrateur VDS. L'activation de cette fonction nécessite que tous les utilisateurs finaux de cet espace de travail s'authentifient auprès de MFA pour accéder à leur bureau et/ou à leurs applications.

Choisissez des applications

Sélectionnez la version du système d'exploitation Windows et la collection de provisionnement créée précédemment dans ce guide.

Il est possible d'ajouter des applications supplémentaires à ce stade, mais pour ce POC, nous examinerons l'admissibilité aux applications après le déploiement.

[]

Ajouter des utilisateurs

Il est possible d'ajouter des utilisateurs en sélectionnant des groupes de sécurité AD existants ou des utilisateurs individuels. Dans ce guide POC, nous ajouterons des utilisateurs après le déploiement.

[]

Révision et mise en service

Sur la dernière page, passez en revue les options choisies et cliquez sur *provisioning* pour lancer la conception automatisée des ressources RDS.

[]

Au cours du processus de déploiement, des journaux sont créés et sont accessibles sous *Historique des tâches* en bas de la page Détails du déploiement. Accessible en accédant à *VDS > déploiements > Nom du déploiement*

Étapes suivantes

Le processus d'automatisation de l'environnement de travail déploie à présent de nouvelles ressources RDS avec les options que vous avez sélectionnées tout au long de l'assistant de déploiement.

Une fois le processus terminé, vous suivrez plusieurs flux de travail courants pour personnaliser le déploiement RDS classique.

- "Ajouter des utilisateurs"
- "Accès des utilisateurs finaux"
- "Droits des applications"
- "Optimisation des coûts"

Prérequis pour Google Compute Platform (GCP) et VDS

Exigences et notes de GCP et VDS

Ce document décrit les éléments requis pour le déploiement de services RDS (Remote Desktop Services) à l'aide de NetApp Virtual Desktop Service (VDS). La « liste de contrôle rapide » fournit une brève liste des composants requis et des étapes de pré-déploiement à suivre pour assurer un déploiement efficace. Le reste du guide fournit des détails plus détaillés sur chaque élément, en fonction des choix de configuration effectués.

[largeur=75 %]

Liste de contrôle rapide

Exigences GCP

- Locataire GCP
- Projet GCP
- Compte de service avec rôle propriétaire attribué

Informations de prédéploiement

- Déterminez le nombre total d'utilisateurs
- Déterminez la région et la zone GCP
- Déterminez le type de répertoire actif
- Déterminez le type de stockage
- Identifier l'image ou les besoins de la session hôte de la machine virtuelle
- Évaluation de la configuration réseau GCP et locale

Exigences détaillées relatives au déploiement VDS

Exigences de connexion de l'utilisateur final

Les clients de postes de travail à distance suivants prennent en charge RDS dans GCP :

- "Client NetApp VDS pour Windows"
  - Exigences de sécurité relatives aux url sortantes NetApp VDS pour Windows
    - api.cloudworkspace.com
    - vdsclient.app
    - api.vdsclient.app
    - bin.vdsclient.app
  - Fonctionnalités améliorées :
    - Réveil VDS à la demande
    - ThinPrint client et des poux
    - Réinitialisation du mot de passe en libre-service
    - Négociation automatique de l'adresse des serveurs et de la passerelle
    - Prise en charge complète des applications de bureau et de diffusion en continu
    - Marques personnalisées disponibles
    - Commutateurs du programme d'installation pour le déploiement et la configuration automatisés
    - Outils de dépannage intégrés
- "Client web NetApp VDS"
- "Client Microsoft RD"
  - Répertoires de base
  - Mac OS
  - ISO
  - Android
- logiciels tiers et/ou clients légers
  - Exigence : prise en charge de la configuration de la passerelle RD

La couche de stockage

Dans RDS déployé par VDS, la stratégie de stockage est conçue de sorte que les données utilisateur/entreprise persistantes ne résident pas sur les machines virtuelles de session AVD. Les données persistantes des profils utilisateur, des fichiers et des dossiers utilisateur, ainsi que les données d'entreprise/d'application sont hébergées sur un ou plusieurs volumes de données hébergés sur une couche de données indépendante.

FSLogix est une technologie de conteneurisation de profil qui résout de nombreux problèmes de profil utilisateur (comme la prolifération des données et les connexions lentes) en montant un conteneur de profil utilisateur (format VHD ou VHDX) vers l'hôte de session lors de l'initialisation de la session.

Cette architecture exige donc une fonctionnalité de stockage des données. Cette fonction doit être capable de gérer le transfert de données nécessaire chaque matin/après-midi lorsqu'une partie importante de l'utilisateur se connecte/se déconnecter en même temps. Même les environnements de taille moyenne peuvent présenter des exigences importantes en termes de transfert de données. Les performances des disques de la couche de stockage des données font partie des variables principales de performances des utilisateurs finaux et il

convient de veiller à ce que ces performances soient correctement ajoutées au stockage, et pas seulement au volume de stockage. En règle générale, la couche de stockage doit être dimensionnée pour prendre en charge 5-15 IOPS par utilisateur.

Mise en réseau

Requis : un inventaire de tous les sous-réseaux réseau existants, y compris les sous-réseaux visibles par le projet GCP via un VPN. Le déploiement doit éviter le chevauchement des sous-réseaux.

L'assistant de configuration VDS vous permet de définir l'étendue du réseau au cas où une plage est requise ou doit être évitée, dans le cadre de l'intégration planifiée avec les réseaux existants.

Déterminez une plage IP pour l'utilisateur pendant votre déploiement. Conformément aux bonnes pratiques, seules les adresses IP d'une plage privée sont prises en charge.

Les choix pris en charge incluent les options suivantes, mais la plage /20 par défaut :

- 192.168.0.0 à 192.168.255.255
- 172.16.0.0 à 172.31.255.255
- 10.0.0.0 à 10.255.255.255

CWMGR1

Certaines des capacités uniques de VDS, telles que la planification des charges de travail et la mise à l'échelle dynamique, requièrent une présence administrative au sein de l'organisation et du projet. Par conséquent, une VM administrative appelée CWMGR1 est déployée dans le cadre de l'automatisation de l'assistant d'installation VDS. Outre les tâches d'automatisation VDS, cette machine virtuelle contient également la configuration VDS dans une base de données SQL Express, les fichiers journaux locaux et un utilitaire de configuration avancée appelé DCConfig.

En fonction des sélections effectuées dans l'assistant de configuration VDS, cette machine virtuelle peut être utilisée pour héberger des fonctionnalités supplémentaires, notamment :

- Une passerelle RDS
- Une passerelle HTML 5
- Un serveur de licences RDS
- Un contrôleur de domaine

Arbre de décision dans l'assistant de déploiement

Dans le cadre du déploiement initial, il vous est répondu de plusieurs questions afin de personnaliser les paramètres du nouvel environnement. Vous trouverez ci-dessous un aperçu des principales décisions à prendre.

Région GCP

Déterminez la ou les régions GCP qui hébergera vos machines virtuelles VDS. Notez que la région doit être sélectionnée en fonction de la proximité des utilisateurs finaux et des services disponibles.

Stockage des données

Déterminez l'emplacement de stockage des données des profils utilisateur, des fichiers individuels et des partages de l'entreprise. Les choix possibles sont :

- Cloud Volumes Service pour GCP
- Serveur de fichiers traditionnel

Conditions de déploiement de NetApp VDS pour les composants existants

Déploiement NetApp VDS avec les contrôleurs de domaine Active Directory existants

Ce type de configuration étend un domaine Active Directory existant pour prendre en charge l'instance RDS. Dans ce cas, VDS déploie un ensemble limité de composants dans le domaine afin de prendre en charge les tâches de provisionnement et de gestion automatisées des composants RDS.

Cette configuration nécessite :

- Un contrôleur de domaine Active Directory existant accessible par les machines virtuelles sur le réseau VPC GCP, en général via un VPN ou un contrôleur de domaine créé dans GCP.
- Ajout de composants VDS et des autorisations nécessaires à la gestion VDS des hôtes RDS et des volumes de données lors de leur intégration au domaine. Le processus de déploiement nécessite un utilisateur de domaine disposant de privilèges de domaine pour exécuter le script qui créera les éléments nécessaires.
- Notez que le déploiement VDS crée un réseau VPC par défaut pour les machines virtuelles créées par VDS. Le réseau VPC peut être configuré avec des réseaux VPC existants ou la machine virtuelle CWMGR1 peut être déplacée vers un réseau VPC existant dont les sous-réseaux requis sont prédéfinis.

Informations d'identification et outil de préparation de domaine

Les administrateurs doivent fournir des informations d'identification d'administrateur de domaine à un moment donné du processus de déploiement. Une information d'identification temporaire de l'administrateur de domaine peut être créée, utilisée et supprimée ultérieurement (une fois le processus de déploiement terminé). Les clients qui ont besoin d'aide pour l'élaboration des prérequis peuvent également utiliser l'outil de préparation du domaine.

Déploiement NetApp VDS avec un système de fichiers existant

VDS crée des partages Windows qui permettent l'accès aux profils utilisateur, aux dossiers personnels et aux données d'entreprise à partir des hôtes de session RDS. VDS déploiera le serveur de fichiers par défaut, mais si vous disposez d'un composant de stockage de fichiers existant, VDS peut pointer les partages vers ce composant une fois le déploiement VDS terminé.

Conditions requises pour l'utilisation de et du composant de stockage existant :

- Le composant doit prendre en charge SMB v3
- Le composant doit être joint au même domaine Active Directory que le ou les hôtes de session RDS
- Le composant doit pouvoir exposer un chemin UNC à utiliser dans la configuration VDS ; un chemin peut être utilisé pour les trois partages ou des chemins distincts peuvent être spécifiés pour chacun. Notez que VDS définit les autorisations de niveau utilisateur sur ces partages, elle garantit que les autorisations appropriées ont été accordées aux services d'automatisation VDS.

ANNEXE A : adresses IP et URL du plan de contrôle VDS

Les composants VDS du projet GCP communiquent avec les composants du plan de contrôle global VDS hébergés dans Azure, y compris l'application Web VDS et les terminaux API VDS. Pour l'accès, les adresses URI de base suivantes doivent être safelistées pour un accès bidirectionnel sur le port 443 :

"" "" "" ""

Si votre dispositif de contrôle d'accès ne peut afficher que la liste de sécurité par adresse IP, la liste d'adresses IP suivante doit être sécurisée. Notez que VDS utilise un équilibreur de charge avec des adresses IP publiques redondantes. Cette liste peut donc changer au fil du temps :

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

Facteurs de performance optimaux

Pour des performances optimales, assurez-vous que votre réseau répond aux exigences suivantes :

- La latence aller-retour du réseau du client vers la région GCP dans laquelle les hôtes de session ont été déployés doit être inférieure à 150 ms.
- Le trafic réseau peut circuler en dehors des frontières du pays ou de la région lorsque les machines virtuelles hébergeant des postes de travail et des applications se connectent au service de gestion.
- Pour optimiser les performances du réseau, nous recommandons que les machines virtuelles de l'hôte de session soient situées dans la même région que le service de gestion.

Images du système d'exploitation des machines virtuelles prises en charge

Les hsots de session RDS, déployés par VDS, prennent en charge les images du système d'exploitation x64 suivantes :

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

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.