Administration des utilisateurs

Virtual Desktop Service

NetApp
November 18, 2022

Table des matières

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/groupes 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/groupes 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 saisir 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. MFA for Individual Users,Activation de l'authentification multifacteur pour les utilisateurs individuels
2. MFA for All Users,Nécessite MFA pour tous les utilisateurs
3. MFA for Individual Administrators ,Activation de l'authentification multifacteur pour les administrateurs individuels
4. User Initial Setup,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.