Administration de système

Virtual Desktop Service

NetApp
November 18, 2022

Table des matières

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] |

Management.System_Administration.create_domain_admin_account-0fc27.png

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 TSData, 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 ‘Paramètress’, cliquez sur ‘tourets’. 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/IaaS. 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\ (TSD1signifie 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 D1signifie 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.[]