



Gestion

Virtual Desktop Service

NetApp
February 20, 2023

Table des matières

- Gestion 1
 - De nombreux déploiements 1
 - En termes de latence 16
 - Événements avec script 29
 - Centre de commande 34
 - Optimisation des ressources 44
 - Administration des utilisateurs 48
 - Administration de système 59

Gestion

De nombreux déploiements

Provisionnement des Collections

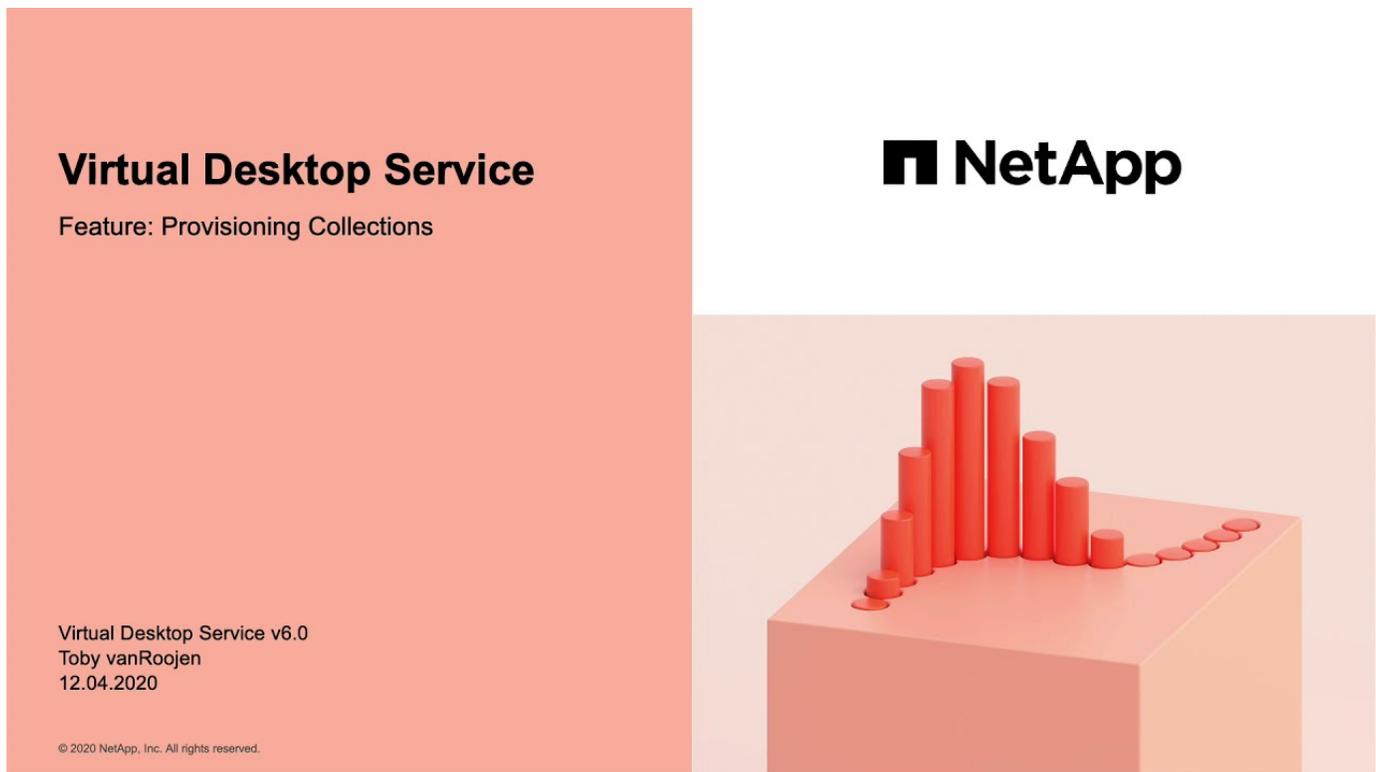
Présentation

Provisioning Collections est une fonction de VDS liée à la création et à la gestion des images VM.

À un niveau élevé, le flux de travail Provisioning Collection est le suivant :

1. Serveur virtuel temporaire (par exemple « CWT1 ») est basé sur une image existante (une image de stock ou une collection de provisioning précédemment enregistrée).
2. L'administrateur VDS personnalise la machine virtuelle temporaire en fonction de leurs besoins à l'aide de "Événements avec script", "Connectez-vous au serveur" ou des outils de gestion tiers.
3. Une fois personnalisé, l'administrateur VDS clique sur **Validate** et déclenche un processus de validation qui automatise la finalisation de l'image, l'exécution de Sysprep, la suppression de la VM temporaire et la mise à disposition de l'image pour le déploiement dans VDS.

Vidéo Démo : gestion des images VM pour les hôtes de session VDI



Types de collecte de provisionnement

Il existe deux types de collection distincts avec des cas d'utilisation spécifiques, **Shared** et **VDI**.

Partagée

Le type **Shared** est un ensemble d'images de machines virtuelles conçues pour déployer un environnement

complet avec plusieurs images de machines virtuelles et des rôles de machines virtuelles distincts.

LES VDI

Le type **VDI** est une image de machine virtuelle unique conçue pour être utilisée et réutilisée pour déployer plusieurs machines virtuelles identiques, généralement utilisées pour héberger des sessions utilisateur. Pour tous les types d'hôtes de session AVD, le **VDI** type doit être sélectionné, même pour les hôtes qui exécutent plusieurs sessions par VM.

Création d'une collection de provisioning

Les collections de provisionnement se trouvent dans l'interface VDS au sein de chaque déploiement, sous le sous-onglet **Provisioning Collections**.

[largeur=75 %]

Pour créer une nouvelle collection

1. Cliquez sur le bouton **+ Ajouter une collection**.
2. Renseignez les champs suivants :
 - a. **Nom**
 - b. **Description** (facultatif)
 - c. **Type** - partagé ou VDI
 - d. **Système d'exploitation**
 - e. **Share Drive** - si cette machine virtuelle sera utilisée pour héberger des profils d'utilisateurs ou des données de partage d'entreprise, sélectionnez la lettre de lecteur sur laquelle sera hébergé. Si ce n'est pas le cas, laissez « C »
 - f. **Cache minimum** - Si vous et VDS créez des machines virtuelles à conserver pour un déploiement instantané, spécifiez le nombre minimal de machines virtuelles mises en cache qui doivent être conservées. Si le déploiement de nouvelles machines virtuelles peut attendre tant que l'hyperviseur met en place une machine virtuelle, cela peut être défini sur 0 pour réduire les coûts.
 - g. **Ajouter des serveurs**
 - i. **Rôle** (si le type « partagé » est sélectionné)
 - A. **TS** - ce VM n'agira qu'en tant qu'hôte de session
 - B. **Data** - cette machine virtuelle n'héberge aucune session utilisateur
 - C. **TSDData** - ce VM sera à la fois l'hôte de session et l'hôte de stockage (maximum : un TSDData par espace de travail)
 - ii. **Modèle VM** - sélectionnez dans la liste disponible les images de l'hyperviseur stock et les collections de provisionnement précédemment enregistrées sont disponibles pour la sélection.
 - A. REMARQUE : PowerShell Remoting n'est pas activé sur les images Windows 7 d'Azure Marketplace. Pour utiliser une image Windows 7, vous devez fournir une image personnalisée dans votre galerie d'images partagée avec PowerShell Remoting activé.
 - B. REMARQUE : en utilisant une collection de provisioning existante, vous pouvez mettre à jour et redéploier des images existantes dans le cadre d'un processus de mise à niveau d'image planifié.
 - iii. **Type de stockage** - sélectionnez la vitesse du disque du système d'exploitation en tenant compte du coût et des performances

- iv. **Lecteur de données** - activez en option un 2e disque relié à cette image, généralement pour la couche de stockage de données mentionnée ci-dessus dans la section 2.e.
 - A. **Type de lecteur de données** - sélectionnez la vitesse du 2e disque (données) en tenant compte du coût et des performances
 - B. **Taille du lecteur de données (Go)** - définissez la taille du 2e disque (données) en fonction de la capacité, du coût et des performances
- h. **Ajouter des applications** - sélectionnez une application de la bibliothèque d'applications qui sera (1) installée sur cette image et (2) gérée par les droits d'application VDS. (Ceci ne s'applique qu'aux déploiements RDS. Il doit rester vide pour les espaces de travail AVD)

Personnalisation de la machine virtuelle temporaire

VDS comprend une fonctionnalité qui autorise la suppression de l'accès aux machines virtuelles depuis l'interface Web VDS. Par défaut, un compte administrateur Windows local est créé avec un mot de passe rotatif et transmis à la machine virtuelle afin de permettre à l'administrateur VDS d'accéder aux informations d'identification administrateur local sans connaître les identifiants d'administrateur local.



La fonction connexion au serveur comporte un autre paramètre où l'administrateur VDS sera invité à saisir les informations d'identification avec chaque connexion. Ce paramètre peut être activé/désactivé en modifiant le compte admin VDS à partir de la section « Admin » de VDS. La fonctionnalité s'appelle *Tech Account* et la vérification de la case nécessite la saisie d'informations d'identification lors de l'utilisation de Connect to Server. La décocher cette case active l'injection automatique des informations d'identification d'administration Windows locales à chaque connexion.

L'administrateur VDS doit simplement se connecter à la machine virtuelle temporaire à l'aide de Connect to Server ou d'un autre processus et apporter les modifications nécessaires pour répondre à ses besoins.

Validation de la collection

Une fois la personnalisation terminée, l'administrateur VDS peut fermer l'image et Sysprep en cliquant sur **Validate** dans l'icône actions.

[Management.Deployments.provisioning collections ed97e] |

Utilisation de la Collection

Une fois la validation terminée, le statut de la collection de provisionnement devient **disponible**. À partir de la collection de provisionnement, l'administrateur VDS peut identifier le nom **VM Template** qui est utilisé pour identifier cette collection de provisionnement dans VDS.

[Management.Deployments.provisioning_collections f5a49] |

Nouveau serveur

À partir de la page espace de travail > serveurs, un nouveau serveur peut être créé et la boîte de dialogue vous invite à entrer le modèle VM. Le nom du modèle ci-dessus se trouve dans cette liste :

[largeur=75 %]



VDS fournit un moyen facile de mettre à jour les hôtes de session dans un environnement RDS en utilisant Provisioning Collections et la fonctionnalité **Add Server**. Ce processus peut être réalisé sans impact sur les utilisateurs finaux et répété à plusieurs reprises avec les mises à jour d'images suivantes, en fonction des itérations d'images précédentes. Pour obtenir un flux de travail détaillé sur ce processus, reportez-vous au "[Processus de mise à jour de l'hôte de session RDS](#)" section ci-dessous.

Nouveau pool hôte AVD

À partir de la page espace de travail > AVD > pools d'hôtes, vous pouvez créer un nouveau pool d'hôtes AVD en cliquant sur **+ Ajouter un pool d'hôtes** et la boîte de dialogue vous invite à entrer le modèle VM. Le nom du modèle ci-dessus se trouve dans cette liste :

[Management.Deployments.provisioning_collections ba2f5] |

Nouvel hôte de session AVD

À partir de la page espace de travail > AVD > Pool hôte > hôtes de session, de nouveaux hôtes de session AVD peuvent être créés en cliquant sur **+ Ajouter hôte de session** et la boîte de dialogue vous invite à entrer le modèle VM. Le nom du modèle ci-dessus se trouve dans cette liste :

[Management.Deployments.provisioning_collections ba5e9] |



VDS fournit un moyen facile de mettre à jour les hôtes de session dans un pool hôte AVD en utilisant Provisioning Collections et la fonctionnalité **Add session Host**. Ce processus peut être réalisé sans impact sur les utilisateurs finaux et répété à plusieurs reprises avec les mises à jour d'images suivantes, en fonction des itérations d'images précédentes. Pour obtenir un flux de travail détaillé sur ce processus, reportez-vous au "[Processus de mise à jour de l'hôte de session AVD](#)" section ci-dessous.

Nouvel espace de travail

À partir de la page espaces de travail, un nouvel espace de travail peut être créé en cliquant sur **+ Nouveau espace de travail** et la boîte de dialogue invite à spécifier la collection de provisionnement. Le nom de la collection de provisionnement partagé se trouve dans cette liste.

[Management.Deployments.provisioning_collections 5c941] |

Nouvelle collection de provisionnement

À partir de la page déploiement > Collection de provisionnement, il est possible de créer une nouvelle collection de provisionnement en cliquant sur **+ Ajouter une collection**. Lors de l'ajout de serveurs à cette collection, la boîte de dialogue vous invite à entrer le modèle VM. Le nom du modèle ci-dessus se trouve dans cette liste :

[Management.Deployments.provisioning_collections 9eac4] |

Addendum 1 - hôtes de session RDS

Processus de mise à jour de l'hôte de session RDS

VDS fournit un moyen facile de mettre à jour les hôtes de session dans un environnement RDS en utilisant Provisioning Collections et la fonctionnalité **Add Server**. Ce processus peut être réalisé sans impact sur les utilisateurs finaux et répété à plusieurs reprises avec les mises à jour d'images suivantes, en fonction des itérations d'images précédentes.

Le processus de mise à jour de l'hôte de session RDS est le suivant :

1. Créez une nouvelle collection de provisionnement VDI, personnalisez et validez la collection conformément aux instructions ci-dessus.
 - a. Généralement, cette collection de provisionnement sera construite sur le modèle VM précédent, en émulant un processus « Ouvrir, Enregistrer sous ».
2. Une fois la collection de provisionnement validée, accédez à la page *Workspace* > *Servers*, puis cliquez sur **+ Add Server**

[Management.Deployments.provisioning_collections.la session rds héberge e8204] |

3. Sélectionnez **TS** comme **rôle serveur**
4. Sélectionnez le dernier **modèle VM**. Effectuez les sélections **taille de la machine** et **Type de stockage** appropriées en fonction de vos besoins. Laisser **lecteur de données** non coché.
5. Répétez cette opération pour le nombre total d'hôtes de session requis pour l'environnement.
6. Cliquez sur **Ajouter serveur**, les hôtes de session seront basés sur le modèle de VM sélectionné et seront mis en ligne dans un délai de 10-15 minutes (selon l'hyperviseur).
 - a. Notez que les hôtes session actuellement dans l'environnement seront finalement déclassés après la mise en ligne de ces nouveaux hôtes. Planifiez la création d'un nombre suffisant de nouveaux hôtes pour prendre en charge la charge de travail complète dans cet environnement.
7. Lorsqu'un nouvel hôte est connecté, le paramètre par défaut est de rester dans **interdire nouvelles sessions**. Pour chaque hôte de session, la bascule **Autoriser les nouvelles sessions** peut être utilisée pour gérer les hôtes qui peuvent recevoir de nouvelles sessions utilisateur. Ce paramètre est accessible en modifiant les paramètres de chaque serveur hôte de session individuel. Une fois qu'un nombre suffisant d'hôtes a été créé et que la fonctionnalité a été confirmée, ce paramètre peut être géré à la fois sur les hôtes anciens et nouveaux pour acheminer toutes les nouvelles sessions vers les nouveaux hôtes. Les anciens hôtes, avec **Autoriser les nouvelles sessions** définis sur **Désactivé**, peuvent continuer à s'exécuter et héberger les sessions utilisateur existantes.

[Management.Deployments.provisioning_collections.la session rds héberge 726d1] |

Management.Deployments.provisioning_collections.rds_session_hosts-726d1.png

8. Lorsque les utilisateurs se déconnectent de l'ancien ou des anciens hôtes et qu'aucune nouvelle session utilisateur n'est associée à l'ancien ou aux anciens hôtes, les anciens hôtes où **sessions = 0** peuvent être supprimés en cliquant sur l'icône **actions** et en sélectionnant **supprimer**.

[Management.Deployments.provisioning_collections.la session rds héberge 45d32] |

Addendum 2 - hôtes de session AVD

Processus de mise à jour de l'hôte de session AVD

VDS fournit un moyen facile de mettre à jour les hôtes de session dans un pool hôte AVD en utilisant Provisioning Collections et la fonctionnalité **Add session Host**. Ce processus peut être réalisé sans impact sur les utilisateurs finaux et répété à plusieurs reprises avec les mises à jour d'images suivantes, en fonction des itérations d'images précédentes.

Le processus de mise à jour de l'hôte de session AVD est le suivant :

1. Créez une nouvelle collection de provisionnement VDI, personnalisez et validez la collection conformément aux instructions ci-dessus.
 - a. Généralement, cette collection de provisionnement sera construite sur le modèle VM précédent, en émulant un processus « Ouvrir, Enregistrer sous ».
2. Une fois la collection de provisionnement validée, accédez à la page *Workspace* > *AVD* > *Host pools* et cliquez sur le nom du pool d'hôtes
3. Dans la page *Host Pool* > *session hosts*, cliquez sur **+ Ajouter session Host**

[Management.Deployments.provisioning_collections 9ed95] |

4. Sélectionnez le dernier **modèle VM**. Effectuez les sélections **taille de la machine** et **Type de stockage** appropriées en fonction de vos besoins.
5. Entrez le **nombre d'instances** égal au nombre total d'hôtes de session requis. Il s'agit généralement du même numéro que celui actuellement dans le pool d'hôtes, mais il peut s'agir d'un nombre quelconque.
 - a. Notez que les hôtes de session actuellement dans le pool hôte seront finalement déclassés après la mise en ligne de ces nouveaux hôtes. Le plan du **nombre d'instances** saisi est suffisant pour prendre en charge l'ensemble de la charge de travail dans ce pool d'hôtes.
6. Cliquez sur **Enregistrer**, les hôtes de session seront basés sur le modèle de VM sélectionné et seront mis en ligne dès 10-15 minutes (selon l'hyperviseur).
7. Lorsqu'un nouvel hôte est connecté, le paramètre par défaut est de rester dans **interdire nouvelles sessions**. Pour chaque hôte de session, la bascule **Autoriser les nouvelles sessions** peut être utilisée pour gérer les hôtes qui peuvent recevoir de nouvelles sessions utilisateur. Une fois qu'un nombre suffisant d'hôtes a été créé et que la fonctionnalité a été confirmée, ce paramètre peut être géré à la fois sur les hôtes anciens et nouveaux pour acheminer toutes les nouvelles sessions vers les nouveaux hôtes. Les anciens hôtes, avec **Autoriser les nouvelles sessions** définis sur **Désactivé**, peuvent continuer à s'exécuter et héberger les sessions utilisateur existantes.

[Management.Deployments.provisioning_collections be47e] |

Management.Deployments.provisioning_collections-be47e.png

8. Lorsque les utilisateurs se déconnectent de l'ancien ou des anciens hôtes et qu'aucune nouvelle session utilisateur n'est associée à l'ancien ou aux anciens hôtes, les anciens hôtes où **sessions = 0** peuvent être supprimés en cliquant sur l'icône **actions** et en sélectionnant **supprimer**.

[Management.Deployments.provisioning_collections cefb9] |

Présentation de la hiérarchie logique VDS

Présentation

VDS organise les concepts en plusieurs couches d'une hiérarchie logique. Cet article vous permet de présenter leur association.

Schéma organisationnel VDS

Le portail de gestion VDS est accessible à l'adresse <https://manage.vds.netapp.com>. Cette interface Web est une fenêtre unique permettant de gérer tous les objets liés au VDS. Dans l'interface utilisateur Web VDS, il existe la hiérarchie suivante de composants et de conteneurs logiques.

Déploiement VDS

Le *Deployment* est un concept VDS qui a organisé et contenant *VDS Workspace(s)*. Dans certaines architectures de déploiement, un déploiement peut contenir plusieurs espaces de travail VDS.



L'exécution de plusieurs espaces de travail VDS dans un déploiement unique est appelée « colocation ». Elle n'est qu'une option dans les déploiements RDS, les déploiements AVD ne prennent pas en charge cette approche.

Un déploiement est défini par son domaine Active Directory et il existe une relation 1:1 entre le domaine AD et un déploiement.

Certaines ressources de machine virtuelle sont déployées pour prendre en charge un déploiement partagé entre tous les espaces de travail VDS dans le déploiement. Par exemple, chaque déploiement contient une machine virtuelle nommée « CWMGR1 », qui est un serveur qui exécute des applications VDS, une base de données SQL Express et facilite la gestion des espaces de travail VDS (et des ressources contenues) au sein du déploiement.

Espace de travail VDS



Il y a une différence entre un espace de travail "**VDS**" et un espace de travail "**AVD**".

Un espace de travail VDS est un conteneur logique dans le déploiement des ressources client (utilisateur final). Ces ressources comprennent les ordinateurs virtuels (pour les hôtes de session, les serveurs d'applications, les serveurs de base de données, les serveurs de fichiers, etc.), la mise en réseau virtuelle, le stockage et une autre infrastructure hyper-viseur.

VDS Workspace contient également des fonctions de gestion permettant de gérer les utilisateurs, les groupes de sécurité, la planification des charges de travail, les applications, l'automatisation, Les machines virtuelles et la configuration AVD.

En général, un espace de travail VDS est aligné avec une seule société ou (dans les déploiements d'entreprise), une unité commerciale.

Sites VDS

Dans le cadre d'un déploiement, plusieurs sites peuvent être créés pour représenter différents fournisseurs d'infrastructure, tous gérés dans un seul déploiement.

Cette approche est utile lorsqu'une seule entreprise ou une seule unité commerciale doit héberger des utilisateurs et des applications sur plusieurs sites physiques (par exemple en Amérique du Nord et en Europe, au Moyen-Orient et en Afrique), des abonnements à d'hyperviseurs (pour aligner les coûts sur les unités commerciales) et même des hyperviseurs (par exemple, des utilisateurs sur Azure, Google Compute et HCI sur site sur vSphere).

Espaces de travail AVD



Il y a une différence entre un espace de travail "VDS" et un espace de travail "AVD".

Un espace de travail AVD est un conteneur logique qui se trouve à l'intérieur d'un espace de travail VDS et d'un site VDS. Il peut être utilisé de façon similaire à un site VDS pour segmenter les stratégies de gestion et d'exploitation dans le même déploiement.

Pools hôtes AVD

Les pools d'hôtes AVD sont des conteneurs logiques situés à l'intérieur d'un espace de travail AVD et qui contiennent les hôtes de session et les groupes d'applications pour Server les sessions utilisateur et contrôler l'accès aux ressources individuelles.

Groupes d'applications AVD

Chaque pool d'hôtes AVD commence par un seul groupe d'applications de bureau. Des utilisateurs et/ou des groupes peuvent être affectés à ce (ou à d'autres) groupe d'applications pour permettre l'accès aux ressources du groupe d'applications aux utilisateurs affectés.

Des groupes d'applications supplémentaires peuvent être créés dans un pool hôte dans VDS. Tous les autres groupes d'applications sont des groupes d'applications « RemoteApp » et prennent en charge les ressources RemoteApp par opposition à une expérience de poste de travail complète avec Windows.

En termes de latence

Droits des applications

Présentation

VDS dispose d'une fonctionnalité intégrée robuste d'automatisation des applications et de droits. Cette fonctionnalité permet aux utilisateurs d'avoir accès à différentes applications lors de la connexion à un ou plusieurs hôtes de session. Pour ce faire, certaines stratégies de groupe personnalisées masquant les raccourcis ainsi que l'automatisation placent des raccourcis de manière sélective sur les bureaux des utilisateurs.



Ce workflow ne s'applique qu'aux déploiements RDS. Pour obtenir de la documentation sur les droits d'application AVD, reportez-vous à la section "[Flux de travail des droits d'application pour AVD](#)".

Les applications peuvent être affectées directement aux utilisateurs ou via des groupes de sécurité gérés dans VDS.

La procédure de provisionnement des applications suit de manière générale cette procédure.

1. Ajouter des applications au catalogue d'applications

2. Ajouter des applications à l'espace de travail
3. Installez l'application sur tous les hôtes de session
4. Sélectionnez le chemin du raccourci
5. Attribuez des applications aux utilisateurs et/ou aux groupes



Les étapes 3 et 4 peuvent être entièrement automatisées avec des événements avec script comme illustré ci-dessous



Présentation vidéo

Ajouter des applications au catalogue d'applications

La licence d'application VDS commence par le catalogue d'applications. Il s'agit d'une liste de toutes les applications disponibles pour le déploiement dans les environnements utilisateur final.

Pour ajouter des applications au catalogue, procédez comme suit

1. Connectez-vous à VDS at <https://manage.cloudworkspace.com> à l'aide de vos informations d'identification d'administrateur principales.
2. Dans le coin supérieur droit, cliquez sur la flèche située en regard de votre Nom d'utilisateur et sélectionnez Paramètres.
3. Cliquez sur l'onglet Catalogue d'applications.
4. Cliquez sur l'option Ajouter une application dans la barre de titre du catalogue d'applications.
5. Pour ajouter un groupe d'applications, choisissez l'option Importer des applications.
 - a. Une boîte de dialogue s'affiche et fournit un modèle Excel à télécharger qui crée le format correct pour la liste des applications.
 - b. Pour cette évaluation, NetApp VDS a créé un exemple de liste d'applications destinées à être importée. Il est disponible [ici](#).

- c. Cliquez sur la zone Télécharger et choisissez le fichier de modèle d'application, puis cliquez sur le bouton Importer.
6. Pour ajouter des applications individuelles, cliquez sur le bouton Ajouter une application et une boîte de dialogue s'affiche.
 - a. Entrez le nom de l'application.
 - b. L'ID externe peut être utilisé pour saisir un identifiant de suivi interne tel qu'une référence de produit ou un code de suivi de facturation (facultatif).
 - c. Cochez la case abonnement si vous souhaitez créer un rapport sur les applications en tant que produit abonnement (facultatif).
 - d. Si le produit ne s'installe pas par version (par exemple Chrome), cochez la case version non requise. Cela permet d'installer les produits de mise à jour continue sans suivre leurs versions.
 - e. Inversement, si un produit prend en charge plusieurs versions nommées (par exemple QuickBooks), vous devez cocher cette case pour pouvoir installer plusieurs versions et avoir VDS spécifique chaque version disponible dans la liste des applications pouvant être autorisées pour et pour l'utilisateur final.
 - f. Cochez "aucune icône de bureau utilisateur" si vous ne souhaitez pas que VDS provisionne une icône de bureau pour ce produit. Il est utilisé pour les produits « backend » comme SQL Server, car les utilisateurs finaux n'ont pas d'application à accéder.
 - g. « L'application doit être associée » impose l'installation d'une application associée. Par exemple, une application client Server peut nécessiter l'installation de SQL Server ou de MySQL.
 - h. La case Licence requise indique que VDS doit demander le téléchargement d'un fichier de licence pour une installation de cette application avant de définir l'état de l'application sur actif. Cette étape est effectuée sur la page application detail de VDS.
 - i. Visible pour tous – l'admissibilité aux applications peut être limitée à des sous-partenaires spécifiques dans une hiérarchie multicanal. Pour l'évaluation, cliquez sur la case à cocher afin que tous les utilisateurs puissent la voir dans leur liste d'applications disponibles.

Ajoutez l'application à l'espace de travail

Pour démarrer le processus de déploiement, vous allez ajouter l'application à l'espace de travail.

Pour ce faire, procédez comme suit

1. Cliquez sur espaces de travail
2. Faites défiler jusqu'à applications
3. Cliquez sur Ajouter
4. Cochez la ou les applications, entrez les informations requises, cliquez sur Ajouter une application, puis sur Ajouter des applications.

Installez l'application manuellement

Une fois l'application ajoutée à l'espace de travail, vous devez installer cette application sur tous les hôtes de session. Cette opération peut être effectuée manuellement et/ou automatiquement.

Pour installer manuellement des applications sur des hôtes de session, procédez comme suit

1. Accédez à la carte de service.
2. Cliquez sur la tâche de la carte de service.
3. Cliquez sur le(s) nom(s) du serveur pour vous connecter en tant qu'administrateur local.

4. Installez les applications, confirmez que le raccourci vers cette application se trouve dans le chemin du menu Démarrer.
 - a. Pour Server 2016 et Windows 10 : C:\ProgramData\Microsoft\Windows\Démarrer Menu\programmes.
5. Retournez à la tâche de la carte de service, cliquez sur Parcourir et choisissez le raccourci ou un dossier contenant des raccourcis.
6. Quelle que soit la sélection choisie, ce qui s'affiche sur le bureau de l'utilisateur final lorsqu'il est attribué à l'application.
7. Les dossiers sont parfaits lorsqu'une application est en fait plusieurs applications. Par exemple, « Microsoft Office » est plus facile à déployer comme dossier avec chaque application comme raccourci dans le dossier.
8. Cliquez sur Terminer l'installation.
9. Si nécessaire, ouvrez l'icône créée Ajouter une tâche de carte de service et confirmez que l'icône a été ajoutée.

Attribuez des applications aux utilisateurs

Les droits d'application sont gérés par VDS et l'application peut être attribuée aux utilisateurs de trois manières

Attribuer des applications aux utilisateurs

1. Accédez à la page User Detail.
2. Accédez à la section applications.
3. Cochez la case en regard de toutes les applications requises par cet utilisateur.

Attribuer des utilisateurs à une application

1. Accédez à la section applications de la page Détails de l'espace de travail.
2. Cliquez sur le nom de l'application.
3. Cochez la case en regard des utilisateurs de l'application.

Attribuez des applications et des utilisateurs à des groupes d'utilisateurs

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.

Flux de travail des droits d'application pour AVD

Présentation

Dans un environnement Azure Virtual Desktop (AVD), l'accès aux applications est géré par l'appartenance aux groupes d'applications.



Ce flux de travail s'applique uniquement aux déploiements AVD. Pour obtenir de la documentation sur les droits d'application RDS, reportez-vous à la section "[Workflow des droits d'application pour RDS](#)"



AVD est un service bien documenté et il y en a beaucoup "[ressources publiques pour information](#)". VDS ne surpasse pas la manière standard de fonctionnement de l'AVD. Cet article est plutôt conçu pour illustrer comment VDS approche le concept standard de tous les déploiements AVD.



Révision du "[Présentation de la hiérarchie logique VDS](#)" l'article peut être utile avant ou pendant la révision de cet article.

Vue de l'utilisateur final

Dans Azure Virtual Desktop, chaque utilisateur final dispose d'un accès à RemoteApp et/ou Desktop(s) par son administrateur AVD. Ceci s'effectue via l'affectation de groupe d'applications dans VDS.

RemoteApp désigne une application qui s'exécute à distance sur l'hôte de session mais qui est présentée sur le périphérique local sans le contexte de bureau. Cette application, communément appelée « application de streaming », ressemble à une application locale sur l'appareil local, mais elle s'exécute dans le contexte de sécurité, ainsi que sur la couche de stockage et de calcul de l'hôte de session.

Desktop fait référence à l'expérience Windows complète exécutée sur l'hôte de session et présentée sur le périphérique local, généralement dans une fenêtre plein écran. Communément appelé « poste de travail distant », ce poste de travail lui-même contiendra toutes les applications installées sur cet hôte de session qui peuvent être lancées par l'utilisateur depuis la fenêtre de session du poste de travail.

Lors de la connexion, l'utilisateur final est présenté avec les ressources qui lui sont assignées par son administrateur. Vous trouverez ci-dessous un exemple de vue qu'un utilisateur final peut voir lors de la connexion avec son client AVD. Cet exemple est plus complexe, souvent un utilisateur final ne peut lui attribuer qu'un poste de travail d'angle ou RemoteApp. L'utilisateur final peut double-cliquer sur l'une de ces ressources pour lancer cette application/ce poste de travail.

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

Dans cet exemple plus complexe, cet utilisateur a accès à deux sessions de poste de travail différentes et à 4 applications de streaming différentes :

- **Bureaux disponibles**
 - NVIDIA GPU Desktop (bureau NVIDIA GPU)
 - Poste de travail AVD Pool partagé
 - Opération 2 Pool Desktop
- **RemoteApps disponibles**
 - AutoCAD 2021
 - Rappel 2021
 - Microsoft Edge
 - Bloc-notes

En coulisses, ces applications et postes de travail sont hébergés sur un grand nombre d'hôtes de sessions, ainsi que dans des espaces de travail AVD et pourraient même être hébergés dans différentes régions Azure.

La figure ci-dessous illustre l'hébergement de chacune de ces ressources et leur affectation à cet utilisateur final.

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

Comme illustré ci-dessus, les différentes ressources disponibles pour cet utilisateur final sont hébergées dans différents hôtes de session, dans différents pools hôtes et potentiellement gérées par différentes organisations INFORMATIQUES dans différents espaces de travail AVD. Bien que ces ressources ne soient pas visibles dans cet exemple, elles peuvent également être hébergées dans différentes régions Azure et/ou dans des abonnements utilisant la fonction sites VDS.

Fourniture d'accès au bureau

Par défaut, chaque pool hôte commence par un groupe d'applications unique, utilisé pour attribuer l'accès à l'expérience Windows Desktop. Toutes les applications installées sur ces hôtes de session seront accessibles aux utilisateurs finaux affectés à ce groupe d'applications.

Pour activer la ressource Desktop pour les utilisateurs dans VDS :

1. Accédez à la page espaces de travail > AVD > Pool hôte > groupes d'applications, puis cliquez sur le groupe d'applications pour accéder à la ressource « Bureau ».

[Gestion.applications.avd - flux de travail des droits d'application 349fe] |

Management.Applications.avd_application_entitlement_workflow-349fe.png

2. Une fois dans le groupe d'applications, cliquez sur Modifier

[Gestion.applications.avd flux d'application 3bcfc] |

Management.Applications.avd_application_entitlement_workflow-3bcfc.png

3. Dans la boîte de dialogue de modification, vous pouvez ajouter ou supprimer des utilisateurs à ce groupe d'applications par utilisateur et/ou par groupe.

[Gestion.applications.avd flux de travail des droits d'application 07ff0] |

Accès à RemoteApp

Afin de provisionner l'accès à RemoteApps, un nouveau groupe d'applications doit être créé au sein du pool hôte. Une fois créées, les applications appropriées doivent être affectées à ce groupe d'applications.



Toutes les applications de ces sessions hôtes seront déjà disponibles pour tous les utilisateurs affectés à l'APPGROUP de ce pool d'hôtes. Il n'est pas nécessaire de provisionner également l'accès via un groupe d'applications RemoteApp simplement pour permettre l'accès aux applications. Un groupe d'applications RemoteApp n'est nécessaire que pour permettre l'accès aux applications qui s'exécutent en tant qu'application de streaming sur le terminal local.

Créer un nouveau groupe d'applications

1. Accédez à la page Workspaces > AVD > Host Pool > App Groups et cliquez sur le bouton + *Add App Group*

[Gestion.applications.avd flux de travail des droits d'application d33da] |

Management.Applications.avd_application_entitlement_workflow-d33da.png

2. Entrez le nom, l'espace de travail et le nom convivial de ce groupe d'applications. Sélectionnez les utilisateurs et/ou les groupes à attribuer et cliquez sur *Save*

[Gestion.applications.avd déroulement des procédures d'application 242eb] |

Ajouter des applications au groupe d'applications

1. Accédez à la page espaces de travail > AVD > Pool hôte > groupes d'applications, puis cliquez sur le groupe d'applications pour la ressource « RemoteApp ».

[Gestion.applications.avd flux de travail des droits d'application 3dcde] |

Management.Applications.avd_application_entitlement_workflow-3dcde.png

2. Une fois dans le groupe d'applications, cliquez sur Modifier

[Gestion.applications.avd flux de travail de droits d'application 27a41] |

Management.Applications.avd_application_entitlement_workflow-27a41.png

3. Faites défiler jusqu'à la section « applications distantes ». Cette section peut prendre un certain temps pour se remplir car VDS effectue une requête directe sur les hôtes de session afin d'afficher les applications disponibles pour la diffusion en continu.

[Gestion.applications.avd flux de travail des droits d'application 1e9f2] |

4. Recherchez et sélectionnez toutes les applications auxquelles les utilisateurs de ces groupes d'applications doivent avoir accès en tant que ressource RemoteApp.

Événements avec script

Événements avec script

Présentation

Les événements avec script fournissent à l'administrateur avancé un mécanisme permettant de créer une automatisation personnalisée pour la maintenance du système, les alertes utilisateur, la gestion des stratégies de groupe ou d'autres événements. Les scripts peuvent être désignés pour s'exécuter en tant que processus exécutable avec des arguments ou être utilisés comme arguments pour un programme exécutable différent. Cette fonctionnalité permet de combiner et d'imbriquer des scripts pour prendre en charge des besoins complexes en matière de personnalisation et d'intégration.

Un exemple détaillé d'événements avec script en action se trouve dans le ["Guide des droits d'application"](#).

En outre, les événements avec script permettent la création d'une automatisation qui ne nécessite pas de script pour le traitement, mais le flux d'automatisation est lancé par un déclencheur système et exécute un programme ou utilitaire système existant avec des arguments facultatifs.

Scripts événements contient à la fois un **référentiel** de scripts et **activités**. Les scripts contiennent les instructions sur **ce que** faire pendant que les activités relient les scripts avec le déclencheur et la cible appropriés (**quand et où**) pour le script.

Référentiel

L'onglet référentiel affiche la liste de tous les scripts disponibles à déployer à partir de votre compte VDS. Il s'agit d'un référentiel personnalisé partagé par tous les administrateurs de votre instance VDS. L'accès aux événements avec script peut être géré sur la page *VDS > Admins > autorisations*.

[Sub.Management.Scripted Events.script Events 1ce76] | *sub.Management.Scripted_Events.scripted_events-*

Filtre client

Chaque organisation administrateur VDS dispose d'une bibliothèque privée de scripts créés et/ou personnalisés par son organisation. Ces scripts sont définis comme type de script « client ». Les scripts client doivent être supprimés et modifiés par tout administrateur VDS disposant des autorisations d'administration appropriées à la section événements avec script.

Filtre global

NetApp publie et conserve également une bibliothèque de scripts « globaux », qui est la même pour toutes les organisations d'administrateurs VDS. Ces scripts sont définis comme le type de script « Global ». Les scripts globaux ne peuvent pas être modifiés ni supprimés par un administrateur VDS. Au contraire, les scripts globaux peuvent être "clonés" et le script résultant est un script "client" qui peut être édité et utilisé.

Télécharger le script

La possibilité de télécharger le fichier script associé à un événement script permet à l'administrateur VDS d'examiner et de modifier le fichier script sous-jacent avant le déploiement. L'exécution d'un script que vous ne comprenez pas entièrement n'est jamais recommandée.

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

Ajouter un script

Cliquez sur le bouton + *Ajouter un script* pour ouvrir une nouvelle page permettant de créer un script et de l'enregistrer dans le référentiel.

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

Les champs suivants doivent être renseignés pour créer un nouveau script :

- **Nom**
- **Inclure fichier script**
 - Oui - permet de télécharger et d'exécuter un fichier script (par exemple un fichier .ps1) par l'exécutable « Exécuter avec ».
 - Non - supprime le champ « fichier script » (ci-dessous) et exécute simplement la commande « Exécuter avec » et « arguments »
- **Fichier script**
 - Si *inclure un fichier script* = *Oui* ce champ est visible et permet le téléchargement d'un fichier script.
- **Exécuter avec**
 - Définit le chemin d'accès de l'exécutable utilisé pour exécuter le fichier script ou la commande exécutée.
 - Par exemple, pour exécuter avec PowerShell, la valeur « Exécuter avec » est `C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe`
- **Arguments**
 - Définit tout argument supplémentaire exécuté par rapport à la commande « s'exécute avec ».
 - VDS offre certaines variables contextuelles qui peuvent être utilisées, notamment :
 - %Company code% - Code de la société à l'exécution
 - %Servername% - nom de la machine virtuelle au moment de l'exécution
 - %samaccountname% - <username>.<code société>
 - %Applicationname% - nom de l'application demandé lors de l'exécution
 - %Scriptname% - Nom du script à l'exécution
 - %username% - username@loginidentifiant au moment de l'exécution
- **URL de documentation**
 - Ce champ permet au rédacteur du script de le lier à la documentation trouvée en dehors de VDS, comme un système de base de connaissances utilisé par l'organisation des administrateurs VDS.

Modifier le script

Un clic sur le nom d'un script dans le référentiel ouvre une nouvelle page avec des détails sur le script et un bouton d'action à **éditer**.

Lors de la modification d'un script, les mêmes champs sont modifiables comme indiqué ci-dessus dans "[Ajouter un script](#)" section.

Sur cette page de détails de script, vous pouvez aussi **supprimer** le script et **télécharger** tout fichier de script

téléchargé.

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

Activités

Les activités relient un script du référentiel à un déploiement, un sous-ensemble de machines virtuelles et un événement déclencheur.

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

Ajouter une activité

Cliquez sur le bouton + *Ajouter une activité* pour ouvrir une nouvelle page permettant de créer une activité.

[Management.script Events.script Events 02ef8] | *Management.Scripted_Events.scripted_events-02ef8.png*

Les champs suivants doivent être renseignés pour créer une nouvelle activité :

- **Nom**
- **Description** (facultatif)
- **Déploiement**
- **Script**
- **Arguments**
- **Activé**
- **Paramètres d'événement**

Déclencheurs d'activité

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

- **Installation de l'application**

- Cette action est déclenchée lorsque l'administrateur VDS clique sur « + Ajouter... » dans la page *Workspace > applications*.
- Cette sélection vous permet de sélectionner une application dans la Bibliothèque d'applications et de prédéfinir le raccourci de l'application.
- Les instructions détaillées pour ce déclencheur sont mises en surbrillance dans le "[Installer la documentation du script Adobe Reader DC](#)".

- **Désinstallation de l'application**

- Cette action est déclenchée lorsque l'administrateur VDS clique sur « actions > Désinstaller » dans la page *Workspace > applications*.
- Cette sélection vous permet de sélectionner une application dans la Bibliothèque d'applications et de prédéfinir le raccourci de l'application.
- Les instructions détaillées pour ce déclencheur sont mises en surbrillance dans le "[Désinstaller la documentation du script Adobe Reader DC](#)".

- **Serveur de clonage**

- Cette opération est déclenchée lorsque la fonction de clonage est exécutée sur un serveur virtuel existant

- **Créer cache**

- Cette action est déclenchée chaque fois qu'une nouvelle machine virtuelle est créée par VDS pour un cache de collecte de provisionnement

- **Créer un client**

- Cette action est déclenchée chaque fois qu'une nouvelle organisation client est ajoutée à VDS

- **Créer serveur**

- Cette action est déclenchée chaque fois qu'un nouveau serveur virtuel est créé par VDS

- **Créer un utilisateur**

- Cette action est déclenchée chaque fois qu'un nouvel utilisateur est ajouté via VDS

- **Supprimer l'utilisateur**

- Cette action est déclenchée chaque fois qu'un nouvel utilisateur est supprimé via VDS

- **Manuel**

- Ceci est déclenché manuellement par un administrateur VDS à partir de la page « événements avec script > activité »

- **Mise à jour manuelle de l'application**

- **Planifié**

- Cette action est déclenchée lorsque la date/l'heure définie est atteinte

- **Démarrer serveur**

- Cet effet est déclenché sur un serveur virtuel à chaque démarrage

Cliquer sur *Name* ouvre une boîte de dialogue dans laquelle l'activité peut être modifiée.

Centre de commande

Commande Command Center : présentation

Présentation

Le Centre de commandes est un exécutable qui s'exécute sur le serveur de plate-forme CWMGR1 dans le déploiement. Il est accessible en se connectant à la machine virtuelle CWMGR1 et en l'exécutant localement sur cette machine virtuelle.

Cette application a été conçue pour les fonctions de dépannage, de diagnostic et de gestion avancée. Cette application est principalement utilisée par les équipes de support et de développement internes de NetApp, mais certaines fonctions sont parfois utilisées par les administrateurs des clients. Cette documentation est fournie pour prendre en charge l'utilisation des fonctions de sélection. L'utilisation de ces commandes doit être effectuée avec soin et en collaboration avec l'équipe de support NetApp.

Exécution de Command Center

Pour exécuter l'application Command Center :

1. Connectez-vous au serveur à partir de la page *VDS > déploiement > serveurs de plate-forme* cliquez sur l'icône *actions* et sélectionnez « connexion ».

[Management.command vue d'ensemble du centre 68087] | *Management.command_center_overview-*

68087.png

2. Lorsque vous êtes invité à saisir les informations d'identification du domaine, saisissez les informations d'identification du
 - a. L'utilisateur doit être membre du groupe de sécurité « CW-Infrastructure ». Pour des raisons de cohérence, nous recommandons d'ajouter cette appartenance en faisant de l'utilisateur un membre du groupe « techniciens de niveau 3 » dans *AD > Cloud Workspace > utilisateurs Tech Cloud Workspace > groupes*

[Management.command vue d'ensemble du centre 1c42d] | *Management.command_center_overview-*

1c42d.png

3. Recherchez l'icône du bureau pour *Command Center* et exécutez-la

[Management.command vue d'ensemble du centre 3c860] | *Management.command_center_overview-*

3c860.png

- a. Pour activer l'onglet Avancé, lancez l'application avec le commutateur "-showadvancedtab".

Onglet opérations

[Management.command vue d'ensemble du centre b614e] | *Management.command_center_overview-*

b614e.png

Dans le menu **Command**, vous pouvez sélectionner une des actions (répertoriées ci-dessous).

Une fois qu'une commande est sélectionnée, les données peuvent être renseignées avec les données de déploiement à partir du bouton **Charger les données**. Le bouton Charger les données est également utilisé pour interroger l'hyperviseur pour les données une fois les sélections précédentes effectuées (par exemple Chargement d'une liste de dates de sauvegarde disponibles après la sélection d'un VM spécifique dans une liste déroulante)

[Management.command vue d'ensemble du centre 85417] | *Management.command_center_overview-*

85417.png

Après avoir effectué des sélections sur une commande, cliquez sur **Exécuter la commande** pour exécuter le processus sélectionné.

Pour consulter les journaux, cliquez sur le bouton **Afficher tous les journaux**. Le fichier de texte brut s'ouvre, avec les entrées les plus récentes en bas.

Liste de commandes

- ["Copier le modèle dans la galerie"](#)

Exploitation

Commande Centre de commande : copier le modèle dans la galerie

Avertissement du centre de commande



Le Centre de commandes est une application qui s'exécute sur le serveur de plate-forme CWMGR1 dans le déploiement. Cette application a été conçue pour les fonctions de dépannage, de diagnostic et de gestion avancée. Cette application est principalement utilisée par les équipes de support et de développement internes de NetApp, mais certaines fonctions sont parfois utilisées par les administrateurs des clients. Cette documentation est fournie pour prendre en charge l'utilisation des fonctions de sélection. L'utilisation de ces commandes doit être effectuée avec soin et en collaboration avec l'équipe de support NetApp. Vous trouverez plus d'informations dans le ["Vue d'ensemble du centre de commande"](#) article.

Copier le modèle vers la Gallery Présentation

[Management.command Center.Operations.copy template to galerie 67ea4] |

Management.command_center.operations.copy_template_to_gallery-67ea4.png

Lorsqu'une collection de provisionnement VDI est finalisée, l'image est stockée dans Azure sous forme d'image et peut être déployée sur le même site VDS. Pour rendre l'image disponible pour le déploiement dans une autre région Azure au sein de la même souscription, la fonction « Copier le modèle vers la galerie » est utilisée. Cette action copie l'image VM dans la galerie partagée et la réplique dans toutes les régions sélectionnées.

[Management.command Center.Operations.copy template to Gallery ed821] |

Management.command_center.operations.copy_template_to_gallery-ed821.png

Liste déroulante disponibilité des modèles VM dans VDS

Une fois la réplication terminée, l'image s'affiche dans VDS dans la liste déroulante pour la sélection des modèles VM lors du déploiement de nouvelles VM. L'image partagée sera disponible pour le déploiement dans n'importe quelle région sélectionnée lors de la copie.

[Management.command Center.Operations.copy template to galerie 04bd8] |

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

Les images VM stockées dans la galerie partagée sont ajoutées avec leur version sous la forme « -x.x.x », où la version correspond à la version d'image dans le portail Azure.

[Management.command Center.Operations.copy template to galerie ee598] |



La réplique de l'image peut prendre un certain temps (en fonction de la taille de l'image) et l'état peut être vu en cliquant sur la version (par exemple, 1.0.0) dans la colonne "Nom" comme mis en évidence dans la capture d'écran ci-dessus.

Disponibilité régionale

Les déploiements ne peuvent être effectués que dans les régions où l'image a été répliquée. Vous pouvez vérifier ces informations sur le portail Azure en cliquant sur 1.x.x, puis sur *Update Replication* comme indiqué ici :

[Management.command Center.Operations.copy template to galerie 9b63a] |

Optimisation des ressources

Planification des charges de travail

La planification de la charge de travail est une fonction qui permet de planifier la fenêtre de temps dans laquelle l'environnement est actif.

La planification des charges de travail peut être définie sur « Always On », « Always off » ou « planifié ». Lorsqu'il est défini sur « programmé », les heures d'activation et de désactivation peuvent être définies de façon aussi granulaire qu'une fenêtre d'heure différente pour chaque jour de la semaine.

[]

Lorsqu'elle est prévue pour être désactivée, soit via « toujours désactivée » soit « planifiée », toutes les machines virtuelles locataires sont arrêtées. Les serveurs de plate-forme (comme CWMGR1) resteront actifs pour faciliter les fonctionnalités telles que wake on Demand.

La planification des charges de travail fonctionne conjointement avec d'autres fonctionnalités d'optimisation des ressources, notamment Live Scaling et Wake on Demand.

Réveil à la demande

Wake on Demand (Wod) est une technologie en attente de brevet qui peut réveiller les ressources VM appropriées pour un utilisateur final afin de faciliter l'accès sans surveillance 24 h/24, 7 j/7 et 7 jours par an, même lorsque les ressources sont désactivées.

Wod pour services de bureau à distance

Dans RDS, le client Windows VDS est intégré à l'intégration Wake on Demand et peut réactiver les ressources appropriées sans actions supplémentaires de l'utilisateur final. Il leur suffit de lancer leur connexion standard pour que le client l'informe d'un bref délai que la ou les VM sont activées. Ce client (et donc cette fonctionnalité d'automatisation du réveil à la demande) n'est disponible que lors de la connexion d'un périphérique Windows à un environnement RDS.

Une fonctionnalité similaire est intégrée au client Web VDS pour les déploiements RDS. Le client Web VDS se trouve à l'adresse suivante : ""

La fonctionnalité Wake on Demand n'est pas intégrée au client Microsoft RD (pour Windows ou toute autre plate-forme) ni aux autres clients RD tiers.

Service de réveil à la demande pour Azure Virtual Desktop

Dans AVD, les seuls clients pouvant être utilisés pour se connecter sont fournis par Microsoft et ne contiennent donc pas la fonctionnalité de réveil à la demande.

VDS comprend une fonction de réveil à la demande en libre-service pour AVD via le client Web VDS. Le client Web peut être utilisé pour réveiller les ressources appropriées, puis la connexion peut être initiée via le client AVD standard.

Pour réactiver les ressources VM dans AVD :

1. Connectez-vous au client Web VDS à l'adresse ""

2. Connectez-vous à l'aide des informations d'identification AVD de l'utilisateur
 - Un message d'avertissement vous invite à indiquer « *les services AVD de Microsoft sont disponibles. Cliquez ICI pour afficher l'état et démarrer les pools d'hôtes hors ligne.* »
3. Après avoir cliqué sur « *HERE* », vous verrez une liste des pools d'hôtes disponibles ainsi qu'un lien vers le lien « cliquer pour démarrer » sous la colonne d'état



4. Cliquez sur *Démarrer* le lien et attendez 1-5 minutes que l'état passe à « en ligne » et affiche une icône d'état verte
5. Connectez-vous à AVD en utilisant votre processus normal

Mise à l'échelle dynamique

Live Scaling fonctionne conjointement avec la planification de la charge de travail en gérant le nombre d'hôtes de session en ligne pendant l'heure d'activité planifiée telle que configurée dans la planification de la charge de travail. Lorsqu'il est programmé pour être hors ligne, Live Scaling ne contrôle pas la disponibilité de l'hôte de session. L'évolutivité en direct n'a qu'un impact sur les utilisateurs partagés et les serveurs partagés dans les environnements RDS et AVD, les utilisateurs VDI et les VM sont exclus de ces calculs. Tous les autres types de VM ne sont pas affectés.



Le paramètre *AVD Load Balancer type* interagit avec cette configuration. Il convient donc de prendre également soin de choisir ce paramètre. Les économies sont optimisées avec un premier type de profondeur tandis que les performances des utilisateurs finaux sont optimisées avec un premier type de largeur.

Activation de la mise à l'échelle directe sans option activée, le moteur d'automatisation sélectionne automatiquement les valeurs du nombre d'utilisateurs supplémentaires alimentés sur les serveurs, des utilisateurs partagés par serveur et du nombre maximal d'utilisateurs partagés par serveur.

- Le *Number of Extra Powered on Servers* passe par défaut à 0, c'est-à-dire 1 serveur fonctionne 24/7.
- Par défaut, le paramètre *Shared Users par serveur* indique le nombre d'utilisateurs de la société divisé par le nombre de serveurs.
- La valeur par défaut de *Max Shared Users par serveur* est infinie.

Live Scaling active les serveurs lorsque les utilisateurs se connectent et les désactive lorsque les utilisateurs se déconnectent.

La mise sous tension d'un serveur supplémentaire est automatiquement déclenchée une fois que le nombre total d'utilisateurs actifs atteint le nombre d'utilisateurs partagés par serveur multiplié par le nombre total de serveurs mis sous tension.

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

Live Scaling va également désactiver les serveurs pour réduire les coûts. Lorsqu'un serveur a 0 utilisateurs actifs et qu'un autre serveur dispose d'une capacité disponible inférieure à `_utilisateurs partagés par serveur_` le serveur vide est mis hors tension.

La mise sous tension du serveur suivant peut prendre quelques minutes. Dans certaines situations, la vitesse des connexions peut dépasser celle des nouveaux serveurs. Par exemple, si 15 personnes se connectent en 5 minutes, elles atterriront toutes sur le premier serveur (ou se verront refuser une session) pendant une deuxième et une troisième mise sous tension. Deux stratégies peuvent être utilisées pour atténuer la surcharge d'un seul serveur dans ce scénario :

1. Activez *Number of Extra Powered on Servers* afin que le ou les serveurs supplémentaires soient sous tension et disponibles pour accepter les connexions et permettre à la plate-forme de lancer des serveurs supplémentaires.
 - a. Lorsqu'il est activé, le numéro est ajouté au besoin calculé. Par exemple, si la valeur est définie sur 1 serveur supplémentaire (et avec 6 utilisateurs connectés), deux serveurs sont actifs en raison du nombre d'utilisateurs, plus un troisième en raison du paramètre *Extra Powered on Servers*.
2. Activez *Max Shared users per Server* pour placer une limite matérielle du nombre d'utilisateurs autorisés par serveur. Les nouvelles connexions dépassant cette limite seront refusées, l'utilisateur final affichera un message d'erreur et devra réessayer dans quelques minutes une fois que le serveur supplémentaire sera disponible. Si ce nombre est défini, il définit également la profondeur des serveurs partagés AVD.
 - a. En supposant que le delta entre *utilisateurs partagés par serveur* et *Max utilisateurs partagés par serveur* soit approprié, les nouveaux serveurs devraient être disponibles avant que la max ne soit atteinte dans toutes les situations sauf dans les situations les plus extrêmes (des tempêtes de connexion exceptionnellement grandes).

L'évolutivité des ressources des ordinateurs virtuels

L'évolutivité des ressources des machines virtuelles est une fonction facultative qui permet de modifier la taille et la quantité des machines virtuelles hôtes dans un environnement.

Lorsque cette option est activée, VDS calcule la taille et la quantité appropriées des machines virtuelles hôtes de session en fonction des critères sélectionnés. Ces options comprennent : les utilisateurs actifs, les utilisateurs nommés, la charge du serveur et la correction.

□

La taille des machines virtuelles est contenue dans la famille de machines virtuelles sélectionnées dans l'interface utilisateur et peut être modifiée par liste déroulante. (p. ex. *Série DV3 famille* dans Azure)



Évolutivité en fonction des utilisateurs



La fonction ci-dessous se comporte de la même manière pour « utilisateurs actifs » ou « nombre d'utilisateurs ». User Count est un nombre simple de tous les utilisateurs activés avec un poste de travail VDS. Les utilisateurs actifs sont une variable calculée sur la base des 2 semaines précédentes de données de session utilisateur.

Lors du calcul en fonction des utilisateurs, la taille (et la quantité) des machines virtuelles hôtes de session est calculée en fonction des besoins définis en mémoire vive et en CPU. L'administrateur peut définir le Go de RAM, ainsi que le nombre de cœurs de CPU virtuels par utilisateur, en plus des ressources supplémentaires sans variables.

Dans la capture d'écran ci-dessous, chaque utilisateur dispose d'une mémoire RAM de 2 Go et de 1/2 cœurs de CPU virtuels. En outre, le serveur commence avec 2 cœurs de CPU virtuels et 8 Go de RAM.



En outre, l'administrateur peut définir la taille maximale qu'une machine virtuelle peut atteindre. Lorsque la limite est atteinte, les environnements évoluent horizontalement en ajoutant des hôtes de session de VM supplémentaires.

Dans la capture d'écran ci-dessous, chaque machine virtuelle est limitée à 32 Go de RAM et à 8 cœurs de vCPU.



Lorsque toutes ces variables sont définies, VDS peut calculer la taille et la quantité appropriées des machines virtuelles hôtes de session. Cette opération simplifie grandement le processus de maintien de l'affectation appropriée des ressources, même lorsque les utilisateurs sont ajoutés et supprimés.

Évolutivité en fonction de la charge du serveur

Lors du calcul en fonction de la charge du serveur, la taille (et la quantité) des machines virtuelles hôtes de session est calculée en fonction des taux moyens d'utilisation du CPU/de la RAM observés par VDS sur la période 2 semaines précédente.

Lorsque le seuil maximal est dépassé, VDS augmente la taille ou augmente la quantité pour ramener l'utilisation moyenne dans la plage.

À l'instar de l'évolutivité basée sur l'utilisateur, il est possible de définir la famille de machines virtuelles et la taille maximale des machines virtuelles.



Autres ressources actives

La planification de la charge de travail ne contrôle pas les serveurs de plate-forme tels que CWMGR1 car ils sont nécessaires pour déclencher la fonctionnalité de réveil à la demande et faciliter les autres tâches de la plate-forme et doit exécuter 24/7 pour un fonctionnement normal de l'environnement.

Des économies supplémentaires peuvent être réalisées en désactivant l'ensemble de l'environnement, mais elles sont uniquement recommandées pour les environnements hors production. Il s'agit d'une action manuelle

qui peut être effectuée dans la section déploiements de VDS. Pour rétablir l'état normal de l'environnement, il est également nécessaire d'effectuer une étape manuelle sur la même page.

□ □

Administration des utilisateurs

Gestion des comptes d'utilisateurs

Créer un ou plusieurs utilisateurs

Les administrateurs peuvent ajouter des utilisateurs en cliquant sur espace de travail > utilisateurs et groupes > Ajouter/importer

Les utilisateurs peuvent être ajoutés individuellement ou avec une importation groupée.

[largeur=25 %]



L'inclusion d'un e-mail et d'un numéro de téléphone portable précis à ce stade améliore considérablement le processus d'activation de l'authentification multifacteur par la suite.

Une fois que vous avez créé des utilisateurs, vous pouvez cliquer sur leur nom pour voir les détails comme quand ils ont été créés, leur état de connexion (qu'ils soient actuellement connectés ou non) et quels sont leurs paramètres spécifiques.

Activation du bureau virtuel pour les utilisateurs AD existants

Si des utilisateurs sont déjà présents dans AD, vous pouvez activer le bureau virtuel des utilisateurs simplement en cliquant sur l'équipement en regard de leur nom, puis en activant leur poste de travail.[largeur=50 %]



Pour Azure AD Domain Service uniquement : pour que les connexions fonctionnent, 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 Service de domaine peut prendre jusqu'à 20 minutes. Les modifications des mots de passe dans Azure AD prennent généralement 20 minutes pour être répercutées dans ADDS et donc dans l'environnement VDS.

Supprimer le(s) compte(s) utilisateur(s)

Modifier les informations utilisateur

Sur la page de détails utilisateur, des modifications peuvent être apportées aux informations utilisateur telles que le nom d'utilisateur et les coordonnées. Les valeurs e-mail et téléphone sont utilisées pour le processus de réinitialisation du mot de passe en libre-service (SSPR).

□

Modifier les paramètres de sécurité utilisateur

- Utilisateur VDI activé – paramètre RDS qui, lorsqu'il est activé, crée un hôte de session VM dédié et affecte cet utilisateur comme seul utilisateur qui s'y connecte. Dans le cadre de l'activation de cette case, l'administrateur CWMS est invité à sélectionner l'image VM, la taille et le type de stockage.
 - Les utilisateurs VDI AVD doivent être gérés sur la page AVD en tant que pool d'hôtes VDI.
- Expiration du compte activée – permet à l'administrateur CWMS de définir une date d'expiration sur le compte d'utilisateur final.
- Forcer la réinitialisation du mot de passe lors de la prochaine connexion – invite l'utilisateur final à modifier son mot de passe lors de la prochaine connexion.
- Authentification multifacteur activée – active l'authentification multifacteur pour l'utilisateur final et l'invite à configurer l'authentification multifacteur lors de la prochaine connexion.
- Mobile Drive activé : fonction héritée non utilisée dans les déploiements actuels de RDS ou AVD.
- Accès au lecteur local activé – permet à l'utilisateur d'accéder à son périphérique local à partir de l'environnement cloud, notamment copier/coller, stockage de masse USB et lecteurs système.
- Activation du réveil à la demande : pour les utilisateurs RDS qui se connectent via le client CW pour Windows, cela leur donne la permission de prendre leur environnement lorsqu'ils se connectent en dehors des heures normales de travail définies par la planification de la charge de travail.

Compte verrouillé

Par défaut, cinq tentatives de connexion échoueront pour verrouiller le compte utilisateur. Le compte utilisateur se déverrouille au bout de 30 minutes, sauf si *Activer la complexité du mot de passe* est activé. Lorsque la complexité du mot de passe est activée, le compte ne sera pas automatiquement déverrouillé. Dans les deux cas, l'administrateur VDS peut déverrouiller manuellement le compte utilisateur à partir de la page utilisateurs/groupe dans VDS.

Réinitialiser le mot de passe utilisateur

Réinitialise le mot de passe utilisateur.

Remarque : lors de la réinitialisation des mots de passe utilisateur Azure AD (ou du déverrouillage d'un compte), il peut y avoir un délai de 20 minutes au fur et à mesure que la réinitialisation se propage via Azure AD.

Accès administrateur

En activant cette option, l'utilisateur final bénéficie d'un accès limité au portail de gestion de son locataire. Les utilisations courantes incluent l'accès d'un employé sur site à la réinitialisation des mots de passe des pairs, l'attribution d'une application ou l'autorisation d'un accès manuel au réveil du serveur. Les autorisations qui contrôlent les zones de la console peuvent être consultées sont également définies ici.

Utilisateur(s) de déconnexion

Les utilisateurs connectés peuvent être déconnectés par l'administrateur VDS à partir de la page utilisateurs/groupe dans VDS.

En termes de latence

Affiche l'application déployée dans cet espace de travail. La case à cocher contient les applications pour cet utilisateur spécifique. La documentation complète sur la gestion des applications se trouve ici. L'accès aux

applications peut également être accordé à partir de l'interface de l'application ou à des groupes de sécurité.

Afficher/tuer les processus utilisateur

Affiche les processus en cours d'exécution dans la session de cet utilisateur. Il est également possible de terminer les processus à partir de cette interface.

Gestion des autorisations des données

Du point de vue de l'utilisateur final

Les utilisateurs de Virtual Desktop peuvent avoir accès à plusieurs lecteurs mappés. Ces disques comprennent un partage d'équipe accessible aux FTPS, un partage de fichiers d'entreprise et leur disque dur d'origine (pour leurs documents, bureau, etc.) . Tous ces disques mappés font référence à une couche de stockage centrale soit sur des services de stockage (comme Azure NetApp Files), soit sur une machine virtuelle de serveur de fichiers.

Selon la configuration dont l'utilisateur peut ne pas avoir les lecteurs H: Ou F: Exposés, ils peuvent uniquement voir leur bureau, documents, etc... dossiers. En outre, différentes lettres de lecteur sont parfois définies par l'administrateur VDS au moment du déploiement.[]

[]

Gestion des autorisations

VDS permet aux administrateurs de modifier les groupes de sécurité et les autorisations de dossiers, tous depuis le portail VDS.

Groupes de sécurité

La gestion des groupes de sécurité s'effectue en cliquant sur : espaces de travail > Nom du locataire > utilisateurs et groupes > dans la section groupes

Dans cette section, vous pouvez :

1. Créer de nouveaux groupes de sécurité
2. Ajouter/Supprimer des utilisateurs aux groupes
3. Affecter des applications à des groupes
4. Activer/désactiver l'accès au lecteur local aux groupes

[]

Autorisations de dossier

Les autorisations de dossier sont gérées en cliquant sur espaces de travail > Nom du locataire > gérer (dans la section dossiers).

Dans cette section, vous pouvez :

1. Ajouter/Supprimer des dossiers
2. Attribuez des autorisations à un ou plusieurs groupes
3. Personnalisez les autorisations en lecture seule, contrôle total et aucun

[]

Droits des applications

Présentation

VDS dispose d'une fonctionnalité intégrée robuste d'automatisation des applications et de droits. Cette fonctionnalité permet aux utilisateurs d'avoir accès à différentes applications lors de la connexion à un ou plusieurs hôtes de session. Pour ce faire, certaines stratégies de groupe personnalisées masquant les raccourcis ainsi que l'automatisation placent des raccourcis de manière sélective sur les bureaux des utilisateurs.



Ce workflow ne s'applique qu'aux déploiements RDS. Pour obtenir de la documentation sur les droits d'application AVD, reportez-vous à la section "[Flux de travail des droits d'application pour AVD](#)"

Les applications peuvent être affectées directement aux utilisateurs ou via des groupes de sécurité gérés dans VDS.

La procédure de provisionnement des applications suit de manière générale cette procédure.

1. Ajouter des applications au catalogue d'applications
2. Ajouter des applications à l'espace de travail
3. Installez l'application sur tous les hôtes de session
4. Sélectionnez le chemin du raccourci
5. Attribuez des applications aux utilisateurs et/ou aux groupes



Les étapes 3 et 4 peuvent être entièrement automatisées avec des événements avec script comme illustré ci-dessous



Présentation vidéo

Ajouter des applications au catalogue d'applications

La licence d'application VDS commence par le catalogue d'applications. Il s'agit d'une liste de toutes les applications disponibles pour le déploiement dans les environnements utilisateur final.

Pour ajouter des applications au catalogue, procédez comme suit

1. Connectez-vous à VDS at <https://manage.cloudworkspace.com> à l'aide de vos informations d'identification d'administrateur principales.
2. Dans le coin supérieur droit, cliquez sur la flèche située en regard de votre Nom d'utilisateur et sélectionnez Paramètres.
3. Cliquez sur l'onglet Catalogue d'applications.
4. Cliquez sur l'option Ajouter une application dans la barre de titre du catalogue d'applications.
5. Pour ajouter un groupe d'applications, choisissez l'option Importer des applications.
 - a. Une boîte de dialogue s'affiche et fournit un modèle Excel à télécharger qui crée le format correct pour la liste des applications.
 - b. Pour cette évaluation, NetApp VDS a créé un exemple de liste d'applications destinées à être importée. Il est disponible [ici](#).
 - c. Cliquez sur la zone Télécharger et choisissez le fichier de modèle d'application, puis cliquez sur le bouton Importer.
6. Pour ajouter des applications individuelles, cliquez sur le bouton Ajouter une application et une boîte de dialogue s'affiche.
 - a. Entrez le nom de l'application.
 - b. L'ID externe peut être utilisé pour saisir un identifiant de suivi interne tel qu'une référence de produit ou un code de suivi de facturation (facultatif).
 - c. Cochez la case abonnement si vous souhaitez créer un rapport sur les applications en tant que produit abonnement (facultatif).
 - d. Si le produit ne s'installe pas par version (par exemple Chrome), cochez la case version non requise. Cela permet d'installer les produits de mise à jour continue sans suivre leurs versions.
 - e. Inversement, si un produit prend en charge plusieurs versions nommées (par exemple QuickBooks), vous devez cocher cette case pour pouvoir installer plusieurs versions et avoir VDS spécifique chaque version disponible dans la liste des applications pouvant être autorisées pour et pour l'utilisateur final.
 - f. Cochez "aucune icône de bureau utilisateur" si vous ne souhaitez pas que VDS provisionne une icône de bureau pour ce produit. Il est utilisé pour les produits « backend » comme SQL Server, car les utilisateurs finaux n'ont pas d'application à accéder.
 - g. « L'application doit être associée » impose l'installation d'une application associée. Par exemple, une application client Server peut nécessiter l'installation de SQL Server ou de MySQL.
 - h. La case Licence requise indique que VDS doit demander le téléchargement d'un fichier de licence pour une installation de cette application avant de définir l'état de l'application sur actif. Cette étape est effectuée sur la page application detail de VDS.
 - i. Visible pour tous – l'admissibilité aux applications peut être limitée à des sous-partenaires spécifiques dans une hiérarchie multicanal. Pour l'évaluation, cliquez sur la case à cocher afin que tous les utilisateurs puissent la voir dans leur liste d'applications disponibles.

Ajoutez l'application à l'espace de travail

Pour démarrer le processus de déploiement, vous allez ajouter l'application à l'espace de travail.

Pour ce faire, procédez comme suit

1. Cliquez sur espaces de travail
2. Faites défiler jusqu'à applications
3. Cliquez sur Ajouter
4. Cochez la ou les applications, entrez les informations requises, cliquez sur Ajouter une application, puis sur Ajouter des applications.

Installez l'application manuellement

Une fois l'application ajoutée à l'espace de travail, vous devez installer cette application sur tous les hôtes de session. Cette opération peut être effectuée manuellement et/ou automatiquement.

Pour installer manuellement des applications sur des hôtes de session, procédez comme suit

1. Accédez à la carte de service.
2. Cliquez sur la tâche de la carte de service.
3. Cliquez sur le(s) nom(s) du serveur pour vous connecter en tant qu'administrateur local.
4. Installez les applications, confirmez que le raccourci vers cette application se trouve dans le chemin du menu Démarrer.
 - a. Pour Server 2016 et Windows 10 : C:\ProgramData\Microsoft\Windows\Démarrer Menu\programmes.
5. Retournez à la tâche de la carte de service, cliquez sur Parcourir et choisissez le raccourci ou un dossier contenant des raccourcis.
6. Quelle que soit la sélection choisie, ce qui s'affiche sur le bureau de l'utilisateur final lorsqu'il est attribué à l'application.
7. Les dossiers sont parfaits lorsqu'une application est en fait plusieurs applications. Par exemple, « Microsoft Office » est plus facile à déployer comme dossier avec chaque application comme raccourci dans le dossier.
8. Cliquez sur Terminer l'installation.
9. Si nécessaire, ouvrez l'icône créée Ajouter une tâche de carte de service et confirmez que l'icône a été ajoutée.

Attribuez des applications aux utilisateurs

Les droits d'application sont gérés par VDS et l'application peut être attribuée aux utilisateurs de trois manières

Attribuer des applications aux utilisateurs

1. Accédez à la page User Detail.
2. Accédez à la section applications.
3. Cochez la case en regard de toutes les applications requises par cet utilisateur.

Attribuer des utilisateurs à une application

1. Accédez à la section applications de la page Détails de l'espace de travail.
2. Cliquez sur le nom de l'application.
3. Cochez la case en regard des utilisateurs de l'application.

Attribuez des applications et des utilisateurs à des groupes d'utilisateurs

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.

Réinitialiser le mot de passe utilisateur

Réinitialisez les étapes du mot de passe utilisateur

1. Accédez à la page Détails utilisés dans VDS

□

2. Recherchez la section Mot de passe, entrez le nouveau mot de passe deux fois et cliquez sur

□

□

Il est temps de prendre effet

- Pour les environnements exécutant une AD « interne » sur les VM de l'environnement, la modification du mot de passe doit prendre effet immédiatement.
- Pour les environnements exécutant Azure AD Domain Services (ADDS), la modification du mot de passe doit prendre environ 20 minutes pour prendre effet.
- Le type d'AD peut être déterminé sur la page des détails du déploiement :

□

Réinitialisation du mot de passe en libre-service (SSRP)

Le client Windows VDS NetApp et le client web VDS NetApp fourniront une invite aux utilisateurs qui saisis un mot de passe incorrect lors de la connexion à un déploiement de poste de travail virtuel v5.2 (ou ultérieur). Si l'utilisateur a verrouillé son compte, ce processus déverrouille également le compte d'un utilisateur.

Remarque : les utilisateurs doivent avoir déjà saisi un numéro de téléphone mobile ou une adresse e-mail pour que ce processus fonctionne.

SSPR est pris en charge par :

- Client NetApp VDS Window
- Client Web VDS NetApp

Dans cet ensemble d'instructions, vous allez suivre le processus d'utilisation de SSPR comme moyen simple pour permettre aux utilisateurs de réinitialiser leurs mots de passe et de déverrouiller leurs comptes.

Client Windows VDS NetApp

1. En tant qu'utilisateur final, cliquez sur le lien Mot de passe oublié pour continuer.

□

2. Indiquez si vous souhaitez recevoir votre code par téléphone mobile ou par e-mail.

□

3. Si un utilisateur final n'a fourni qu'une de ces méthodes de contact, il s'agit de la seule méthode affichée.

□

4. Après cette étape, les utilisateurs s'affichent avec un champ Code dans lequel ils doivent saisir la valeur numérique reçue soit sur leur appareil mobile, soit dans leur boîte de réception (selon la sélection). Entrez ce code suivi du nouveau mot de passe et cliquez sur Réinitialiser pour continuer.

□

5. Les utilisateurs peuvent voir une invite leur indiquant que la réinitialisation de leur mot de passe a réussi. Cliquez sur terminé pour poursuivre le processus d'ouverture de session.



Si votre déploiement utilise Azure Active Directory Domain Services, il existe une période de synchronisation des mots de passe définie par Microsoft, toutes les 20 minutes. Là encore, cette opération est contrôlée par Microsoft et ne peut pas être modifiée. Ceci étant important, VDS affiche que l'utilisateur doit attendre jusqu'à 20 minutes que son nouveau mot de passe prenne effet. Si votre déploiement n'utilise pas les services de domaine Azure Active Directory, l'utilisateur pourra se reconnecter en quelques secondes.

□

Portail HTML5

1. Si l'utilisateur ne parvient pas à saisir le mot de passe correct lorsqu'il tente de se connecter via le HTML5, il s'affiche avec une option pour réinitialiser le mot de passe :

□

2. Après avoir cliqué sur l'option pour réinitialiser leur mot de passe, ils sont présentés avec leurs options de réinitialisation :

□

3. Le bouton "demande" envoie un code généré à l'option sélectionnée (dans ce cas, l'e-mail de l'utilisateur). Le code est valide pendant 15 minutes.

□

4. Le mot de passe a été réinitialisé ! Il est important de se rappeler que Windows Active Directory aura souvent besoin d'un moment pour propager la modification de sorte que si le nouveau mot de passe ne fonctionne pas immédiatement, juste attendre quelques minutes et essayer à nouveau. Ceci est particulièrement important pour les utilisateurs résidant dans un déploiement Azure Active Directory Domain Services, où la réinitialisation d'un mot de passe peut prendre jusqu'à 20 minutes pour se propager.

□

Activation de la réinitialisation du mot de passe en libre-service (SSPR) pour les utilisateurs

Pour utiliser la fonction SSPR (Self Service Password Reset), les administrateurs doivent d'abord entrer un numéro de téléphone mobile et/ou un compte de messagerie pour un utilisateur final. Il existe deux façons de

saisir un numéro de téléphone mobile et des adresses e-mail pour un utilisateur de bureau virtuel, comme indiqué ci-dessous.

Dans cet ensemble d'instructions, vous allez suivre le processus de configuration de SSPR comme moyen simple pour les utilisateurs finaux de réinitialiser leurs mots de passe.

Importation d'utilisateurs en bloc via VDS

Commencez par naviguer jusqu'au module espaces de travail, puis utilisateurs et groupes, puis cliquez sur Ajouter/Importer.

Vous pouvez entrer ces valeurs pour les utilisateurs lors de leur création une à une :[]

Vous pouvez également les inclure lors de l'importation en bloc d'utilisateurs téléchargeant et téléchargeant le fichier XLSX préconfiguré avec ce contenu rempli :[]

Fournir les données via l'API VDS

API VDS NetApp – spécifiquement cet appel https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – permet de mettre à jour ces informations.

Mise à jour du téléphone utilisateur existant

Mettez à jour le numéro de téléphone des utilisateurs sur la page User Detail Overview dans VDS.

[]

Utilisation d'autres consoles

Remarque : actuellement, vous ne pouvez pas fournir de numéro de téléphone à un utilisateur via Azure Console, Partner Center ou depuis la console d'administration Office 365.

Personnaliser l'adresse d'envoi SSPR

Vous pouvez configurer VDS NetApp pour envoyer l'e-mail de confirmation *de* une adresse personnalisée. Il s'agit d'un service fourni à nos partenaires fournisseurs de services qui souhaitent que leurs utilisateurs finaux reçoivent l'e-mail de réinitialisation de mot de passe à envoyer à partir de leur propre domaine de messagerie personnalisé.

Cette personnalisation nécessite des étapes supplémentaires pour vérifier l'adresse d'envoi. Pour commencer ce processus, veuillez ouvrir un dossier de support avec le support VDS demandant une « adresse source de réinitialisation du mot de passe en libre-service » personnalisée. Veuillez définir les éléments suivants :

- Votre code partenaire (vous pouvez le trouver en cliquant sur *settings* dans le menu flèche haut droite vers le bas. Voir la capture d'écran ci-dessous)

[]

- Adresse « de » souhaitée (qui doit être valide)
- Pour quels clients le paramètre doit s'appliquer (ou tous)

Pour ouvrir un dossier de demande d'assistance, envoyez un e-mail à l'adresse suivante : support@spotpc.netapp.com

Une fois reçues, le support VDS s'active pour valider l'adresse avec notre service SMTP et activer ce

paramètre. Idéalement, vous aurez la possibilité de mettre à jour les enregistrements DNS publics sur le domaine d'adresse source afin d'optimiser la délivrance des e-mails.

Complexité du mot de passe

VDS peut être configurée pour imposer la complexité des mots de passe. Ce paramètre se trouve sur la page Détails de l'espace de travail de la section Paramètres de l'espace de travail cloud.

[]

[]

Complexité du mot de passe : désactivé

Politique	Directive
Longueur minimale du mot de passe	8 caractères
Âge maximum du mot de passe	110 jours
Âge minimum du mot de passe	0 jour
Appliquer l'historique du mot de passe	24 mots de passe mémorisés
Verrouillage du mot de passe	Le verrouillage automatique se produit après 5 entrées incorrectes
Durée du verrouillage	30 minutes

Complexité du mot de passe : on

Politique	Directive
Longueur minimale du mot de passe	8 caractères ne contiennent pas le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur qui dépassent deux caractères consécutifs contiennent des caractères de trois des quatre catégories suivantes : Caractères majuscules anglais (A à Z) caractères minuscules anglais (a à z) base 10 chiffres (0 à 9) caractères non alphabétiques (par exemple, !, \$, #, %) les exigences de complexité sont appliquées lorsque les mots de passe sont modifiés ou créés.
Âge maximum du mot de passe	110 jours
Âge minimum du mot de passe	0 jour
Appliquer l'historique du mot de passe	24 mots de passe mémorisés
Verrouillage du mot de passe	Le verrouillage automatique se produit après 5 entrées incorrectes
Durée du verrouillage	Reste verrouillé jusqu'à ce que l'administrateur se déverrouille

Authentification multifacteur (MFA)

Présentation

Le service NetApp Virtual Desktop Service (VDS) comprend un service MFA basé sur des SMS/e-mails sans

frais supplémentaires. Ce service est indépendant de tout autre service (p. ex. Azure conditionnel Access) et peut être utilisé pour sécuriser les connexions d'administrateur dans VDS et les connexions utilisateur aux postes de travail virtuels.

Principes de base de l'authentification multifacteur

- VDS MFA peut être attribuée aux utilisateurs admin, aux utilisateurs finaux individuels ou à tous les utilisateurs finaux
- VDS MFA peut envoyer des notifications par SMS ou par e-mail
- VDS MFA dispose d'une fonction de configuration initiale et de réinitialisation en libre-service

Portée du guide

Ce guide vous guide tout au long de la configuration de l'authentification multifacteur, ainsi qu'une illustration de l'expérience utilisateur

Ce guide aborde les sujets suivants :

1. [Activation de l'authentification multifacteur pour les utilisateurs individuels](#)
2. [Nécessite MFA pour tous les utilisateurs](#)
3. [Activation de l'authentification multifacteur pour les administrateurs individuels](#)
4. [Configuration initiale de l'utilisateur final](#)

Activation de l'authentification multifacteur pour les utilisateurs individuels

L'authentification multifacteur peut être activée pour les utilisateurs individuels sur la page de détails de l'utilisateur en cliquant sur *authentification multi-facteurs activée*

Espaces de travail > Nom de l'espace de travail > utilisateurs et groupes > Nom d'utilisateur > autorisation multi-facteurs activée > mettre à jour

L'authentification multifacteur peut également être attribuée à tous les utilisateurs. Si ce paramètre est en place, la case à cocher sera activée et (*via les paramètres du client*) sera ajouté à l'étiquette de la case à cocher.

Nécessite MFA pour tous les utilisateurs

L'authentification multifacteur peut être activée et appliquée à tous les utilisateurs de la page de détails de l'espace de travail en cliquant sur *MFA pour tous les utilisateurs activés*

Espaces de travail > Nom de l'espace de travail > MFA pour tous les utilisateurs activés > mettre à jour

Activation de l'authentification multifacteur pour les différents administrateurs

L'authentification multifacteur est également disponible pour les comptes d'administrateur accédant au portail VDS. Cette option peut être activée par administrateur sur la page de détails administrateur. Admins > Nom d'administrateur > authentification multifacteur requise > mettre à jour

Configuration initiale

Lors de la première connexion après l'activation de l'authentification multifacteur, l'utilisateur ou l'administrateur est invité à saisir une adresse électronique ou un numéro de téléphone portable. Ils recevront un code de confirmation pour saisir et confirmer la réussite de l'inscription.

Administration de système

Créez un compte d'administrateur de domaine (« niveau 3 »)

Présentation

Il arrive que les administrateurs VDS aient besoin d'informations d'identification au niveau du domaine pour gérer l'environnement. Dans VDS, il s'agit d'un compte « niveau 3 » ou «.tech ».

Ces instructions montrent comment ces comptes peuvent être créés avec les autorisations appropriées.

Contrôleur de domaine Windows Server

Lors de l'exécution d'un contrôleur de domaine hébergé en interne (ou d'un DC local lié à Azure via un routage VPN/Express) la gestion des comptes .tech peut être effectuée directement dans Active Directory Manager.

1. Connectez-vous au contrôleur de domaine (CWMGR1, DC01 ou le VM existant) avec un compte admin de domaine (.tech).
2. Créez un nouvel utilisateur (si nécessaire).
3. Ajoutez l'utilisateur au groupe de sécurité « techniciens de niveau 3 »

[Management.System Administration.create domain admin compte 9ee17] |

Management.System_Administration.create_domain_admin_account-9ee17.png

- a. Si le groupe de sécurité « Level3 Technicians » n'est pas rempli, créez-le et faites-le membre du groupe de sécurité « CW-Infrastructure ».

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



L'ajout de ".tech" à la fin du nom d'utilisateur est une meilleure pratique recommandée pour délimiter les comptes d'administrateur des comptes d'utilisateur final.

Services de domaine Azure AD

S'ils s'exécutent sur Azure AD Domain Services ou si un utilisateur gère dans Azure AD, ces comptes peuvent être gérés (par exemple, une modification du mot de passe) dans le portail de gestion Azure en tant qu'utilisateur AD Azure.

De nouveaux comptes peuvent être créés, les ajouter à ces rôles doivent leur donner les autorisations requises :

1. Administrateurs AAD DC
2. ClientDHPAccess
3. Administrateur global dans le répertoire.



L'ajout de ".tech" à la fin du nom d'utilisateur est une meilleure pratique recommandée pour délimiter les comptes d'administrateur des comptes d'utilisateur final.



Fournir un accès temporaire aux tiers

Présentation

La méthode de fourniture d'accès à des tiers est courante lors de la migration vers une solution cloud.

Les administrateurs VDS choisissent souvent de ne pas donner à ces tiers le même niveau d'accès qu'ils ont, afin de suivre une politique d'accès à la sécurité « la moins requise ».

Pour configurer l'accès administrateur pour les tiers, connectez-vous dans VDS et accédez au module organisations, cliquez sur dans l'organisation et cliquez sur utilisateurs & groupes.

Ensuite, créez un nouveau compte utilisateur pour le tiers et faites défiler vers le bas jusqu'à ce que la section accès administrateur s'affiche et cochez la case pour activer les droits d'administrateur.



L'administrateur VDS est ensuite présenté avec l'écran de configuration de l'accès administrateur. Il n'est pas nécessaire de modifier le nom d'utilisateur, le nom de connexion ou le mot de passe. Il vous suffit d'ajouter un numéro de téléphone et/ou un e-mail si vous souhaitez appliquer l'authentification multifacteur et de sélectionner le niveau d'accès à accorder.

Pour les administrateurs de bases de données comme un VAR ou un ISV, *Servers* est généralement le seul module d'accès requis.



Une fois enregistré, l'utilisateur final peut accéder aux fonctions de gestion automatique en se connectant à VDS à l'aide de ses identifiants utilisateur standard du bureau virtuel.

Lorsque l'utilisateur nouvellement créé se connecte, il ne voit que les modules que vous lui avez affectés. Ils peuvent sélectionner l'organisation, faire défiler jusqu'à la section serveurs et se connecter au nom du serveur auquel vous leur indiquez (par exemple, <XYZ> D1, où XYZ correspond au code de votre société et D1 désigne que le serveur est un serveur de données. Dans l'exemple ci-dessous, nous leur disons de se connecter au serveur TSD1 pour effectuer leurs affectations.

□

Configurer la planification des sauvegardes

Présentation

VDS a la possibilité de configurer et de gérer les services de sauvegarde natifs dans certains fournisseurs d'infrastructure, notamment Azure.

Azure

Dans Azure, VDS peut configurer automatiquement les sauvegardes à l'aide de la fonctionnalité native "[La sauvegarde dans le cloud Azure](#)" Avec stockage redondant local (LRS). Le stockage redondant géographique (GRS) peut être configuré sur le portail de gestion Azure, si nécessaire.

- Des stratégies de sauvegarde individuelles peuvent être définies pour chaque type de serveur (avec les recommandations par défaut). En outre, il est possible d'attribuer à chaque machine un planning indépendant (de son type de serveur) depuis l'interface utilisateur VDS. Ce paramètre peut être appliqué en naviguant vers la vue détaillée du serveur en cliquant sur le nom du serveur sur la page espace de travail (voir la vidéo ci-dessous : définition de stratégies de sauvegarde individuelles).
 - Les données
 - Sauvegarde avec 7 sauvegardes quotidiennes, 5 hebdomadaires et 2 sauvegardes mensuelles. Augmentez vos périodes de conservation en fonction des besoins de votre entreprise.
 - Ceci est vrai à la fois pour un serveur de données dédié et pour les machines virtuelles VPS supplémentaires pour les applications et les bases de données.
 - Infrastructures
 - CWMGR1 – sauvegarde quotidienne et conservation de 7 000 quotidiens, 5 hebdomadaires, 2 mensuels.
 - Passerelle RDS – sauvegarde hebdomadaire et conservation de 4 h/24, 7 jours/7.
 - Passerelle HTML5 : sauvegarde hebdomadaire et conservation des données toutes les 4 hebdomadaires
 - Poweruser (ou utilisateur VDI)
 - Ne sauvegardez pas la machine virtuelle car les données doivent être stockées sur un serveur D1 ou TSD1.
 - Notez que certaines applications stockent les données localement et qu'il convient de tenir compte de certaines considérations particulières.
 - En cas de défaillance d'un serveur virtuel, il est possible de créer un nouveau serveur virtuel via le clonage d'une autre. S'il n'y a qu'une seule machine virtuelle VDI (ou une seule VM build), il est conseillé de la sauvegarder afin de ne pas avoir besoin d'une reconstruction complète de ce VM.
 - Si nécessaire, au lieu de sauvegarder tous les serveurs VDI, les coûts peuvent être réduits en configurant manuellement une machine virtuelle pour effectuer des sauvegardes directement dans le portail de gestion Azure.

- TS

- Ne sauvegardez pas la machine virtuelle car les données doivent être stockées sur un serveur D1 ou TSD1.
- Notez que certaines applications stockent les données localement et qu'il convient de tenir compte de certaines considérations particulières.
- En cas de défaillance d'un serveur virtuel, il est possible de créer un nouveau serveur virtuel via le clonage d'une autre. Dans le cas où il n'y a qu'un seul TS VM, il est conseillé de le sauvegarder afin qu'une reconstruction complète de ce VM ne soit pas requise.
- Si nécessaire, plutôt que de sauvegarder tous les serveurs TS, les coûts peuvent être réduits en configurant manuellement une machine virtuelle pour effectuer une sauvegarde directement sur le portail de gestion Azure.

- TSData

- Sauvegarde avec 7 sauvegardes quotidiennes, 5 hebdomadaires et 2 sauvegardes mensuelles. Augmentez vos périodes de conservation en fonction des besoins de votre entreprise.

- Azure ne prend pas en charge plus de planifications, il est possible de définir des règles pour effectuer les sauvegardes quotidiennes ou hebdomadaires.
- Pour les planifications quotidiennes, entrez le temps préféré pour effectuer la sauvegarde. Pour les planifications hebdomadaires, saisissez le jour et l'heure préférés de la sauvegarde. Remarque : le réglage de l'heure sur exactement 12:00 AM peut entraîner des problèmes dans Azure Backup, donc 12:01 AM est recommandé.
- Définissez le nombre de sauvegardes quotidiennes, hebdomadaires, mensuelles et annuelles à conserver.

Définition des paramètres de déploiement par défaut

[]

Pour configurer Azure Backup pour l'intégralité du déploiement, effectuez la procédure suivante :

1. Accédez à la page de détails des déploiements, sélectionnez Sauvegarder les valeurs par défaut
2. Sélectionnez un type de serveur dans le menu déroulant. Les types de serveur sont :

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

- Les paramètres de sauvegarde globaux pour le déploiement complet seront définis. Ces paramètres peuvent être remplacés et définis ultérieurement à un niveau spécifique au serveur.

3. Cliquez sur la molette des paramètres, puis sur la fenêtre contextuelle Modifier qui s'affiche.
4. Sélectionnez les paramètres de sauvegarde suivants :

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

5. Enfin, cliquez sur Créer (ou Modifier) planification pour mettre ces paramètres en place.

Définition de règles de sauvegarde individuelles

Pour appliquer des paramètres de sauvegarde intégrée spécifiques au serveur, accédez à une page de détails Workspace.

1. Faites défiler jusqu'à la section serveurs et cliquez sur le nom d'un serveur
2. Cliquez sur Ajouter un planning
3. Appliquez les paramètres de sauvegarde selon vos besoins et cliquez sur Créer un programme

Restauration à partir de la sauvegarde

Pour restaurer les sauvegardes d'une machine virtuelle donnée, commencez par naviguer jusqu'à la page Détails de cet espace de travail.

1. Faites défiler jusqu'à la section serveurs et cliquez sur le nom d'un serveur
2. Faites défiler jusqu'à la section sauvegardes et cliquez sur la molette pour développer vos options, puis sélectionnez l'une ou l'autre
3. Restaurer vers le serveur ou restaurer sur le disque (reliez un lecteur de la sauvegarde afin de pouvoir copier les données de la sauvegarde vers la version existante de la machine virtuelle).
4. Procédez à la restauration à partir de ce point, comme vous le feriez dans tout autre scénario de restauration.



Les coûts dépendent de la planification que vous souhaitez gérer et sont entièrement déterminés par le coût de la sauvegarde Azure. Pour la sauvegarde des machines virtuelles, consultez le calculateur de coûts Azure : <https://azure.microsoft.com/en-us/pricing/calculator/>

Clonage de machines virtuelles

Présentation

Virtual Desktop Service (VDS) permet de cloner une machine virtuelle existante. Cette fonctionnalité est conçue pour augmenter automatiquement la disponibilité du nombre d'unités serveur en fonction du nombre d'utilisateurs défini, ou pour augmenter le nombre de serveurs en fonction des pools de ressources disponibles.

Les administrateurs utilisent le clonage dans VDS de deux manières :

1. Création automatisée à la demande d'un nouveau serveur à partir d'un serveur client existant
2. Création automatisée proactive de nouveaux serveurs clients pour la mise à l'échelle automatique des ressources en fonction des règles définies et contrôlées par les partenaires

Clonage pour ajouter des serveurs partagés supplémentaires

Un clone désigne la copie d'une machine virtuelle existante. L'installation d'un système d'exploitation invité et d'applications peut prendre du temps et permettre aux administrateurs d'évoluer. Avec les clones, vous pouvez effectuer de nombreuses copies d'une machine virtuelle depuis un processus d'installation et de configuration unique. Cela se présente généralement comme suit :

1. Installez toutes les applications et tous les paramètres souhaités sur un serveur TS ou TSD
2. Accédez à : espace de travail > Section serveurs > icône engrenage du serveur source > cliquez sur Cloner
3. Exécuter le processus de clonage (généralement 45-90 minutes)
4. La dernière étape active le serveur cloné, en le mettant dans le pool RDS pour accepter de nouvelles connexions. Les serveurs clonés peuvent nécessiter une configuration individuelle après le clonage. Ainsi, VDS attend que l'administrateur place manuellement le serveur en rotation.

Répétez autant de fois que nécessaire.[]

Pour augmenter la capacité des utilisateurs dans un environnement hôte de session partagée, le clonage d'un hôte de session est un processus simple nécessitant seulement quelques étapes.

1. Sélectionnez un hôte de session à cloner, vérifiez qu'aucun utilisateur n'est actuellement connecté à la machine.
2. Dans VDS, accédez à l'espace de travail du client cible. Faites défiler jusqu'à la section serveurs, cliquez sur l'icône engrenage et sélectionnez Cloner. Ce processus prend beaucoup de temps et met la machine source hors ligne. Plus de 30 minutes suffisent pour le faire.

[] []

3. Le processus arrête le serveur, le clone vers une autre image et Sysprep l'image vers le TS# suivant pour le client. Le serveur s'affiche sous la forme *Type=échelleed* et *Status=activation required* dans la liste serveurs.

[]

4. Connectez-vous au serveur et vérifiez que le serveur est prêt pour la production.

[]

5. Lorsque vous êtes prêt, cliquez sur Activer pour ajouter le serveur au pool hôte de session pour commencer à accepter les connexions utilisateur.

[]

Définition du processus de clonage VDS

Le processus étape par étape est détaillé dans VDS > déploiement > Historique des tâches sous toutes les opérations du serveur de clonage. Le processus comprend plus de 20 étapes qui commencent par accéder à l'hyperviseur pour démarrer le processus de clonage et se termine par l'activation du serveur cloné. Le processus de clonage comprend des étapes clés :

- Configurez DNS et définissez le nom du serveur
- Attribuez l'adresse StaticIP
- Ajouter au domaine

- Mettre à jour Active Directory
- Mettre à jour la base de données VDS (instance SQL sur CWMGR1)
- Créer des règles de pare-feu pour le clone

Outre l'historique des tâches, vous pouvez afficher les étapes détaillées de tout processus de clonage dans le journal CwVmAutomationService de CWMGR1 de chaque partenaire Virtual Desktop Deployment. La vérification de ces fichiers journaux est documentée ["ici"](#).

Création automatisée de nouveau(s) serveur(s)

Cette fonctionnalité VDS a été conçue pour augmenter automatiquement la disponibilité du nombre d'unités serveur en fonction de l'augmentation du nombre d'utilisateurs défini.

Le partenaire définit et gère via VDS ("") > client > Présentation – VM Resources > Auto-Scaling. Plusieurs contrôles sont exposés pour permettre aux partenaires d'activer/désactiver la mise à l'échelle automatique et de créer des règles personnalisées pour chaque client, telles que : nombre/utilisateurs/serveur, RAM supplémentaire par utilisateur et nombre d'utilisateurs par CPU.



Avant tout, le clonage automatisé est activé pour l'intégralité du déploiement de postes de travail virtuels. Par exemple, pour arrêter tout le clonage automatisé, utilisez DCConfig, dans la fenêtre Avancé, décochez la case création du serveur → clonage automatisé activé.

Quand le processus de clonage automatisé s'exécute-t-il ?

Le processus de clonage automatisé s'exécute lorsque la maintenance quotidienne est configurée. La valeur par défaut est minuit, mais elle peut être modifiée. Une partie de la maintenance quotidienne consiste à exécuter le thread de modification des ressources pour chaque pool de ressources. Le thread Modifier les ressources détermine le nombre de serveurs partagés requis en fonction du nombre d'utilisateurs de la configuration du pool (personnalisable ; peut être 10, 21, 30, etc. Par serveur).

Création automatisée de nouveau serveur « à la demande »

Cette fonctionnalité VDS permet le clonage automatique « à la demande » de serveurs supplémentaires vers les pools de ressources disponibles.

L'administrateur VDS se connecte à VDS et sous les organisations ou modules espaces de travail, trouve le client spécifique et ouvre l'onglet Présentation. La mosaïque serveurs répertorie tous les serveurs (TSD1, TS1, D1, etc.). Pour cloner un serveur individuel, cliquez simplement sur le bouton à l'extrême droite du nom du serveur et sélectionnez l'option Cloner.

Le processus devrait généralement prendre environ une heure. Toutefois, la durée dépend de la taille de la machine virtuelle et des ressources disponibles de l'hyperviseur sous-jacent. Notez que le serveur cloné doit être redémarré. Les partenaires doivent donc généralement fonctionner après plusieurs heures ou durant une fenêtre de maintenance planifiée.

Lors du clonage d'un serveur TSDData, l'une des étapes consiste à supprimer les dossiers c:\Home, c:\Data et c:\Pro de sorte qu'ils ne sont pas des fichiers en double. Dans ce cas, le processus de clonage a échoué lors de la suppression de ces fichiers, Cette erreur est vague. En général, cela signifie que l'événement de clonage a échoué parce qu'un fichier ou un processus est ouvert. Prochaine tentative, désactivez tout AV (car cela pourrait expliquer cette erreur).

Augmenter automatiquement l'espace disque

Présentation

NetApp reconnaît le besoin de donner aux administrateurs un moyen simple de s'assurer que les utilisateurs ont toujours de l'espace pour accéder et enregistrer les documents. Cela permet également de s'assurer que les machines virtuelles disposent d'un espace suffisant pour effectuer correctement les sauvegardes, ce qui donne aux administrateurs et aux plans de reprise après incident et de continuité de l'activité. Dans cette optique, nous avons mis en place une fonctionnalité qui étend automatiquement le disque géré utilisé au niveau suivant lorsqu'un disque manque d'espace.

Il s'agit d'un paramètre appliqué par défaut sur tous les nouveaux déploiements VDS dans Azure, garantissant que tous les déploiements protègent les utilisateurs et les sauvegardes du locataire par défaut.

Les administrateurs peuvent vérifier qu'ils sont en place en accédant à l'onglet déploiements, en sélectionnant un déploiement, puis en se connectant à leur serveur CWMGR1 à partir de là. Ouvrez ensuite le raccourci DCConfig sur le bureau, puis cliquez sur Avancé et faites défiler vers le bas.

[]

Les administrateurs peuvent modifier la quantité d'espace libre souhaitée en Go libre ou en pourcentage du lecteur qui doit être libre avant de passer au niveau suivant des disques gérés dans la même section avancée de DCConfig.

[]

Quelques exemples d'application pratiques :

- Si vous souhaitez vous assurer qu'au moins 50 Go sont disponibles sur votre lecteur, définissez MinFreeSpaceGB sur 50
- Si vous voulez vous assurer qu'au moins 15 % de votre disque est libre, réglez MinFreeSpacePercent de 10 à 15.

Cette action a lieu à minuit sur le fuseau horaire du serveur.

Accès aux identifiants VDS dans Azure Key Vault

Présentation

CWASetup 5.4 est une solution de départ des méthodes de déploiement Azure précédentes. Le processus de configuration et de validation est rationalisé et réduit la quantité d'informations nécessaires au déploiement. Nombre de ces invites supprimées concernent des informations d'identification ou des comptes tels que l'administrateur VM local, le compte SMTP, le compte Tech, SQL sa, etc. Ces comptes sont désormais générés et stockés automatiquement dans un coffre-fort Azure Key. Par défaut, l'accès à ces comptes générés automatiquement nécessite une étape supplémentaire, décrite ci-dessous.

- Recherchez la ressource « coffre-fort de clés » et cliquez dessus :

[largeur=75 %]

- Sous 'Paramètrés', cliquez sur 'tours'. Vous verrez un message indiquant que vous n'êtes pas autorisé à afficher :

[largeur=75 %]

- Ajoutez une « politique d'accès » pour accorder un compte AD Azure (comme un administrateur global ou un administrateur système) à ces clés sensibles :

[largeur=75 %]

- Un administrateur global est utilisé dans cet exemple. Après avoir sélectionné le principal, cliquez sur 'Sélectionner', puis sur 'Ajouter' :

[largeur=75 %]

- Cliquez sur « Enregistrer » :

[largeur=75 %]

- La stratégie d'accès a été ajoutée avec succès :

[largeur=75 %]

- Revoyez les « tourelles » pour vérifier que le compte a désormais accès aux comptes de déploiement :

[largeur=75 %]

- Par exemple, si vous avez demandé à l'administrateur de domaine de se connecter à CWMGR1 et de mettre à jour la stratégie de groupe, vérifiez les chaînes sous `cjDomainAdministratorName` et `cjDomainAdministratorPassword` en cliquant sur chaque entrée :

[largeur=75 %]

[largeur=75 %]

- Afficher ou copier la valeur :

[largeur=75 %]

Appliquez les fonctions de surveillance et d'antivirus

Présentation

Les administrateurs VDS (Virtual Desktop Service) sont responsables de la surveillance de l'infrastructure de leur plateforme (composée au minimum de CWMGR1) et de toutes les autres infrastructures et machines virtuelles (VM). Dans la plupart des cas, les administrateurs organisent la surveillance de l'infrastructure (hyperviseur/SAN) directement avec leur fournisseur de services de data Center/laaS. Les administrateurs sont responsables de la surveillance des serveurs terminal Server et des serveurs de données, généralement en déployant leur solution de gestion et de surveillance à distance (RMM) préférée.

L'antivirus est de la responsabilité de l'administrateur (à la fois pour l'infrastructure de plate-forme et les machines virtuelles de serveur terminal/données). Pour rationaliser ce processus, Windows Defender est appliqué par défaut sur les serveurs VDS pour Azure.



Lors de l'installation de solutions tierces, veillez à ne pas inclure de pare-feu ou d'autres composants susceptibles d'interférer avec l'automatisation VDS.

Plus précisément, lorsque des stratégies antivirus très spécifiques sont en place par défaut, cela peut entraîner des effets indésirables lorsque ces agents antivirus sont installés sur un serveur géré par Virtual

Desktop Service.

Nous avons pour objectif général que, bien que l'automatisation de la plate-forme VDS n'ait généralement pas d'incidence sur les produits anti-virus ou anti-Malware, il est recommandé d'ajouter des exceptions/exclusions pour les processus suivants sur tous les serveurs de plate-forme (CWMGR1, RDGS0, HTML5Gateways, FTP, etc.) :

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

De plus, nous vous recommandons de lister en toute sécurité les processus suivants sur les serveurs clients :

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

Ajout et déplacement de lecteurs mappés

Présentation

Par défaut, trois dossiers partagés sont exposés aux sessions de l'utilisateur final. Ces dossiers se trouvent sur la couche de stockage définie. Cela peut se trouver sur le serveur de fichiers (TSD1 ou D1) ou sur un service de stockage tel qu'Azure Files, Azure NetApp Files, NetApp CVO et NetApp CVS.

Pour faciliter la clarté, cet article utilisera un exemple de client avec le code de société "NECA". Cet exemple suppose qu'un seul serveur TDS1 a été déployé, appelé NECATSD1. Nous travaillerons tout au long du processus de déplacement d'un dossier vers une autre VM (nommée "NECAD1"). Cette stratégie peut être utilisée pour se déplacer entre la partition sur la même machine ou vers une autre machine comme indiqué dans l'exemple suivant...

Dossier emplacement de départ :

- Données : NECATSD1\C:\data\NECA\ (TSD1 signifie qu'il s'agit du premier serveur terminal Server et qu'il fonctionne également comme serveur de données)
- FTP : NECATSD1\C:\FTP\NECA\
- Home: NECATSD1\C:\home\NECA\

Emplacement de fin des dossiers :

- Données : NECAD1\G:\data\NECA\ (le D1 signifie qu'il s'agit du 1er serveur de données)
- FTP : le même processus s'applique, il n'est pas nécessaire de le décrire trois fois
- Accueil : le même processus s'applique, pas besoin de le décrire trois fois

Ajouter un disque pour G : sur NECAD1

1. Pour placer le dossier partagé sur le lecteur E:, nous devons en ajouter un par l'intermédiaire de l'hyperviseur (par exemple Azure Management Portal), puis initialise et formatez-le

□

2. Copier le dossier existant (sur NECATSD1, C:\) chemin vers le nouvel emplacement (sur NECAD1, G:\)
3. Copiez le(s) dossier(s) de l'emplacement d'origine vers le nouvel emplacement.

□

Collecter des informations à partir du partage de dossiers d'origine (NECATSD1, C:\data\NECA)

1. Partagez le nouveau dossier en utilisant exactement le même chemin que le dossier à l'emplacement d'origine.
2. Ouvrez le nouveau dossier NECAD1, G:\data\ et vous verrez dans notre exemple un dossier nommé code société, « NECA ».

□

3. Notez les autorisations de sécurité du partage de dossier d'origine :

□

4. Voici la configuration type, mais il est important de copier les paramètres d'origine au cas où il existe des personnalisations existantes que nous devons conserver. Toutes les autres autorisations utilisateur/groupe doivent être supprimées du nouveau partage de dossier
 - SYSTÈME:toutes les autorisations autorisées
 - LocalClientDHPAccess (sur l'ordinateur local):toutes les autorisations sont autorisées
 - ClientDHPAccess (sur le domaine) : toutes les autorisations sont autorisées
 - NECA-tous les utilisateurs (sur le domaine) : toutes les autorisations sauf "contrôle total" autorisées

Répliquez le chemin de partage et les autorisations de sécurité dans le nouveau dossier partagé

1. Revenir au nouvel emplacement (NECAD1, G:\data\NECA\ et partager le dossier NECA avec le même chemin réseau (à l'exception de la machine), dans notre exemple « neca-data\$ »

□

2. Pour la sécurité des utilisateurs, ajoutez tous les utilisateurs, définissez leurs autorisations de manière à ce qu'elles correspondent.

□

3. Supprimez toutes les autres autorisations utilisateur/groupe qui existent peut-être déjà.



Modifier la stratégie de groupe (uniquement si le dossier est déplacé vers une nouvelle machine)

1. Vous allez ensuite modifier les cartes de lecteur dans l'éditeur de gestion des stratégies de groupe. Pour les services de domaine Azure AD, le mappage est situé dans :

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



2. Une fois la stratégie de groupe mise à jour, la prochaine fois que chaque utilisateur se connecte, il voit les lecteurs mappés qui sont dirigés vers le nouvel emplacement.
3. A ce stade, vous pouvez supprimer les dossiers d'origine sur NECATSD1, C:\.

Dépannage

Si l'utilisateur final voit les lecteurs mappés avec un X rouge, cliquez avec le bouton droit de la souris sur le lecteur et sélectionnez déconnecter. Déconnectez-vous puis revenez dans le lecteur correctement.[]

Informations sur le copyright

Copyright © 2023 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 DÉLICTEUELLE (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.