Gestion du stockage NAS

ONTAP 9

NetApp
August 14, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/concept_nas_provision_overview.html on August 14, 2025. Always check docs.netapp.com for the latest.

Sommaire

Gestion du stockage NAS . . . 1
Gérez les protocoles NAS avec System Manager . . . 1
En savoir plus sur la gestion NAS avec ONTAP System Manager . . . 1
Provisionnez le stockage NFS pour les banques de données VMware avec ONTAP System Manager . . . 1
Provisionnez le stockage NAS pour les répertoires personnels avec ONTAP System Manager . . . 2
Provisionner le stockage NAS pour les serveurs Linux à l'aide de NFS avec ONTAP System Manager . . . 3
Gérer l'accès à l'aide de politiques d'exportation avec ONTAP System Manager . . . 5
Provisionnez le stockage NAS pour les serveurs Windows à l'aide de SMB avec ONTAP System Manager . . . 6
Provisionnez le stockage NAS pour Windows et Linux en utilisant NFS et SMB avec ONTAP System Manager . . . 8
Accès client sécurisé avec Kerberos à l'aide d'ONTAP System Manager . . . 11
Fournir un accès client avec des services de noms à l'aide d'ONTAP System Manager . . . 12
Gérez les répertoires et les fichiers avec ONTAP System Manager . . . 13
Gérez les utilisateurs et les groupes spécifiques à l'hôte avec ONTAP System Manager . . . 13
Surveiller les clients NFS actifs avec ONTAP System Manager . . . 17
Activez le stockage NAS . . . 17
Configurez NFS avec l'interface de ligne de commande . . . 21
En savoir plus sur la configuration NFS avec l'interface de ligne de commande ONTAP . . . 21
En savoir plus sur le flux de travail de configuration ONTAP NFS . . . 22
Préparation . . . 23
Configurer l'accès NFS à un SVM . . . 36
Ajout de capacité de stockage à un SVM compatible NFS . . . 73
Où trouver des informations supplémentaires sur ONTAP NFS . . . 87
La différence entre les exportations ONTAP et les exportations 7-mode . . . 89
Gérez NFS avec l'interface de ligne de commande . . . 93
En savoir plus sur l'accès aux fichiers ONTAP pour le protocole NFS . . . 93
Compréhension de l'accès aux fichiers NAS . . . 93
Création et gestion des volumes de données dans les espaces de noms NAS . . . 101
Configurer les styles de sécurité . . . 107
Configurez l'accès aux fichiers à l'aide de NFS . . . 112
Gérer l'accès aux fichiers à l'aide de NFS . . . 150
Versions NFS et clients pris en charge . . . 206
Dépendances de nommage des fichiers et des répertoires NFS et SMB . . . 210
Gérer l'agrégation NFS . . . 216
En savoir plus sur l'agrégation de liens ONTAP NFS . . . 216
Configurer un nouveau serveur NFS et des exportations pour l'agrégation . . . 217
Adaptation des exportations NFS existantes pour l'agrégation . . . 222
Gestion de NFS sur RDMA . . . 227
Découvrez NFS over RDMA dans ONTAP . . . 227
Configurer les cartes réseau pour NFS sur RDMA . . . 229
Configuration des LIF pour NFS sur RDMA . . . 231
Modifier la configuration NFS . . . 234

Configurez SMB avec l'interface de ligne de commandes . . . 234
En savoir plus sur la configuration SMB avec l'interface de ligne de commande ONTAP . . . 234
Flux de travail de configuration SMB ONTAP . . . 235
Préparation . . . 236
Configuration de l'accès SMB à un SVM . . . 247
Configurez l'accès client SMB au stockage partagé . . . 269
Gestion de SMB avec l'interface de ligne de commandes . . . 279
Découvrez ONTAP SMB . . . 279
Prise en charge du serveur SMB . . . 279
Gérer les serveurs SMB . . . 286
Configurez l'accès aux fichiers à l'aide de SMB . . . 386
Gérer l'accès aux fichiers via SMB . . . 454
Déploiement des services basés sur les clients SMB . . . 549
Déployez les services basés sur serveur SMB . . . 564
Dépendances de nommage des fichiers et des répertoires NFS et SMB . . . 636
Offrez un accès client S3 aux données NAS . . . 642
En savoir plus sur la prise en charge multiprotocole ONTAP S3 . . . 642
En savoir plus sur les exigences de données NAS pour l'accès client ONTAP S3 . . . 645
Activer l'accès au protocole S3 aux données NAS sur une SVM ONTAP . . . 646
Créer un bucket NAS ONTAP S3 . . . 649
Activer les utilisateurs du client ONTAP S3 . . . 651
Configuration SMB pour Microsoft Hyper-V et SQL Server . . . 654
Présentation de la configuration SMB pour Microsoft Hyper-V et SQL Server . . . 654
Configuration de ONTAP pour Microsoft Hyper-V et SQL Server sur les solutions SMB . . . 655
Continuité de l'activité pour Hyper-V et SQL Server over SMB . . . 656
Partage de sauvegardes avec VSS distant . . . 660
Comment l'allègement de la charge des copies d'ODX est utilisé avec Hyper-V et SQL Server sur des partages SMB . . . 664
Configuration requise et considérations . . . 665
Recommandations concernant les configurations SQL Server et Hyper-V sur SMB . . . 673
Planifiez la configuration Hyper-V ou SQL Server sur SMB . . . 674
Créez des configurations ONTAP pour la continuité de l'activité avec Hyper-V et SQL Server over SMB . . . 677
Gérez les configurations Hyper-V et SQL Server sur SMB . . . 691
Utilisez les statistiques pour surveiller l'activité Hyper-V et SQL Server sur SMB . . . 696
Vérifiez que la configuration permet la continuité de l'activité . . . 699

Gestion du stockage NAS

Gérez les protocoles NAS avec System Manager

En savoir plus sur la gestion NAS avec ONTAP System Manager

Les rubriques de cette section vous expliquent comment configurer et gérer les environnements NAS avec System Manager dans ONTAP 9.7 et versions ultérieures.

Si vous utilisez System Manager classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous aux rubriques suivantes :

- "Présentation de la configuration NFS"
- "Présentation de la configuration SMB"

System Manager prend en charge les flux de production pour :

- Configuration initiale des clusters que vous prévoyez d'utiliser pour les services de fichiers NAS.
- Provisionnement de volumes supplémentaire pour répondre à l'évolution des besoins de stockage.
- Configuration et maintenance pour les installations de sécurité et d'authentification standard.

System Manager vous permet de gérer les services NAS au niveau des composants :

- Protocoles : NFS, SMB ou les deux (NAS multiprotocole)
- Services de noms : DNS, LDAP et NIS
- Nommer le commutateur de service
- Sécurité Kerberos et TLS
- Exportations et partages
- Qtrees
- Mappage des noms des utilisateurs et des groupes

Provisionnez le stockage NFS pour les banques de données VMware avec ONTAP System Manager

Avant d'utiliser Virtual Storage Console pour VMware vSphere (VSC) pour provisionner des volumes NFS sur un système de stockage ONTAP pour les hôtes ESXi, activez NFS à l'aide de System Manager pour ONTAP 9.7 ou version ultérieure.

Après avoir créé un "Machine virtuelle de stockage compatible NFS" Dans System Manager, vous pouvez ensuite provisionner des volumes NFS et gérer des datastores à l'aide de VSC.

VSC fait partie du produit depuis la version 7.0 de VSC "Appliance virtuelle ONTAP Tools pour VMware vSphere", Qui inclut VSC, le fournisseur vStorage APIs for Storage Awareness (VASA) et l'outil Storage Replication adapter (SRA) pour les fonctionnalités VMware vSphere.

Assurez-vous de vérifier le "Matrice d'interopérabilité NetApp" Pour vérifier la compatibilité entre vos versions actuelles de ONTAP et VSC.

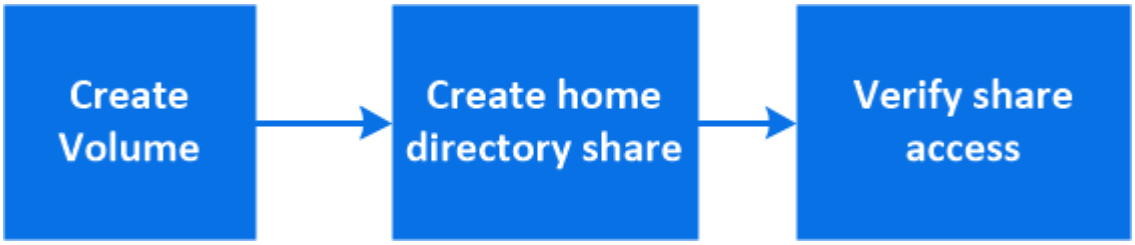
Pour configurer l'accès NFS pour les hôtes ESXi aux datastores à l'aide de System Manager Classic (pour ONTAP 9.7 et les versions antérieures), voir "Présentation de la configuration NFS pour ESXi à l'aide de VSC"

Pour plus d'informations, voir "Tr-4597 : VMware vSphere pour ONTAP" Et de la documentation relative à la version de VSC.

Provisionnez le stockage NAS pour les répertoires personnels avec ONTAP System Manager

Créez des volumes pour fournir un stockage pour les répertoires locaux à l'aide du protocole SMB.

Cette procédure crée de nouveaux volumes pour des répertoires locaux sur un "VM de stockage compatible SMB". Vous pouvez accepter les valeurs par défaut des systèmes lors de la configuration de volumes ou de la spécification de configurations personnalisées.



Vous pouvez créer des volumes FlexVol ou, pour les systèmes de fichiers volumineux avec des exigences de performances élevées, vous pouvez créer des volumes FlexGroup . Voir aussi "Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes" .

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page "Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN".

Étapes

1. Ajout d'un nouveau volume dans une machine virtuelle de stockage compatible SMB
   a. Sélectionnez **stockage > volumes**, puis cliquez sur **Ajouter**.
   b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

      Seules les machines virtuelles de stockage configurées avec le protocole SMB sont répertoriées. Si une seule machine virtuelle de stockage configurée avec le protocole SMB est disponible, le champ **Storage VM** n'est pas affiché.

      - Si vous cliquez sur **Enregistrer** à ce stade, System Manager utilise les valeurs par défaut du système pour créer et ajouter un volume FlexVol.
      - Vous pouvez cliquer sur **plus d'options** pour personnaliser la configuration du volume afin d'activer des services tels que l'autorisation, la qualité de service et la protection des données. Reportez-vous à la section Personnaliser la configuration de volume, puis revenez ici pour effectuer les étapes suivantes.
2. cliquez sur **stockage > partages**, cliquez sur **Ajouter** et sélectionnez **répertoire d'accueil**.
3. Sur un client Windows, procédez comme suit pour vérifier que le partage est accessible.
   a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant : `\\<SMB_Server_Name>\<Share_Name>`

Si le nom du partage a été créé avec des variables (%w, %d ou %u), vérifiez l'accès avec un nom résolu.

b. Sur le lecteur nouvellement créé, créez un fichier test, puis supprimez le fichier.

Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

Étapes

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

  Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

  - Pour désactiver QoS, sélectionnez **personnalisé**, **existant**, puis **aucun**.
  - Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
  - À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

    Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

  Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.

Une fois le volume enregistré, revenez à étape 2 dans le flux de travail pour effectuer le provisionnement complet des répertoires locaux.

Provisionner le stockage NAS pour les serveurs Linux à l'aide de NFS avec ONTAP System Manager

Créez des volumes pour fournir un stockage pour les serveurs Linux en utilisant le protocole NFS avec ONTAP System Manager (9.7 et versions ultérieures).

Cette procédure crée de nouveaux volumes sur un "VM de stockage existante compatible NFS". Vous pouvez accepter les valeurs par défaut du système lors de la configuration de volumes ou spécifier des configurations

personnalisées.

Vous pouvez créer des volumes FlexVol ou, pour les systèmes de fichiers volumineux avec des exigences de performances élevées, vous pouvez créer des volumes FlexGroup . Voir aussi "Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes" .

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page "Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN".

Pour plus d'informations sur la gamme de fonctionnalités du protocole ONTAP NFS, consultez le "En savoir plus sur l'accès aux fichiers ONTAP pour le protocole NFS".

Étapes

1. Ajoutez un nouveau volume dans une VM de stockage compatible NFS.
   a. Cliquez sur **Storage > volumes**, puis sur **Add**.
   b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

      Seules les machines virtuelles de stockage configurées avec le protocole NFS sont répertoriées. Si une seule machine virtuelle de stockage configurée avec le protocole SMB est disponible, le champ **Storage VM** n'est pas affiché.

      - Si vous cliquez sur **Enregistrer** à ce stade, System Manager utilise les valeurs par défaut du système pour créer et ajouter un volume FlexVol.

        La stratégie d'exportation par défaut accorde un accès complet à tous les utilisateurs.

      - Vous pouvez cliquer sur **plus d'options** pour personnaliser la configuration du volume afin d'activer des services tels que l'autorisation, la qualité de service et la protection des données. Reportez-vous à la section Personnaliser la configuration de volume, puis revenez ici pour effectuer les étapes suivantes.
2. sur un client Linux, procédez comme suit pour vérifier l'accès.
   a. Créez et montez le volume à l'aide de l'interface réseau du VM de stockage.
   b. Sur le volume récemment monté, créez un fichier test, écrivez du texte et supprimez le fichier.

   Après avoir vérifié l'accès, vous pouvez "limitez l'accès client grâce à l'export policy du volume" Et définissez les droits de propriété et les autorisations UNIX souhaités sur le volume monté.

Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

Étapes

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

  - Pour désactiver QoS, sélectionnez **personnalisé**, **existant**, puis **aucun**.
  - Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
  - À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

    Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

  Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.

Une fois le volume enregistré, revenez à [step2-complete-prov] Pour terminer le provisionnement des serveurs Linux à l'aide de NFS.

D'autres façons de le faire dans ONTAP

Pour effectuer cette tâche avec…	Reportez-vous à…
System Manager Classic (ONTAP 9.7 et versions antérieures)	"Présentation de la configuration NFS"
Interface de ligne de commande ONTAP	"En savoir plus sur la configuration NFS avec l'interface de ligne de commande ONTAP"

Gérer l'accès à l'aide de politiques d'exportation avec ONTAP System Manager

Activez l'accès client Linux aux serveurs NFS à l'aide de règles d'exportation.

Cette procédure crée ou modifie des export-policies pour un "VM de stockage existante compatible NFS".

Étapes

1. Dans System Manager, cliquez sur **Storage** > **volumes**.
2. Cliquez sur un volume compatible NFS et cliquez sur **plus**.
3. Cliquez sur **Modifier la stratégie d'exportation**, puis sur **Sélectionner une stratégie existante** ou **Ajouter une nouvelle stratégie**.

Provisionnez le stockage NAS pour les serveurs Windows à l'aide de SMB avec ONTAP System Manager

Créer des volumes pour fournir un stockage aux serveurs Windows à l'aide du protocole SMB utilisant System Manager, disponible avec ONTAP 9.7 et versions ultérieures.

Cette procédure crée de nouveaux volumes sur un "VM de stockage compatible SMB" et crée un partage pour le répertoire racine du volume (/). Vous pouvez accepter les valeurs par défaut des systèmes lors de la configuration de volumes ou de la spécification de configurations personnalisées. Une fois la configuration SMB initiale effectuée, vous pouvez également créer des partages supplémentaires et modifier leurs propriétés.

Vous pouvez créer des volumes FlexVol ou, pour les systèmes de fichiers volumineux avec des exigences de performances élevées, vous pouvez créer des volumes FlexGroup . Voir aussi "Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes" .

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page "Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN".

Pour plus d'informations sur la gamme de fonctionnalités du protocole SMB de ONTAP, consultez le "Aperçu des références".

Avant de commencer

- Depuis ONTAP 9.13.1, vous pouvez activer l'analyse de la capacité et le suivi des activités par défaut sur les nouveaux volumes. Dans System Manager, vous pouvez gérer les paramètres par défaut au niveau du cluster ou de la VM de stockage. Pour plus d'informations, voir "Activez l'analyse du système de fichiers".

Étapes

1. Ajout d'un nouveau volume dans une machine virtuelle de stockage compatible SMB
   a. Cliquez sur **Storage > volumes**, puis sur **Add**.
   b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

      Seules les machines virtuelles de stockage configurées avec le protocole SMB sont répertoriées. Si une seule machine virtuelle de stockage configurée avec le protocole SMB est disponible, le champ **Storage VM** n'est pas affiché.

      - Si vous sélectionnez **Enregistrer** à ce stade, System Manager utilise les paramètres par défaut du système pour créer et ajouter un volume FlexVol.
      - Vous pouvez sélectionner **plus d'options** pour personnaliser la configuration du volume afin d'activer des services tels que l'autorisation, la qualité de service et la protection des données. Reportez-vous à la section Personnaliser la configuration de volume, puis revenez ici pour effectuer les étapes suivantes.
2. [[step2-complète-Prov-win,étape 2 du flux de travail] passer à un client Windows pour vérifier que le partage est accessible.
   a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant : `\\_SMB_Server_Name__Share_Name_`
   b. Sur le lecteur nouvellement créé, créez un fichier test, écrivez du texte et supprimez le fichier.

Après vérification de l'accès, vous pouvez restreindre l'accès du client à l'aide de la liste de contrôle d'accès du partage et définir toutes les propriétés de sécurité souhaitées sur le lecteur mappé. Voir "Créer des

partages" pour plus d'informations.

Ajouter ou modifier des partages

Vous pouvez ajouter des partages supplémentaires après la configuration SMB initiale. Les partages sont créés avec les valeurs et les propriétés par défaut que vous sélectionnez. Ils peuvent être modifiés ultérieurement.

Vous pouvez définir les propriétés de partage suivantes lors de la configuration d'un partage :

- Autorisations d'accès
- Propriétés du partage
  - Disponibilité sans interruption pour les partages qui contiennent des données Hyper-V et SQL Server sur SMB (à partir de ONTAP 9.10.1). Voir aussi :
    - "Exigences de partage disponibles en continu pour Hyper-V sur SMB"
    - "Exigences de partage constamment disponibles pour SQL Server sur SMB"
  - Chiffrez les données avec SMB 3.0 lors de l'accès à ce partage.

Après la configuration initiale, vous pouvez également modifier les propriétés suivantes :

- Liens symboliques
  - Activez ou désactivez les liens symlinks et les boutons de fonction
- Propriétés du partage
  - Autoriser les clients à accéder au répertoire des snapshots.
  - Activez oplocks, ce qui permet aux clients de verrouiller les fichiers et le contenu en cache localement (par défaut).
  - Activez l'énumération basée sur l'accès (ABE) pour afficher les ressources partagées en fonction des autorisations d'accès de l'utilisateur.

Étapes

1. Pour ajouter un nouveau partage dans un volume compatible SMB, cliquez sur **stockage > partages**, cliquez sur **Ajouter** et sélectionnez **partage**.
2. Pour modifier un partage existant, cliquez sur **stockage > partages**, puis cliquez sur ⋮ et sélectionnez **Modifier**.

Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les valeurs par défaut du système.

Étapes

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

  Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

- Pour désactiver QoS, sélectionnez **personnalisé**, **existant**, puis **aucun**.
- Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
- À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

  Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

  Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.

Une fois le volume enregistré, revenez à [step2-compl-prov-win] Pour effectuer le provisionnement complet des serveurs Windows avec SMB.

D'autres façons de le faire dans ONTAP

Pour effectuer cette tâche avec…	Reportez-vous à…
System Manager Classic (ONTAP 9.7 et versions antérieures)	"Présentation de la configuration SMB"
Interface de ligne de commande ONTAP	"Présentation de la configuration SMB avec l'interface de ligne de commande"

Provisionnez le stockage NAS pour Windows et Linux en utilisant NFS et SMB avec ONTAP System Manager

Créer des volumes afin de fournir un stockage aux clients qui utilisent le protocole NFS ou SMB.

Cette procédure crée de nouveaux volumes sur un "VM de stockage existante activée pour les protocoles NFS et SMB".

Le protocole NFS est généralement utilisé dans les environnements Linux. Le protocole SMB est généralement utilisé dans les environnements Windows. Cependant, NFS et SMB peuvent être utilisés avec Linux ou Windows.

Vous pouvez créer des volumes FlexVol ou, pour les systèmes de fichiers volumineux avec des exigences de performances élevées, vous pouvez créer des volumes FlexGroup . Voir "Provisionnez le stockage NAS pour les systèmes de fichiers volumineux à l'aide de FlexGroup volumes" .

Vous pouvez également enregistrer les spécifications de ce volume dans un PlayBook Ansible. Pour plus d'informations, consultez la page "Utilisez les manuels de vente Ansible pour ajouter ou modifier des volumes ou des LUN".

Étapes

1. Ajoutez un nouveau volume dans une machine virtuelle de stockage activée pour les protocoles NFS et SMB.

   a. Cliquez sur **Storage > volumes**, puis sur **Add**.

   b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

      Seules les machines virtuelles de stockage configurées avec les protocoles NFS et SMB sont répertoriées. Si une seule machine virtuelle de stockage configurée avec les protocoles NFS et SMB est disponible, le champ **Storage VM** n'est pas affiché.

   c. Cliquez sur **plus d'options** et sélectionnez **Exporter via NFS**.

      Le paramètre par défaut permet un accès complet à tous les utilisateurs. Vous pouvez ajouter ultérieurement des règles plus restrictives à l'export policy.

   d. Sélectionnez **partager via SMB/CIFS**.

      Le partage est créé avec une liste de contrôle d'accès par défaut (ACL) définie sur « contrôle total » pour le groupe **Everyone**. Vous pouvez ajouter des restrictions à la liste de contrôle d'accès ultérieurement.

   e. Si vous cliquez sur **Enregistrer** à ce stade, System Manager utilise les valeurs par défaut du système pour créer et ajouter un volume FlexVol.

   Vous pouvez également continuer à activer tous les services supplémentaires requis, tels que l'autorisation, la qualité de services et la protection des données. Reportez-vous à la section Personnaliser la configuration de volume, puis revenez ici pour effectuer les étapes suivantes.

2. sur un client Linux, vérifiez que l'exportation est accessible.

   a. Créez et montez le volume à l'aide de l'interface réseau du VM de stockage.

   b. Sur le volume récemment monté, créez un fichier test, écrivez du texte et supprimez le fichier.

3. Sur un client Windows, procédez comme suit pour vérifier que le partage est accessible.

   a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant : `\\_SMB_Server_Name__Share_Name_`

   b. Sur le lecteur nouvellement créé, créez un fichier test, écrivez du texte et supprimez le fichier.

   Après avoir vérifié l'accès, vous pouvez "Limitez l'accès client à l'aide de la règle d'export du volume ; limitez l'accès client à l'aide de la liste de contrôle d'accès de partage"et définir la propriété et les autorisations souhaitées sur le volume exporté et partagé.

Personnaliser la configuration de volume

Vous pouvez personnaliser la configuration du volume lorsque vous ajoutez des volumes au lieu d'accepter les

valeurs par défaut du système.

Étapes

Après avoir cliqué sur **plus d'options**, sélectionnez la fonctionnalité dont vous avez besoin et saisissez les valeurs requises.

- Cache pour le volume distant.
- Niveau de service de performance (qualité de service, QoS)

  Depuis la version ONTAP 9.8, vous pouvez spécifier une règle de QoS personnalisée ou désactiver la QoS, en plus de la sélection de valeur par défaut.

  - Pour désactiver QoS, sélectionnez **personnalisé**, **existant**, puis **aucun**.
  - Si vous sélectionnez **personnalisé** et spécifiez un niveau de service existant, un niveau local est automatiquement choisi.
  - À partir de ONTAP 9.9.1, si vous choisissez de créer un niveau de service de performances personnalisé, vous pouvez utiliser System Manager pour sélectionner manuellement le niveau local (**placement manuel**) sur lequel vous souhaitez placer le volume que vous créez.

    Cette option n'est pas disponible si vous sélectionnez les options de cache distant ou de volume FlexGroup.

- Volumes FlexGroup (sélectionnez **distribuer les données de volume sur le cluster**).

  Cette option n'est pas disponible si vous avez précédemment sélectionné **placement manuel** sous **niveau de service de performance**. Sinon, le volume que vous ajoutez devient par défaut un volume FlexVol.

- Autorisations d'accès pour les protocoles pour lesquels le volume est configuré.
- Protection des données avec SnapMirror (local ou distant), spécifiez ensuite la règle de protection et les paramètres du cluster de destination dans les listes déroulantes.
- Sélectionnez **Save** pour créer le volume et l'ajouter au cluster et à la machine virtuelle de stockage.

Une fois le volume enregistré, revenez à [step2-compl-prov-nfs-smb] Pour assurer un provisionnement multiprotocole complet pour les serveurs Windows et Linux.

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager Classic (ONTAP 9.7 et versions antérieures)	"Présentation de la configuration multiprotocole SMB et NFS"
Interface de ligne de commande ONTAP	• "Présentation de la configuration SMB avec l'interface de ligne de commande" • "En savoir plus sur la configuration NFS avec l'interface de ligne de commande ONTAP" • "En savoir plus sur les styles de sécurité et leurs effets" • "Sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole"

Accès client sécurisé avec Kerberos à l'aide d'ONTAP System Manager

Activez Kerberos pour sécuriser l'accès au stockage des clients NAS.

Cette procédure configure Kerberos sur une machine virtuelle de stockage existante activée pour "NFS" ou "PME".

Avant de commencer, vous devez avoir configuré les DNS, NTP et "LDAP" sur le système de stockage.

Étapes

1. Sur la ligne de commande ONTAP, définissez les autorisations UNIX pour le volume racine de la machine virtuelle de stockage.

   a. Affichez les autorisations pertinentes sur le volume racine de la VM de stockage : `volume show -volume root_vol_name-fields user,group,unix-permissions`. Pour en savoir plus, `volume show` consultez le "Référence de commande ONTAP".

      Le volume root du VM de stockage doit avoir la configuration suivante :

Nom…	Paramètre…
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	755

   a. Si ces valeurs ne sont pas affichées, utilisez la `volume modify` commande pour les mettre à jour. Pour en savoir plus, `volume modify` consultez le "Référence de commande ONTAP".

2. Définissez les autorisations utilisateur pour le volume racine de l'ordinateur virtuel de stockage.

   a. Afficher les utilisateurs UNIX locaux : `vserver services name-service unix-user show -vserver vserver_name`. Pour en savoir plus, `vserver services name-service unix-user show` consultez le "Référence de commande ONTAP".

      La machine virtuelle de stockage doit avoir les utilisateurs UNIX suivants configurés :

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal
nfs	500	0
racine	0	0

+
Remarque : l'utilisateur NFS n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS ; voir l'étape 5.

   a. Si ces valeurs ne sont pas affichées, utilisez la `vserver services name-service unix-user modify` commande pour les mettre à jour. Pour en savoir plus, `vserver services name-service unix-user modify` consultez le "Référence de commande ONTAP".

3. Définissez les autorisations de groupe pour le volume racine de VM de stockage.

   a. Afficher les groupes UNIX locaux : `vserver services name-service unix-group show -vserver vserver_name`. Pour en savoir plus, `vserver services name-service unix-group show` consultez le "Référence de commande ONTAP".

      La machine virtuelle de stockage doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0

   a. Si ces valeurs ne sont pas affichées, utilisez la `vserver services name-service unix-group modify` commande pour les mettre à jour. Pour en savoir plus, `vserver services name-service unix-group modify` consultez le "Référence de commande ONTAP".

4. Basculez dans System Manager pour configurer Kerberos
5. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage** et sélectionnez la machine virtuelle de stockage.
6. Cliquez sur **Paramètres**.
7. Cliquez → sous Kerberos.
8. Cliquez sur **Ajouter** sous domaine Kerberos, puis complétez les sections suivantes :
   - Ajouter un Royaume Kerberos

     Entrez les détails de configuration selon le fournisseur de KDC.

   - Ajouter l'interface réseau au Royaume

     Cliquez sur **Ajouter** et sélectionnez une interface réseau.

9. Si vous le souhaitez, ajoutez des mappages à partir des noms de principal Kerberos aux noms d'utilisateur locaux.
   a. Cliquez sur **Storage > Storage VM** et sélectionnez la VM de stockage.
   b. Cliquez sur **Paramètres**, puis cliquez → sous **mappage de noms**.
   c. Sous **Kerberos à UNIX**, ajoutez des modèles et des remplacements à l'aide d'expressions régulières.

Fournir un accès client avec des services de noms à l'aide d'ONTAP System Manager

Activez ONTAP pour rechercher des informations sur l'hôte, l'utilisateur, le groupe ou le groupe réseau à l'aide de LDAP ou NIS pour authentifier les clients NAS.

Cette procédure crée ou modifie des configurations LDAP ou NIS sur une VM de stockage existante activée pour "NFS" ou "PME".

Pour les configurations LDAP, vous devez disposer des détails de configuration LDAP requis dans votre environnement et vous devez utiliser un schéma LDAP ONTAP par défaut.

Étapes

1. Configurez le service requis : cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sur pour LDAP ou NIS.
3. Inclure toute modification dans le commutateur de services de noms : cliquez sous commutateur de services de noms.

Gérez les répertoires et les fichiers avec ONTAP System Manager

Développez l'affichage des volumes de System Manager pour afficher et supprimer des répertoires et des fichiers.

Depuis ONTAP 9.9.1, les répertoires sont supprimés avec la fonctionnalité de suppression asynchrone de répertoires à faible latence.

Pour plus d'informations sur l'affichage des systèmes de fichiers dans ONTAP 9.9.1 et versions ultérieures, voir "Présentation de l'analytique du système de fichiers".

Étape

1. Sélectionnez **stockage > volumes**. Développez un volume pour afficher son contenu.

Gérez les utilisateurs et les groupes spécifiques à l'hôte avec ONTAP System Manager

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour gérer les utilisateurs et les groupes spécifiques à un hôte UNIX ou Windows.

Vous pouvez effectuer les opérations suivantes :

Répertoires de base	UNIX
• Afficher les utilisateurs et les groupes Windows • [add-edit-delete-Windows] • [manage-windows-users]	• Afficher les utilisateurs et les groupes UNIX • [add-edit-delete-UNIX] • [manage-unix-users]

Afficher les utilisateurs et les groupes Windows

Dans System Manager, vous pouvez afficher la liste des utilisateurs et groupes Windows.

Étapes

1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez la VM de stockage, puis sélectionnez l'onglet **Paramètres**.
3. Faites défiler jusqu'à la zone **utilisateurs et groupes hôtes**.

   La section **Windows** affiche un récapitulatif du nombre d'utilisateurs dans chaque groupe associé à la machine virtuelle de stockage sélectionnée.

4. Cliquez dans la section **Windows**.
5. Cliquez sur l'onglet **groupes**, puis cliquez sur en regard d'un nom de groupe pour afficher les détails sur ce groupe.

6. Pour afficher les utilisateurs d'un groupe, sélectionnez-le, puis cliquez sur l'onglet **utilisateurs**.

Ajouter, modifier ou supprimer un groupe Windows

Dans System Manager, vous pouvez gérer les groupes Windows en les ajoutant, en les modifiant ou en les supprimant.

Étapes

1. Dans System Manager, affichez la liste des groupes Windows. Reportez-vous à la section Afficher les utilisateurs et les groupes Windows.
2. Dans l'onglet **groupes**, vous pouvez gérer les groupes avec les tâches suivantes :

Pour effectuer cette action…	Procédez comme suit…
Ajouter un groupe	1. Cliquez sur + Add . 2. Entrez les informations du groupe. 3. Spécifiez les privilèges. 4. Spécifiez les membres du groupe (ajoutez des utilisateurs locaux, des utilisateurs de domaine ou des groupes de domaines).
Modifier un groupe	1. En regard du nom du groupe, cliquez sur ⋮, puis sur **Modifier**. 2. Modifier les informations du groupe.
Supprimer un groupe	1. Cochez la case en regard du ou des groupes que vous souhaitez supprimer. 2. Cliquez sur Delete . **Remarque :** vous pouvez également supprimer un seul groupe en cliquant ⋮ à côté du nom du groupe, puis en cliquant sur **Supprimer**.

Gérer les utilisateurs Windows

Dans System Manager, vous pouvez gérer les utilisateurs Windows en les ajoutant, en les modifiant, en les supprimant, en les activant ou en les désactivant. Vous pouvez également modifier le mot de passe d'un utilisateur Windows.

Étapes

1. Dans System Manager, affichez la liste des utilisateurs du groupe. Reportez-vous à la section Afficher les utilisateurs et les groupes Windows.
2. Dans l'onglet **Users**, vous pouvez gérer les utilisateurs avec les tâches suivantes :

Pour effectuer cette action…	Procédez comme suit…

Ajouter un utilisateur	1. Cliquez sur + Add . 2. Entrez les informations utilisateur.
Modifier un utilisateur	1. En regard du nom d'utilisateur, cliquez sur ⋮, puis sur **Modifier**. 2. Modifier les informations utilisateur.
Supprimer un utilisateur	1. Cochez la case en regard du ou des utilisateurs que vous souhaitez supprimer. 2. Cliquez sur Delete . **Remarque :** vous pouvez également supprimer un seul utilisateur en cliquant ⋮ à côté du nom d'utilisateur, puis en cliquant sur **Supprimer**.
Modifier le mot de passe utilisateur	1. En regard du nom d'utilisateur, cliquez sur ⋮, puis sur **Modifier le mot de passe**. 2. Entrez le nouveau mot de passe et confirmez-le.
Activez un utilisateur	1. Cochez la case en regard de chaque utilisateur désactivé que vous souhaitez activer. 2. Cliquez sur Enable .
Désactiver un utilisateur	1. Cochez la case en regard de chaque utilisateur activé que vous souhaitez désactiver. 2. Cliquez sur Disable .

Afficher les utilisateurs et les groupes UNIX

Dans System Manager, vous pouvez afficher la liste des utilisateurs et groupes UNIX.

Étapes

1. Dans System Manager, cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez la VM de stockage, puis sélectionnez l'onglet **Paramètres**.
3. Faites défiler jusqu'à la zone **utilisateurs et groupes hôtes**.

   La section **UNIX** affiche un récapitulatif du nombre d'utilisateurs dans chaque groupe associé à la machine virtuelle de stockage sélectionnée.

4. Cliquez → dans la section **UNIX**.
5. Cliquez sur l'onglet **groupes** pour afficher les détails de ce groupe.
6. Pour afficher les utilisateurs d'un groupe, sélectionnez-le, puis cliquez sur l'onglet **utilisateurs**.

Ajouter, modifier ou supprimer un groupe UNIX

Dans System Manager, vous pouvez gérer les groupes UNIX en les ajoutant, en les modifiant ou en les supprimant.

Étapes

1. Dans System Manager, afficher la liste des groupes UNIX. Reportez-vous à la section Afficher les utilisateurs et les groupes UNIX.
2. Dans l'onglet **groupes**, vous pouvez gérer les groupes avec les tâches suivantes :

Pour effectuer cette action…	Procédez comme suit…
Ajouter un groupe	1. Cliquez sur + Add . 2. Entrez les informations du groupe. 3. (Facultatif) spécifiez les utilisateurs associés.
Modifier un groupe	1. Sélectionnez le groupe. 2. Cliquez sur Edit . 3. Modifier les informations du groupe. 4. (Facultatif) Ajouter ou supprimer des utilisateurs.
Supprimer un groupe	1. Sélectionnez le ou les groupes que vous souhaitez supprimer. 2. Cliquez sur Delete .

Gérer les utilisateurs UNIX

Dans System Manager, vous pouvez gérer les utilisateurs Windows en les ajoutant, en les modifiant ou en les supprimant.

Étapes

1. Dans System Manager, affichez la liste des utilisateurs du groupe. Reportez-vous à la section Afficher les utilisateurs et les groupes UNIX.
2. Dans l'onglet **Users**, vous pouvez gérer les utilisateurs avec les tâches suivantes :

Pour effectuer cette action…	Procédez comme suit…
Ajouter un utilisateur	1. Cliquez sur + Add . 2. Entrez les informations utilisateur.
Modifier un utilisateur	1. Sélectionnez l'utilisateur que vous souhaitez modifier. 2. Cliquez sur Edit . 3. Modifier les informations utilisateur.

Supprimer un utilisateur	1. Sélectionnez le ou les utilisateurs que vous souhaitez supprimer. 2. Cliquez sur Delete .

Surveiller les clients NFS actifs avec ONTAP System Manager

Depuis ONTAP 9.8, System Manager affiche les connexions client NFS actives lorsque NFS est sous licence sur un cluster.

Vous pouvez ainsi vérifier rapidement quels clients NFS sont activement connectés à une machine virtuelle de stockage, qui est connectée mais inactive et qui sont déconnectés.

Pour chaque adresse IP de client NFS, l'affichage **NFS clients** indique :
* Heure du dernier accès
* Adresse IP de l'interface réseau
* Version de connexion NFS
* Nom de la VM de stockage

En outre, une liste de clients NFS actifs au cours des 48 dernières heures est également affichée dans l'affichage **Storage> volumes** et un nombre de clients NFS est inclus dans l'affichage **Dashboard**.

Étape

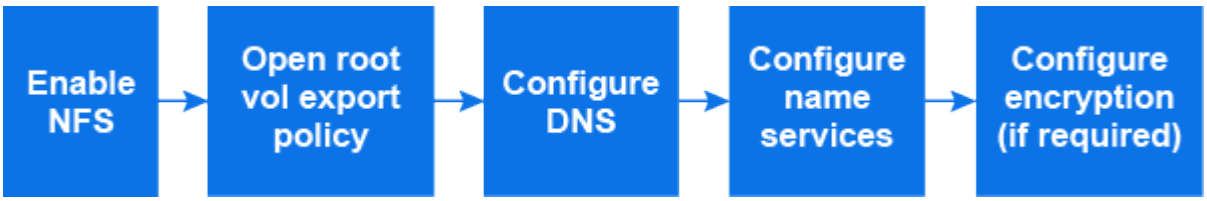
1. Afficher l'activité client NFS : cliquez sur **hôtes > clients NFS**.

Activez le stockage NAS

Activer le stockage NAS pour les serveurs Linux à l'aide de NFS avec ONTAP System Manager

Créez ou modifiez des VM de stockage afin de permettre aux serveurs NFS de transmettre des données aux clients Linux.

Utilisez cette procédure pour activer une machine virtuelle de stockage nouvelle ou existante pour le protocole NFS.



Avant de commencer

Vérifiez que vous avez bien noté les détails de configuration des services de réseau, d'authentification ou de sécurité requis dans votre environnement.

Étapes

1. Activez NFS sur une VM de stockage.
    - Pour les nouvelles machines virtuelles de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur **Ajouter**, entrez un nom de machine virtuelle de stockage et, dans l'onglet **SMB/CIFS, NFS, S3**, sélectionnez **Activer NFS**.

i. Confirmez la langue par défaut.

ii. Ajouter des interfaces réseau.

iii. Mise à jour des informations de compte administrateur de VM de stockage (facultatif)

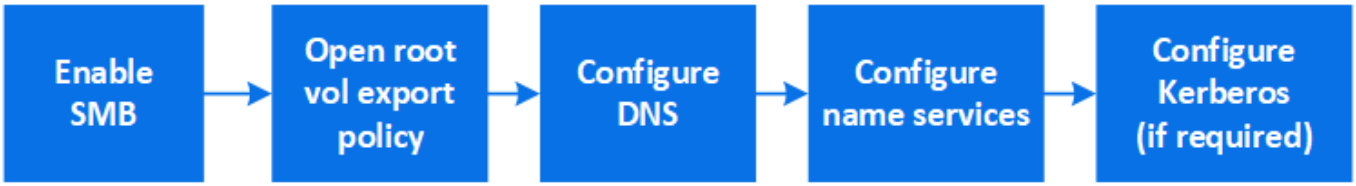
- Pour les machines virtuelles de stockage existantes : cliquez sur **Storage > Storage VMs**, sélectionnez une machine virtuelle de stockage, cliquez sur **Settings**, puis cliquez sous **NFS**.

2. Ouvrir la export policy du volume root de la VM de stockage :
   a. Cliquez sur **Storage > volumes**, sélectionnez le volume racine de la machine virtuelle de stockage (qui est par défaut *nom-volume* _root), puis cliquez sur la stratégie affichée sous **règles d'exportation**.
   b. Cliquez sur **Ajouter** pour ajouter une règle.
      - Spécification client = `0.0.0.0/0`
      - Protocoles d'accès = NFS
      - Détails d'accès = UNIX en lecture seule
3. Configurer DNS pour la résolution des noms d'hôte : cliquez sur **stockage > Storage VM**, sélectionnez la VM de stockage, cliquez sur **Paramètres**, puis cliquez sous **DNS** .
4. Configurez les services de noms si nécessaire.
   a. Cliquez sur **stockage > Storage VMs**, sélectionnez la VM de stockage, cliquez sur **Paramètres**, puis cliquez sur pour LDAP ou NIS.
   b. Cliquez sur la mosaïque changement de services de noms pour inclure les modifications.
5. Configurez Kerberos si nécessaire :
   a. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
   b. Cliquez dans la mosaïque Kerberos, puis cliquez sur **Ajouter**.

Activer le stockage NAS pour les serveurs Windows à l'aide de SMB avec ONTAP System Manager

Créez ou modifiez des VM de stockage afin de permettre aux serveurs SMB de transmettre des données aux clients Windows.

Cette procédure active une machine virtuelle de stockage nouvelle ou existante pour le protocole SMB. Nous partons du principe que des informations de configuration sont disponibles pour tous les services de réseau, d'authentification ou de sécurité requis dans votre environnement.



Étapes

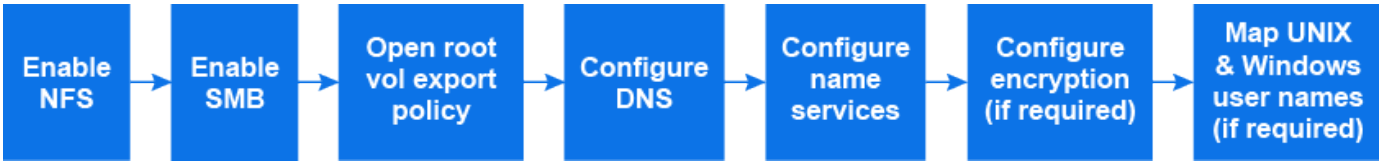
1. Activation de SMB sur une VM de stockage
   a. Pour les nouvelles machines virtuelles de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur **Ajouter**, entrez un nom de machine virtuelle de stockage et, dans l'onglet **SMB/CIFS, NFS, S3**, sélectionnez **Activer SMB/CIFS**.
      - Saisissez les informations suivantes :

        - Nom et mot de passe de l'administrateur
        - Nom du serveur
        - Domaine Active Directory
      - Confirmez l'unité organisationnelle.
      - Confirmez les valeurs DNS.
      - Confirmez la langue par défaut.
      - Ajouter des interfaces réseau.
      - Mise à jour des informations de compte administrateur de VM de stockage (facultatif)
    b. Pour les machines virtuelles de stockage existantes : cliquez sur **Storage > Storage VMS**, sélectionnez une machine virtuelle de stockage, cliquez sur **Settings**, puis cliquez sous **SMB** .
2. Ouvrir la export policy du volume root de la VM de stockage :
    a. Cliquez sur **Storage > volumes**, sélectionnez le volume racine de la machine virtuelle de stockage (qui est par défaut *nom-volume_root*), puis cliquez sur la stratégie affichée sous **règles d'exportation**.
    b. Cliquez sur **Ajouter** pour ajouter une règle.
      - Spécification client = `0.0.0.0/0`
      - Protocoles d'accès = SMB
      - Informations d'accès = NTFS lecture seule
3. Configurer le DNS pour la résolution de nom d'hôte :
    a. Cliquez sur **Storage > Storage VMs**, sélectionnez la VM de stockage, cliquez sur **Settings**, puis cliquez sous **DNS**.
    b. Basculez sur le serveur DNS et mappez le serveur SMB.
      - Créer des entrées de recherche de transfert (A - enregistrement d'adresse) et de retour (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de l'interface du réseau de données.
      - Si vous utilisez des alias NetBIOS, créez une entrée de recherche nom canonique d'alias (enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de l'interface de réseau de données du serveur SMB.
4. Configurez les services de noms si nécessaire
    a. Cliquez sur **stockage > Storage VMS**, sélectionnez la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sous **LDAP** ou **NIS**.
    b. Incluez les modifications dans le fichier de commutateur de services de noms : cliquez sous **commutateur de services de noms**.
5. Configurez Kerberos si nécessaire :
    a. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
    b. Cliquez sous **Kerberos**, puis cliquez sur **Add**.

Activez le stockage NAS pour Windows et Linux en utilisant NFS et SMB avec ONTAP System Manager

Créez ou modifiez des VM de stockage afin que les serveurs NFS et SMB puissent transmettre des données aux clients Linux et Windows.

Utilisez cette procédure pour activer une machine virtuelle de stockage, nouvelle ou existante, et desservir à la fois les protocoles NFS et SMB.



Avant de commencer

Vérifiez que vous avez bien noté les détails de configuration des services de réseau, d'authentification ou de sécurité requis dans votre environnement.

Étapes

1. Activez les protocoles NFS et SMB sur une VM de stockage.
   a. Pour les nouvelles machines virtuelles de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur **Ajouter**, entrez un nom de machine virtuelle de stockage et, dans l'onglet **SMB/CIFS, NFS, S3**, sélectionnez **Activer SMB/CIFS** et **Activer NFS**.
   b. Saisissez les informations suivantes :
      - Nom et mot de passe de l'administrateur
      - Nom du serveur
      - Domaine Active Directory
   c. Confirmez l'unité organisationnelle.
   d. Confirmez les valeurs DNS.
   e. Confirmez la langue par défaut.
   f. Ajouter des interfaces réseau.
   g. Mise à jour des informations de compte administrateur de VM de stockage (facultatif)
   h. Pour les machines virtuelles de stockage existantes : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage, puis cliquez sur **Paramètres**. Suivez les sous-étapes suivantes si NFS ou SMB n'est pas déjà activé.
      - Cliquez ⚙ sous **NFS**.
      - Cliquez ⚙ sous **SMB**.
2. Ouvrir la export policy du volume root de la VM de stockage :
   a. Cliquez sur **Storage > volumes**, sélectionnez le volume racine de la machine virtuelle de stockage (qui est par défaut *nom-volume_root*), puis cliquez sur la stratégie affichée sous **règles d'exportation**.
   b. Cliquez sur **Ajouter** pour ajouter une règle.
      - Spécification client = `0.0.0.0/0`
      - Protocoles d'accès = NFS
      - Détails d'accès = NFS en lecture seule
3. Configurer le DNS pour la résolution de nom d'hôte :
   a. Cliquez sur **Storage > Storage VMs**, sélectionnez la VM de stockage, cliquez sur **Settings**, puis cliquez ⚙ sous **DNS**.
   b. Une fois la configuration DNS terminée, basculer sur le serveur DNS et mapper le serveur SMB.

- Créer des entrées de recherche de transfert (A - enregistrement d'adresse) et de retour (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de l'interface du réseau de données.
- Si vous utilisez des alias NetBIOS, créez une entrée de recherche nom canonique d'alias (enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de l'interface de réseau de données du serveur SMB.

4. Configurer les services de noms selon les besoins :
   a. Cliquez sur **stockage > Storage VMs**, sélectionnez la VM de stockage, cliquez sur **Paramètres**, puis cliquez sur pour LDAP ou NIS.
   b. Incluez les modifications dans le fichier de commutateur de services de noms : cliquez sous **commutateur de services de noms**.
5. Configurez Kerberos si nécessaire :
   a. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.
   b. Cliquez dans la mosaïque Kerberos, puis cliquez sur **Ajouter**.
6. Mappez les noms d'utilisateur UNIX et Windows si nécessaire : cliquez sous **mappage de noms**, puis cliquez sur **Ajouter**.

   Vous ne devez le faire que si votre site possède des comptes d'utilisateur Windows et UNIX qui ne correspondent pas implicitement, c'est-à-dire lorsque la version minuscule de chaque nom d'utilisateur Windows correspond au nom d'utilisateur UNIX. Vous pouvez mapper des noms d'utilisateur à l'aide de LDAP, NIS ou utilisateurs locaux. Si vous avez deux ensembles d'utilisateurs qui ne correspondent pas, vous devez configurer le mappage de noms.

Configurez NFS avec l'interface de ligne de commande

En savoir plus sur la configuration NFS avec l'interface de ligne de commande ONTAP

Vous pouvez utiliser les commandes de l'interface de ligne de commande de ONTAP 9 pour configurer l'accès des clients NFS aux fichiers contenus dans un nouveau volume ou qtree dans une nouvelle machine virtuelle de stockage (SVM) ou existante.

Suivez les procédures ci-dessous pour configurer l'accès à un volume ou à un qtree de la manière suivante :

- Vous souhaitez utiliser toute version de NFS actuellement prise en charge par ONTAP : NFS v3, NFS V4, NFS v4.1, NFSv4.2 ou NFSv4.1 avec pNFS.
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

  Pour utiliser System Manager pour configurer l'accès multiprotocole NAS, reportez-vous à "Provisionnement de stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB"la section .
- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.

  Pour en savoir plus sur la syntaxe des commandes"Référence de commande ONTAP", consultez le .
- Les autorisations liées au fichier UNIX seront utilisées pour sécuriser le nouveau volume.

- Vous disposez des privilèges d'administrateur de cluster et non des privilèges d'administrateur de SVM.

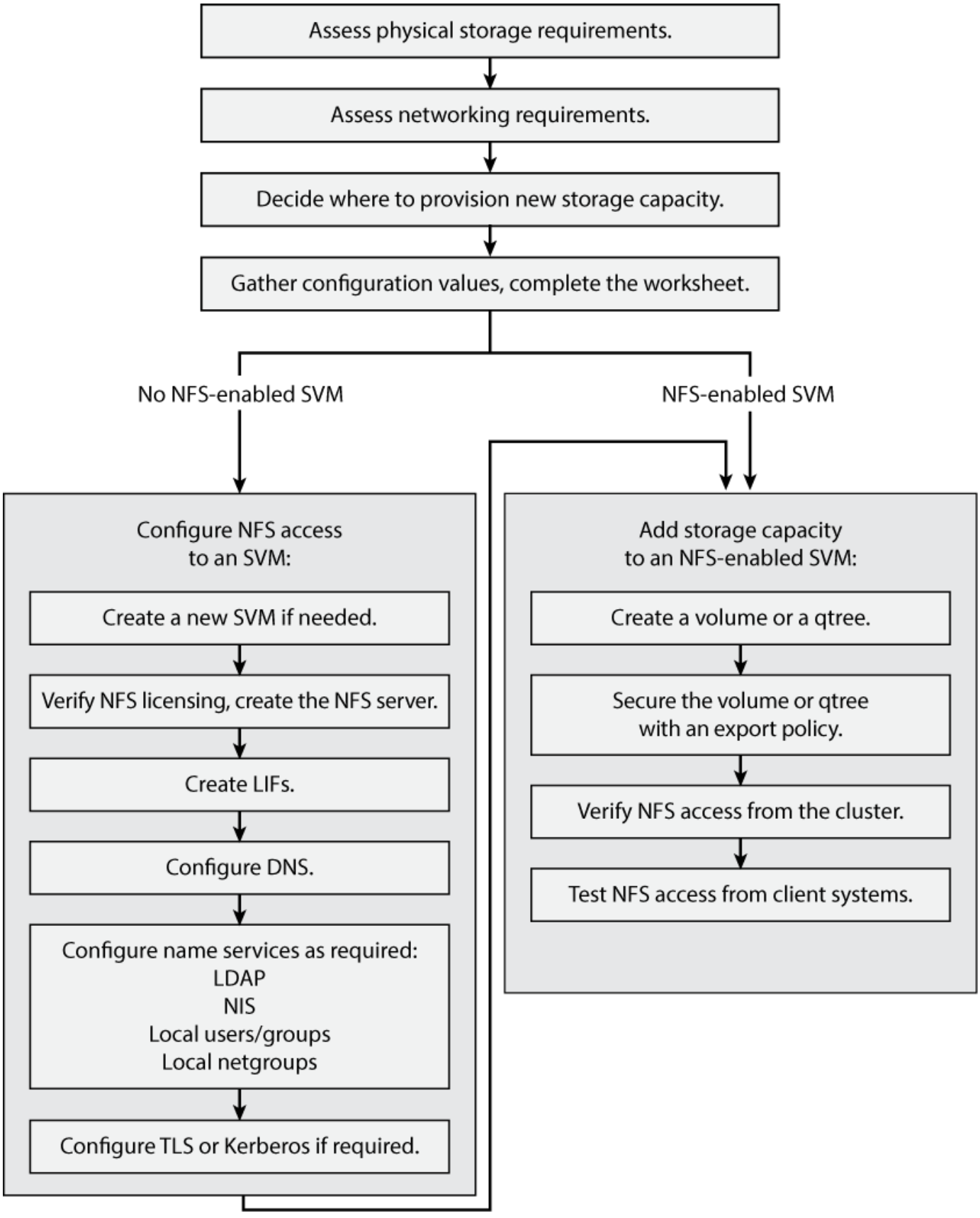
Pour plus d'informations sur la gamme de fonctionnalités du protocole ONTAP NFS, consultez le "En savoir plus sur l'accès aux fichiers ONTAP pour le protocole NFS".

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Reportez-vous à…
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Provisionnement du stockage NAS pour les serveurs Linux via NFS"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la configuration NFS"

En savoir plus sur le flux de travail de configuration ONTAP NFS

La configuration de NFS implique l'évaluation des besoins en stockage physique et en réseau, puis le choix d'un workflow spécifique à votre objectif : configurer l'accès NFS à un SVM nouveau ou existant, ou ajouter un volume ou un qtree à un SVM existant déjà entièrement configuré pour l'accès NFS.



Préparation

Évaluez les besoins en stockage physique ONTAP NFS

Avant de provisionner le stockage NFS pour les clients, vous devez vérifier que l'espace disponible sur un agrégat est suffisant pour le nouveau volume. Si ce n'est pas le cas, vous pouvez ajouter des disques à un agrégat existant ou créer un nouvel agrégat du type souhaité.

Étapes

1. Afficher l'espace disponible dans les agrégats existants :

   ```
   storage aggregate show
   ```

   Si un agrégat dispose d'un espace suffisant, notez son nom dans la fiche de travail.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. Si aucun agrégat n'a suffisamment d'espace, ajoutez des disques à un agrégat existant en utilisant le `storage aggregate add-disks` ou créez un nouvel agrégat à l'aide de `storage aggregate create` commande.

Informations associées

- "Ajout de disques à un niveau local (agrégat)"
- "agrégat de stockage add-disks"
- "création d'agrégats de stockage"

Évaluer les exigences de configuration du réseau ONTAP NFS

Avant de fournir un stockage NFS aux clients, vous devez vérifier que la mise en réseau est correctement configurée pour répondre aux exigences de provisionnement NFS.

Avant de commencer

Les objets de réseau de cluster suivants doivent être configurés :

- Ports physiques et logiques
- Les domaines de diffusion
- Sous-réseaux (le cas échéant)
- IPspaces (selon les besoins, en plus de l'IPspace par défaut)
- Failover Groups (si nécessaire, en plus du groupe de basculement par défaut pour chaque broadcast domain)
- Pare-feu externes

Étapes

1. Afficher les ports physiques et virtuels disponibles :

   `network port show`

   - Dans la mesure du possible, vous devez utiliser le port avec la vitesse la plus élevée pour le réseau de données.
   - Tous les composants du réseau de données doivent avoir le même paramètre MTU pour optimiser les performances.
   - Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

2. Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer l'adresse IP et la valeur du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses disponibles suffisantes : +

   `network subnet show`

   Pour en savoir plus, `network subnet show` consultez le "Référence de commande ONTAP".

   Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Les sous-réseaux sont créés à l'aide du `network subnet create` commande.

   Pour en savoir plus, `network subnet create` consultez le "Référence de commande ONTAP".

3. Affichez les IPspaces disponibles :

   `network ipspace show`

   Vous pouvez utiliser l'IPspace par défaut ou un IPspace personnalisé.

   Pour en savoir plus, `network ipspace show` consultez le "Référence de commande ONTAP".

4. Si vous souhaitez utiliser des adresses IPv6, vérifiez que l'IPv6 est activé sur le cluster :

   `network options ipv6 show`

   Si nécessaire, vous pouvez activer IPv6 en utilisant le `network options ipv6 modify` commande.

   Pour en savoir plus sur `network options ipv6 show` et `network options ipv6 modify` dans le "Référence de commande ONTAP".

En savoir plus sur le provisionnement de la capacité de stockage ONTAP NFS

Avant de créer un nouveau volume NFS ou qtree, vous devez décider de le placer dans une SVM nouvelle ou existante, et du volume de configuration requis par la SVM. Cette décision détermine votre flux de travail.

Choix

- Si vous souhaitez provisionner un volume ou qtree sur un nouveau SVM, ou sur un SVM existant sur lequel NFS est activé mais non configuré, suivez les étapes de « Configuration de l'accès NFS à un SVM » et de « Ajout de stockage NFS à un SVM compatible NFS ».

  Configurer l'accès NFS à un SVM

  Ajout d'un stockage NFS à un SVM compatible NFS

  Vous pouvez choisir de créer un nouveau SVM si l'un des cas suivants est vrai :

  - Vous activez NFS pour la première fois sur un cluster.
  - Un cluster contient des SVM existants, dans lequel vous ne souhaitez pas activer la prise en charge de NFS.
  - Un cluster possède un ou plusieurs SVM compatibles NFS, et vous souhaitez un autre serveur NFS dans un espace de noms isolé (scénario de colocation).
    Vous devez également choisir cette option pour provisionner le stockage sur un SVM existant sur lequel NFS est activé, mais non configuré. Ce peut être le cas si vous avez créé le SVM pour l'accès SAN ou si aucun protocole n'a été activé au moment de la création de la SVM.

  Après avoir activé NFS sur le SVM, procéder au provisionnement d'un volume ou qtree.

- Si vous souhaitez provisionner un volume ou qtree sur un SVM existant entièrement configuré pour l'accès NFS, suivez les étapes de la section « Ajout de stockage NFS à un SVM compatible NFS ».

  Ajout de stockage NFS à un SVM compatible NFS

Fiche technique de configuration NFS de ONTAP

La fiche de configuration NFS vous permet de collecter les informations requises pour configurer l'accès NFS pour les clients.

Vous devez remplir une ou les deux sections de la feuille de travail en fonction de la décision que vous avez prise concernant l'emplacement de provisionnement du stockage :

Si vous configurez l'accès NFS à un SVM, vous devez remplir les deux sections.

- Configuration de l'accès NFS à un SVM
- Ajout de capacité de stockage à un SVM compatible NFS

Si vous ajoutez de la capacité de stockage à un SVM compatible NFS, vous devez remplir uniquement les conditions suivantes :

- Ajout de capacité de stockage à un SVM compatible NFS

Paramètres de création d'un SVM

Ces valeurs sont fournies avec le `vserver create` Commande si vous créez un nouveau SVM.

Champ	Description	Votre valeur
`-vserver`	Un nom que vous fournissez pour le nouveau SVM qui est un nom de domaine complet (FQDN) ou suit une autre convention qui applique des noms de SVM uniques au sein d'un cluster.	
`-aggregate`	Nom d'un agrégat du cluster disposant d'un espace suffisant pour accueillir une nouvelle capacité de stockage NFS.	
`-rootvolume`	Un nom unique que vous fournissez pour le volume root du SVM.	
`-rootvolume-security-style`	Utiliser le style de sécurité UNIX pour la SVM.	`unix`
`-language`	Utilisez le paramètre de langue par défaut de ce flux de travail.	`C.UTF-8`
`ipspace`	Les IPspaces sont des espaces d'adresse IP distincts dans lesquels (SVM) résident les serveurs (Storage Virtual machine).	

Paramètres de création d'un serveur NFS

Ces valeurs sont fournies avec le `vserver nfs create` Commande lorsque vous créez un nouveau serveur NFS et spécifiez les versions NFS prises en charge.

Si vous activez NFSv4 ou une version ultérieure, vous devez utiliser LDAP pour renforcer la sécurité.

Champ	Description	Votre valeur

`-v3`, `-v4.0`, `-v4.1`, `-v4.1-pnfs`	Activez les versions NFS si nécessaire. V4.2 est également pris en charge dans ONTAP 9.8 et versions ultérieures `v4.1` est activé.	
`-v4-id-domain`	ID nom de domaine de mappage.	
`-v4-numeric-ids`	Prise en charge des ID propriétaires numériques (activés ou désactivés).	

Paramètres de création d'une LIF

Vous fournissez ces valeurs avec la `network interface create` commande lors de la création des LIFs. Pour en savoir plus, `network interface create` consultez le "Référence de commande ONTAP".

Si vous utilisez Kerberos, vous devez activer Kerberos sur plusieurs LIFs.

Champ	Description	Votre valeur
`-lif`	Nom que vous fournissez pour la nouvelle LIF.	
`-role`	Utiliser le rôle LIF de données dans ce workflow	`data`
`-data-protocol`	Utilisez uniquement le protocole NFS dans ce workflow.	`nfs`
`-home-node`	Le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF. Pour en savoir plus, `network interface revert` consultez le "Référence de commande ONTAP".	
`-home-port`	Le port ou le groupe d'interface sur lequel la LIF renvoie au moment du `network interface revert` La commande est exécutée sur le LIF.	

`-address`	L’adresse IPv4 ou IPv6 sur le cluster qui seront utilisées pour l’accès aux données par la nouvelle LIF.	
`-netmask`	Le masque de réseau et la passerelle pour le LIF.	
`-subnet`	Un pool d’adresses IP. Utilisé au lieu de `-address` et `-netmask` pour attribuer automatiquement des adresses et des masques réseau.	
`-firewall-policy`	Utilisez la politique de pare-feu de données par défaut dans ce workflow.	`data`

Paramètres de résolution de nom d’hôte DNS

Ces valeurs sont fournies avec le `vserver services name-service dns create` Commande lorsque vous configurez un DNS.

Champ	Description	Votre valeur
`-domains`	Jusqu’à cinq noms de domaine DNS.	
`-name-servers`	Jusqu’à trois adresses IP pour chaque serveur de noms DNS.	

Nom des informations sur le service

Paramètres pour la création d’utilisateurs locaux

Vous fournissez ces valeurs si vous créez des utilisateurs locaux à l’aide de l' `vserver services name-service unix-user create` commande. Si vous configurez des utilisateurs locaux en chargeant un fichier contenant des utilisateurs UNIX à partir d’un URI (Uniform Resource identifier), vous n’avez pas besoin de spécifier ces valeurs manuellement.

	Nom d’utilisateur `(-user)`	ID d’utilisateur `(-id)`	ID de groupe `(-primary-gid)`	Nom complet `(-full-name)`
Exemple	je johnm	123	100	John Miller
1				
2				

3				
…				
n				

Paramètres de création de groupes locaux

Vous fournissez ces valeurs si vous créez des groupes locaux à l'aide de l' `vserver services name-service unix-group create` commande. Si vous configurez des groupes locaux en chargeant un fichier contenant des groupes UNIX à partir d'un URI, vous n'avez pas besoin de spécifier ces valeurs manuellement.

	Nom du groupe (`-name`)	ID de groupe (`-id`)
Exemple	Ingénierie	100
1		
2		
3		
…		
n		

Paramètres pour NIS

Ces valeurs sont fournies avec le `vserver services name-service nis-domain create` commande.

Le `-nis-servers` le champ remplace le `-servers` champ. Vous pouvez utiliser le `-nis-servers` champ pour spécifier soit un nom d'hôte soit une adresse IP pour le serveur NIS.

Champ	Description	Votre valeur
`-domain`	Domaine NIS que la SVM utilisera pour les recherches de noms.	
`-active`	Serveur de domaine NIS actif.	`true` ou `false`
`-nis-servers`	Une liste séparée par des virgules d'adresses IP et de noms d'hôtes pour les serveurs NIS utilisés par la configuration de domaine.	

Paramètres pour LDAP

Ces valeurs sont fournies avec le `vserver services name-service ldap client create` commande.

Vous aurez également besoin d'un certificat d'autorité de certification racine auto-signé `.pem` fichier.

Champ	Description	Votre valeur
`-vserver`	Le nom du SVM pour lequel vous souhaitez créer une configuration client LDAP.	
`-client-config`	Nom que vous attribuez pour la nouvelle configuration du client LDAP.	
`-ldap-servers`	Liste séparée par des virgules d'adresses IP et de noms d'hôte pour les serveurs LDAP.	
`-query-timeout`	Utilisez la valeur par défaut `3` secondes pour ce flux de travail.	`3`
`-min-bind-level`	Niveau d'authentification de liaison minimum. La valeur par défaut est `anonymous`. Doit être réglé sur `sasl` si la signature et le chiffrement sont configurés.	
`-preferred-ad-servers`	Un ou plusieurs serveurs Active Directory préférés par adresse IP dans une liste délimitée par des virgules.	
`-ad-domain`	Domaine Active Directory.	
`-schema`	Le modèle de schéma à utiliser. Vous pouvez utiliser un schéma par défaut ou personnalisé.	
`-port`	Utilisez le port de serveur LDAP par défaut `389` pour ce flux de travail.	`389`
`-bind-dn`	Nom distinctif de l'utilisateur Bind.	
`-base-dn`	Nom distinctif de base. La valeur par défaut est `""` (racine).	

Champ	Description	Votre valeur
`-base-scope`	Utilisez l'étendue de recherche de base par défaut `subnet` pour ce flux de travail.	`subnet`
`-session-security`	Active la signature ou la signature et le chiffrement LDAP. La valeur par défaut est `none`.	
`-use-start-tls`	Active LDAP sur TLS. La valeur par défaut est `false`.	

Paramètres d'authentification Kerberos

Ces valeurs sont fournies avec le `vserver nfs kerberos realm create` commande. Certaines valeurs diffèrent selon que vous utilisez Microsoft Active Directory en tant que serveur KDC (Key distribution Center), MIT ou autre serveur KDC UNIX.

Champ	Description	Votre valeur
`-vserver`	La SVM qui communiquera avec le KDC.	
`-realm`	Le domaine Kerberos.	
`-clock-skew`	Inclinaison de l'horloge autorisée entre les clients et les serveurs.	
`-kdc-ip`	Adresse IP KDC.	
`-kdc-port`	Numéro de port KDC.	
`-adserver-name`	Microsoft KDC uniquement : nom du serveur AD.	
`-adserver-ip`	Microsoft KDC uniquement : adresse IP du serveur AD.	
`-adminserver-ip`	UNIX KDC uniquement : adresse IP du serveur d'administration.	
`-adminserver-port`	UNIX KDC uniquement : numéro de port du serveur d'administration.	
`-passwordserver-ip`	UNIX KDC uniquement : adresse IP du serveur de mots de passe.	

`-passwordserver-port`	UNIX KDC uniquement : port du serveur de mots de passe.	
`-kdc-vendor`	Fournisseur KDC.	{ `Microsoft`
`Other` }	`-comment`	Tout commentaire souhaité.

Ces valeurs sont fournies avec le `vserver nfs kerberos interface enable` commande.

Champ	Description	Votre valeur
`-vserver`	Le nom du SVM pour lequel vous souhaitez créer une configuration Kerberos.	
`-lif`	La LIF de données sur laquelle vous activez Kerberos. Vous pouvez activer Kerberos sur plusieurs LIFs.	
`-spn`	Le nom du principe de service (SPN)	
`-permitted-enc-types`	Les types de chiffrement autorisés pour Kerberos sur NFS ; `aes-256` est recommandé en fonction des capacités du client.	
`-admin-username`	Les informations d'identification de l'administrateur KDC pour récupérer la clé secrète SPN directement à partir du KDC. Un mot de passe est requis	
`-keytab-uri`	Le fichier keytab du KDC contenant la clé SPN si vous ne disposez pas d'informations d'identification administrateur KDC.	
`-ou`	L'unité organisationnelle sous laquelle le compte du serveur Microsoft Active Directory sera créé lorsque vous activez Kerberos à l'aide d'un Royaume pour Microsoft KDC.	

Paramètres de création de règles et de politiques d'exportation

Ces valeurs sont fournies avec le `vserver export-policy create` commande.

Champ	Description	Votre valeur
`-vserver`	Nom du SVM qui hébergera le nouveau volume.	
`-policyname`	Nom que vous fournissez pour une nouvelle export-policy.	

Vous fournissez ces valeurs pour chaque règle avec le `vserver export-policy rule create` commande.

Champ	Description	Votre valeur
`-clientmatch`	Spécification de correspondance du client.	
`-ruleindex`	Position de la règle d'exportation dans la liste des règles.	
`-protocol`	Utiliser NFS dans ce flux de production.	`nfs`
`-rorule`	Méthode d'authentification pour l'accès en lecture seule.	
`-rwrule`	Méthode d'authentification pour l'accès en lecture-écriture.	
`-superuser`	Méthode d'authentification pour l'accès superutilisateur.	
`-anon`	ID utilisateur auquel les utilisateurs anonymes sont mappés.	

Vous devez créer une ou plusieurs règles pour chaque export-policy.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Exemples	0.0.0.0/0,@rootaccess_netgroup	toutes	krb5	system	65534
1					

2					
3					
…					
n					

Paramètres de création d'un volume

Ces valeurs sont fournies avec le `volume create` commande si vous créez un volume à la place d'un qtree.

Champ	Description	Votre valeur
`-vserver`	Nom d'un SVM nouveau ou existant qui hébergera le nouveau volume.	
`-volume`	Un nom descriptif unique que vous fournissez pour le nouveau volume.	
`-aggregate`	Nom d'un agrégat du cluster disposant d'un espace suffisant pour le nouveau volume NFS.	
`-size`	Un entier que vous fournissez pour la taille du nouveau volume.	
`-user`	Nom ou ID de l'utilisateur défini en tant que propriétaire de la racine du volume.	
`-group`	Nom ou ID du groupe défini comme propriétaire de la racine du volume.	
`--security-style`	Utilisez le style de sécurité UNIX pour ce flux de travail.	`unix`
`-junction-path`	Emplacement sous la racine (/) où le nouveau volume doit être monté.	
`-export-policy`	Si vous prévoyez d'utiliser une export-policy existante, vous pouvez entrer son nom lors de la création du volume.	

Paramètres pour la création d'un qtree

Ces valeurs sont fournies avec le `volume qtree create` commande si vous créez un qtree à la place d'un volume.

Champ	Description	Votre valeur
`-vserver`	Nom de la SVM sur lequel réside le volume contenant le qtree.	
`-volume`	Nom du volume qui contiendra le nouveau qtree.	
`-qtree`	Un nom descriptif unique que vous fournissez pour le nouveau qtree, 64 caractères maximum.	
`-qtree-path`	L'argument de chemin qtree dans le format `/vol/volume_name/qtree_name\>` peut être spécifié au lieu de spécifier volume et qtree en tant qu'arguments distincts.	
`-unix-permissions`	Facultatif : les autorisations UNIX pour le qtree.	
`-export-policy`	Si vous prévoyez d'utiliser une export policy existante, vous pouvez saisir son nom lors de la création du qtree.	

Informations associées

- "Référence de commande ONTAP"

Configurer l'accès NFS à un SVM

Créer des SVM ONTAP pour l'accès aux données NFS

Si vous ne disposez pas encore d'au moins un SVM dans un cluster afin de fournir l'accès aux données aux clients NFS, vous devez en créer un.

Avant de commencer

- À partir de ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d'informations, voir Gestion de la capacité des SVM.

Étapes

1. Création d'un SVM :

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
```

ipspace_name

- Utilisez le paramètre UNIX pour le `-rootvolume-security-style` option.
- Utilisez le paramètre par défaut C.UTF-8 `-language` option.
- Le `ipspace` le paramètre est facultatif.

2. Vérifier la configuration et le statut du nouveau SVM :

   `vserver show -vserver` *vserver_name*

   Le `Allowed Protocols` NFS doit être inclus dans le champ. Vous pouvez modifier cette liste ultérieurement.

   Le `Vserver Operational State` le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'IPspace ipspaceA :

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

À partir de la version ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite au niveau du débit et du plafond aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir Définissez un modèle de groupe de règles adaptatives.

Vérifier l'activation du protocole NFS sur la SVM ONTAP

Avant de pouvoir configurer et utiliser NFS sur les SVM, vous devez vérifier que le protocole est activé.

Description de la tâche

Cela s'effectue généralement lors de la configuration d'un SVM, mais si vous n'avez pas activé le protocole lors de l'installation, vous pouvez l'activer plus tard à l'aide du `vserver add-protocols` commande.

Vous ne pouvez pas ajouter ou supprimer un protocole d'une LIF une fois qu'il est créé.

Vous pouvez également désactiver les protocoles sur les SVM à l'aide de `vserver remove-protocols` commande.

Étapes

1. Vérifier les protocoles actuellement activés et désactivés pour le SVM :

   ```
   vserver show -vserver vserver_name -protocols
   ```

   Vous pouvez également utiliser le `vserver show-protocols` Commande permettant d'afficher les protocoles actuellement activés sur tous les SVM du cluster.

2. Si nécessaire, activer ou désactiver un protocole :
   - Pour activer le protocole NFS :

     ```
     vserver add-protocols -vserver vserver_name -protocols nfs
     ```

   - Pour désactiver un protocole :

     ```
     vserver remove-protocols -vserver vserver_name -protocols protocol_name
     [,protocol_name,…]
     ```

3. Vérifiez que les protocoles activés et désactivés ont été correctement mis à jour :

   ```
   vserver show -vserver vserver_name -protocols
   ```

Exemple

La commande suivante affiche les protocoles actuellement activés et désactivés (autorisés et interdits) sur le SVM nommé vs1 :

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

La commande suivante permet l'accès via NFS en ajoutant `nfs` Pour la liste des protocoles activés sur le SVM nommé vs1 :

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Ouvrir l'accès client NFS sur la SVM ONTAP

La export policy par défaut du volume root du SVM doit inclure une règle permettant à tous les clients d'y accéder via NFS. Sans une telle règle, tous les clients NFS se voient refuser l'accès au SVM et à ses volumes.

Description de la tâche

Lorsqu'un nouveau SVM est créé, une export policy par défaut (appelée default) est créée automatiquement pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM.

Vous devez vérifier que l'accès est ouvert à tous les clients NFS dans la stratégie d'exportation par défaut, puis limiter l'accès aux volumes individuels en créant des règles d'exportation personnalisées pour les volumes individuels ou les qtrees.

Étapes

1. Si vous utilisez un SVM existant, vérifier la root volume export policy par défaut :

   ```
   vserver export-policy rule show
   ```

   Le résultat de la commande doit être similaire à ce qui suit :

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                     Superuser Security Types: any
                 Honor SetUID Bits in SETATTR: true
                    Allow Creation of Devices: true
   ```

   Si une telle règle existe et autorise l'accès ouvert, cette tâche est terminée. Si ce n'est pas le cas, passez à l'étape suivante.

2. Créer une règle d'export pour le volume root du SVM:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Si la SVM ne contiendra que des volumes sécurisés par Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5` ou `krb5i`. Par exemple :

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. Vérifiez la création de règles à l'aide du `vserver export-policy rule show` commande.

Résultat

Tout client NFS peut désormais accéder à tout volume ou qtree créé sur le SVM.

Créer des serveurs ONTAP NFS

Après avoir vérifié que NFS est sous licence sur le cluster, vous pouvez utiliser le `vserver nfs create` Commande permettant de créer un serveur NFS sur le SVM et de spécifier les versions NFS prises en charge.

Description de la tâche

Le SVM peut être configuré pour prendre en charge une ou plusieurs versions de NFS. Si vous supporte NFSv4 ou version ultérieure :

- Le nom de domaine de mappage de l'ID utilisateur NFSv4 doit être identique sur le serveur NFSv4 et les clients cibles.

  Il n'est pas nécessairement nécessaire d'être identique à un nom de domaine LDAP ou NIS tant que le serveur NFSv4 et les clients utilisent le même nom.

- Les clients cibles doivent prendre en charge le paramètre d'ID numérique NFSv4.
- Pour des raisons de sécurité, vous devez utiliser LDAP pour les services de noms dans les déploiements NFSv4.

Avant de commencer

Le SVM doit avoir été configuré pour permettre le protocole NFS.

Étapes

1. Vérifiez que NFS est sous licence sur le cluster :

   ```
   system license show -package nfs
   ```

   Si ce n'est pas le cas, contactez votre représentant commercial.

2. Créer un serveur NFS :

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Vous pouvez choisir d'activer n'importe quelle combinaison de versions NFS. Si vous souhaitez prendre en charge la norme pNFS, vous devez les activer `-v4.1` et `-v4.1-pnfs` options.

   Si vous activez v4 ou version ultérieure, vous devez également vous assurer que les options suivantes sont correctement définies :

   - `-v4-id-domain`

     Ce paramètre facultatif spécifie la partie domaine de la forme de chaîne de noms d'utilisateurs et de groupes, comme défini par le protocole NFSv4. Par défaut, ONTAP utilise le domaine NIS si l'un est défini ; si ce n'est pas le cas, le domaine DNS est utilisé. Vous devez fournir une valeur correspondant au nom de domaine utilisé par les clients cibles.

   - `-v4-numeric-ids`

     Ce paramètre facultatif indique si la prise en charge des identificateurs de chaîne numériques dans les attributs propriétaire NFSv4 est activée. Le paramètre par défaut est activé mais vous devez vérifier que les clients cibles le prennent en charge.

   Vous pouvez activer d'autres fonctionnalités NFS ultérieurement en utilisant le `vserver nfs modify` commande.

3. Vérifiez que NFS est en cours d'exécution :

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Vérifiez que NFS est configuré comme vous le souhaitez :

   `vserver nfs show -vserver vserver_name`

Exemples

La commande suivante crée un serveur NFS sur le SVM nommé vs1 avec NFSv3 et NFSv4.0 activés :

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Les commandes suivantes vérifient les valeurs d'état et de configuration du nouveau serveur NFS nommé vs1 :

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                 General NFS Access: true
                              NFS v3: enabled
                            NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
             NFSv4 ID Mapping Domain: my_domain.com
...
```

Création des LIF NFS ONTAP

Une LIF est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur le `up` statut administratif. Pour en savoir plus, `up` consultez le "Référence de commande ONTAP".
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

  Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

Pour en savoir plus, `network subnet create` consultez le "Référence de commande ONTAP".

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous utilisez l'authentification Kerberos, activez Kerberos sur plusieurs LIFs.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).

  Pour en savoir plus sur `network interface capacity show` et `network interface capacity details show` dans le "Référence de commande ONTAP".

- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

Le protocole FC-NVMe est pris en charge à partir de la version ONTAP 9.4. Si vous créez une LIF FC-NVMe, notez les éléments suivants :

- Le protocole NVMe doit être pris en charge par l'adaptateur FC sur lequel la LIF est créée.
- FC-NVMe est le seul protocole de données sur les LIF de données.
- Un trafic de gestion des LIF doit être configuré pour chaque SVM (Storage Virtual machine) prenant en charge les protocoles SAN.
- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Un seul protocole LIF NVMe traitant le trafic de données peut être configuré par SVM

Étapes

1. Créer une LIF :

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

   Pour en savoir plus, `network interface create` consultez le "Référence de commande ONTAP".

Option	Description
ONTAP 9.5 et versions antérieures	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*

-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
ONTAP 9.6 et ultérieur	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- Le `-role` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de avecONTAP 9.6).
- Le `-data-protocol` Le paramètre doit être spécifié lors de la création de la LIF et ne peut pas être modifié par la suite sans destruction et recréez la LIF de données.

  Le `-data-protocol` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6).

- `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

  Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

  Pour en savoir plus, `network interface revert` consultez le "Référence de commande ONTAP".

- `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Pour en savoir plus sur `network route create` et créer une route statique au sein d'une SVM, consultez la "Référence de commande ONTAP".
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

  Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.

  > Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.

a. Vérifier que le LIF a été créé avec succès en utilisant le `network interface show` commande.

b. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier…	Utiliser…
Adresse IPv4	`network ping`
Adresse IPv6	`network ping6`

c. Si vous utilisez Kerberos, répétez les étapes 1 à 3 pour en créer d'autres.

Kerberos doit être activé séparément sur chacune de ces LIFs.

Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé client1_sub) :

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données datalif1 et datalif3 sont configurées avec des adresses IPv4 et le datalif4 est configuré avec une adresse IPv6 :

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

La commande suivante montre comment créer une LIF de données NAS attribuée avec le `default-data-files` règle de service :

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Informations associées

- "ping réseau"
- "interface réseau"

Activer DNS pour la résolution du nom d'hôte ONTAP NFS SVM

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

Avant de commencer

Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. Le `vserver services name-service dns create` Commande émet un avertissement si vous entrez un seul nom de serveur DNS.

Description de la tâche

En savoir plus sur "Configuration du DNS dynamique sur la SVM".

Étapes

1. Activer le DNS sur le SVM :

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > Le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

2. Afficher les configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande.

   La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configurer NAME-services

En savoir plus sur les services de noms ONTAP NFS

En fonction de la configuration de votre système de stockage, ONTAP doit pouvoir rechercher des informations sur l'hôte, l'utilisateur, le groupe ou le groupe réseau afin de fournir un accès approprié aux clients. Vous devez configurer les services de noms pour permettre à ONTAP d'accéder aux services de noms locaux ou externes afin d'obtenir ces informations.

Vous devez utiliser un service de noms tel que NIS ou LDAP pour faciliter les recherches de noms lors de l'authentification client. Il est préférable d'utiliser LDAP dans la mesure du possible pour renforcer la sécurité, notamment lors du déploiement de NFSv4 ou de versions ultérieures. Vous devez également configurer des utilisateurs et des groupes locaux si des serveurs de noms externes ne sont pas disponibles.

Les informations de service de nom doivent être conservées synchronisées sur toutes les sources.

Configurer la table de commutation du service de noms NFS ONTAP

Vous devez configurer correctement la table de commutateur de service de nom pour permettre à ONTAP de consulter les services de noms locaux ou externes pour récupérer les informations relatives à l'hôte, à l'utilisateur, au groupe, au groupe réseau ou au mappage de noms.

Avant de commencer

Vous devez avoir déterminé les services de noms que vous souhaitez utiliser pour le mappage de l'hôte, de l'utilisateur, du groupe, du groupe réseau ou du nom, selon votre environnement.

Si vous prévoyez d'utiliser des netgroups, toutes les adresses IPv6 spécifiées dans netgroups doivent être raccourcies et compressées comme spécifié dans RFC 5952.

Description de la tâche

N'incluez pas de sources d'information qui ne sont pas utilisées. Par exemple, si NIS n'est pas utilisé dans votre environnement, ne spécifiez pas `-sources nis` option.

Étapes

1. Ajoutez les entrées nécessaires à la table de changement de nom du service :

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Vérifiez que le tableau des commutateurs de service de noms contient les entrées attendues dans l'ordre souhaité :

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   Si vous souhaitez apporter des corrections, vous devez utiliser le `vserver services name-service ns-switch modify` ou `vserver services name-service ns-switch delete` commandes.

Exemple

L'exemple suivant crée une nouvelle entrée dans la table name service switch pour que le SVM vs1 puisse utiliser le fichier netgroup local et un serveur NIS externe pour rechercher les informations netgroup dans cet ordre :

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Une fois que vous avez terminé

- Vous devez configurer les services de noms que vous avez spécifiés pour la SVM afin de fournir un accès aux données.
- Si vous supprimez un service de noms pour la SVM, vous devez le supprimer de la table name service switch également.

  L'accès client au système de stockage risque de ne pas fonctionner comme prévu si vous ne supprimez pas le service de noms de la table du commutateur de service de noms.

Configuration des utilisateurs et des groupes UNIX locaux

En savoir plus sur les utilisateurs et groupes UNIX locaux pour les SVM ONTAP NFS

Vous pouvez utiliser les utilisateurs et groupes UNIX locaux sur le SVM pour l'authentification et les mappages de noms. Vous pouvez créer des utilisateurs et des groupes UNIX manuellement ou charger un fichier contenant des utilisateurs ou des groupes UNIX à partir d'un URI (Uniform Resource identifier).

Il existe une limite maximale par défaut de 32,768 groupes d'utilisateurs UNIX locaux et membres de groupes regroupés dans le cluster. L'administrateur du cluster peut modifier cette limite.

Créer des utilisateurs UNIX locaux sur les SVM ONTAP NFS

Vous pouvez utiliser le `vserver services name-service unix-user create` Commande permettant de créer des utilisateurs UNIX locaux. Un utilisateur UNIX local est un utilisateur UNIX que vous créez sur le SVM en tant qu'option de services de noms UNIX à utiliser lors du traitement des mappages de noms.

Étape

1. Créer un utilisateur UNIX local :

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* spécifie le nom d'utilisateur. La longueur du nom d'utilisateur doit être inférieure ou égale à 64 caractères.

   `-id` *`integer`* Spécifie l'ID utilisateur que vous attribuez.

   `-primary-gid` *`integer`* Spécifie l'ID du groupe principal. L'utilisateur est ainsi ajouté au groupe principal. Après avoir créé l'utilisateur, vous pouvez l'ajouter manuellement à tout groupe supplémentaire souhaité.

Exemple

La commande suivante crée un utilisateur UNIX local nommé johnm (nom complet « John Miller ») sur la SVM nommée vs1. L'utilisateur possède l'ID 123 et le groupe principal ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Charger les listes d'utilisateurs UNIX locales sur les SVM NFS ONTAP

Comme alternative à la création manuelle d'utilisateurs UNIX locaux dans des SVM, vous pouvez simplifier la tâche en chargeant une liste d'utilisateurs UNIX locaux dans des SVM depuis un identificateur de ressource uniforme (URI) (`vserver services name-service unix-user load-from-uri`).

Étapes

1. Créez un fichier contenant la liste des utilisateurs UNIX locaux que vous souhaitez charger.

   Le fichier doit contenir des informations utilisateur sous UNIX `/etc/passwd` format :

   `user_name: password: user_ID: group_ID: full_name`

   La commande supprime la valeur de l' *`password`* et les valeurs des champs après le *`full_name`* légale

(*home_directory* et *shell*).

La taille maximale de fichier prise en charge est de 2.5 Mo.

2. Vérifiez que la liste ne contient aucune information dupliquée.

   Si la liste contient des entrées dupliquées, le chargement de la liste échoue et un message d'erreur s'affiche.

3. Copiez le fichier sur un serveur.

   Le serveur doit être accessible par le système de stockage via HTTP, HTTPS, FTP ou FTPS.

4. Déterminez l'URI du fichier.

   L'URI est l'adresse que vous fournissez au système de stockage pour indiquer l'emplacement du fichier.

5. Charger le fichier contenant la liste des utilisateurs UNIX locaux dans les SVM à partir de l'URI :

   `vserver services name-service unix-user load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite {true false}` spécifie s'il faut remplacer les entrées. La valeur par défaut est `false`.

Exemple

La commande suivante charge la liste des utilisateurs UNIX locaux à partir de l'URI `ftp://ftp.example.com/passwd` Au SVM nommé vs1. Les utilisateurs existants du SVM ne sont pas remplacés par des informations de l'URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Créer des groupes UNIX locaux sur les SVM ONTAP NFS

Vous pouvez utiliser le `vserver services name-service unix-group create` Commande pour créer des groupes UNIX locaux à la SVM. Les groupes UNIX locaux sont utilisés avec des utilisateurs UNIX locaux.

Étape

1. Créer un groupe UNIX local :

   `vserver services name-service unix-group create -vserver` *vserver_name* `-name` *group_name* `-id` *integer*

   `-name` *group_name* spécifie le nom du groupe. Le nom du groupe doit comporter 64 caractères ou moins.

   `-id` *integer* Spécifie l'ID de groupe que vous attribuez.

Exemple

La commande suivante crée un groupe local nommé eng sur le SVM nommé vs1. Le groupe a l'ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Ajouter des utilisateurs au groupe UNIX local sur les SVM NFS ONTAP

Vous pouvez utiliser le `vserver services name-service unix-group adduser` Commande pour ajouter un utilisateur à un groupe UNIX complémentaire qui est local au SVM.

Étape

1. Ajouter un utilisateur à un groupe UNIX local :

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* Spécifie le nom du groupe UNIX auquel ajouter l'utilisateur en plus du groupe principal de l'utilisateur.

Exemple

La commande suivante ajoute un utilisateur nommé max à un groupe UNIX local nommé eng sur le SVM nommé vs1 :

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Charger des groupes UNIX locaux à partir d'URI sur des SVM NFS ONTAP

Comme alternative à la création manuelle de groupes UNIX locaux, vous pouvez charger une liste de groupes UNIX locaux dans des SVM à partir d'un URI (Uniform Resource identifier) en utilisant le `vserver services name-service unix-group load-from-uri` commande.

Étapes

1. Créez un fichier contenant la liste des groupes UNIX locaux que vous souhaitez charger.

   Le fichier doit contenir des informations de groupe dans UNIX `/etc/group` format :

   `group_name: password: group_ID: comma_separated_list_of_users`

   La commande supprime la valeur de l' *`password`* légale.

   La taille de fichier maximale prise en charge est de 1 Mo.

   La longueur maximale de chaque ligne du fichier de groupe est de 32,768 caractères.

2. Vérifiez que la liste ne contient aucune information dupliquée.

   La liste ne doit pas contenir d'entrées dupliquées, sinon le chargement de la liste échoue. Si des entrées sont déjà présentes dans le SVM, il faut soit définir le `-overwrite` paramètre à `true` pour remplacer toutes les entrées existantes par le nouveau fichier ou s'assurer que le nouveau fichier ne contient pas d'entrées qui dupliquent des entrées existantes.

3. Copiez le fichier sur un serveur.

   Le serveur doit être accessible par le système de stockage via HTTP, HTTPS, FTP ou FTPS.

4. Déterminez l'URI du fichier.

   L'URI est l'adresse que vous fournissez au système de stockage pour indiquer l'emplacement du fichier.

5. Charger le fichier contenant la liste des groupes UNIX locaux dans le SVM depuis l'URI :

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`} spécifie s'il faut remplacer les entrées. La valeur par défaut est `false`. Si vous spécifiez ce paramètre comme `true`, ONTAP remplace la totalité de la base de données du groupe UNIX local existant du SVM spécifié par les entrées du fichier que vous chargez.

Exemple

La commande suivante charge la liste des groupes UNIX locaux à partir de l'URI `ftp://ftp.example.com/group` Au SVM nommé vs1. Les groupes existants sur le SVM ne sont pas remplacés par les informations de l'URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Travailler avec des groupes réseau

En savoir plus sur les groupes réseau sur les SVM NFS ONTAP

Vous pouvez utiliser netgroups pour l'authentification des utilisateurs et pour correspondre des clients dans les règles d'export policy. Vous pouvez fournir l'accès aux netgroups à partir de serveurs de noms externes (LDAP ou NIS), ou vous pouvez charger des netgroups à partir d'un identifiant de ressource uniforme (URI) dans des SVM à l'aide de `vserver services name-service netgroup load` commande.

Avant de commencer

Avant de travailler avec des groupes réseau, vous devez vous assurer que les conditions suivantes sont remplies :

- Tous les hôtes dans des groupes réseau, indépendamment de la source (fichiers NIS, LDAP ou locaux), doivent avoir des enregistrements DNS avant (A) et arrière (PTR) pour fournir des recherches DNS avant et arrière cohérentes.

  En outre, si une adresse IP d'un client possède plusieurs enregistrements PTR, tous ces noms d'hôte

doivent être membres du groupe réseau et avoir les enregistrements correspondants.

- Les noms de tous les hôtes dans des groupes réseau, indépendamment de leur source (fichiers NIS, LDAP ou locaux), doivent être correctement orthographiés et utiliser le cas correct. Les incohérences de cas dans les noms d'hôte utilisés dans les netgroups peuvent entraîner un comportement inattendu, tel que l'échec des vérifications d'exportation.
- Toutes les adresses IPv6 spécifiées dans netgroups doivent être raccourcies et compressées comme indiqué dans RFC 5952.

  Par exemple, 2011:hu9:0:0:0:0:0:3:1 doit être réduit à 2011:hu9::3:1.

Description de la tâche

Lorsque vous travaillez avec des groupes réseau, vous pouvez effectuer les opérations suivantes :

- Vous pouvez utiliser le `vserver export-policy netgroup check-membership` Commande permettant de déterminer si une adresse IP client est membre d'un certain groupe réseau.
- Vous pouvez utiliser le `vserver services name-service getxxbyyy netgrp` commande pour vérifier si un client fait partie d'un groupe réseau.

  Le service sous-jacent pour effectuer la recherche est sélectionné en fonction de l'ordre de commutation de service de nom configuré.

Charger des groupes réseau à partir d'URI sur des SVM NFS ONTAP

L'une des méthodes que vous pouvez utiliser pour faire correspondre les clients dans les règles d'export policy consiste à utiliser les hôtes répertoriés dans netgroups. Vous pouvez charger des netgroups à partir d'un URI (Uniform Resource identifier) dans des SVM, au lieu d'utiliser des netgroups stockés dans des serveurs de noms externes (`vserver services name-service netgroup load`).

Avant de commencer

Les fichiers netgroup doivent respecter les conditions suivantes avant d'être chargés dans un SVM :

- Le fichier doit utiliser le même format de fichier texte de groupe réseau que celui utilisé pour remplir NIS.

  ONTAP vérifie le format du fichier texte du groupe réseau avant de le charger. Si le fichier contient des erreurs, il ne sera pas chargé et un message s'affiche indiquant les corrections que vous devez effectuer dans le fichier. Après avoir corrigé les erreurs, vous pouvez recharger le fichier netgroup dans la SVM spécifiée.

- Les caractères alphabétiques des noms d'hôte dans le fichier de groupe réseau doivent être en minuscules.
- La taille de fichier maximale prise en charge est de 5 Mo.
- Le niveau maximal pris en charge pour l'imbrication de groupes réseau est 1000.
- Seuls les noms d'hôte DNS principaux peuvent être utilisés lors de la définition de noms d'hôte dans le fichier netgroup.

  Pour éviter les problèmes d'accès à l'exportation, les noms d'hôte ne doivent pas être définis à l'aide d'enregistrements DNS CNAME ou Round Robin.

- Les parties utilisateur et domaine des triples du fichier netgroup doivent être conservées vides car ONTAP ne les prend pas en charge.

  Seule la partie hôte/IP est prise en charge.

Description de la tâche

ONTAP prend en charge les recherches netgroup-by-host pour le fichier netgroup local. Une fois le fichier netgroup chargé, ONTAP crée automatiquement un mappage netgroup.byhost pour activer les recherches netgroup-par-hôte. Cela peut accélérer considérablement les recherches des groupes réseau locaux lors du traitement des règles d'export pour évaluer l'accès client.

Étape

1. Chargement des netgroups dans des SVM depuis un URI :

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Le chargement du fichier netgroup et la création du mappage netgroup.byhost peuvent prendre plusieurs minutes.

   Si vous souhaitez mettre à jour les netgroups, vous pouvez modifier le fichier et charger le fichier netgroup mis à jour dans la SVM.

Exemple

La commande suivante charge les définitions netgroup dans le SVM nommé vs1 à partir de l'URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Vérifier les définitions de groupes de réseaux SVM NFS ONTAP

Après avoir chargé des netgroups dans la SVM, vous pouvez utiliser `vserver services name-service netgroup status` commande pour vérifier le statut des définitions de groupe réseau. Vous pouvez ainsi déterminer si les définitions de groupe réseau sont cohérentes sur tous les nœuds qui suivent la SVM.

Étapes

1. Définissez le niveau de privilège sur avancé :

   `set -privilege advanced`

2. Vérifiez l'état des définitions de groupe réseau :

   `vserver services name-service netgroup status`

   Vous pouvez afficher des informations supplémentaires dans une vue plus détaillée.

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

Une fois le niveau de privilège défini, la commande suivante affiche le statut netgroup pour tous les SVM :

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
---------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Créer des configurations de domaine NIS pour les SVM ONTAP NFS

Si un NIS (Network information Service) est utilisé dans votre environnement pour les services de noms, vous devez créer une configuration de domaine NIS pour la SVM en utilisant le `vserver services name-service nis-domain create` commande.

Avant de commencer

Tous les serveurs NIS configurés doivent être disponibles et accessibles avant de configurer le domaine NIS sur le SVM.

Si vous prévoyez d'utiliser NIS pour les recherches de répertoires, les cartes de vos serveurs NIS ne peuvent pas comporter plus de 1,024 caractères pour chaque entrée. Ne spécifiez pas le serveur NIS qui ne respecte pas cette limite. Sinon, l'accès client dépendant des entrées NIS risque d'échouer.

Description de la tâche

Si votre base de données NIS contient un `netgroup.byhost` Map, ONTAP peut l'utiliser pour des recherches plus rapides. Le `netgroup.byhost` et `netgroup` les cartes du répertoire doivent être synchronisées en permanence pour éviter tout problème d'accès client. ONTAP 9.7, NIS `netgroup.byhost` les entrées peuvent être mises en cache à l'aide du `vserver services name-service nis-domain netgroup-database` commandes.

L'utilisation de NIS pour la résolution de nom d'hôte n'est pas prise en charge.

Étapes

1. Créez une configuration de domaine NIS :

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   Vous pouvez spécifier jusqu'à 10 serveurs NIS.

   > Le `-nis-servers` le champ remplace le `-servers` champ. Vous pouvez utiliser le `-nis-servers` champ pour spécifier soit un nom d'hôte soit une adresse IP pour le serveur NIS.

2. Vérifiez que le domaine est créé :

   ```
   vserver services name-service nis-domain show
   ```

Exemple

La commande suivante crée une configuration de domaine NIS pour un domaine NIS appelé `nisdomain` sur le SVM nommé `vs1` avec un serveur NIS à l'adresse IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

Utiliser LDAP

En savoir plus sur l'utilisation des services de noms LDAP sur les SVM ONTAP NFS

Si LDAP est utilisé dans votre environnement pour des services de noms, vous devez travailler avec votre administrateur LDAP pour déterminer les exigences et les configurations de système de stockage appropriées, puis activer la SVM en tant que client LDAP.

Depuis ONTAP 9.10.1, la liaison de canal LDAP est prise en charge par défaut pour les connexions LDAP Active Directory et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison de canal LDAP avec les serveurs de noms, utilisez le `-try-channel-binding` paramètre avec le `ldap client modify` commande.

Pour plus d'informations, voir
"2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows".

- Avant de configurer LDAP pour ONTAP, vérifiez que votre déploiement de site respecte les bonnes pratiques en matière de configuration de serveur LDAP et de client. En particulier, les conditions suivantes doivent être remplies :
  - Le nom de domaine du serveur LDAP doit correspondre à l'entrée du client LDAP.
  - Les types de hachage de mot de passe utilisateur LDAP pris en charge par le serveur LDAP doivent inclure ceux pris en charge par ONTAP :

- CRYPT (tous types) et SHA-1 (SHA, SSHA).
- Depuis ONTAP 9.8, des hachages SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 et SSHA-512) sont également pris en charge.

◦ Si le serveur LDAP nécessite des mesures de sécurité de session, vous devez les configurer dans le client LDAP.

Les options de sécurité de session suivantes sont disponibles :

- La signature LDAP (fournit un contrôle de l'intégrité des données), la signature et le chiffrement LDAP (assure le contrôle de l'intégrité des données et le chiffrement)
- DÉMARRER TLS
- LDAPS (LDAP sur TLS ou SSL)

◦ Pour activer les requêtes LDAP signées et scellées, les services suivants doivent être configurés :

- Les serveurs LDAP doivent prendre en charge le mécanisme GSSAPI (Kerberos) SASL.
- Les serveurs LDAP doivent avoir des enregistrements DNS A/AAAA ainsi que des enregistrements PTR configurés sur le serveur DNS.
- Les serveurs Kerberos doivent contenir des enregistrements SRV sur le serveur DNS.

◦ Pour activer START TLS ou LDAPS, les points suivants doivent être pris en compte.

- Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.
- Si LDAPS est utilisé, le serveur LDAP doit être activé pour TLS ou pour SSL dans ONTAP 9.5 et versions ultérieures. SSL n'est pas pris en charge dans ONTAP 9.0-9.4.
- Un serveur de certificats doit déjà être configuré dans le domaine.

◦ Pour activer la recherche de recommandation LDAP (dans ONTAP 9.5 et versions ultérieures), les conditions suivantes doivent être remplies :

- Les deux domaines doivent être configurés avec l'une des relations d'approbation suivantes :
  - Bidirectionnel
  - Aller simple, où le principal fait confiance au domaine de référence
  - Parent-enfant
- Le DNS doit être configuré pour résoudre tous les noms de serveur mentionnés.
- Les mots de passe du domaine doivent être identiques pour s'authentifier lorsque --bind-as-cifs -Server est défini sur true.

Les configurations suivantes ne sont pas prises en charge avec la recherche de références LDAP.

◦ Pour toutes les versions de ONTAP :

- Clients LDAP sur un SVM d'admin

◦ Pour ONTAP 9.8 et versions antérieures (ils sont pris en charge dans la version 9.9.1 et ultérieures) :

- Signature et chiffrement LDAP (le `-session-security` en option)
- Connexions TLS cryptées (`-use-start-tls` en option)
- Communications via le port LDAPS 636 (le `-use-ldaps-for-ad-ldap` en option)

- Vous devez entrer un schéma LDAP lors de la configuration du client LDAP sur le SVM.

  Dans la plupart des cas, l'un des schémas ONTAP par défaut sera approprié. Toutefois, si le schéma LDAP de votre environnement diffère de celui-ci, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer le client LDAP. Consultez votre administrateur LDAP pour connaître les conditions requises pour votre environnement.

- L'utilisation de LDAP pour la résolution du nom d'hôte n'est pas prise en charge.

Pour en savoir plus

- "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"
- "Installer les certificats CA racine auto-signés sur le SVM SMB ONTAP"

Créer de nouveaux schémas clients LDAP pour les SVM ONTAP NFS

Si le schéma LDAP de votre environnement diffère des valeurs par défaut de ONTAP, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer la configuration du client LDAP.

Description de la tâche

La plupart des serveurs LDAP peuvent utiliser les schémas par défaut fournis par ONTAP :

- MS-AD-BIS (schéma préféré pour la plupart des serveurs AD Windows 2012 et versions ultérieures)
- AD-IDMU (serveurs AD Windows 2008, Windows 2012 et versions ultérieures)
- AD-SFU (serveurs AD Windows 2003 et versions antérieures)
- RFC-2307 (SERVEURS LDAP UNIX)

Si vous devez utiliser un schéma LDAP autre que celui par défaut, vous devez le créer avant de créer la configuration du client LDAP. Consultez votre administrateur LDAP avant de créer un nouveau schéma.

Les schémas LDAP par défaut fournis par ONTAP ne peuvent pas être modifiés. Pour créer un nouveau schéma, vous créez une copie, puis modifiez la copie en conséquence.

Étapes

1. Affichez les modèles de schéma client LDAP existants pour identifier celui que vous souhaitez copier :

   ```
   vserver services name-service ldap client schema show
   ```

2. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

3. Faites une copie d'un schéma client LDAP existant :

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Modifiez le nouveau schéma et personnalisez-le pour votre environnement :

   ```
   vserver services name-service ldap client schema modify
   ```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

Créer des configurations de client LDAP pour l'accès NFS ONTAP

Si vous souhaitez que ONTAP accède aux services LDAP ou Active Directory externes de votre environnement, vous devez d'abord configurer un client LDAP sur le système de stockage.

Avant de commencer

L'un des trois premiers serveurs de la liste des domaines résolus d'Active Directory doit être actif et transmettre des données. Dans le cas contraire, cette tâche échoue.

Il existe plusieurs serveurs, dont plus de deux serveurs sont en panne à tout moment.

Étapes

1. Consultez votre administrateur LDAP pour déterminer les valeurs de configuration appropriées pour le `vserver services name-service ldap client create` commande :

   a. Spécifiez une connexion basée sur un domaine ou une adresse aux serveurs LDAP.

      Le `-ad-domain` et `-servers` les options s'excluent mutuellement.

      - Utilisez le `-ad-domain` Option permettant d'activer la découverte de serveur LDAP dans le domaine Active Directory.
        - Vous pouvez utiliser le `-restrict-discovery-to-site` Option permettant de restreindre la découverte du serveur LDAP au site CIFS par défaut du domaine spécifié. Si vous utilisez cette option, vous devez également spécifier le site CIFS par défaut avec `-default-site`.
      - Vous pouvez utiliser le `-preferred-ad-servers` Option permettant de spécifier un ou plusieurs serveurs Active Directory préférés par adresse IP dans une liste délimitée par des virgules. Une fois le client créé, vous pouvez modifier cette liste en utilisant le `vserver services name-service ldap client modify` commande.
      - Utilisez le `-servers` Option permettant de spécifier un ou plusieurs serveurs LDAP (Active Directory ou UNIX) par adresse IP dans une liste délimitée par des virgules.

        option est obsolète. `-ldap-servers` le champ remplace le `-servers` champ. Ce champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

   b. Spécifiez un schéma LDAP par défaut ou personnalisé.

      La plupart des serveurs LDAP peuvent utiliser les schémas en lecture seule par défaut fournis par ONTAP. Il est préférable d'utiliser ces schémas par défaut à moins qu'il n'y ait une obligation de le faire autrement. Si c'est le cas, vous pouvez créer votre propre schéma en copiant un schéma par défaut (en lecture seule), puis en modifiant la copie.

      Schémas par défaut :

      - MS-AD-BIS

Basé sur RFC-2307bis, il s'agit du schéma LDAP préféré pour la plupart des déploiements LDAP standard de Windows 2012 et versions ultérieures.

- `AD-IDMU`

  Basé sur Active Directory Identity Management pour UNIX, ce schéma est adapté à la plupart des serveurs AD Windows 2008, Windows 2012 et versions ultérieures.

- `AD-SFU`

  Basé sur Active Directory Services pour UNIX, ce schéma est approprié pour la plupart des serveurs AD Windows 2003 et versions antérieures.

- `RFC-2307`

  Basé sur RFC-2307 (*une approche pour l'utilisation de LDAP en tant que service d'informations réseau*), ce schéma est approprié pour la plupart des serveurs AD UNIX.

c. Sélectionnez les valeurs de liaison.

- `-min-bind-level {anonymous|simple|sasl}` spécifie le niveau d'authentification de liaison minimum.

  La valeur par défaut est **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* spécifie l'utilisateur de liaison.

  Pour les serveurs Active Directory, vous devez spécifier l'utilisateur dans le formulaire compte (DOMAINE\utilisateur) ou principal (user@domain.com). Sinon, vous devez spécifier l'utilisateur sous le format nom distinctif (CN=user,DC=domain,DC=com).

- `-bind-password` *`password`* spécifie le mot de passe de liaison.

d. Sélectionnez les options de sécurité de session, si nécessaire.

Vous pouvez activer soit la signature et le chiffrement LDAP, soit LDAP sur TLS si le serveur LDAP en a besoin.

- `--session-security {none|sign|seal}`

  Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

  Vous devez également définir `-min-bind-level {sasl}` à moins que vous ne souhaitiez que l'authentification de la liaison revienne à **`anonymous`** ou **`simple`** en cas d'échec de la signature et de la liaison d'étanchéité.

- `-use-start-tls {true|false}`

  S'il est réglé sur **`true`** Et le serveur LDAP le prend en charge, le client LDAP utilise une connexion TLS chiffrée vers le serveur. La valeur par défaut est **`false`**. Vous devez installer un certificat d'autorité de certification racine auto-signé du serveur LDAP pour utiliser cette option.

Si un serveur SMB est ajouté à un domaine de la machine virtuelle de stockage et que le serveur LDAP fait partie des contrôleurs de domaine du domaine principal du serveur SMB, vous pouvez modifier la `-session-security-for-ad-ldap` à l'aide de `vserver cifs security modify` commande.

e. Sélectionnez les valeurs de port, de requête et de base.

Les valeurs par défaut sont recommandées, mais vous devez vérifier auprès de votre administrateur LDAP qu'elles sont adaptées à votre environnement.

- `-port` *`port`* Spécifie le port du serveur LDAP.

  La valeur par défaut est `389`.

Si vous prévoyez d'utiliser Démarrer TLS pour sécuriser la connexion LDAP, vous devez utiliser le port par défaut 389. Start TLS commence comme une connexion en texte clair sur le port par défaut LDAP 389, et cette connexion est ensuite mise à niveau vers TLS. Si vous modifiez le port, le démarrage TLS échoue.

- `-query-timeout` *`integer`* spécifie le délai d'expiration de la requête en secondes.

  La plage autorisée est de 1 à 10 secondes. La valeur par défaut est `3` secondes.

- `-base-dn` *`LDAP_DN`* Spécifie le DN de base.

  Plusieurs valeurs peuvent être saisies si nécessaire (par exemple, si la recherche de références LDAP est activée). La valeur par défaut est `""` (racine).

- `-base-scope` {`base`|`onelevel`|`subtree`} spécifie l'étendue de la recherche de base.

  La valeur par défaut est `subtree`.

- `-referral-enabled` {`true`|`false`} Indique si la recherche de recommandation LDAP est activée.

  Depuis ONTAP 9.5, ceci permet au client LDAP de ONTAP de renvoyer des demandes de recherche à d'autres serveurs LDAP si une réponse de recommandation LDAP est renvoyée par le serveur LDAP principal indiquant que les enregistrements souhaités sont présents sur les serveurs LDAP mentionnés. La valeur par défaut est **`false`**.

Pour rechercher des enregistrements présents dans les serveurs LDAP désignés, la base-dn des enregistrements recommandés doit être ajoutée à la base-dn dans le cadre de la configuration du client LDAP.

2. Créer une configuration client LDAP sur la VM de stockage :

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

Vous devez fournir le nom de la VM de stockage lors de la création d'une configuration client LDAP.

3. Vérifiez que la configuration du client LDAP a bien été créée :

```
vserver services name-service ldap client show -client-config
client_config_name
```

Exemples

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la VM de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la machine virtuelle de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP sur lequel la signature et le chiffrement sont nécessaires, et la découverte du serveur LDAP est limitée à un site particulier pour le domaine spécifié :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

La commande suivante crée une nouvelle configuration de client LDAP nommée ldap1 pour que la VM de stockage vs1 fonctionne avec un serveur Active Directory pour LDAP où la recherche de référence LDAP est requise :

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

La commande suivante modifie la configuration du client LDAP nommée ldap1 pour la VM de stockage vs1 en spécifiant le DN de base :

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

La commande suivante modifie la configuration du client LDAP appelée ldap1 pour la VM de stockage vs1 en activant la recherche de référence :

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Associer les configurations client LDAP aux SVM ONTAP NFS

Pour activer LDAP sur un SVM, vous devez utiliser `vserver services name-service ldap create` Commande permettant d'associer une configuration client LDAP à la SVM.

Avant de commencer

- Un domaine LDAP doit déjà exister au sein du réseau et doit être accessible au cluster sur lequel le SVM est situé.
- Une configuration client LDAP doit exister sur le SVM.

Étapes

1. Activer LDAP sur le SVM :

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > Le `vserver services name-service ldap create` La commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

   La commande suivante permet à LDAP sur le SVM « vs1 » et le configure pour utiliser la configuration du client LDAP « ldap1 » :

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Valider le statut des serveurs name en utilisant la commande vserver services name-service ldap check.

   La commande suivante valide les serveurs LDAP sur le SVM vs1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                   |
```

Vérifier les sources LDAP pour les SVM ONTAP NFS

On doit vérifier que les sources LDAP pour les services de noms sont correctement répertoriées dans la table de commutation de services de noms pour la SVM.

Étapes

1. Afficher le contenu de la table du commutateur de service du nom actuel :

   `vserver services name-service ns-switch show -vserver svm_name`

   La commande suivante affiche les résultats du SVM My_SVM :

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
My_SVM          hosts            files,
                                 dns
My_SVM          group            files,ldap
My_SVM          passwd           files,ldap
My_SVM          netgroup         files
My_SVM          namemap          files
5 entries were displayed.
```

   `namemap` spécifie les sources pour rechercher des informations de mappage de noms et dans quel ordre. Dans un environnement UNIX uniquement, cette entrée n'est pas nécessaire. Le mappage de noms n'est requis que dans un environnement mixte utilisant à la fois UNIX et Windows.

2. Mettez à jour le `ns-switch` saisie au besoin :

Si vous souhaitez mettre à jour l'entrée du commutateur ns pour…	Entrez la commande…
Informations utilisateur	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

Si vous souhaitez mettre à jour l'entrée du commutateur ns pour…	Entrez la commande…
Informations de groupe	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Informations sur le groupe réseau	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Utilisez Kerberos avec NFS pour une sécurité renforcée

En savoir plus sur l'utilisation de Kerberos avec ONTAP NFS pour l'authentification de sécurité

Si Kerberos est utilisé dans votre environnement pour une authentification renforcée, vous devez travailler avec votre administrateur Kerberos pour déterminer les exigences et les configurations de système de stockage appropriées, puis activer la SVM en tant que client Kerberos.

Votre environnement doit respecter les consignes suivantes :

- Votre déploiement de site doit respecter les bonnes pratiques en matière de configuration du serveur Kerberos et du client avant de configurer Kerberos pour ONTAP.
- Si possible, utilisez NFSv4 ou une version ultérieure si l'authentification Kerberos est requise.

  NFSv3 peut être utilisé avec Kerberos. Toutefois, les avantages de la sécurité totale de Kerberos ne sont réalisés que dans les déploiements ONTAP de NFSv4 ou versions ultérieures.

- Pour promouvoir un accès serveur redondant, Kerberos doit être activé sur plusieurs LIFs de données sur plusieurs nœuds du cluster à l'aide du même SPN.
- Lorsque Kerberos est activé sur le SVM, l'une des méthodes de sécurité suivantes doit être spécifiée dans des règles d'exportation pour les volumes ou les qtrees, en fonction de votre configuration client NFS.
  - `krb5` (Protocole Kerberos v5)
  - `krb5i` (Protocole Kerberos v5 avec contrôle d'intégrité à l'aide de checksums)
  - `krb5p` (Protocole Kerberos v5 avec service de confidentialité)

En plus du serveur Kerberos et des clients, les services externes suivants doivent être configurés pour ONTAP afin de prendre en charge Kerberos :

- Service d'annuaire

  Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS. N'utilisez pas NIS, dont les demandes sont envoyées en clair et ne sont donc pas sécurisées.

- NTP

  Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour

éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

  Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

Vérifier les autorisations UNIX pour les configurations NFS Kerberos sur les SVM ONTAP

Kerberos requiert que certaines autorisations UNIX soient définies pour le volume root du SVM et pour les utilisateurs et groupes locaux.

Étapes

1. Afficher les autorisations appropriées sur le volume root du SVM :

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   Le volume root du SVM doit avoir la configuration suivante :

Nom…	Paramètre…
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	755

   Si ces valeurs ne sont pas affichées, utiliser le `volume modify` pour les mettre à jour.

2. Afficher les utilisateurs UNIX locaux :

   `vserver services name-service unix-user show -vserver vserver_name`

   Le SVM doit avoir les utilisateurs UNIX suivants configurés :

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
nfs	500	0	Requis pour la phase INIT GSS. Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur. L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
racine	0	0	Nécessaire pour le montage.

Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-user modify` pour les mettre à jour.

3. Afficher les groupes UNIX locaux :

   `vserver services name-service unix-group show -vserver` *`vserver`* `_name`

   La SVM doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0

Si ces valeurs ne sont pas affichées, vous pouvez utiliser le `vserver services name-service unix-group modify` pour les mettre à jour.

Créer des configurations de domaine Kerberos NFS sur les SVM ONTAP

Si vous souhaitez que le ONTAP accède à des serveurs Kerberos externes dans votre environnement, vous devez d'abord configurer le SVM de manière à utiliser un Royaume Kerberos existant. Pour ce faire, vous devez rassembler les valeurs de configuration du serveur KDC Kerberos, puis utiliser l' `vserver nfs kerberos realm create` Commande pour créer la configuration du domaine Kerberos sur un SVM.

Avant de commencer

L'administrateur du cluster doit avoir configuré le protocole NTP sur le système de stockage, le client et le serveur KDC afin d'éviter les problèmes d'authentification. Les différences de temps entre un client et un serveur (inclinaison de l'horloge) sont une cause courante d'échecs d'authentification.

Étapes

1. Consultez votre administrateur Kerberos pour déterminer les valeurs de configuration appropriées à fournir avec le `vserver nfs kerberos realm create` commande.
2. Créer une configuration de domaine Kerberos sur le SVM :

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name {AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Vérifiez que la configuration du domaine Kerberos a bien été créée :

   `vserver nfs kerberos realm show`

Exemples

La commande suivante crée une configuration de domaine NFS Kerberos pour le SVM vs1 qui utilise un serveur Microsoft Active Directory comme serveur KDC. Le domaine Kerberos est AUTH.EXAMPLE.COM. Le serveur Active Directory est nommé ad-1 et son adresse IP est 10.10.8.14. L'inclinaison de l'horloge autorisée est de 300 secondes (par défaut). L'adresse IP du serveur KDC est 10.10.8.14 et son numéro de port est 88 (par défaut). « Microsoft Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

La commande suivante crée une configuration de Royaume NFS Kerberos pour le SVM vs1 qui utilise un MIT KDC. Le domaine Kerberos est SECURITY.EXAMPLE.COM. L'inclinaison de l'horloge autorisée est de 300 secondes. L'adresse IP du serveur KDC est 10.10.9.1 et son numéro de port est 88. Le fournisseur de KDC est autre que d'indiquer un fournisseur UNIX. L'adresse IP du serveur d'administration est 10.10.9.1 et son numéro de port est 749 (par défaut). L'adresse IP du serveur de mots de passe est 10.10.9.1 et son numéro de port est 464 (par défaut). « UNIX Kerberos config » est le commentaire.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurer les types de chiffrement Kerberos NFS autorisés pour les SVM ONTAP

Par défaut, ONTAP prend en charge les types de cryptage suivants pour Kerberos NFS : DES, 3DES, AES-128 et AES-256. Vous pouvez configurer les types de cryptage autorisés pour chaque SVM en fonction des exigences de sécurité de votre environnement en utilisant le `vserver nfs modify` commande avec `-permitted -enc-types` paramètre.

Description de la tâche

Pour une compatibilité client optimale, ONTAP prend en charge à la fois le chiffrement DES faible et le chiffrement AES fort par défaut. Cela signifie, par exemple, que si vous voulez augmenter la sécurité et que votre environnement le prend en charge, vous pouvez utiliser cette procédure pour désactiver DES et 3DES et demander aux clients d'utiliser uniquement le cryptage AES.

Vous devez utiliser le chiffrement le plus fort disponible. Pour ONTAP, c'est AES-256. Vous devez confirmer auprès de votre administrateur KDC que ce niveau de cryptage est pris en charge dans votre environnement.

- L'activation ou la désactivation totale d'AES (AES-128 et AES-256) sur les SVM provoque des perturbations, car elle détruit le fichier principal/keytab d'origine, ce qui requiert la désactivation de la configuration Kerberos sur toutes les LIFs du SVM.

  Avant d'effectuer ces modifications, vérifiez que les clients NFS ne reposent pas sur le chiffrement AES du

SVM.

- L’activation ou la désactivation DES ou 3DES ne nécessite aucune modification de la configuration Kerberos sur les LIF.

Étape

1. Activez ou désactivez le type de cryptage autorisé que vous souhaitez :

Pour activer ou désactiver…	Suivez ces étapes…
DES ou 3DES	a. Configurer les types de cryptage NFS Kerberos autorisés du SVM : `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Séparez les différents types de cryptage par une virgule. b. Vérifiez que la modification a réussi : `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Pour activer ou désactiver…	Suivez ces étapes…

AES-128 ou AES-256	a. Identifier sur quel SVM et LIF Kerberos sont activés :
	
	`vserver nfs kerberos interface show`
	
	b. Désactiver Kerberos sur toutes les LIFs sur le SVM dont NFS Kerberos autorisé type de cryptage que vous souhaitez modifier :
	
	`vserver nfs kerberos interface disable -lif lif_name`
	
	c. Configurer les types de cryptage NFS Kerberos autorisés du SVM :
	
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	Séparez les différents types de cryptage par une virgule.
	
	d. Vérifiez que la modification a réussi :
	
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	
	e. Réactiver Kerberos sur toutes les LIFs sur le SVM :
	
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	
	f. Vérifier que Kerberos est activé sur toutes les LIFs :
	
	`vserver nfs kerberos interface show`

Activer NFS Kerberos sur les LIF ONTAP

Vous pouvez utiliser le `vserver nfs kerberos interface enable` Commande pour activer Kerberos sur une LIF de données. Cela permet au SVM d'utiliser les services de sécurité Kerberos pour NFS.

Description de la tâche

Si vous utilisez un KDC Active Directory, les 15 premiers caractères de tous les noms de domaine utilisés doivent être uniques sur les SVM au sein d'un domaine ou d'un domaine.

Étapes

1. Créez la configuration NFS Kerberos :

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   ONTAP nécessite la clé secrète pour le SPN à partir du KDC pour activer l'interface Kerberos.

   Pour les VDC Microsoft, le KDC est contacté et un nom d'utilisateur et un mot de passe sont émis sur l'CLI pour obtenir la clé secrète. Si vous devez créer le SPN dans une autre UO du domaine Kerberos, vous pouvez spécifier l'option `-ou` paramètre.

   Pour les KDC non Microsoft, la clé secrète peut être obtenue en utilisant l'une des deux méthodes suivantes :

Si…	**Vous devez également inclure le paramètre suivant avec la commande…**
Demandez à l'administrateur KDC de récupérer la clé directement à partir du KDC	`-admin-username` *`kdc_admin_username`*
Ne disposez pas des informations d'identification de l'administrateur KDC mais d'un fichier keytab du KDC contenant la clé	`-keytab-uri` {ftp

2. Vérifier que Kerberos a été activé sur la LIF :

   `vserver nfs kerberos-config show`

3. Répétez les étapes 1 et 2 pour activer Kerberos sur plusieurs LIFs.

Exemple

La commande suivante crée et vérifie une configuration Kerberos NFS pour le SVM nommé vs1 sur l'interface logique ves03-d1, avec le SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM dans l'UO lab2ou :

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- ------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Ajout de capacité de stockage à un SVM compatible NFS

En savoir plus sur l'ajout de capacité de stockage à un SVM compatible NFS ONTAP

Pour ajouter de la capacité de stockage à un SVM compatible NFS, vous devez créer un volume ou qtree pour fournir un conteneur de stockage, et créer ou modifier une export policy pour ce conteneur. Vous pouvez ensuite vérifier l'accès client NFS depuis le cluster et tester l'accès depuis les systèmes client.

Avant de commencer

- NFS doit être entièrement configuré sur le SVM.
- La export policy default du volume root du SVM doit contenir une règle qui permet d'accéder à tous les clients.
- Toute mise à jour de la configuration des services de noms doit être terminée.
- Tout ajout ou modification d'une configuration Kerberos doit être effectué.

Créer une politique d'exportation NFS ONTAP

Avant de créer des règles d'exportation, vous devez créer une export-policy pour les tenir. Vous pouvez utiliser le `vserver export-policy create` commande pour créer une export policy.

Étapes

1. Créer une export-policy :

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   Le nom de la stratégie peut comporter jusqu'à 256 caractères.

2. Vérifier que l'export policy a été créée :

   `vserver export-policy show -policyname` *`policy_name`*

Exemple

Les commandes suivantes créent et vérifient la création d'une export policy nommée exp1 sur le SVM nommé vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Ajouter une règle à une politique d'exportation NFS ONTAP

Sans règles, l'export policy ne peut pas fournir aux clients l'accès aux données. Pour

créer une nouvelle règle d'exportation, vous devez identifier les clients et sélectionner un format de correspondance client, sélectionner les types d'accès et de sécurité, spécifier un mappage d'ID utilisateur anonyme, sélectionner un numéro d'index de règle et sélectionner le protocole d'accès. Vous pouvez ensuite utiliser le `vserver export-policy rule create` commande pour ajouter la nouvelle règle à une export-policy.

Avant de commencer

- L'export policy à laquelle vous souhaitez ajouter les règles d'exportation doit déjà exister.
- Le DNS doit être correctement configuré sur le SVM de données et les serveurs DNS doivent avoir des entrées correctes pour les clients NFS.

  En effet, ONTAP effectue des recherches DNS en utilisant la configuration DNS du SVM de données pour certains formats de correspondance client, et les échecs de mise en correspondance de règles d'export peuvent empêcher l'accès aux données client.

- Si vous authentifiez avec Kerberos, vous devez avoir déterminé les méthodes de sécurité suivantes utilisées sur vos clients NFS :
  - `krb5` (Protocole Kerberos V5)
  - `krb5i` (Protocole Kerberos V5 avec contrôle d'intégrité à l'aide de checksums)
  - `krb5p` (Protocole Kerberos V5 avec service de confidentialité)

Description de la tâche

Il n'est pas nécessaire de créer une nouvelle règle si une règle existante d'une stratégie d'exportation couvre la correspondance de vos clients et les exigences d'accès.

Si vous authentifiez avec Kerberos et si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5`, `krb5i`, ou `krb5p`.

Étapes

1. Identifiez les clients et le format de correspondance client pour la nouvelle règle.

   Le `-clientmatch` spécifie les clients auxquels la règle s'applique. Des valeurs de correspondance client uniques ou multiples peuvent être spécifiées ; les spécifications de valeurs multiples doivent être séparées par des virgules. Vous pouvez spécifier la correspondance dans l'un des formats suivants :

Format de correspondance client	Exemple
Nom de domaine précédé du caractère "."	`.example.com` ou `.example.com,.example.net,...`
Nom d'hôte	`host1` ou `host1,host2, ...`
Adresse IPv4	`10.1.12.24` ou `10.1.12.24,10.1.12.25, ...`

Format de correspondance client	Exemple
Adresse IPv4 avec un masque de sous-réseau exprimé en nombre de bits	`10.1.12.10/4` ou `10.1.12.10/4,10.1.12.11/4,...`
Adresse IPv4 avec un masque de réseau	`10.1.16.0/255.255.255.0` ou `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Adresse IPv6 en format pointillé	`::1.2.3.4` ou `::1.2.3.4,::1.2.3.5,...`
Adresse IPv6 avec un masque de sous-réseau exprimé en nombre de bits	`ff::00/32` ou `ff::00/32,ff::01/32,...`
Un seul groupe de réseau avec le nom de groupe de réseau précédé du caractère @	`@netgroup1` ou `@netgroup1,@netgroup2,...`

Vous pouvez également combiner des types de définitions de client, par exemple, `.example.com,@netgroup1`.

Lors de la définition des adresses IP, notez les éléments suivants :

- La saisie d'une plage d'adresses IP, par exemple 10.1.12.10-10.1.12.70, n'est pas autorisée.

  Les entrées de ce format sont interprétées comme une chaîne de texte et sont traitées comme un nom d'hôte.

- Lors de la spécification d'adresses IP individuelles dans des règles d'exportation pour la gestion granulaire de l'accès client, ne spécifiez pas d'adresses IP dynamiquement (par exemple, DHCP) ou temporairement (par exemple, IPv6) attribuées.

  Sinon, le client perd l'accès lorsque son adresse IP change.

- La saisie d'une adresse IPv6 avec un masque de réseau, par exemple ff::12/ff::00, n'est pas autorisée.

2. Sélectionnez les types d'accès et de sécurité pour les correspondances client.

   Vous pouvez spécifier un ou plusieurs des modes d'accès suivants aux clients qui s'authentifient avec les types de sécurité spécifiés :

   - `-rorule` (accès en lecture seule)
   - `-rwrule` (accès en lecture/écriture)
   - `-superuser` (accès racine)

   > Un client peut uniquement obtenir un accès en lecture/écriture pour un type de sécurité spécifique si la règle d'exportation autorise également un accès en lecture seule pour ce type de sécurité. Si le paramètre lecture seule est plus restrictif pour un type de sécurité que le paramètre lecture-écriture, il se peut que le client n'ait pas accès en lecture-écriture. Il en va de même pour l'accès superutilisateur.

Vous pouvez spécifier une liste de plusieurs types de sécurité séparés par des virgules pour une règle. Si vous spécifiez le type de sécurité comme `any` ou `never`, ne spécifiez aucun autre type de sécurité. Choisissez parmi les types de sécurité valides suivants :

Lorsque le type de sécurité est défini sur…	Un client correspondant peut accéder aux données exportées…
`any`	Toujours, quel que soit le type de sécurité entrant.
`none`	S'ils sont répertoriés seuls, l'accès des clients possédant n'importe quel type de sécurité est accordé en tant qu'anonyme. Si elle est répertoriée avec d'autres types de sécurité, les clients avec un type de sécurité spécifié bénéficient d'un accès et les clients avec un autre type de sécurité bénéficient d'un accès anonyme.
`never`	Jamais, quel que soit le type de sécurité entrant.
`krb5`	S'il est authentifié par Kerberos 5. Authentification uniquement : l'en-tête de chaque requête et réponse est signé.
`krb5i`	S'il est authentifié par Kerberos 5i. Authentification et intégrité : l'en-tête et le corps de chaque requête et réponse sont signés.
`krb5p`	S'il est authentifié par Kerberos 5p. Authentification, intégrité et confidentialité : l'en-tête et le corps de chaque requête et réponse sont signés, et la charge utile des données NFS est chiffrée.
`ntlm`	S'il est authentifié par CIFS NTLM.
`sys`	S'il est authentifié par NFS AUTH_SYS.

Le type de sécurité recommandé est `sys`, Ou si Kerberos est utilisé, `krb5`, `krb5i`, ou `krb5p`.

Si vous utilisez Kerberos avec NFSv3, la règle de export policy doit autoriser `-rorule` et `-rwrule` accès à `sys` en plus de `krb5`. Ceci est dû au besoin d'autoriser l'accès à Network Lock Manager (NLM) pour l'exportation.

3. Spécifiez un mappage d'ID utilisateur anonyme.

   Le `-anon` Option spécifie un ID utilisateur ou un nom d'utilisateur UNIX qui est mappé aux demandes client qui arrivent avec un ID utilisateur de 0 (zéro), généralement associé à la racine du nom d'utilisateur. La valeur par défaut est `65534`. Les clients NFS associent généralement l'ID utilisateur 65534 au nom d'utilisateur personne (également appelé *root scaling*). Dans ONTAP, cet ID utilisateur est associé à l'utilisateur pcuser. Pour désactiver l'accès par tout client ayant un ID utilisateur de 0, spécifiez une valeur

de `65535`.

4. Sélectionnez l'ordre d'index des règles.

   Le `-ruleindex` option spécifie le numéro d'index de la règle. Les règles sont évaluées en fonction de leur ordre dans la liste des numéros d'index ; les règles avec des numéros d'index inférieurs sont évaluées en premier. Par exemple, la règle avec l'index numéro 1 est évaluée avant la règle avec l'index numéro 2.

Si vous ajoutez…	Alors…
La première règle vers une export-policy	Entrez `1`.
Règles supplémentaires à une export-policy	a. Afficher les règles existantes dans la stratégie : `vserver export-policy rule show -instance -policyname` *`your_policy`* b. Sélectionnez un numéro d'index pour la nouvelle règle en fonction de l'ordre dans lequel elle doit être évaluée.

5. Sélectionnez la valeur d'accès NFS applicable : {`nfs`|`nfs3`|`nfs4`}.

   `nfs` correspond à n'importe quelle version, `nfs3` et `nfs4` correspondent uniquement à ces versions spécifiques.

6. Créer la règle d'exportation et l'ajouter à une export policy existante :

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. Afficher les règles pour l'export policy pour vérifier que la nouvelle règle est présente :

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   La commande affiche un récapitulatif de cette export policy, y compris une liste des règles appliquées à cette policy. ONTAP attribue à chaque règle un numéro d'index de règle. Après avoir connu le numéro d'index de la règle, vous pouvez l'utiliser pour afficher des informations détaillées sur la règle d'exportation spécifiée.

8. Vérifiez que les règles appliquées à l'export policy sont configurées correctement :

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

Exemples

Les commandes suivantes créent et vérifient la création d'une règle d'exportation sur le SVM nommé vs1 dans une export policy nommée rs1. La règle a l'index numéro 1. La règle correspond à n'importe quel client du domaine eng.company.com et au groupe réseau @netgroup1. La règle active tous les accès NFS. Il active l'accès en lecture seule et en lecture-écriture aux utilisateurs authentifiés avec AUTH_SYS. Les clients

possédant l'ID utilisateur UNIX 0 (zéro) sont anonymisés sauf s'ils sont authentifiés avec Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Les commandes suivantes créent et vérifient la création d'une règle d'export sur le SVM nommé vs2 dans une export policy nommée expol2. La règle a le numéro d'index 21. La règle correspond aux clients aux membres du groupe réseau dev_netgroup_main. La règle active tous les accès NFS. Il active un accès en lecture seule pour les utilisateurs authentifiés avec AUTH_SYS et nécessite une authentification Kerberos pour l'accès en lecture-écriture et racine. Les clients possédant l'ID utilisateur UNIX 0 (zéro) se voient refuser l'accès racine sauf s'ils sont authentifiés avec Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                Vserver: vs2
                            Policy Name: expol2
                             Rule Index: 21
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
                          RO Access Rule: sys
                          RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Créer un volume ou un conteneur de stockage qtree

Créer un volume NFS ONTAP

Vous pouvez créer un volume et spécifier son point de jonction et d'autres propriétés en utilisant le `volume create` commande.

Description de la tâche

Un volume doit inclure une *Junction path* pour que ses données soient mises à disposition des clients. Vous pouvez spécifier le chemin de jonction lorsque vous créez un nouveau volume. Si vous créez un volume sans spécifier un chemin de jonction, vous devez *mount* le volume du namespace du SVM à l'aide de `volume mount` commande.

Avant de commencer

- NFS doit être configuré et exécuté.
- La sécurité du SVM doit être de style UNIX.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes avec les fonctions d'analyse de la capacité et de suivi des activités activées. Pour activer le suivi de capacité ou d'activité, exécutez la `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` définissez sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "Activez l'analyse du système de fichiers". Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

Étapes

1. Créer le volume avec un point de jonction :

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   Les choix pour `-junction-path` sont les suivants :

   - Directement sous la racine, par exemple, */new_vol*

     Vous pouvez créer un nouveau volume et préciser qu'il peut être monté directement sur le volume root du SVM.

   - Sous un répertoire existant, par exemple, */existing_dir/new_vol*

     Vous pouvez créer un nouveau volume et spécifier qu'il doit être monté sur un volume existant (dans une hiérarchie existante), exprimé en tant que répertoire.

     Si vous souhaitez créer un volume dans un nouveau répertoire (dans une nouvelle hiérarchie sous un nouveau volume), par exemple, */new_dir/new_vol*, Ensuite, vous devez d'abord créer un nouveau volume parent qui est relié par une jonction au volume racine de la SVM. Vous devez ensuite créer le nouveau volume enfant dans la Junction path du nouveau volume parent (nouveau répertoire).

     Si vous prévoyez d'utiliser une export policy existante, vous pouvez la spécifier lors de la création du volume. Vous pouvez également ajouter une export-policy plus tard avec le `volume modify` commande.

2. Vérifier que le volume a été créé avec le point de jonction souhaité :

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Exemples

La commande suivante crée un nouveau volume nommé users1 sur le SVM vs1.example.com et l'agrégat aggr1. Le nouveau volume est disponible sur le site `/users`. Le volume a une taille de 750 Go et sa garantie de volume est de type volume (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

La commande suivante crée un nouveau volume nommé « home4 » sur le SVM « vs1.example.com » et l'agrégat « aggr1 ». Le répertoire `/eng/` Existe déjà dans l'espace de nommage de la SVM vs1, et le nouveau volume est mis à disposition à `/eng/home`, qui devient le répertoire de base de l' `/eng/` espace de noms. Le volume a une taille de 750 Go et sa garantie de volume est de type `volume` (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Créer un qtree ONTAP NFS

Vous pouvez créer un qtree pour contenir vos données et spécifier ses propriétés en utilisant le `volume qtree create` commande.

Avant de commencer

- La SVM et le volume qui contiendra le nouveau qtree doivent déjà exister.
- La méthode de sécurité SVM doit être UNIX et NFS doit être configuré et en cours d'exécution.

Étapes

1. Créer le qtree :

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Vous pouvez spécifier le volume et qtree en tant qu'arguments distincts ou spécifier l'argument du chemin qtree au format `/vol/`*`volume_name/_qtree_name`*.

   Par défaut, les qtrees héritent des règles d'exportation du volume parent, mais ils peuvent être configurés pour leur propre volume. Si vous prévoyez d'utiliser une export policy existante, vous pouvez l'indiquer lors

de la création du qtree. Vous pouvez également ajouter une export-policy plus tard avec le `volume qtree modify` commande.

2. Vérifier que le qtree a été créé avec le chemin de jonction souhaité :

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Exemple

L'exemple suivant crée un qtree nommé qt01 situé sur le SVM vs1.example.com qui dispose d'un chemin de jonction `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                    Vserver Name: vs1.example.com
                     Volume Name: data1
                      Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                  Security Style: unix
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                         Qtree Id: 2
                     Qtree Status: normal
                   Export Policy: default
        Is Export Policy Inherited: true
```

Sécurisation de l'accès NFS à l'aide de règles d'exportation

En savoir plus sur la sécurisation de l'accès NFS ONTAP à l'aide de politiques d'exportation

Vous pouvez utiliser des règles d'exportation pour restreindre l'accès NFS aux volumes ou aux qtrees aux clients correspondant à des paramètres spécifiques. Lorsque vous provisionnez un nouveau stockage, vous pouvez utiliser une stratégie et des règles existantes, ajouter des règles à une stratégie existante, ou créer une nouvelle règle et de nouvelles règles. Vous pouvez également vérifier la configuration des export-policies

Depuis ONTAP 9.3, vous pouvez activer la vérification de la configuration des règles d'exportation en tant que tâche d'arrière-plan qui enregistre toutes les violations de règles dans une liste de règles d'erreur. Le `vserver export-policy config-checker` Les commandes appellent le vérificateur et affichent les résultats, que vous pouvez utiliser pour vérifier votre configuration et supprimer des règles erronées de la stratégie. Les commandes ne valident que la configuration d'exportation pour les noms d'hôte, les groupes réseau et les utilisateurs anonymes.

Gérer l'ordre de traitement des règles d'exportation ONTAP NFS

Vous pouvez utiliser le `vserver export-policy rule setindex` commande permettant de définir manuellement le numéro d'index d'une règle d'exportation existante. Cela vous permet de spécifier la priorité selon laquelle ONTAP applique des règles d'exportation aux requêtes client.

Description de la tâche

Si le nouveau numéro d'index est déjà utilisé, la commande insère la règle au point spécifié et réorganise la liste en conséquence.

Étape

1. Modifier le numéro d'index d'une règle d'exportation spécifiée :

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Exemple

La commande suivante modifie l'index numéro d'une règle d'exportation au niveau de l'index numéro 3 en index numéro 2 dans une export policy nommée rs1 sur le SVM nommée vs1 :

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Attribuer une politique d'exportation ONTAP NFS à un volume

Chaque volume contenu au SVM doit être associé à une export policy qui contient les export rules auxquelles les clients ont accès les données au sein du volume.

Description de la tâche

Vous pouvez associer une export policy à un volume lors de la création du volume ou à tout moment après sa création. Vous pouvez associer une export policy au volume, bien qu'une seule policy puisse être associée à de nombreux volumes.

Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du volume, affectez une export policy au volume :

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Vérifiez que la policy a été assignée au volume :

   ```
   volume show -volume volume_name -fields policy
   ```

Exemple

Les commandes suivantes affectent l'export policy nfs_policy vers le volume vol1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Attribuer une politique d'exportation ONTAP NFS à un qtree

Au lieu d'exporter un volume entier, vous pouvez également exporter un qtree spécifique sur un volume afin de le rendre directement accessible aux clients. Vous pouvez exporter un qtree en lui attribuant une export policy. Vous pouvez affecter la export policy lorsque vous créez un qtree ou en modifiant un qtree existant.

Avant de commencer

La export policy doit exister.

Description de la tâche

Par défaut, les qtrees héritent de la politique d'exportation parent du volume contenant, si elle n'est pas spécifiée au moment de la création.

Vous pouvez associer une export policy à un qtree lors de la création du qtree ou à tout moment après la création du qtree. Vous pouvez associer une export policy au qtree, bien qu'une seule règle puisse être associée à de nombreux qtrees.

Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du qtree, assigner une export policy au qtree :

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. Vérifier que la règle a été attribuée au qtree :

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Exemple

Les commandes suivantes affectent l'export policy nfs_policy au qtree qt1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Vérifier l'accès du client NFS ONTAP à partir du cluster

Vous pouvez donner à certains clients l'accès au partage en définissant les autorisations de fichier UNIX sur un hôte d'administration UNIX. Vous pouvez vérifier l'accès client à l'aide de `vserver export-policy check-access` commande, en ajustant les règles d'exportation si nécessaire.

Étapes

1. Sur le cluster, vérifiez l'accès des clients aux exportations à l'aide de `vserver export-policy check-access` commande.

   La commande suivante vérifie l'accès en lecture/écriture pour un client NFSv3 avec l'adresse IP 1.2.3.4 vers la commande volume home2. La sortie de la commande indique que le volume utilise la export policy `exp-home-dir` et cet accès est refusé.

   ```
   cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
   1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
   -type read-write
                                       Policy    Policy     Rule
   Path                    Policy      Owner     Owner Type Index  Access
   ----------------------- ----------- --------- ---------- ------
   ----------
   /                       default     vs1_root  volume          1 read
   /eng                    default     vs1_root  volume          1 read
   /eng/home2              exp-home-dir home2    volume          1 denied

   3 entries were displayed.
   ```

2. Examinez la sortie pour déterminer si l'export policy fonctionne comme prévu et si l'accès client se comporte comme prévu.

   Plus précisément, vous devez vérifier quelles export policy est utilisée par le volume ou qtree et ce type d'accès par le client.

3. Si nécessaire, reconfigurer les règles d'export policy.

Tester l'accès ONTAP NFS à partir des systèmes clients

Après avoir vérifié l'accès NFS au nouvel objet de stockage, il est important de tester la configuration en vous connectant à un hôte d'administration NFS et en lisant les données à partir de et en écrivant les données sur la SVM. Vous devez ensuite répéter le processus en tant qu'utilisateur non-root sur un système client.

Avant de commencer

- Le système client doit disposer d'une adresse IP autorisée par la règle d'exportation que vous avez spécifiée précédemment.
- Vous devez disposer des informations de connexion pour l'utilisateur root.

Étapes

1. Sur le cluster, vérifier l'adresse IP de la LIF qui héberge le nouveau volume :

   `network interface show –vserver` *`svm_name`*

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

2. Connectez-vous en tant qu'utilisateur racine au système client hôte d'administration.
3. Changez le répertoire pour le dossier de montage :

   `cd /mnt/`

4. Créer et monter un nouveau dossier en utilisant l'adresse IP de la SVM :

   a. Créer un nouveau dossier :

      `mkdir /mnt/`*`folder`*

   b. Montez le nouveau volume dans ce nouveau répertoire :

      `mount -t nfs -o hard` *`IPAddress`*`:/`*`volume_name`* `/mnt/`*`folder`*

   c. Changez le répertoire pour le nouveau dossier :

      `cd` *`folder`*

      Les commandes suivantes créent un dossier nommé test1, montent le volume vol1 à l'adresse IP 192.0.2.130 du dossier de montage tes1 et changent dans le nouveau répertoire tes1 :

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Créez un nouveau fichier, vérifiez qu'il existe et écrivez du texte :

   a. Créer un fichier de test :

      `touch` *`filename`*

b. Vérifiez que le fichier existe :

```
ls -l filename
```

c. Entrez :

```
cat > filename
```

Tapez du texte, puis appuyez sur Ctrl+D pour écrire du texte dans le fichier test.

d. Afficher le contenu du fichier de test.

```
cat filename
```

e. Supprimez le fichier de test :

```
rm filename
```

f. Retour au répertoire parent :

```
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. En tant que root, définissez les droits de propriété et les autorisations UNIX souhaités sur le volume monté.
7. Sur un système client UNIX identifié dans vos règles d'exportation, connectez-vous en tant qu'un des utilisateurs autorisés qui ont désormais accès au nouveau volume, puis répétez les procédures des étapes 3 à 5 pour vérifier que vous pouvez monter le volume et créer un fichier.

Où trouver des informations supplémentaires sur ONTAP NFS

Après avoir testé l'accès client NFS avec succès, vous pouvez effectuer une configuration NFS supplémentaire ou ajouter un accès SAN. Une fois les protocoles accès terminés, vous devez protéger le volume root de la machine virtuelle de stockage (SVM).

Configuration NFS

Vous pouvez configurer davantage l'accès NFS à l'aide des informations et rapports techniques suivants :

- "Gestion NFS"

Décrit comment configurer et gérer l'accès aux fichiers à l'aide de NFS.

- "Rapport technique NetApp 4067 : Guide des meilleures pratiques et de mise en œuvre de NFS"

  Sert de guide opérationnel NFSv3 et NFSv4, et présente le système d'exploitation ONTAP avec un accent sur NFSv4.

- "Rapport technique NetApp 4073 : authentification unifiée sécurisée"

  Explique comment configurer ONTAP pour une utilisation avec des serveurs Kerberos version 5 (krb5) UNIX pour l'authentification du stockage NFS et Windows Server Active Directory (AD) en tant que fournisseur d'identité KDC et Lightweight Directory Access Protocol (LDAP).

- "Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"

  Décrit les meilleures pratiques à suivre lors de l'implémentation des composants NFSv4 sur des clients AIX, Linux ou Solaris reliés à des systèmes exécutant ONTAP.

Configuration de la mise en réseau

Vous pouvez configurer davantage les fonctions de réseau et les services de noms à l'aide des informations et rapports techniques suivants :

- "Gestion NFS"

  Décrit la configuration et la gestion de la mise en réseau ONTAP.

- "Rapport technique NetApp 4182 : considérations relatives à la conception du stockage Ethernet et meilleures pratiques pour les configurations clustered Data ONTAP"

  Décrit l'implémentation des configurations réseau ONTAP et fournit des scénarios de déploiement réseau communs et des recommandations sur les meilleures pratiques.

- "Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

  Explique comment configurer LDAP, NIS, DNS et la configuration de fichiers locaux à des fins d'authentification.

Configuration du protocole SAN

Si vous souhaitez fournir ou modifier un accès SAN au nouveau SVM, vous pouvez utiliser les informations de configuration FC ou iSCSI disponibles pour plusieurs systèmes d'exploitation hôtes.

Protection du volume racine

Après avoir configuré les protocoles sur le SVM, il faut s'assurer que son volume root est protégé :

- "Protection des données"

  Décrit la procédure de création d'un miroir de partage de charge pour protéger le volume racine du SVM, une pratique recommandée par NetApp pour les SVM compatibles avec NAS. Décrit également la procédure de restauration rapide en cas de défaillances ou de pertes de volumes en promouvant le volume racine du SVM à partir d'un miroir de partage de charge.

La différence entre les exportations ONTAP et les exportations 7-mode

La différence entre les exportations ONTAP et les exportations 7-mode

Si vous ne savez pas comment ONTAP implémente les exports NFS, vous pouvez comparer les outils de configuration d'exportation 7-mode et ONTAP, ainsi que les exemples 7-mode `/etc/exports` fichiers avec des règles et règles en cluster.

En ONTAP, il n'y a pas de `/etc/exports` fichier et non `exportfs` commande. Vous devez plutôt définir une export-policy. Les export-policies vous permettent de contrôler l'accès des clients de la même manière que dans 7-mode. Toutefois, vous offrent des fonctionnalités supplémentaires, telles que la possibilité de réutiliser la même export policy pour plusieurs volumes.

Informations associées

"Gestion NFS"

"Rapport technique NetApp 4067 : Guide des meilleures pratiques et de mise en œuvre de NFS"

En savoir plus sur les comparaisons d'exportation NFS 7-Mode et ONTAP

Dans ONTAP, les exportations sont définies et utilisées différemment des environnements 7-mode.

Domaines de différence	7-mode	ONTAP
Définition des exportations	Les exportations sont définies dans le `/etc/exports` fichier.	Les exportations sont définies par la création d'une export policy au sein d'un SVM. Un SVM peut inclure plusieurs export policy.
Champ d'application de l'exportation	• Les exportations s'appliquent à un chemin de fichiers ou à un qtree spécifié. • Vous devez créer une entrée séparée dans `/etc/exports` pour chaque chemin de fichier ou qtree. • Les exportations ne sont persistantes que si elles sont définies dans le `/etc/exports` fichier.	• Les règles d'exportation s'appliquent à tout un volume, y compris l'ensemble des chemins de fichiers et qtrees contenu dans le volume. • Si vous le souhaitez, des règles d'exportation peuvent être appliquées à plusieurs volumes. • Toutes les règles d'exportation sont conservées sur l'ensemble des redémarrages du système.

Escrime (spécification d'un accès différent pour des clients spécifiques aux mêmes ressources)	Pour fournir à des clients spécifiques un accès différent à une seule ressource exportée, vous devez répertorier chaque client et son accès autorisé dans `/etc/exports` fichier.	Les export-policies se composent d'un certain nombre de règles d'exportation individuelles. Chaque règle d'exportation définit des autorisations d'accès spécifiques pour une ressource et répertorie les clients disposant de ces autorisations. Pour spécifier un accès différent pour des clients spécifiques, vous devez créer une règle d'exportation pour chaque ensemble spécifique d'autorisations d'accès, répertorier les clients disposant de ces autorisations, puis ajouter les règles à la export policy.
Changement de nom	Lorsque vous définissez une exportation, vous pouvez choisir de modifier le nom de l'exportation par rapport au nom du chemin du fichier. Vous devez utiliser le `-actual` paramètre lors de la définition d'une telle exportation dans le `/etc/exports` fichier.	Vous pouvez choisir de rendre le nom du volume exporté différent de celui du volume réel. Pour ce faire, il faut monter le volume avec un nom de chemin de jonction personnalisé au sein du namespace du SVM. Par défaut, les volumes sont montés avec leur nom de volume. Pour personnaliser le chemin de jonction d'un volume, vous devez le démonter, le renommer, puis le remonter.

En savoir plus sur les exemples de politiques d'exportation NFS ONTAP

Vous pouvez consulter des exemples de règles d'exportation pour mieux comprendre le fonctionnement des règles d'exportation dans ONTAP.

Exemple d'implémentation ONTAP d'une exportation 7-mode

L'exemple suivant montre une exportation 7-mode telle qu'elle s'affiche dans la `/etc/export` fichier :

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Pour reproduire cet export policy en cluster, il faut créer une export policy avec trois règles d'exportation, puis

assigner la export policy au volume vol1.

Règle	Elément	Valeur
Règle 1	`-clientmatch` (spécification client)	`@readonly_netgroup`
`-ruleindex`(position de la règle d'exportation dans la liste des règles)	`1`	`-protocol`
`nfs`	`-rorule`(autoriser l'accès en lecture seule)	`sys` (Client authentifié avec AUTH_SYS)
`-rwrule`(autoriser l'accès en lecture/écriture)	`never`	`-superuser`(autoriser l'accès superutilisateur)
`none`(racine *écrasée* à anon)	Règle 2	`-clientmatch`
`@rootaccess_netgroup`	`-ruleindex`	`2`
`-protocol`	`nfs`	`-rorule`
`sys`	`-rwrule`	`sys`
`-superuser`	`sys`	Règle 3
`-clientmatch`	`@readwrite_netgroup1,@readwrite_netgroup2`	`-ruleindex`
`3`	`-protocol`	`nfs`
`-rorule`	`sys`	`-rwrule`
`sys`	`-superuser`	`none`

1. Créez une export policy appelée exp_vol1 :

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Créer trois règles avec les paramètres suivants pour la commande de base :
   - Commande de base :

     ```
     vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
     ```

   - Paramètres de règle :

```
-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
-rwrule never -superuser none

-clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
-rwrule sys -superuser sys

-clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
-protocol nfs -rorule sys -rwrule sys -superuser none
```

3. Affectez la policy au volume vol1 :

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

Exemple de consolidation des exports 7-mode

L'exemple suivant montre 7-mode `/etc/export` fichier qui inclut une ligne pour chacun des 10 qtrees :

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

Dans ONTAP, une des deux règles est nécessaire pour chaque qtree : l'une avec une règle incluant `-clientmatch host1519s`, ou un avec une règle incluant `-clientmatch host2057s`.

1. Créez deux règles d'exportation appelées exp_vol1q1 et exp_vol1q2 :
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Créer une règle pour chaque règle :
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. Appliquer les règles aux qtrees :
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [4 qtrees suivants…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`

◦ [4 qtrees suivants…]

Si vous devez ajouter des qtrees supplémentaires pour ces hôtes, vous utiliserez les mêmes règles d'exportation.

Gérez NFS avec l'interface de ligne de commande

En savoir plus sur l'accès aux fichiers ONTAP pour le protocole NFS

ONTAP inclut des fonctionnalités d'accès aux fichiers disponibles pour le protocole NFS. Vous pouvez activer un serveur NFS et exporter des volumes ou des qtrees.

Vous effectuez cette procédure dans les cas suivants :

- Vous souhaitez connaître la gamme de fonctionnalités de protocole NFS de ONTAP.
- Vous souhaitez effectuer des tâches de configuration et de maintenance moins courantes, pas une configuration NFS de base.
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

Compréhension de l'accès aux fichiers NAS

Espaces de noms et points de jonction

En savoir plus sur les espaces de noms et les points de jonction NAS ONTAP

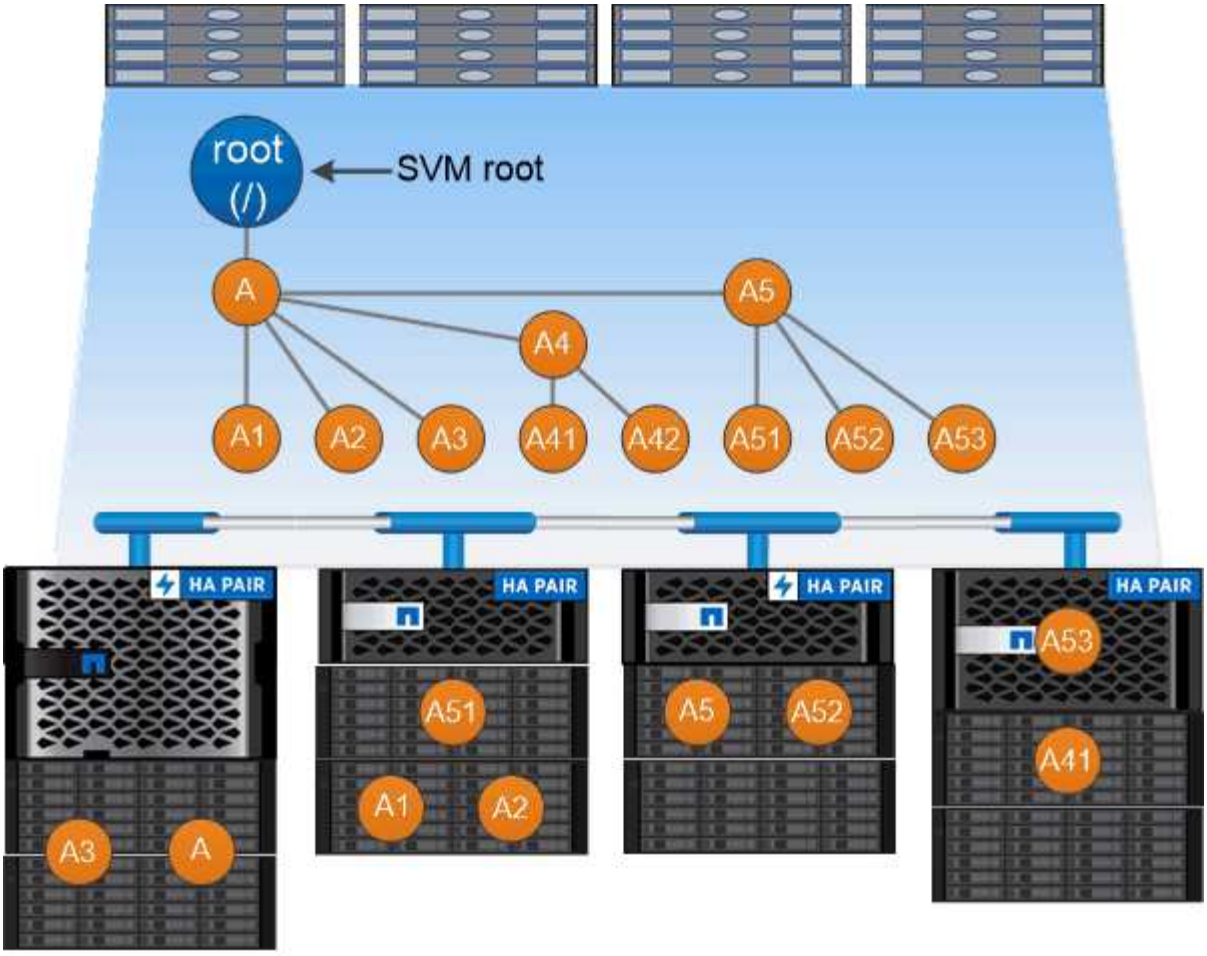
Un NAS *namespace* est un regroupement logique de volumes regroupés à *Junction points* pour créer une seule hiérarchie de système de fichiers. Un client disposant des autorisations suffisantes peut accéder aux fichiers dans l'espace de noms sans spécifier l'emplacement des fichiers dans le stockage. Des volumes regroupés dans le cluster peuvent se trouver n'importe où.

Plutôt que de monter chaque volume contenant un fichier d'intérêt, les clients NAS monter un NFS *export* ou accéder à un partage SMB._ l'exportation ou le partage représente l'intégralité de l'espace de noms ou un emplacement intermédiaire dans l'espace de noms. Le client n'accède qu'aux volumes montés sous son point d'accès.

Vous pouvez ajouter des volumes au namespace selon vos besoins. Vous pouvez créer des points de jonction directement en-dessous d'une jonction de volume parent ou sur un répertoire au sein d'un volume. Il se peut qu'un chemin vers une jonction de volume pour un volume nommé « vol3 » soit possible `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou même `/dir1/dir2/vol3`. Le chemin est appelé *Junction path.*

Chaque SVM possède un espace de noms unique. Le volume root du SVM est le point d'entrée de la hiérarchie de l'espace de noms.

Pour garantir la disponibilité des données en cas de panne du nœud ou de basculement, vous devez créer une copie *load-sharing mirror* pour le volume root du SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

En savoir plus sur les architectures d'espace de noms NAS ONTAP

Plusieurs architectures d'espace de noms NAS classiques peuvent être utilisées lors de la création d'un espace de noms de SVM. Vous pouvez choisir l'architecture d'espace de noms qui correspond le mieux à vos besoins métiers et de flux de travail.

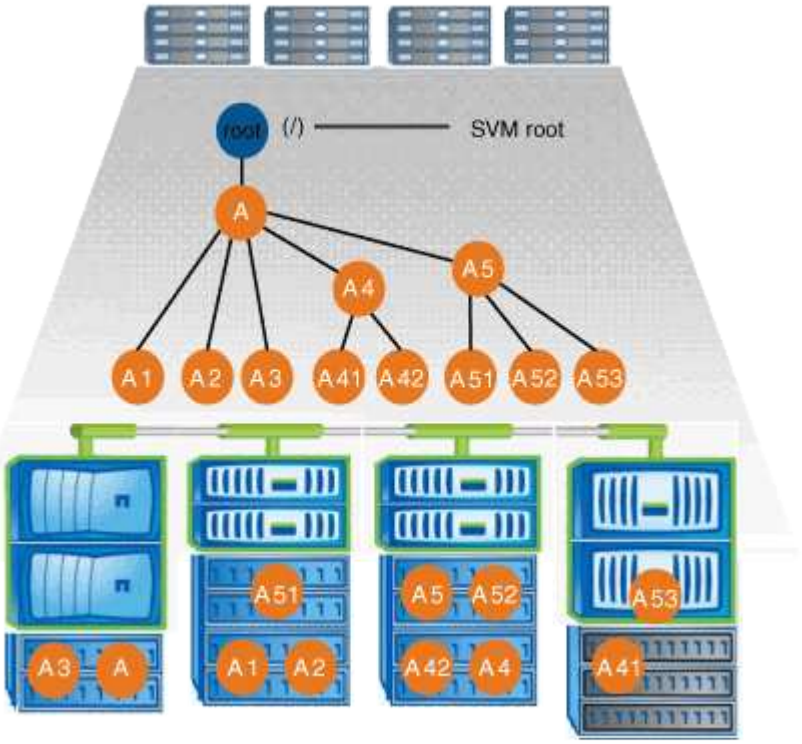
Le haut du namespace est toujours le volume root, représenté par une barre oblique (/). L'architecture d'espace de noms sous la racine se divise en trois catégories de base :

- Arbre branché unique, avec une seule jonction à la racine de l'espace de noms

- Plusieurs arborescences ramifiées, avec plusieurs points de jonction à la racine de l'espace de noms
- Plusieurs volumes autonomes, chacun avec un point de jonction séparé à la racine de l'espace de noms

Espace de noms avec une seule arborescence ramifiée

Une architecture avec une seule arborescence de branche possède un point d'insertion unique à la racine du namespace du SVM. Le point d'insertion unique peut être un volume relié par jonction ou un répertoire sous la racine. Tous les autres volumes sont montés aux points de jonction sous le point d'insertion unique (qui peut être un volume ou un répertoire).

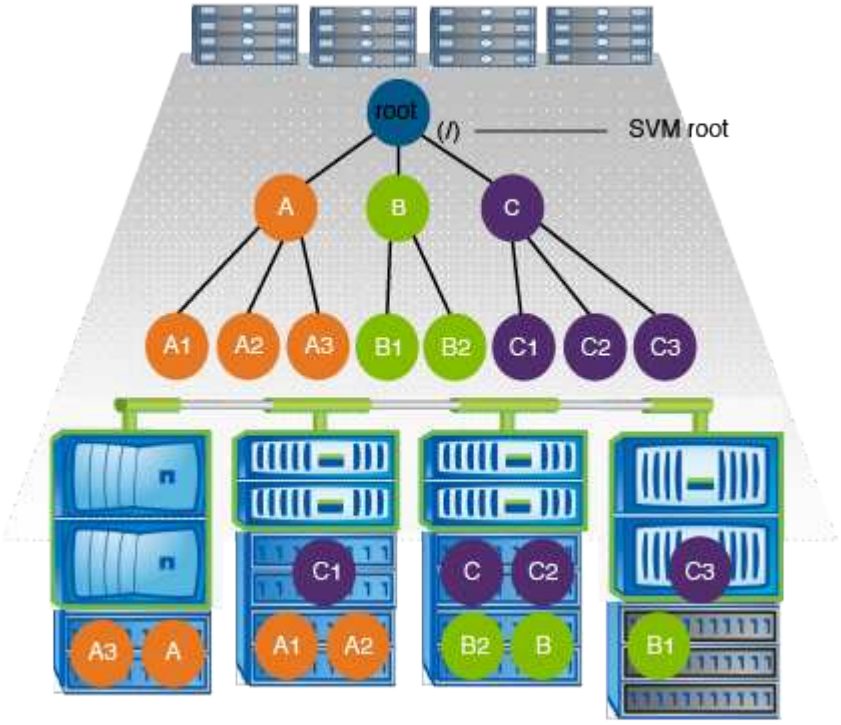


Par exemple, une configuration de jonction de volume typique avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où tous les volumes sont reliés sous le point d'insertion unique, qui est un répertoire nommé « `data' » :

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     corp1       true     /data/dir1/corp1       RW_volume
vs1     corp2       true     /data/dir1/corp2       RW_volume
vs1     data1       true     /data/data1            RW_volume
vs1     eng1        true     /data/data1/eng1       RW_volume
vs1     eng2        true     /data/data1/eng2       RW_volume
vs1     sales       true     /data/data1/sales      RW_volume
vs1     vol1        true     /data/vol1             RW_volume
vs1     vol2        true     /data/vol2             RW_volume
vs1     vol3        true     /data/vol3             RW_volume
vs1     vs1_root    -        /                      -
```

Espace de noms avec plusieurs arborescences ramifiées

Une architecture avec plusieurs arbres ramifiés a plusieurs points d'insertion à la racine du namespace du SVM. Les points d'insertion peuvent être des volumes ou des répertoires sous la racine. Tous les autres volumes sont montés aux points de jonction sous les points d'insertion (qui peuvent être des volumes ou des répertoires).

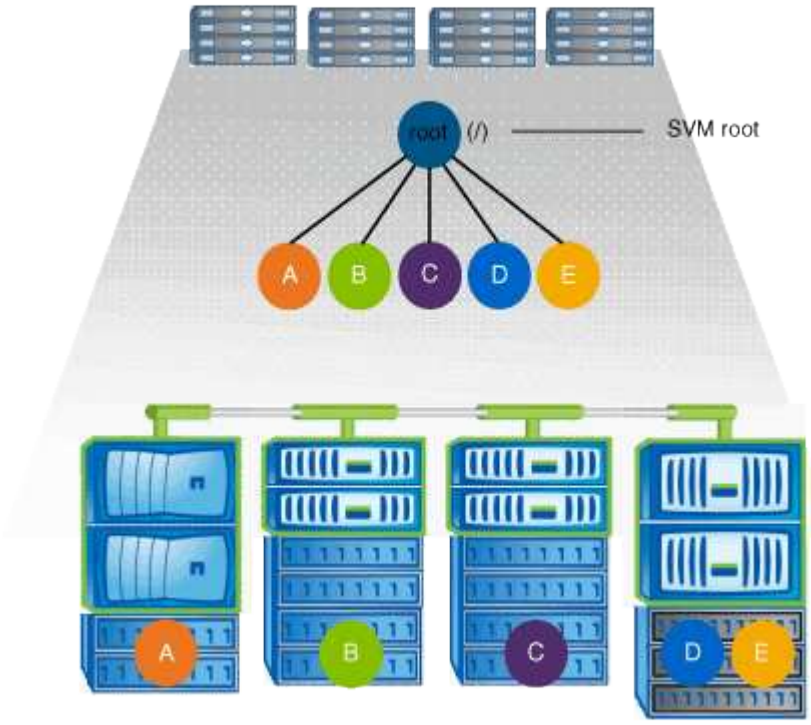


Par exemple, une configuration de jonction de volume standard avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où il existe trois points d'insertion pour le volume racine de la SVM. Deux points d'insertion sont des répertoires nommés "data" et "projets". Un point d'insertion est un volume relié par jonction nommé « audit » :

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     audit         true     /audit                   RW_volume
vs1     audit_logs1   true     /audit/logs1             RW_volume
vs1     audit_logs2   true     /audit/logs2             RW_volume
vs1     audit_logs3   true     /audit/logs3             RW_volume
vs1     eng           true     /data/eng                RW_volume
vs1     mktg1         true     /data/mktg1              RW_volume
vs1     mktg2         true     /data/mktg2              RW_volume
vs1     project1      true     /projects/project1       RW_volume
vs1     project2      true     /projects/project2       RW_volume
vs1     vs1_root      -        /                        -
```

Espace de noms avec plusieurs volumes autonomes

Dans une architecture avec des volumes autonomes, chaque volume a un point d'insertion à la racine de l'espace de noms SVM ; cependant, le volume n'est pas relié par jonction sous un autre volume. Chaque volume a un chemin unique, avec une jonction directe sous la racine ou sous un répertoire sous la racine.



Par exemple, une configuration de jonction de volume standard avec l'architecture de l'espace de noms ci-dessus peut ressembler à la configuration suivante, où il existe cinq points d'insertion pour le volume racine de la SVM, avec chaque point d'insertion représentant un chemin vers un volume.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

Comment ONTAP contrôle l'accès aux fichiers

En savoir plus sur le contrôle d'accès aux fichiers NAS ONTAP

ONTAP contrôle l'accès aux fichiers en fonction des restrictions basées sur l'authentification et les fichiers que vous avez spécifiées.

Lorsqu'un client se connecte au système de stockage pour accéder aux fichiers, ONTAP doit effectuer deux tâches :

- Authentification

  ONTAP doit authentifier le client en vérifiant l'identité avec une source de confiance. De plus, le type d'authentification du client est une méthode qui peut être utilisée pour déterminer si un client peut accéder aux données lors de la configuration des export policies (facultatif pour CIFS).

- Autorisation

  ONTAP doit autoriser l'utilisateur en comparant les informations d'identification de l'utilisateur avec les autorisations configurées sur le fichier ou le répertoire et en déterminant le type d'accès à fournir, le cas échéant.

Pour gérer correctement le contrôle d'accès aux fichiers, ONTAP doit communiquer avec des services externes tels que des serveurs NIS, LDAP et Active Directory. La configuration d'un système de stockage pour l'accès aux fichiers via CIFS ou NFS nécessite la configuration des services appropriés, en fonction de votre environnement dans ONTAP.

En savoir plus sur les restrictions basées sur l'authentification pour les SVM NAS ONTAP

En cas de restrictions basées sur l'authentification, vous pouvez spécifier les ordinateurs clients et les utilisateurs autorisés à se connecter à la machine virtuelle de stockage (SVM).

ONTAP prend en charge l'authentification Kerberos depuis des serveurs UNIX et Windows.

En savoir plus sur les restrictions basées sur les fichiers pour les SVM NAS ONTAP

ONTAP évalue trois niveaux de sécurité pour déterminer si une entité est autorisée à effectuer une action demandée sur les fichiers et répertoires résidant sur une SVM.

L’accès est déterminé par les autorisations effectives après évaluation des trois niveaux de sécurité.

Tout objet de stockage peut contenir jusqu’à trois types de couches de sécurité :

- Sécurité des exportations (NFS) et des partages (SMB)

  La sécurité des exportations et des partages s’applique à l’accès client à une exportation NFS ou à un partage SMB donné. Les utilisateurs disposant de privilèges d’administration peuvent gérer la sécurité au niveau de l’exportation et du partage à partir des clients SMB et NFS.

- Sécurité des fichiers et répertoires Access Guard du niveau de stockage

  La sécurité Access Guard du niveau de stockage s’applique aux accès des clients SMB et NFS pour les volumes SVM. Seules les autorisations d’accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d’accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l’utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

  > Si vous affichez les paramètres de sécurité d’un fichier ou d’un répertoire à partir d’un client NFS ou SMB, vous ne verrez pas la sécurité de Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d’un client, même par un administrateur système (Windows ou UNIX).

- Sécurité native au niveau des fichiers NTFS, UNIX et NFSv4

  La sécurité native au niveau du fichier existe sur le fichier ou le répertoire qui représente l’objet de stockage. Vous pouvez définir la sécurité au niveau des fichiers à partir d’un client. Les autorisations liées aux fichiers sont efficaces, que SMB ou NFS soit utilisé pour accéder aux données.

Comment ONTAP gère l’authentification client NFS

En savoir plus sur l’authentification ONTAP pour les clients NAS

Les clients NFS doivent être authentifiés correctement avant que leur système puisse accéder aux données sur la SVM. ONTAP authentifie les clients en comparant leurs informations d’identification UNIX aux services de nom que vous configurez.

Lorsqu’un client NFS se connecte au SVM, ONTAP obtient les identifiants UNIX pour l’utilisateur en cochant différents services de noms selon la configuration des services de noms du SVM. ONTAP peut vérifier les informations d’identification des comptes UNIX locaux, des domaines NIS et des domaines LDAP. Au moins l’un d’entre eux doit être configuré de manière à ce que ONTAP puisse authentifier l’utilisateur avec succès. Vous pouvez spécifier plusieurs services de noms et l’ordre dans lequel ONTAP les recherche.

Dans un environnement NFS pur avec des styles de sécurité de volume UNIX, cette configuration suffit à authentifier et à fournir l’accès approprié aux fichiers pour un utilisateur connecté à partir d’un client NFS.

Si vous utilisez des styles de sécurité de volumes mixtes, NTFS ou Unified, ONTAP doit obtenir un nom d’utilisateur SMB pour l’utilisateur UNIX pour l’authentification avec un contrôleur de domaine Windows. Cela peut se produire soit en mappant des utilisateurs individuels à l’aide de comptes UNIX locaux ou de domaines LDAP, soit en utilisant un utilisateur SMB par défaut. Vous pouvez spécifier le nom des services que ONTAP recherche dans l’ordre ou spécifier un utilisateur SMB par défaut.

Découvrez comment ONTAP utilise les services de noms

ONTAP utilise les services de noms pour obtenir des informations sur les utilisateurs et les clients. ONTAP utilise ces informations pour authentifier les utilisateurs qui accèdent aux données sur ou administrent le système de stockage, et mapper les identifiants des utilisateurs dans un environnement mixte.

Lorsque vous configurez le système de stockage, vous devez spécifier les services de nom que vous souhaitez que ONTAP utilise pour obtenir les identifiants utilisateur pour l'authentification. ONTAP prend en charge les noms suivants :

- Utilisateurs locaux (fichier)
- Domaines NIS externes (NIS)
- Domaines LDAP externes (LDAP)

Vous utilisez le `vserver services name-service ns-switch` Famille de commandes afin de configurer les SVM avec les sources pour rechercher les informations relatives au réseau et l'ordre dans lequel les rechercher. Ces commandes fournissent l'équivalent des fonctionnalités de `/etc/nsswitch.conf` Fichier sur les systèmes UNIX.

Lorsqu'un client NFS se connecte au SVM, ONTAP vérifie les services de nom spécifiés pour obtenir les informations d'identification UNIX pour l'utilisateur. Si les services de nom sont correctement configurés et que ONTAP peut obtenir les informations d'identification UNIX, ONTAP authentifie l'utilisateur avec succès.

Dans un environnement avec des styles de sécurité mixtes, ONTAP peut avoir à mapper les informations d'identification de l'utilisateur. Vous devez configurer les services de noms de manière appropriée pour votre environnement afin que ONTAP puisse correctement mapper les identifiants des utilisateurs.

ONTAP utilise également des services de noms pour l'authentification des comptes d'administrateur des SVM. Vous devez garder cela à l'esprit lors de la configuration ou de la modification du commutateur de service de nom afin d'éviter toute désactivation accidentelle de l'authentification pour les comptes d'administrateur SVM. Pour plus d'informations sur les utilisateurs d'administration des SVM, voir "Authentification de l'administrateur et RBAC".

Accorder l'accès aux fichiers SMB ONTAP à partir des clients NFS

ONTAP utilise la sémantique de sécurité du système de fichiers NTFS (Windows NT File System) pour déterminer si un utilisateur UNIX, sur un client NFS, a accès à un fichier avec des autorisations NTFS.

Pour ce faire, ONTAP convertit l'ID utilisateur UNIX (UID) de l'utilisateur en informations d'identification SMB, puis utilise les informations d'identification SMB pour vérifier que l'utilisateur dispose des droits d'accès au fichier. Un identifiant SMB se compose d'un identificateur de sécurité principal (SID), généralement le nom d'utilisateur Windows de l'utilisateur, et d'un ou plusieurs SID de groupe qui correspondent à des groupes Windows dont l'utilisateur est membre.

Le temps ONTAP nécessaire à la conversion de l'UID UNIX en identifiants SMB peut être de plusieurs dizaines de millisecondes à des centaines de millisecondes, car le processus implique de contacter un contrôleur de domaine. ONTAP mappe l'UID sur les identifiants SMB et entre le mappage dans un cache d'identifiants afin de réduire le temps de vérification provoqué par la conversion.

Comment fonctionne le cache d'informations d'identification NFS ONTAP

Lorsqu'un utilisateur NFS demande l'accès aux exports NFS sur le système de stockage, ONTAP doit récupérer les identifiants de l'utilisateur à partir de serveurs de noms externes ou de fichiers locaux afin de l'authentifier. ONTAP stocke ensuite ces informations d'identification dans un cache d'informations d'identification interne pour référence ultérieure. Il est donc essentiel de comprendre le fonctionnement des caches d'identifiants NFS pour gérer les problèmes de performance et d'accès qui peuvent survenir.

Sans le cache des informations d'identification, ONTAP devra interroger les services de noms chaque fois qu'un utilisateur NFS a demandé l'accès. Sur un système de stockage surchargé auquel de nombreux utilisateurs accèdent, cela peut rapidement entraîner des problèmes de performance graves, entraînant des retards non désirés ou même des dénis de l'accès client NFS.

Avec le cache des informations d'identification, ONTAP récupère les informations d'identification de l'utilisateur, puis les stocke pendant un délai prédéterminé pour un accès rapide et facile en cas d'envoi d'une autre demande par le client NFS. Cette méthode offre les avantages suivants :

- Il facilite la charge du système de stockage en gérant moins de requêtes vers des serveurs de noms externes (par exemple NIS ou LDAP).
- Il facilite la charge sur les serveurs de noms externes en leur envoyant moins de demandes.
- Il accélère l'accès des utilisateurs en éliminant le temps d'attente pour obtenir des informations d'identification de sources externes avant que l'utilisateur puisse être authentifié.

ONTAP stocke les informations d'identification positives et négatives dans le cache des informations d'identification. Des informations d'identification positives signifient que l'utilisateur a été authentifié et a accordé l'accès. Les identifiants négatifs signifient que l'utilisateur n'a pas été authentifié et a refusé l'accès.

Par défaut, ONTAP stocke des identifiants positifs pendant 24 heures. Ainsi, après l'authentification initiale d'un utilisateur, ONTAP utilise les identifiants mis en cache pour toutes les demandes d'accès de cet utilisateur pendant 24 heures. Si l'utilisateur demande l'accès après 24 heures, le cycle commence : ONTAP supprime les informations d'identification mises en cache et obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des 24 dernières heures, ONTAP met en cache les informations d'identification mises à jour pour les 24 prochaines heures.

Par défaut, ONTAP stocke les informations d'identification négatives pendant deux heures. Ainsi, après avoir initialement refusé l'accès à un utilisateur, ONTAP continue à refuser toute demande d'accès à cet utilisateur pendant deux heures. Si l'utilisateur demande l'accès au bout de 2 heures, le cycle commence : ONTAP obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des deux heures précédentes, ONTAP met en cache les informations d'identification mises à jour pour les deux heures suivantes.

Création et gestion des volumes de données dans les espaces de noms NAS

Créer des volumes NAS ONTAP avec des points de jonction spécifiés

Vous pouvez spécifier le point de jonction lorsque vous créez un volume de données. Le volume ainsi obtenu est automatiquement monté au point de jonction et est immédiatement disponible pour la configuration pour l'accès NAS.

Avant de commencer

- L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes avec les fonctions d'analyse de la capacité et de suivi des activités activées. Pour activer le suivi de capacité ou d'activité, exécutez la `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` définissez sur `on`.

  Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "Activez l'analyse du système de fichiers". Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

> Les caractères suivants ne peuvent pas être utilisés dans le chemin de jonction : `* # " > < | ? \`

De plus, la longueur du chemin de jonction ne peut pas dépasser 255 caractères.

Étapes

1. Créer le volume avec un point de jonction :

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

   Le chemin de jonction doit commencer par la racine (/) et peut contenir à la fois des répertoires et des volumes reliés. Il n'est pas nécessaire que la Junction path contienne le nom du volume. Les Junction paths sont indépendants du nom du volume.

   La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Cependant, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données que vous créez. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

   Le chemin de jonction n'est pas sensible à la casse ; `/ENG` est identique à `/eng`. Si vous créez un partage CIFS, Windows traite le chemin de jonction comme s'il est sensible à la casse. Par exemple, si la jonction est de `/ENG`, Le chemin d'un partage SMB doit commencer par `/ENG`pas `/eng`.

   De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

2. Vérifier que le volume a été créé avec le point de jonction souhaité :

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

Exemple

L'exemple suivant crée un volume nommé `home4` situé sur le SVM vs1 qui a une Junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Créer des volumes NAS ONTAP sans points de jonction spécifiques

Vous pouvez créer un volume de données sans spécifier de point de jonction. Le volume résultant n'est pas monté automatiquement et n'est pas disponible pour configurer l'accès NAS. Vous devez monter le volume avant de configurer les partages SMB ou les exportations NFS pour ce volume.

Avant de commencer

- L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes avec les fonctions d'analyse de la capacité et de suivi des activités activées. Pour activer le suivi de capacité ou d'activité, exécutez la `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` définissez sur `on`.

  Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "Activez l'analyse du système de fichiers". Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

Étapes

1. Créer le volume sans point de jonction en utilisant la commande suivante :

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Toutefois, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

   De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

2. Vérifier que le volume a été créé sans point de jonction :

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Exemple

L'exemple suivant crée un volume nommé « sales » situé sur la SVM vs1 qui n'est pas monté à un point de jonction :

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Monter ou démonter des volumes ONTAP NFS dans l'espace de noms NAS

Un volume doit être monté sur le namespace NAS avant de pouvoir configurer l'accès des clients NAS aux données contenues dans les volumes SVM (Storage Virtual machine). Vous pouvez monter un volume sur un point de jonction s'il n'est pas actuellement monté. Vous pouvez également démonter des volumes.

Description de la tâche

Si vous démontez et mettez un volume hors ligne, toutes les données du point de jonction, y compris les données des volumes dont les points de jonction se trouvent dans l'espace de noms du volume non monté, sont inaccessibles aux clients NAS.

> Pour interrompre l'accès client NAS à un volume, il ne suffit pas de démonter le volume. Vous devez mettre le volume hors ligne ou prendre d'autres mesures pour vous assurer que les caches de descripteur de fichier côté client sont invalidés. Pour plus d'informations, consultez l'article suivant de la base de connaissances :
>
> "Les clients NFSv3 ont toujours accès à un volume après avoir été supprimés du namespace dans ONTAP"

Lorsque vous démontez et mettez hors ligne un volume, les données ne sont pas perdues au sein du volume. En outre, les règles d'exportation de volume et les partages SMB créés sur le volume ou sur des répertoires et des points de jonction au sein du volume démonté sont conservés. Si vous remontez le volume démonté, les clients NAS peuvent accéder aux données contenues dans le volume à l'aide des règles d'exportation et des partages SMB existants.

Étapes

1. Effectuez l'action souhaitée :

Les fonctions que vous recherchez…	Entrez les commandes…
Montez un volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Démonter un volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Vérifiez que le volume est dans l'état de montage souhaité :

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Exemples

L'exemple suivant monte un volume nommé « ventes » situé sur la SVM « vs1 » au point de jonction « /ventes » :

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

L'exemple suivant démonte et met hors ligne un volume nommé « `data' situé sur le SVM « vs1` » :

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Affiche les informations sur le point de jonction et le montage du volume NAS ONTAP

Vous pouvez afficher des informations sur les volumes montés pour les SVM et les points de jonction auxquels les volumes sont montés. Vous pouvez également déterminer quels volumes ne sont pas montés sur un point de jonction. Vous pouvez utiliser ces informations pour comprendre et gérer votre namespace SVM.

Étape

1. Effectuez l'action souhaitée :

Si vous voulez afficher…	Entrez la commande…
Récapitulatif des informations sur les volumes montés et démontés sur le SVM	`volume show -vserver vserver_name -junction`
Informations détaillées sur les volumes montés et démontés sur le SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Informations spécifiques sur les volumes montés et démontés sur le SVM	a. Si nécessaire, vous pouvez afficher des champs valides pour l' `-fields` paramètre via la commande suivante : `volume show -fields ?` b. Afficher les informations souhaitées à l'aide de l' `-fields` paramètre : `volume show -vserver vserver_name -fields fieldname,…`

Exemples

L'exemple suivant affiche un récapitulatif des volumes montés et démontés sur le SVM vs1 :

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

L'exemple suivant affiche des informations sur les champs spécifiés pour les volumes situés sur le SVM vs2 :

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurer les styles de sécurité

Comment les styles de sécurité affectent l'accès aux données

En savoir plus sur les styles de sécurité NAS ONTAP

Il existe quatre styles de sécurité différents : UNIX, NTFS, mixte et unifié. Chaque style de sécurité a un effet différent sur la façon dont les autorisations sont traitées pour les données. Vous devez comprendre les différents effets pour vous assurer que vous sélectionnez le style de sécurité approprié à vos fins.

Il est important de comprendre que les styles de sécurité ne déterminent pas quels types de clients peuvent ou ne peuvent pas accéder aux données. Les styles de sécurité déterminent uniquement le type d'autorisations que ONTAP utilise pour contrôler l'accès aux données et le type de client pouvant modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu'ils s'authentifient et autorisent correctement) en raison de la nature multiprotocole de ONTAP. Toutefois, ONTAP utilise des autorisations UNIX que seuls les clients UNIX peuvent modifier à l'aide d'outils natifs.

Style de sécurité	Clients pouvant modifier des autorisations	Autorisations que les clients peuvent utiliser	Un style de sécurité efficace	Clients pouvant accéder aux fichiers
UNIX	NFS	Bits de mode NFSv3	UNIX	NFS et SMB
		Listes de contrôle d'accès NFSv4.x		
NTFS	PME	ALC NTFS	NTFS	
Mixte	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL.NFSv4		
		ALC NTFS	NTFS	
Unifiée (Pour Infinite volumes uniquement, dans ONTAP 9.4 et les versions antérieures.)	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL NFSv4.1		
		ALC NTFS	NTFS	

Les volumes FlexVol prennent en charge les styles de sécurité UNIX, NTFS et mixte. Lorsque le style de sécurité est mixte ou unifié, les autorisations effectives dépendent du type de client qui a modifié les autorisations pour la dernière fois, car les utilisateurs définissent le style de sécurité sur une base individuelle. Si le dernier client ayant modifié des autorisations était un client NFSv3, les autorisations sont des bits en mode UNIX NFSv3. Si le dernier client était un client NFSv4, les autorisations sont définies comme listes de contrôle d'accès NFSv4. Si le dernier client était un client SMB, les autorisations sont des listes de contrôle d'accès Windows NTFS.

La méthode de sécurité unifiée est uniquement disponible avec des volumes infinis, qui ne sont plus pris en charge dans ONTAP 9.5 et versions ultérieures. Pour plus d'informations, voir Présentation de la gestion des volumes FlexGroup.

Le `show-effective-permissions` paramètre avec le `vserver security file-directory` La commande vous permet d'afficher les autorisations effectives accordées à un utilisateur Windows ou UNIX sur le chemin de fichier ou de dossier spécifié. En outre, le paramètre facultatif `-share-name` vous permet d'afficher l'autorisation de partage effectif. Pour en savoir plus, `vserver security file-directory show-effective-permissions` consultez le "Référence de commande ONTAP".

ONTAP définit au départ certaines autorisations de fichier par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité UNIX, mixte et unifié est UNIX et le type d'autorisation effectif est bits de mode UNIX (0755 sauf indication contraire) jusqu'à ce qu'un client soit configuré comme autorisé par le style de sécurité par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité NTFS est NTFS et dispose d'une liste de contrôle d'accès permettant un contrôle total à tous.

Informations associées

- "Référence de commande ONTAP"

En savoir plus sur les styles de sécurité sur les volumes ONTAP NFS FlexVol

Les styles de sécurité peuvent être définis sur les volumes FlexVol (volumes root ou de données) et les qtrees. Les styles de sécurité peuvent être définis manuellement au moment de la création, hérités automatiquement ou modifiés ultérieurement.

Décidez quel style de sécurité utiliser sur les SVM NAS ONTAP

Pour vous aider à choisir le style de sécurité à utiliser sur un volume, vous devez tenir compte de deux facteurs. Le facteur principal est le type d'administrateur qui gère le système de fichiers. Le facteur secondaire désigne le type d'utilisateur ou de service qui accède aux données du volume.

Lorsque vous configurez le style de sécurité sur un volume, vous devez tenir compte des besoins de votre environnement pour vous assurer que vous sélectionnez le meilleur style de sécurité et éviter les problèmes liés à la gestion des autorisations. Vous pouvez décider des considérations suivantes :

Style de sécurité	Choisissez si…
UNIX	• Le système de fichiers est géré par un administrateur UNIX. • La plupart des utilisateurs sont des clients NFS. • Une application accédant aux données utilise un utilisateur UNIX comme compte de service.
NTFS	• Le système de fichiers est géré par un administrateur Windows. • La majorité des utilisateurs sont des clients SMB. • Une application accédant aux données utilise un utilisateur Windows comme compte de service.
Mixte	• Le système de fichiers est géré à la fois par les administrateurs et utilisateurs d'UNIX et de Windows, et il se compose de clients NFS et SMB.

En savoir plus sur l'héritage de style de sécurité NFS de ONTAP

Si vous ne spécifiez pas le style de sécurité lors de la création d'un nouveau volume FlexVol ou d'un qtree, il hérite de son style de sécurité de différentes manières.

Les styles de sécurité sont hérités de la manière suivante :

- Un volume FlexVol hérite du style de sécurité du volume root de son SVM contenant.
- Un qtree hérite du style de sécurité de son volume FlexVol.
- Un fichier ou un répertoire hérite du style de sécurité de son volume FlexVol ou qtree.

En savoir plus sur la préservation des autorisations ONTAP NFS UNIX

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

Gérer les autorisations UNIX sur les SVM ONTAP NFS à l'aide de l'onglet Sécurité Windows

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtrees de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- Modification des autorisations UNIX

  Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

  Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- Modification des autorisations UNIX en autorisations NTFS

  Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

  Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

  Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

Configurer les styles de sécurité sur les volumes racine ONTAP NFS SVM

Il configure la style de sécurité du volume root de la machine virtuelle de stockage (SVM) afin de déterminer le type d'autorisations utilisées pour les données sur le volume root de la SVM.

Étapes

1. Utilisez le `vserver create` commande avec `-rootvolume-security-style` paramètre pour définir le style de sécurité.

   Les options possibles pour le style de sécurité du volume racine sont `unix`, `ntfs`, ou `mixed`.

2. Afficher et vérifier la configuration, y compris le style de sécurité du volume root du SVM que vous avez créé :

   `vserver show -vserver` *`vserver_name`*

Configurer les styles de sécurité sur les volumes ONTAP NFS FlexVol

Configurez le style de sécurité des volumes FlexVol afin de déterminer le type d'autorisations utilisées pour les données sur des volumes FlexVol de la machine virtuelle de stockage (SVM).

Étapes

1. Effectuez l'une des opérations suivantes :

Si le volume FlexVol…	Utilisez la commande…
N'existe pas encore	`volume create` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.
Existe déjà	`volume modify` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.

   Les options possibles pour le style de sécurité du volume FlexVol sont `unix`, `ntfs`, ou `mixed`.

   Si vous ne spécifiez pas de style de sécurité lors de la création d'un volume FlexVol, le volume hérite du style de sécurité du volume racine.

   Pour plus d'informations sur le `volume create` ou `volume modify` commandes, voir "Gestion du stockage logique".

2. Pour afficher la configuration, en incluant le style de sécurité du volume FlexVol que vous avez créé, entrez la commande suivante :

   `volume show -volume volume_name -instance`

Configurer les styles de sécurité sur les qtrees ONTAP NFS

Vous configurez le style de sécurité du volume qtree afin de déterminer le type d'autorisations utilisées pour les données sur des qtrees.

Étapes

1. Effectuez l'une des opérations suivantes :

Si le qtree…	Utilisez la commande…
N'existe pas encore	`volume qtree create` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.
Existe déjà	`volume qtree modify` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.

Les options possibles pour la méthode de sécurité qtree sont `unix`, `ntfs`, ou `mixed`.

Si vous ne spécifiez pas de style de sécurité lors de la création d'un qtree, le style de sécurité par défaut est `mixed`.

Pour plus d'informations sur le `volume qtree create` ou `volume qtree modify` commandes, voir "Gestion du stockage logique".

2. Pour afficher la configuration, y compris le style de sécurité du qtree que vous avez créé, entrez la commande suivante : `volume qtree show -qtree` *`qtree_name`* `-instance`

Configurez l'accès aux fichiers à l'aide de NFS

En savoir plus sur la configuration de l'accès aux fichiers NFS sur les SVM ONTAP

Vous devez suivre un certain nombre d'étapes pour permettre aux clients d'accéder aux fichiers sur des SVM (Storage Virtual machine) à l'aide de NFS. Certaines étapes supplémentaires sont facultatives en fonction de la configuration actuelle de votre environnement.

Pour que les clients puissent accéder aux fichiers sur des SVM via NFS, vous devez effectuer les tâches suivantes :

1. Activer le protocole NFS sur le SVM.

   On doit configurer le SVM de façon à permettre l'accès aux données des clients sur NFS.

2. Créer un serveur NFS sur le SVM.

   Un serveur NFS est une entité logique du SVM qui permet à la SVM de transmettre des fichiers via NFS. Vous devez créer le serveur NFS et spécifier les versions de protocole NFS que vous souhaitez autoriser.

3. Configurer les export policy sur le SVM.

   Vous devez configurer des règles d'exportation pour que les volumes et les qtrees soient disponibles pour les clients.

4. Configurez le serveur NFS avec les paramètres de sécurité appropriés et d'autres paramètres en fonction du réseau et de l'environnement de stockage.

   Cette étape peut inclure la configuration de Kerberos, LDAP, NIS, mappages de noms et utilisateurs locaux.

Sécurisation de l’accès NFS à l’aide de règles d’exportation

Comment les politiques d’exportation contrôlent l’accès des clients aux volumes NFS ou qtrees ONTAP

Les règles d’exportation contiennent une ou plusieurs *export rules* qui traitent chaque demande d’accès client. Le résultat du processus détermine si le client est refusé ou accordé et quel niveau d’accès. Un export policy avec règles d’export doit exister sur la machine virtuelle de stockage (SVM) afin que les clients puissent accéder aux données.

Vous associez exactement une export policy à chaque volume ou qtree pour configurer l’accès client au volume ou qtree. Le SVM peut contenir plusieurs export policy. Vous pouvez ainsi effectuer les opérations suivantes pour les SVM avec plusieurs volumes ou qtrees :

- Assigner différentes export policy à chaque volume ou qtree du SVM pour le contrôle d’accès client individuel à chaque volume ou qtree du SVM.
- Assigner la même export policy à plusieurs volumes ou qtree du SVM pour un contrôle d’accès client identique sans avoir à créer une nouvelle export policy pour chaque volume ou qtree.

Si un client effectue une demande d’accès qui n’est pas autorisée par la stratégie d’exportation applicable, la requête échoue et un message d’autorisation est refusé. Si un client ne correspond à aucune règle de l’export policy, l’accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés.

Vous pouvez modifier une export-policy de manière dynamique sur un système exécutant ONTAP.

Stratégies d’exportation par défaut pour les SVM NFS ONTAP

Chaque SVM dispose d’une export policy par défaut qui ne contient aucune règle. Un export policy avec règles doit exister pour que les clients puissent accéder aux données sur la SVM. Chaque volume FlexVol contenu au SVM doit être associé à une export policy.

Lorsque vous créez un SVM, le système de stockage crée automatiquement une export policy par défaut appelée `default` Pour le volume root du SVM. On doit créer une ou plusieurs règles pour l’export policy par défaut avant que les clients puissent accéder aux données sur la SVM. Vous pouvez également créer une export-policy personnalisée avec des règles. Vous pouvez modifier et renommer l’export policy par défaut, mais vous ne pouvez pas supprimer l’export policy par défaut.

Lorsque vous créez un volume FlexVol dans son SVM contenant, le système de stockage crée le volume et associe le volume avec la export policy par défaut pour le volume root du SVM. Par défaut, chaque volume créé au sein du SVM est associé à l’export policy par défaut pour le volume root. Vous pouvez utiliser l’export policy par défaut pour tous les volumes contenus dans le SVM, ou bien créer une export policy unique pour chaque volume. Vous pouvez associer plusieurs volumes à la même export policy.

Comment fonctionnent les règles d’exportation NFS ONTAP

Les règles d’exportation sont les éléments fonctionnels d’une export-policy. Les règles d’exportation correspondent aux demandes d’accès client à un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment traiter les demandes d’accès client.

Une export-policy doit contenir au moins une règle d’exportation pour permettre l’accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l’ordre dans lequel elles apparaissent dans

l'export-policy. L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Vous pouvez configurer des règles d'exportation pour déterminer les autorisations d'accès client à l'aide des critères suivants :

- Protocole d'accès aux fichiers utilisé par le client envoyant la requête, par exemple, NFSv4 ou SMB.
- Identifiant client, par exemple, nom d'hôte ou adresse IP.

  La taille maximale du `-clientmatch` le champ est composé de 4096 caractères.

- Type de sécurité utilisé par le client pour l'authentification, par exemple Kerberos v5, NTLM ou AUTH_SYS.

Si une règle spécifie plusieurs critères, le client doit tous les correspondre pour que la règle s'applique.

> Depuis ONTAP 9.3, vous pouvez activer la vérification de la configuration des règles d'exportation en tant que tâche d'arrière-plan qui enregistre toutes les violations de règles dans une liste de règles d'erreur. Le `vserver export-policy config-checker` les commandes invoquent le vérificateur et affichent les résultats, que vous pouvez utiliser pour vérifier votre configuration et supprimer des règles erronées de la stratégie.
>
> Les commandes valident uniquement la configuration d'exportation pour les noms d'hôte, les groupes réseau et les utilisateurs anonymes.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée à l'aide du protocole NFSv3 et le client a l'adresse IP 10.1.17.37.

Bien que le protocole d'accès client corresponde, l'adresse IP du client se trouve dans un sous-réseau différent de celui spécifié dans la règle d'exportation. Par conséquent, la correspondance des clients échoue et cette règle ne s'applique pas à ce client.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée via le protocole NFSv4 et le client a l'adresse IP 10.1.16.54.

Le protocole d'accès client correspond et l'adresse IP du client se trouve dans le sous-réseau spécifié. Par conséquent, la correspondance du client a réussi et cette règle s'applique à ce client. Le client obtient un accès en lecture-écriture quel que soit son type de sécurité.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Par conséquent, les deux clients bénéficient d'un accès en lecture seule. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

Gérer l'accès ONTAP SVM pour les clients NFS avec des types de sécurité non répertoriés

Lorsqu'un client se présente avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès d'une règle d'exportation, vous pouvez soit refuser l'accès au client, soit le mapper à l'ID utilisateur anonyme à la place de l'aide de l'option `none` dans le paramètre d'accès.

Un client peut se présenter avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès car il a été authentifié avec un type de sécurité différent ou n'a pas été authentifié du tout (type de sécurité AUTH_NONE). Par défaut, l'accès au client est automatiquement refusé. Toutefois, vous pouvez ajouter l'option `none` au paramètre d'accès. Par conséquent, les clients dont le style de sécurité n'est pas répertorié sont mappés sur l'ID utilisateur anonyme. Le `-anon` Paramètre détermine quel ID utilisateur est attribué à ces clients. ID utilisateur spécifié pour le `-anon` le paramètre doit être un utilisateur valide configuré avec des autorisations appropriées pour l'utilisateur anonyme.

Valeurs valides pour le `-anon` plage de paramètres de `0` à `65535`.

ID utilisateur attribué à `-anon`	**Traitement des demandes d'accès client résultant**
`0 - 65533`	La demande d'accès client est mappée à l'ID utilisateur anonyme et obtient l'accès en fonction des autorisations configurées pour cet utilisateur.

ID utilisateur attribué à `-anon`	Traitement des demandes d'accès client résultant
`65534`	La demande d'accès client est mappée à l'utilisateur personne et obtient l'accès en fonction des autorisations configurées pour cet utilisateur. Il s'agit de la valeur par défaut.
`65535`	La demande d'accès de n'importe quel client est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec le type de sécurité AUTH_NONE. La demande d'accès des clients avec l'ID utilisateur 0 est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec tout autre type de sécurité.

Lorsque vous utilisez l'option `none`, il est important de se rappeler que le paramètre lecture seule est traité en premier. Lors de la configuration des règles d'exportation pour les clients dont les types de sécurité ne sont pas répertoriés, prenez en compte les consignes suivantes :

La lecture seule inclut `none`	Lecture-écriture incluse `none`	Accès résultant pour les clients avec des types de sécurité non répertoriés
Non	Non	Refusée
Non	Oui.	Refusé car la lecture seule est traitée en premier
Oui.	Non	Lecture seule comme anonyme
Oui.	Oui.	Lecture-écriture comme anonyme

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne

s’authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d’accès client et l’adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l’accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l’accès en lecture seule en tant qu’utilisateur anonyme avec l’ID utilisateur 70 aux clients authentifiés à l’aide de n’importe quel autre type de sécurité. Le paramètre lecture-écriture permet l’accès en lecture-écriture à n’importe quel type de sécurité, mais s’applique uniquement aux clients déjà filtrés par la règle en lecture seule.

Par conséquent, les clients n° 1 et n° 3 bénéficient de l’accès en lecture-écriture uniquement en tant qu’utilisateur anonyme avec l’ID utilisateur 70. Le client #2 obtient un accès en lecture-écriture avec son propre ID utilisateur.

Exemple

La export policy contient une règle d’exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

Le client #1 a l’adresse IP 10.1.16.207, envoie une demande d’accès à l’aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l’adresse IP 10.1.16.211, envoie une demande d’accès à l’aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le client #3 a l’adresse IP 10.1.16.234, envoie une demande d’accès à l’aide du protocole NFSv3 et ne s’authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d’accès client et l’adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l’accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l’accès en lecture seule en tant qu’utilisateur anonyme avec l’ID utilisateur 70 aux clients authentifiés à l’aide de n’importe quel autre type de sécurité. Le paramètre lecture-écriture permet l’accès en lecture-écriture uniquement en tant qu’utilisateur anonyme.

Par conséquent, les clients #1 et le client #3 obtiennent un accès en lecture-écriture uniquement en tant qu’utilisateur anonyme avec l’ID utilisateur 70. Le client #2 obtient un accès en lecture seule avec son propre ID utilisateur, mais il est refusé l’accès en lecture-écriture.

Comment les types de sécurité ONTAP déterminent les niveaux d’accès des clients NFS

Le type de sécurité auquel le client s’est authentifié joue un rôle particulier dans les règles d’exportation. Vous devez comprendre la manière dont le type de sécurité détermine les niveaux d’accès du client à un volume ou à un qtree.

Les trois niveaux d’accès possibles sont les suivants :

1. Lecture seule
2. Lecture-écriture

3. Super-utilisateur (pour les clients ayant l'ID utilisateur 0)

Dans la mesure où le niveau d'accès par type de sécurité est évalué dans cet ordre, vous devez respecter les règles suivantes lors de la construction de paramètres de niveau d'accès dans les règles d'exportation :

Pour qu'un client puisse obtenir le niveau d'accès…	**Ces paramètres d'accès doivent correspondre au type de sécurité du client…**
Lecture seule normale par l'utilisateur	Lecture seule (`-rorule`)
Lecture-écriture utilisateur normale	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`)
Super-utilisateur en lecture seule	Lecture seule (`-rorule`) et `-superuser`
Super-utilisateur lecture-écriture	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`) et `-superuser`

Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

- `any`
- `none`
- `never`

  Ce type de sécurité n'est pas valide pour une utilisation avec `-superuser` paramètre.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Lorsque vous faites correspondre le type de sécurité d'un client à chacun des trois paramètres d'accès, trois résultats sont possibles :

Si le type de sécurité du client…	**Ensuite, le client…**
Correspond à celui spécifié dans le paramètre d'accès.	Obtient l'accès à ce niveau avec son propre ID utilisateur.
Ne correspond pas à celui spécifié, mais le paramètre d'accès inclut l'option `none`.	Obtient l'accès pour ce niveau, mais en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre.

Si le type de sécurité du client…	Ensuite, le client…
Ne correspond pas à celui spécifié et le paramètre d'accès n'inclut pas l'option `none`.	Ne dispose d'aucun accès pour ce niveau.cela ne s'applique pas à l' `-superuser` paramètre car il inclut toujours `none` même si elle n'est pas spécifiée.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et n'a pas authentifié (AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent aux trois clients. Le paramètre lecture seule permet un accès en lecture seule à tous les clients, quel que soit leur type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture aux clients avec leur propre ID utilisateur authentifié par AUTH_SYS ou Kerberos v5. Le paramètre superuser permet un accès superuser aux clients avec l'ID utilisateur 0 authentifié avec Kerberos v5.

Par conséquent, le client #1 obtient l'accès en lecture-écriture superutilisateur car il correspond aux trois paramètres d'accès. Le client #2 obtient un accès en lecture-écriture mais pas un accès super-utilisateur. Le client #3 obtient un accès en lecture seule mais pas un accès super-utilisateur.

En savoir plus sur la gestion des demandes d'accès superutilisateur ONTAP NFS

Lorsque vous configurez des stratégies d'exportation, vous devez tenir compte de ce que vous voulez faire si le système de stockage reçoit une demande d'accès client avec l'ID utilisateur 0, c'est-à-dire en tant que superutilisateur, et définir vos règles d'exportation en conséquence.

Dans le monde UNIX, un utilisateur avec l'ID utilisateur 0 est appelé superutilisateur, généralement appelé root, qui dispose de droits d'accès illimités sur un système. L'utilisation des privilèges de superutilisateur peut être dangereuse pour plusieurs raisons, y compris une violation du système et de la sécurité des données.

Par défaut, ONTAP mappe les clients présentant l'ID utilisateur 0 à l'utilisateur anonyme. Toutefois, vous pouvez spécifier le `-superuser` Paramètre dans les règles d'exportation pour déterminer comment gérer les clients présentant l'ID utilisateur 0 en fonction de leur type de sécurité. Les options suivantes sont valides pour le `-superuser` paramètre :

- any
- none

  Il s'agit du paramètre par défaut si vous ne spécifiez pas le -superuser paramètre.

- krb5
- ntlm
- sys

Il existe deux façons différentes de gérer les clients présentant l'ID utilisateur 0, selon le -superuser configuration des paramètres :

Si le -superuser et le type de sécurité du client…	Ensuite, le client…
Correspondance	Obtient l'accès superutilisateur avec l'ID utilisateur 0.
Ne correspondent pas	Obtient l'accès en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le -anon paramètre et ses autorisations attribuées. Cette option est précise si le paramètre lecture seule ou lecture-écriture spécifie l'option none.

Si un client se présente avec l'ID utilisateur 0 pour accéder à un volume avec le style de sécurité NTFS et le -superuser le paramètre est défini sur none, ONTAP utilise le mappage de noms pour l'utilisateur anonyme afin d'obtenir les informations d'identification appropriées.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule krb5,ntlm
- -anon 127

Le client n° 1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 746, envoie une demande d'accès à l'aide du protocole NFSv3 et s'authentifie avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier.

Le client #2 ne dispose pas d'un accès super-utilisateur. Au lieu de cela, il est mappé sur anonyme car le -superuser paramètre non spécifié. Cela signifie que la valeur par défaut est none Et mappe

automatiquement l'ID utilisateur 0 sur anonyme. Le client #2 obtient également un accès en lecture seule car son type de sécurité ne correspond pas au paramètre lecture-écriture.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

La règle d'exportation permet l'accès superutilisateur pour les clients avec l'ID utilisateur 0. Le client #1 obtient l'accès superutilisateur car il correspond à l'ID utilisateur et au type de sécurité pour la lecture seule et `-superuser` paramètres. Le client #2 ne dispose pas d'un accès en lecture-écriture ou super-utilisateur, car son type de sécurité ne correspond pas au paramètre en lecture-écriture ou au `-superuser` paramètre. Au lieu de cela, le client #2 est mappé à l'utilisateur anonyme, qui a dans ce cas l'ID utilisateur 0.

En savoir plus sur les caches de stratégie d'exportation NFS ONTAP

Pour améliorer les performances système, ONTAP utilise des caches locaux pour stocker des informations telles que les noms d'hôtes et les groupes de réseaux. Cela permet à ONTAP de traiter les règles des export-policy plus rapidement que de récupérer les informations à partir de sources externes. Comprendre ce qu'sont les caches et ce qu'ils font pour vous aider à résoudre les problèmes d'accès client.

Vous configurez les export policy pour contrôler l'accès client aux exports NFS. Chaque export policy contient des règles, et chaque règle contient des paramètres qui correspondent à la règle avec les clients demandant un accès. Certains de ces paramètres exigent que ONTAP contacte une source externe, telle que des serveurs DNS ou NIS, pour résoudre des objets tels que des noms de domaine, des noms d'hôtes ou des groupes réseau.

Ces communications avec des sources externes prennent peu de temps. Afin d'améliorer les performances, ONTAP réduit le temps nécessaire à la résolution des objets de règles d'exportation en stockant les informations localement sur chaque nœud dans plusieurs caches.

Nom du cache	Type d'information stockée
L'accès	Mise en correspondance des clients avec les règles d'exportation correspondantes
Nom	Mappage des noms d'utilisateur UNIX avec les ID utilisateur UNIX correspondants
ID	Mappage des ID utilisateur UNIX avec les ID utilisateur UNIX correspondants et les ID de groupe UNIX étendus
Hôte	Mappages de noms d'hôtes sur les adresses IP correspondantes
Groupe réseau	Mappages de groupes réseau aux adresses IP correspondantes des membres
Showmount	Liste des répertoires exportés depuis le namespace du SVM

Si vous modifiez les informations sur les serveurs de noms externes de votre environnement après la récupération et le stockage en local par ONTAP, les caches peuvent désormais contenir des informations obsolètes. Bien que les mises à jour ONTAP se placent automatiquement après certaines périodes, différents caches ont des temps d'expiration et d'actualisation et des algorithmes différents.

Une autre raison possible pour que les caches contiennent des informations obsolètes est le moment où ONTAP tente d'actualiser les informations en cache mais rencontre un échec lors de tentatives de communication avec des serveurs de noms. Dans ce cas, ONTAP continue d'utiliser les informations actuellement stockées dans les caches locaux pour éviter toute perturbation du client.

Par conséquent, les demandes d'accès des clients qui sont censées réussir risquent d'échouer et les demandes d'accès des clients qui sont censées échouer pourraient réussir. Vous pouvez afficher et vider manuellement certains caches de règles d'exportation lors du dépannage de tels problèmes d'accès client.

En savoir plus sur les caches d'accès NFS ONTAP

ONTAP utilise un cache d'accès pour stocker les résultats de l'évaluation de la règle d'export policy pour les opérations d'accès client à un volume ou à un qtree. Il en résulte une amélioration des performances, car les informations peuvent être récupérées beaucoup plus rapidement depuis le cache d'accès qu'un processus d'évaluation des règles d'export-policy à chaque fois qu'un client envoie une requête d'E/S.

Lorsqu'un client NFS envoie une requête d'E/S pour accéder aux données d'un volume ou qtree, ONTAP doit évaluer chaque demande d'E/S afin de déterminer s'il faut accorder ou refuser la demande d'E/S. Cette évaluation implique de vérifier chaque règle d'export policy de la export policy associée au volume ou à qtree. Si le chemin vers le volume ou qtree implique de franchir un ou plusieurs points de jonction, cette vérification peut s'avérer nécessaire pour rechercher plusieurs règles d'exportation le long du chemin.

Notez que cette évaluation est effectuée pour chaque demande d'E/S envoyée depuis un client NFS, par exemple pour la lecture, l'écriture, la liste, la copie et d'autres opérations. Il ne s'agit pas uniquement de

demandes de montage initiales.

Une fois que ONTAP a identifié les règles d'export policy applicables et a décidé d'autoriser ou de refuser la requête, ONTAP crée ensuite une entrée dans le cache d'accès pour stocker ces informations.

Lorsqu'un client NFS envoie une requête d'E/S, ONTAP note l'adresse IP du client, l'ID de la SVM et la export policy associée au volume cible ou au qtree, et recherche d'abord une entrée correspondante dans le cache d'accès. S'il existe une entrée correspondante dans le cache d'accès, ONTAP utilise les informations stockées pour autoriser ou refuser la demande d'E/S. Si aucune entrée correspondante n'existe, ONTAP passe par le processus normal d'évaluation de toutes les règles de politique applicables, comme expliqué ci-dessus.

Les entrées du cache d'accès qui ne sont pas utilisées activement ne sont pas actualisées. Cela permet de réduire les communications inutiles et inutiles avec des services de noms externes.

La récupération des informations à partir du cache d'accès est bien plus rapide qu'au cours de l'intégralité du processus d'évaluation des règles des règles d'export-policy pour chaque demande d'E/S. Par conséquent, l'utilisation du cache d'accès améliore nettement les performances en réduisant la surcharge liée aux vérifications d'accès client.

En savoir plus sur les paramètres du cache d'accès NFS ONTAP

Plusieurs paramètres contrôlent les périodes d'actualisation des entrées dans le cache d'accès. Le fonctionnement de ces paramètres vous permet de les modifier pour régler le cache d'accès et équilibrer les performances avec la récente information stockée.

Le cache d'accès stocke des entrées composées d'une ou plusieurs règles d'exportation qui s'appliquent aux clients qui essaient d'accéder aux volumes ou aux qtrees. Ces entrées sont stockées pendant un certain temps avant leur actualisation. La durée d'actualisation est déterminée par les paramètres du cache d'accès et dépend du type d'entrée du cache d'accès.

Vous pouvez spécifier les paramètres du cache d'accès pour chaque SVM. Cela permet aux paramètres de différer en fonction des exigences d'accès des SVM. Les entrées de cache d'accès qui ne sont pas utilisées activement ne sont pas réactualisées, ce qui réduit les communications inutiles et inutiles avec le nom externe sert.

Accès au type d'entrée du cache	Description	Période d'actualisation en secondes
Entrées positives	Les entrées du cache d'accès qui n'ont pas entraîné de refus d'accès aux clients.	Minimum: 300 Maximum : 86,400 Valeur par défaut : 3,600
Entrées négatives	Les entrées du cache d'accès qui ont entraîné un refus d'accès aux clients.	Minimum : 60 Maximum : 86,400 Valeur par défaut : 3,600

Exemple

Un client NFS tente d'accéder à un volume sur un cluster. ONTAP mappe le client sur une règle export policy et détermine que le client accède à cette règle en fonction de la configuration de la règle export policy. ONTAP

stocke la règle d'export policy dans le cache d'accès sous forme d'entrée positive. Par défaut, ONTAP conserve l'entrée positive dans le cache d'accès pendant une heure (3,600 secondes), puis actualise automatiquement l'entrée pour maintenir les informations à jour.

Pour éviter que le cache d'accès ne se remplit inutilement, il existe un paramètre supplémentaire pour effacer les entrées existantes du cache d'accès qui n'ont pas été utilisées pendant une certaine période pour décider de l'accès client. C'est ça `-harvest-timeout` le paramètre a une plage autorisée de 60 à 2,592,000 secondes et un réglage par défaut de 86,400 secondes.

Supprimer les politiques d'exportation des qtrees ONTAP NFS

Si vous décidez de ne plus vouloir attribuer une export policy spécifique à un qtree, vous pouvez supprimer la export policy en modifiant le qtree de manière à hériter de la export policy du volume contenant. Pour ce faire, utilisez le `volume qtree modify` commande avec `-export-policy` paramètre et chaîne de nom vide ("").

Étapes

1. Pour supprimer une export policy d'un qtree, entrez la commande suivante :

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Vérifier que le qtree a été modifié en conséquence :

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Valider les identifiants qtree ONTAP NFS pour les opérations de fichiers qtree

ONTAP peut procéder à une validation supplémentaire facultative des ID de qtree. Cette validation garantit que les demandes d'opérations de fichiers client utilisent un ID qtree valide et que les clients ne peuvent déplacer que les fichiers au sein du même qtree. Vous pouvez activer ou désactiver cette validation en modifiant le `-validate-qtree -export` paramètre. Ce paramètre est activé par défaut.

Description de la tâche

Ce paramètre n'est efficace que lorsque vous avez attribué une export policy directement à un ou plusieurs qtrees sur la machine virtuelle de stockage (SVM).

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Pour que la validation de l'ID qtree soit…	Saisissez la commande suivante…
Activé	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`

Pour que la validation de l'ID qtree soit…	Saisissez la commande suivante…
Désactivé	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Restrictions de politique d'exportation et jonctions imbriquées pour les volumes ONTAP NFS FlexVol

Si vous avez configuré des stratégies d'exportation pour définir une stratégie moins restrictive sur une jonction imbriquée mais une règle plus restrictive sur une jonction de niveau supérieur, l'accès à la jonction de niveau inférieur peut échouer.

Vous devez vous assurer que les jonctions de niveau supérieur disposent de règles d'exportation moins restrictives que les jonctions de niveau inférieur.

Utilisation de Kerberos avec NFS pour une sécurité renforcée

Prise en charge ONTAP NFS pour Kerberos

Kerberos fournit une authentification sécurisée renforcée pour les applications client/Server. L'authentification permet de vérifier les identités des utilisateurs et des processus à un serveur. Dans l'environnement ONTAP, Kerberos assure une authentification entre les SVM (Storage Virtual machine) et les clients NFS.

Dans ONTAP 9, les fonctionnalités Kerberos suivantes sont prises en charge :

- Authentification Kerberos 5 avec contrôle d'intégrité (krb5i)

  Krb5i utilise des checksums pour vérifier l'intégrité de chaque message NFS transféré entre le client et le serveur. Cette fonction est utile pour des raisons de sécurité (par exemple pour s'assurer que les données n'ont pas été falsifiées) et pour des raisons d'intégrité des données (par exemple, pour empêcher la corruption des données lors de l'utilisation de NFS sur des réseaux non fiables).

- Authentification Kerberos 5 avec vérification de la confidentialité (krb5p)

  Krb5p utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. Ceci est plus sûr et entraîne également plus de charge.

- Chiffrement AES 128 bits et 256 bits

  Advanced Encryption Standard (AES) est un algorithme de cryptage permettant de sécuriser les données électroniques. ONTAP prend en charge AES avec des clés 128 bits (AES-128) et AES avec des clés 256 bits (AES-256) pour Kerberos pour une sécurité renforcée.

- Les configurations de Royaume Kerberos au niveau du SVM

  Les administrateurs des SVM peuvent désormais créer des configurations de domaine Kerberos au niveau du SVM. Les administrateurs des SVM n'ont plus besoin de se reposer sur l'administrateur du cluster pour

la configuration des royaumes Kerberos. Ils peuvent donc créer des configurations de Royaume Kerberos individuelles dans un environnement mutualisé.

Conditions requises pour la configuration de Kerberos avec ONTAP NFS

Avant de configurer Kerberos avec NFS sur votre système, vous devez vérifier que certains éléments de votre réseau et de votre environnement de stockage sont correctement configurés.

> Les étapes de configuration de votre environnement dépendent de la version et du type du système d'exploitation client, du contrôleur de domaine, de Kerberos, DNS, etc. Que vous utilisez. La documentation de toutes ces variables dépasse le cadre de ce document. Pour plus d'informations, reportez-vous à la documentation correspondante pour chaque composant.
>
> Pour obtenir un exemple détaillé de la configuration de ONTAP et de Kerberos 5 avec NFSv3 et NFSv4 dans un environnement utilisant des hôtes Windows Server 2008 R2 Active Directory et Linux, consultez le rapport technique 4073.

Les éléments suivants doivent d'abord être configurés :

Conditions requises pour l'environnement réseau

- Kerberos

  Vous devez avoir une configuration Kerberos fonctionnant avec un centre de distribution de clés (KDC), tel que Windows Active Directory Based Kerberos ou MIT Kerberos.

  Les serveurs NFS doivent utiliser `nfs` en tant que composant principal de leur machine principale.

- Service d'annuaire

  Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS.

- NTP

  Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

  Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

- Comptes d'utilisateur

  Chaque client doit disposer d'un compte utilisateur dans le domaine Kerberos. Les serveurs NFS doivent utiliser « nfs » comme composant principal de leur machine principale.

Exigences du client NFS

- NFS

Chaque client doit être correctement configuré pour communiquer sur le réseau en utilisant NFSv3 ou NFSv4.

Les clients doivent prendre en charge les RFC1964 et RFC2203.

- Kerberos

  Chaque client doit être correctement configuré pour utiliser l'authentification Kerberos, avec les informations suivantes :

  - Le chiffrement pour les communications TGS est activé.

    AES-256 pour une sécurité optimale.

  - Le type de cryptage le plus sécurisé pour les communications TGT est activé.
  - Le domaine et le domaine Kerberos sont configurés correctement.
  - GSS est activé.

    Lors de l'utilisation des informations d'identification de la machine

  - Ne pas exécuter `gssd` avec le `-n` paramètre.
  - Ne pas exécuter `kinit` en tant qu'utilisateur root.
- Chaque client doit utiliser la version la plus récente et la plus récente du système d'exploitation.

  Cela offre la meilleure compatibilité et fiabilité pour le chiffrement AES avec Kerberos.

- DNS

  Chaque client doit être correctement configuré pour utiliser DNS pour la résolution correcte du nom.

- NTP

  Chaque client doit être en cours de synchronisation avec le serveur NTP.

- Informations sur l'hôte et le domaine

  Chaque client `/etc/hosts` et `/etc/resolv.conf` Les fichiers doivent contenir le nom d'hôte et les informations DNS correctes, respectivement.

- Fichiers keytab

  Chaque client doit avoir un fichier keytab du KDC. Le Royaume doit être en majuscules. Le type de chiffrement doit être AES-256 pour une sécurité optimale.

- Facultatif : pour des performances optimales, les clients bénéficient d'au moins deux interfaces réseau : l'une pour communiquer avec le réseau local et l'autre pour communiquer avec le réseau de stockage.

Configuration requise pour le système de stockage

- Licence NFS

  Une licence NFS valide doit être installée sur le système de stockage.

- Licence CIFS

  La licence CIFS est facultative. Il n'est nécessaire de vérifier les informations d'identification Windows que lors de l'utilisation du mappage de noms multiprotocole. Elle n'est pas requise dans un environnement UNIX strict.

- SVM

  Au moins un SVM doit être configuré sur le système.

- DNS sur le SVM

  On doit avoir configuré DNS sur chaque SVM.

- Serveur NFS

  Vous devez avoir configuré NFS sur le SVM.

- Cryptage AES

  Pour une sécurité optimale, vous devez configurer le serveur NFS de sorte qu'il n'autorise que le chiffrement AES-256 pour Kerberos.

- Serveur SMB

  Si vous exécutez un environnement multiprotocole, vous devez avoir configuré SMB sur le SVM. Le serveur SMB est requis pour le mappage de noms multiprotocole.

- Volumes

  On doit disposer d'un volume root et d'au moins un volume de données configuré pour une utilisation par la SVM.

- Volume racine

  Le volume root du SVM doit avoir la configuration suivante :

Nom	Réglage
Style de sécurité	UNIX
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	776

  Contrairement au volume racine, les volumes de données peuvent avoir n'importe quel style de sécurité.

- Groupes UNIX

  La SVM doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0
pcuser	65534 (créé automatiquement par ONTAP lors de la création du SVM)

- Utilisateurs UNIX

  Le SVM doit avoir les utilisateurs UNIX suivants configurés :

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
nfs	500	0	Requis pour la phase INITIALE GSS Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur.
pcuser	65534	65534	Obligatoire pour une utilisation multiprotocole NFS et CIFS Créé et ajouté au groupe pcuser automatiquement par ONTAP lors de la création de la SVM.
racine	0	0	Nécessaire pour le montage

  L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.

- Export-policies et rules

  Vous devez avoir configuré des export policy avec les règles d'exportation nécessaires pour les volumes root et de données et les qtrees. Si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5` , `krb5i`, ou `krb5p`.

- Mapping de noms Kerberos-UNIX

  Si vous souhaitez que l'utilisateur identifié par l'utilisateur client NFS SPN dispose d'autorisations root, vous devez créer un mappage de nom à la racine.

Informations associées

"Rapport technique NetApp 4073 : authentification unifiée sécurisée"

"Matrice d'interopérabilité NetApp"

"Administration du système"

"Gestion du stockage logique"

Spécifiez le domaine d'ID utilisateur ONTAP pour NFSv4

Pour spécifier le domaine d'ID utilisateur, vous pouvez définir le `-v4-id-domain` option.

Description de la tâche

Par défaut, ONTAP utilise le domaine NIS pour le mappage d'ID utilisateur NFSv4, si un est défini. Si aucun domaine NIS n'est défini, le domaine DNS est utilisé. Vous devrez peut-être définir le domaine d'ID utilisateur si, par exemple, vous disposez de plusieurs domaines d'ID utilisateur. Le nom de domaine doit correspondre à la configuration de domaine sur le contrôleur de domaine. Elle n'est pas requise pour NFSv3.

Étape

1. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Configurer NAME-services

En savoir plus sur la configuration des commutateurs du service de nom NFS de ONTAP

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX. Vous devez connaître les fonctions du tableau et savoir comment ONTAP l'utilise pour que vous puissiez le configurer de façon appropriée pour votre environnement.

La table commutateur de service de nom ONTAP détermine les sources de service de nom auxquelles ONTAP consulte afin de récupérer les informations relatives à un certain type d'informations de service de nom. ONTAP conserve une table de commutateur de service de noms distincte pour chaque SVM.

Types de base de données

La table stocke une liste de services de noms distincte pour chacun des types de bases de données suivants :

Type de base de données	Définit les sources de service de noms pour…	Les sources valides sont…
hôtes	Conversion des noms d'hôte en adresses IP	fichiers, dns
groupe	Recherche des informations sur les groupes d'utilisateurs	fichiers, nis, ldap
passwd	Recherche des informations utilisateur	fichiers, nis, ldap

Type de base de données	Définit les sources de service de noms pour…	Les sources valides sont…
groupe réseau	Recherche des informations de groupe réseau	fichiers, nis, ldap
carte de nom	Mappage des noms d'utilisateur	fichiers, ldap

Types de source

Les sources indiquent quelle source de service de nom utiliser pour récupérer les informations appropriées.

Spécifiez le type de source…	Pour rechercher des informations dans…	Géré par les familles de commande…

fichiers	Fichiers source locaux	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Serveurs NIS externes tels que spécifiés dans la configuration de domaine NIS du SVM	`vserver services name-service nis-domain`
ldap	Serveurs LDAP externes comme spécifié dans la configuration du client LDAP du SVM	`vserver services name-service ldap`
dns	Serveurs DNS externes comme spécifié dans la configuration DNS du SVM	`vserver services name-service dns`

Même si vous prévoyez d'utiliser NIS ou LDAP pour l'accès aux données et l'authentification d'administration des SVM, vous devez toujours inclure `files` Et configurer des utilisateurs locaux comme un repli en cas d'échec de l'authentification NIS ou LDAP.

Protocoles utilisés pour accéder à des sources externes

Pour accéder aux serveurs pour des sources externes, ONTAP utilise les protocoles suivants :

Source de service de nom externe	Protocole utilisé pour l'accès
NIS	UDP

Source de service de nom externe	Protocole utilisé pour l'accès
DNS	UDP
LDAP	TCP

Exemple

L'exemple suivant montre la configuration du switch de service de nom pour le SVM svm svm_1 :

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Pour rechercher les adresses IP des hôtes, ONTAP consulte d'abord les fichiers source locaux. Si la requête ne renvoie aucun résultat, les serveurs DNS sont vérifiés ensuite.

Pour rechercher des informations sur les utilisateurs ou les groupes, ONTAP consulte uniquement les fichiers sources locales. Si la requête ne renvoie aucun résultat, la recherche échoue.

Pour rechercher des informations sur le groupe réseau, ONTAP consulte d'abord les serveurs NIS externes. Si la requête ne renvoie aucun résultat, le fichier netgroup local est coché ensuite.

Il n'y a pas d'entrées de nom de service pour le mappage de noms dans le tableau pour le SVM svm_1. Par conséquent, ONTAP consulte uniquement les fichiers source locaux par défaut.

Informations associées

"Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

Utiliser LDAP

En savoir plus sur LDAP pour les SVM NFS ONTAP

Un serveur LDAP (Lightweight Directory Access Protocol) vous permet de gérer de manière centralisée les informations utilisateur. Si vous stockez votre base de données utilisateur sur un serveur LDAP dans votre environnement, vous pouvez configurer votre système de stockage pour rechercher les informations utilisateur dans votre base de données LDAP existante.

- Avant de configurer LDAP pour ONTAP, vérifiez que votre déploiement de site respecte les bonnes pratiques en matière de configuration de serveur LDAP et de client. En particulier, les conditions suivantes

doivent être remplies :

- Le nom de domaine du serveur LDAP doit correspondre à l'entrée du client LDAP.
- Les types de hachage de mot de passe utilisateur LDAP pris en charge par le serveur LDAP doivent inclure ceux pris en charge par ONTAP :
  - CRYPT (tous types) et SHA-1 (SHA, SSHA).
  - Depuis ONTAP 9.8, des hachages SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 et SSHA-512) sont également pris en charge.
- Si le serveur LDAP nécessite des mesures de sécurité de session, vous devez les configurer dans le client LDAP.

  Les options de sécurité de session suivantes sont disponibles :

  - La signature LDAP (fournit un contrôle de l'intégrité des données), la signature et le chiffrement LDAP (assure le contrôle de l'intégrité des données et le chiffrement)
  - DÉMARRER TLS
  - LDAPS (LDAP sur TLS ou SSL)
- Pour activer les requêtes LDAP signées et scellées, les services suivants doivent être configurés :
  - Les serveurs LDAP doivent prendre en charge le mécanisme GSSAPI (Kerberos) SASL.
  - Les serveurs LDAP doivent avoir des enregistrements DNS A/AAAA ainsi que des enregistrements PTR configurés sur le serveur DNS.
  - Les serveurs Kerberos doivent contenir des enregistrements SRV sur le serveur DNS.
- Pour activer START TLS ou LDAPS, les points suivants doivent être pris en compte.
  - Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.
  - Si LDAPS est utilisé, le serveur LDAP doit être activé pour TLS ou pour SSL dans ONTAP 9.5 et versions ultérieures. SSL n'est pas pris en charge dans ONTAP 9.0-9.4.
  - Un serveur de certificats doit déjà être configuré dans le domaine.
- Pour activer la recherche de recommandation LDAP (dans ONTAP 9.5 et versions ultérieures), les conditions suivantes doivent être remplies :
  - Les deux domaines doivent être configurés avec l'une des relations d'approbation suivantes :
    - Bidirectionnel
    - Aller simple, où le principal fait confiance au domaine de référence
    - Parent-enfant
  - Le DNS doit être configuré pour résoudre tous les noms de serveur mentionnés.
  - Les mots de passe du domaine doivent être identiques pour s'authentifier lorsque `--bind-as-cifs-server` défini sur vrai.

Les configurations suivantes ne sont pas prises en charge avec la recherche de références LDAP.

- Pour toutes les versions de ONTAP :
- Clients LDAP sur un SVM d'admin
- Pour ONTAP 9.8 et versions antérieures (ils sont pris en charge dans la version 9.9.1 et ultérieures) :
- Signature et chiffrement LDAP (le `-session-security` en option)
- Connexions TLS cryptées (`-use-start-tls` en option)
- Communications via le port LDAPS 636 (le `-use-ldaps-for-ad-ldap` en option)

- A partir de ONTAP 9.11.1, vous pouvez utiliser "Utilisez la liaison rapide LDAP pour l'authentification nsswitch pour les SVM ONTAP NFS."
- Vous devez entrer un schéma LDAP lors de la configuration du client LDAP sur le SVM.

  Dans la plupart des cas, l'un des schémas ONTAP par défaut sera approprié. Toutefois, si le schéma LDAP de votre environnement diffère de celui-ci, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer le client LDAP. Consultez votre administrateur LDAP pour connaître les conditions requises pour votre environnement.

- L'utilisation de LDAP pour la résolution du nom d'hôte n'est pas prise en charge.

Pour plus d'informations, reportez-vous à la section "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP".

En savoir plus sur la signature et le scellement LDAP pour les SVM NFS ONTAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous devez configurer les paramètres de sécurité du serveur NFS sur la machine virtuelle de stockage (SVM) de manière à ce qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`. testez

La signature et le chiffrement LDAP sur le trafic SMB sont activés sur le SVM avec le `-session-security -for-ad-ldap` à la `vserver cifs security modify` commande.

En savoir plus sur LDAPS pour les SVM NFS ONTAP

Vous devez comprendre certains termes et concepts relatifs à la sécurisation de la communication LDAP par ONTAP. ONTAP peut utiliser START TLS ou LDAPS pour configurer des sessions authentifiées entre des serveurs LDAP intégrés à Active Directory ou des serveurs LDAP basés sur UNIX.

Terminologie

Il existe certains termes que vous devez comprendre sur la manière dont ONTAP utilise LDAPS pour sécuriser les communications LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) Protocole permettant d'accéder aux répertoires d'informations et de les gérer. LDAP est utilisé comme répertoire d'informations pour le stockage d'objets tels que des utilisateurs, des groupes et des groupes réseau. LDAP fournit également des services d'annuaire qui gèrent ces objets et répondent aux demandes LDAP des clients LDAP.

- **SSL**

  (Secure Sockets Layer) Protocole développé pour envoyer des informations en toute sécurité via Internet. Le protocole SSL est pris en charge par ONTAP 9 et versions ultérieures, mais il est obsolète en faveur de TLS.

- **TLS**

  (Sécurité de la couche de transport) un protocole de suivi conforme aux normes IETF, basé sur les spécifications SSL précédentes. C'est le successeur de SSL. TLS est pris en charge par ONTAP 9.5 et versions ultérieures.

- **LDAPS (LDAP sur SSL ou TLS)**

  Protocole utilisant TLS ou SSL pour sécuriser la communication entre les clients LDAP et les serveurs LDAP. Les termes *LDAP sur SSL* et *LDAP sur TLS* sont parfois utilisés de manière interchangeable. LDAPS est pris en charge par ONTAP 9.5 et versions ultérieures.

  - Dans ONTAP 9.5-9.8, LDAPS ne peut être activé que sur le port 636. Pour ce faire, utilisez le `-use-ldaps-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.
  - À partir de ONTAP 9.9.1, LDAPS peut être activé sur n'importe quel port, bien que le port 636 reste le port par défaut. Pour ce faire, réglez le `-ldaps-enabled` paramètre sur `true` et spécifiez le paramètre souhaité `-port`. Pour en savoir plus, `vserver services name-service ldap client create` consultez le "Référence de commande ONTAP".

  > Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.

- **Démarrer TLS**

  (Également appelé *start_tls*, *STARTTLS* et *StartTLS*) Un mécanisme de communication sécurisée à l'aide des protocoles TLS.

  ONTAP utilise STARTTLS pour sécuriser les communications LDAP et utilise le port LDAP par défaut (389) pour communiquer avec le serveur LDAP. Le serveur LDAP doit être configuré de manière à autoriser les connexions via le port LDAP 389 ; sinon, les connexions LDAP TLS du SVM vers le serveur LDAP échouent.

Comment ONTAP utilise LDAPS

ONTAP prend en charge l'authentification du serveur TLS qui permet au client SVM LDAP de confirmer l'identité du serveur LDAP lors de l'opération BIND. Les clients LDAP compatibles TLS peuvent utiliser des techniques standard de cryptographie à clé publique pour vérifier que le certificat et l'ID public d'un serveur

sont valides et ont été émis par une autorité de certification (AC) répertoriée dans la liste des autorités de certification de confiance du client.

LDAP prend en charge STARTTLS pour crypter les communications à l'aide de TLS. STARTTLS commence comme une connexion texte clair sur le port LDAP standard (389), et cette connexion est ensuite mise à niveau vers TLS.

ONTAP supporte les éléments suivants :

- LDAPS pour le trafic lié au SMB entre les serveurs LDAP intégrés à Active Directory et le SVM
- LDAPS pour le trafic LDAP pour le mappage de noms et autres informations UNIX

  Les serveurs LDAP intégrés à Active Directory ou les serveurs LDAP basés sur UNIX peuvent être utilisés pour stocker des informations pour le mappage de noms LDAP et d'autres informations UNIX, telles que des utilisateurs, des groupes et des netgroups.

- Certificats CA racine auto-signés

  Lors de l'utilisation d'un LDAP intégré à Active-Directory, le certificat racine auto-signé est généré lorsque le service de certificat Windows Server est installé dans le domaine. Lors de l'utilisation d'un serveur LDAP UNIX pour le mappage de noms LDAP, le certificat racine auto-signé est généré et enregistré à l'aide de moyens appropriés à cette application LDAP.

Par défaut, LDAPS est désactivé.

Activer la prise en charge LDAP RFC2307bis pour les SVM ONTAP NFS

Si vous souhaitez utiliser LDAP et que vous avez besoin de la fonctionnalité supplémentaire d'utilisation des appartenances aux groupes imbriqués, vous pouvez configurer ONTAP pour activer la prise en charge de LDAP RFC2307bis.

Avant de commencer

Vous devez avoir créé une copie de l'un des schémas de client LDAP par défaut que vous souhaitez utiliser.

Description de la tâche

Dans les schémas client LDAP, les objets de groupe utilisent l'attribut memberUID. Cet attribut peut contenir plusieurs valeurs et répertorie les noms des utilisateurs appartenant à ce groupe. Dans les schémas de client LDAP compatibles avec RFC2307bis, les objets de groupe utilisent l'attribut uniqueMember. Cet attribut peut contenir le nom unique complet (DN) d'un autre objet dans le répertoire LDAP. Cela vous permet d'utiliser des groupes imbriqués car les groupes peuvent avoir d'autres groupes en tant que membres.

L'utilisateur ne doit pas être membre de plus de 256 groupes, y compris des groupes imbriqués. ONTAP ignore tous les groupes dépassant la limite de 256 groupes.

Par défaut, le support RFC2307bis est désactivé.

> La prise en charge RFC2307bis est activée automatiquement dans ONTAP lorsqu'un client LDAP est créé avec le schéma MS-AD-BIS.

Pour plus d'informations, reportez-vous à la section "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP".

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Modifiez le schéma de client LDAP RFC2307 copié pour activer la prise en charge de RFC2307bis :

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifiez le schéma pour qu'il corresponde à la classe d'objet prise en charge par le serveur LDAP :

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifiez le schéma pour qu'il corresponde au nom d'attribut pris en charge par le serveur LDAP :

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Options de configuration ONTAP NFS pour les recherches dans l'annuaire LDAP

Vous pouvez optimiser les recherches d'annuaire LDAP, y compris les informations sur les utilisateurs, les groupes et les groupes réseau, en configurant le client LDAP ONTAP pour vous connecter aux serveurs LDAP de la manière la plus appropriée pour votre environnement. Vous devez savoir quand les valeurs de base LDAP et de recherche d'étendue par défaut sont suffisantes et quels paramètres doivent spécifier lorsque les valeurs personnalisées sont plus appropriées.

Les options de recherche du client LDAP pour les informations utilisateur, groupe et groupe réseau permettent d'éviter les requêtes LDAP échoués et, par conséquent, l'échec de l'accès du client aux systèmes de stockage. Ils permettent également de s'assurer que les recherches sont aussi efficaces que possible pour éviter les problèmes de performance du client.

Valeurs par défaut de recherche de base et de portée

La base LDAP est le DN de base par défaut utilisé par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide du DN de base. Cette option est appropriée lorsque votre répertoire LDAP est relativement petit et que toutes les entrées pertinentes se trouvent dans le même DN.

Si vous ne spécifiez pas de NA de base personnalisé, la valeur par défaut est `root`. Cela signifie que chaque requête recherche l'intégralité du répertoire. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

L'étendue de base LDAP est l'étendue de recherche par défaut utilisée par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide de la portée de base. Elle détermine si la requête LDAP recherche uniquement l'entrée

nommée, entre un niveau sous le DN ou l'ensemble de la sous-arborescence sous le DN.

Si vous ne spécifiez pas d'étendue de base personnalisée, la valeur par défaut est `subtree`. Cela signifie que chaque requête effectue une recherche dans toute la sous-arborescence située sous le nom unique. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

Valeurs de base et d'étendue personnalisées

Vous pouvez éventuellement spécifier des valeurs de base et de portée distinctes pour les recherches utilisateur, groupe et groupe réseau. Limiter la base de recherche et l'étendue des requêtes de cette façon peut améliorer considérablement les performances car elle limite la recherche à une sous-section plus petite de l'annuaire LDAP.

Si vous spécifiez des valeurs de base et d'étendue personnalisées, elles remplacent la base de recherche générale par défaut et la portée pour les recherches utilisateur, groupe et groupe réseau. Les paramètres permettant de spécifier des valeurs de base et d'étendue personnalisées sont disponibles au niveau de privilège avancé.

Paramètre client LDAP…	Spécifie personnalisé…
`-base-dn`	Nom unique de base pour toutes les recherches LDAP. Plusieurs valeurs peuvent être saisies si nécessaire (par exemple, si la recherche de référence LDAP est activée dans ONTAP 9.5 et versions ultérieures).
`-base-scope`	Portée de base pour toutes les recherches LDAP.
`-user-dn`	Noms distinctifs de base pour toutes les recherches d'utilisateurs LDAP. Ce paramètre s'applique également aux recherches de mappage de noms d'utilisateurs.
`-user-scope`	Portée de base pour toutes les recherches d'utilisateurs LDAP. Ce paramètre s'applique également aux recherches de mappage de noms d'utilisateurs.
`-group-dn`	DN de base pour toutes les recherches de groupes LDAP.
`-group-scope`	Portée de base pour toutes les recherches de groupe LDAP.
`-netgroup-dn`	DN de base pour toutes les recherches de groupes réseau LDAP.
`-netgroup-scope`	Portée de base pour toutes les recherches de groupes réseau LDAP.

Plusieurs valeurs DN de base personnalisées

Si votre structure d'annuaire LDAP est plus complexe, vous devrez peut-être spécifier plusieurs DNS de base pour rechercher des informations dans plusieurs parties de votre annuaire LDAP. Vous pouvez spécifier plusieurs DNS pour les paramètres DN utilisateur, groupe et groupe réseau en les séparant par un point-virgule (;) et en enfermant toute la liste de recherche DN avec des guillemets doubles ("). Si un DN contient un

point-virgule, vous devez ajouter un caractère d'échappement (\) immédiatement avant le point-virgule dans le DN.

Notez que le périmètre s'applique à la liste complète de DNS spécifiée pour le paramètre correspondant. Par exemple, si vous spécifiez une liste de trois noms d'utilisateur différents et de sous-arborescence pour l'étendue utilisateur, l'utilisateur LDAP recherche dans l'ensemble de la sous-arborescence pour chacun des trois DNS spécifiés.

Depuis ONTAP 9.5, vous pouvez également spécifier LDAP *recommandation traquer*, qui permet au client LDAP ONTAP de renvoyer des demandes de recherche à d'autres serveurs LDAP si une réponse de recommandation LDAP n'est pas renvoyée par le serveur LDAP principal. Le client utilise ces données de référence pour extraire l'objet cible du serveur décrit dans les données de référence. Pour rechercher des objets présents dans les serveurs LDAP désignés, le dn de base des objets désignés peut être ajouté au dn de base dans le cadre de la configuration du client LDAP. Cependant, les objets renvoyés ne sont examinés que lorsque la recherche de renvoi est activée (à l'aide du `-referral-enabled true`) lors de la création ou de la modification d'un client LDAP.

Filtres de recherche LDAP personnalisés

Vous pouvez utiliser le paramètre d'option de configuration LDAP pour créer un filtre de recherche personnalisé. Le `-group-membership-filter` paramètre spécifie le filtre de recherche à utiliser lors de la recherche de l'appartenance à un groupe à partir d'un serveur LDAP.

Voici un exemple de filtres valides :

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

En savoir plus sur "Comment configurer LDAP dans ONTAP".

Améliorer les performances des recherches de groupe réseau par hôte dans l'annuaire LDAP pour les SVM NFS ONTAP

Si votre environnement LDAP est configuré pour permettre des recherches netgroup-par-hôte, vous pouvez configurer ONTAP pour en tirer parti et effectuer des recherches netgroup-par-hôte. Cela permet d'accélérer considérablement les recherches sur les groupes réseau et de réduire les problèmes d'accès aux clients NFS possibles en raison de la latence lors des recherches sur les groupes réseau.

Avant de commencer

Votre annuaire LDAP doit contenir un `netgroup.byhost` carte.

Vos serveurs DNS doivent contenir des enregistrements de recherche avant (A) et arrière (PTR) pour les clients NFS.

Lorsque vous spécifiez des adresses IPv6 dans les groupes réseau, vous devez toujours raccourcir et compresser chaque adresse comme spécifié dans RFC 5952.

Description de la tâche

Les serveurs NIS stockent les informations de groupe réseau sous trois cartes distinctes appelées `netgroup`, `netgroup.byuser`, et `netgroup.byhost`. Le but du `netgroup.byuser` et `netgroup.byhost` les cartes permettent d'accélérer la recherche de groupes réseau. ONTAP peut effectuer des recherches netgroup par

hôte sur les serveurs NIS pour améliorer les temps de réponse de montage.

Par défaut, les répertoires LDAP ne possèdent pas ce type de `netgroup.byhost` Effectuez des mappes comme les serveurs NIS. Il est cependant possible, avec l'aide d'outils tiers, d'importer un NIS `netgroup.byhost` Effectuez un mappage vers des répertoires LDAP pour permettre des recherches réseau par hôte rapides. Si vous avez configuré votre environnement LDAP pour autoriser des recherches netgroup-par-hôte, vous pouvez configurer le client LDAP ONTAP avec le système `netgroup.byhost` Nom de mappage, DN et étendue de recherche pour des recherches plus rapides avec netgroup par hôte.

La réception plus rapide des résultats de recherches netgroup par hôte permet à ONTAP de traiter les règles d'exportation plus rapidement lorsque les clients NFS demandent un accès aux exportations. Cela permet de réduire les risques de retard d'accès en raison des problèmes de latence de recherche de groupe réseau.

Étapes

1. Obtenir le nom distinctif complet exact du NIS `netgroup.byhost` Mapper que vous avez importé dans votre répertoire LDAP.

   Le NA de carte peut varier en fonction de l'outil tiers utilisé pour l'importation. Pour des performances optimales, vous devez spécifier le NA correspondant exact.

2. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
3. Activer les recherches netgroup-by-host dans la configuration client LDAP de la machine virtuelle de stockage (SVM) : `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} Active ou désactive la recherche netgroup-par-hôte pour les répertoires LDAP. La valeur par défaut est `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` spécifie le nom distinctif du `netgroup.byhost` Mapper dans le répertoire LDAP. Il remplace le DN de base pour les recherches netgroup-par-hôte. Si vous ne spécifiez pas ce paramètre, ONTAP utilise plutôt le DN de base.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} spécifie l'étendue de recherche pour les recherches netgroup-par-hôte. Si vous ne spécifiez pas ce paramètre, le paramètre par défaut est `subtree`.

   Si la configuration client LDAP n'existe pas encore, vous pouvez activer les recherches netgroup-par-hôte en spécifiant ces paramètres lors de la création d'une nouvelle configuration client LDAP à l'aide de l' `vserver services name-service ldap client create` commande.

   > Le `-ldap-servers` le champ remplace le `-servers` champ. Vous pouvez utiliser le `-ldap-servers` champ pour spécifier soit un nom d'hôte soit une adresse IP pour le serveur LDAP.

4. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

La commande suivante modifie la configuration du client LDAP existante nommée « ldap_corp » pour activer les recherches netgroup par hôte à l'aide de l' `netgroup.byhost` Carte nommée ""nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com" et champ de recherche par défaut `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Une fois que vous avez terminé

Le `netgroup.byhost` et `netgroup` les cartes du répertoire doivent être synchronisées en permanence pour éviter tout problème d'accès client.

Informations associées

"IETF RFC 5952 : une recommandation pour la représentation texte de l'adresse IPv6"

Utiliser la liaison rapide LDAP pour l'authentification nsswitch pour les SVM NFS ONTAP

Depuis ONTAP 9.11.1, vous pouvez bénéficier de la fonctionnalité LDAP *FAST bind* (également appelée *bind* simultanée) pour des requêtes d'authentification client plus rapides et plus simples. Pour utiliser cette fonctionnalité, le serveur LDAP doit prendre en charge la fonctionnalité de liaison rapide.

Description de la tâche

Sans liaison rapide, ONTAP utilise LDAP simple BIND pour authentifier les utilisateurs admin avec le serveur LDAP. Avec cette méthode d'authentification, ONTAP envoie un nom d'utilisateur ou de groupe au serveur LDAP, reçoit le mot de passe de hachage stocké et compare le code de hachage du serveur avec le code de hachage généré localement à partir du mot de passe de l'utilisateur. S'ils sont identiques, ONTAP accorde l'autorisation de connexion.

Grâce à la fonctionnalité de liaison rapide, ONTAP n'envoie que les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) au serveur LDAP via une connexion sécurisée. Le serveur LDAP valide ensuite ces informations d'identification et demande à ONTAP d'accorder des autorisations de connexion.

L'un des avantages de Fast bind est qu'il n'est pas nécessaire que ONTAP prenne en charge chaque nouvel algorithme de hachage pris en charge par les serveurs LDAP, car le hachage du mot de passe est effectué par le serveur LDAP.

"En savoir plus sur l'utilisation de FAST BIND."

Vous pouvez utiliser les configurations client LDAP existantes pour la liaison rapide LDAP. Cependant, il est fortement recommandé de configurer le client LDAP pour TLS ou LDAPS ; dans le cas contraire, le mot de passe est envoyé sur le réseau en texte brut.

Pour activer la liaison rapide LDAP dans un environnement ONTAP, vous devez répondre aux exigences suivantes :

- Les utilisateurs admin ONTAP doivent être configurés sur un serveur LDAP qui prend en charge la liaison rapide.
- Le SVM ONTAP doit être configuré pour LDAP dans la base de données du switch des services de noms (nsswitch).
- Les comptes utilisateur et groupe admin ONTAP doivent être configurés pour l'authentification nsswitch avec le bind rapide.

Étapes

1. Vérifiez auprès de votre administrateur LDAP que la liaison rapide LDAP est prise en charge sur le serveur LDAP.
2. Assurez-vous que les informations d'identification de l'utilisateur administrateur ONTAP sont configurées sur le serveur LDAP.
3. Vérifier que le SVM admin ou données est configuré correctement pour LDAP FAST BIND.

   a. Pour confirmer que le serveur LDAP FAST BIND est répertorié dans la configuration du client LDAP, entrez :

      `vserver services name-service ldap client show`

      "En savoir plus sur la configuration du client LDAP."

   b. Pour le confirmer `ldap` est l'une des sources configurées pour le nsswitch `passwd` base de données, entrez :

      `vserver services name-service ns-switch show`

   "Découvrez la configuration nsswitch."

4. Assurez-vous que les utilisateurs admin s'authentifient auprès de nsswitch et que l'authentification LDAP FAST BIND est activée dans leurs comptes.

   ◦ Pour les utilisateurs existants, entrez `security login modify` et vérifiez les paramètres suivants :

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   Pour en savoir plus, `security login modify` consultez le "Référence de commande ONTAP".

   ◦ Pour les nouveaux utilisateurs admin, voir "Activez l'accès au compte ONTAP LDAP ou NIS".

Afficher les statistiques LDAP pour les SVM ONTAP NFS

Vous pouvez afficher les statistiques LDAP pour les machines virtuelles de stockage (SVM) sur un système de stockage pour surveiller les performances et diagnostiquer les problèmes.

Avant de commencer

- Vous devez avoir configuré un client LDAP sur la SVM.
- Vous devez avoir identifié des objets LDAP à partir desquels vous pouvez afficher des données.

Étape

1. Afficher les données de performance des objets compteur :

   `statistics show`

Exemples

L'exemple suivant affiche les statistiques de l'échantillon nommé **smpl_1** pour les compteurs : avg_processor_Busy et cpu_Busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Informations associées

- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Configurez les mappages de noms

En savoir plus sur la configuration du mappage de noms pour les SVM NAS ONTAP

ONTAP utilise le mappage de noms pour mapper les identités SMB aux identités UNIX, aux identités Kerberos aux identités UNIX et aux identités UNIX aux identités SMB. Il a besoin de ces informations pour obtenir les informations d'identification des utilisateurs et fournir un accès approprié aux fichiers, qu'ils se connectent depuis un client NFS ou un client SMB.

Il existe deux exceptions lorsque vous n'avez pas besoin d'utiliser le mappage de noms :

- Vous configurez un environnement UNIX pur et ne prévoyez pas d'utiliser l'accès SMB ou le style de sécurité NTFS sur les volumes.
- Vous configurez l'utilisateur par défaut à utiliser à la place.

  Dans ce scénario, le mappage de noms n'est pas nécessaire car au lieu de mapper chaque identifiant client individuel, toutes les informations d'identification client sont mappées au même utilisateur par défaut.

Notez que vous pouvez utiliser le mappage de noms uniquement pour les utilisateurs, pas pour les groupes.

Toutefois, vous pouvez mapper un groupe d'utilisateurs individuels à un utilisateur spécifique. Par exemple, vous pouvez mapper tous les utilisateurs AD qui commencent ou se terminent par le mot VENTES à un utilisateur UNIX spécifique et à l'UID de l'utilisateur.

En savoir plus sur les mappages de noms pour les SVM NAS ONTAP

Lorsque ONTAP doit mapper les informations d'identification d'un utilisateur, il recherche tout d'abord un mappage existant dans la base de données de mappage de noms locaux et le serveur LDAP. Qu'elle vérifie un ou les deux et dans quel ordre est déterminé par la configuration du service de nom du SVM.

- Pour le mappage Windows à UNIX

  Si aucun mappage n'est trouvé, ONTAP vérifie si le nom d'utilisateur Windows minuscule est un nom d'utilisateur valide dans le domaine UNIX. Si cela ne fonctionne pas, il utilise l'utilisateur UNIX par défaut à condition qu'il soit configuré. Si l'utilisateur UNIX par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

- Pour le mappage d'UNIX à Windows

  Si aucun mappage n'est trouvé, ONTAP tente de trouver un compte Windows correspondant au nom UNIX dans le domaine SMB. Si cela ne fonctionne pas, il utilise l'utilisateur SMB par défaut, à condition qu'il soit configuré. Si l'utilisateur SMB par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

Par défaut, les comptes machine sont mappés à l'utilisateur UNIX par défaut spécifié. Si aucun utilisateur UNIX par défaut n'est spécifié, les mappages de compte machine échouent.

- À partir de ONTAP 9.5, vous pouvez mapper des comptes machine à des utilisateurs autres que l'utilisateur UNIX par défaut.
- Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas mapper les comptes machine à d'autres utilisateurs.

  Même si des mappages de noms pour des comptes machine sont définis, les mappages sont ignorés.

Recherches multidomaines pour les mappages de noms d'utilisateur UNIX vers Windows sur les SVM NAS ONTAP

ONTAP prend en charge les recherches multidomaine lors du mappage d'utilisateurs UNIX aux utilisateurs Windows. Tous les domaines de confiance découverts sont recherchés pour trouver des correspondances avec le modèle de remplacement jusqu'à ce qu'un résultat correspondant soit renvoyé. Vous pouvez également configurer une liste de domaines de confiance préférés, qui est utilisée à la place de la liste de domaines de confiance découverts et est recherchée dans l'ordre jusqu'à ce qu'un résultat correspondant soit renvoyé.

La manière dont les approbations de domaine affectent les recherches de mappage de noms d'utilisateur UNIX à des noms d'utilisateur Windows

Pour comprendre le fonctionnement du mappage de noms d'utilisateur multidomaine, vous devez comprendre comment les approbations de domaine fonctionnent avec ONTAP. Les relations d'approbation Active Directory avec le domaine d'accueil du serveur SMB peuvent être une confiance bidirectionnelle ou l'un des deux types de fiducies unidirectionnelles, soit une confiance entrante, soit une confiance sortante. Le home domain est le domaine auquel le serveur SMB sur le SVM appartient.

- *Confiance bidirectionnelle*

Avec des approbations bidirectionnelles, les deux domaines se font confiance. Si le domaine de base du serveur SMB possède une approbation bidirectionnelle avec un autre domaine, le domaine de base peut authentifier et autoriser un utilisateur appartenant au domaine de confiance, et vice versa.

Les recherches de mappage de noms d'utilisateur UNIX à Windows peuvent être effectuées uniquement sur les domaines avec des approbations bidirectionnelles entre le domaine principal et l'autre domaine.

- *Confiance sortante*

  Avec une confiance sortante, le domaine d'origine approuve l'autre domaine. Dans ce cas, le domaine home peut authentifier et autoriser un utilisateur appartenant au domaine de confiance sortant.

  Un domaine avec une confiance sortante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

- *Confiance entrante*

  Avec une confiance entrante, l'autre domaine fait confiance au domaine d'origine du serveur SMB. Dans ce cas, le domaine personnel ne peut pas authentifier ni autoriser un utilisateur appartenant au domaine de confiance entrant.

  Un domaine avec une confiance entrante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

Comment les caractères génériques (*) sont utilisés pour configurer les recherches multidomaines pour le mappage de noms

Les recherches de mappage de noms de domaines multiples sont facilitées par l'utilisation de caractères génériques dans la section domaine du nom d'utilisateur Windows. Le tableau suivant illustre comment utiliser des caractères génériques dans la partie domaine d'une entrée de mappage de nom pour activer les recherches multidomaine :

Motif	Remplacement	Résultat
racine	{astérisque}\\administrateur	L'utilisateur UNIX « root » est mappé à l'utilisateur nommé « administrateur ». Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant nommé « administrateur » soit trouvé.

Motif	Remplacement	Résultat
*	{astérisque}\\{asterslash}*	Les utilisateurs UNIX valides sont mappés aux utilisateurs Windows correspondants. Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant à ce nom soit trouvé. Le motif {astérisque}\\{Asterslash} est valable uniquement pour le mappage de noms d'UNIX à Windows, pas l'inverse.

Mode d'exécution des recherches sur plusieurs noms de domaine

Vous pouvez choisir l'une des deux méthodes pour déterminer la liste des domaines approuvés utilisés pour les recherches de noms multidomaines :

- Utilisez la liste d'approbation bidirectionnelle automatiquement découverte compilée par ONTAP
- Utilisez la liste de domaines approuvés que vous compilez

Si un utilisateur UNIX est mappé à un utilisateur Windows avec un caractère générique utilisé pour la section domaine du nom d'utilisateur, l'utilisateur Windows est recherché dans tous les domaines approuvés comme suit :

- Si une liste de domaines de confiance est configurée, l'utilisateur Windows mappé est uniquement recherché dans cette liste de recherche, dans l'ordre.
- Si une liste préférée de domaines approuvés n'est pas configurée, l'utilisateur Windows est alors recherché dans tous les domaines de confiance bidirectionnels du domaine de départ.
- S'il n'existe pas de domaines de confiance bidirectionnellement pour le domaine personnel, l'utilisateur est recherché dans le domaine personnel.

Si un utilisateur UNIX est mappé à un utilisateur Windows sans section de domaine dans le nom d'utilisateur, l'utilisateur Windows est recherché dans le domaine personnel.

Règles de conversion de mappage de noms pour les SVM NAS ONTAP

Un système ONTAP conserve un ensemble de règles de conversion pour chaque SVM. Chaque règle se compose de deux éléments : un *pattern* et un *remplacement*. Les conversions commencent au début de la liste appropriée et effectuent une substitution basée sur la première règle correspondante. Le motif est une expression régulière de style UNIX. Le remplacement est une chaîne contenant des séquences d'échappement représentant des sous-expressions du motif, comme dans UNIX `sed` programme.

Créer des mappages de noms pour les SVM NAS ONTAP

Vous pouvez utiliser le `vserver name-mapping create` commande permettant de créer un mappage de noms. Vous utilisez les mappages de noms pour permettre aux utilisateurs Windows d'accéder aux volumes du style de sécurité UNIX et les inverser.

Description de la tâche

Par SVM, ONTAP prend en charge jusqu'à 12,500 mappages de noms dans chaque direction.

Étape

1. Créer un mappage de noms :

   ```
   vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
   ```

   > Les `-pattern` instructions et `-replacement` peuvent être formulées en tant qu'expressions régulières. Vous pouvez également utiliser l'`-replacement`instruction pour refuser explicitement un mappage à l'utilisateur en utilisant la chaîne de remplacement NULL `" "` (caractère d'espace). Pour en savoir plus, `vserver name-mapping create` consultez le "Référence de commande ONTAP".

   Lorsque des mappages entre Windows et UNIX sont créés, tous les clients SMB disposant de connexions ouvertes au système ONTAP au moment de la création des nouveaux mappages doivent se déconnecter et se reconnecter pour voir les nouveaux mappages.

Exemples

La commande suivante crée un nom de mappage sur le SVM nommé vs1. Le mappage est un mappage d'UNIX à Windows à la position 1 dans la liste des priorités. Le mappage mappe l'utilisateur UNIX johnd à l'utilisateur Windows ENG\johndoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Le mappage est un mappage de Windows à UNIX à la position 1 dans la liste des priorités. Dans ce cas, le motif et le remplacement incluent des expressions régulières. Le mapping mappe chaque utilisateur CIFS du domaine ENG aux utilisateurs du domaine LDAP associé avec la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Ici, le schéma inclut "`$"` comme élément du nom d'utilisateur Windows qui doit être échappé. Le mappage mappe l'utilisateur Windows ENG\ john$OPS à l'utilisateur UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configurer l'utilisateur par défaut pour les SVM NAS ONTAP

Vous pouvez configurer un utilisateur par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l'authentification des utilisateurs non mappés échoue, vous ne devez pas configurer un utilisateur par défaut.

Description de la tâche

Pour l'authentification CIFS, si vous ne souhaitez pas mapper chaque utilisateur Windows à un utilisateur UNIX individuel, vous pouvez spécifier un utilisateur UNIX par défaut.

Pour l'authentification NFS, si vous ne souhaitez pas mapper chaque utilisateur UNIX à un utilisateur Windows individuel, vous pouvez spécifier un utilisateur Windows par défaut.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Configurez l'utilisateur UNIX par défaut	`vserver cifs options modify -default-unix-user user_name`
Configurez l'utilisateur Windows par défaut	`vserver nfs modify -default-win-user user_name`

Commandes ONTAP pour la gestion des mappages de noms NFS

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un mappage de nom	`vserver name-mapping create`
Insérez un mappage de nom à une position spécifique	`vserver name-mapping insert`
Afficher les mappages de noms	`vserver name-mapping show`

Échange de la position de deux mappages de noms REMARQUE : un échange n'est pas autorisé lorsque le mappage-noms est configuré avec une entrée de qualificatif-ip.	`vserver name-mapping swap`
Modifier un mappage de noms	`vserver name-mapping modify`
Supprime un mappage de noms	`vserver name-mapping delete`
Valider le mappage de nom correct	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Pour en savoir plus, `vserver name-mapping` consultez le "Référence de commande ONTAP".

Activer l'accès des clients Windows NFS pour les SVM ONTAP

ONTAP prend en charge l'accès aux fichiers à partir de clients Windows NFSv3. Cela signifie que les clients exécutant des systèmes d'exploitation Windows avec prise en charge de NFSv3 peuvent accéder aux fichiers lors des exports NFSv3 sur le cluster. Pour utiliser correctement cette fonctionnalité, vous devez configurer correctement le serveur virtuel de stockage (SVM) et connaître certaines exigences et limites.

Description de la tâche

Par défaut, la prise en charge du client Windows NFSv3 est désactivée.

Avant de commencer

NFSv3 doit être activé sur le SVM.

Étapes

1. Activer la prise en charge des clients Windows NFSv3 :

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Sur tous les SVM qui prennent en charge les clients Windows NFSv3, désactivez le `-enable-ejukebox` et `-v3-connection-drop` paramètres :

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

   Les clients Windows NFSv3 peuvent désormais monter des exportations sur le système de stockage.

3. Assurez-vous que chaque client Windows NFSv3 utilise des montages durs en spécifiant le `-o mtype=hard` option.

   Ceci est nécessaire pour garantir la fiabilité des supports.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

Activer l'affichage des exportations sur les clients NFS pour les SVM ONTAP

Les clients NFS peuvent utiliser le `showmount -e` Commande pour afficher la liste des exportations disponibles à partir d'un serveur NFS ONTAP. Cela peut aider les utilisateurs à identifier le système de fichiers qu'ils souhaitent monter.

ONTAP permet aux clients NFS d'afficher la liste d'exportation par défaut. Dans les versions précédentes, l' `showmount`option de la `vserver nfs modify` commande doit être activée explicitement. Pour afficher la liste d'export, NFSv3 doit être activé sur le SVM.

Exemple

La commande suivante présente la fonctionnalité showmount sur le SVM nommé vs1 :

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

La commande suivante exécutée sur un client NFS affiche la liste des exportations sur un serveur NFS avec l'adresse IP 10.63.21.9 :

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Gérer l'accès aux fichiers à l'aide de NFS

Activer ou désactiver NFSv3 pour les SVM ONTAP

Vous pouvez activer ou désactiver NFSv3 en modifiant le `-v3` option. Cette fonctionnalité permet aux clients d'accéder aux fichiers via le protocole NFSv3. NFSv3 est activé par défaut.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activez NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`

Désactiver NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Activer ou désactiver NFSv4.0 pour les SVM ONTAP

Vous pouvez activer ou désactiver NFSv4.0 en modifiant le `-v4.0` option. Cela permet d'accéder aux fichiers pour les clients utilisant le protocole NFSv4.0. Dans ONTAP 9.9.1, NFSv4.0 est activé par défaut ; dans les versions antérieures, il est désactivé par défaut.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Désactivez NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Activer ou désactiver NFSv4.1 pour les SVM ONTAP

Vous pouvez activer ou désactiver NFSv4.1 en modifiant `-v4.1` option. Ainsi, les clients bénéficient d'un accès aux fichiers à l'aide du protocole NFSv4.1. Dans ONTAP 9.9.1, NFSv4.1 est activé par défaut. Dans les versions antérieures, il est désactivé par défaut.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activation de NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Désactiver NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Gérer les limites du pool de stockage ONTAP NFSv4

À partir de ONTAP 9.13, les administrateurs peuvent activer leurs serveurs NFSv4 pour refuser des ressources aux clients NFSv4 lorsqu'ils ont atteint les limites de ressources de pool de stockage par client. Lorsque les clients consomment trop de ressources de pool de stockage NFSv4, cela peut entraîner le blocage d'autres clients NFSv4 en raison de l'indisponibilité des ressources de pool de stockage NFSv4.

L'activation de cette fonction permet également aux clients d'afficher la consommation de ressources du pool

de stockage actif par chaque client. Cela facilite l'identification des clients qui épuise les ressources système et permet d'imposer des limites de ressources par client.

Afficher les ressources de pool de stockage consommées

Le `vserver nfs storepool show` affiche le nombre de ressources de pool de stockage utilisées. Un pool de stockage est un pool de ressources utilisé par les clients NFSv4.

Étape

1. En tant qu'administrateur, exécutez `vserver nfs storepool show` Commande permettant d'afficher les informations de réserve des clients NFSv4.

Exemple

Cet exemple affiche les informations relatives au pool de stockage des clients NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Activer ou désactiver les contrôles de limite de pool de stockage

Les administrateurs peuvent utiliser les commandes suivantes pour activer ou désactiver les contrôles de limite de pool de stockage.

Étape

1. En tant qu'administrateur, effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer les contrôles de limite de pool de stockage	`vserver nfs storepool config modify -limit-enforce enabled`

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Désactiver les contrôles de limite de pool de stockage	`vserver nfs storepool config modify -limit-enforce disabled`

Afficher la liste des clients bloqués

Si la limite de réserve est activée, les administrateurs peuvent voir quels clients ont été bloqués lorsqu'ils ont atteint leur seuil de ressources par client. Les administrateurs peuvent utiliser la commande suivante pour voir quels clients ont été marqués comme des clients bloqués.

Étapes

1. Utilisez le `vserver nfs storepool blocked-client show` Commande permettant d'afficher la liste des clients bloqués par NFSv4.

Supprimer un client de la liste des clients bloqués

Les clients qui atteignent leur seuil par client seront déconnectés et ajoutés au cache client-bloc. Les administrateurs peuvent utiliser la commande suivante pour supprimer le client du cache du client de bloc. Cela permettra au client de se connecter au serveur ONTAP NFSV4.

Étapes

1. Utilisez le `vserver nfs storepool blocked-client flush -client-ip <ip address>` commande permettant de vider le cache client bloqué du pool de stockage.
2. Utilisez le `vserver nfs storepool blocked-client show` commande permettant de vérifier que le client a été supprimé du cache du client en mode bloc.

Exemple

Cet exemple affiche un client bloqué dont l'adresse IP "10.2.1.1" est vidée de tous les nœuds.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

Activer ou désactiver pNFS pour les SVM ONTAP

PNFS améliore les performances en permettant aux clients NFS d'effectuer des opérations de lecture/écriture sur les périphériques de stockage directement et en parallèle, en contournant le serveur NFS comme un goulot d'étranglement potentiel. Pour

activer ou désactiver pNFS (Parallel NFS), vous pouvez modifier le `-v4.1-pnfs` option.

Si la version de ONTAP est…	La norme pNFS par défaut est…
9.8 ou ultérieure	désactivé
9.7 ou antérieure	activé

Avant de commencer

La prise en charge de NFSv4.1 est requise pour pouvoir utiliser pNFS.

Si vous souhaitez activer pNFS, vous devez d'abord désactiver les référencements NFS. Les deux ne peuvent pas être activées en même temps.

Si vous utilisez pNFS avec Kerberos sur des SVM, il faut activer Kerberos sur chaque LIF de la SVM.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activez pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Désactiver pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Informations associées

- Présentation de l'agrégation NFS

Contrôler l'accès NFS via TCP et UDP pour les SVM ONTAP

Vous pouvez activer ou désactiver l'accès NFS aux serveurs virtuels de stockage (SVM) via TCP et UDP en modifiant le `-tcp` et `-udp` paramètres, respectivement. Vous pouvez ainsi contrôler l'accès des clients NFS aux données via TCP ou UDP dans votre environnement.

Description de la tâche

Ces paramètres s'appliquent uniquement à NFS. Ils n'affectent pas les protocoles auxiliaires. Par exemple, si NFS sur TCP est désactivé, les opérations de montage sur TCP ont toujours réussi. Pour bloquer complètement le trafic TCP ou UDP, vous pouvez utiliser des règles d'export-policy.

> Vous devez désactiver le serveur RPC SnapDiff avant de désactiver TCP pour NFS pour éviter une erreur de commande. Vous pouvez désactiver TCP en utilisant la commande `vserver snapdiff-rpc-server off -vserver vserver name`.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez obtenir un accès NFS…	Entrez la commande…
Activé sur TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Désactivé sur TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Activé sur UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Désactivé sur UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Contrôler les requêtes NFS à partir de ports non réservés pour les SVM ONTAP

Vous pouvez rejeter les demandes de montage NFS à partir de ports non réservés en activant le `-mount-rootonly` option. Pour rejeter toutes les demandes NFS de ports non réservés, vous pouvez activer le `-nfs-rootonly` option.

Description de la tâche

Par défaut, l'option `-mount-rootonly` est `enabled`.

Par défaut, l'option `-nfs-rootonly` est `disabled`.

Ces options ne s'appliquent pas à la procédure NULL.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Autoriser les demandes de montage NFS à partir de ports non réservés	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Rejeter les demandes de montage NFS à partir de ports non réservés	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Autoriser toutes les demandes NFS à partir de ports non réservés	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Rejeter toutes les demandes NFS de ports non réservés	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Gérer l'accès NFS aux volumes ONTAP NTFS ou aux qtrees pour les utilisateurs UNIX inconnus

Si ONTAP ne peut pas identifier les utilisateurs UNIX qui tentent de se connecter à des

volumes ou des qtrees avec le style de sécurité NTFS, il ne peut donc pas mapper l'utilisateur de façon explicite à un utilisateur Windows. Vous pouvez configurer ONTAP de manière à refuser l'accès à ces utilisateurs pour une sécurité plus stricte ou les mapper à un utilisateur Windows par défaut afin d'assurer un niveau d'accès minimum pour tous les utilisateurs.

Avant de commencer

Un utilisateur Windows par défaut doit être configuré si vous souhaitez activer cette option.

Description de la tâche

Si un utilisateur UNIX tente d'accéder aux volumes ou aux qtrees avec un style de sécurité NTFS, l'utilisateur UNIX doit d'abord être mappé à un utilisateur Windows afin que ONTAP puisse correctement évaluer les autorisations NTFS. Cependant, si ONTAP ne peut pas rechercher le nom de l'utilisateur UNIX dans les sources de service de nom d'informations utilisateur configurées, il ne peut pas explicitement mapper l'utilisateur UNIX à un utilisateur Windows spécifique. Vous pouvez décider comment gérer ces utilisateurs UNIX inconnus de la manière suivante :

- Refuser l'accès aux utilisateurs UNIX inconnus.

  Ceci met en œuvre une sécurité plus stricte en nécessitant un mappage explicite pour tous les utilisateurs UNIX afin d'accéder aux volumes ou aux qtrees NTFS.

- Mapper des utilisateurs UNIX inconnus à un utilisateur Windows par défaut.

  Cette fonctionnalité offre moins de sécurité et davantage de commodité, en veillant à ce que tous les utilisateurs aient un niveau d'accès minimal aux volumes NTFS ou aux qtrees par l'intermédiaire d'un utilisateur Windows par défaut.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Si vous voulez que l'utilisateur Windows par défaut pour les utilisateurs UNIX inconnus…	Entrez la commande…
Activé	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Désactivé	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Considérations pour les clients qui montent des exportations NFS ONTAP sur des ports non réservés

Le `-mount-rootonly` L'option doit être désactivée sur un système de stockage qui doit prendre en charge les clients qui montent des exportations NFS à l'aide d'un port non réservé, même lorsque l'utilisateur est connecté en tant que root. Ces clients comprennent les clients Hummingbird et les clients Solaris NFS/IPv6.

Si le `-mount-rootonly` ONTAP n'autorise pas les clients NFS utilisant des ports non réservés. Ainsi, les ports dont les numéros sont supérieurs à 1,023, ne permettent pas le montage des exports NFS.

Effectuez une vérification d'accès plus stricte pour les groupes réseau en vérifiant les domaines pour les SVM NFS ONTAP

Par défaut, ONTAP effectue une vérification supplémentaire lors de l'évaluation de l'accès client pour un groupe réseau. Cette vérification supplémentaire garantit que le domaine du client correspond à la configuration de domaine de la machine virtuelle de stockage (SVM). Sinon, ONTAP refuse l'accès client.

Description de la tâche

Lorsque ONTAP évalue les règles d'export policy pour l'accès client et qu'une règle d'export policy contient un netgroup, ONTAP doit déterminer si l'adresse IP d'un client appartient au netgroup. Pour ce faire, ONTAP convertit l'adresse IP du client en un nom d'hôte à l'aide du DNS et obtient un nom de domaine complet (FQDN).

Si le fichier netgroup répertorie uniquement un nom court pour l'hôte et que le nom court de l'hôte existe dans plusieurs domaines, il est possible qu'un client d'un domaine différent obtienne un accès sans cette vérification.

Pour empêcher cela, ONTAP compare le domaine renvoyé par DNS pour l'hôte avec la liste des noms de domaine DNS configurés pour le SVM. Si la correspondance correspond, l'accès est autorisé. Si ce n'est pas le cas, l'accès est refusé.

Cette vérification est activée par défaut. Vous pouvez le gérer en modifiant le `-netgroup-dns-domain -search` paramètre, disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'action souhaitée :

Si vous voulez que la vérification de domaine pour les groupes réseau soit…	Entrer…
Activé	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`

Si vous voulez que la vérification de domaine pour les groupes réseau soit…	Entrer…
Désactivé	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Définissez le niveau de privilège sur admin :

   ```
   set -privilege admin
   ```

Modifier les ports utilisés pour les services NFSv3 pour les SVM ONTAP

Le serveur NFS du système de stockage utilise des services tels que le démon de montage et Network Lock Manager pour communiquer avec les clients NFS sur des ports réseau par défaut spécifiques. Dans la plupart des environnements NFS, les ports par défaut fonctionnent correctement et ne nécessitent pas de modification, mais si vous souhaitez utiliser différents ports réseau NFS dans votre environnement NFSv3, vous pouvez le faire.

Avant de commencer

La modification des ports NFS sur le système de stockage requiert que tous les clients NFS se connectent au système. Il est donc important de communiquer ces informations aux utilisateurs avant de faire la modification.

Description de la tâche

Vous pouvez définir les ports utilisés par les services du démon de montage NFS, Network Lock Manager, Network Status Monitor et NFS quota daemon pour chaque machine virtuelle de stockage (SVM). La modification du numéro de port affecte l'accès des clients NFS aux données via TCP et UDP.

Les ports pour NFSv4 et NFSv4.1 ne peuvent pas être modifiés.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Désactivation de l'accès à NFS :

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Définissez le port NFS pour le service NFS spécifique :

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

Paramètre du port NFS	Description	Port par défaut
`-mountd-port`	Démon de montage NFS	658

Paramètre du port NFS	Description	Port par défaut
`-nlm-port`	Gestionnaire de verrouillage réseau	4045
`-nsm-port`	Moniteur d'état du réseau	4046
`-rquotad-port`	Démon de quota NFS	4049

Outre le port par défaut, la plage autorisée de numéros de port est comprise entre 1024 et 65535. Chaque service NFS doit utiliser un port unique.

4. Activation de l'accès au NFS :

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Utilisez le `network connections listening show` pour vérifier que le numéro de port change.

   Pour en savoir plus, `network connections listening show` consultez le "Référence de commande ONTAP".

6. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Exemple

Les commandes suivantes définissent le port NFS Mount Daemon sur 1113 sur le SVM nommé vs1 :

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

Commandes ONTAP pour la gestion des serveurs NFS

Il existe des commandes ONTAP spécifiques pour gérer les serveurs NFS.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un serveur NFS	`vserver nfs create`
Affichez les serveurs NFS	`vserver nfs show`
Modifier un serveur NFS	`vserver nfs modify`
Supprimer un serveur NFS	`vserver nfs delete`

Masquer le `.snapshot` Liste de répertoires sous points de montage NFSv3 Accès explicite au `.snapshot` le répertoire reste autorisé même si l'option est activée.	`vserver nfs` commandes avec le `-v3-hide-snapshot` option activée

Pour en savoir plus, `vserver nfs` consultez le "Référence de commande ONTAP".

Résoudre les problèmes de service de noms pour les SVM NAS ONTAP

Lorsque les clients rencontrent des échecs d'accès en raison de problèmes de service de nom, vous pouvez utiliser le `vserver services name-service getxxbyyy` famille de commandes pour effectuer manuellement différentes recherches de services de noms et examiner les détails et les résultats de la recherche pour faciliter le dépannage.

Description de la tâche

- Pour chaque commande, vous pouvez spécifier les éléments suivants :
  - Nom du nœud ou de la machine virtuelle de stockage (SVM) à effectuer la recherche.

    Cela vous permet de tester les recherches de service de noms pour un nœud ou un SVM spécifique afin de limiter la recherche de problèmes potentiels de configuration du service de noms.

  - Indique si la source utilisée pour la recherche doit être utilisée.

    Cela vous permet de vérifier si la source correcte a été utilisée.
- ONTAP sélectionne le service pour effectuer la recherche en fonction de l'ordre de commutation de service de noms configuré.
- Ces commandes sont disponibles au niveau de privilège avancé.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour récupérer…	Utilisez la commande…
Adresse IP d'un nom d'hôte	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (Adresses IPv4 uniquement)
Membres d'un groupe par ID de groupe	`vserver services name-service getxxbyyy getgrbygid`

Membres d'un groupe par nom de groupe	`vserver services name-service getxxbyyy getgrbyname`
Liste des groupes auxquels un utilisateur appartient	`vserver services name-service getxxbyyy getgrlist`
Nom d'hôte d'une adresse IP	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (Adresses IPv4 uniquement)
Informations sur l'utilisateur par nom d'utilisateur	`vserver services name-service getxxbyyy getpwbyname` Vous pouvez tester la résolution des noms des utilisateurs RBAC en spécifiant le `-use -rbac` ens. paramètre `true`.
Informations utilisateur par ID utilisateur	`vserver services name-service getxxbyyy getpwbyuid` Vous pouvez tester la résolution des noms des utilisateurs RBAC en spécifiant le `-use-rbac` ens. paramètre `true`.
Appartenance au groupe réseau d'un client	`vserver services name-service getxxbyyy netgrp`
Appartenance à un groupe réseau d'un client à l'aide de la recherche netgroup par hôte	`vserver services name-service getxxbyyy netgrpbyhost`

L'exemple suivant montre un test de recherche DNS pour le SVM vs1 en essayant d'obtenir l'adresse IP pour l'hôte acast1.eng.example.com :

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

L'exemple suivant montre un test de recherche NIS pour le SVM vs1 en essayant de récupérer les informations utilisateur pour un utilisateur avec l'UID 501768 :

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

L'exemple suivant montre un test de recherche LDAP pour le SVM vs1 en tentant de récupérer les informations utilisateur d'un utilisateur portant le nom ldap1 :

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

L'exemple suivant montre un test de recherche de groupe réseau pour le SVM vs1 en essayant de déterminer si le client dnshost0 est membre du groupe netgroup136 :

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analysez les résultats du test que vous avez effectué et prenez les mesures nécessaires.

Si…	Vérifiez le…
La recherche de nom d'hôte ou d'adresse IP a échoué ou a produit des résultats incorrects	Configuration DNS
Recherche interrogea une source incorrecte	Nommer la configuration du commutateur de service

Si…	Vérifiez le…
La recherche d'utilisateur ou de groupe a échoué ou a produit des résultats incorrects	• Nommer la configuration du commutateur de service • Configuration source (fichiers locaux, domaine NIS, client LDAP) • Configuration du réseau (par exemple, LIFs et routes)
La recherche de nom d'hôte a échoué ou a expiré et le serveur DNS ne résout pas les noms courts DNS (par exemple, host1).	Configuration DNS pour les requêtes de domaine de premier niveau (TLD). Vous pouvez désactiver les requêtes TLD à l'aide du `-is-tld-query -enabled false` à la `vserver services name-service dns modify` commande.

Informations associées

"Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

Vérifier les connexions au service de noms pour les SVM NAS ONTAP

Vous pouvez vérifier les serveurs de noms DNS et Lightweight Directory Access Protocol (LDAP) pour vérifier qu'ils sont connectés à ONTAP. Ces commandes sont disponibles au niveau de privilège admin.

Description de la tâche

Vous pouvez vérifier que la configuration du service de noms DNS ou LDAP est valide selon les besoins à l'aide du vérificateur de configuration du service de noms. Cette vérification de validation peut être lancée en ligne de commande ou dans System Manager.

Pour les configurations DNS, tous les serveurs sont testés et doivent fonctionner pour que la configuration soit considérée comme valide. Pour les configurations LDAP, tant qu'un serveur est en service, la configuration est valide. Les commandes name service appliquent le vérificateur de configuration sauf `skip-config-validation` le champ est vrai (la valeur par défaut est faux).

Étape

1. Utiliser la commande appropriée pour vérifier la configuration du service de noms. L'interface utilisateur affiche l'état des serveurs configurés.

Pour vérifier…	Utilisez cette commande…
État de la configuration DNS	`vserver services name-service dns check`
État de la configuration LDAP	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+---------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                 |
| Client Configuration Name: c1                                |
| LDAP Status: up                                              |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                 |
```

La validation de la configuration est réussie si au moins un des serveurs configurés (name-Server/ldap-servers) est accessible et fournit le service. Un avertissement est affiché si certains serveurs sont inaccessibles.

Commandes ONTAP pour la gestion des entrées de commutateur de service de noms NAS

Vous pouvez gérer les entrées de commutateur de service de noms en les créant, en les affichant, en les modifiant et en les supprimant.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer une entrée de commutateur de service de nom	`vserver services name-service ns-switch create`
Afficher les entrées du commutateur d'entretien du nom	`vserver services name-service ns-switch show`
Modifier une entrée de commutateur de service de nom	`vserver services name-service ns-switch modify`
Supprimer une entrée de commutateur de service de nom	`vserver services name-service ns-switch delete`

Pour en savoir plus, `vserver services name-service ns-switch` consultez le "Référence de commande ONTAP".

Informations associées

"Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques

des services de noms)"

Commandes ONTAP pour la gestion du cache du service de noms NAS

Vous pouvez gérer le cache du service de noms en modifiant la valeur TTL (Time to live). La valeur TTL détermine la persistance des informations de service de noms longs dans le cache.

Si vous souhaitez modifier la valeur TTL pour…	Utilisez cette commande…
Utilisateurs UNIX	`vserver services name-service cache unix-user settings`
Groupes UNIX	`vserver services name-service cache unix-group settings`
Netgroups UNIX	`vserver services name-service cache netgroups settings`
Hôtes	`vserver services name-service cache hosts settings`
Appartenance à un groupe	`vserver services name-service cache group-membership settings`

Informations associées

"Référence de commande ONTAP"

Commandes ONTAP pour la gestion des mappages de noms NFS

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un mappage de nom	`vserver name-mapping create`
Insérez un mappage de nom à une position spécifique	`vserver name-mapping insert`
Afficher les mappages de noms	`vserver name-mapping show`

Échange de la position de deux mappages de noms REMARQUE : un échange n'est pas autorisé lorsque le mappage-noms est configuré avec une entrée de qualificatif-ip.	`vserver name-mapping swap`
Modifier un mappage de noms	`vserver name-mapping modify`
Supprime un mappage de noms	`vserver name-mapping delete`
Valider le mappage de nom correct	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Pour en savoir plus, `vserver name-mapping` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des utilisateurs UNIX locaux NAS

Il existe des commandes ONTAP spécifiques pour gérer les utilisateurs UNIX locaux.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un utilisateur UNIX local	`vserver services name-service unix-user create`
Chargement des utilisateurs UNIX locaux à partir d'un URI	`vserver services name-service unix-user load-from-uri`
Afficher les utilisateurs UNIX locaux	`vserver services name-service unix-user show`
Modifier un utilisateur UNIX local	`vserver services name-service unix-user modify`
Supprimer un utilisateur UNIX local	`vserver services name-service unix-user delete`

Pour en savoir plus, `vserver services name-service unix-user` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des groupes UNIX locaux NAS

Il existe des commandes ONTAP spécifiques pour gérer les groupes UNIX locaux.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un groupe UNIX local	`vserver services name-service unix-group create`

Ajouter un utilisateur à un groupe UNIX local	`vserver services name-service unix-group adduser`
Chargement des groupes UNIX locaux à partir d'un URI	`vserver services name-service unix-group load-from-uri`
Afficher les groupes UNIX locaux	`vserver services name-service unix-group show`
Modifier un groupe UNIX local	`vserver services name-service unix-group modify`
Supprimer un utilisateur d'un groupe UNIX local	`vserver services name-service unix-group deluser`
Supprimer un groupe UNIX local	`vserver services name-service unix-group delete`

Pour en savoir plus, `vserver services name-service unix-group` consultez le "Référence de commande ONTAP".

Limites pour les utilisateurs, groupes et membres de groupe UNIX locaux pour les SVM NFS ONTAP

ONTAP a introduit des limites au nombre maximal d'utilisateurs et de groupes UNIX dans le cluster, et des commandes pour gérer ces limites. Ces limites peuvent aider à éviter les problèmes de performances en empêchant les administrateurs de créer un trop grand nombre d'utilisateurs et de groupes UNIX locaux au sein du cluster.

Il existe une limite pour le nombre combiné de groupes d'utilisateurs UNIX locaux et de membres de groupe. Il existe une limite distincte pour les utilisateurs UNIX locaux. Les limites portent à l'échelle du cluster. Chacune de ces nouvelles limites est définie sur une valeur par défaut que vous pouvez modifier jusqu'à une limite stricte préaffectée.

Base de données	Limite par défaut	Limitation stricte
Utilisateurs UNIX locaux	32,768	65,536
Groupes UNIX locaux et membres de groupes	32,768	65,536

Gérer les limites des utilisateurs et groupes UNIX locaux pour les SVM ONTAP NFS

Il existe des commandes ONTAP spécifiques permettant de gérer les limites des utilisateurs et groupes UNIX locaux. Les administrateurs du cluster peuvent utiliser ces commandes pour résoudre les problèmes de performances qui, selon eux, seraient liés à un nombre excessif d'utilisateurs et de groupes UNIX locaux.

Description de la tâche

Ces commandes sont disponibles pour l'administrateur du cluster au niveau de privilège avancé.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Utilisez la commande…
Affiche des informations sur les limites des utilisateurs UNIX locaux	`vserver services unix-user max-limit show`
Affiche des informations sur les limites de groupe UNIX locales	`vserver services unix-group max-limit show`
Modifier les limites des utilisateurs UNIX locaux	`vserver services unix-user max-limit modify`
Modifier les limites du groupe UNIX local	`vserver services unix-group max-limit modify`

Pour en savoir plus, `vserver services unix` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des groupes de réseaux locaux NFS

Vous pouvez gérer les groupes réseau locaux en les chargeant à partir d'un URI, en vérifiant leur état sur les nœuds, en les affichant et en les supprimant.

Les fonctions que vous recherchez…	Utilisez la commande…
Charger des groupes réseau à partir d'un URI	`vserver services name-service netgroup load`
Vérifiez l'état des groupes réseau sur les nœuds	`vserver services name-service netgroup status` Disponible au niveau de privilège avancé et au niveau supérieur.
Afficher les groupes réseau locaux	`vserver services name-service netgroup file show`
Supprimer un groupe réseau local	`vserver services name-service netgroup file delete`

Pour en savoir plus, `vserver services name-service netgroup file` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations de domaine NFS NIS

Il existe des commandes ONTAP spécifiques pour gérer les configurations de domaine NIS.

Les fonctions que vous recherchez…	Utilisez cette commande…

Créez une configuration de domaine NIS	`vserver services name-service nis-domain create`
Affiche les configurations de domaine NIS	`vserver services name-service nis-domain show`
Affiche l'état de liaison d'une configuration de domaine NIS	`vserver services name-service nis-domain show-bound`
Affiche les statistiques NIS	`vserver services name-service nis-domain show-statistics` Disponible au niveau de privilège avancé et au niveau supérieur.
Effacer les statistiques NIS	`vserver services name-service nis-domain clear-statistics` Disponible au niveau de privilège avancé et au niveau supérieur.
Modifier une configuration de domaine NIS	`vserver services name-service nis-domain modify`
Supprimer une configuration de domaine NIS	`vserver services name-service nis-domain delete`
Activer la mise en cache pour les recherches netgroup-par-hôte	`vserver services name-service nis-domain netgroup-database config modify` Disponible au niveau de privilège avancé et au niveau supérieur.

Pour en savoir plus, `vserver services name-service nis-domain` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations client NFS LDAP

Il existe des commandes ONTAP spécifiques pour gérer les configurations du client LDAP.

Les administrateurs du SVM ne peuvent ni modifier ni supprimer les configurations du client LDAP créées par les administrateurs du cluster.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez une configuration client LDAP	`vserver services name-service ldap client create`
Affiche les configurations du client LDAP	`vserver services name-service ldap client show`
Modifier une configuration client LDAP	`vserver services name-service ldap client modify`

Modifiez le mot de passe DE LIAISON du client LDAP	`vserver services name-service ldap client modify-bind-password`
Supprimez une configuration client LDAP	`vserver services name-service ldap client delete`

Pour en savoir plus, `vserver services name-service ldap client` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations LDAP NFS

Il existe des commandes ONTAP spécifiques pour gérer les configurations LDAP.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez une configuration LDAP	`vserver services name-service ldap create`
Afficher les configurations LDAP	`vserver services name-service ldap show`
Modifier une configuration LDAP	`vserver services name-service ldap modify`
Supprimez une configuration LDAP	`vserver services name-service ldap delete`

Pour en savoir plus, `vserver services name-service ldap` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des modèles de schéma client LDAP NFS

Il existe des commandes ONTAP spécifiques pour gérer les modèles de schéma client LDAP.

> Les administrateurs SVM ne peuvent ni modifier ni supprimer les schémas des clients LDAP qui ont été créés par les administrateurs du cluster.

Les fonctions que vous recherchez…	Utilisez cette commande…
Copier un modèle de schéma LDAP existant	`vserver services name-service ldap client schema copy` Disponible au niveau de privilège avancé et au niveau supérieur.
Afficher les modèles de schéma LDAP	`vserver services name-service ldap client schema show`
Modifier un modèle de schéma LDAP	`vserver services name-service ldap client schema modify` Disponible au niveau de privilège avancé et au niveau supérieur.

Supprimer un modèle de schéma LDAP	`vserver services name-service ldap client schema delete` Disponible au niveau de privilège avancé et au niveau supérieur.

Pour en savoir plus, `vserver services name-service ldap client schema` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations d'interface NFS Kerberos

Il existe des commandes ONTAP spécifiques pour gérer les configurations de l'interface Kerberos NFS.

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez NFS Kerberos sur une LIF	`vserver nfs kerberos interface enable`
Affiche les configurations de l'interface Kerberos NFS	`vserver nfs kerberos interface show`
Modifiez une configuration d'interface Kerberos NFS	`vserver nfs kerberos interface modify`
Désactivation de NFS Kerberos sur une LIF	`vserver nfs kerberos interface disable`

Pour en savoir plus, `vserver nfs kerberos interface` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations de domaine NFS Kerberos

Il existe des commandes ONTAP spécifiques pour gérer les configurations de Royaume Kerberos NFS.

Les fonctions que vous recherchez…	**Utilisez cette commande…**
Créez une configuration de domaine NFS Kerberos	`vserver nfs kerberos realm create`
Affiche les configurations de domaine NFS Kerberos	`vserver nfs kerberos realm show`
Modifiez une configuration de domaine NFS Kerberos	`vserver nfs kerberos realm modify`
Supprimez une configuration de domaine NFS Kerberos	`vserver nfs kerberos realm delete`

Pour en savoir plus, `vserver nfs kerberos realm` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des politiques d'exportation

Il existe des commandes ONTAP spécifiques pour gérer les export-policies.

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les export-policy	`vserver export-policy show`
Renommez une export-policy	`vserver export-policy rename`
Copier une export-policy	`vserver export-policy copy`
Supprime une export-policy	`vserver export-policy delete`

Pour en savoir plus, `vserver export-policy` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des règles d'exportation

Il existe des commandes ONTAP spécifiques pour gérer les règles d'exportation.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer une règle d'exportation	`vserver export-policy rule create`
Affiche des informations sur les règles d'exportation	`vserver export-policy rule show`
Modifier une règle d'exportation	`vserver export-policy rule modify`
Supprimer une règle d'exportation	`vserver export-policy rule delete`

Si vous avez configuré plusieurs règles d'exportation identiques correspondant à différents clients, veillez à les garder synchronisées lors de la gestion des règles d'exportation.

Pour en savoir plus, `vserver export-policy` consultez le "Référence de commande ONTAP".

Configurez le cache des informations d'identification NFS

Raisons de la modification de la durée de vie du cache d'informations d'identification NFS pour les SVM ONTAP

ONTAP utilise un cache d'identifiants pour stocker les informations nécessaires à l'authentification utilisateur pour l'accès aux exportations NFS afin d'accélérer l'accès et d'améliorer les performances. Vous pouvez configurer la durée de stockage des informations d'identification dans le cache des informations d'identification pour les

personnaliser en fonction de votre environnement.

La modification du TTL (Time-to-Live) du cache d'identifiants NFS permet de résoudre certains problèmes. Vous devez comprendre ce que sont ces scénarios ainsi que les conséquences de ces modifications.

Raisons

Envisagez de modifier le TTL par défaut dans les cas suivants :

Problème	Action corrective
Les noms de serveurs de votre environnement subissent une dégradation des performances en raison d'une charge élevée de requêtes de ONTAP.	Augmentez le TTL des identifiants positifs et négatifs en cache afin de réduire le nombre de requêtes de ONTAP vers les serveurs de noms.
L'administrateur du serveur de noms a apporté des modifications pour autoriser l'accès aux utilisateurs NFS qui étaient précédemment refusés.	Réduisez le TTL des identifiants négatifs en cache afin de réduire le temps que les utilisateurs NFS doivent attendre que ONTAP demande de nouvelles informations d'identification à partir de serveurs de noms externes afin qu'ils puissent obtenir un accès.
L'administrateur du serveur de noms a apporté des modifications pour refuser l'accès aux utilisateurs NFS précédemment autorisés.	Réduisez le TTL des identifiants positifs qui ont été mis en cache afin de réduire le temps avant que ONTAP ne demande de nouvelles informations d'identification auprès de serveurs de noms externes, de sorte que les utilisateurs NFS ne puissent plus accéder à ces derniers.

Conséquences

Vous pouvez modifier la durée individuellement pour la mise en cache des informations d'identification positives et négatives. Cependant, vous devriez être conscient à la fois des avantages et des inconvénients de le faire.

Si…	L'avantage, c'est…	L'inconvénient est…
Augmenter la durée du cache des informations d'identification positives	ONTAP envoie moins souvent des demandes d'informations d'identification pour nommer des serveurs, ce qui réduit la charge sur les serveurs de noms.	Il faut plus de temps pour refuser l'accès aux utilisateurs NFS, mais qui étaient auparavant autorisés à y accéder.
Réduisez la durée du cache des informations d'identification positives	Le refus d'accès aux utilisateurs NFS, qui étaient auparavant autorisés, prend moins de temps.	ONTAP envoie plus fréquemment des demandes d'informations d'identification pour nommer des serveurs, ce qui augmente la charge sur les serveurs de noms.

Si…	L’avantage, c’est…	L’inconvénient est…
Augmenter la durée du cache des informations d’identification négatives	ONTAP envoie moins souvent des demandes d’informations d’identification pour nommer des serveurs, ce qui réduit la charge sur les serveurs de noms.	Il faut plus de temps pour accorder l’accès aux utilisateurs NFS qui n’étaient auparavant pas autorisés mais qui le sont maintenant.
Réduisez le temps négatif du cache des informations d’identification	Il faut moins de temps pour accorder l’accès aux utilisateurs NFS qui n’étaient auparavant pas autorisés mais qui le sont maintenant.	ONTAP envoie plus fréquemment des demandes d’informations d’identification pour nommer des serveurs, ce qui augmente la charge sur les serveurs de noms.

Configurer la durée de vie des informations d’identification utilisateur NFS mises en cache pour les SVM ONTAP

Vous pouvez configurer la durée pendant laquelle ONTAP stocke les identifiants des utilisateurs NFS dans son cache interne (TTL ou délai avant activation) en modifiant le serveur NFS de la machine virtuelle de stockage (SVM). Vous pourrez ainsi remédier à certains problèmes liés à une charge élevée sur les serveurs de noms ou à des modifications d’identifiants qui affectent l’accès des utilisateurs NFS.

Description de la tâche

Ces paramètres sont disponibles au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l’action souhaitée :

Si vous souhaitez modifier le TTL pour le cache…	Utilisez la commande…
Références positives	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` Le TTL est mesuré en millisecondes. À partir de ONTAP 9.10.1 et versions ultérieures, la valeur par défaut est 1 heure (3,600,000 millisecondes). Dans ONTAP 9.9.1 et les versions antérieures, la valeur par défaut est de 24 heures (86,400,000 millisecondes). La plage autorisée pour cette valeur est de 1 minute (60000 millisecondes) à 7 jours (604,800,000 millisecondes).

Références négatives	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` Le TTL est mesuré en millisecondes. La valeur par défaut est 2 heures (7,200,000 millisecondes). La plage autorisée pour cette valeur est de 1 minute (60000 millisecondes) à 7 jours (604,800,000 millisecondes).

3. Retour au niveau de privilège admin :

   `set -privilege admin`

Gestion des caches de règles d'exportation

Vider les caches de politique d'exportation pour les SVM NAS ONTAP

ONTAP utilise plusieurs caches de règles d'exportation pour stocker les informations relatives aux règles d'exportation afin d'accélérer les accès. Vidage manuel des caches des règles d'exportation (`vserver export-policy cache flush`) Supprime les informations potentiellement obsolètes et force ONTAP à extraire les informations actuelles des ressources externes appropriées. Cela peut aider à résoudre de nombreux problèmes liés à l'accès client aux exportations NFS.

Description de la tâche

Les informations du cache de la politique d'exportation peuvent être obsolètes pour les raisons suivantes :

- Modification récente des règles d'export-policy
- Modification récente des enregistrements de nom d'hôte dans les serveurs de noms
- Modification récente des entrées de groupe réseau dans les serveurs de noms
- Récupération suite à une panne réseau qui a empêché le chargement complet des groupes réseau

Étapes

1. Si le cache du service de noms n'est pas activé, effectuez l'une des opérations suivantes en mode privilèges avancés :

Si vous voulez rincer…	Entrez la commande…
Tous les caches des règles d'exportation (sauf showmount)	`vserver export-policy cache flush -vserver vserver_name`
Cache d'accès aux règles export-policy	`vserver export-policy cache flush -vserver vserver_name -cache access` Vous pouvez inclure l'option `-node` paramètre pour spécifier le nœud sur lequel vous souhaitez vider le cache d'accès.

Si vous voulez rincer…	Entrez la commande…
Cache de nom d'hôte	`vserver export-policy cache flush -vserver vserver_name -cache host`
Le cache netgroup	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` Le traitement des groupes réseau est intensif en ressources. Vous ne devez vider le cache netgroup que si vous essayez de résoudre un problème d'accès client causé par un groupe réseau obsolète.
Le cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Si le cache du service de nom est activé, effectuez l'une des opérations suivantes :

Si vous voulez rincer…	Entrez la commande…
Cache d'accès aux règles export-policy	`vserver export-policy cache flush -vserver vserver_name -cache access` Vous pouvez inclure l'option `-node` paramètre pour spécifier le nœud sur lequel vous souhaitez vider le cache d'accès.
Cache de nom d'hôte	`vserver services name-service cache hosts forward-lookup delete-all`
Le cache netgroup	`vserver services name-service cache netgroups ip-to-netgroup delete-all vserver services name-service cache netgroups members delete-all` Le traitement des groupes réseau est intensif en ressources. Vous ne devez vider le cache netgroup que si vous essayez de résoudre un problème d'accès client causé par un groupe réseau obsolète.
Le cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Afficher la file d'attente et le cache du groupe réseau de la politique d'exportation pour les SVM NFS ONTAP

ONTAP utilise la file d'attente du groupe réseau lors de l'importation et de la résolution des groupes réseau et utilise le cache du groupe réseau pour stocker les informations obtenues. Lors de la résolution des problèmes liés à la stratégie d'exportation netgroup, vous pouvez utiliser le `vserver export-policy netgroup queue show` et `vserver export-policy netgroup cache show` commandes permettant

d’afficher l’état de la file d’attente netgroup et le contenu du cache netgroup.

Étape

1. Effectuez l’une des opérations suivantes :

Pour afficher le groupe réseau de la export policy…	Entrez la commande…
File d’attente	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Pour en savoir plus, `vserver export-policy netgroup` consultez le "Référence de commande ONTAP".

Vérifiez si une adresse IP client est membre d’un groupe réseau ONTAP NFS

Lors du dépannage des problèmes d’accès client NFS liés aux netgroups, vous pouvez utiliser le `vserver export-policy netgroup check-membership` Commande permettant de déterminer si une adresse IP client est membre d’un certain groupe réseau.

Description de la tâche

La vérification de l’appartenance à un groupe réseau vous permet de déterminer si ONTAP est conscient qu’un client est ou non membre d’un groupe réseau. Il vous permet également de savoir si le cache ONTAP netgroup est à l’état transitoire lors de l’actualisation des informations de groupe réseau. Ces informations peuvent vous aider à comprendre pourquoi un client peut être accordé ou refusé de façon inattendue.

Étape

1. Vérifiez l’appartenance d’un groupe réseau à une adresse IP client : `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   La commande peut renvoyer les résultats suivants :

   - Le client est membre du groupe réseau.

     Cette opération a été confirmée par une analyse de recherche inversée ou une recherche netgroup-par-hôte.

   - Le client est membre du groupe réseau.

     Elle a été trouvée dans le cache du groupe réseau ONTAP.

   - Le client n’est pas membre du groupe réseau.
   - L’appartenance du client ne peut pas encore être déterminée car ONTAP actualisant actuellement la mémoire cache du groupe réseau.

Jusqu'à ce que cela soit fait, l'adhésion ne peut être explicitement exclue. Utilisez le `vserver export-policy netgroup queue show` commande permettant de surveiller le chargement du groupe réseau et de relancer la vérification une fois la vérification terminée.

Exemple

L'exemple suivant vérifie si un client avec l'adresse IP 172.17.16.72 est membre du netgroup Mercury sur la SVM vs1 :

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Optimiser les performances du cache d'accès pour les SVM ONTAP NFS

Vous pouvez configurer plusieurs paramètres afin d'optimiser le cache d'accès et trouver le juste équilibre entre les performances et la mise à jour des informations stockées dans le cache d'accès.

Description de la tâche

Lorsque vous configurez les périodes d'actualisation du cache d'accès, gardez les éléments suivants à l'esprit :

- Des valeurs plus élevées signifient que les entrées restent plus longues dans le cache d'accès.

  Ses performances sont meilleures, car ONTAP consacre moins de ressources à l'actualisation des entrées du cache d'accès. L'inconvénient est que si les règles d'export-policy changent et que les entrées de cache d'accès deviennent obsolètes, il faut donc plus de temps pour les mettre à jour. Par conséquent, il est possible que les clients qui devraient obtenir un accès soient refusés et que les clients qui devraient en être refusés aient un accès.

- Les valeurs faibles signifient que ONTAP actualise les entrées du cache d'accès plus souvent.

  L'avantage est que les entrées sont plus récentes et que les clients sont plus susceptibles d'obtenir correctement ou de refuser l'accès. L'inconvénient est que les performances sont diminueraient, car ONTAP dépense davantage de ressources lors de la mise à jour des entrées du cache d'accès.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'action souhaitée :

Pour modifier…	Entrer…
Actualiser la période pour les entrées positives	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`

Pour modifier…	Entrer…
Actualiser la période pour les entrées négatives	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Délai d'expiration pour les anciennes entrées	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Vérifiez les nouveaux paramètres :

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Gérer les verrous de fichier

En savoir plus sur le verrouillage des fichiers entre les protocoles pour les SVM ONTAP NFS

Le verrouillage de fichier est une méthode utilisée par les applications client pour empêcher un utilisateur d'accéder à un fichier précédemment ouvert par un autre utilisateur. Le mode de verrouillage des fichiers par ONTAP dépend du protocole du client.

Si le client est un client NFS, les verrouillages sont consultatifs ; si le client est un client SMB, les verrous sont obligatoires.

En raison des différences entre les verrouillages de fichiers NFS et SMB, un client NFS peut ne pas accéder à un fichier précédemment ouvert par une application SMB.

Ce qui suit se produit lorsqu'un client NFS tente d'accéder à un fichier verrouillé par une application SMB :

- Dans les volumes mixtes ou NTFS, les opérations de manipulation de fichiers telles que `rm`, `rmdir`, et `mv` Peut entraîner l'échec de l'application NFS.
- Les opérations de lecture et d'écriture NFS sont refusées par les modes SMB Deny-read et deny-write open, respectivement.
- Les opérations d'écriture NFS échouent lorsque la plage d'écriture du fichier est verrouillée par un bytelock SMB exclusif.

Dans les volumes de style de sécurité UNIX, les opérations de dissociation NFS et de renommage ignorent l'état du verrouillage SMB et permettent l'accès au fichier. Toutes les autres opérations NFS sur des volumes de type sécurité UNIX respectent l'état de verrouillage SMB.

En savoir plus sur les bits en lecture seule pour les SVM ONTAP NFS

Le bit de lecture seule est défini fichier par fichier pour indiquer si un fichier est inscriptible (désactivé) ou en lecture seule (activé).

Les clients SMB qui utilisent Windows peuvent définir un bit en lecture seule par fichier. Les clients NFS ne définissent pas de bit en lecture seule par fichier, car les clients NFS ne disposent d'aucune opération de protocole utilisant un bit en lecture seule par fichier.

ONTAP peut définir un bit en lecture seule sur un fichier lorsqu'un client SMB utilisant Windows crée ce fichier. ONTAP peut également définir un bit en lecture seule lorsqu'un fichier est partagé entre les clients NFS et les clients SMB. Certains logiciels, lorsqu'ils sont utilisés par des clients NFS et SMB, nécessitent l'activation du bit en lecture seule.

Pour que ONTAP garde les autorisations appropriées en lecture et écriture sur un fichier partagé entre les clients NFS et les clients SMB, il traite le bit en lecture seule conformément aux règles suivantes :

- NFS traite tous les fichiers dont le bit de lecture seule est activé comme s'il n'a pas de bits d'autorisation d'écriture activés.
- Si un client NFS désactive tous les bits d'autorisation d'écriture et qu'au moins un de ces bits avait été précédemment activé, ONTAP active le bit en lecture seule pour ce fichier.
- Si un client NFS active un bit d'autorisation d'écriture, ONTAP désactive le bit en lecture seule pour ce fichier.
- Si le bit de lecture seule d'un fichier est activé et qu'un client NFS tente de détecter les autorisations pour le fichier, les bits d'autorisation du fichier ne sont pas envoyés au client NFS. ONTAP envoie les bits d'autorisation au client NFS avec les bits d'autorisation d'écriture masqués.
- Si le bit de lecture seule d'un fichier est activé et qu'un client SMB désactive le bit de lecture seule, ONTAP active le bit d'autorisation d'écriture du propriétaire pour le fichier.
- Les fichiers dont le bit de lecture seule est activé sont accessibles en écriture uniquement par root.

Le bit en lecture seule interagit avec les bits de mode ACL et Unix des manières suivantes :

Lorsque le bit de lecture seule est défini sur un fichier :

- Aucune modification n'est apportée à la liste de contrôle d'accès (ACL) pour ce fichier. Les clients NFS verront la même liste de contrôle d'accès qu'avant la définition du bit de lecture seule.
- Tous les bits du mode Unix qui autorisent l'accès en écriture au fichier sont ignorés.
- Les clients NFS et SMB peuvent lire le fichier, mais ils ne peuvent pas le modifier.
- Les ACL et les bits du mode UNIX sont ignorés au profit du bit de lecture seule. Cela signifie que même si l'ACL autorise l'accès en écriture, le bit de lecture seule empêche toute modification.

Lorsque le bit de lecture seule n'est pas défini sur un fichier :

- ONTAP détermine l'accès en fonction des bits de mode ACL et UNIX.
  - Si l'ACL ou les bits du mode UNIX refusent l'accès en écriture, les clients NFS et SMB ne peuvent pas modifier le fichier.
  - Si ni les bits de mode ACL ni les bits de mode UNIX ne refusent l'accès en écriture, les clients NFS et SMB peuvent modifier le fichier.

Les modifications des autorisations liées aux fichiers sont immédiatement appliquées aux clients SMB, mais elles peuvent ne pas être immédiatement appliquées aux clients NFS si le client NFS active la mise en cache des attributs.

Découvrez en quoi ONTAP NFS et Windows diffèrent dans la gestion des verrous sur les composants du chemin de partage

Contrairement à Windows, ONTAP ne verrouille pas chaque composant du chemin d'accès à un fichier ouvert lorsque le fichier est ouvert. Ce comportement affecte également les chemins de partage SMB.

Étant donné que ONTAP ne verrouille pas chaque composant du chemin d'accès, il est possible de renommer un composant de chemin au-dessus du fichier ou du partage ouvert, ce qui peut causer des problèmes pour certaines applications ou peut rendre le chemin de partage dans la configuration SMB invalide. Cela peut rendre le partage inaccessible.

Pour éviter les problèmes causés par le changement de nom des composants du chemin d'accès, vous pouvez appliquer des paramètres de sécurité de la liste de contrôle d'accès Windows (ACL) qui empêchent les utilisateurs ou les applications de renommer les répertoires critiques.

En savoir plus sur "Comment empêcher le changement de nom des répertoires lorsque les clients y accèdent".

Afficher des informations sur les verrous pour les SVM ONTAP NFS

Vous pouvez afficher des informations sur les verrous de fichier en cours, y compris les types de verrous qui sont conservés et l'état de verrouillage, les détails sur les verrous de plage d'octets, les modes de verrouillage de sharelock, les verrous de délégation et les verrous opportunistes, et si les verrous sont ouverts avec des poignées durables ou persistantes.

Description de la tâche

L'adresse IP du client ne peut pas être affichée pour les verrouillages établis via NFS V4 ou NFS v4.1.

Par défaut, la commande affiche des informations relatives à tous les verrouillages. Vous pouvez utiliser les paramètres de la commande pour afficher des informations sur les verrous d'une machine virtuelle de stockage (SVM) spécifique ou pour filtrer les résultats de la commande par d'autres critères.

Le `vserver locks show` la commande affiche des informations sur quatre types de verrous :

- Les verrous de plage d'octets, qui verrouillent uniquement une partie d'un fichier.
- Verrous de partage, qui verrouillent les fichiers ouverts.
- Verrouillages opportunistes, qui contrôlent la mise en cache côté client sur SMB.
- Des délégations qui contrôlent la mise en cache côté client sur NFSv4.x.

En spécifiant des paramètres facultatifs, vous pouvez déterminer des informations importantes sur chaque type de verrou. Pour en savoir plus, `vserver locks show` consultez le "Référence de commande ONTAP".

Étape

1. Affiche des informations sur les verrous à l'aide de `vserver locks show` commande.

Exemples

L'exemple suivant présente un récapitulatif des informations relatives à un verrouillage NFSv4 sur un fichier avec le chemin d'accès `/vol1/file1`. Le mode d'accès de sharelock est Write-deny_none et le verrou a été accordé avec la délégation d'écriture :

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

L'exemple suivant affiche des informations détaillées sur le verrou SMB d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un descripteur durable est accordé sur le fichier avec un mode d'accès à verrouillage de partage Write-Deny_none à un client dont l'adresse IP est 10.3.1.3. Un oplock de location est accordé avec un niveau de oplock de lot :

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
```

```
                    Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Briser les verrous de fichiers pour les SVM NFS ONTAP

Lorsque des verrous de fichier empêchent l'accès client aux fichiers, vous pouvez afficher des informations sur les verrous actuellement mis en attente, puis interrompre des verrous spécifiques. Les applications de débogage sont des exemples de scénarios dans lesquels vous devrez peut-être interrompre les verrous.

Description de la tâche

```
`vserver locks break`La commande n'est disponible qu'au niveau de
privilège avancé et supérieur. Pour en savoir plus, `vserver locks break`
consultez le link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-
break.html["Référence de commande ONTAP"^].
```

Étapes

1. Pour trouver les informations dont vous avez besoin pour interrompre un verrouillage, utilisez le `vserver locks show` commande.

   Pour en savoir plus, `vserver locks show` consultez le "Référence de commande ONTAP".

2. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

3. Effectuez l'une des opérations suivantes :

Si vous voulez rompre un verrou en spécifiant…	Entrez la commande…
Le nom du SVM, le nom du volume, le nom de la LIF et le chemin de fichier	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
L'ID de verrouillage	`vserver locks break -lockid UUID`

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

Découvrez comment les filtres de première lecture et de première écriture ONTAP FPolicy fonctionnent avec NFS

Les clients NFS bénéficient d'un temps de réponse élevé lors du trafic important de requêtes en lecture/écriture lorsque FPolicy est activé à l'aide d'un serveur FPolicy externe avec des opérations de lecture/écriture sous forme d'événements surveillés. Pour les clients NFS, l'utilisation de filtres de première lecture et de première écriture dans FPolicy réduit le nombre de notifications FPolicy et améliore les performances.

Dans NFS, le client effectue des E/S sur un fichier en récupérant son descripteur. Cet descripteur peut rester valide entre les redémarrages du serveur et du client. Par conséquent, le client est libre de mettre en cache le descripteur et d'y envoyer des requêtes sans récupérer de nouveau les poignées. Dans une session ordinaire, un grand nombre de requêtes de lecture/écriture sont envoyées au serveur de fichiers. Si des notifications sont générées pour toutes ces demandes, cela peut entraîner les problèmes suivants :

- Une charge plus importante grâce à un traitement supplémentaire des notifications et des temps de réponse plus courts.
- Envoi de nombreuses notifications au serveur FPolicy même si toutes les notifications ne sont pas affectées.

Après réception de la première demande de lecture/écriture d'un client pour un fichier particulier, une entrée de cache est créée et le nombre de lectures/écritures est incrémenté. Cette requête est marquée comme opération de première lecture/écriture et un événement FPolicy est généré. Avant de planifier et de créer les filtres FPolicy pour un client NFS, il est important de connaître les principes de base du fonctionnement des filtres FPolicy.

- Première lecture : filtre les demandes de lecture du client pour la première lecture.

  Lorsque ce filtre est utilisé pour les événements NFS, le `-file-session-io-grouping-count` et `-file-session-io-grouping-duration` Les paramètres déterminent la demande de première lecture pour laquelle FPolicy est traité.

- Première écriture : filtre les demandes d'écriture du client pour la première écriture.

Lorsque ce filtre est utilisé pour les événements NFS, le `-file-session-io-grouping-count` et `-file-session-io-grouping-duration` Les paramètres déterminent la première requête d'écriture pour laquelle FPolicy a traité.

Les options suivantes sont ajoutées dans la base de données des serveurs NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modifier l'ID d'implémentation du serveur NFSv4.1 pour les SVM ONTAP

Le protocole NFSv4.1 inclut un ID de mise en œuvre du serveur qui documente le domaine, le nom et la date du serveur. Vous pouvez modifier les valeurs par défaut de l'ID d'implémentation du serveur. La modification des valeurs par défaut peut être utile, par exemple, lors de la collecte des statistiques d'utilisation ou de la résolution des problèmes d'interopérabilité. Pour plus d'informations, consultez RFC 5661.

Description de la tâche

Les valeurs par défaut des trois options sont les suivantes :

Option	Nom de l'option	Valeur par défaut
Domaine d'ID d'implémentation NFSv4.1	`-v4.1-implementation -domain`	netapp.com
Nom de l'ID de mise en œuvre NFSv4.1	`-v4.1-implementation-name`	Nom de version du cluster
Date ID mise en œuvre NFSv4.1	`-v4.1-implementation-date`	Date de version du cluster

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Si vous voulez modifier l'ID d'implémentation NFSv4.1…	Entrez la commande…
Domaine	`vserver nfs modify -v4.1 -implementation-domain domain`

Si vous voulez modifier l'ID d'implémentation NFSv4.1…	Entrez la commande…
Nom	`vserver nfs modify -v4.1 -implementation-name name`
Date	`vserver nfs modify -v4.1 -implementation-date date`

3. Retour au niveau de privilège admin :

   `set -privilege admin`

Gérer les listes de contrôle d'accès NFSv4

Découvrez les avantages de l'activation des ACL NFSv4 pour les SVM ONTAP

Il existe de nombreux avantages pour activer les listes de contrôle d'accès NFSv4.

Voici quelques-uns des avantages majeurs apportés par les ACL NFSv4 :

- Contrôle plus précis de l'accès des utilisateurs aux fichiers et aux répertoires
- Sécurité NFS renforcée
- Interopérabilité accrue avec CIFS
- Suppression de la limitation NFS de 16 groupes par utilisateur

En savoir plus sur les ACL NFSv4 pour les SVM ONTAP

Un client utilisant des listes de contrôle d'accès NFSv4 peut définir et afficher des listes de contrôle d'accès sur les fichiers et les répertoires du système. Lorsqu'un nouveau fichier ou sous-répertoire est créé dans un répertoire contenant une liste de contrôle d'accès, le nouveau fichier ou sous-répertoire hérite de toutes les entrées de contrôle d'accès (ACE) de la liste de contrôle d'accès qui ont été marquées avec les indicateurs d'héritage appropriés.

Lorsqu'un fichier ou un répertoire est créé à la suite d'une requête NFSv4, l'ACL du fichier ou répertoire résultant dépend du fait que la demande de création de fichier inclut une ACL ou uniquement les autorisations d'accès aux fichiers UNIX standard, et si le répertoire parent possède une ACL :

- Si la requête inclut une liste de contrôle d'accès, cette liste de contrôle d'accès est utilisée.
- Si la demande comprend uniquement des autorisations d'accès aux fichiers UNIX standard mais que le répertoire parent possède une ACL, les ACE de l'ACL du répertoire parent sont hérités par le nouveau fichier ou répertoire tant que les ACE ont été balisés avec les indicateurs d'héritage appropriés.

  Une ACL parent est héritée même si `-v4.0-acl` est défini sur `off`.

- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent ne dispose pas d'ACL, le mode fichier client est utilisé pour définir les autorisations d'accès aux

fichiers UNIX standard.

- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent dispose d'une ACL non héritable, le nouvel objet est créé uniquement avec des bits de mode.

> Si le `-chown-mode` paramètre a été défini sur `restricted` avec des commandes dans les `vserver nfs` familles ou `vserver export-policy rule`, la propriété du fichier ne peut être modifiée que par le superutilisateur, même si les autorisations sur disque définies avec les listes de contrôle d'accès NFSv4 permettent à un utilisateur non root de modifier la propriété du fichier. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Activer ou désactiver la modification de l'ACL NFSv4 pour les SVM ONTAP

Lorsque ONTAP reçoit un `chmod` Commande pour un fichier ou un répertoire avec une liste de contrôle d'accès, la liste de contrôle d'accès est par défaut conservée et modifiée pour refléter le changement de bit de mode. Vous pouvez désactiver le `-v4-acl -preserve` Paramètre pour modifier le comportement si vous souhaitez que la liste de contrôle d'accès soit supprimée.

Description de la tâche

Lors de l'utilisation d'un style de sécurité unifié, ce paramètre indique également si les autorisations de fichier NTFS sont conservées ou supprimées lorsqu'un client envoie une commande chmod, chgroup ou chown pour un fichier ou un répertoire.

La valeur par défaut de ce paramètre est activée.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer la conservation et la modification des listes de contrôle d'accès NFSv4 existantes (par défaut)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Désactivez la conservation et déposez les ACL NFSv4 lors du changement de bits de mode	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Découvrez comment ONTAP utilise les ACL NFSv4 pour déterminer s'il peut supprimer des fichiers

Pour déterminer s'il peut supprimer un fichier, ONTAP utilise une combinaison du bit DE SUPPRESSION du fichier et du bit DE SUPPRESSION_ENFANT du répertoire contenant. Pour plus d'informations, consultez le document NFS 4.1 RFC 5661.

Activer ou désactiver les ACL NFSv4 pour les SVM ONTAP

Pour activer ou désactiver les ACL NFSv4, vous pouvez modifier le `-v4.0-acl` et `-v4.1-acl` options. Ces options sont désactivées par défaut.

Description de la tâche

Le `-v4.0-acl` ou `-v4.1-acl` Option contrôle la définition et l'affichage des ACL NFSv4 ; elle ne contrôle pas l'application de ces listes de contrôle d'accès pour la vérification de l'accès.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Alors…
Activez les listes de contrôle d'accès NFSv4.0	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Désactivez les listes de contrôle d'accès NFSv4.0	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Activer les ACL NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Désactiver les listes de contrôle d'accès NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modifier la limite ACE maximale pour les ACL NFSv4 pour les SVM ONTAP

Vous pouvez modifier le nombre maximal d'ACE autorisés pour chaque ACL NFSv4 en modifiant le paramètre `-v4-acl-max-aces`. Par défaut, la limite est définie sur 400 ACE pour chaque ACL. L'augmentation de cette limite peut permettre de réussir la migration des données avec des listes de contrôle d'accès contenant plus de 400 ACE vers les systèmes de stockage exécutant ONTAP.

Description de la tâche

L'augmentation de cette limite peut avoir un impact sur les performances des clients accédant aux fichiers avec des listes de contrôle d'accès NFSv4.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Modifier la limite ACE maximale pour les listes de contrôle d'accès NFSv4 :

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   Plage valide de

   `max_ace_limit` est `192` à `1024`.

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Gérer les délégations de fichiers NFSv4

Activer ou désactiver les délégations de fichiers de lecture NFSv4 pour les SVM ONTAP

Pour activer ou désactiver les délégations de fichiers en lecture NFSv4, vous pouvez modifier `-v4.0-read-delegation`ou option. En activant les délégations de fichiers de lecture, vous pouvez éliminer une grande partie de la surcharge de messages associée à l'ouverture et à la fermeture des fichiers.

Description de la tâche

Par défaut, les délégations des fichiers lus sont désactivées.

L'inconvénient de l'activation des délégations de fichiers en lecture est que le serveur et ses clients doivent restaurer des délégations après le redémarrage ou le redémarrage du serveur, qu'un client redémarre ou qu'une partition réseau se produit.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Alors…
Activer les délégations des fichiers lus NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`

Activer les délégations des fichiers de lecture NFSv4.1	Saisissez la commande suivante : + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Désactiver les délégations des fichiers de lecture NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Désactiver les délégations de fichiers de lecture NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Résultat

Les options de délégation de fichiers prennent effet dès qu'elles sont modifiées. Il n'est pas nécessaire de redémarrer ou de redémarrer NFS.

Activer ou désactiver les délégations de fichiers d'écriture NFSv4 pour les SVM ONTAP

Pour activer ou désactiver les délégations de fichiers d'écriture, vous pouvez modifier le `-v4.0-write-delegation`ou option. En activant les délégations de fichiers d'écriture, vous pouvez éliminer la majeure partie des surcharges de messages associées au verrouillage des fichiers et des enregistrements, en plus de l'ouverture et de la fermeture des fichiers.

Description de la tâche

Par défaut, les délégations des fichiers d'écriture sont désactivées.

L'inconvénient de l'activation des délégations de fichiers d'écriture est que le serveur et ses clients doivent effectuer des tâches supplémentaires pour restaurer des délégations après le redémarrage ou le redémarrage du serveur, qu'un client redémarre ou qu'une partition réseau se produit.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Alors…
Activer les délégations des fichiers d'écriture NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Activer les délégations de fichiers d'écriture NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`

Les fonctions que vous recherchez…	Alors…
Désactiver les délégations des fichiers d'écriture NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Désactiver les délégations de fichiers d'écriture NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Résultat

Les options de délégation de fichiers prennent effet dès qu'elles sont modifiées. Il n'est pas nécessaire de redémarrer ou de redémarrer NFS.

Configurez le verrouillage des fichiers NFSv4 et des enregistrements

En savoir plus sur le verrouillage des fichiers et des enregistrements NFSv4 pour les SVM ONTAP

Pour les clients NFSv4, ONTAP supporte le mécanisme de verrouillage des fichiers NFSv4, tout en conservant l'état de tous les verrouillages de fichiers sous un modèle basé sur la location.

"Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"

Spécifier la période de bail de verrouillage NFSv4 pour les SVM ONTAP

Pour spécifier la période de verrouillage NFSv4 (c'est-à-dire la période pendant laquelle ONTAP accorde irrévocablement un verrouillage à un client), vous pouvez modifier le `-v4-lease-seconds` option. Des délais de location plus courts accélèrent la restauration des serveurs, tandis que des périodes de location plus longues sont avantageuses pour les serveurs qui gèrent un nombre très important de clients.

Description de la tâche

Par défaut, cette option est définie sur `30`. La valeur minimale de cette option est `10`. La valeur maximale pour cette option est le délai de grâce de verrouillage, que vous pouvez définir avec l' `locking.lease_seconds` option.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Saisissez la commande suivante :

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Spécifier la période de grâce de verrouillage NFSv4 pour les SVM ONTAP

Pour spécifier la période de grâce de verrouillage NFSv4 (c'est-à-dire le délai durant lequel les clients tentent de récupérer leur état de verrouillage à partir de ONTAP lors de la restauration du serveur), vous pouvez modifier le `-v4-grace-seconds` option.

Description de la tâche

Par défaut, cette option est définie sur `45`.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Saisissez la commande suivante :

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

En savoir plus sur les références NFSv4 pour les SVM ONTAP

Lorsque vous activez les référencements NFSv4, ONTAP fournit des référencements « intra-SVM » aux clients NFSv4. La référence intra-SVM est utilisée lorsqu'un nœud de cluster recevant la requête NFSv4 fait référence au client NFSv4 à une autre interface logique (LIF) sur la machine virtuelle de stockage (SVM).

Le client NFSv4 doit accéder au chemin qui a reçu la recommandation au niveau du LIF cible à partir de ce point. Le nœud de cluster d'origine fournit une telle recommandation lorsqu'il détermine qu'il existe une LIF dans le SVM qui réside sur le nœud de cluster sur lequel réside le volume de données, ce qui permet aux clients d'accéder plus rapidement aux données et d'éviter toute communication supplémentaire du cluster.

Activer ou désactiver les références NFSv4 pour les SVM ONTAP

Vous pouvez activer les référencements NFSv4 sur les machines virtuelles de stockage (SVM) en activant les options `-v4-fsid-change` et `-v4.0-referrals`ou. L'activation des référencements NFSV4 peut entraîner un accès plus rapide aux données pour les clients NFSv4 qui prennent en charge cette fonctionnalité.

Avant de commencer

Si vous souhaitez activer les référencements NFS, vous devez d'abord désactiver Parallel NFS. Vous ne pouvez pas activer les deux en même temps.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activez les référencements NFSv4	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Désactiver les référencements NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Activer les référencements NFSv4.1	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Désactiver les référencements NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Afficher les statistiques pour les SVM ONTAP NFS

Pour surveiller les performances et diagnostiquer les problèmes, vous pouvez afficher les statistiques NFS des serveurs virtuels de stockage (SVM) sur le système de stockage.

Étapes

1. Utilisez le `statistics catalog object show` Commande permettant d'identifier les objets NFS à partir desquels vous pouvez afficher les données.

```
statistics catalog object show -object nfs*
```

2. Utilisez le `statistics start` et en option `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

Exemple : contrôle des performances NFSv3

L'exemple suivant montre les données de performances pour le protocole NFSv3.

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui indiquent le

nombre de demandes de lecture et d'écriture réussies par rapport au nombre total de demandes de lecture et d'écriture :

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                              1492052
    write_total                                1492052
```

Informations associées

- "Configuration du contrôle des performances"
- "objet de catalogue de statistiques afficher"
- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Afficher les statistiques DNS pour les SVM ONTAP NFS

Vous pouvez afficher les statistiques DNS des ordinateurs virtuels de stockage (SVM) sur le système de stockage afin de surveiller les performances et de diagnostiquer les problèmes.

Étapes

1. Utilisez le `statistics catalog object show` Commande permettant d'identifier les objets DNS à partir desquels vous pouvez afficher les données.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Utilisez le `statistics start` et `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

Surveillance des statistiques DNS

Les exemples suivants présentent les données de performances des requêtes DNS. Les commandes suivantes permettent de lancer la collecte de données pour un nouvel échantillon :

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui affichent le nombre de requêtes DNS envoyées par rapport au nombre de requêtes DNS reçues, échouées ou expirées :

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui affichent le nombre de fois qu'une erreur spécifique a été reçue pour une requête DNS sur le serveur particulier :

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Informations associées

- "Configuration du contrôle des performances"
- "objet de catalogue de statistiques afficher"
- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Afficher les statistiques NIS pour les SVM ONTAP NFS

Pour surveiller les performances et diagnostiquer les problèmes, vous pouvez afficher les statistiques NIS des machines virtuelles de stockage (SVM) sur le système de stockage.

Étapes

1. Utilisez le `statistics catalog object show` Pour identifier les objets NIS à partir desquels vous pouvez afficher des données.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Utilisez le `statistics start` et `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

Surveillance des statistiques NIS

Les exemples suivants affichent des données de performances pour les requêtes NIS. Les commandes suivantes permettent de lancer la collecte de données pour un nouvel échantillon :

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs indiquant le nombre de requêtes NIS envoyées par rapport au nombre de requêtes NIS reçues, en échec ou en expiration :

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           1
    num_requests_sent                                              2
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs indiquant le nombre de fois où une erreur spécifique a été reçue pour une requête NIS sur le serveur particulier :

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                          YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

Informations associées

- "Configuration du contrôle des performances"
- "objet de catalogue de statistiques afficher"
- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

En savoir plus sur la prise en charge de VMware vStorage sur ONTAP NFS

ONTAP prend en charge certaines fonctionnalités VMware vStorage APIs for Array Integration (VAAI) dans un environnement NFS.

Fonctionnalités prises en charge

Les fonctionnalités suivantes sont prises en charge :

- Copie auxiliaire

  Permet à un hôte ESXi de copier des machines virtuelles ou des disques de machines virtuelles directement entre les emplacements de datastore source et de destination sans impliquer l'hôte. Cela permet d'économiser les cycles du processeur de l'hôte ESXi et la bande passante du réseau. Le déchargement des copies préserve l'efficacité de l'espace si le volume source est faible.

- Réservation d'espace

  Garantit l'espace de stockage d'un fichier VMDK en réservant de l'espace pour celui-ci.

Limites

VMware vStorage over NFS présente les limites suivantes :

- Les opérations de déchargement des copies peuvent échouer dans les scénarios suivants :
  - Lors de l'exécution de waffer sur le volume source ou de destination, car il met temporairement le volume hors ligne
  - Pendant le déplacement du volume source ou de destination
  - Lors du déplacement de LIF source ou de destination
  - Lors des opérations de basculement ou de rétablissement
  - Lors des opérations de basculement ou de rétablissement
- La copie côté serveur peut échouer en raison des différences de format de descripteur de fichier dans le scénario suivant :

  Tentative de copie des données à partir des SVM dont les qtrees n'ont pas encore été exportés vers des SVM, ou qui ont déjà été exportés. Pour contourner cette limitation, vous pouvez exporter au moins un qtree sur le SVM de destination.

Informations associées

"Quelles opérations VAAI Offloaded sont prises en charge par Data ONTAP ?"

Activer ou désactiver VMware vStorage sur ONTAP NFS

Vous pouvez activer ou désactiver la prise en charge de VMware vStorage sur NFS sur des SVM (Storage Virtual machines) à l'aide du `vserver nfs modify` commande.

Description de la tâche

Par défaut, la prise en charge de VMware vStorage over NFS est désactivée.

Étapes

1. Afficher l'état actuel de la prise en charge de vStorage pour les SVM :

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Prise en charge de VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Désactivez la prise en charge de VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Une fois que vous avez terminé

Vous devez installer le plug-in NFS pour VMware VAAI avant de pouvoir utiliser cette fonctionnalité. Pour plus d'informations, consultez *installation du plug-in NetApp NFS pour VMware VAAI*.

Informations associées

"Documentation NetApp : plug-in NetApp NFS pour VMware VAAI"

Activer ou désactiver la prise en charge de rquota sur les SVM NFS ONTAP

Le protocole de quota distant (rquota) permet aux clients NFS d'obtenir des informations de quota pour les utilisateurs à partir d'une machine distante. La prise en charge des versions de rquota varie en fonction de votre version de ONTAP.

- Rquota v1 est pris en charge dans ONTAP 9 et les versions ultérieures.
- Rquota v2 est pris en charge dans ONTAP 9.12.1 et les versions ultérieures.

  Si vous passez de rquota v1 à rquota v2, vous remarquerez peut-être une modification inattendue de votre limite de quota utilisateur. Ce changement est dû à la différence dans la façon dont le quota est calculé entre rquota v1 et rquota v2. Pour plus d'informations, consultez l'article de la base de connaissances "Pourquoi la limite de quota utilisateur a-t-elle été modifiée de façon inattendue".

Description de la tâche

Par défaut, rquota est désactivé.

Étape

1. Activer ou désactiver rquota :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer la prise en charge de rquota pour les SVM	`vserver nfs modify -vserver vserver_name -rquota enable`
Désactiver la prise en charge de rquota pour les SVM	`vserver nfs modify -vserver vserver_name -rquota disable`

Pour plus d'informations sur les quotas, reportez-vous à la section "Gestion du stockage logique".

Découvrez les améliorations des performances NFSv3 et NFSv4 et la taille de transfert TCP pour les SVM ONTAP

Vous pouvez améliorer les performances des clients NFSv3 et NFSv4 qui se connectent aux systèmes de stockage sur un réseau à latence élevée en modifiant la taille maximale du transfert TCP.

Lorsque les clients accèdent aux systèmes de stockage sur un réseau à latence élevée, tel qu'un réseau WAN (Wide Area Network) ou un réseau MAN (Metro Area Network) avec une latence supérieure à 10 millisecondes, vous pouvez améliorer les performances de connexion en modifiant la taille maximale du transfert TCP. Les clients qui accèdent aux systèmes de stockage dans un réseau à faible latence, tel qu'un réseau local (LAN), ne peuvent guère bénéficier de la modification de ces paramètres. Si l'amélioration du débit ne l'emporte pas sur l'impact sur la latence, vous ne devez pas utiliser ces paramètres.

Pour déterminer si votre environnement de stockage peut tirer parti de la modification de ces paramètres, vous devez d'abord effectuer une évaluation complète des performances d'un client NFS peu performant. Vérifiez si

les faibles performances sont à cause d'une latence aller-retour excessive et d'une petite demande sur le client. Dans ces conditions, le client et le serveur ne peuvent pas utiliser pleinement la bande passante disponible parce qu'ils passent la majorité de leurs cycles de service en attente de petites demandes et réponses à transmettre par le biais de la connexion.

En augmentant la taille des requêtes NFSv3 et NFSv4, le client et le serveur peuvent utiliser la bande passante disponible plus efficacement pour déplacer plus de données par unité de temps, ce qui accroît l'efficacité globale de la connexion.

N'oubliez pas que la configuration entre le système de stockage et le client peut varier. Le système de stockage et le client prennent en charge une taille maximale de 1 Mo pour les opérations de transfert. Cependant, si vous configurez le système de stockage pour prendre en charge une taille de transfert maximale de 1 Mo mais que le client ne prend en charge que 64 Ko, la taille de transfert de montage est limitée à 64 Ko ou moins.

Avant de modifier ces paramètres, notez qu'il entraîne une consommation de mémoire supplémentaire sur le système de stockage pendant la durée nécessaire à l'assemblage et à la transmission d'une réponse importante. Plus les connexions à latence élevée sont nombreuses, plus la consommation de mémoire supplémentaire augmente. Les systèmes de stockage dont la capacité de mémoire est élevée ne subissent que très peu d'effet. Les systèmes de stockage dont la capacité de mémoire est faible peuvent constater une dégradation notable des performances.

La réussite de l'utilisation de ces paramètres repose sur la capacité à récupérer les données provenant de plusieurs nœuds d'un cluster. La latence inhérente au réseau du cluster peut augmenter la latence globale de la réponse. La latence globale a tendance à augmenter lors de l'utilisation de ces paramètres. Ainsi, les charges de travail sensibles à la latence peuvent avoir un impact négatif.

Modifier la taille de transfert maximale TCP NFSv3 et NFSv4 pour les SVM ONTAP

Vous pouvez modifier le `-tcp-max-xfer-size` Option permettant de configurer les tailles de transfert maximales pour toutes les connexions TCP en utilisant les protocoles NFSv3 et NFSv4.x.

Description de la tâche

Vous pouvez modifier ces options individuellement pour chaque serveur virtuel de stockage (SVM).

À partir de ONTAP 9, le `v3-tcp-max-read-size` et `v3-tcp-max-write-size` les options sont obsolètes. Vous devez utiliser le `-tcp-max-xfer-size` à la place.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Modifier la taille maximale du transfert TCP NFSv3 ou NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Option	Gamme	Valeur par défaut
`-tcp-max-xfer-size`	8192 à 1048576 octets	65536 octets

> La taille de transfert maximale que vous saisissez doit être un multiple de 4 Ko (4096 octets). Les demandes qui ne sont pas correctement alignées ont un impact négatif sur les performances.

3. Utilisez le `vserver nfs show -fields tcp-max-xfer-size` pour vérifier les modifications.
4. Si des clients utilisent des montages statiques, démontez et remontez la nouvelle taille de paramètre pour prendre effet.

Exemple

La commande suivante définit la taille maximale du transfert NFSv3 et NFSv4.x TCP à 1048576 octets sur le SVM nommé vs1 :

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configurer le nombre d'ID de groupe autorisés pour les utilisateurs NFS pour les SVM ONTAP

Par défaut, ONTAP prend en charge jusqu'à 32 ID de groupe lors du traitement des informations d'identification des utilisateurs NFS à l'aide de l'authentification Kerberos (RPCSEC_GSS). Lors de l'utilisation de l'authentification AUTH_SYS, le nombre maximal par défaut d'ID de groupe est de 16, comme défini dans RFC 5531. Vous pouvez augmenter le maximum jusqu'à 1,024 si vous avez des utilisateurs qui sont membres de plus que le nombre par défaut de groupes.

Description de la tâche

Si un utilisateur a plus que le nombre par défaut d'ID de groupe dans ses informations d'identification, les ID de groupe restants sont tronqués et l'utilisateur peut recevoir des erreurs lorsqu'il tente d'accéder aux fichiers du système de stockage. Vous devez définir le nombre maximal de groupes par SVM sur un nombre qui représente le maximum de groupes dans votre environnement.

> Pour comprendre les conditions préalables à l'authentification AUTH_SYS pour l'activation des groupes étendus (`-auth-sys-extended-groups`) qui utilisent des ID de groupe au-delà du maximum par défaut de 16, reportez-vous à cet article de la base de connaissances : "Quels sont les prérequis pour l'activation de auth-sys-extended-groups ?"

Le tableau suivant montre les deux paramètres du `vserver nfs modify` Commande qui détermine le nombre maximal d'ID de groupe dans trois exemples de configuration :

Paramètres	Paramètres	Limite des ID de groupe résultant

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Il s'agit des paramètres par défaut.
		RPCSEC_GSS : 32
		
		AUTH_SYS : 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS : 256
		
		AUTH_SYS : 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS : 512
		
		AUTH_SYS : 512

Étapes

1. Définissez le niveau de privilège sur avancé :

   `set -privilege advanced`

2. Effectuez l'action souhaitée :

Si vous souhaitez définir le nombre maximum de groupes auxiliaires autorisés…	Entrez la commande…
Uniquement pour RPCSEC_GSS et laisser AUTH_SYS à la valeur par défaut 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Pour RPCSEC_GSS et AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Vérifiez le `-extended-groups-limit` Et vérifier si AUTH_SYS utilise des groupes étendus : `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Retour au niveau de privilège admin :

   `set -privilege admin`

Exemple

L'exemple suivant active les groupes étendus pour l'authentification AUTH_SYS et définit le nombre maximal de groupes étendus sur 512 pour l'authentification AUTH_SYS et RPCSEC_GSS. Ces modifications sont effectuées uniquement pour les clients qui accèdent à la SVM nommée vs1 :

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Informations associées

- Article de la base de connaissance : "AUTH_SYS modifications des groupes étendus pour l'authentification NFS pour ONTAP 9"

Contrôler l'accès des utilisateurs root aux données de style sécurité NTFS pour les SVM ONTAP

Vous pouvez configurer ONTAP de manière à permettre aux clients NFS d'accéder aux données de type sécurité NTFS et aux clients NTFS pour accéder aux données de type sécurité NFS. Lorsque vous utilisez le style de sécurité NTFS dans un magasin de données NFS, vous devez décider comment traiter l'accès par l'utilisateur root et configurer la machine virtuelle de stockage (SVM) en conséquence.

Description de la tâche

Lorsqu'un utilisateur root accède aux données de style de sécurité NTFS, vous disposez de deux options :

- Mappez l'utilisateur root à un utilisateur Windows comme tout autre utilisateur NFS et gérez l'accès en fonction des listes de contrôle d'accès NTFS.
- Ignorez les listes de contrôle d'accès NTFS et offrez un accès complet à la racine.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'action souhaitée :

Si vous voulez que l'utilisateur root…	Entrez la commande…
Être mappé à un utilisateur Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`

Ignorer la vérification de la liste de contrôle d'accès NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

Par défaut, ce paramètre est désactivé.

Si ce paramètre est activé mais qu'il n'y a pas de mappage de noms pour l'utilisateur root, ONTAP utilise les informations d'identification d'administrateur SMB par défaut pour l'audit.

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Versions NFS et clients pris en charge

En savoir plus sur les versions et les clients ONTAP NFS pris en charge

Avant d'utiliser NFS dans votre réseau, vous devez connaître les versions NFS et les clients pris en charge par ONTAP.

Ce tableau indique lorsque des versions majeures et mineures des protocoles NFS sont prises en charge par défaut dans ONTAP. Par défaut, la prise en charge n'indique pas qu'il s'agit de la version la plus ancienne de ONTAP prenant en charge ce protocole NFS.

Version	Pris en charge	Introduction
NFSv3	Oui.	Toutes les versions de ONTAP
NFSv4.0	Oui.	ONTAP 8
NFSv4.1	Oui.	ONTAP 8,1
NFSv4.2	Oui.	ONTAP 9.8
PNFS	Oui.	ONTAP 8,1

Pour obtenir les dernières informations sur les clients NFS pris en charge par ONTAP, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

En savoir plus sur la prise en charge ONTAP pour la fonctionnalité NFSv4.0

ONTAP prend en charge toutes les fonctionnalités obligatoires dans NFSv4.0, à l'exception des mécanismes de sécurité SPKM3 et LIPKEY.

Les fonctionnalités NFSV4 suivantes sont prises en charge :

- **COMPOSÉ**

Permet à un client de demander plusieurs opérations de fichier dans une seule demande RPC (Remote Procedure Call).

- **Délégation de fichiers**

  Permet au serveur de déléguer le contrôle de fichiers à certains types de clients pour l'accès en lecture et en écriture.

- **Pseudo-fs**

  Utilisé par les serveurs NFSv4 pour déterminer les points de montage sur le système de stockage. Il n'y a pas de protocole de montage dans NFSv4.

- **Verrouillage**

  Basé sur la location. Il n'existe pas de protocoles NLM (Network Lock Manager) ou NSM (Network Status Monitor) distincts dans NFSv4.

Pour plus d'informations sur le protocole NFSv4.0, voir RFC 3530.

En savoir plus sur les limitations de prise en charge ONTAP pour NFSv4

Vous devez tenir compte de plusieurs restrictions liées à la prise en charge de ONTAP pour NFSv4.

- La fonction de délégation n'est pas prise en charge par tous les types de clients.
- Dans ONTAP 9.4 et versions antérieures, le système de stockage rejette les noms comportant des caractères non ASCII sur des volumes autres que les volumes UTF8.

  Dans ONTAP 9.5 et versions ultérieures, les volumes créés avec le paramètre de langue utf8mb4 et montés via NFS v4 ne sont plus soumis à cette restriction.

- Tous les descripteurs de fichier sont persistants ; le serveur ne fournit pas de descripteurs de fichier volatiles.
- La migration et la réplication ne sont pas prises en charge.
- Les clients NFSv4 ne sont pas pris en charge par les miroirs de partage de charge en lecture seule.

  ONTAP achemine les clients NFSv4 vers la source du miroir de partage de charge pour un accès en lecture et en écriture directs.

- Les attributs nommés ne sont pas pris en charge.
- Tous les attributs recommandés sont pris en charge, à l'exception des éléments suivants :
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`

- quota_used
- system
- time_backup

> Même s'il ne prend pas en charge le `quota*` Attributs, ONTAP prend en charge les quotas d'utilisateurs et de groupes via le protocole de bande latérale RQUOTA.

En savoir plus sur la prise en charge ONTAP pour NFSv4.1

Depuis ONTAP 9.8, la fonctionnalité nconnect est disponible par défaut lorsque NFSv4.1 est activé.

Les implémentations de clients NFS antérieures n'utilisent qu'une connexion TCP unique avec un montage. En ONTAP, une connexion TCP unique peut former un goulot d'étranglement lorsque le nombre d'IOPS augmente.

Cependant, un client compatible nconnect peut avoir plusieurs connexions TCP (jusqu'à 16) associées à un seul montage NFS. NConnect utilise une seule adresse IP et établit plusieurs connexions TCP sur cette même adresse IP pour monter l'exportation NFS. Ce type de client NFS distribue les opérations de fichiers sur plusieurs connexions TCP de manière circulaire, ce qui permet d'obtenir un débit plus élevé à partir de la bande passante réseau disponible. NConnect est recommandé uniquement pour les montages NFS v3 et NFS v4.1.

Consultez la documentation de votre client NFS pour vérifier si nconnect est pris en charge dans la version de votre client.

NFSv4.1 est activé par défaut dans ONTAP 9.9.1 et versions ultérieures. Dans les versions antérieures, vous pouvez l'activer en spécifiant le `-v4.1` et le définir sur `enabled` Lors de la création d'un serveur NFS sur la machine virtuelle de stockage (SVM).

ONTAP ne prend pas en charge les délégations au niveau des fichiers et des répertoires NFSv4.1.

En savoir plus sur la prise en charge ONTAP pour NFSv4.2

À partir de ONTAP 9.8, ONTAP prend en charge le protocole NFSv4.2 pour permettre l'accès aux clients compatibles NFSv4.2.

NFSv4.2 est activé par défaut dans ONTAP 9.9.1 et versions ultérieures. Dans ONTAP 9.8, vous devez activer manuellement la version 4.2 en spécifiant le `-v4.1` et le définir sur `enabled` Lors de la création d'un serveur NFS sur la machine virtuelle de stockage (SVM). L'activation de NFSv4.1 permet également aux clients d'utiliser les fonctionnalités NFSv4.1 lorsqu'ils sont montés en tant que v4.2.

Les versions successives de ONTAP étendent la prise en charge des fonctionnalités facultatives NFSv4.2.

À commencer par…	NFSv4.2 fonctionnalités facultatives comprennent …
ONTAP 9.12.1	• Attributs étendus NFS • Fichiers épars • Réservations d'espace
ONTAP 9.9.1	Contrôle d'accès obligatoire (MAC) nommé NFS

Étiquettes de sécurité NFS v4.2

Depuis ONTAP 9.9.1, les étiquettes de sécurité NFS peuvent être activées. Ils sont désactivés par défaut.

Avec les étiquettes de sécurité NFS v4.2, les serveurs NFS ONTAP prennent en charge le contrôle d'accès obligatoire (MAC), en stockant et en récupérant les attributs sec_label envoyés par les clients.

Pour plus d'informations, voir "RFC 7240".

Depuis la version ONTAP 9.12.1, les étiquettes de sécurité NFS v4.2 sont prises en charge pour les opérations de dump NDMP. Si des étiquettes de sécurité sont rencontrées sur des fichiers ou des répertoires dans des versions antérieures, le vidage échoue.

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Activer les étiquettes de sécurité :

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Attributs étendus NFS

Depuis ONTAP 9.12.1, les attributs étendus NFS (xattrs) sont activés par défaut.

Les attributs étendus sont des attributs NFS standard définis par "RFC 8276" Et compatible avec les clients NFS modernes. Elles peuvent servir à associer des métadonnées définies par l'utilisateur à des objets de système de fichiers et présentent un intérêt dans des déploiements de sécurité avancés.

Les attributs étendus NFS ne sont actuellement pas pris en charge pour les opérations de dump NDMP. Si des attributs étendus sont rencontrés sur des fichiers ou des répertoires, le vidage procède mais ne sauvegarde pas les attributs étendus sur ces fichiers ou répertoires.

Si vous devez désactiver les attributs étendus, utilisez le `vserver nfs modify -v4.2-xattrs disabled` commande.

En savoir plus sur la prise en charge ONTAP pour NFS parallèle

ONTAP prend en charge Parallel NFS (pNFS). Le protocole pNFS améliore les

performances en offrant aux clients un accès direct aux données d'un ensemble de fichiers distribués sur plusieurs nœuds d'un cluster. Elle aide les clients à trouver le chemin optimal vers un volume.

En savoir plus sur les montages matériels ONTAP NFS

Lors du dépannage des problèmes de montage, veillez à utiliser le type de montage approprié. NFS prend en charge deux types de montage : les montages souples et les montages durs. Pour des raisons de fiabilité, n'utilisez que des supports durs.

Vous ne devez pas utiliser de montages souples, en particulier en cas de retards NFS fréquents. Ces délais peuvent entraîner la corruption des données.

Dépendances de nommage des fichiers et des répertoires NFS et SMB

En savoir plus sur les dépendances de nommage des fichiers et des répertoires ONTAP NFS et SMB

Les conventions d'appellation des fichiers et des répertoires dépendent à la fois des systèmes d'exploitation des clients réseau et des protocoles de partage de fichiers, en plus des paramètres de langue sur le cluster ONTAP et les clients.

Le système d'exploitation et les protocoles de partage de fichiers déterminent ce qui suit :

- Caractères un nom de fichier peut utiliser
- Sensibilité à la casse d'un nom de fichier

ONTAP prend en charge les caractères multi-octets dans les noms de fichier, de répertoire et de qtree, en fonction de la version de ONTAP utilisée.

Découvrez les caractères valides dans différents systèmes d'exploitation pour les SVM ONTAP NFS

Si vous accédez à un fichier ou à un répertoire à partir de clients ayant différents systèmes d'exploitation, vous devez utiliser des caractères valides dans les deux systèmes d'exploitation.

Par exemple, si vous utilisez UNIX pour créer un fichier ou un répertoire, n'utilisez pas de deux-points (:) dans le nom car le deux-points n'est pas autorisé dans les noms de fichiers ou de répertoires MS-DOS. Comme les restrictions sur les caractères valides varient d'un système d'exploitation à l'autre, consultez la documentation de votre système d'exploitation client pour plus d'informations sur les caractères interdits.

En savoir plus sur la sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole ONTAP NFS

Les noms de fichiers et de répertoires sont sensibles à la casse pour les clients NFS et non sensibles à la casse, mais ils préservent la casse pour les clients SMB. Vous devez comprendre les implications dans un environnement multiprotocole et les actions nécessaires lorsque vous spécifiez le chemin lors de la création des partages SMB et lors de l'accès aux données au sein des partages.

Si un client SMB crée un répertoire nommé `testdir`, Les clients SMB et NFS affichent le nom de fichier

comme `testdir`. Toutefois, si un utilisateur SMB tente par la suite de créer un nom de répertoire `TESTDIR`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un répertoire nommé `TESTDIR`, Les clients NFS et SMB affichent le nom du répertoire différemment, comme suit :

- Sur les clients NFS, vous voyez les deux noms de répertoire tels qu'ils ont été créés, par exemple `testdir` et `TESTDIR`, car les noms de répertoire sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour faire la distinction entre les deux répertoires. Un répertoire porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux répertoires supplémentaires.
  - Sur les clients SMB, vous voyez `testdir` et `TESTDI~1`.
  - ONTAP crée le `TESTDI~1` nom du répertoire pour différencier les deux répertoires.

    Dans ce cas, vous devez utiliser le nom 8.3 lorsque vous spécifiez un chemin de partage lors de la création ou de la modification d'un partage sur un SVM (Storage Virtual machine).

De la même manière pour les fichiers, si un client SMB crée `test.txt`, Les clients SMB et NFS affichent le nom de fichier comme `text.txt`. Toutefois, si un utilisateur SMB tente par la suite de le créer `Test.txt`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un fichier nommé `Test.txt`, Les clients NFS et SMB affichent le nom de fichier différemment, comme suit :

- Sur les clients NFS, les deux noms de fichiers sont ceux qu'ils ont créés, `test.txt` et `Test.txt`, car les noms de fichiers sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour distinguer les deux fichiers. Un fichier porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux fichiers supplémentaires.
  - Sur les clients SMB, vous voyez `test.txt` et `TEST~1.TXT`.
  - ONTAP crée le `TEST~1.TXT` nom de fichier pour différencier les deux fichiers.

> Si un mappage de caractères a été créé à l'aide des commandes de mappage de caractères CIFS du Vserver, une recherche Windows qui ne serait normalement pas sensible à la casse peut être sensible à la casse. Cela signifie que les recherches de nom de fichier ne seront sensibles à la casse que si le mappage de caractères a été créé et que le nom de fichier utilise ce mappage de caractères.

En savoir plus sur la création de noms de fichiers et de répertoires ONTAP NFS

ONTAP crée et conserve deux noms pour les fichiers ou les répertoires de tout répertoire ayant accès à partir d'un client SMB : le nom long et le nom d'origine au format 8.3.

Pour les noms de fichier ou de répertoire dépassant le nom de huit caractères ou la limite d'extension de trois caractères (pour les fichiers), ONTAP génère un nom de format 8.3 comme suit :

- Il tronque le nom de fichier ou de répertoire d'origine à six caractères, si le nom dépasse six caractères.
- Il ajoute un tilde (~) et un nombre, un à cinq, aux noms de fichier ou de répertoire qui ne sont plus uniques après être tronqués.

  S'il manque des nombres parce qu'il y a plus de cinq noms similaires, il crée un nom unique qui n'a aucune relation avec le nom original.

- Dans le cas des fichiers, il tronque l'extension du nom de fichier à trois caractères.

Par exemple, si un client NFS crée un fichier nommé `specifications.html`, Le nom de fichier au format 8.3 créé par ONTAP est `specif~1.htm`. Si ce nom existe déjà, ONTAP utilise un numéro différent à la fin du nom du fichier. Par exemple, si un client NFS crée un autre fichier nommé `specifications_new.html`, le format 8.3 de `specifications_new.html` est `specif~2.htm`.

En savoir plus sur la gestion ONTAP NFS des noms de fichiers, de répertoires et de qtree multi-octets

À partir de ONTAP 9.5, la prise en charge des noms codés UTF-8 de 4 octets permet la création et l'affichage des noms de fichier, de répertoire et d'arborescence qui incluent des caractères supplémentaires Unicode à l'extérieur du plan multilingue de base (BMP). Dans les versions précédentes, ces caractères supplémentaires ne s'affichent pas correctement dans les environnements multiprotocoles.

Pour activer la prise en charge des noms codés UTF-8 à 4 octets, un nouveau code de langue *utf8mb4* est disponible pour l' `vserver` et `volume` familles de commandement.

- Vous devez créer un volume de l'une des manières suivantes :
- Réglage du volume `-language` explicitement option :

```
volume create -language utf8mb4 {…}
```

- Hériter du volume `-language` Option d'un SVM qui a été créé avec ou modifié pour l'option :

```
vserver [create|modify] -language utf8mb4 {…}``volume create {…}
```

- Si vous utilisez ONTAP 9.6 et des versions antérieures, vous ne pouvez pas modifier les volumes existants pour le support utf8mb4 ; vous devez créer un nouveau volume prêt à utf8mb4, puis migrer les données à l'aide d'outils de copie basés sur le client.

  Si vous utilisez ONTAP 9.7P1 ou une version ultérieure, vous pouvez modifier les volumes existants pour utf8mb4 avec une demande de support. Pour plus d'informations, voir "Est-il possible de modifier la langue du volume après sa création dans ONTAP ?".

  Vous pouvez mettre à jour les SVM pour la prise en charge de utf8mb4, mais les volumes existants conservent leurs codes de langue d'origine.

> Les noms de LUN portant des caractères UTF-8 de 4 octets ne sont pas pris en charge actuellement.

- Les données de caractères Unicode sont généralement représentées dans les applications de systèmes de fichiers Windows utilisant le format de transformation Unicode 16 bits (UTF-16) et dans les systèmes de fichiers NFS utilisant le format de transformation Unicode 8 bits (UTF-8).

  Dans les versions antérieures à ONTAP 9.5, les noms, y compris les caractères supplémentaires UTF-16 créés par les clients Windows, étaient correctement affichés sur d'autres clients Windows mais n'étaient pas traduits correctement en UTF-8 pour les clients NFS. De même, les noms comportant des caractères supplémentaires UTF-8 par les clients NFS créés n'ont pas été correctement traduits en UTF-16 pour les clients Windows.

- Lorsque vous créez des noms de fichier sur des systèmes exécutant ONTAP 9.4 ou une version antérieure contenant des caractères supplémentaires valides ou non valides, ONTAP rejette le nom de fichier et renvoie une erreur de nom de fichier non valide.

  Pour éviter ce problème, utilisez uniquement des caractères BMP dans les noms de fichiers et évitez d'utiliser des caractères supplémentaires, ou mettez à niveau vers ONTAP 9.5 ou version ultérieure.

Les caractères Unicode sont autorisés dans les noms de qtree.

- Vous pouvez utiliser le `volume qtree` Famille de commandes ou System Manager pour définir ou modifier les noms des qtree.
- Les noms des qtrees peuvent inclure des caractères multi-octets au format Unicode, comme les caractères japonais et chinois.
- Dans les versions antérieures à ONTAP 9.5, seuls les caractères BMP (c'est-à-dire ceux qui pouvaient être représentés en 3 octets) étaient pris en charge.

> Dans les versions antérieures à ONTAP 9.5, le Junction-path du volume parent du qtree peut contenir des noms de qtree et de répertoire avec des caractères Unicode. Le `volume show` La commande affiche ces noms correctement lorsque le volume parent a un paramètre de langue UTF-8. Cependant, si la langue du volume parent n'est pas l'un des paramètres de langue UTF-8, certaines parties du chemin de jonction sont affichées à l'aide d'un nom de remplacement NFS numérique.

- Dans les versions 9.5 et ultérieures, les noms des qtree prennent en charge des caractères de 4 octets, à condition que le qtree se trouve dans un volume activé pour utf8m4.

Configurer le mappage de caractères pour la traduction des noms de fichiers SMB sur les volumes ONTAP NFS

Les clients NFS peuvent créer des noms de fichiers contenant des caractères non valides pour les clients SMB et certaines applications Windows. Vous pouvez configurer le mappage de caractères pour la conversion de noms de fichiers sur des volumes pour permettre aux clients SMB d'accéder aux fichiers avec des noms NFS qui ne seraient autrement pas valides.

Description de la tâche

Lorsque les fichiers créés par des clients NFS sont accessibles par des clients SMB, ONTAP recherche le nom du fichier. Si le nom n'est pas un nom de fichier SMB valide (par exemple, s'il comporte un caractère «`:`") inclus, ONTAP renvoie le nom de fichier 8.3 qui est conservé pour chaque fichier. Cependant, cela cause des problèmes pour les applications qui codent des informations importantes dans des noms de fichiers longs.

Par conséquent, si vous partagez un fichier entre des clients sur des systèmes d'exploitation différents, vous devez utiliser des caractères dans les noms de fichiers valides dans les deux systèmes d'exploitation.

Cependant, si vous avez des clients NFS qui créent des noms de fichier contenant des caractères qui ne sont pas des noms de fichier valides pour les clients SMB, vous pouvez définir une carte qui convertit les caractères NFS non valides en caractères Unicode acceptés par SMB et certaines applications Windows. Par exemple, cette fonctionnalité prend en charge les applications CATIA MCAD et Mathematica, ainsi que d'autres applications qui ont cette exigence.

Vous pouvez configurer le mappage de caractères sur une base volume par volume.

Lors de la configuration du mappage de caractères sur un volume, vous devez garder à l'esprit les éléments suivants :

- Le mappage de caractères n'est pas appliqué à travers les points de jonction.

  Vous devez configurer explicitement le mappage de caractères pour chaque volume de jonction.

- Vous devez vous assurer que les caractères Unicode utilisés pour représenter des caractères non valides ou illégaux sont des caractères qui n'apparaissent normalement pas dans les noms de fichiers ; sinon, des mappages indésirables se produisent.

  Par exemple, si vous essayez de mapper un deux-points (:) à un tiret (-) mais que le tiret (-) a été utilisé correctement dans le nom de fichier, un client Windows essayant d'accéder à un fichier nommé ""a-b" aurait sa demande mappée au nom NFS de ""a:b" (pas le résultat souhaité).

- Après l'application du mappage de caractères, si le mappage contient toujours un caractère Windows non valide, ONTAP revient aux noms de fichier Windows 8.3.
- Dans les notifications FPolicy, les journaux d'audit NAS et les messages de suivi de sécurité, les noms de fichiers mappés sont affichés.
- Lors de la création d'une relation SnapMirror de type DP, le mappage de caractères du volume source n'est pas répliqué sur le volume DP de destination.
- Sensibilité à la casse : comme les noms Windows mappés se transforment en noms NFS, la recherche des noms suit la sémantique NFS. Ainsi, les recherches NFS sont sensibles à la casse. Cela signifie que les applications qui accèdent aux partages mappés ne doivent pas se fier au comportement non sensible à la casse de Windows. Cependant, le nom 8.3 est disponible, et cela n'est pas sensible à la casse.
- Mappages partiels ou non valides : après le mappage d'un nom pour revenir aux clients faisant une énumération de répertoire (« dir »), le nom Unicode obtenu est vérifié pour la validité de Windows. Si ce nom contient toujours des caractères non valides ou s'il n'est pas valide pour Windows (par exemple, il se termine par "." ou vierge), le nom 8.3 est renvoyé à la place du nom non valide.

Étape

1. Configurer le mappage de caractères :

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   Le mappage se compose d'une liste de paires de caractères source-cible séparées par «»:». Les caractères sont des caractères Unicode saisis à l'aide de chiffres hexadécimaux. Par exemple : 3C:E03C.

   La première valeur de chaque `mapping_text` La paire séparée par deux-points est la valeur hexadécimale du caractère NFS que vous souhaitez traduire, et la seconde est la valeur Unicode utilisée par SMB. Les paires de mappage doivent être uniques (un mappage un-à-un doit exister).

   - Mappage de source

     Le tableau suivant montre le jeu de caractères Unicode autorisé pour le mappage de source :

Caractère Unicode	Caractère imprimé	Description
0x01-0x19	Sans objet	Caractères de contrôle sans impression

0x5C	\	Barre oblique inversée
0x3A	:	Deux-points
0x2A	*	Astérisque
0x3F	?	Point d'interrogation
0x22	«	Devis
0x3C	<	Inférieur à
0x3E	>	Supérieur à
0x7C		
Ligne verticale	0xb1	±

◦ Mappage de cible

Vous pouvez spécifier des caractères cibles dans la « zone d'utilisation privée » d'Unicode dans la plage suivante : U+E0000…U+F8FF.

Exemple

La commande suivante crée un mappage de caractères pour un volume nommé « `dates' » sur la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Commandes ONTAP NFS pour la gestion des mappages de caractères pour la traduction des noms de fichiers SMB

Vous pouvez gérer le mappage de caractères en créant, en modifiant, en affichant des informations sur et en supprimant des mappages de caractères de fichiers utilisés pour la conversion de noms de fichiers SMB sur des volumes FlexVol.

Les fonctions que vous recherchez…	Utilisez cette commande…

Créer de nouveaux mappages de caractères de fichier	`vserver cifs character-mapping create`
Affiche des informations sur les mappages de caractères de fichier	`vserver cifs character-mapping show`
Modifier les mappages de caractères de fichier existants	`vserver cifs character-mapping modify`
Supprimer les mappages de caractères de fichier	`vserver cifs character-mapping delete`

Pour en savoir plus, `vserver cifs character-mapping` consultez le "Référence de commande ONTAP".

Gérer l'agrégation NFS

En savoir plus sur l'agrégation de liens ONTAP NFS

À partir de ONTAP 9.14.1, les clients NFSv4.1 peuvent exploiter la mise en circuit de session pour ouvrir plusieurs connexions à différentes LIF sur le serveur NFS, augmentant ainsi la vitesse du transfert de données et fournissant de la résilience via les chemins d'accès multiples.

L'agrégation est avantageuse pour l'exportation de volumes FlexVol vers des clients compatibles avec l'agrégation, en particulier des clients VMware et Linux, ou pour NFS via RDMA, TCP ou pNFS.

Dans ONTAP 9.14.1, la mise en circuits est limitée aux LIF sur un seul nœud ; la mise en circuits ne peut pas couvrir des LIF sur plusieurs nœuds.

Les volumes FlexGroup sont pris en charge pour l'agrégation. Bien que cela puisse fournir de meilleures performances, l'accès multivoie à un volume FlexGroup ne peut être configuré que sur un seul nœud.

Dans cette version, seule la mise en circuit de session est prise en charge pour les chemins d'accès multiples.

Comment utiliser l'agrégation

Pour tirer parti des avantages des chemins d'accès multiples offerts par l'agrégation, vous devez disposer d'un ensemble de LIF, appelé *trunking group*, associées au SVM contenant un serveur NFS à ressources partagées. Les LIF d'un groupe à trunking doivent avoir des ports home sur le même nœud du cluster, et elles doivent résider sur ces ports home. Il est recommandé que toutes les LIFs d'un groupe à ressources partagées appartiennent au même groupe de basculement.

ONTAP prend en charge jusqu'à 16 connexions à ressources partagées par nœud à partir d'un client donné.

Lorsqu'un client monte des exportations à partir d'un serveur à ressources partagées, il spécifie un certain nombre d'adresses IP pour les LIF d'un groupe à ressources partagées. Une fois le client connecté à la première LIF, des LIFs supplémentaires ne sont ajoutées à la session NFSv4.1 et utilisées pour la mise en circuit que si elles sont conformes aux exigences des groupes à ressources partagées. Le client distribue ensuite les opérations NFS sur plusieurs connexions en fonction de son propre algorithme (comme la séquence round-Robin).

Pour optimiser les performances, il est conseillé de configurer l'agrégation dans un SVM qui fournit des exportations multivoies, et non des exportations à chemin unique. En d'autres termes, vous devez activer la mise en circuits uniquement sur un serveur NFS d'un SVM dont les exportations sont fournies aux clients à ressources partagées uniquement.

Clients pris en charge

Le serveur ONTAP NFSv4.1 prend en charge la mise en circuit avec tout client capable de la mise en circuit de session NFSv4.1.

Les clients suivants ont été testés avec ONTAP 9.14.1 :

- VMware - ESXi 7.0U3F et versions ultérieures
- Linux : Red Hat Enterprise Linux (RHEL) 8.8 et 9.3

> Le client NFS RHEL ne réétablit pas la mise en circuits si les LIF à ressources partagées sont migrées vers un autre nœud lors d'un basculement (par exemple, un basculement de contrôleur). Lorsque les LIF sont migrées vers un autre nœud, elles sont supprimées du groupe d'agrégation. Si toutes les LIFs du groupe à ressources partagées sont migrées, le client NFS utilisera uniquement la première LIF pour continuer les E/S.

> Lorsque l'agrégation est activée sur un serveur NFS, les utilisateurs qui accèdent à des partages exportés sur des clients NFS qui ne prennent pas en charge l'agrégation peuvent voir une baisse des performances. En effet, une seule connexion TCP est utilisée pour plusieurs montages des LIFs de données du SVM.

Différence entre l'agrégation NFS et nconnect

Depuis ONTAP 9.8, la fonctionnalité nconnect est disponible par défaut lorsque NFSv4.1 est activé. Sur les clients compatibles nconnect, un seul montage NFS peut avoir plusieurs connexions TCP (jusqu'à 16) sur une seule LIF.

En revanche, l'agrégation est *multipathing* fonctionnalité, qui fournit plusieurs connexions TCP sur plusieurs LIFs. Si vous avez la possibilité d'utiliser des cartes réseau supplémentaires dans votre environnement, l'agrégation offre un parallélisme et des performances supérieurs à ceux de nconnect.

En savoir plus sur "nconnect".

Configurer un nouveau serveur NFS et des exportations pour l'agrégation

Créer un serveur NFS à ressources partagées sur un SVM ONTAP

À partir de ONTAP 9.14.1, l'agrégation peut être activée sur les serveurs NFS. NFSv4.1 est activé par défaut lors de la création des serveurs NFS.

Avant de commencer

La création d'un serveur NFS à ressources partagées nécessite une SVM. La SVM doit être :

- stockage suffisant pour répondre aux besoins en données des clients.
- Activé pour NFS.

Vous pouvez utiliser un SVM existant, mais l'activation de la mise en circuits nécessite le montage de tous les

clients NFSv4.x, ce qui peut entraîner des perturbations. Si le remontage n'est pas possible, créer un nouveau SVM pour le serveur NFS.

Étapes

1. Si aucun SVM approprié n'existe, en créer un :

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Vérifier la configuration et le statut du nouveau SVM :

   ```
   vserver show -vserver svm_name
   ```

   En savoir plus sur "Création d'un SVM".

3. Créez le serveur NFS :

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. Vérifiez que NFS est en cours d'exécution :

   ```
   vserver nfs status -vserver svm_name
   ```

5. Vérifiez que NFS est configuré comme vous le souhaitez :

   ```
   vserver nfs show -vserver svm_name
   ```

   En savoir plus sur "Configuration du serveur NFS."

Une fois que vous avez terminé

Configurez les services suivants si nécessaire :

- "DNS"
- "LDAP"
- "Kerberos"

Préparez votre réseau pour l'agrégation ONTAP NFS

Pour tirer parti de la mise en circuit NFSv4.1, les LIFs d'un groupe à agrégation doivent résider sur le même nœud et avoir des ports home sur le même nœud. Les LIFs doivent être configurées dans un failover group sur le même node.

Description de la tâche

Un mappage un-à-un des LIF et des cartes réseau offre un gain de performance optimal, mais il n'est pas nécessaire d'activer l'agrégation. Avoir au moins deux cartes réseau installées peut offrir un avantage en termes de performances, mais ce n'est pas nécessaire.

Toutes les LIFs du groupe à ressources partagées doivent appartenir au même groupe de basculement. Notez que lorsque les LIFs sont configurées dans un groupe de failover sur le même nœud, un basculement de contrôleur sur ce nœud peut mettre les LIFs hors ligne. Si les LIFs ne sont pas configurées dans un groupe de basculement sur le même nœud et si elles basculent sur un autre nœud, la mise en circuits ne fonctionnera

plus.

Vous devez ajuster le groupe de basculement à ressources partagées chaque fois que vous ajoutez ou supprimez des connexions (et des cartes réseau sous-jacentes) d'un groupe de basculement.

Avant de commencer

- Vous devez connaître les noms de port associés aux cartes réseau pour créer un groupe de basculement.
- Tous les ports doivent se trouver sur le même nœud.

Étapes

1. Vérifiez les noms et l'état des ports réseau que vous prévoyez d'utiliser :

   ```
   network port show
   ```

2. Créer le failover group :

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   La mise en place d'un groupe de basculement n'est pas obligatoire, mais il est fortement recommandé.

   - `<svm_name>` Est le nom du SVM contenant le serveur NFS.
   - `<ports_list>` est la liste des ports qui seront ajoutés au failover group.

     Les ports sont ajoutés au format `<node_name>:<port_number>`, par exemple : `node1:e0c`.

     La commande suivante crée le groupe de basculement fg3 pour SVM vs1 et ajoute trois ports :

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

     En savoir plus sur "groupes de basculement."

   Pour en savoir plus, `network interface failover-groups create` consultez le "Référence de commande ONTAP".

3. Si nécessaire, créez des LIFs pour les membres du groupe de trunking :

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node` - Le nœud auquel la LIF retourne lorsque la commande network interface revert est exécutée sur la LIF.

     Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

   - `-home-port` Est le port physique ou logique renvoyé par la LIF lorsque la commande network

interface revert est exécutée sur la LIF.

- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` et non avec le `-subnet` option.
- Lorsque vous attribuez des adresses IP, vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un sous-réseau IP différent. Pour en savoir plus sur `network route create` et créer une route statique au sein d'une SVM, consultez la "Référence de commande ONTAP".
- `-service-policy` - La politique de service de la LIF. Si aucune règle n'est spécifiée, une règle par défaut sera attribuée automatiquement. Utilisez le `network interface service-policy show` pour consulter les stratégies de service disponibles.
- `-auto-revert` - Spécifier si une LIF de données est automatiquement rétablie sur son nœud de rattachement dans des circonstances telles que le démarrage, les modifications du statut de la base de données de gestion ou lorsque la connexion réseau est établie. Le paramètre par défaut est FALSE, mais vous pouvez le définir sur TRUE en fonction des stratégies de gestion de réseau de votre environnement.

  Répéter cette étape pour chaque LIF du groupe de trunking.

  La commande suivante crée `lif-A` Pour la SVM `vs1`, sur le port `e0c` du nœud `cluster1_01`:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

En savoir plus sur "Création de LIF."

4. Vérifier que les LIFs ont été créées :

   ```
   network interface show
   ```

5. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier…	Utiliser…
Adresse IPv4	`network ping`
Adresse IPv6	`network ping6`

Informations associées

- "ping réseau"
- "interface réseau"
- "port réseau show"

Créez une export policy de volume ONTAP

Pour que le client puisse accéder aux partages de données, vous devez créer un ou plusieurs volumes et disposer de règles d'exportation au moins une pour le volume.

Conditions requises pour l'exportation du client :

- Les clients Linux doivent disposer d'un point de montage et d'un point de montage distincts pour chaque connexion à ressources partagées (c'est-à-dire, pour chaque LIF).
- Les clients VMware requièrent un seul point de montage pour un volume exporté, avec plusieurs LIF spécifiées.

  Les clients VMware nécessitent un accès racine dans la règle d'export.

Étapes

1. Créer une export-policy :

   `vserver export-policy create -vserver svm_name -policyname policy_name`

   Le nom de la stratégie peut comporter jusqu'à 256 caractères.

2. Vérifier que l'export policy a été créée :

   `vserver export-policy show -policyname policy_name`

   Exemple

   Les commandes suivantes créent et vérifient la création d'une export policy nommée exp1 sur le SVM nommé vs1:

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. Créez une règle d'export et ajoutez-la à une export-policy existante :

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   Le `-clientmatch` Le paramètre doit identifier les clients Linux ou VMware compatibles avec l'agrégation qui vont monter l'exportation.

   En savoir plus sur "création de règles d'exportation."

4. Créer le volume avec un point de jonction :

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path -policy
   export_policy_name
   ```

   Découvrez "création de volumes."

5. Vérifier que le volume a été créé avec le point de jonction souhaité :

   `volume show -vserver svm_name -volume volume_name -junction-path`

Montez des volumes ONTAP ou des partages de données pour l'agrégation NFS

Les clients Linux et VMware qui prennent en charge l'agrégation peuvent monter des

volumes ou des partages de données à partir d'un serveur ONTAP NFSv4.1 qui est activé pour l'agrégation.

Découvrez "clients pris en charge".

Configuration requise pour le client Linux

Si vous utilisez ONTAP 9.16.1 ou une version ultérieure et Red Hat Enterprise Linux version 8.7 ou ultérieure (pour RHEL 8) ou 9.2 ou ultérieure (pour RHEL 9) comme client Linux, un seul point de montage est requis pour le groupe de ressources partagées. Monter les volumes exportés avec cette commande, en utilisant l' `trunkdiscovery`option :

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Dans le cas contraire, un point de montage distinct est requis pour chaque connexion dans le groupe d'agrégation. Montez le volume exporté avec des commandes similaires à celles ci-dessous, en utilisant l' `max_connect`option :

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

La version (`vers`) la valeur doit être de `4.1` ou ultérieure.

Le `max_connect` la valeur correspond au nombre de connexions dans le groupe d'agrégation.

Configuration requise pour le client VMware

Une instruction mount est requise, qui inclut une adresse IP pour chaque connexion du groupe d'agrégation.

Montez le datastore exporté avec une commande similaire à la suivante :

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Le `-H` les valeurs correspondent aux connexions dans le groupe d'agrégation.

Adaptation des exportations NFS existantes pour l'agrégation

Adaptez les exportations à chemin unique pour l'agrégation ONTAP NFS

Vous pouvez adapter une exportation NFSv4.1 à chemin unique existante (sans ressources partagées) pour utiliser la mise en circuit. Les clients prenant en charge l'agrégation peuvent bénéficier de performances améliorées dès que l'agrégation est activée sur le serveur, à condition que les conditions préalables du serveur et du client aient été satisfaites.

L'adaptation d'une exportation à chemin unique pour l'agrégation vous permet de maintenir les jeux de données exportés dans leurs volumes et SVM existants. Pour ce faire, vous devez activer l'agrégation sur le serveur NFS, mettre à jour la mise en réseau et la configuration d'exportation, et remonter le partage exporté sur les clients.

L'activation de l'agrégation a pour effet de redémarrer le serveur. Les clients VMware doivent ensuite remonter les datastores exportés ; les clients Linux doivent remonter les volumes exportés avec le `max_connect` option.

Activer l'agrégation sur un serveur ONTAP NFS

L'agrégation doit être explicitement activée sur les serveurs NFS. NFSv4.1 est activé par défaut lors de la création des serveurs NFS.

Après avoir activé l'agrégation, vérifiez que les services suivants sont configurés selon les besoins.

- "DNS"
- "LDAP"
- "Kerberos"

Étapes

1. Activez la mise en circuit et assurez-vous que NFSv4.1 est activé :

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. Vérifiez que NFS est en cours d'exécution :
   `vserver nfs status -vserver svm_name`
3. Vérifiez que NFS est configuré comme vous le souhaitez :

   ```
   vserver nfs show -vserver svm_name
   ```

   En savoir plus sur "Configuration du serveur NFS."
   .. Si vous êtes affectés à des clients Windows à partir de ce SVM, déplacez les partages puis supprimez le serveur.
   `vserver cifs show -vserver svm_name`

   +
   `vserver cifs delete -vserver svm_name`

Mettez à jour votre réseau pour l'agrégation ONTAP NFS

Pour tirer parti de la mise en circuit NFSv4.1, les LIFs d'un groupe à agrégation doivent résider sur le même nœud et avoir des ports home sur le même nœud. Les LIFs doivent être configurées dans un failover group sur le même node.

Description de la tâche

Un mappage un-à-un des LIF et des cartes réseau offre un gain de performance optimal, mais il n'est pas nécessaire d'activer l'agrégation. Avoir au moins deux cartes réseau installées peut offrir un avantage en termes de performances, mais ce n'est pas nécessaire.

Toutes les LIFs du groupe à ressources partagées doivent appartenir au même groupe de basculement. Notez

que lorsque les LIFs sont configurées dans un groupe de failover sur le même nœud, un basculement de contrôleur sur ce nœud peut mettre les LIFs hors ligne. Si les LIFs ne sont pas configurées dans un groupe de basculement sur le même nœud et si elles basculent sur un autre nœud, la mise en circuits ne fonctionnera plus.

Vous devez ajuster le groupe de basculement à ressources partagées chaque fois que vous ajoutez ou supprimez des connexions (et des cartes réseau sous-jacentes) d'un groupe de basculement.

Avant de commencer

- Vous devez connaître les noms de port associés aux cartes réseau pour créer un groupe de basculement.
- Tous les ports doivent se trouver sur le même nœud.

Étapes

1. Vérifiez les noms et l'état des ports réseau que vous prévoyez d'utiliser :

   ```
   network port show
   ```

   Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

2. Créez un groupe de basculement à ressources partagées ou modifiez un groupe existant pour la mise en circuits :

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   ```
   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   > La mise en place d'un groupe de basculement n'est pas obligatoire, mais il est fortement recommandé.

   - `<svm_name>` Est le nom du SVM contenant le serveur NFS.
   - `<ports_list>` est la liste des ports qui seront ajoutés au failover group.

     Les ports sont ajoutés au format `<node_name>:<port_number>`, par exemple `node1:e0c` .

     La commande suivante crée le failover group `fg3` Pour SVM vs1 et ajoute trois ports :

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   En savoir plus sur "groupes de basculement."

3. Créez des LIFs supplémentaires pour les membres du groupe d'agrégation, si nécessaire :

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node` - Le nœud auquel la LIF retourne lorsque la commande network interface revert est exécutée sur la LIF.

Vous pouvez indiquer si la LIF doit automatiquement revenir au nœud de rattachement et au port de rattachement avec le `-auto-revert` option.

- `-home-port` Est le port physique ou logique renvoyé par la LIF lorsque la commande network interface revert est exécutée sur la LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` options.
- Lorsque vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un sous-réseau IP différent. La `network route create` page de commande contient des informations sur la création d'une route statique au sein d'un SVM. Pour en savoir plus, `network route create` consultez le "Référence de commande ONTAP".
- `-service-policy` - La politique de service de la LIF. Si aucune règle n'est spécifiée, une règle par défaut sera attribuée automatiquement. Utilisez le `network interface service-policy show` pour consulter les stratégies de service disponibles.

  Pour en savoir plus, `network interface service-policy show` consultez le "Référence de commande ONTAP".
- `-auto-revert` - Spécifier si une LIF de données est automatiquement rétablie sur son nœud de rattachement dans des circonstances telles que le démarrage, les modifications du statut de la base de données de gestion ou lorsque la connexion réseau est établie. **Le paramètre par défaut est FALSE**, mais vous pouvez le définir sur TRUE en fonction des stratégies de gestion de réseau de votre environnement.

  Répéter cette étape pour chaque LIF supplémentaire nécessaire dans le groupe de trunking.

  La commande suivante crée `lif-A` Pour la SVM `vs1`, sur le port `e0c` du nœud `cluster1_01`:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

En savoir plus sur "Création de LIF."

4. Vérifier que les LIFs ont été créées :

   ```
   network interface show
   ```

5. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier…	Utiliser…
Adresse IPv4	`network ping`
Adresse IPv6	`network ping6`

Informations associées

- "ping réseau"
- "interface réseau"

Modifiez les règles d'export de volumes ONTAP

Pour permettre aux clients de tirer parti de l'agrégation pour les partages de données existants, vous devrez peut-être modifier les règles et règles d'exportation ainsi que les volumes auxquels ils sont rattachés. Les exigences d'exportation pour les clients Linux et les datastores VMware sont différentes.

Conditions requises pour l'exportation du client :

- Les clients Linux doivent disposer d'un point de montage et d'un point de montage distincts pour chaque connexion à ressources partagées (c'est-à-dire, pour chaque LIF).

  Si vous effectuez une mise à niveau vers ONTAP 9.14.1 et que vous avez déjà exporté un volume, vous pouvez continuer à utiliser ce volume dans un groupe de ressources partagées.

- Les clients VMware requièrent un seul point de montage pour un volume exporté, avec plusieurs LIF spécifiées.

  Les clients VMware nécessitent un accès racine dans la règle d'export.

Étapes

1. Vérifier qu'une export policy existante est en place :

   ```
   vserver export-policy show
   ```

2. Vérifiez que les règles d'export policy existantes sont appropriées à la configuration de trunking :

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   En particulier, vérifiez que le `-clientmatch` Le paramètre identifie correctement les clients Linux ou VMware compatibles avec l'agrégation qui vont monter l'exportation.

   Si des ajustements sont nécessaires, modifiez la règle à l'aide du `vserver export-policy rule modify` ou créez une nouvelle règle :

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   En savoir plus sur "création de règles d'exportation."

3. Vérifier que les volumes exportés existants sont en ligne :

   ```
   volume show -vserver svm_name
   ```

Remontez des volumes ONTAP ou des partages de données pour la mise en circuits NFS

Pour convertir les connexions client sans ressources partagées en connexions à ressources partagées, les montages existants sur les clients Linux et VMware doivent être démontés et remontés à l'aide des informations relatives aux LIF.

Découvrez "clients pris en charge".

> Le démontage des clients VMware entraîne des interruptions pour toutes les machines virtuelles du datastore. Une alternative consisterait à créer un nouveau datastore activé pour l'agrégation et à utiliser **Storage vmotion** pour déplacer vos machines virtuelles de l'ancien datastore vers le nouveau. Pour plus de détails, reportez-vous à votre documentation VMware.

Configuration requise pour le client Linux

Si vous utilisez ONTAP 9.16.1 ou une version ultérieure et Red Hat Enterprise Linux version 8.7 ou ultérieure (pour RHEL 8) ou 9.2 ou ultérieure (pour RHEL 9) comme client Linux, un seul point de montage est requis pour le groupe de ressources partagées. Monter les volumes exportés avec cette commande, en utilisant l' `trunkdiscovery`option :

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Dans le cas contraire, un point de montage distinct est requis pour chaque connexion dans le groupe d'agrégation. Montez les volumes exportés avec des commandes similaires à celles ci-dessous, à l'aide de l' `max_connect`option :

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

La version (`vers`) la valeur doit être de `4.1` ou ultérieure.

Le `max_connect` la valeur correspond au nombre de connexions dans le groupe d'agrégation.

Configuration requise pour le client VMware

Une instruction mount est requise, qui inclut une adresse IP pour chaque connexion du groupe d'agrégation.

Montez le datastore exporté avec une commande similaire à la suivante :

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Le `-H` les valeurs doivent correspondre aux connexions dans le groupe d'agrégation.

Gestion de NFS sur RDMA

Découvrez NFS over RDMA dans ONTAP

NFS over RDMA utilise des adaptateurs réseau compatibles RDMA. Il est ainsi possible de copier les données directement entre la mémoire du système de stockage et la mémoire du système hôte, évitant ainsi les interruptions et la surcharge du processeur.

Les configurations NFS sur RDMA sont conçues pour les clients qui possèdent des charges de travail sensibles à la latence ou à large bande passante, telles que l'apprentissage machine et l'analytique. ONTAP NFS over RDMA peut être utilisé pour toutes les charges de travail basées sur NFS. De plus, NVIDIA a étendu NFS sur RDMA pour activer le stockage direct des GPU (GDS). Le GDS accélère encore plus les charges de travail grâce aux GPU en contournant complètement le processeur et la mémoire principale, et en utilisant RDMA pour transférer directement les données entre le système de stockage et la mémoire GPU.

À partir de ONTAP 9.10.1, les configurations NFS sur RDMA sont prises en charge pour le protocole NFSv4.0. Les versions suivantes de ONTAP prennent en charge d'autres versions de NFS.

De formation

- Vérifiez que vous exécutez la version correcte de ONTAP pour la version NFS que vous souhaitez utiliser.

Version NFS	Prise en charge de ONTAP
NFSv4.0	ONTAP 9.10.1 et versions ultérieures
NFSv4.1	ONTAP 9.14.1 et versions ultérieures
NFSv3	ONTAP 9.15.1 et versions ultérieures

  - Il est possible de configurer NFS sur RDMA avec System Manager, à partir de ONTAP 9.12.1. Dans ONTAP 9.10.1 et 9.11.1, vous devez utiliser l'interface de ligne de commande pour configurer NFS sur RDMA.
- Les deux nœuds de la paire haute disponibilité (HA) doivent être de la même version.
- Les contrôleurs du système de stockage doivent prendre en charge RDMA :

Depuis ONTAP…	Les contrôleurs suivants prennent en charge RDMA…
9.10.1 et versions ultérieures	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14.1 et versions ultérieures	• AFF série C. • AFF A900
ONTAP 9.15.1 et versions ultérieures	• AFF A1K • AFF A90 • AFF A70
ONTAP 9.16.1 et versions ultérieures	• AFF A50 • AFF A30 • AFF A20

- Les LIF de données doivent être configurées pour prendre en charge RDMA.
- Pour plus d'informations sur la prise en charge de RNIC cible, reportez-vous au "NetApp Hardware Universe".

- Pour plus d'informations sur les systèmes d'exploitation clients pris en charge pour NFS sur RDMA, reportez-vous au "Matrice d'interopérabilité NetApp (IMT)" . Pour les RNIC RoCE v2 pris en charge, reportez-vous à la documentation du fournisseur RNIC correspondant.

Les groupes d'interface ne sont pas pris en charge avec NFS sur RDMA.

Étapes suivantes

- Configurer les cartes réseau pour NFS sur RDMA
- Configuration des LIF pour NFS sur RDMA
- Paramètres NFS pour NFS sur RDMA

Informations associées

- "RDMA"
- Présentation de l'agrégation NFS
- "RFC 7530 : protocole NFS version 4"
- "RFC 8166 : transport d'accès direct à la mémoire à distance pour l'appel de procédure à distance version 1"
- "RFC 8167 : appel de procédure bidirectionnelle à distance sur les transports RPC-over-RDMA"
- "RFC 8267 : liaison de couche supérieure NFS à RPC-over-RDMA version 1"

Configurer les cartes réseau pour NFS sur RDMA

NFS sur RDMA requiert une configuration de carte réseau pour le système client et la plateforme de stockage.

Configuration de la plateforme de stockage

Pour plus d'informations sur la prise en charge de RNIC cible, reportez-vous au "NetApp Hardware Universe".

Si vous utilisez une configuration haute disponibilité, les deux nœuds doivent utiliser le même RNIC pour prendre en charge le basculement RDMA. La carte réseau doit être compatible RoCE.

- Depuis ONTAP 9.10.1, vous pouvez afficher la liste des protocoles de déchargement RDMA avec la commande :

```
network port show -rdma-protocols roce
```

Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

- A partir de ONTAP 9.16.1, il est recommandé d'utiliser le contrôle de débit prioritaire (PFC). Configurer le PFC à l'aide de la `network port modify` commande :

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
pfc -pfc-queues-admin 3
```

- Avant ONTAP 9.16.1, il est recommandé d'utiliser le contrôle de flux global par défaut (GFC). Si le paramètre de contrôle de flux a été modifié, configurez GFC à l'aide de la `network port modify` commande :

  ```
  network port modify -node <nodename> -port <portname> -flowcontrol-admin
  full
  ```

  Pour en savoir plus, `network port modify` consultez le "Référence de commande ONTAP".

Configuration du système client

Pour plus d'informations sur les systèmes d'exploitation clients pris en charge pour NFS sur RDMA, reportez-vous au "Matrice d'interopérabilité NetApp (IMT)" . Pour les RNIC RoCE v2 pris en charge, reportez-vous à la documentation du fournisseur RNIC correspondant.

Bien que le client et le serveur puissent être directement connectés, l'utilisation de commutateurs est recommandée pour améliorer les performances de basculement.

Le client, le serveur, tous les commutateurs et tous les ports des commutateurs doivent être configurés à l'aide de trames Jumbo. La configuration de contrôle de flux sur les clients et les commutateurs doit correspondre à la configuration de contrôle de flux de ONTAP. À partir de ONTAP 9.16.1, il est recommandé d'activer et de configurer le contrôle de flux par priorité sur ONTAP, les commutateurs et les clients. Avant ONTAP 9.16.1, il est recommandé d'utiliser le contrôle de flux global.

Une fois cette configuration confirmée, vous pouvez monter l'exportation NFS à l'aide de RDMA.

System Manager

Vous devez utiliser ONTAP 9.12.1 ou version ultérieure pour configurer les interfaces réseau avec NFS sur RDMA à l'aide de System Manager.

Étapes

1. Vérifier si le protocole RDMA est pris en charge. Accédez à **réseau > ports Ethernet** et sélectionnez le nœud approprié dans la vue de groupe. Lorsque vous développez le nœud, examinez le champ **protocoles RDMA** pour un port donné : la valeur **RoCE** indique que RDMA est pris en charge ; un tiret (**-**) indique qu'il n'est pas pris en charge.
2. Pour ajouter un VLAN, sélectionnez **+ VLAN**. Sélectionnez le nœud approprié. Dans le menu déroulant **Port**, les ports disponibles affichent le texte **RoCE Enabled** s'ils prennent en charge RDMA. Aucun texte ne s'affiche s'ils ne prennent pas en charge RDMA.
3. Suivez le flux de travail dans Activez le stockage NAS pour les serveurs Linux à l'aide de NFS Pour configurer un nouveau serveur NFS.

   Lorsque vous ajoutez des interfaces réseau, vous avez la possibilité de sélectionner **utiliser les ports RoCE**. Sélectionnez cette option pour les interfaces réseau que vous souhaitez utiliser NFS sur RDMA.

CLI

1. Vérifier si l'accès RDMA est activé sur le serveur NFS avec la commande :

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   Par défaut, `-rdma` doit être activé. Si ce n'est pas le cas, activer l'accès RDMA sur le serveur NFS :

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. Monter le client via NFSv4.0 sur RDMA :
   a. L'entrée du paramètre proto dépend de la version du protocole IP du serveur. S'il s'agit d'IPv4, utilisez `proto=rdma`. S'il s'agit du protocole IPv6, utilisez-le `proto=rdma6`.
   b. Spécifiez le port cible NFS en tant que `port=20049` au lieu du port standard 2049 :

   ```
   mount -o vers=4,minorversion=0,proto=rdma,port=20049
   <Server_IP_address>:/<volume_path> <mount_point>
   ```

3. **FACULTATIF** : si vous devez démonter le client, exécutez la commande `unmount <mount_path>`

Plus d'informations

- Créer des serveurs ONTAP NFS
- Activez le stockage NAS pour les serveurs Linux à l'aide de NFS

Configuration des LIF pour NFS sur RDMA

Pour utiliser NFS sur RDMA, vous devez configurer vos LIF (interface réseau) pour qu'elles soient compatibles. La LIF et sa paire de basculement doivent pouvoir prendre en charge RDMA.

Créer une nouvelle LIF

System Manager

Vous devez exécuter ONTAP 9.12.1 ou une version ultérieure pour créer une interface réseau pour NFS sur RDMA avec System Manager.

Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez + Add .
3. Lorsque vous sélectionnez **NFS,SMB/CIFS,S3**, vous pouvez **utiliser les ports RoCE**. Cochez la case utiliser les ports RoCE*.
4. Sélectionnez le VM de stockage et le nœud de rattachement. Attribuez un **Nom**, une **adresse IP** et un **masque de sous-réseau**.
5. Une fois que vous avez saisi l'adresse IP et le masque de sous-réseau, System Manager filtre la liste des domaines de diffusion à ceux qui disposent de ports compatibles RoCE. Sélectionnez un domaine de diffusion. Vous pouvez éventuellement ajouter une passerelle.
6. Sélectionnez **Enregistrer**.

CLI

Étapes

1. Créer une LIF :

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - La politique de service doit être des fichiers de données par défaut ou une règle personnalisée qui inclut le service d'interface réseau Data-nfs.
   - Le `-rdma-protocols` paramètre accepte une liste, qui est par défaut vide. Quand `roce` Est une valeur ajoutée, le LIF ne peut être configuré que sur des ports prenant en charge RoCE Offload, affectant la migration et le basculement des LIF bot.

Modifier une LIF

System Manager

Vous devez exécuter ONTAP 9.12.1 ou une version ultérieure pour créer une interface réseau pour NFS sur RDMA avec System Manager.

Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez ⋮ **> Modifier** en regard de l'interface réseau que vous souhaitez modifier.
3. Cochez **utiliser les ports RoCE** pour activer NFS sur RDMA ou décochez la case pour la désactiver. Si l'interface réseau se trouve sur un port compatible RoCE, la case à cocher située en regard de **Use RoCE ports** s'affiche.
4. Modifiez les autres paramètres si nécessaire.
5. Sélectionnez **Enregistrer** pour confirmer vos modifications.

CLI

1. Vous pouvez vérifier le statut de vos LIFs à l'aide de `network interface show` commande. La politique de service doit inclure le service de l'interface réseau Data-nfs. Le `-rdma-protocols` la liste doit inclure `roce`. Si l'une de ces conditions est fausse, modifiez la LIF.

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

2. Pour modifier le LIF, lancer :

   ```
   network interface modify vserver SVM_name -lif lif_name -service-policy
   service_policy_name -home-node node_name -home-port port_name {-address
   IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
   -policy policy_name -auto-revert {true|false} -rdma-protocols roce
   ```

   Pour en savoir plus, `network interface modify` consultez le "Référence de commande ONTAP".

> ⓘ La modification d'une LIF afin de nécessiter un protocole de déchargement particulier lorsque la LIF n'est pas actuellement attribuée à un port qui prend en charge ce protocole entraînera une erreur.

Migrer un LIF

ONTAP vous permet également de migrer les interfaces réseau (LIF) pour utiliser NFS sur RDMA. Lors de cette migration, vous devez vous assurer que le port de destination est compatible RoCE. Depuis ONTAP 9.12.1, vous pouvez effectuer cette procédure dans System Manager. Lors de la sélection d'un port de destination pour l'interface réseau, System Manager désignera si les ports sont compatibles RoCE.

Vous pouvez migrer un LIF vers une configuration NFS sur RDMA uniquement si :

- Il s'agit d'une interface réseau NFS RDMA (LIF) hébergée sur un port compatible RoCE.
- Il s'agit d'une interface réseau TCP NFS (LIF) hébergée sur un port compatible RoCE.
- Il s'agit d'une interface réseau TCP NFS (LIF) hébergée sur un port non compatible RoCE.

Pour plus d'informations sur la migration d'une interface réseau, reportez-vous à la section Migrer un LIF.

Informations associées

- Créer une LIF
- Créer une LIF
- Modifier une LIF
- Migrer un LIF

Modifier la configuration NFS

Dans la plupart des cas, il n'est pas nécessaire de modifier la configuration du serveur virtuel de stockage NFS pour NFS sur RDMA.

Si vous êtes toutefois chargé de résoudre les problèmes liés aux puces Mellanox et à la migration de LIF, il est recommandé d'augmenter la période de grâce au verrouillage NFSv4. Par défaut, le délai de grâce est défini sur 45 secondes. Depuis ONTAP 9.10.1, la valeur maximale du délai de grâce est de 180 (secondes).

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Saisissez la commande suivante :

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

Pour plus d'informations sur cette tâche, reportez-vous à Spécifier la période de grâce de verrouillage NFSv4 pour les SVM ONTAPla section .

Configurez SMB avec l'interface de ligne de commandes

En savoir plus sur la configuration SMB avec l'interface de ligne de commande ONTAP

Vous pouvez utiliser les commandes de l'interface de ligne de commande de ONTAP 9 pour configurer l'accès des clients SMB aux fichiers contenus dans un nouveau volume ou qtree dans un SVM nouveau ou existant.

SMB (Server message Block) désigne les dialectes modernes du protocole CIFS (Common Internet File System). Vous verrez toujours *CIFS* dans l'interface de ligne de commande (CLI) ONTAP et dans les outils de gestion OnCommand.

Utilisez les procédures suivantes pour configurer l'accès SMB à un volume ou à un qtree de la manière suivante :

- Vous souhaitez utiliser SMB version 2 ou ultérieure.
- Vous ne souhaitez servir que les clients SMB, pas les clients NFS (pas une configuration multiprotocole).
- Les autorisations d'accès au fichier NTFS seront utilisées pour sécuriser le nouveau volume.
- Vous disposez des privilèges d'administrateur de cluster et non des privilèges d'administrateur de SVM.

Les privilèges d'administrateur du cluster sont requis pour créer des SVM et des LIFs. Les privilèges d'administrateur SVM sont suffisants pour d'autres tâches de configuration SMB.

- Vous souhaitez utiliser l'interface de ligne de commandes, et non System Manager ou un outil de script automatisé.

  Pour utiliser System Manager pour configurer l'accès multiprotocole NAS, reportez-vous à "Provisionnement de stockage NAS pour Windows et Linux à l'aide des protocoles NFS et SMB"la section .

- Vous voulez appliquer les bonnes pratiques, pas explorer toutes les options disponibles.

  Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

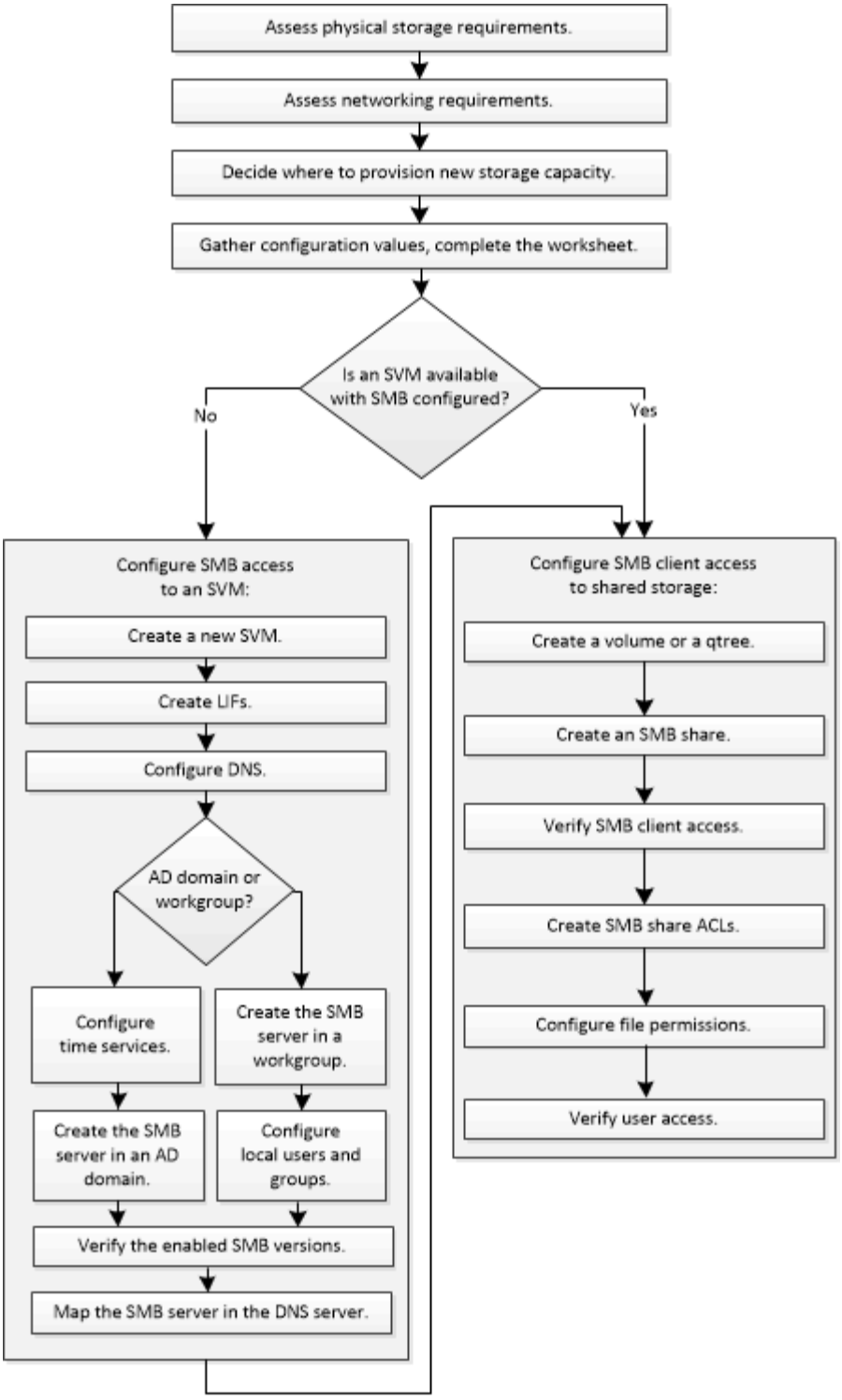
Pour plus d'informations sur la plage de fonctionnalités du protocole SMB de ONTAP, consultez le "Présentation des références SMB".

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Reportez-vous à…
System Manager redessiné (disponible avec ONTAP 9.7 et versions ultérieures)	"Provisionnement du stockage NAS pour les serveurs Windows avec SMB"
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la configuration SMB"

Flux de travail de configuration SMB ONTAP

La configuration de SMB implique l'évaluation des besoins en réseau et en stockage physique, puis le choix d'un workflow spécifique à votre objectif ; la configuration de l'accès SMB à un SVM nouveau ou existant ; ou l'ajout d'un volume ou d'un qtree à un SVM existant déjà entièrement configuré pour l'accès SMB.



Préparation

Évaluez les besoins en stockage physique ONTAP SMB

Avant de provisionner le stockage SMB pour les clients, vous devez vérifier que l'espace est suffisant dans un agrégat existant pour le nouveau volume. Si ce n'est pas le cas, vous pouvez ajouter des disques à un agrégat existant ou créer un nouvel agrégat du type souhaité.

Étapes

1. Afficher l'espace disponible dans les agrégats existants : `storage aggregate show`

   Si un agrégat dispose d'un espace suffisant, notez son nom dans la fiche de travail.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. Si aucun agrégat n'a suffisamment d'espace, ajoutez des disques à un agrégat existant en utilisant le `storage aggregate add-disks` ou créez un nouvel agrégat à l'aide de `storage aggregate create` commande.

Informations associées

- "agrégat de stockage add-disks"
- "création d'agrégats de stockage"

Évaluez les exigences réseau de ONTAP SMB

Avant de fournir un stockage SMB aux clients, vous devez vérifier que le réseau est correctement configuré pour répondre aux exigences de provisionnement SMB.

Avant de commencer

Les objets de réseau de cluster suivants doivent être configurés :

- Ports physiques et logiques
- Les domaines de diffusion
- Sous-réseaux (le cas échéant)
- IPspaces (selon les besoins, en plus de l'IPspace par défaut)
- Failover Groups (si nécessaire, en plus du groupe de basculement par défaut pour chaque broadcast domain)
- Pare-feu externes

Étapes

1. Afficher les ports physiques et virtuels disponibles : `network port show`

   - Dans la mesure du possible, vous devez utiliser le port avec la vitesse la plus élevée pour le réseau de données.
   - Tous les composants du réseau de données doivent avoir le même paramètre MTU pour optimiser les performances.

   Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

2. Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses suffisantes : `network subnet show`

   Pour en savoir plus, `network subnet show` consultez le "Référence de commande ONTAP".

   Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Les sous-réseaux sont créés à l'aide du `network subnet create` commande.

   Pour en savoir plus, `network subnet create` consultez le "Référence de commande ONTAP".

3. Affichez les IPspaces disponibles : `network ipspace show`

   Vous pouvez utiliser l'IPspace par défaut ou un IPspace personnalisé.

   Pour en savoir plus, `network ipspace show` consultez le "Référence de commande ONTAP".

4. Si vous souhaitez utiliser des adresses IPv6, vérifiez que l'IPv6 est activé sur le cluster : `network options ipv6 show`

   Si nécessaire, vous pouvez activer IPv6 en utilisant le `network options ipv6 modify` commande.

   Pour en savoir plus sur `network options ipv6 show` et `network options ipv6 modify` dans le "Référence de commande ONTAP".

Découvrez le provisionnement de capacité de stockage ONTAP pour PME

Avant de créer un nouveau volume SMB ou qtree, vous devez décider de le placer dans un SVM nouveau ou existant, et de la configuration requise par la SVM. Cette décision détermine votre flux de travail.

Choix

- Si vous souhaitez provisionner un volume ou qtree sur un nouveau SVM, ou sur un SVM existant sur lequel SMB est activé mais non configuré, suivez les étapes des sections « Configuration de l'accès SMB à un SVM » et « Ajout de capacité de stockage à un SVM SMB ».

  Configuration de l'accès SMB à un SVM

  Configuration de l'accès client SMB au stockage partagé

  Vous pouvez choisir de créer un nouveau SVM si l'un des cas suivants est vrai :

- Vous activez SMB sur un cluster pour la première fois.
- Un cluster contient des SVM existants dans lequel vous ne souhaitez pas activer la prise en charge SMB.
- Au sein d'un cluster, un ou plusieurs SVM compatibles SMB doivent être connectés :
  - Vers une autre forêt ou groupe de travail Active Directory.
  - Vers un serveur SMB dans un espace de noms isolé (scénario de colocation).
    Vous devez également choisir cette option pour provisionner le stockage sur un SVM existant pour lequel SMB est activé, mais pas configuré. Ce peut être le cas si vous avez créé le SVM pour l'accès SAN ou si aucun protocole n'a été activé au moment de la création de la SVM.

Après l'activation de SMB sur le SVM, procéder au provisionnement d'un volume ou qtree.

- Si vous souhaitez provisionner un volume ou qtree sur un SVM existant entièrement configuré pour l'accès SMB, suivez les étapes de la section « Ajout de capacité de stockage à un SVM compatible SMB ».

  Configuration de l'accès client SMB au stockage partagé

Fiche technique de configuration SMB de ONTAP

La fiche de configuration SMB vous permet de collecter les informations requises pour configurer l'accès SMB pour les clients.

Vous devez remplir une ou les deux sections de la feuille de travail, en fonction de la décision que vous avez prise concernant l'emplacement de stockage :

- Si vous configurez l'accès SMB à un SVM, vous devez compléter les deux sections.

  Configuration de l'accès SMB à un SVM

  Configuration de l'accès client SMB au stockage partagé

- Si vous ajoutez de la capacité de stockage à un SVM compatible SMB, vous ne devez remplir que la deuxième section.

  Configuration de l'accès client SMB au stockage partagé

Pour en savoir plus sur les paramètres "Référence de commande ONTAP"de la .

Configuration de l'accès SMB à un SVM

Paramètres de création d'un SVM

Si vous créez un nouveau SVM, vous fournissez ces valeurs avec la `vserver create` commande. Pour en savoir plus, `vserver create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Un nom que vous fournissez pour le nouveau SVM qui est un nom de domaine complet (FQDN) ou suit une autre convention qui applique des noms de SVM uniques au sein d'un cluster.	
`-aggregate`	Le nom d'un agrégat du cluster disposant d'un espace suffisant pour la nouvelle capacité de stockage SMB.	
`-rootvolume`	Un nom unique que vous fournissez pour le volume root du SVM.	
`-rootvolume-security-style`	Utiliser le style de sécurité NTFS pour le SVM.	`ntfs`
`-language`	Utilisez le paramètre de langue par défaut de ce flux de travail.	`C.UTF-8`
`ipspace`	Facultatif : les IPspaces sont des espaces d'adresse IP distincts dans lesquels les SVM résident.	

Paramètres de création d'une LIF

Vous fournissez ces valeurs avec la `network interface create` commande lors de la création des LIFs. Pour en savoir plus, `network interface create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-lif`	Nom que vous fournissez pour la nouvelle LIF.	
`-role`	Utiliser le rôle LIF de données dans ce workflow	`data`
`-data-protocol`	Utilisez uniquement le protocole SMB dans ce flux de production.	`cifs`

Champ	Description	Votre valeur
`-home-node`	Le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF. Pour en savoir plus, `network interface revert` consultez le "Référence de commande ONTAP".	
`-home-port`	Le port ou le groupe d'interface sur lequel la LIF renvoie au moment du `network interface revert` La commande est exécutée sur le LIF.	
`-address`	L'adresse IPv4 ou IPv6 sur le cluster qui seront utilisées pour l'accès aux données par la nouvelle LIF.	
`-netmask`	Le masque de réseau et la passerelle pour le LIF.	
`-subnet`	Un pool d'adresses IP. Utilisé au lieu de `-address` et `-netmask` pour attribuer automatiquement des adresses et des masques réseau.	
`-firewall-policy`	Utilisez la politique de pare-feu de données par défaut dans ce workflow.	`data`
`-auto-revert`	Facultatif : spécifie si une LIF de données est automatiquement reconvertie vers son nœud de rattachement au démarrage ou dans d'autres circonstances. Le paramètre par défaut est `false`.	

Paramètres de résolution de nom d'hôte DNS

Vous fournissez ces valeurs avec la `vserver services name-service dns create` commande lorsque vous configurez DNS. Pour en savoir plus, `vserver services name-service dns create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-domains`	Jusqu'à cinq noms de domaine DNS.	
`-name-servers`	Jusqu'à trois adresses IP pour chaque serveur de noms DNS.	

Configuration d'un serveur SMB dans un domaine Active Directory

Paramètres de configuration du service de temps

Vous fournissez ces valeurs avec la `cluster time-service ntp server create` commande lorsque vous configurez les services de temps. Pour en savoir plus, `cluster time-service ntp server create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-server`	Nom d'hôte ou adresse IP du serveur NTP pour le domaine Active Directory.	

Paramètres de création d'un serveur SMB dans un domaine Active Directory

Vous fournissez ces valeurs avec la `vserver cifs create` commande lorsque vous créez un nouveau serveur SMB et que vous spécifiez les informations de domaine. Pour en savoir plus, `vserver cifs create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le serveur SMB.	
`-cifs-server`	Nom du serveur SMB (15 caractères maximum).	
`-domain`	Nom de domaine complet (FQDN) du domaine Active Directory à associer au serveur SMB.	
`-ou`	Facultatif : unité organisationnelle du domaine Active Directory à associer au serveur SMB. Par défaut, ce paramètre est défini sur CN=Computers.	
`-netbios-aliases`	Facultatif : liste des alias NetBIOS, qui sont des noms alternatifs au nom du serveur SMB.	

Champ	Description	Votre valeur
`-comment`	Facultatif : commentaire texte pour le serveur. Les clients Windows peuvent voir cette description du serveur SMB lors de la navigation sur les serveurs du réseau.	

Configuration d'un serveur SMB dans un groupe de travail

Paramètres pour la création d'un serveur SMB dans un groupe de travail

Vous fournissez ces valeurs avec la `vserver cifs create` commande lorsque vous créez un nouveau serveur SMB et que vous spécifiez les versions SMB prises en charge. Pour en savoir plus, `vserver cifs create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le serveur SMB.	
`-cifs-server`	Nom du serveur SMB (15 caractères maximum).	
`-workgroup`	Nom du groupe de travail (jusqu'à 15 caractères).	
`-comment`	Facultatif : commentaire texte pour le serveur. Les clients Windows peuvent voir cette description du serveur SMB lors de la navigation sur les serveurs du réseau.	

Paramètres pour la création d'utilisateurs locaux

Vous fournissez ces valeurs lorsque vous créez des utilisateurs locaux à l'aide de la `vserver cifs users-and-groups local-user create` commande. Elles sont requises pour les serveurs SMB des groupes de travail et facultatives dans les domaines AD. Pour en savoir plus, `vserver cifs users-and-groups local-user create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer l'utilisateur local.	
`-user-name`	Nom de l'utilisateur local (20 caractères maximum).	

Champ	Description	Votre valeur
`-full-name`	Facultatif : nom complet de l'utilisateur. Si le nom complet contient un espace, placez le nom complet entre guillemets.	
`-description`	Facultatif : description de l'utilisateur local. Si la description contient un espace, placez le paramètre entre guillemets.	
`-is-account-disabled`	Facultatif : indique si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, la valeur par défaut est d'activer le compte utilisateur.	

Paramètres de création de groupes locaux

Vous fournissez ces valeurs lorsque vous créez des groupes locaux à l'aide de la `vserver cifs users-and-groups local-group create` commande. Elles sont facultatives pour les serveurs SMB dans les domaines AD et les groupes de travail. Pour en savoir plus, `vserver cifs users-and-groups local-group create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le groupe local.	
`-group-name`	Nom du groupe local (256 caractères maximum).	
`-description`	Facultatif : description du groupe local. Si la description contient un espace, placez le paramètre entre guillemets.	

Ajout de capacité de stockage à un SVM compatible SMB

Paramètres de création d'un volume

Si vous créez un volume à la place d'un qtree, vous fournissez ces valeurs avec la `volume create` commande. Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom d'un SVM nouveau ou existant qui hébergera le nouveau volume.	

Champ	Description	Votre valeur
`-volume`	Un nom descriptif unique que vous fournissez pour le nouveau volume.	
`-aggregate`	Nom d'un agrégat dans le cluster disposant d'un espace suffisant pour le nouveau volume SMB.	
`-size`	Un entier que vous fournissez pour la taille du nouveau volume.	
`-security-style`	Utilisez le style de sécurité NTFS pour ce flux de travail.	`ntfs`
`-junction-path`	Emplacement sous la racine (/) où le nouveau volume doit être monté.	

Paramètres pour la création d'un qtree

Vous fournissez ces valeurs avec la `volume qtree create` commande si vous créez un qtree au lieu d'un volume. Pour en savoir plus, `volume qtree create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom de la SVM sur lequel réside le volume contenant le qtree.	
`-volume`	Nom du volume qui contiendra le nouveau qtree.	
`-qtree`	Un nom descriptif unique que vous fournissez pour le nouveau qtree, 64 caractères maximum.	
`-qtree-path`	L'argument de chemin qtree dans le format `/vol/volume_name/qtree_name\>` peut être spécifié au lieu de spécifier volume et qtree en tant qu'arguments distincts.	

Paramètres de création de partages SMB

Vous fournissez ces valeurs avec la `vserver cifs share create` commande. Pour en savoir plus, `vserver cifs share create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer le partage SMB.	
`-share-name`	Nom du partage SMB que vous souhaitez créer (256 caractères maximum).	
`-path`	Nom du chemin d'accès au partage SMB (256 caractères maximum). Ce chemin doit exister dans un volume avant de créer le partage.	
`-share-properties`	Facultatif : liste des propriétés de partage. Les paramètres par défaut sont `oplocks`, `browsable`, `changenotify`, et `show-previous-versions`.	
`-comment`	Facultatif : commentaire texte pour le serveur (256 caractères maximum). Les clients Windows peuvent voir cette description de partage SMB lors de la navigation sur le réseau.	

Paramètres de création de listes de contrôle d'accès de partage SMB (ACL)

Vous fournissez ces valeurs avec la `vserver cifs share access-control create` commande. Pour en savoir plus, `vserver cifs share access-control create` consultez le "Référence de commande ONTAP".

Champ	Description	Votre valeur
`-vserver`	Nom du SVM sur lequel créer la ACL SMB.	
`-share`	Nom du partage SMB sur lequel créer.	
`-user-group-type`	Type de l'utilisateur ou du groupe à ajouter à la liste de contrôle d'accès du partage. Le type par défaut est `windows`	`windows`

Champ	Description	Votre valeur
`-user-or-group`	Utilisateur ou groupe à ajouter à la liste ACL du partage. Si vous spécifiez le nom d'utilisateur, vous devez inclure le domaine de l'utilisateur au format "daomain\username".	
`-permission`	Spécifie les autorisations pour l'utilisateur ou le groupe.	`[No_access
Read	Change	Full_Control]`

Configuration de l'accès SMB à un SVM

Configuration de l'accès SMB aux SVM ONTAP

Si aucune SVM n'est déjà configurée pour l'accès client SMB, vous devez créer et configurer un nouveau SVM ou configurer un SVM existant. La configuration SMB implique l'ouverture d'un accès au volume root du SVM, la création d'un serveur SMB, la création d'une LIF, l'activation de la résolution de nom d'hôte, la configuration des services de noms et, si nécessaire, Activation de la sécurité Kerberos.

Création de SVM ONTAP pour l'accès aux données SMB

Si vous ne disposez pas encore d'au moins un SVM dans un cluster pour fournir un accès aux données aux clients SMB, vous devez en créer un.

Avant de commencer

- À partir de ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d'informations, voir Gestion de la capacité des SVM.

Étapes

1. Création d'un SVM : `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - Utilisez le paramètre NTFS pour le `-rootvolume-security-style` option.
   - Utilisez le paramètre par défaut C.UTF-8 `-language` option.
   - Le `ipspace` le paramètre est facultatif.
2. Vérifier la configuration et le statut du nouveau SVM : `vserver show -vserver` *`vserver_name`*

   Le `Allowed Protocols` Le champ doit inclure CIFS. Vous pouvez modifier cette liste ultérieurement.

   Le `Vserver Operational State` le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'IPspace `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                       Vserver Admin State: running
                 Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

À partir de la version ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite au niveau du débit et du plafond aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir Définissez un modèle de groupe de règles adaptatives.

Vérifier que le protocole SMB est activé sur le SVM ONTAP

Avant de pouvoir configurer et utiliser SMB sur les SVM, il faut vérifier que le protocole est activé.

Description de la tâche

Cela s'effectue généralement lors de la configuration d'un SVM, mais si vous n'avez pas activé le protocole lors de l'installation, vous pouvez l'activer plus tard à l'aide du `vserver add-protocols` commande.

> Vous ne pouvez pas ajouter ou supprimer un protocole d'une LIF une fois qu'il est créé.

Vous pouvez également désactiver les protocoles sur les SVM à l'aide de `vserver remove-protocols` commande.

Étapes

1. Vérifier les protocoles actuellement activés et désactivés pour le SVM : `vserver show -vserver vserver_name -protocols`

   Vous pouvez également utiliser le `vserver show-protocols` Commande permettant d'afficher les protocoles actuellement activés sur tous les SVM du cluster.

2. Si nécessaire, activer ou désactiver un protocole :
   - Pour activer le protocole SMB : `vserver add-protocols -vserver vserver_name -protocols cifs`
   - Pour désactiver un protocole : `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Vérifiez que les protocoles activés et désactivés ont été correctement mis à jour : `vserver show -vserver vserver_name -protocols`

Exemple

La commande suivante affiche les protocoles actuellement activés et désactivés (autorisés et interdits) sur le SVM nommé vs1 :

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ---------------------     ----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

La commande suivante permet d'accéder à via SMB par ajout `cifs` Pour la liste des protocoles activés sur le SVM nommé vs1 :

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Ouvrir les SMB export policy du volume root du SVM ONTAP

L'export policy default du volume root du SVM doit inclure une règle afin de permettre à

tous les clients d'y accéder via SMB. Sans cette règle, tous les clients SMB se voient refuser l'accès au SVM et à ses volumes.

Description de la tâche

Lorsqu'un nouveau SVM est créé, une export policy par défaut (appelée default) est créée automatiquement pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM.

Vérifiez que tous les accès SMB sont ouverts dans la stratégie d'export par défaut, puis limitez l'accès aux volumes individuels en créant des règles d'export personnalisées pour les volumes individuels ou les qtrees.

Étapes

1. Si vous utilisez un SVM existant, vérifier la root volume export policy par défaut : `vserver export-policy rule show`

   Le résultat de la commande doit être similaire à ce qui suit :

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

   Si une telle règle existe et autorise l'accès ouvert, cette tâche est terminée. Si ce n'est pas le cas, passez à l'étape suivante.

2. Créer une règle d'export pour le volume root du SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Vérifiez la création de règles à l'aide du `vserver export-policy rule show` commande.

Résultats

Tout client SMB peut désormais accéder à n'importe quel volume ou qtree créé sur la SVM.

Création des LIF SMB ONTAP

Une LIF est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur le `up` statut administratif. Pour en savoir plus, `up` consultez le "Référence de commande ONTAP".
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

  Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

  Pour en savoir plus, `network subnet create` consultez le "Référence de commande ONTAP".

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).

  Pour en savoir plus, `network interface` consultez le "Référence de commande ONTAP".

- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

Étapes

1. Créer une LIF :

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

ONTAP 9.5 et versions antérieures
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

ONTAP 9.6 et ultérieur
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true

false}`

- Le `-role` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6).
- Le `-data-protocol` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6). Lors de l'utilisation de ONTAP 9.5 et versions antérieures, le `-data-protocol` Le paramètre doit être spécifié lors de la création de la LIF et ne peut pas être modifié par la suite sans destruction et recréez la LIF de données.
- `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

  Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

- `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Pour en savoir plus sur `network route create` et créer une route statique au sein d'une SVM, consultez la "Référence de commande ONTAP".
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

  Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.

  > Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.

2. Vérifier que le LIF a été créé correctement :

   ```
   network interface show
   ```

3. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier…	Utiliser…
Adresse IPv4	`network ping`

Adresse IPv6	`network ping6`

Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé client1_sub) :

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données datalif1 et datalif3 sont configurées avec des adresses IPv4 et le datalif4 est configuré avec une adresse IPv6 :

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

La commande suivante montre comment créer une LIF de données NAS attribuée avec le `default-data-files` règle de service :

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Informations associées

- "ping réseau"
- "restauration de l'interface réseau"

Activez DNS pour la résolution de nom d'hôte SMB ONTAP

Vous pouvez utiliser `vserver services name-service dns` la commande pour activer DNS sur un SVM et le configurer pour utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes. Pour en savoir plus, `vserver services name-service dns` consultez le "Référence de commande ONTAP".

Avant de commencer

Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. La `vserver services name-service dns create` commande émet un avertissement si vous entrez un seul nom de serveur DNS. Pour en savoir plus, `vserver services name-service dns create` consultez le "Référence de commande ONTAP".

Description de la tâche

En savoir plus sur "Configuration du DNS dynamique sur la SVM".

Étapes

1. Activer le DNS sur le SVM : `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > ⓘ Le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

2. Afficher les configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande.

   La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configurez un serveur SMB dans un domaine Active Directory

Configurez les services de temps ONTAP pour les serveurs SMB

Avant de créer un serveur SMB dans un contrôleur Active Domain, vous devez vous assurer que l'heure du cluster et l'heure sur les contrôleurs de domaine du domaine auquel le serveur SMB appartient correspondent dans les cinq minutes.

Description de la tâche

Vous devez configurer les services NTP du cluster pour utiliser les mêmes serveurs NTP pour la synchronisation que ceux utilisés par le domaine Active Directory.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Étapes

1. Configurer les services de temps à l'aide du `cluster time-service ntp server create` commande.
   - Pour configurer des services de temps sans authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address`
   - Pour configurer des services de temps avec une authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address -key-id key_id`
     `cluster time-service ntp server create -server 10.10.10.1` `cluster time-service ntp server create -server 10.10.10.2`

2. Vérifiez que les services de temps sont correctement configurés à l'aide du `cluster time-service ntp server show` commande.

   `cluster time-service ntp server show`

```
Server                         Version
------------------------------ -------
10.10.10.1                     auto
10.10.10.2                     auto
```

Informations associées

- "ntp du service de temps du cluster"

Commandes ONTAP pour la gestion de l'authentification symétrique sur les serveurs NTP

Depuis ONTAP 9.5, le protocole NTP (Network Time Protocol) version 3 est pris en charge. NTPv3 inclut une authentification symétrique à l'aide de clés SHA-1 qui augmente la sécurité du réseau.

Pour cela…	Utilisez cette commande…
Configurer un serveur NTP sans authentification symétrique	`cluster time-service ntp server create -server server_name`
Configurez un serveur NTP avec une authentification symétrique	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Activer l'authentification symétrique pour un serveur NTP existant le serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configurez une clé NTP partagée	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP
Configurez un serveur NTP avec un ID de clé inconnu	`cluster time-service ntp server create -server server_name -key-id key_id`

Pour cela…	Utilisez cette commande…
Configurez un serveur dont l'ID de clé n'est pas configuré sur le serveur NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` L'ID, le type et la valeur de clé doivent être identiques à l'ID, au type et à la valeur de clé configurés sur le serveur NTP.
Désactiver l'authentification symétrique	`cluster time-service ntp server modify -server server_name -authentication disabled`

Informations associées

- "ntp du service de temps du cluster"

Créez des serveurs SMB dans un domaine ONTAP Active Directory

Vous pouvez utiliser le `vserver cifs create` Commande pour créer un serveur SMB sur le SVM et spécifier le domaine Active Directory (AD) auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM et à un contrôleur de domaine AD du domaine auquel vous souhaitez rejoindre le serveur SMB.

Tout utilisateur autorisé à créer des comptes machine dans le domaine AD auquel vous rejoignez le serveur SMB peut créer le serveur SMB sur la SVM. Cela peut inclure des utilisateurs d'autres domaines.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

Description de la tâche

Lors de la création d'un serveur SMB dans un domaine d'annuaire d'activités :

- Vous devez utiliser le nom de domaine complet (FQDN) lors de la spécification du domaine.
- Le paramètre par défaut consiste à ajouter le compte de machine du serveur SMB à l'objet CN=Computer Active Directory.
- Vous pouvez choisir d'ajouter le serveur SMB à une autre unité organisationnelle (ou) en utilisant le `-ou` option.
- Vous pouvez choisir d'ajouter une liste délimitée par des virgules d'un ou de plusieurs alias NetBIOS (jusqu'à 200) pour le serveur SMB.

  La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs d'origine.

Pour en savoir plus sur les `vserver cifs` paramètres facultatifs et les exigences de dénomination, consultez le "Référence de commande ONTAP".

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine. ONTAP nécessite un cryptage pour les communications du contrôleur de domaine lorsque `-encryption-required -for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3. .

"Gestion SMB" Contient plus d'informations sur les options de configuration du serveur SMB.

Étapes

1. Vérifiez que la licence SMB est installée sur votre cluster : `system license show -package cifs`

   La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

   Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un domaine AD : `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Lorsque vous entrez dans un domaine, cette commande peut prendre plusieurs minutes.

   La commande suivante crée le serveur SMB "`mb_server01"' dans le domaine ""example.com":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   La commande suivante crée le serveur SMB "smb_server02" dans le domaine "m`ydomain.com`" et authentifie l'administrateur ONTAP avec un fichier keytab:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Vérifiez la configuration du serveur SMB à l'aide du `vserver cifs show` commande.

   Dans cet exemple, le résultat de la commande montre qu'un serveur SMB nommé « `SMB_SERVER01' » a été créé sur la SVM vs1.example.com et a été rejoint au domaine « example.com`" domain.

```
cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. Si vous le souhaitez, activez la communication chiffrée avec le contrôleur de domaine (ONTAP 9.8 et versions ultérieures) : `vserver cifs security modify -vserver svm_name -encryption -required-for-dc-connection true`

Exemples

La commande suivante crée un serveur SMB nommé « `smb_server02' » sur le SVM vs2.example.com dans le domaine « example.com`" domain. Le compte machine est créé dans le conteneur « ou=eng,ou=corp,DC=exemple,DC=com ». Un alias NetBIOS est attribué au serveur SMB.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

La commande suivante permet à un utilisateur d'un domaine différent, dans ce cas un administrateur d'un domaine de confiance, de créer un serveur SMB nommé « `MB_server03' » sur le SVM vs3.example.com. Le `-domain` Option spécifie le nom du domaine de départ (spécifié dans la configuration DNS) dans lequel vous souhaitez créer le serveur SMB. Le `username` spécifie l'administrateur du domaine de confiance.

- Home domain : example.com
- Domaine de confiance : trust.lab.com
- Nom d'utilisateur du domaine de confiance : Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Créez des fichiers keytab pour l'authentification SMB ONTAP

Depuis ONTAP 9.7, ONTAP prend en charge l'authentification des SVM avec des serveurs Active Directory (AD) utilisant des fichiers keytab. Les administrateurs AD génèrent un fichier keytab et le rendent disponible aux administrateurs ONTAP sous la forme d'un URI (Uniform Resource identifier), qui est fourni lorsque `vserver cifs` Les commandes exigent une authentification Kerberos avec le domaine AD.

Les administrateurs D'AD peuvent créer les fichiers keytab à l'aide du serveur Windows standard `ktpass` commande. La commande doit être exécutée sur le domaine principal où une authentification est requise. Le `ktpass` la commande peut être utilisée pour générer des fichiers keytab uniquement pour les utilisateurs du domaine principal ; les clés générées à l'aide d'utilisateurs du domaine approuvé ne sont pas prises en charge.

Les fichiers keytab sont générés pour des utilisateurs ONTAP admin spécifiques. Tant que le mot de passe de l'utilisateur administrateur ne change pas, les clés générées pour le type de cryptage et le domaine spécifiques ne changent pas. Par conséquent, un nouveau fichier keytab est requis chaque fois que le mot de passe de l'utilisateur admin est modifié.

Les types de cryptage suivants sont pris en charge :

- AES256-SHA1
- DES-CBC-MD5

  ⓘ ONTAP ne prend pas en charge le type de cryptage DES-CBC-CRC.

- RC4-HMAC

AES256 est le type de cryptage le plus élevé et doit être utilisé si activé sur le système ONTAP.

Les fichiers keytab peuvent être générés en spécifiant le mot de passe admin ou en utilisant un mot de passe généré de manière aléatoire. Toutefois, une seule option de mot de passe peut être utilisée à un moment donné, car une clé privée spécifique à l'utilisateur admin est nécessaire au serveur AD pour déchiffrer les clés à l'intérieur du fichier keytab. Toute modification de la clé privée d'un administrateur spécifique invalidera le fichier keytab.

Configurer un serveur SMB dans un groupe de travail

Découvrez la configuration des serveurs SMB dans les groupes de travail ONTAP

La configuration d'un serveur SMB en tant que membre d'un groupe de travail consiste à créer le serveur SMB, puis à créer des utilisateurs et des groupes locaux.

Vous pouvez configurer un serveur SMB dans un groupe de travail lorsque l'infrastructure de domaine Microsoft Active Directory n'est pas disponible.

Un serveur SMB en mode groupe de travail prend uniquement en charge l'authentification NTLM et ne prend pas en charge l'authentification Kerberos.

Créez des serveurs SMB sur le SVM ONTAP avec des groupes de travail spécifiques

Vous pouvez utiliser le `vserver cifs create` Commande permettant de créer un serveur SMB sur le SVM et de spécifier le groupe de travail auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM.

Description de la tâche

Les serveurs SMB en mode groupe de travail ne prennent pas en charge les fonctions SMB suivantes :

- Protocole SMB3 témoin
- Partages CA SMB3
- SQL sur SMB
- Redirection de dossiers
- Profils d'itinérance
- Objet de stratégie de groupe (GPO)
- Service Snapshot de volume (VSS)

Pour en savoir plus sur les `vserver cifs` paramètres de configuration facultatifs et les exigences de dénomination, reportez-vous à "Référence de commande ONTAP"la section .

Étapes

1. Vérifiez que la licence SMB est installée sur votre cluster : `system license show -package cifs`

   La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

   Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un groupe de travail : `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   La commande suivante crée le serveur SMB "``mb_server01'" dans le groupe de travail ""workgroup01"":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Vérifiez la configuration du serveur SMB à l'aide du `vserver cifs show` commande.

   Dans l'exemple suivant, la sortie de la commande montre qu'un serveur SMB nommé « `MB_server01' » a été créé sur SVM vs1.example.com dans le groupe de travail « workgroup01 » :

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Une fois que vous avez terminé

Pour un serveur CIFS au sein d'un groupe de travail, vous devez créer des utilisateurs locaux, et éventuellement des groupes locaux, sur la SVM.

Informations associées

"Gestion SMB"

Créez des comptes utilisateur SMB ONTAP locaux

Vous pouvez créer un compte utilisateur local qui peut être utilisé pour autoriser l'accès aux données contenues dans la SVM sur une connexion SMB. Vous pouvez également utiliser les comptes utilisateur locaux pour l'authentification lors de la création d'une session SMB.

Description de la tâche

La fonctionnalité des utilisateurs locaux est activée par défaut lors de la création du SVM.

Lorsque vous créez un compte utilisateur local, vous devez spécifier un nom d'utilisateur et spécifier le SVM avec lequel associer le compte.

Pour en savoir plus sur les `vserver cifs users-and-groups local-user` paramètres facultatifs et les exigences de dénomination, consultez le "Référence de commande ONTAP".

Étapes

1. Créez l'utilisateur local : `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Les paramètres facultatifs suivants peuvent s'avérer utiles :

   - `-full-name`

     Nom complet de l'utilisateur.

   - `-description`

Description de l'utilisateur local.

- `-is-account-disabled {true|false}`

  Indique si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, la valeur par défaut est d'activer le compte utilisateur.

La commande demande le mot de passe de l'utilisateur local.

2. Entrez un mot de passe pour l'utilisateur local, puis confirmez le mot de passe.
3. Vérifiez que l'utilisateur a bien été créé : `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemple

L'exemple suivant crée un utilisateur local « `SMB_SERVER01\sue`, avec un nom complet « `Sue Chang` », associé à SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Créez des groupes SMB ONTAP locaux

Vous pouvez créer des groupes locaux qui peuvent être utilisés pour autoriser l'accès aux données associées à la SVM sur une connexion SMB. Vous pouvez également attribuer des privilèges qui définissent les droits d'utilisateur ou les capacités dont dispose un membre du groupe.

Description de la tâche

La fonctionnalité de groupe local est activée par défaut lors de la création du SVM.

Lorsque vous créez un groupe local, vous devez spécifier un nom pour le groupe et vous devez spécifier la SVM avec laquelle associer le groupe. Vous pouvez spécifier un nom de groupe avec ou sans le nom de domaine local, et vous pouvez éventuellement spécifier une description pour le groupe local. Vous ne pouvez pas ajouter un groupe local à un autre groupe local.

Pour en savoir plus sur les `vserver cifs users-and-groups local-group` paramètres facultatifs et les exigences de dénomination, consultez le "Référence de commande ONTAP".

Étapes

1. Créez le groupe local : `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   Le paramètre facultatif suivant peut être utile :

   - `-description`

     Description du groupe local.

2. Vérifiez que le groupe a bien été créé : `vserver cifs users-and-groups local-group show -vserver vserver_name`

Exemple

L'exemple suivant crée un groupe local « `SMB_SERVER01\engineering" associé à la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ------------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Une fois que vous avez terminé

Vous devez ajouter des membres au nouveau groupe.

Gérez l'appartenance au groupe SMB ONTAP local

Vous pouvez gérer l'appartenance à un groupe local en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et supprimant des groupes de domaines. Cette option est utile si vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe.

Description de la tâche

Si vous ne souhaitez plus qu'un utilisateur local, un utilisateur de domaine ou un groupe de domaines dispose de droits d'accès ou de privilèges en fonction de l'appartenance à un groupe, vous pouvez supprimer le membre du groupe.

Lorsque vous ajoutez des membres à un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial *Everyone*.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, ONTAP doit pouvoir résoudre le nom en SID.

Lorsque vous supprimez des membres d'un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas supprimer des membres du groupe spécial *Everyone*.
- Pour supprimer un membre d'un groupe local, ONTAP doit pouvoir résoudre son nom en SID.

Étapes

1. Ajouter un membre à un groupe ou en supprimer.
   - Ajouter un membre : `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à ajouter au groupe local spécifié.

   - Supprimer un membre : `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à supprimer du groupe local spécifié.

Exemples

L'exemple suivant ajoute un utilisateur local « `SMB_SERVER01\sue' au groupe local « `SMB_SERVER01\engineering' » sur le SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

L'exemple suivant supprime les utilisateurs locaux « `SMB_SERVER01\sue` » et « SMB_SERVER01\james` du groupe local « `SMB_SERVER01\engineering' » sur la SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Vérifiez les versions SMB de ONTAP activées

Votre version de ONTAP 9 détermine quelles versions de SMB sont activées par défaut pour les connexions avec les clients et les contrôleurs de domaine. Vérifiez que le serveur SMB prend en charge les clients et les fonctionnalités requis dans votre environnement.

Description de la tâche

Pour les connexions avec les clients et les contrôleurs de domaine, vous devez activer SMB 2.0 et versions ultérieures autant que possible. Pour des raisons de sécurité, évitez d'utiliser SMB 1.0 et désactivez-le si vous avez vérifié qu'il n'est pas nécessaire dans votre environnement.

Depuis ONTAP 9.3, il est désactivé par défaut sur les nouveaux SVM.

> Si `-smb1-enabled-for-dc-connections` est défini sur `false` pendant `-smb1-enabled` est défini sur `true`, ONTAP refuse les connexions SMB 1.0 en tant que client, mais continue à accepter les connexions SMB 1.0 entrantes en tant que serveur.

"Gestion SMB" Le contient des détails sur les versions et fonctionnalités SMB prises en charge.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez les versions SMB activées :

   ```
   vserver cifs options show
   ```

   Vous pouvez faire défiler la liste pour afficher les versions SMB activées pour les connexions client et si vous configurez un serveur SMB dans un domaine AD, pour les connexions de domaine AD.

3. Activez ou désactivez le protocole SMB pour les connexions client si nécessaire :
   - Pour activer une version SMB :

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     true
     ```

     Valeurs possibles pour `smb_version`:

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

       La commande suivante active SMB 3.1 sur SVM vs1.example.com :
       `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31 -enabled true`

   - Pour désactiver une version SMB :

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Si votre serveur SMB se trouve dans un domaine Active Directory, activez ou désactivez le protocole SMB pour les connexions DC selon les besoins :
   - Pour activer une version SMB :

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - Pour désactiver une version SMB :

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

Mappez les serveurs SMB ONTAP sur le serveur DNS

Le serveur DNS de votre site doit avoir une entrée pointant sur le nom du serveur SMB, et tous les alias NetBIOS, à l'adresse IP de la LIF de données afin que les utilisateurs Windows puissent mapper un disque au nom du serveur SMB.

Avant de commencer

Vous devez avoir un accès administratif au serveur DNS de votre site. Si vous ne disposez pas d'un accès administratif, vous devez demander à l'administrateur DNS d'effectuer cette tâche.

Description de la tâche

Si vous utilisez des alias NetBIOS pour le nom du serveur SMB, il est recommandé de créer des points d'entrée de serveur DNS pour chaque alias.

Étapes

1. Connectez-vous au serveur DNS.
2. Créer des entrées de recherche de type a - Address record (enregistrement d'adresse A) et inverse (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de la LIF de données.
3. Si vous utilisez des alias NetBIOS, créez une entrée de recherche alias nom canonique (enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de la LIF de données du serveur SMB.

Résultats

Une fois le mappage propagé sur le réseau, les utilisateurs Windows peuvent mapper un lecteur au nom du serveur SMB ou à ses alias NetBIOS.

Configurez l'accès client SMB au stockage partagé

Configurez l'accès du client SMB au stockage ONTAP partagé

Pour fournir un accès client SMB au stockage partagé d'un SVM, vous devez créer un volume ou qtree pour fournir un conteneur de stockage, puis créer ou modifier un partage pour ce conteneur. Vous pouvez ensuite configurer les autorisations de partage et de fichier, et tester l'accès depuis les systèmes clients.

Avant de commencer

- SMB doit être entièrement configuré sur le SVM.
- Toute mise à jour de la configuration des services de noms doit être terminée.
- Tout ajout ou modification d'un domaine Active Directory ou d'une configuration de groupe de travail doit être effectué.

Créer un volume ou un conteneur de stockage qtree

Créez des volumes SMB ONTAP

Vous pouvez créer un volume et spécifier son point de jonction et d'autres propriétés en utilisant le `volume create` commande.

Description de la tâche

Un volume doit inclure une *Junction path* pour que ses données soient mises à disposition des clients. Vous pouvez spécifier le chemin de jonction lorsque vous créez un nouveau volume. Si vous créez un volume sans spécifier un chemin de jonction, vous devez *mount* le volume du namespace du SVM à l'aide de `volume mount` commande.

Avant de commencer

- SMB doit être configuré et opérationnel.
- La sécurité de type SVM doit être NTFS.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes avec les fonctions d'analyse de la capacité et de suivi des activités activées. Pour activer le suivi de capacité ou d'activité, exécutez la `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` définissez sur `on`.

  Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "Activez l'analyse du système de fichiers". Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

Étapes

1. Créer le volume avec un point de jonction : `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*`]`

   Les choix pour `-junction-path` sont les suivants :

   - Directement sous la racine, par exemple, `/new_vol`

     Vous pouvez créer un nouveau volume et préciser qu'il peut être monté directement sur le volume root

du SVM.

- Sous un répertoire existant, par exemple, `/existing_dir/new_vol`

  Vous pouvez créer un nouveau volume et spécifier qu'il doit être monté sur un volume existant (dans une hiérarchie existante), exprimé en tant que répertoire.

Si vous souhaitez créer un volume dans un nouveau répertoire (dans une nouvelle hiérarchie sous un nouveau volume), par exemple, `/new_dir/new_vol`, Ensuite, vous devez d'abord créer un nouveau volume parent qui est relié par une jonction au volume racine de la SVM. Vous devez ensuite créer le nouveau volume enfant dans la Junction path du nouveau volume parent (nouveau répertoire).

2. Vérifier que le volume a été créé avec le point de jonction souhaité : `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Exemples

La commande suivante crée un nouveau volume nommé users1 sur le SVM vs1.example.com et l'agrégat aggr1. Le nouveau volume est disponible sur le site `/users`. Le volume a une taille de 750 Go et sa garantie de volume est de type volume (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

La commande suivante crée un nouveau volume nommé « maison 4 » sur la SVM « vs1.example.com`" » et l'agrégat « aggr1 ». Le répertoire `/eng/` Existe déjà dans l'espace de nommage de la SVM vs1, et le nouveau volume est mis à disposition à `/eng/home`, qui devient le répertoire de base de l' `/eng/` espace de noms. Le volume a une taille de 750 Go et sa garantie de volume est de type `volume` (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Création de qtrees ONTAP SMB

Vous pouvez créer un qtree pour contenir vos données et spécifier ses propriétés en utilisant le `volume qtree create` commande.

Avant de commencer

- La SVM et le volume qui contiendra le nouveau qtree doivent déjà exister.
- Le style de sécurité du SVM doit être NTFS et SMB doit être configuré et en cours d'exécution.

Étapes

1. Créer le qtree : `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   Vous pouvez spécifier le volume et qtree en tant qu'arguments distincts ou spécifier l'argument du chemin qtree au format `/vol/volume_name/_qtree_name`.

2. Vérifier que le qtree a été créé avec le chemin de jonction souhaité : `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Exemple

L'exemple suivant crée un qtree nommé qt01 situé sur le SVM vs1.example.com qui dispose d'un chemin de jonction `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                    Vserver Name: vs1.example.com
                     Volume Name: data1
                      Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                  Security Style: ntfs
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                         Qtree Id: 2
                     Qtree Status: normal
                   Export Policy: default
        Is Export Policy Inherited: true
```

Configuration requise et éléments à prendre en compte lors de la création de partages SMB ONTAP

Avant de créer un partage SMB, vous devez comprendre les exigences en matière de chemins de partage et de propriétés de partage, en particulier pour les répertoires

locaux.

La création d'un partage SMB implique la spécification d'une structure de chemin d'accès au répertoire (à l'aide de `-path` dans le `vserver cifs share create` commande) à laquelle les clients accèdent. Le chemin du répertoire correspond à la Junction path d'un volume ou qtree que vous avez créé dans le SVM namespace. Le chemin du répertoire et le chemin de jonction correspondant doivent exister avant de créer votre partage.

Les chemins de partage ont les exigences suivantes :

- Le chemin d'accès à un répertoire peut comporter jusqu'à 255 caractères.
- Si un espace est présent dans le chemin d'accès, toute la chaîne doit être placée entre guillemets (par exemple, `"/new volume/mount here"`).
- Si le chemin UNC (`\\servername\sharename\filepath`) Du partage contient plus de 256 caractères (à l'exception de la valeur initiale "\" dans le chemin UNC), alors l'onglet **Security** de la zone Propriétés de Windows n'est pas disponible.

  Il s'agit d'un problème de client Windows plutôt que d'un problème ONTAP. Pour éviter ce problème, ne créez pas de partages avec des chemins UNC de plus de 256 caractères.

Les valeurs par défaut des propriétés de partage peuvent être modifiées :

- Les propriétés initiales par défaut de tous les partages sont `oplocks`, `browsable`, `changenotify`, et `show-previous-versions`.
- Lorsque vous créez un partage, il est facultatif de spécifier des propriétés de partage.

  Toutefois, si vous spécifiez des propriétés de partage lorsque vous créez le partage, les valeurs par défaut ne sont pas utilisées. Si vous utilisez le `-share-properties` paramètre lorsque vous créez un partage, vous devez spécifier toutes les propriétés de partage que vous souhaitez appliquer au partage à l'aide d'une liste délimitée par des virgules.

- Pour désigner un partage de répertoire personnel, utilisez le `homedirectory` propriété.

  Cette fonctionnalité vous permet de configurer un partage qui correspond à différents répertoires en fonction de l'utilisateur qui se connecte à celui-ci et d'un ensemble de variables. Au lieu de devoir créer des partages distincts pour chaque utilisateur, vous pouvez configurer un partage unique avec quelques paramètres de home Directory afin de définir la relation d'un utilisateur entre un point d'entrée (le partage) et son home Directory (un répertoire sur le SVM).

  Vous ne pouvez pas ajouter ou supprimer cette propriété après avoir créé le partage.

Les partages de home Directory présentent les exigences suivantes :

- Avant de créer des home directories SMB, vous devez ajouter au moins un chemin de recherche de répertoire personnel à l'aide de l' `vserver cifs home-directory search-path add` commande.
- Partages de répertoire personnel spécifiés par la valeur de `homedirectory` sur le `-share-properties` le paramètre doit inclure le `%w` (Nom d'utilisateur Windows) variable dynamique dans le nom de partage.

  Le nom du partage peut également contenir le `%d` (nom de domaine) variable dynamique (par exemple, `%d/%w`) ou une partie statique dans le nom du partage (par exemple, `home1_%w`).

- Si le partage est utilisé par les administrateurs ou les utilisateurs pour se connecter aux répertoires d'accueil d'autres utilisateurs (à l'aide des options de l' `vserver cifs home-directory modify` commande), le modèle de nom de partage dynamique doit être précédé d'un tilde (~).

Pour en savoir plus, `vserver cifs share` consultez le "Référence de commande ONTAP".

Informations associées

- "Gestion SMB"

Créer des partages SMB ONTAP

Vous devez créer un partage SMB avant de pouvoir partager des données d'un serveur SMB avec des clients SMB. Lorsque vous créez un partage, vous pouvez définir des propriétés de partage, telles que la désignation du partage comme répertoire de base. Vous pouvez également personnaliser le partage en configurant des paramètres facultatifs.

Avant de commencer

Le chemin de répertoire du volume ou qtree doit exister dans le namespace du SVM avant de créer le partage.

Description de la tâche

Lorsque vous créez un partage, l'ACL de partage par défaut (autorisations de partage par défaut) est `Everyone / Full Control`. Après avoir testé l'accès au partage, vous devez supprimer la liste ACL de partage par défaut et la remplacer par une alternative plus sécurisée.

Étapes

1. Si nécessaire, créez la structure du chemin d'accès au répertoire pour le partage.

   Le `vserver cifs share create` la commande vérifie le chemin d'accès spécifié dans `-path` option pendant la création du partage. Si le chemin spécifié n'existe pas, la commande échoue.

2. Créer un partage SMB associé au SVM spécifié : `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Vérifiez que le partage a été créé :`vserver cifs share show -share-name share_name`

Exemples

La commande suivante crée un partage SMB nommé « `PARE1' » sur le SVM `vs1.example.com`. Son chemin de répertoire est `/users`, et il est créé avec les propriétés par défaut.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Vérifiez l'accès du client SMB ONTAP

Vérifiez que SMB est correctement configuré en accédant au partage et en écrivant les données. Vous devez tester l'accès à l'aide du nom du serveur SMB et de tout alias NetBIOS.

Étapes

1. Connectez-vous à un client Windows.
2. Testez l'accès à l'aide du nom du serveur SMB :

   a. Dans l'Explorateur Windows, mappez un lecteur sur le partage au format suivant : `\\SMB_Server_Name\Share_Name`

      Si le mappage ne réussit pas, il est possible que le mappage DNS ne se soit pas encore propagé sur l'ensemble du réseau. Vous devez tester l'accès par la suite à l'aide du nom de serveur SMB.

      Si le serveur SMB est nommé vs1.example.com et que le partage est nommé SHARE1, vous devez entrer ce qui suit : `\\vs0.example.com\SHARE1`

   b. Sur le lecteur nouvellement créé, créez un fichier test, puis supprimez le fichier.

   Vous avez vérifié l'accès en écriture au partage à l'aide du nom du serveur SMB.

3. Répétez l'étape 2 pour tous les alias NetBIOS.

Créez des listes de contrôle d'accès pour les partages SMB ONTAP

La configuration des autorisations de partage en créant des listes de contrôle d'accès (ACL) pour les partages SMB vous permet de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes.

Avant de commencer

Vous devez avoir déterminé quels utilisateurs ou groupes auront accès au partage.

Description de la tâche

Vous pouvez configurer des listes de contrôle d'accès au niveau du partage en utilisant des noms d'utilisateur

ou de groupe Windows locaux ou de domaine.

Avant de créer une nouvelle liste de contrôle d'accès, vous devez supprimer la liste de contrôle d'accès de partage par défaut `Everyone / Full Control`, qui pose un risque pour la sécurité.

En mode Workgroup, le nom de domaine local est le nom du serveur SMB.

Étapes

1. Supprimez la liste ACL de partage par défaut :`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configurer la nouvelle liste de contrôle d'accès :

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un…	Entrez la commande…
Utilisateur Windows	`vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right`
Groupe Windows	`vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right`

3. Vérifiez que la liste de contrôle d'accès appliquée au partage est correcte à l'aide de la `vserver cifs share access-control show` commande.

Exemple

La commande suivante donne `Change` Autorisations au groupe Windows "sales Team" pour la part "sales" sur le groupe ""vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$         BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales      DOMAIN\"Sales Team"     windows     Change
```

Les commandes suivantes fournissent `Change` L'autorisation au groupe Windows local nommé « Tiger Team » et `Full_Control` Autorisation à l'utilisateur Windows local nommé "rue Chang" pour le partage "vatavol5" sur le SVM ""vs1":

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configurez les autorisations de fichier NTFS dans les partages SMB ONTAP

Pour permettre l'accès aux fichiers aux utilisateurs ou aux groupes qui ont accès à un partage, vous devez configurer les autorisations de fichiers NTFS sur les fichiers et les répertoires de ce partage à partir d'un client Windows.

Avant de commencer

L'administrateur effectuant cette tâche doit disposer d'autorisations NTFS suffisantes pour modifier les autorisations sur les objets sélectionnés.

Description de la tâche

"Gestion SMB" De plus, votre documentation Windows contient des informations sur la définition des autorisations NTFS standard et avancées.

Étapes

1. Connectez-vous à un client Windows en tant qu'administrateur.
2. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
3. Complétez la boîte **Map Network Drive** :

   a. Sélectionnez une lettre **lecteur**.

   b. Dans la zone **dossier**, saisissez le nom du serveur SMB contenant le partage contenant les données auxquelles vous souhaitez appliquer les autorisations, ainsi que le nom du partage.

      Si le nom de votre serveur SMB est SMB_SERVER01 et que votre partage est nommé "SHARE1", entrez `\\SMB_SERVER01\SHARE1`.

      Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

   c. Cliquez sur **Terminer**.

   Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

4. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez définir les autorisations de fichier NTFS.
5. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
6. Sélectionnez l'onglet **sécurité**.

   L'onglet sécurité affiche la liste des utilisateurs et des groupes pour lesquels les autorisations NTFS sont définies. La zone autorisations pour <objet> affiche la liste des autorisations Autoriser et refuser en vigueur pour l'utilisateur ou le groupe sélectionné.

7. Cliquez sur **Modifier**.

   La case autorisations pour <objet> s'ouvre.

8. Effectuez les opérations souhaitées :

Si vous voulez	Procédez comme suit…
Définissez les autorisations NTFS standard pour un nouvel utilisateur ou un nouveau groupe	a. Cliquez sur **Ajouter**. La fenêtre Sélectionner un utilisateur, des ordinateurs, des comptes de service ou des groupes s'ouvre. b. Dans la zone **Entrez les noms d'objet à sélectionner**, saisissez le nom de l'utilisateur ou du groupe sur lequel vous souhaitez ajouter l'autorisation NTFS. c. Cliquez sur **OK**.
Modifiez ou supprimez des autorisations NTFS standard d'un utilisateur ou d'un groupe	Dans la zone **Groupe ou noms d'utilisateur**, sélectionnez l'utilisateur ou le groupe que vous souhaitez modifier ou supprimer.

9. Effectuez les opérations souhaitées :

Les fonctions que vous recherchez…	Procédez comme suit
Définissez les autorisations NTFS standard pour un utilisateur ou un groupe existant ou nouveau	Dans la zone **permissions pour <objet>**, sélectionnez les cases **Autoriser** ou **refuser** pour le type d'accès que vous souhaitez autoriser ou non pour l'utilisateur ou le groupe sélectionné.
Supprimer un utilisateur ou un groupe	Cliquez sur **Supprimer**.

Si certaines ou toutes les zones d'autorisation standard ne sont pas sélectionnables, c'est parce que les autorisations sont héritées de l'objet parent. La case **autorisations spéciales** n'est pas sélectionnable. Si elle est sélectionnée, cela signifie qu'un ou plusieurs des droits avancés granulaires ont été définis pour l'utilisateur ou le groupe sélectionné.

10. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des autorisations NTFS sur cet objet, cliquez sur **OK**.

Vérifiez l'accès au partage d'utilisateurs SMB ONTAP

Vous devez tester que les utilisateurs que vous avez configurés peuvent accéder au partage SMB et aux fichiers qu'il contient.

Étapes

1. Sur un client Windows, connectez-vous en tant qu'un des utilisateurs qui ont désormais accès au partage.
2. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
3. Complétez la boîte **Map Network Drive** :

   a. Sélectionnez une lettre **lecteur**.

   b. Dans la zone **dossier**, saisissez le nom de partage que vous fournissez aux utilisateurs.

Si le nom de votre serveur SMB est SMB_SERVER01 et que votre partage est nommé "SHARE1", entrez `\\SMB_SERVER01\share1`.

c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

4. Créez un fichier de test, vérifiez qu'il existe, écrivez du texte et supprimez le fichier de test.

Gestion de SMB avec l'interface de ligne de commandes

Découvrez ONTAP SMB

Les fonctionnalités d'accès aux fichiers ONTAP sont disponibles pour le protocole SMB. Vous pouvez activer un serveur CIFS, créer des partages et activer les services Microsoft.

SMB (Server message Block) désigne les dialectes modernes du protocole CIFS (Common Internet File System). Vous verrez toujours *CIFS* dans l'interface de ligne de commande (CLI) ONTAP et dans les outils de gestion OnCommand.

Prise en charge du serveur SMB

En savoir plus sur la prise en charge des serveurs SMB ONTAP

Vous pouvez activer et configurer des serveurs SMB sur des SVM (Storage Virtual machines) pour que les clients SMB puissent accéder aux fichiers du cluster.

- Chaque SVM de données du cluster peut être lié à un domaine Active Directory exactement.
- Les SVM de données n'ont pas besoin d'être liés au même domaine.
- Plusieurs SVM peuvent être liés au même domaine.

Vous devez configurer les SVM et les LIF que vous utilisez pour transmettre des données avant de pouvoir créer un serveur SMB. Si votre réseau de données n'est pas stable, vous devrez peut-être aussi configurer les IPspaces, les domaines de diffusion et les sous-réseaux.

Informations associées

"Gestion du réseau"

Modifier les serveurs

"Administration du système"

Prise en charge des versions SMB et des fonctionnalités de ONTAP

Server message Block (SMB) est un protocole de partage de fichiers distant utilisé par les clients et les serveurs Microsoft Windows. Toutes les versions de SMB sont prises en charge. Vérifiez que le serveur ONTAP SMB prend en charge les clients et les fonctionnalités requis dans votre environnement.

Les dernières informations sur les clients SMB et les contrôleurs de domaine pris en charge par ONTAP sont disponibles dans l'outil *Interoperability Matrix Tool*.

SMB 2.0 et les versions ultérieures sont activées par défaut pour les serveurs SMB ONTAP et peuvent être activées ou désactivées selon les besoins. SMB 1.0 peut être activé ou désactivé selon les besoins.

> Les paramètres par défaut des connexions SMB 1.0 et 2.0 aux contrôleurs de domaine dépendent également de la version de ONTAP. Pour en savoir plus, `vserver cifs security modify` consultez le "Référence de commande ONTAP". Pour les environnements avec des serveurs CIFS existants exécutant SMB 1.0, vous devez migrer vers une version SMB ultérieure dès que possible pour préparer des améliorations en matière de sécurité et de conformité. Contactez votre représentant NetApp pour plus d'informations.

Le tableau suivant indique les fonctionnalités SMB prises en charge dans chaque version de SMB. Certaines fonctionnalités SMB sont activées par défaut et d'autres requièrent une configuration supplémentaire.

Cette fonctionnalité:	**Nécessite une activation:**	**Est pris en charge dans ONTAP 9 pour ces versions SMB:**	
		3.0	3.1.1
Fonctionnalité SMB 1.0 héritée		X	X
Poignées durables		X	X
Opérations cumulées		X	X
Opérations asynchrones		X	X
Tailles de tampon de lecture et d'écriture améliorées		X	X
Évolutivité optimisée		X	X
Signature SMB	X	X	X
Autre format de fichier ADS (Data Stream)	X	X	X
MTU important (activé par défaut à partir de ONTAP 9.7)	X	X	X
Oplocks de location		X	X
Partages disponibles en permanence	X	X	X

Cette fonctionnalité:	Nécessite une activation:	Est pris en charge dans ONTAP 9 pour ces versions SMB:	
Pointeurs permanents		X	X
Témoin		X	X
CHIFFREMENT SMB : AES-128-CCM	X	X	X
Évolutivité horizontale (requise par les partages de CA)		X	X
Basculement transparent		X	X
Multicanal SMB (à partir de ONTAP 9.4)	X	X	X
Intégrité de la pré-authentification			X
Basculement client cluster v.2 (CCFv2)			X
CHIFFREMENT SMB : AES-128-GCM	X		X

Informations associées

Découvrez comment utiliser la signature ONTAP pour améliorer la sécurité du réseau

Définir le niveau de sécurité minimum d'authentification du serveur

Configuration du chiffrement SMB requis sur les serveurs SMB pour les transferts de données sur SMB

"Interopérabilité NetApp"

Fonctionnalités Windows non prises en charge dans ONTAP SMB

Avant d'utiliser CIFS sur votre réseau, vous devez connaître certaines fonctionnalités Windows que ONTAP ne prend pas en charge.

ONTAP ne prend pas en charge les fonctionnalités Windows suivantes :

- Système de fichiers crypté (EFS)
- Consignation des événements NTFS (NT File System) dans le journal des modifications
- Service FRS (File Replication Service) Microsoft
- Service d'indexation Microsoft Windows

- Stockage distant via HSM (gestion hiérarchique du stockage)
- Gestion des quotas des clients Windows
- Sémantique du quota Windows
- Le fichier LMHOSTS
- Compression native NTFS

Configurer les services de noms NIS ou LDAP sur les SVM SMB ONTAP

L'accès SMB permet de mapper un utilisateur UNIX, même en cas d'accès aux données d'un volume NTFS de type sécurité. Si vous associez des utilisateurs Windows aux utilisateurs UNIX correspondants dont les informations sont stockées dans des magasins d'annuaire NIS ou LDAP, ou si vous utilisez LDAP pour le mappage de noms, vous devez configurer ces services de noms au cours de l'installation SMB.

Avant de commencer

Vous devez avoir personnalisé la configuration de votre base de données de services de noms afin qu'elle corresponde à votre infrastructure de service de noms.

Description de la tâche

Les SVM utilisent les bases de données de name services ns-switch pour déterminer l'ordre dans lequel rechercher les sources d'une base de données de name-service donnée. La source du commutateur ns peut être n'importe quelle combinaison de `files`, , `nis` ou `ldap`. Pour la base de données des groupes, ONTAP tente d'obtenir les appartenances de groupe de toutes les sources configurées, puis utilise les informations d'appartenance de groupe consolidées pour les contrôles d'accès. Si l'une de ces sources n'est pas disponible au moment de l'obtention des informations du groupe UNIX, ONTAP ne peut pas obtenir les informations d'identification UNIX complètes et les vérifications d'accès ultérieures peuvent échouer. Par conséquent, vous devez toujours vérifier que toutes les sources du commutateur ns sont configurées pour la base de données du groupe dans les paramètres du commutateur ns.

Par défaut, le serveur SMB doit mapper tous les utilisateurs Windows à l'utilisateur UNIX par défaut stocké dans le serveur local `passwd` base de données. Si vous souhaitez utiliser la configuration par défaut, la configuration des services de nom d'utilisateur et de groupe NIS ou LDAP UNIX ou le mappage d'utilisateur LDAP est facultative pour l'accès SMB.

Étapes

1. Si les informations utilisateur, groupe et groupe de réseau UNIX sont gérées par les services de noms NIS, configurez les services de noms NIS :

   a. Déterminez la commande actuelle des services de noms à l'aide du `vserver services name-service ns-switch show` commande.

      Dans cet exemple, les trois bases de données (`group`, `passwd`, et `netgroup`) qui peut utiliser `nis` en tant que source de service de nom n'utilisent que `files` comme source.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

```
                                                          Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            files
vs1             passwd         true            files
vs1             netgroup       true            files
vs1             namemap        true            files
```

Vous devez ajouter le `nis` source vers le `group` et `passwd` les bases de données, et éventuellement au `netgroup` base de données.

b. Réglez l'ordre de la base de données du commutateur ns-service de noms en utilisant le `vserver services name-service ns-switch modify` commande.

   Pour obtenir des performances optimales, vous ne devez pas ajouter de service de noms à une base de données de services de noms, sauf si vous prévoyez de configurer ce service de noms sur la SVM.

   Si vous modifiez la configuration de plusieurs bases de données de service de noms, vous devez exécuter la commande séparément pour chaque base de données de service de noms que vous souhaitez modifier.

   Dans cet exemple, `nis` et `files` sont configurés comme sources pour le `group` et `passwd` les bases de données, dans cet ordre. Les bases de données restantes du service de noms ne sont pas modifiées.

   ```
   vserver services name-service ns-switch modify -vserver vs1 -database group
   -sources nis,files vserver services name-service ns-switch modify -vserver
   vs1 -database passwd -sources nis,files
   ```

c. Vérifiez que l'ordre des services de noms est correct en utilisant le `vserver services name-service ns-switch show` commande.

   ```
   vserver services name-service ns-switch show -vserver vs1
   ```

```
                                                          Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            nis,
                                                files
vs1             passwd         true            nis,
                                                files
vs1             netgroup       true            files
vs1             namemap        true            files
```

d. Créez la configuration du service de nom NIS :
`vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…`

`vserver services name-service nis-domain create -vserver vs1 -domain example.com -servers 10.0.0.60`

d' hôte, soit une adresse IP pour le serveur NIS.

e. Vérifiez que le service de nom NIS est correctement configuré : `vserver services name-service nis-domain show vserver <vserver_name>`

`vserver services name-service nis-domain show vserver vs1`

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. Si les informations utilisateur, groupe et groupe de réseau UNIX ou le mappage de nom sont gérés par les services de noms LDAP, configurez les services de noms LDAP à l'aide des informations situées "Gestion NFS".

En savoir plus sur la configuration des commutateurs du service de nom SMB de ONTAP

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX. Vous devez connaître les fonctions du tableau et savoir comment ONTAP l'utilise pour que vous puissiez le configurer de façon appropriée pour votre environnement.

La table commutateur de service de nom ONTAP détermine les sources de service de nom auxquelles ONTAP consulte afin de récupérer les informations relatives à un certain type d'informations de service de nom. ONTAP conserve une table de commutateur de service de noms distincte pour chaque SVM.

Types de base de données

La table stocke une liste de services de noms distincte pour chacun des types de bases de données suivants :

Type de base de données	Définit les sources de service de noms pour…	Les sources valides sont…
hôtes	Conversion des noms d'hôte en adresses IP	fichiers, dns
groupe	Recherche des informations sur les groupes d'utilisateurs	fichiers, nis, ldap
passwd	Recherche des informations utilisateur	fichiers, nis, ldap

Type de base de données	Définit les sources de service de noms pour…	Les sources valides sont…
groupe réseau	Recherche des informations de groupe réseau	fichiers, nis, ldap
carte de nom	Mappage des noms d'utilisateur	fichiers, ldap

Types de source

Les sources indiquent quelle source de service de nom utiliser pour récupérer les informations appropriées.

Spécifiez le type de source…	Pour rechercher des informations dans…	Géré par les familles de commande…

fichiers	Fichiers source locaux	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Serveurs NIS externes tels que spécifiés dans la configuration de domaine NIS du SVM	`vserver services name-service nis-domain`
ldap	Serveurs LDAP externes comme spécifié dans la configuration du client LDAP du SVM	`vserver services name-service ldap`
dns	Serveurs DNS externes comme spécifié dans la configuration DNS du SVM	`vserver services name-service dns`

Même si vous prévoyez d'utiliser NIS ou LDAP pour l'accès aux données et l'authentification d'administration des SVM, vous devez toujours inclure `files` Et configurer des utilisateurs locaux comme un repli en cas d'échec de l'authentification NIS ou LDAP.

Protocoles utilisés pour accéder à des sources externes

Pour accéder aux serveurs pour des sources externes, ONTAP utilise les protocoles suivants :

Source de service de nom externe	Protocole utilisé pour l'accès
NIS	UDP
DNS	UDP

Source de service de nom externe	Protocole utilisé pour l'accès
LDAP	TCP

Exemple

L'exemple suivant affiche la configuration du commutateur de service de nom pour le SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Pour rechercher des informations sur les utilisateurs ou les groupes, ONTAP consulte uniquement les fichiers sources locales. Si la requête ne renvoie aucun résultat, la recherche échoue.

Pour rechercher des informations sur le groupe réseau, ONTAP consulte d'abord les serveurs NIS externes. Si la requête ne renvoie aucun résultat, le fichier netgroup local est coché ensuite.

Il n'y a pas d'entrées de nom de service pour le mappage de noms dans le tableau pour le SVM svm_1. Par conséquent, ONTAP consulte uniquement les fichiers source locaux par défaut.

Gérer les serveurs SMB

Modifier les serveurs SMB ONTAP

Vous pouvez déplacer un serveur SMB d'un groupe de travail vers un domaine Active Directory, d'un groupe de travail vers un autre groupe de travail, ou d'un domaine Active Directory vers un groupe de travail à l'aide de l' `vserver cifs modify` commande.

Description de la tâche

Vous pouvez également modifier d'autres attributs du serveur SMB, tels que le nom du serveur SMB et l'état administratif. Pour en savoir plus, `vserver cifs modify` consultez le "Référence de commande ONTAP".

Choix

- Déplacer le serveur SMB d'un groupe de travail vers un domaine Active Directory :

  a. Définissez l'état administratif du serveur SMB sur `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

b. Déplacer le serveur SMB du groupe de travail vers un domaine Active Directory : `vsserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

Pour créer un compte de machine Active Directory pour le serveur SMB, vous devez fournir le nom et le mot de passe d'un compte Windows disposant des privilèges suffisants pour ajouter des ordinateurs à l' `ou=example ou` conteneur dans le `example`domaine .com.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

- Déplacer le serveur SMB d'un groupe de travail vers un autre groupe de travail :
  a. Définissez l'état administratif du serveur SMB sur `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Modifiez le groupe de travail pour le serveur SMB : `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Déplacer le serveur SMB d'un domaine Active Directory vers un groupe de travail :
  a. Définissez l'état administratif du serveur SMB sur `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Déplacer le serveur SMB du domaine Active Directory vers un groupe de travail : `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

Pour passer en mode groupe de travail, toutes les fonctions basées sur un domaine doivent être désactivées et leur configuration doit être supprimée automatiquement par le système, y compris les partages disponibles en continu, les clichés instantanés et AES. Cependant, les listes de contrôle d'accès de partage configurées par domaine telles que « EXAMPLE.COM\userName" ne fonctionneront pas correctement, mais ne peuvent pas être supprimées par ONTAP. Supprimez ces ACL de partage dès que possible à l'aide d'outils externes une fois la commande terminée. Si AES est activé, vous pouvez être invité à fournir le nom et le mot de passe d'un compte Windows disposant de privilèges suffisants pour le désactiver dans le domaine "example.com".

- Modifiez d'autres attributs en utilisant le paramètre approprié de l' `vserver cifs modify` commande.

Utilisez les options pour personnaliser les serveurs SMB

Options de serveur SMB ONTAP disponibles

Il est utile de connaître les options disponibles lorsque vous envisagez de personnaliser le serveur SMB. Bien que certaines options soient destinées à une utilisation générale sur le serveur SMB, plusieurs sont utilisées pour activer et configurer des fonctionnalités SMB spécifiques. Les options de serveur SMB sont contrôlées avec le `vserver cifs options modify` option.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège admin :

- **Configuration de la valeur du délai d'expiration de session SMB**

  La configuration de cette option vous permet de spécifier le nombre de secondes d'inactivité avant la déconnexion d'une session SMB. Une session inactive est une session dans laquelle un utilisateur ne dispose pas de fichiers ou de répertoires ouverts sur le client. La valeur par défaut est 900 secondes.

- **Configuration de l'utilisateur UNIX par défaut**

  La configuration de cette option vous permet de spécifier l'utilisateur UNIX par défaut utilisé par le serveur SMB. ONTAP crée automatiquement un utilisateur par défaut nommé « pcuser » (avec un UID de 65534), crée un groupe nommé « pcuser » (avec un GID de 65534) et ajoute l'utilisateur par défaut au groupe « pcuser ». Lorsque vous créez un serveur SMB, ONTAP configure automatiquement « pcuser » en tant qu'utilisateur UNIX par défaut.

- **Configuration de l'utilisateur UNIX invité**

  La configuration de cette option vous permet de spécifier le nom d'un utilisateur UNIX auquel les utilisateurs qui se connectent à partir de domaines non fiables sont mappés, ce qui permet à un utilisateur d'un domaine non fiable de se connecter au serveur SMB. Par défaut, cette option n'est pas configurée (il n'y a pas de valeur par défaut) ; par conséquent, la valeur par défaut ne permet pas aux utilisateurs de domaines non approuvés de se connecter au serveur SMB.

- **Activation ou désactivation de l'exécution d'une subvention en lecture pour les bits de mode**

  L'activation ou la désactivation de cette option vous permet de spécifier si les clients SMB doivent autoriser l'exécution de fichiers exécutables avec les bits de mode UNIX auxquels ils ont accès en lecture, même lorsque le bit exécutable UNIX n'est pas défini. Cette option est désactivée par défaut.

- **Activation ou désactivation de la possibilité de supprimer des fichiers en lecture seule des clients NFS**

  L'activation ou la désactivation de cette option détermine s'il faut autoriser les clients NFS à supprimer des fichiers ou des dossiers avec l'ensemble d'attributs en lecture seule. La sémantique de suppression NTFS n'autorise pas la suppression d'un fichier ou d'un dossier lorsque l'attribut en lecture seule est défini. La sémantique de suppression UNIX ignore le bit en lecture seule, en utilisant les autorisations du répertoire parent à la place pour déterminer si un fichier ou un dossier peut être supprimé. Le paramètre par défaut est `disabled`, Ce qui entraîne la suppression de la sémantique en NTFS.

- **Configuration des adresses du serveur du service de noms Internet Windows**

  La configuration de cette option vous permet de spécifier une liste d'adresses de serveur WINS (Windows Internet Name Service) en tant que liste délimitée par des virgules. Vous devez indiquer des adresses IPv4. Les adresses IPv6 ne sont pas prises en charge. Il n'y a pas de valeur par défaut.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège avancé :

- **Octroi d'autorisations de groupe UNIX aux utilisateurs CIFS**

  La configuration de cette option détermine si l'utilisateur CIFS entrant qui n'est pas le propriétaire du fichier peut obtenir l'autorisation de groupe. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `true`, puis l'autorisation de groupe est accordée pour le fichier. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `false`, Les règles UNIX normales sont alors applicables pour accorder l'autorisation de fichier. Ce paramètre s'applique aux fichiers de style de sécurité UNIX dont l'autorisation est définie sur `mode bits` Et ne s'applique pas aux fichiers utilisant le mode de sécurité NTFS ou NFSv4. Le paramètre par défaut est `false`.

- **Activation ou désactivation de SMB 1.0**

  SMB 1.0 est désactivé par défaut sur un SVM pour lequel un serveur SMB est créé dans ONTAP 9.3.

  > À partir de ONTAP 9.3, SMB 1.0 est désactivé par défaut pour les nouveaux serveurs SMB créés dans ONTAP 9.3. Vous devez migrer vers une version SMB plus récente dès que possible pour préparer des améliorations en matière de sécurité et de conformité. Contactez votre représentant NetApp pour plus d'informations.

- **Activation ou désactivation de SMB 2.x**

  SMB 2.0 est la version minimale de SMB qui prend en charge le basculement de LIF. Si vous désactivez SMB 2.x, ONTAP désactive également automatiquement SMB 3.X.

  SMB 2.0 est pris en charge uniquement sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.0**

  SMB 3.0 est la version minimale de SMB qui prend en charge les partages disponibles en continu. Windows Server 2012 et Windows 8 sont les versions minimales de Windows qui prennent en charge SMB 3.0.

  SMB 3.0 n'est pris en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.1**

  Windows 10 est la seule version de Windows qui prend en charge SMB 3.1.

  SMB 3.1 n'est pris en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de l'allègement de charge des copies ODX**

  L'allègement de la charge des copies ODX est utilisé automatiquement par les clients Windows qui la prennent en charge. Cette option est activée par défaut.

- **Activation ou désactivation du mécanisme de copie directe pour le déchargement de copies ODX**

  Le mécanisme de copie directe augmente les performances de l'opération de déchargement de copie lorsque les clients Windows essaient d'ouvrir le fichier source d'une copie dans un mode qui empêche la modification du fichier pendant la copie. Par défaut, le mécanisme de copie directe est activé.

- **Activation ou désactivation des renvois de nœuds automatiques**

  Avec les référencements automatiques des nœuds, le serveur SMB fait automatiquement référence aux clients à une LIF de données locale au nœud qui héberge les données accédées via le partage demandé.

- **Activation ou désactivation des stratégies d'exportation pour SMB**

  Cette option est désactivée par défaut.

- **Activation ou désactivation de l'utilisation de points de jonction en tant que points de réanalyse**

  Si cette option est activée, le serveur SMB expose les points de jonction aux clients SMB comme points de réanalyse. Cette option n'est valide que pour les connexions SMB 2.x ou SMB 3.0. Cette option est activée par défaut.

  Cette option n'est prise en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Configuration du nombre maximal d'opérations simultanées par connexion TCP**

  La valeur par défaut est 255.

- **Activation ou désactivation de la fonctionnalité des groupes et des utilisateurs Windows locaux**

  Cette option est activée par défaut.

- **Activation ou désactivation de l'authentification des utilisateurs Windows locaux**

  Cette option est activée par défaut.

- **Activation ou désactivation de la fonctionnalité de copie en double VSS**

  ONTAP utilise la fonctionnalité Shadow Copy pour effectuer des sauvegardes distantes des données stockées à l'aide de la solution Hyper-V sur SMB.

  Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Configuration de la profondeur du répertoire de copie en double**

  La configuration de cette option vous permet de définir la profondeur maximale des répertoires sur lesquels créer des clichés instantanés lors de l'utilisation de la fonctionnalité copie en double.

  Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Activation ou désactivation des fonctionnalités de recherche multidomaine pour le mappage de noms**

  Si cette option est activée, lorsqu'un utilisateur UNIX est mappé à un utilisateur de domaine Windows à l'aide d'un caractère générique (*) dans la partie domaine du nom d'utilisateur Windows (par exemple

*\joe), ONTAP recherche l'utilisateur spécifié dans tous les domaines avec des approbations bidirectionnelles vers le domaine d'origine. Le domaine personnel est le domaine qui contient le compte informatique du serveur SMB.

Vous pouvez également configurer une liste de domaines de confiance préférés en alternative à la recherche de tous les domaines de confiance bidirectionnels. Si cette option est activée et qu'une liste préférée est configurée, la liste préférée est utilisée pour effectuer des recherches de mappage de noms de domaines multiples.

La valeur par défaut est d'activer les recherches de mappage de noms multidomaine.

- **Configuration de la taille du secteur du système de fichiers**

  La configuration de cette option vous permet de configurer la taille du secteur du système de fichiers en octets que ONTAP communique aux clients SMB. Cette option comporte deux valeurs valides : `4096` et `512`. La valeur par défaut est `4096`. Vous devrez peut-être définir cette valeur sur `512` Si l'application Windows ne prend en charge qu'une taille de secteur de 512 octets.

- **Activation ou désactivation du contrôle d'accès dynamique**

  L'activation de cette option vous permet de sécuriser les objets sur le serveur SMB à l'aide du contrôle d'accès dynamique (DAC), y compris l'utilisation de l'audit pour définir des règles d'accès centrales et l'utilisation d'objets de stratégie de groupe pour mettre en œuvre des règles d'accès centrales. L'option est désactivée par défaut.

  Cette option n'est prise en charge que sur les SVM.

- **Définition des restrictions d'accès pour les sessions non authentifiées (restriction anonyme)**

  La définition de cette option détermine les restrictions d'accès pour les sessions non authentifiées. Les restrictions sont appliquées aux utilisateurs anonymes. Par défaut, il n'existe aucune restriction d'accès pour les utilisateurs anonymes.

- **Activation ou désactivation de la présentation des listes de contrôle d'accès NTFS sur des volumes avec sécurité effective UNIX (volumes de type sécurité UNIX ou volumes de type sécurité mixte avec sécurité effective UNIX)**

  L'activation ou la désactivation de cette option détermine comment la sécurité des fichiers sur les fichiers et les dossiers avec la sécurité UNIX est présentée aux clients SMB. Lorsqu'elle est activée, ONTAP présente aux clients SMB les fichiers et les dossiers des volumes dotés de la sécurité UNIX comme ayant la sécurité des fichiers NTFS avec les ACL NTFS. S'il est désactivé, ONTAP présente les volumes dont la sécurité UNIX est de type FAT, sans aucun fichier sécurisé. Par défaut, les volumes sont présentés comme ayant la sécurité de fichiers NTFS avec les ACL NTFS.

- **Activation ou désactivation de la fonctionnalité fausse ouverture SMB**

  L'activation de cette fonctionnalité améliore les performances de SMB 2.x et de SMB 3.0 en optimisant la manière dont ONTAP effectue des requêtes ouvertes et fermés lors des requêtes relatives aux attributs des fichiers et des répertoires. Par défaut, la fonctionnalité de faux ouverture SMB est activée. Cette option est utile uniquement pour les connexions effectuées avec SMB 2.x ou version ultérieure.

- **Activation ou désactivation des extensions UNIX**

  L'activation de cette option active les extensions UNIX sur un serveur SMB. Les extensions UNIX permettent d'afficher la sécurité du style POSIX/UNIX via le protocole SMB. Par défaut, cette option est désactivée.

Si vous avez des clients SMB basés sur UNIX, tels que des clients Mac OSX, dans votre environnement, vous devez activer les extensions UNIX. L'activation des extensions UNIX permet au serveur SMB de transmettre des informations de sécurité POSIX/UNIX sur SMB au client UNIX, qui convertit ensuite les informations de sécurité en sécurité POSIX/UNIX.

- **Activation ou désactivation du support pour les recherches de noms courts**

  L'activation de cette option permet au serveur SMB d'effectuer des recherches sur des noms courts. Une requête de recherche avec cette option activée tente de faire correspondre 8.3 noms de fichier avec des noms de fichier longs. La valeur par défaut de ce paramètre est `false`.

- **Activation ou désactivation de la prise en charge de la publicité automatique des capacités DFS**

  L'activation ou la désactivation de cette option détermine si les serveurs SMB annoncent automatiquement les fonctionnalités DFS aux clients SMB 2.x et SMB 3.0 qui se connectent aux partages. ONTAP utilise des référencements DFS dans la mise en œuvre de liens symboliques pour l'accès SMB. Si cette option est activée, le serveur SMB annonce toujours les fonctionnalités DFS, que l'accès à la liaison symbolique soit activé ou non. S'il est désactivé, le serveur SMB annonce les fonctionnalités DFS uniquement lorsque les clients se connectent aux partages où l'accès à la liaison symbolique est activé.

- **Configuration du nombre maximum de crédits SMB**

  Depuis ONTAP 9.4, configurer le `-max-credits` Vous permet de limiter le nombre de crédits à accorder sur une connexion SMB lorsque les clients et le serveur exécutent SMB version 2 ou ultérieure. La valeur par défaut est 128.

- **Activation ou désactivation de la prise en charge de SMB Multichannel**

  Activation du `-is-multichannel-enabled` Option dans les versions ONTAP 9.4 et ultérieures permet au serveur SMB d'établir plusieurs connexions pour une seule session SMB lorsque les cartes réseau appropriées sont déployées sur le cluster et ses clients. Cela améliore le débit et la tolérance aux pannes. La valeur par défaut de ce paramètre est `false`.

  Lorsque SMB Multichannel est activé, vous pouvez également spécifier les paramètres suivants :

  - Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut de ce paramètre est 32.
  - Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut de ce paramètre est 256.

Configurez les options du serveur SMB ONTAP

Vous pouvez configurer les options du serveur SMB à tout moment après avoir créé un serveur SMB sur une machine virtuelle de stockage (SVM).

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez configurer les options du serveur SMB…	Entrez la commande…
Au niveau de privilège admin	`vserver cifs options modify -vserver` *`vserver_name options`*
Au niveau de privilège avancé	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Pour en savoir plus sur les `vserver cifs options modify` options de serveur SMB et leur configuration, consultez le "Référence de commande ONTAP".

Configurez l'autorisation accorder un groupe UNIX aux utilisateurs SMB ONTAP

Vous pouvez configurer cette option pour accorder des autorisations de groupe à des fichiers ou des répertoires, même si l'utilisateur SMB entrant n'est pas le propriétaire du fichier.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez l'autorisation Grant UNIX Group comme il convient :

Si vous le souhaitez	Saisissez la commande
Activez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	`vserver cifs options modify -grant-unix-group-perms-to-others true`
Désactivez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Retour au niveau de privilège admin : `set -privilege admin`

Configurez les restrictions d'accès SMB ONTAP pour les utilisateurs anonymes

Par défaut, un utilisateur anonyme et non authentifié (également appelé *null user*) peut accéder à certaines informations sur le réseau. Vous pouvez utiliser une option de serveur SMB pour configurer les restrictions d'accès pour l'utilisateur anonyme.

Description de la tâche

Le `-restrict-anonymous` L'option de serveur SMB correspond au `RestrictAnonymous` Entrée de registre dans Windows.

Les utilisateurs anonymes peuvent lister ou énumérer certains types d'informations système provenant des hôtes Windows sur le réseau, y compris les noms d'utilisateur et les détails, les stratégies de compte et les noms de partage. Vous pouvez contrôler l'accès de l'utilisateur anonyme en spécifiant l'un des trois paramètres de restriction d'accès suivants :

Valeur	Description
`no-restriction` (valeur par défaut)	Spécifie aucune restriction d'accès pour les utilisateurs anonymes.
`no-enumeration`	Spécifie que seule l'énumération est restreinte pour les utilisateurs anonymes.
`no-access`	Spécifie que l'accès est restreint pour les utilisateurs anonymes.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre restreindre l'anonymat : `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver` *`vserver_name`*
4. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

Options de serveur disponibles

Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour les données de type sécurité UNIX

Découvrez la présentation de la sécurité des fichiers ONTAP aux clients SMB pour les données de type sécurité UNIX

Vous pouvez choisir comment présenter la sécurité des fichiers aux clients SMB pour les données de style de sécurité UNIX en activant ou désactivant la présentation d'ACL NTFS aux clients SMB. Chaque paramètre présente des avantages, que vous devez comprendre pour choisir le paramètre le mieux adapté aux besoins de votre entreprise.

Par défaut, ONTAP présente des autorisations UNIX sur des volumes de type sécurité UNIX aux clients SMB comme des listes de contrôle d'accès NTFS. Dans certains cas, cette option est souhaitable, notamment :

- Vous souhaitez afficher et modifier les autorisations UNIX à l'aide de l'onglet **sécurité** de la zone Propriétés de Windows.

  Vous ne pouvez pas modifier les autorisations d'un client Windows si l'opération n'est pas autorisée par le système UNIX. Par exemple, vous ne pouvez pas modifier la propriété d'un fichier que vous ne possédez pas, car le système UNIX ne permet pas cette opération. Cette restriction empêche les clients SMB de contourner les autorisations UNIX définies sur les fichiers et dossiers.

- Les utilisateurs modifient et enregistrent des fichiers sur le volume de style de sécurité UNIX en utilisant certaines applications Windows, par exemple Microsoft Office, où ONTAP doit préserver les autorisations

UNIX pendant les opérations de sauvegarde.

- Votre environnement compte certaines applications Windows qui doivent lire les listes de contrôle d'accès NTFS sur les fichiers qu'elles utilisent.

Dans certaines circonstances, vous pouvez désactiver la présentation des autorisations UNIX en tant que listes de contrôle d'accès NTFS. Si cette fonctionnalité est désactivée, ONTAP présente les volumes de style de sécurité UNIX en tant que volumes FAT aux clients SMB. Il existe des raisons spécifiques de vouloir présenter des volumes de style sécurité UNIX en tant que volumes FAT aux clients SMB :

- Vous ne modifiez que les autorisations UNIX en utilisant des montages sur des clients UNIX.

  L'onglet sécurité n'est pas disponible lorsqu'un volume de style de sécurité UNIX est mappé sur un client SMB. Le lecteur mappé semble être formaté avec le système de fichiers FAT, qui ne dispose pas d'autorisations de fichier.

- Vous utilisez des applications sur SMB qui définissent les listes de contrôle d'accès NTFS sur les fichiers et dossiers auxquels vous accédez, ce qui peut échouer si les données résident sur des volumes de style de sécurité UNIX.

  Si ONTAP signale le volume comme FAT, l'application n'essaie pas de modifier une ACL.

Informations associées

- Configurer des styles de sécurité sur les volumes FlexVol
- Configurer des styles de sécurité sur les qtrees

Configurez la présentation des ACL NTFS aux clients SMB ONTAP pour les données de type sécurité UNIX

Vous pouvez activer ou désactiver la présentation des listes de contrôle d'accès NTFS aux clients SMB pour les données de style de sécurité UNIX (volumes de style sécurité UNIX et volumes de type sécurité mixte avec sécurité effective UNIX).

Description de la tâche

Si vous activez cette option, ONTAP présente les fichiers et les dossiers sur les volumes avec un style de sécurité UNIX efficace aux clients SMB comme ayant des listes de contrôle d'accès NTFS. Si vous désactivez cette option, les volumes sont présentés en tant que volumes FAT aux clients SMB. Par défaut, cette valeur doit présenter des listes de contrôle d'accès NTFS aux clients SMB.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre d'option ACL NTFS UNIX : `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver` *`vserver_name`*
4. Retour au niveau de privilège admin : `set -privilege admin`

Découvrez comment conserver les autorisations UNIX pour les volumes ONTAP SMB FlexVol

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les

autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

Découvrez comment gérer les autorisations UNIX à l'aide de l'onglet sécurité Windows pour les serveurs SMB ONTAP

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtrees de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- Modification des autorisations UNIX

  Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

  Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- Modification des autorisations UNIX en autorisations NTFS

  Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

  Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

  Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

Gérer les paramètres de sécurité du serveur SMB

En savoir plus sur la gestion de l'authentification de clients SMB ONTAP

Avant que les utilisateurs puissent créer des connexions SMB pour accéder aux données contenues dans la SVM, ils doivent être authentifiés par le domaine auquel le serveur SMB appartient. Le serveur SMB prend en charge deux méthodes d'authentification, Kerberos et NTLM (NTLMv1 ou NTLMv2). Kerberos est la méthode par défaut utilisée pour authentifier les utilisateurs du domaine.

Authentification Kerberos

ONTAP supporte l'authentification Kerberos lors de la création de sessions SMB authentifiées.

Kerberos est le service principal d'authentification pour Active Directory. Le serveur Kerberos, ou le Kerberos Key distribution Center (KDC) service, stocke et récupère des informations sur les principes de sécurité dans Active Directory. A la différence du modèle NTLM, les clients Active Directory qui souhaitent établir une session avec un autre ordinateur, tel que le serveur SMB, contactez directement un KDC pour obtenir leurs credentials de session.

Authentification NTLM

L'authentification du client NTLM est effectuée à l'aide d'un protocole de réponse de défi basé sur une connaissance partagée d'un secret spécifique à un utilisateur basé sur un mot de passe.

Si un utilisateur crée une connexion SMB à l'aide d'un compte utilisateur Windows local, l'authentification est effectuée localement par le serveur SMB à l'aide de NTLMv2.

En savoir plus sur les paramètres de sécurité du serveur SMB pour la configuration de la reprise d'activité du SVM ONTAP

Avant de créer un SVM configuré en tant que destination de reprise d'activité pour laquelle l'identité n'est pas conservée (le `-identity-preserve` l'option est définie sur `false` En configuration SnapMirror), il est important de savoir comment les paramètres de sécurité des serveurs SMB sont gérés sur la SVM de destination.

- Les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination.

  Lorsque vous créez un serveur SMB sur le SVM de destination, tous les paramètres de sécurité du serveur SMB sont définis sur les valeurs par défaut. Lors de l'initialisation, de la destination de reprise après incident du SVM, de la mise à jour ou de la resynchronisation, les paramètres de sécurité du serveur SMB sur la source ne sont pas répliqués sur la destination.

- Vous devez configurer manuellement les paramètres de sécurité du serveur SMB non par défaut.

  Si vous avez configuré sur la SVM source des paramètres de sécurité du serveur SMB non par défaut, vous devez configurer manuellement ces mêmes paramètres sur le SVM de destination après que la destination devienne read-write (après une interruption de la relation SnapMirror).

Affiche des informations sur les paramètres de sécurité du serveur SMB ONTAP

Vous pouvez afficher des informations sur les paramètres de sécurité du serveur SMB sur vos serveurs virtuels de stockage (SVM). Vous pouvez utiliser ces informations pour vérifier que les paramètres de sécurité sont corrects.

Description de la tâche

Un paramètre de sécurité affiché peut être la valeur par défaut pour cet objet ou une valeur non par défaut configurée à l'aide de l'interface de ligne de commande ONTAP ou à l'aide d'objets de stratégie de groupe Active Directory.

N'utilisez pas le `vserver cifs security show` Commande pour les serveurs SMB en mode groupe de travail, car certaines options ne sont pas valides.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur…	Entrez la commande…
Tous les paramètres de sécurité sur un SVM spécifié	`vserver cifs security show -vserver` *`vserver_name`*
Un paramètre de sécurité ou des paramètres spécifiques sur la SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

Exemple

L'exemple suivant montre tous les paramètres de sécurité pour SVM vs1 :

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
         Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
                SMB1 Enabled for DC Connections:        false
                SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
              Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Notez que les paramètres affichés dépendent de la version ONTAP en cours d'exécution.

L'exemple suivant montre l'inclinaison de l'horloge Kerberos pour le SVM vs1 :

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Informations associées

Affiche des informations sur les configurations GPO

Configurez la complexité des mots de passe ONTAP pour les utilisateurs SMB locaux

Au-dessus de vos SVM, la complexité requise par mot de passe renforce la sécurité des utilisateurs SMB locaux. La fonction de complexité de mot de passe requise est activée par défaut. Vous pouvez le désactiver et le réactiver à tout moment.

Avant de commencer

Les utilisateurs locaux, les groupes locaux et l'authentification des utilisateurs locaux doivent être activés sur le serveur CIFS.

Description de la tâche

N'utilisez pas `vserver cifs security modify` la commande pour un serveur CIFS en mode Workgroup car certaines options ne sont pas valides.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez que les utilisateurs de PME locales aient besoin de complexité de mot de passe…	Entrez la commande…
Activé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Désactivé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Vérifiez le paramètre de sécurité pour connaître la complexité requise du mot de passe : `vserver cifs security show -vserver` *`vserver_name`*

Exemple

L'exemple suivant montre que la complexité requise des mots de passe est activée pour les utilisateurs SMB

locaux pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- ------------------------------
vs1     true
```

Informations associées

- Afficher des informations sur les paramètres de sécurité du serveur
- En savoir plus sur les utilisateurs et les groupes locaux
- Conditions requises pour les mots de passe des utilisateurs locaux
- Modifier les mots de passe des comptes utilisateur locaux

Modifiez les paramètres de sécurité Kerberos du serveur SMB ONTAP

Vous pouvez modifier certains paramètres de sécurité Kerberos pour le serveur CIFS, notamment le temps d'inclinaison maximal autorisé de l'horloge Kerberos, la durée de vie du ticket Kerberos et le nombre maximum de jours de renouvellement de ticket.

Description de la tâche

Modification des paramètres Kerberos du serveur CIFS à l'aide de `vserver cifs security modify` La commande modifie les paramètres uniquement sur la machine virtuelle de stockage (SVM) que vous spécifiez avec le `-vserver` paramètre. Vous pouvez gérer de manière centralisée les paramètres de sécurité Kerberos pour tous les SVM du cluster appartenant au même domaine Active Directory à l'aide des objets de stratégie de groupe Active Directory.

Étapes

1. Effectuez une ou plusieurs des opérations suivantes :

Les fonctions que vous recherchez…	Entrer…
Spécifiez le temps maximal autorisé d'inclinaison de l'horloge Kerberos en minutes (9.13.1 et versions ultérieures) ou en secondes (9.12.1 ou versions antérieures).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* La valeur par défaut est 5 minutes.
Spécifiez la durée de vie du ticket Kerberos en heures.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` Le paramètre par défaut est 10 heures.

Spécifiez le nombre maximum de jours de renouvellement de billet.	`vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days` Le paramètre par défaut est 7 jours.
Spécifiez le délai d'expiration des sockets sur les KDC après lequel tous les KDC sont marqués comme inaccessibles.	`vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds` Le réglage par défaut est de 3 secondes.

2. Vérifiez les paramètres de sécurité Kerberos :

   `vserver cifs security show -vserver vserver_name`

Exemple

L'exemple suivant apporte les modifications suivantes à la sécurité Kerberos : « Kerberos Clock Skew » est défini sur 3 minutes et « Kerberos Ticket Age » est défini sur 8 heures pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
        Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                false
              Is AES Encryption Enabled:                false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                false
```

Informations associées

"Afficher des informations sur les paramètres de sécurité du serveur"

"Stratégies de groupe prises en charge"

"Application d'objets de stratégie de groupe aux serveurs CIFS"

Définissez le niveau de sécurité d'authentification minimum du serveur SMB ONTAP

Vous pouvez définir le niveau de sécurité minimum du serveur SMB, également appelé *LMCompatibilityLevel*, sur votre serveur SMB afin de répondre aux besoins de sécurité de votre entreprise pour l'accès client SMB. Le niveau de sécurité minimum est le niveau minimum des jetons de sécurité que le serveur SMB accepte des clients SMB.

Description de la tâche

- Les serveurs SMB en mode groupe de travail prennent uniquement en charge l'authentification NTLM. L'authentification Kerberos n'est pas prise en charge.
- LMCompatibilityLevel s'applique uniquement à l'authentification du client SMB, et non à l'authentification de l'administrateur.

Vous pouvez définir le niveau de sécurité d'authentification minimum sur l'un des quatre niveaux de sécurité pris en charge.

Valeur	Description
`lm-ntlm-ntlmv2-krb` (valeur par défaut)	La machine virtuelle de stockage (SVM) accepte les authentifications LM, NTLM, NTLMv2 et Kerberos.
`ntlm-ntlmv2-krb`	Le SVM accepte la sécurité d'authentification NTLM, NTLMv2, et Kerberos. Le SVM refuse l'authentification LM.
`ntlmv2-krb`	Le SVM accepte la sécurité d'authentification NTLMv2 et Kerberos. Le SVM refuse l'authentification LM et NTLM.
`krb`	Le SVM n'accepte que la sécurité d'authentification Kerberos. Le SVM refuse l'authentification LM, NTLM et NTLMv2.

Étapes

1. Définissez le niveau de sécurité d'authentification minimum : `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Vérifiez que le niveau de sécurité d'authentification est défini sur le niveau souhaité : `vserver cifs security show -vserver vserver_name`

Informations associées

Configurer le chiffrement AES pour la communication basée sur Kerberos

Configurez la sécurité SMB ONTAP renforcée pour les communications Kerberos à l'aide du chiffrement AES

Pour une sécurité renforcée avec les communications basées sur Kerberos, vous pouvez activer le chiffrement AES-256 et AES-128 sur le serveur SMB. Par défaut, lorsque vous créez un serveur SMB sur le SVM, le chiffrement Advanced Encryption Standard (AES)

est désactivé. Elle doit permettre aux services IT de bénéficier de la sécurité renforcée fournie par le cryptage AES.

La communication Kerberos pour SMB est utilisée lors de la création du serveur SMB sur le SVM, ainsi que lors de la phase d'installation de la session SMB. Le serveur SMB prend en charge les types de chiffrement suivants pour les communications Kerberos :

- AES 256
- AES 128
- DES
- RC4-HMAC

Si vous souhaitez utiliser le type de chiffrement le plus élevé pour les communications Kerberos, vous devez activer le chiffrement AES pour la communication Kerberos sur la SVM.

Lorsque le serveur SMB est créé, le contrôleur de domaine crée un compte de machine informatique dans Active Directory. À l'heure actuelle, le KDC prend connaissance des capacités de cryptage du compte machine particulier. Par la suite, un type de chiffrement particulier est sélectionné pour le chiffrement du ticket de service que le client présente au serveur lors de l'authentification.

À partir de ONTAP 9.12.1, vous pouvez spécifier les types de cryptage à publier sur le KDC Active Directory (AD). Vous pouvez `-advertised-enc-types` utiliser l'option pour activer les types de cryptage recommandés et vous pouvez l'utiliser pour désactiver les types de cryptage les plus faibles. Découvrez comment "Configurer le chiffrement AES pour la communication basée sur Kerberos".

> Intel AES New instructions (Intel AES ni) est disponible dans SMB 3.0. Il améliore l'algorithme AES et accélère le chiffrement des données avec les familles de processeurs prises en charge.à partir de SMB 3.1.1, AES-128-GCM remplace AES-128-CCM en tant qu'algorithme de hachage utilisé par le chiffrement SMB.

Informations associées

Modifier les paramètres de sécurité du serveur

Configurez le chiffrement AES pour les communications ONTAP SMB basées sur Kerberos

Pour bénéficier de la sécurité la plus forte des communications basées sur Kerberos, vous devez utiliser le chiffrement AES-256 et AES-128 sur le serveur SMB. À partir de ONTAP 9.13.1, le chiffrement AES est activé par défaut. Si vous ne souhaitez pas que le serveur SMB sélectionne les types de cryptage AES pour les communications basées sur Kerberos avec le KDC Active Directory (AD), vous pouvez désactiver le cryptage AES.

Le fait que le cryptage AES soit activé par défaut et que vous puissiez spécifier des types de cryptage dépend de votre version de ONTAP.

Version ONTAP	Le cryptage AES est activé …	Vous pouvez spécifier des types de cryptage ?
9.13.1 et versions ultérieures	Par défaut	Oui.
9.12.1	Manuellement	Oui.
9.11.1 et versions antérieures	Manuellement	Non

Depuis ONTAP 9.12.1, le chiffrement AES est activé et désactivé à l'aide du `-advertised-enc-types` Cette option permet de spécifier les types de cryptage annoncés dans AD KDC. Le paramètre par défaut est `rc4` et `des`, Mais lorsqu'un type AES est spécifié, le cryptage AES est activé. Vous pouvez également utiliser l'option pour désactiver explicitement les types de cryptage RC4 et DES les plus faibles. Dans ONTAP 9.11.1 et les versions antérieures, vous devez utiliser le `-is-aes-encryption-enabled` Option permettant d'activer et de désactiver le cryptage AES, et les types de cryptage ne peuvent pas être spécifiés.

Pour renforcer la sécurité, la machine virtuelle de stockage (SVM) modifie le mot de passe de son compte machine dans l'AD à chaque modification de l'option de sécurité AES. La modification du mot de passe peut nécessiter des informations d'identification AD administratives pour l'unité organisationnelle qui contient le compte de la machine.

Si un SVM est configuré en tant que destination de reprise sur incident où l'identité n'est pas conservée (le `-identity-preserve` l'option est définie sur `false` Dans la configuration SnapMirror), les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination. Si vous avez activé le chiffrement AES sur la SVM source, vous devez l'activer manuellement.

Exemple 1. Étapes

ONTAP 9.12.1 et versions ultérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos…	Entrez la commande…
Activé	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Désactivé	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Remarque : le `-is-aes-encryption-enabled` Cette option est obsolète dans ONTAP 9.12.1 et peut être supprimée dans une version ultérieure.

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins : `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2. L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 et versions antérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos…	Entrez la commande…
Activé	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Désactivé	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins : `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Le `is-aes-encryption-enabled` s'affiche `true` Si le cryptage AES est activé et `false` s'il est désactivé.

Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2. L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Informations associées

"L'utilisateur du domaine ne parvient pas à se connecter au cluster avec Domain-tunnel"

Utilisez la signature SMB pour améliorer la sécurité du réseau

Découvrez comment utiliser la signature SMB ONTAP pour améliorer la sécurité du réseau

La signature SMB contribue à garantir que le trafic réseau entre le serveur SMB et le client n'est pas compromis. Elle empêche les attaques de relecture. Par défaut, ONTAP prend en charge la signature SMB sur demande du client. L'administrateur du stockage peut éventuellement configurer le serveur SMB afin de nécessiter une signature SMB.

Découvrez comment les règles de signature affectent la communication avec les serveurs SMB ONTAP

Outre les paramètres de sécurité de signature SMB du serveur CIFS, deux stratégies de signature SMB sur les clients Windows contrôlent la signature numérique des communications entre les clients et le serveur CIFS. Vous pouvez configurer le paramètre qui répond aux besoins de votre entreprise.

Les stratégies SMB du client sont contrôlées via les paramètres de stratégie de sécurité locale de Windows, qui sont configurés à l'aide des stratégies de groupe MMC (Microsoft Management Console) ou Active Directory. Pour plus d'informations sur les problèmes de sécurité et de signature SMB du client, consultez la documentation Microsoft Windows.

Voici les descriptions des deux stratégies de signature SMB sur les clients Microsoft :

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Ce paramètre détermine si la fonctionnalité de signature SMB du client est activée. Elle est activée par défaut. Lorsque ce paramètre est désactivé sur le client, les communications client avec le serveur CIFS dépendent du paramètre de signature SMB sur le serveur CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Ce paramètre détermine si le client requiert la signature SMB pour communiquer avec un serveur. Elle est désactivée par défaut. Lorsque ce paramètre est désactivé sur le client, le comportement de signature SMB est basé sur le paramètre de stratégie pour `Microsoft network client: Digitally sign communications (if server agrees)` Et le paramètre sur le serveur CIFS.

> Si votre environnement inclut des clients Windows configurés pour exiger une signature SMB, vous devez activer la signature SMB sur le serveur CIFS. Dans le cas contraire, le serveur CIFS ne peut pas transmettre de données à ces systèmes.

Les résultats effectifs des paramètres de signature SMB du client et du serveur CIFS dépendent du fait que les sessions SMB utilisent SMB 1.0 ou SMB 2.x et versions ultérieures.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 1.0 :

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature désactivée et non requise	Non signé	Signé
Signature activée et non requise	Non signé	Signé
Signature désactivée et requise	Signé	Signé
Signature activée et requise	Signé	Signé

> Les anciens clients Windows SMB 1 et certains clients non Windows SMB 1 peuvent ne pas se connecter si la signature est désactivée sur le client mais requise sur le serveur CIFS.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 2.x ou SMB 3.0 :

Pour les clients SMB 2.x et SMB 3.0, la signature SMB est toujours activée. Elle ne peut pas être désactivée.

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature non requise	Non signé	Signé
Signature requise	Signé	Signé

Le tableau suivant récapitule le comportement de signature SMB du serveur et du client Microsoft par défaut :

Protocole	Algorithme de hachage	Peut activer/désactiver	Peut exiger/non requis	Client par défaut	Serveur par défaut	DC par défaut
SMB 1.0	MD5	Oui.	Oui.	Activé (non requis)	Désactivé (non requis)	Obligatoire
SMB 2.x	HMAC SHA-256	Non	Oui.	Non requis	Non requis	Obligatoire
SMB 3.0	AES-CMAC.	Non	Oui.	Non requis	Non requis	Obligatoire

Microsoft ne recommande plus d'utiliser `Digitally sign communications (if client agrees)` ou `Digitally sign communications (if server agrees)` Paramètres de stratégie de groupe. Microsoft ne recommande plus par ailleurs l'utilisation du `EnableSecuritySignature` paramètres du registre. Ces options n'affectent que le comportement du SMB 1 et peuvent être remplacées par le `Digitally sign communications (always)` Stratégie de groupe ou `RequireSecuritySignature` paramètre de registre. Vous pouvez également obtenir plus d'informations sur le blog Microsoft.principes de base de la signature SMB The (SMB1 et SMB2)

En savoir plus sur l'impact de la signature SMB ONTAP sur les performances

Lorsque les sessions SMB utilisent la signature SMB, toutes les communications SMB vers et depuis les clients Windows subissent un impact sur les performances, ce qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM contenant le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis ONTAP 9.7, un nouvel algorithme de déchargement du cryptage peut permettre d'améliorer les performances du trafic SMB signé. L'allègement de la charge des signatures SMB est activé par défaut lorsque la signature SMB est activée.

L'amélioration des performances de signature SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact de la signature SMB sur les performances peut varier fortement. Vous pouvez la vérifier uniquement par le biais de tests dans l'environnement réseau.

La plupart des clients Windows négocient la signature SMB par défaut si elle est activée sur le serveur. Si vous avez besoin d'une protection SMB pour certains de vos clients Windows et si le SMB Signing génère des problèmes de performances, vous pouvez désactiver la signature SMB sur l'un de vos clients Windows ne nécessitant pas de protection contre les attaques de rejeu. Pour plus d'informations sur la désactivation de la signature SMB sur les clients Windows, consultez la documentation Microsoft Windows.

Recommandations sur la configuration de la signature SMB de ONTAP

Vous pouvez configurer le comportement de signature SMB entre les clients SMB et le serveur CIFS pour répondre à vos exigences de sécurité. Les paramètres que vous choisissez lors de la configuration de la signature SMB sur votre serveur CIFS dépendent de vos exigences de sécurité.

Vous pouvez configurer la signature SMB sur le client ou sur le serveur CIFS. Tenez compte des recommandations suivantes lors de la configuration de la signature SMB :

Si…	Recommandation…
Vous souhaitez augmenter la sécurité de la communication entre le client et le serveur	Assurez-vous que le SMB Signing est requis au niveau du client en activant le `Require Option (Sign always)` paramètre de sécurité sur le client.
Vous souhaitez que tous les trafics SMB vers une certaine machine virtuelle de stockage (SVM) signée	Configurez les paramètres de sécurité pour exiger la signature SMB sur le serveur CIFS.

Pour plus d'informations sur la configuration des paramètres de sécurité du client Windows, reportez-vous à la documentation Microsoft.

En savoir plus sur la configuration de signature SMB de ONTAP pour plusieurs LIF DE données

Si vous activez ou désactivez le SMB Signing requis sur le serveur SMB, vous devez connaître les instructions relatives aux configurations de plusieurs LIF de données pour un SVM.

Lorsque vous configurez un serveur SMB, plusieurs LIF de données peuvent être configurées. Si c'est le cas, le serveur DNS contient plusieurs `A` Entrées d'enregistrement pour le serveur CIFS, toutes utilisant le même nom d'hôte de serveur SMB, mais chacune avec une adresse IP unique. Par exemple, un serveur SMB dont deux LIF de données sont configurées peut avoir le DNS suivant `A` entrées d'enregistrement :

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Le comportement normal est qu'après modification du paramètre de signature SMB requis, seules les nouvelles connexions des clients sont affectées par la modification du paramètre de signature SMB. Cependant, il y a une exception à ce comportement. Il existe un cas où un client dispose d'une connexion existante à un partage, et le client crée une nouvelle connexion au même partage après la modification du paramètre, tout en maintenant la connexion d'origine. Dans ce cas, la connexion SMB, nouvelle et existante, adopte les nouvelles exigences de signature SMB.

Prenons l'exemple suivant :

1. Client1 se connecte à un partage sans avoir à signer SMB à l'aide du chemin `O:\`.
2. L'administrateur du stockage modifie la configuration du serveur SMB afin de exiger la signature SMB.
3. Client1 se connecte au même partage avec la signature SMB requise à l'aide du chemin `S:\` (tout en maintenant la connexion à l'aide du chemin `O:\`).
4. Par conséquent, le SMB Signing est utilisé pour accéder aux données sur le système `O:\` et `S:\` disques.

Configurez la signature ONTAP pour le trafic SMB entrant

Vous pouvez imposer aux clients l'exigence de signer les messages SMB en activant la signature SMB requise. S'il est activé, ONTAP n'accepte que les messages SMB s'ils ont une signature valide. Si vous souhaitez autoriser la signature SMB, mais pas l'exiger, vous pouvez désactiver la signature SMB requise.

Description de la tâche

Par défaut, le SMB Signing requis est désactivé. Vous pouvez activer ou désactiver la signature SMB requise à tout moment.

> La signature SMB n'est pas désactivée par défaut dans les cas suivants :
>
> 1. Le signature SMB requis est activé et le cluster est rétabli sur une version d'ONTAP qui ne prend pas en charge la signature SMB.
> 2. Le cluster est ensuite mis à niveau vers une version de ONTAP qui prend en charge la signature SMB.
>
>   Dans ce cas, la configuration de signature SMB qui a été configurée à l'origine sur une version prise en charge de ONTAP est conservée par le biais d'une nouvelle version et d'une mise à niveau ultérieure.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité de signature SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non-ID-preserve), le paramètre de sécurité de

signature SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé la signature SMB requise sur le SVM source, vous devez activer manuellement le SMB Signing requis sur le SVM de destination.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le SMB soit connecté…	Entrez la commande…
Activé	`vserver cifs security modify -vserver vserver_name -is-signing-required true`
Désactivé	`vserver cifs security modify -vserver vserver_name -is-signing-required false`

2. Vérifiez que la signature SMB requise est activée ou désactivée en déterminant si la valeur dans l' `Is Signing Required` le champ de la sortie de la commande suivante est défini sur la valeur souhaitée : `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Exemple

L'exemple suivant active la signature SMB requise pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

Informations associées

- "création snapmirror"

Déterminez si les sessions SMB ONTAP sont signées

Vous pouvez afficher des informations sur les sessions SMB connectées sur le serveur CIFS. Vous pouvez utiliser ces informations pour déterminer si les sessions SMB sont signées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur…	Entrez la commande…
Toutes les sessions signées sur une machine virtuelle de stockage (SVM) spécifiée	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Détails d'une session signée avec un ID de session spécifique sur le SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Exemples

La commande suivante affiche les informations relatives aux sessions signées sur le SVM vs1. La sortie de résumé par défaut n'affiche pas le champ de sortie « session signée is » :

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

La commande suivante affiche des informations détaillées sur la session, notamment si elle est signée, dans une session SMB avec l'ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Informations associées

Contrôle des statistiques de session signées SMB

Surveiller les statistiques de session ONTAP SMB signée

Vous pouvez surveiller les statistiques des sessions SMB et déterminer les sessions établies qui sont signées et qui ne le sont pas.

Description de la tâche

Le `statistics` la commande au niveau de privilège avancé fournit le `signed_sessions` Compteur que vous pouvez utiliser pour surveiller le nombre de sessions SMB signées. Le `signed_sessions` le compteur est disponible avec les objets de statistiques suivants :

- `cifs` Permet de surveiller la signature SMB pour toutes les sessions SMB.
- `smb1` Permet de surveiller la signature SMB pour les sessions SMB 1.0.
- `smb2` Permet de surveiller la signature SMB pour les sessions SMB 2.x et SMB 3.0.

  Les statistiques SMB 3.0 sont incluses dans les résultats de `smb2` objet.

Si vous souhaitez comparer le nombre de sessions signées au nombre total de sessions, vous pouvez comparer les résultats de la session `signed_sessions` compteur avec la sortie pour le `established_sessions` compteur.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données

résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

Étapes

1. Définissez le niveau de privilège sur avancé :
   `set -privilege advanced`
2. Démarrer une collecte de données :
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

   Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.

   Pour en savoir plus, `statistics start` consultez le "Référence de commande ONTAP".
3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.

   En savoir plus sur `statistics stop` dans le "Référence de commande ONTAP" .
4. Afficher les statistiques de signature SMB :

Si vous souhaitez afficher les informations pour…	**Entrer…**
Sessions signées	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sessions signées et sessions établies
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Si vous souhaitez afficher les informations pour un seul nœud, spécifiez l'option `-node` paramètre.

   Pour en savoir plus, `statistics show` consultez le "Référence de commande ONTAP".
5. Revenir au niveau de privilège admin :
   `set -privilege admin`

Exemples

L’exemple suivant montre comment surveiller les statistiques de signature SMB 2.x et SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d’accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

La commande suivante arrête la collecte des données de l’échantillon :

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

La commande suivante affiche les sessions SMB signées et les sessions SMB établies par nœud à partir de l’exemple :

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

La commande suivante affiche les sessions SMB signées pour le nœud 2 à partir de l'exemple :

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

La commande suivante revient au niveau de privilège admin :

```
cluster1::*> set -privilege admin
```

Informations associées

- Déterminez si les sessions SMB sont signées
- "Contrôle des performances et présentation de la gestion"

Configurez le chiffrement SMB requis sur les serveurs SMB pour les transferts de données via SMB

En savoir plus sur le chiffrement SMB ONTAP

Le chiffrement SMB pour les transferts de données via SMB est une amélioration de sécurité que vous pouvez activer ou désactiver sur les serveurs SMB. Vous pouvez également configurer le paramètre de chiffrement SMB souhaité sur une base partage par partage à l'aide d'un paramètre de propriété de partage.

Par défaut, lorsque vous créez un serveur SMB sur la machine virtuelle de stockage (SVM), le chiffrement SMB est désactivé. Vous devez leur permettre de bénéficier de la sécurité améliorée fournie par le chiffrement SMB.

Pour créer une session SMB chiffrée, le client SMB doit prendre en charge le chiffrement SMB. Les clients Windows commençant par Windows Server 2012 et Windows 8 prennent en charge le cryptage SMB.

Le chiffrement SMB sur la SVM est contrôlé par deux paramètres :

- Option de sécurité du serveur SMB qui active la fonctionnalité sur le SVM
- Propriété de partage SMB qui configure le paramètre de chiffrement SMB partage par partage

Vous pouvez décider s'il faut un chiffrement pour accéder à toutes les données de la SVM ou bien demander un chiffrement SMB pour accéder aux données uniquement dans les partages sélectionnés. Les paramètres des SVM prévalent sur les paramètres de niveau partage.

La configuration de cryptage SMB efficace dépend de la combinaison des deux paramètres. Elle est décrite dans le tableau suivant :

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Vrai	Faux	Le chiffrement au niveau du serveur est activé pour tous les partages du SVM. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.
Vrai	Vrai	Le chiffrement au niveau du serveur est activé pour tous les partages de la SVM indépendamment du chiffrement au niveau du partage. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Faux	Vrai	Le chiffrement au niveau du partage est activé pour les partages spécifiques. Avec cette configuration, le chiffrement se produit à partir de l'arborescence à connecter.
Faux	Faux	Aucun chiffrement n'est activé.

Les clients SMB qui ne prennent pas en charge le chiffrement ne peuvent pas se connecter à un serveur SMB ou à un partage qui nécessite un chiffrement.

Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

Découvrez l'impact du chiffrement ONTAP SMB sur les performances

Lorsque les sessions SMB utilisent le chiffrement SMB, toutes les communications SMB vers et depuis les clients Windows rencontrent un impact sur les performances, qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM qui contient le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis ONTAP 9.7, un nouvel algorithme de désactivation du chiffrement permet d'améliorer les performances du trafic SMB chiffré. Le délestage du chiffrement SMB est activé par défaut lorsque le chiffrement SMB est activé.

L'optimisation des performances de chiffrement SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact du cryptage SMB sur les performances peut varier fortement. Vous pouvez le vérifier uniquement par le biais de tests dans l'environnement réseau.

Le chiffrement SMB est désactivé par défaut sur le serveur SMB. Vous devez activer le chiffrement SMB uniquement sur les partages SMB ou les serveurs SMB qui nécessitent un chiffrement. Avec le cryptage SMB, ONTAP effectue un traitement supplémentaire du décryptage des demandes et du cryptage des réponses à chaque demande. Le chiffrement SMB ne doit donc être activé que lorsque cela est nécessaire.

Activez ou désactivez le chiffrement SMB ONTAP pour le trafic entrant

Si vous souhaitez exiger le cryptage SMB pour le trafic SMB entrant, vous pouvez l'activer sur le serveur CIFS ou au niveau du partage. Par défaut, le chiffrement SMB n'est pas requis.

Description de la tâche

Vous pouvez activer le chiffrement SMB sur le serveur CIFS, qui s'applique à tous les partages du serveur CIFS. Si vous ne souhaitez pas utiliser le cryptage SMB requis pour tous les partages du serveur CIFS ou si vous souhaitez activer le cryptage SMB requis pour le trafic SMB entrant, partage par partage, vous pouvez désactiver le cryptage SMB requis sur le serveur CIFS.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité du cryptage SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non ID-preserve), le paramètre de sécurité du cryptage SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé le chiffrement SMB sur le SVM source, vous devez activer manuellement le chiffrement SMB du serveur CIFS sur la destination.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le chiffrement SMB soit requis pour le trafic SMB entrant sur le serveur CIFS…	Entrez la commande…
Activé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Désactivé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Vérifiez que le chiffrement SMB requis sur le serveur CIFS est activé ou désactivé, selon les besoins : `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   Le `is-smb-encryption-required` s'affiche `true` Le cas échéant, le cryptage SMB est activé sur le serveur CIFS et `false` s'il est désactivé.

Exemple

L'exemple suivant permet le cryptage SMB requis pour le trafic SMB entrant pour le serveur CIFS sur le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Informations associées

- "création snapmirror"

Déterminez si les clients sont connectés à l'aide de sessions ONTAP SMB chiffrées

Vous pouvez afficher des informations sur les sessions SMB connectées pour déterminer si les clients utilisent des connexions SMB chiffrées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

Description de la tâche

Les sessions client SMB peuvent avoir l'un des trois niveaux de chiffrement suivants :

- `unencrypted`

  La session SMB n'est pas chiffrée. Ni le chiffrement au niveau des serveurs virtuels de stockage ou du partage n'est configuré.

- `partially-encrypted`

  Le chiffrement est lancé lorsque l'arborescence se connecte. Le chiffrement au niveau du partage est configuré. Le chiffrement au niveau des SVM n'est pas activé.

- `encrypted`

  La session SMB est entièrement chiffrée. Le chiffrement au niveau des SVM est activé. Le chiffrement au niveau du partage peut être activé ou non. Le paramètre de cryptage au niveau SVM remplace le paramètre de cryptage au niveau du partage.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur…	Entrez la commande…
Sessions avec un paramètre de chiffrement spécifié pour les sessions sur un SVM spécifié	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Si vous voulez afficher des informations sur…	Entrez la commande…
Paramètre de chiffrement pour un ID de session spécifique sur un SVM spécifié	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Exemples

La commande suivante affiche des informations détaillées sur la session, y compris le paramètre de chiffrement, sur une session SMB avec l'ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Surveillez les statistiques de chiffrement SMB ONTAP

Vous pouvez surveiller les statistiques de cryptage SMB et déterminer les sessions établies et les connexions de partage qui sont cryptées et qui ne le sont pas.

Description de la tâche

Le `statistics` Le niveau de privilège avancé fournit les compteurs suivants, que vous pouvez utiliser pour surveiller le nombre de sessions SMB chiffrées et de connexions pour le partage :

Nom du compteur	Descriptions
`encrypted_sessions`	Indique le nombre de sessions SMB 3.0 cryptées

Nom du compteur	Descriptions
`encrypted_share_connections`	Indique le nombre de partages cryptés sur lesquels une arborescence s'est connectée
`rejected_unencrypted_sessions`	Indique le nombre de configurations de session rejetées en raison d'un manque de capacité de chiffrement du client
`rejected_unencrypted_shares`	Indique le nombre de mappages de partage rejetés en raison d'un manque de capacité de chiffrement du client

Ces compteurs sont disponibles avec les objets de statistiques suivants :

- `cifs` Permet de surveiller le chiffrement SMB pour toutes les sessions SMB 3.0.

  Les statistiques SMB 3.0 sont incluses dans les résultats de `cifs` objet. Si vous souhaitez comparer le nombre de sessions chiffrées au nombre total de sessions, vous pouvez comparer les résultats de l' `encrypted_sessions` compteur avec la sortie pour le `established_sessions` compteur.

  Si vous souhaitez comparer le nombre de connexions de partage chiffrées au nombre total de connexions de partage, vous pouvez comparer la sortie du `encrypted_share_connections` compteur avec la sortie pour le `connected_shares` compteur.

- `rejected_unencrypted_sessions` Indique le nombre de tentatives d'établissement d'une session SMB nécessitant un chiffrement d'un client qui ne prend pas en charge le chiffrement SMB.
- `rejected_unencrypted_shares` Indique combien de fois une tentative de connexion à un partage SMB nécessite un chiffrement d'un client ne prenant pas en charge le chiffrement SMB.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

Étapes

1. Définissez le niveau de privilège sur avancé :
   `set -privilege advanced`
2. Démarrer une collecte de données :
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

   Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.

Pour en savoir plus, `statistics start` consultez le "Référence de commande ONTAP".

3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.

   En savoir plus sur `statistics stop` dans le "Référence de commande ONTAP" .

4. Afficher les statistiques de chiffrement SMB :

Si vous souhaitez afficher les informations pour…	**Entrer…**
Sessions chiffrées	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sessions chiffrées et sessions établies
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Connexions de partage cryptées
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Connexions de partage cryptées et partages connectés	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sessions non chiffrées rejetées rejetées	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Les connexions de partage non chiffrées ont été rejetées
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

   Si vous souhaitez afficher les informations uniquement pour un seul nœud, spécifiez l'option `-node` paramètre.

   Pour en savoir plus, `statistics show` consultez le "Référence de commande ONTAP".

5. Revenir au niveau de privilège admin :
   `set -privilege admin`

Exemples

L’exemple suivant montre comment surveiller les statistiques de cryptage SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d’accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

La commande suivante arrête la collecte des données pour cet échantillon :

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

La commande suivante affiche les sessions SMB chiffrées et les sessions SMB établies par le nœud à partir de l’exemple :

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

La commande suivante affiche le nombre de sessions SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

La commande suivante indique le nombre de partages SMB connectés et de partages SMB chiffrés par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

La commande suivante affiche le nombre de connexions de partage SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Informations associées

- Déterminer quelles statistiques, quels objets et quels compteurs sont disponibles sur les serveurs
- "Contrôle des performances et présentation de la gestion"

Communication de session LDAP sécurisée

En savoir plus sur la signature et le chiffrement SMB ONTAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous

devez configurer les paramètres de sécurité du serveur CIFS sur la machine virtuelle de stockage (SVM) de sorte qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`.

La signature et le chiffrement LDAP sur le trafic CIFS sont activés sur le SVM avec le `-session-security -for-ad-ldap` à la `vserver cifs security modify` commande.

Activez la signature et le chiffrement LDAP sur les serveurs SMB ONTAP

Avant que votre serveur CIFS puisse utiliser la signature et le chiffrement pour sécuriser la communication avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur CIFS pour activer la signature et le chiffrement LDAP.

Avant de commencer

Vous devez consulter votre administrateur de serveur AD pour déterminer les valeurs de configuration de sécurité appropriées.

Étapes

1. Configurez le paramètre de sécurité du serveur CIFS qui autorise le trafic signé et scellé avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver` *`vserver_name`* `-session -security-for-ad-ldap {none|sign|seal}`

   Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

2. Vérifiez que le paramètre de sécurité de signature et de chiffrement LDAP est défini correctement : `vserver cifs security show -vserver` *`vserver_name`*

> Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX, comme les utilisateurs, les groupes et les netgroups, alors vous devez activer le paramètre correspondant avec le `-session-security` de la `vserver services name-service ldap client modify` commande.

Configurer LDAP sur TLS

Exportation de certificats CA racine auto-signés pour les SVM SMB ONTAP

Pour utiliser LDAP sur SSL/TLS pour sécuriser la communication Active Directory, vous devez d'abord exporter une copie du certificat d'autorité de certification racine auto-signé du service de certificats Active Directory en fichier de certificat et la convertir en fichier texte ASCII. Ce fichier texte est utilisé par ONTAP pour installer le certificat sur la machine virtuelle de stockage (SVM).

Avant de commencer

Le service de certificat Active Directory doit déjà être installé et configuré pour le domaine auquel le serveur CIFS appartient. Vous trouverez des informations sur l'installation et la configuration des services de certificats

Active Director en consultant la bibliothèque Microsoft TechNet.

"Bibliothèque Microsoft TechNet : technet.microsoft.com"

Étape

1. Obtenez un certificat d'autorité de certification racine du contrôleur de domaine qui se trouve dans le `.pem` format de texte.

   "Bibliothèque Microsoft TechNet : technet.microsoft.com"

Une fois que vous avez terminé

Installer le certificat sur le SVM.

Informations associées

"Bibliothèque Microsoft TechNet"

Installer les certificats CA racine auto-signés sur le SVM SMB ONTAP

Si l'authentification LDAP avec TLS est requise lorsqu'il s'agit de serveurs LDAP, vous devez d'abord installer le certificat AC racine auto-signé sur le SVM.

Description de la tâche

Toutes les applications de ONTAP qui utilisent les communications TLS peuvent vérifier l'état du certificat numérique à l'aide du protocole OCSP (Online Certificate Status Protocol). Si OCSP est activé pour LDAP sur TLS, les certificats révoqués sont rejetés et la connexion échoue.

Étapes

1. Installez le certificat d'autorité de certification racine auto-signé :
   a. Commencez l'installation du certificat : `security certificate install -vserver vserver_name -type server-ca`

      La sortie de la console affiche le message suivant : `Please enter Certificate: Press <Enter> when done`

   b. Ouvrez le certificat `.pem` fichier avec un éditeur de texte, copiez le certificat, y compris les lignes commençant par `-----BEGIN CERTIFICATE-----` et se terminant par `-----END CERTIFICATE-----`, puis collez le certificat après l'invite de commande.
   c. Vérifiez que le certificat s'affiche correctement.
   d. Terminez l'installation en appuyant sur entrée.
2. Vérifiez que le certificat est installé : `security certificate show -vserver vserver_name`

Informations associées

- "installation du certificat de sécurité"
- "certificat de sécurité afficher"

Activez LDAP sur TLS sur le serveur SMB ONTAP

Avant que votre serveur SMB puisse utiliser TLS pour sécuriser les communications avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du

serveur SMB pour activer LDAP sur TLS.

Depuis ONTAP 9.10.1, la liaison des canaux LDAP est prise en charge par défaut pour les connexions LDAP Active Directory (AD) et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison des canaux LDAP avec les serveurs AD, utilisez le `-try-channel -binding-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.

Pour en savoir plus, voir :

- "En savoir plus sur LDAP pour les SVM NFS ONTAP"
- "2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows".

Étapes

1. Configurez le paramètre de sécurité du serveur SMB permettant une communication LDAP sécurisée avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Vérifiez que le paramètre de sécurité LDAP sur TLS est défini sur `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX (par exemple, utilisateurs, groupes et netgroups), alors vous devez également modifier `-use-start-tls` à l'aide de `vserver services name-service ldap client modify` commande.

Configurez ONTAP SMB multicanal pour des performances et une redondance optimales

Depuis ONTAP 9.4, vous pouvez configurer SMB Multichannel pour fournir plusieurs connexions entre ONTAP et les clients dans une seule session SMB. Cela améliore le débit et la tolérance aux pannes.

Avant de commencer

La fonctionnalité SMB Multichannel ne peut être utilisée que lorsque les clients négocient avec SMB 3.0 ou une version ultérieure. SMB 3.0 et versions ultérieures sont activés par défaut sur le serveur ONTAP SMB.

Description de la tâche

Les clients SMB détectent et utilisent automatiquement plusieurs connexions réseau si une configuration adéquate est identifiée sur le cluster ONTAP.

Le nombre de connexions simultanées dans une session SMB dépend des cartes réseau que vous avez déployées :

- **NIC 1G sur le client et le cluster ONTAP**

  Le client établit une connexion par carte réseau et lie la session à toutes les connexions.

- **Cartes réseau 10G et de capacité supérieure sur le client et le cluster ONTAP**

  Le client établit jusqu'à quatre connexions par carte réseau et lie la session à toutes les connexions. Le client peut établir des connexions sur plusieurs cartes réseau 10G et supérieures.

Vous pouvez également modifier les paramètres suivants (privilège avancé) :

- `-max-connections-per-session`

  Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut est 32 connexions.

  Si vous souhaitez activer plus de connexions que la configuration par défaut, vous devez effectuer des ajustements comparables à la configuration client, qui possède également une valeur par défaut de 32 connexions.

- `-max-lifs-per-session`

  Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut est 256 interfaces réseau.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Activez SMB Multichannel sur le serveur SMB :

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Vérifiez que ONTAP signale les sessions SMB multicanaux :

```
vserver cifs session show
```

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

L'exemple suivant affiche les informations relatives à toutes les sessions SMB, affichant plusieurs connexions pour une seule session :

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

L'exemple suivant affiche des informations détaillées sur une session SMB avec l'ID-session 1 :

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
       Workstation IP Address: 10.1.1.1
      Authentication Mechanism: NTLMv1
         User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Configurez les mappages utilisateur Windows par défaut sur utilisateur UNIX sur le serveur SMB

Configurez l’utilisateur SMB UNIX ONTAP par défaut

Vous pouvez configurer l’utilisateur UNIX par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l’authentification des utilisateurs non mappés échoue, vous ne devez pas configurer l’utilisateur UNIX par défaut.

Description de la tâche

Par défaut, le nom de l’utilisateur UNIX par défaut est ""pcuser"", ce qui signifie que par défaut, le mappage d’utilisateur à l’utilisateur UNIX par défaut est activé. Vous pouvez spécifier un autre nom à utiliser comme utilisateur UNIX par défaut. Le nom que vous spécifiez doit exister dans les bases de données de service de noms configurées pour la machine virtuelle de stockage (SVM). Si cette option est définie sur une chaîne null, personne ne peut accéder au serveur CIFS en tant qu’utilisateur UNIX par défaut. En d’autres termes, chaque utilisateur doit avoir un compte dans la base de données de mots de passe avant d’accéder au serveur CIFS.

Pour qu’un utilisateur puisse se connecter au serveur CIFS à l’aide du compte utilisateur UNIX par défaut, l’utilisateur doit respecter les conditions préalables suivantes :

- L’utilisateur est authentifié.
- L’utilisateur se trouve dans la base de données utilisateur Windows locale du serveur CIFS, dans le domaine personnel du serveur CIFS ou dans un domaine approuvé (si les recherches de mappage de noms de domaines multiples sont activées sur le serveur CIFS).
- Le nom d’utilisateur n’est pas explicitement mappé à une chaîne nulle.

Étapes

1. Configurez l’utilisateur UNIX par défaut :

Si vous voulez …	Entrer …
Utiliser l’utilisateur UNIX par défaut « pcuser »	`vserver cifs options modify -default -unix-user pcuser`
Utiliser un autre compte utilisateur UNIX comme utilisateur par défaut	`vserver cifs options modify -default -unix-user` *`user_name`*
Désactivez l’utilisateur UNIX par défaut	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Vérifiez que l’utilisateur UNIX par défaut est configuré correctement : `vserver cifs options show -vserver` *`vserver_name`*

   Dans l’exemple suivant, l’utilisateur UNIX par défaut et l’utilisateur UNIX invité sur le SVM vs1 sont configurés pour utiliser l’utilisateur UNIX « pcuser » :

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configurez l'utilisateur ONTAP SMB UNIX invité

Configurer l'option utilisateur UNIX invité signifie que les utilisateurs qui se connectent à partir de domaines non fiables sont mappés à l'utilisateur UNIX invité et peuvent se connecter au serveur CIFS. Si vous souhaitez que l'authentification des utilisateurs de domaines non fiables échoue, vous ne devez pas configurer l'utilisateur UNIX invité. La valeur par défaut est de ne pas autoriser les utilisateurs de domaines non fiables à se connecter au serveur CIFS (le compte UNIX invité n'est pas configuré).

Description de la tâche

Lors de la configuration du compte UNIX invité, vous devez garder à l'esprit les éléments suivants :

- Si le serveur CIFS ne peut pas authentifier l'utilisateur par rapport à un contrôleur de domaine pour le domaine personnel, un domaine approuvé ou la base de données locale et que cette option est activée, le serveur CIFS considère l'utilisateur comme un utilisateur invité et mappe l'utilisateur avec l'utilisateur UNIX spécifié.
- Si cette option est définie sur une chaîne null, l'utilisateur UNIX invité est désactivé.
- Vous devez créer un utilisateur UNIX afin d'utiliser comme utilisateur UNIX invité dans l'une des bases de données de service de nom de la machine virtuelle de stockage (SVM).
- Un utilisateur connecté en tant qu'utilisateur invité est automatiquement membre du groupe BUILTIN\guest sur le serveur CIFS.
- L'option 'homedirs-public' s'applique uniquement aux utilisateurs authentifiés. Un utilisateur connecté en tant qu'utilisateur invité ne dispose pas d'un répertoire personnel et ne peut pas accéder aux répertoires d'accueil des autres utilisateurs.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrer…
Configurer l'utilisateur UNIX invité	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Désactiver l'utilisateur UNIX invité	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Vérifiez que l'utilisateur UNIX invité est configuré correctement : `vserver cifs options show -vserver vserver_name`

   Dans l'exemple suivant, l'utilisateur UNIX par défaut et l'utilisateur UNIX invité sur le SVM vs1 sont configurés pour utiliser l'utilisateur UNIX « pcuser » :

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

Mappez les groupes d'administrateurs à la racine SMB de ONTAP

Si vous ne possédez que des clients CIFS dans votre environnement et que votre machine virtuelle de stockage (SVM) a été configurée comme un système de stockage multiprotocole, vous devez disposer d'au moins un compte Windows disposant de privilège racine pour accéder aux fichiers sur la SVM ; Sinon, vous ne pouvez pas gérer la SVM car vous ne disposez pas de droits d'utilisateur suffisants.

Description de la tâche

Si votre système de stockage a été configuré en NTFS-only, le `/etc` répertoire dispose d'une ACL de niveau fichier qui permet au groupe d'administrateurs d'accéder aux fichiers de configuration ONTAP.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez l'option de serveur CIFS qui mappe le groupe d'administrateurs à root, le cas échéant :

Les fonctions que vous recherchez…	Alors…
Associez les membres du groupe d'administrateurs à la racine	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` Tous les comptes du groupe administrateurs sont considérés comme root, même si vous n'avez pas de `/etc/usermap.cfg` entrée mappant les comptes à la racine. Si vous créez un fichier à l'aide d'un compte appartenant au groupe d'administrateurs, le fichier est détenu par root lorsque vous affichez le fichier à partir d'un client UNIX.
Désactivez le mappage des membres du groupe d'administrateurs à la racine	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` Les comptes du groupe d'administrateurs ne sont plus mis en correspondance avec root. Vous ne pouvez mapper explicitement un seul utilisateur qu'à la racine.

3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver` *`vserver_name`*
4. Retour au niveau de privilège admin : `set -privilege admin`

Affiche des informations sur les types d'utilisateurs connectés via les sessions SMB ONTAP

Vous pouvez afficher des informations sur le type d'utilisateurs connectés via des sessions SMB. Cela vous aide à vous assurer que seul le type d'utilisateur approprié est connecté via des sessions SMB sur la machine virtuelle de stockage (SVM).

Description de la tâche

Les types d'utilisateurs suivants peuvent se connecter via des sessions SMB :

- `local-user`

  Authentifié en tant qu'utilisateur CIFS local

- `domain-user`

  Authentifié en tant qu'utilisateur de domaine (soit à partir du domaine personnel du serveur CIFS ou d'un domaine de confiance)

- `guest-user`

  Authentifié en tant qu'utilisateur invité

- `anonymous-user`

  Authentifié en tant qu'utilisateur anonyme ou nul

Étapes

1. Déterminez le type d'utilisateur connecté au cours d'une session SMB : `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Si vous souhaitez afficher les informations de type d'utilisateur pour les sessions établies…	Saisissez la commande suivante…
Pour toutes les sessions avec un type d'utilisateur spécifié	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Pour un utilisateur spécifique

Exemples

La commande suivante affiche des informations sur le type d'utilisateur pour les sessions sur le SVM vs1 établies par l'utilisateur "` ipubs\user1'":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Options de commande ONTAP pour limiter la consommation excessive de ressources client Windows

Les options du `vserver cifs options modify` La commande vous permet de contrôler la consommation des ressources pour les clients Windows. Cela peut être utile si un client se trouve en dehors des limites normales de consommation des ressources, par exemple si un nombre inhabituellement élevé de fichiers sont ouverts, si des sessions sont ouvertes ou si des demandes de modification sont envoyées.

Les options suivantes pour le `vserver cifs options modify` La commande a été ajoutée pour contrôler la consommation des ressources client Windows. Si la valeur maximale de l'une de ces options est dépassée, la demande est refusée et un message EMS est envoyé. Un message d'avertissement EMS est également envoyé lorsque 80 % de la limite configurée pour ces options sont atteintes.

- `-max-opens-same-file-per-tree`

  Nombre maximum d'ouvertures sur le même fichier par arborescence CIFS

- `-max-same-user-sessions-per-connection`

  Nombre maximal de sessions ouvertes par le même utilisateur par connexion

- `-max-same-tree-connect-per-session`

  Nombre maximal de connexions d'arborescence sur le même partage par session

- `-max-watches-set-per-tree`

  Nombre maximum de montres (également appelé *change notifie*) établi par arbre

Pour en savoir plus, `vserver cifs options modify` consultez le "Référence de commande ONTAP".

Depuis ONTAP 9.4, les serveurs exécutant SMB version 2 ou ultérieure peuvent limiter le nombre de requêtes en attente (*crédits SMB*) que le client peut envoyer au serveur sur une connexion SMB. La gestion des crédits SMB est initiée par le client et contrôlée par le serveur.

Le nombre maximal de requêtes en attente pouvant être accordées sur une connexion SMB est contrôlé par le `-max-credits` option. La valeur par défaut de cette option est 128.

Améliorez les performances de vos clients grâce aux oplocks classiques et de location

Découvrez comment améliorer les performances des clients PME ONTAP grâce aux oplocks classiques et aux locations

Les oplocks traditionnels (verrous opportunistes) et les oplocks de location permettent à un client SMB dans certains scénarios de partage de fichiers d'effectuer une mise en cache côté client des informations de lecture anticipée, d'écriture différée et de verrouillage. Un client peut alors lire ou écrire dans un fichier sans rappeler régulièrement au serveur qu'il a besoin d'accéder au fichier en question. Ceci améliore les performances en réduisant le trafic réseau.

Les oplocks de location sont une forme améliorée de oplocks disponibles avec le protocole SMB 2.1 et les versions ultérieures. Les oplocks de location permettent à un client d'obtenir et de préserver l'état de mise en cache du client sur plusieurs ouvertures SMB en provenance de lui-même.

Les oplocks peuvent être contrôlés de deux façons :

- Par une propriété de partage, en utilisant `vserver cifs share create` lorsque le partage est créé, ou le `vserver share properties` commande après sa création.
- Par une propriété qtree, en utilisant le `volume qtree create` commande lors de la création du qtree, ou le `volume qtree oplock` commandes après leur création.

Apprenez-en plus sur les considérations relatives à la perte de données du cache SMB ONTAP lors de l'utilisation d'oplocks

Dans certaines circonstances, si un processus possède un oplock exclusif sur un fichier et qu'un deuxième processus tente d'ouvrir le fichier, le premier processus doit invalider les données mises en cache et vider les écritures et les verrous. Le client doit ensuite abandonner le oplock et accéder au fichier. En cas de panne du réseau pendant ce vidage, les données d'écriture mises en cache peuvent être perdues.

- Les possibilités de perte de données

  Toute application avec des données en cache d'écriture peut perdre ces données dans les circonstances

suivantes :

- La connexion s'effectue à l'aide de SMB 1.0.
- Il a un oplock exclusif sur le fichier.
- Il est dit de briser ce oplock ou de fermer le fichier.
- Lors du vidage du cache d'écriture, le réseau ou le système cible génère une erreur.

- Erreur de gestion et de fin d'écriture

  Le cache lui-même n'a pas de traitement d'erreur—les applications le font. Lorsque l'application effectue une écriture dans le cache, l'écriture est toujours terminée. Si le cache, à son tour, effectue une écriture sur le système cible via un réseau, il doit supposer que l'écriture est terminée car si ce n'est pas le cas, les données sont perdues.

Activez ou désactivez les oplocks lors de la création de partages SMB ONTAP

Les oplocks permettent aux clients de verrouiller des fichiers et de mettre du contenu en cache localement, ce qui peut augmenter les performances des opérations sur les fichiers. Les oplocks sont activés sur des partages SMB résidant sur des SVM (Storage Virtual machine). Dans certaines circonstances, vous pouvez désactiver les oplocks. Vous pouvez activer ou désactiver les oplocks sur une base de partage par partage.

Description de la tâche

Si les oplocks sont activés sur le volume contenant un partage mais que la propriété de partage oplock pour ce partage est désactivée, les oplocks sont désactivés pour ce partage. La désactivation des oplocks sur un partage a priorité sur le paramètre oplock de volume. La désactivation des oplocks sur le partage désactive à la fois les oplocks opportunistes et les oplocks de location.

Vous pouvez spécifier d'autres propriétés de partage en plus de spécifier la propriété de partage oplock à l'aide d'une liste délimitée par des virgules. Vous pouvez également spécifier d'autres paramètres de partage.

Étapes

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Alors…
Activez les oplocks sur un partage lors de la création du partage	Saisissez la commande suivante : `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Si vous souhaitez que le partage n'ait que les propriétés de partage par défaut, c'est-à-dire `oplocks`, `browsable`, et `changenotify` activé, vous n'avez pas besoin de spécifier le `-share-properties` Paramètre lors de la création d'un partage SMB. Si vous souhaitez utiliser une combinaison de propriétés de partage autre que la valeur par défaut, vous devez spécifier l' `-share-properties` paramètre avec la liste des propriétés de partage à utiliser pour ce partage.
Désactiver les oplocks sur un partage lors de la création du partage	Saisissez la commande suivante : `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Lors de la désactivation des oplocks, vous devez spécifier une liste de propriétés de partage lors de la création du partage, mais vous ne devez pas spécifier le `oplocks` propriété.

Informations associées

Activez ou désactivez les oplocks sur les partages SMB existants

Surveiller l'état du oplock

Commandes ONTAP pour activer ou désactiver les oplocks sur les volumes SMB et les qtrees

Les oplocks permettent aux clients de verrouiller des fichiers et de mettre du contenu en cache localement, ce qui peut augmenter les performances des opérations sur les fichiers. Vous devez connaître les commandes permettant d'activer ou de désactiver les oplocks sur des volumes ou des qtrees. Vous devez également savoir quand vous pouvez activer ou désactiver les oplocks sur des volumes et des qtrees.

- Les oplocks sont activés par défaut sur les volumes.
- Vous ne pouvez pas désactiver les oplocks lorsque vous créez un volume.
- Vous pouvez à tout moment activer ou désactiver les oplocks sur des volumes existants pour des SVM.
- Vous pouvez activer les oplocks sur des qtrees pour les SVM.

  Le paramètre du mode oplock est une propriété de l'ID qtree 0, le qtree par défaut que tous les volumes ont. Si vous ne spécifiez pas de paramètre oplock lors de la création d'un qtree, le qtree hérite du paramètre oplock du volume parent, qui est activé par défaut. Cependant, si vous spécifiez un paramètre oplock sur le nouveau qtree, il est prioritaire sur le paramètre oplock sur le volume.

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez les oplocks sur des volumes ou des qtrees	`volume qtree oplocks` avec le `-oplock-mode` paramètre défini sur `enable`
Désactiver les oplocks sur des volumes ou des qtrees	`volume qtree oplocks` avec le `-oplock-mode` paramètre défini sur `disable`

Informations associées

Surveiller l'état du oplock

Activer ou désactiver les oplocks sur les partages SMB ONTAP existants

Les oplocks sont activés par défaut sur des partages SMB sur des SVM (Storage Virtual machines). Dans certaines circonstances, vous pouvez désactiver les oplocks. Si vous avez précédemment désactivé les oplocks sur un partage, vous pouvez également réactiver les oplocks.

Description de la tâche

Si les oplocks sont activés sur le volume contenant un partage, mais que la propriété de partage oplock pour ce partage est désactivée, les oplocks sont désactivés pour ce partage. La désactivation des oplocks sur un partage a priorité sur l'activation des oplocks sur le volume. La désactivation des oplocks sur la part désactive les oplocks opportunistes et ceux de location. Vous pouvez à tout moment activer ou désactiver les oplocks sur des partages existants.

Étape

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Alors…
Activez les oplocks sur un partage en modifiant un partage existant	Saisissez la commande suivante : `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` Vous pouvez spécifier des propriétés de partage supplémentaires à ajouter à l'aide d'une liste délimitée par des virgules. Les nouvelles propriétés ajoutées sont ajoutées à la liste existante des propriétés de partage. Toutes les propriétés de partage que vous avez précédemment spécifiées restent en vigueur.
Désactivez les oplocks sur un partage en modifiant un partage existant	Saisissez la commande suivante : `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` Vous pouvez spécifier des propriétés de partage supplémentaires à supprimer à l'aide d'une liste délimitée par des virgules. Les propriétés de partage que vous supprimez sont supprimées de la liste existante de propriétés de partage. Cependant, les propriétés de partage configurées précédemment que vous ne supprimez pas restent en vigueur.

Exemples

La commande suivante active les oplocks pour le partage nommé « Ingénierie » sur une machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

La commande suivante désactive les oplocks pour l'action nommée « Engineering » sur le SVM vs1 :

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Informations associées

- Activez ou désactivez les oplocks lors de la création de partages SMB
- Surveiller l'état du oplock
- Ajouter ou supprimer des propriétés de partage sur des partages existants

Surveillez l'état des ONTAP SMB oplock

Vous pouvez surveiller et afficher des informations sur l'état du oplock. Vous pouvez utiliser ces informations pour déterminer quels fichiers ont des oplocks, ce que sont le niveau de oplock et le niveau d'état de oplock et si le leasing oplock est utilisé. Vous pouvez également déterminer des informations sur les verrous que vous devrez peut-être briser manuellement.

Description de la tâche

Vous pouvez afficher des informations sur tous les oplocks sous forme de résumé ou sous forme de liste détaillée. Vous pouvez également utiliser des paramètres facultatifs pour afficher des informations sur un plus petit sous-ensemble de verrous existants. Par exemple, vous pouvez spécifier que le retour de sortie se verrouille uniquement avec l'adresse IP du client spécifiée ou avec le chemin d'accès spécifié.

Vous pouvez afficher les informations suivantes sur les oplocks classiques et de location :

- SVM, node, volume et LIF sur lequel le oplock est établi
- Verrouiller l'UUID
- Adresse IP du client avec le oplock
- Chemin auquel le oplock est établi
- Protocole de verrouillage (SMB) et type (oplock)
- État de verrouillage
- Niveau oplock
- État de connexion et heure d'expiration SMB
- ID de groupe ouvert si un oplock de bail est accordé

Pour en savoir plus, `vserver oplocks show` consultez le "Référence de commande ONTAP".

Étapes

1. Afficher l'état du oplock à l'aide de l' `vserver locks show` commande.

Exemples

La commande suivante affiche des informations par défaut sur tous les verrouillages. Le oplock du fichier affiché est accordé avec un `read-batch` niveau oplock :

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

L'exemple suivant affiche des informations plus détaillées sur le verrouillage d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un oplock de bail est accordé sur le dossier avec un `batch` Niveau oplock vers un client avec une adresse IP de `10.3.1.3`:

> Lors de l'affichage d'informations détaillées, la commande fournit une sortie séparée pour les informations oplock et sharelock. Cet exemple montre uniquement la sortie de la section oplock.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Informations associées

Activez ou désactivez les oplocks lors de la création de partages SMB

Activez ou désactivez les oplocks sur les partages SMB existants

Commandes permettant d'activer ou de désactiver les oplocks sur les volumes SMB et les qtrees

Appliquez des objets de stratégie de groupe aux serveurs SMB

Découvrez comment appliquer des objets de stratégie de groupe aux serveurs SMB ONTAP

Votre serveur SMB prend en charge les objets de stratégie de groupe (GPO, Group Policy Objects), un ensemble de règles appelées attributs de stratégie de groupe_ qui s'appliquent aux ordinateurs dans un environnement Active Directory. Vous pouvez utiliser des GPO pour gérer centralement les paramètres de toutes les machines virtuelles de stockage (SVM) sur le cluster appartenant au même domaine Active Directory.

Lorsque les stratégies de groupe sont activées sur votre serveur SMB, ONTAP envoie des requêtes LDAP au serveur Active Directory pour demander des informations de stratégie de groupe. Si des définitions de GPO sont applicables à votre serveur SMB, le serveur Active Directory renvoie les informations de GPO suivantes :

- Nom de l'objet GPO
- Version GPO actuelle
- Emplacement de la définition de GPO
- Listes d'UUID (identificateurs uniques universels) pour les jeux de stratégies GPO

Informations associées

- En savoir plus sur la sécurité d'accès aux fichiers pour les serveurs
- "Audit et suivi de sécurité SMB et NFS"

Découvrez les objets de stratégie de groupe SMB ONTAP pris en charge

Bien que tous les objets de stratégie de groupe (GPO) ne soient pas applicables à vos SVM (Storage Virtual machines) compatibles CIFS, les SVM peuvent reconnaître et traiter l'ensemble des GPO pertinents.

Les GPO suivants sont actuellement pris en charge sur SVM :

- Paramètres de configuration des règles d'audit avancées :

  Accès aux objets : staging de stratégie d'accès central

  Spécifie le type d'événements à auditer pour l'activation de la stratégie d'accès central (CAP), y compris les paramètres suivants :

  - Ne pas auditer
  - Vérifier uniquement les événements de réussite
  - Audit des événements d'échec uniquement
  - Vérifiez à la fois les événements de réussite et d'échec

  > Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

  Réglez à l'aide du `Audit Central Access Policy Staging` réglage dans le `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Pour utiliser les paramètres de stratégie d'audit avancée, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Paramètres du registre :

  - Intervalle d'actualisation des règles de groupe pour les SVM compatibles CIFS

    Réglez à l'aide du `Registry` GPO.

- Actualisation aléatoire de la stratégie de groupe

  Réglez à l'aide du `Registry` GPO.

- Publication de hachage pour BranchCache

  La publication Hash pour BranchCache correspond au mode de fonctionnement de BranchCache. Les trois modes de fonctionnement pris en charge sont les suivants :

  - Par action
  - Tous les partages
  - Désactivé
    Réglez à l'aide du `Registry` GPO.

- Prise en charge du hachage pour BranchCache

  Les trois paramètres de version de hachage suivants sont pris en charge :

  - BranchCache version 1
  - BranchCache version 2
  - BranchCache versions 1 et 2
    Réglez à l'aide du `Registry` GPO.

> Pour utiliser les paramètres de BranchCache, BranchCache doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si BranchCache n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Les paramètres de sécurité

  - Règle d'audit et journal des événements

    - Audit des événements de connexion

      Spécifie le type d'événements de connexion à auditer, notamment les paramètres suivants :

      - Ne pas auditer
      - Vérifier uniquement les événements de réussite
      - Audit sur les événements de panne
      - Vérifiez à la fois les événements de réussite et d'échec
        Réglez à l'aide du `Audit logon events` réglage dans le `Local Policies/Audit Policy` GPO.

        > Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

    - Auditer l'accès aux objets

      Spécifie le type d'accès aux objets à auditer, y compris les paramètres suivants :

      - Ne pas auditer

        - Vérifier uniquement les événements de réussite
        - Audit sur les événements de panne
        - Vérifiez à la fois les événements de réussite et d'échec
          Réglez à l'aide du `Audit object access` réglage dans le `Local Policies/Audit Policy` GPO.

          Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

      - Méthode de conservation des journaux

        Spécifie la méthode de conservation du journal d'audit, y compris les paramètres suivants :

        - Remplacez le journal des événements lorsque la taille du fichier journal dépasse la taille maximale du journal
        - Ne pas écraser le journal des événements (effacer le journal manuellement)
          Réglez à l'aide du `Retention method for security log` réglage dans le `Event Log` GPO.

      - Taille maximale du journal

        Spécifie la taille maximale du journal d'audit.

        Réglez à l'aide du `Maximum security log size` réglage dans le `Event Log` GPO.

        Pour utiliser les paramètres de stratégie d'audit et de stratégie GPO du journal des événements, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

    - Sécurité du système de fichiers

      Spécifie une liste de fichiers ou de répertoires sur lesquels la sécurité des fichiers est appliquée via un GPO.

      Réglez à l'aide du `File System` GPO.

      Le chemin d'accès au volume auquel la stratégie de sécurité du système de fichiers est configurée doit exister au sein de la SVM.

    - Règle Kerberos

      - Inclinaison maximale de l'horloge

        Spécifie la tolérance maximale en minutes pour la synchronisation de l'horloge de l'ordinateur.

        Réglez à l'aide du `Maximum tolerance for computer clock synchronization` réglage dans le `Account Policies/Kerberos Policy` GPO.

      - Âge maximum du billet

Spécifie la durée de vie maximale en heures pour le ticket utilisateur.

Réglez à l'aide du `Maximum lifetime for user ticket` réglage dans le `Account Policies/Kerberos Policy` GPO.

- Âge maximum de renouvellement du billet

  Spécifie la durée de vie maximale en jours pour le renouvellement du ticket utilisateur.

Réglez à l'aide du `Maximum lifetime for user ticket renewal` réglage dans le `Account Policies/Kerberos Policy` GPO.

◦ Attribution de droits utilisateur (droits de privilège)

- Devenir propriétaire

  Indique la liste des utilisateurs et des groupes qui ont le droit de prendre possession de tout objet sécurisé.

  Réglez à l'aide du `Take ownership of files or other objects` réglage dans le `Local Policies/User Rights Assignment` GPO.

- Privilège de sécurité

  Indique la liste des utilisateurs et des groupes qui peuvent spécifier des options d'audit pour l'accès aux objets de ressources individuelles, telles que des fichiers, des dossiers et des objets Active Directory.

  Réglez à l'aide du `Manage auditing and security log` réglage dans le `Local Policies/User Rights Assignment` GPO.

- Changer le privilège de notification (vérification de la traverse de dérivation)

  Indique la liste des utilisateurs et des groupes qui peuvent traverser les arborescences de répertoires, même si les utilisateurs et les groupes ne disposent pas des autorisations sur le répertoire de traversée.

Le même privilège est requis pour que les utilisateurs reçoivent des notifications sur les modifications apportées aux fichiers et aux répertoires. Réglez à l'aide du `Bypass traverse checking` réglage dans le `Local Policies/User Rights Assignment` GPO.

◦ Valeurs de registre

- Paramètre de signature requis

  Indique si la signature SMB requise est activée ou désactivée.

Réglez à l'aide du `Microsoft network server: Digitally sign communications (always)` réglage dans le `Security Options` GPO.

◦ Limiter l'anonymat

Indique les restrictions pour les utilisateurs anonymes et inclut les trois paramètres de stratégie de groupe suivants :

- Pas d'énumération des comptes de Security Account Manager (SAM) :

  Ce paramètre de sécurité détermine les autorisations supplémentaires accordées pour les connexions anonymes à l'ordinateur. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

  Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts` réglage dans le `Local Policies/Security Options` GPO.

- Pas d'énumération des comptes et des partages SAM

  Ce paramètre de sécurité détermine si l'énumération anonyme des comptes et partages SAM est autorisée. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

  Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts and shares` réglage dans le `Local Policies/Security Options` GPO.

- Limiter l'accès anonyme aux partages et aux canaux nommés

  Ce paramètre de sécurité limite l'accès anonyme aux partages et aux tuyaux. Cette option s'affiche sous la forme `no-access` Dans ONTAP, si elle est activée.

  Réglez à l'aide du `Network access: Restrict anonymous access to Named Pipes and Shares` réglage dans le `Local Policies/Security Options` GPO.

  Lors de l'affichage d'informations sur les stratégies de groupe définies et appliquées, le `Resultant restriction for anonymous user` Le champ sortie fournit des informations sur la restriction résultant des trois paramètres de GPO anonymes de restriction. Les restrictions possibles résultantes sont les suivantes :

° `no-access`

L'utilisateur anonyme refuse l'accès aux partages spécifiés et aux canaux nommés, et ne peut pas utiliser l'énumération des comptes et des partages SAM. Cette restriction résultante est visible si le `Network access: Restrict anonymous access to Named Pipes and Shares` L'objet GPO est activé.

° `no-enumeration`

L'utilisateur anonyme a accès aux partages spécifiés et aux canaux nommés, mais ne peut pas utiliser l'énumération des comptes et partages SAM. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

- Le `Network access: Restrict anonymous access to Named Pipes and Shares` GPO est désactivé.
- Soit le `Network access: Do not allow anonymous enumeration of SAM accounts` ou le `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Les stratégies de groupe sont activées.

° `no-restriction`

L'utilisateur anonyme dispose d'un accès complet et peut utiliser l'énumération. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

- Le `Network access: Restrict anonymous access to Named Pipes and Shares` GPO est désactivé.
- Les deux `Network access: Do not allow anonymous enumeration of SAM accounts` et `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Les GPO sont désactivés.
  - Groupes restreints

    Vous pouvez configurer des groupes restreints pour gérer de manière centralisée l'appartenance à des groupes intégrés ou définis par l'utilisateur. Lorsque vous appliquez un groupe restreint via une stratégie de groupe, l'appartenance à un groupe local de serveur CIFS est automatiquement définie pour correspondre aux paramètres de liste d'appartenance définis dans la stratégie de groupe appliquée.

  Réglez à l'aide du `Restricted Groups` GPO.

- Paramètres de stratégie d'accès centralisé

  Spécifie une liste de stratégies d'accès centralisé. Les politiques d'accès central et les règles de politique d'accès central associées déterminent les autorisations d'accès pour plusieurs fichiers sur la SVM.

Informations associées

- Activer ou désactiver la prise en charge des GPO sur les serveurs
- En savoir plus sur la sécurité d'accès aux fichiers pour les serveurs
- "Audit et suivi de sécurité SMB et NFS"
- Modifier les paramètres de sécurité du serveur
- Découvrez comment utiliser BranchCache pour mettre en cache le contenu partagé dans une succursale
- Découvrez comment utiliser la signature ONTAP pour améliorer la sécurité du réseau
- En savoir plus sur la configuration de la vérification de contournement
- Configurez les restrictions d'accès pour les utilisateurs anonymes

Configuration serveur SMB ONTAP requise pour les GPO

Pour utiliser des stratégies de groupe (GPO, Group Policy Objects) avec votre serveur SMB, votre système doit répondre à plusieurs exigences.

- SMB doit être sous licence sur le cluster. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.
- Un serveur SMB doit être configuré et joint à un domaine Windows Active Directory.
- L'état admin du serveur SMB doit être on.
- Les GPO doivent être configurés et appliqués à l'unité organisationnelle (ou) Windows Active Directory contenant l'objet ordinateur serveur SMB.
- La prise en charge des GPO doit être activée sur le serveur SMB.

Activez ou désactivez la prise en charge des stratégies de groupe sur les serveurs SMB ONTAP

Vous pouvez activer ou désactiver la prise en charge des objets de stratégie de groupe (GPO, Group Policy Object) sur un serveur CIFS. Si vous activez la prise en charge GPO

sur un serveur CIFS, les GPO applicables définis sur la stratégie de groupe—la stratégie appliquée à l'unité organisationnelle (ou) qui contient l'objet ordinateur de serveur CIFS—sont appliqués au serveur CIFS.

Description de la tâche

Les GPO ne peuvent pas être activés sur les serveurs CIFS en mode Workgroup.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activer les stratégies de groupe	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Désactiver les stratégies de groupe	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Vérifiez que la prise en charge des stratégies de groupe est dans l'état souhaité : `vserver cifs group-policy show -vserver +vserver_name_`

   L'état de la stratégie de groupe pour les serveurs CIFS en mode groupe de travail s'affiche en tant que « désactivé ».

Exemple

L'exemple suivant illustre la prise en charge de GPO sur SVM (Storage Virtual machine) vs1 :

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Informations associées

En savoir plus sur les GPO pris en charge

Configuration requise pour les GPO

En savoir plus sur la mise à jour des GPO sur les serveurs SMB

Mettre à jour manuellement les paramètres GPO sur les serveurs SMB

Affiche des informations sur les configurations GPO

Mise à jour des objets GPO sur le serveur SMB

En savoir plus sur la mise à jour des GPO sur les serveurs SMB ONTAP

Par défaut, ONTAP récupère et applique les modifications des objets de stratégie de groupe (GPO) toutes les 90 minutes. Les paramètres de sécurité sont actualisés toutes les 16 heures. Si vous voulez mettre à jour les GPO pour appliquer de nouveaux paramètres de stratégie GPO avant que ONTAP ne les mette à jour automatiquement, vous pouvez déclencher une mise à jour manuelle sur un serveur CIFS à l'aide d'une commande ONTAP.

- Par défaut, tous les GPO sont vérifiés et mis à jour au besoin toutes les 90 minutes.

  Cet intervalle est configurable et peut être défini à l'aide du `Refresh interval` et `Random offset` Paramètres GPO.

  ONTAP interroge Active Directory pour les modifications apportées aux stratégies de groupe. Si les numéros de version de GPO enregistrés dans Active Directory sont supérieurs à ceux du serveur CIFS, ONTAP récupère et applique les nouveaux GPO. Si les numéros de version sont identiques, les GPO sur le serveur CIFS ne sont pas mis à jour.

- Les stratégies de sécurité sont actualisées toutes les 16 heures.

  ONTAP récupère et applique les stratégies de groupe de paramètres de sécurité toutes les 16 heures, que ces stratégies de groupe aient été modifiées ou non.

  > La valeur par défaut de 16 heures ne peut pas être modifiée dans la version ONTAP actuelle. Il s'agit d'un paramètre par défaut du client Windows.

- Tous les GPO peuvent être mis à jour manuellement à l'aide d'une commande ONTAP.

  Cette commande simule Windows `gpupdate.exe``commande /force'.

Informations associées

Mettre à jour manuellement les paramètres GPO sur les serveurs SMB

Mettre à jour manuellement les paramètres GPO sur les serveurs SMB ONTAP

Si vous souhaitez mettre à jour immédiatement les paramètres des objets GPO (Group Policy Object) sur votre serveur CIFS, vous pouvez mettre à jour les paramètres manuellement. Vous pouvez uniquement mettre à jour les paramètres modifiés ou forcer une mise à jour pour tous les paramètres, y compris les paramètres qui ont été appliqués auparavant mais qui n'ont pas été modifiés.

Étape

1. Effectuez l'action appropriée :

Si vous voulez mettre à jour…	Entrez la commande…
Paramètres de GPO modifiés	`vserver cifs group-policy update -vserver` *vserver_name*

Si vous voulez mettre à jour…	Entrez la commande…
Tous les paramètres GPO	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

Informations associées

En savoir plus sur la mise à jour des GPO sur les serveurs SMB

Affiche des informations sur les configurations GPO SMB ONTAP

Vous pouvez afficher des informations sur les configurations GPO (Group Policy Object) définies dans Active Directory et à propos des configurations GPO appliquées au serveur CIFS.

Description de la tâche

Vous pouvez afficher des informations sur toutes les configurations GPO définies dans Active Directory du domaine auquel appartient le serveur CIFS ou afficher des informations uniquement sur les configurations GPO appliquées à un serveur CIFS.

Étapes

1. Pour afficher des informations sur les configurations GPO, effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des informations sur toutes les configurations de stratégie de groupe…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Appliquée à une machine virtuelle de stockage (SVM) compatible CIFS	`vserver cifs group-policy show-applied -vserver vserver_name`

Exemple

L'exemple suivant présente les configurations GPO définies dans Active Directory à laquelle la SVM compatible CIFS vs1 appartient :

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
------------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
```

```
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache : version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
```

```
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

L’exemple suivant présente les configurations GPO appliquées au SVM vs1 compatible CIFS :

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
```

```
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Informations associées

Activer ou désactiver la prise en charge des GPO sur les serveurs

Affiche des informations sur les GPO de groupe restreint SMB ONTAP

Vous pouvez afficher des informations détaillées sur les groupes restreints qui sont définis comme objets de stratégie de groupe (GPO, Group Policy Objects) dans Active Directory et qui sont appliqués au serveur CIFS.

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom de la stratégie de groupe
- Version de la stratégie de groupe
- Lien

  Spécifie le niveau dans lequel la stratégie de groupe est configurée. Les valeurs de sortie possibles sont les suivantes :

- `Local` Lorsque la stratégie de groupe est configurée dans ONTAP
- `Site` lorsque la stratégie de groupe est configurée au niveau du site dans le contrôleur de domaine
- `Domain` lorsque la stratégie de groupe est configurée au niveau du domaine dans le contrôleur de domaine
- `OrganizationalUnit` Lorsque la stratégie de groupe est configurée au niveau de l'unité organisationnelle (ou) dans le contrôleur de domaine
- `RSOP` pour l'ensemble résultant de règles dérivées de toutes les stratégies de groupe définies à différents niveaux

- Nom de groupe restreint
- Utilisateurs et groupes qui appartiennent à et qui n'appartiennent pas au groupe restreint
- Liste des groupes auxquels le groupe restreint est ajouté

  Un groupe peut être membre de groupes autres que ceux répertoriés ici.

Étape

1. Afficher des informations sur tous les GPO de groupe restreints en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur tous les GPO de groupe restreints…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Appliqué à un serveur CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Exemple

L'exemple suivant affiche les informations relatives aux stratégies de groupe restreintes définies dans le domaine Active Directory auquel appartient la SVM compatible CIFS nommée vs1 :

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

L'exemple suivant affiche les informations relatives aux groupes restreints GPO appliqués au SVM vs1 activé pour CIFS :

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

Informations associées

Affiche des informations sur les stratégies d'accès central SMB ONTAP

Vous pouvez afficher des informations détaillées sur les stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les stratégies d'accès central appliquées au serveur CIFS via des objets de stratégie de groupe (GPO).

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom du SVM
- Nom de la stratégie d'accès central
- SID
- Description
- Heure de création
- Heure de modification
- Règles des membres

Les serveurs CIFS en mode groupe de travail ne sont pas affichés car ils ne prennent pas en charge les GPO.

Étape

1. Afficher des informations sur les stratégies d'accès central en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur toutes les stratégies d'accès central…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Appliqué à un serveur CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche les informations pour toutes les stratégies d'accès central définies dans Active Directory :

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

L'exemple suivant affiche les informations de toutes les règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Informations associées

- En savoir plus sur la sécurité d'accès aux fichiers pour les serveurs
- Affiche des informations sur les configurations GPO
- Afficher des informations sur les règles de stratégie d'accès central

Affiche des informations sur les règles de stratégie d'accès central SMB ONTAP

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les règles d'accès central appliquées au serveur CIFS via des stratégies d'accès centrales (objets de stratégie de groupe).

Description de la tâche

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central définies et appliquées. Par défaut, les informations suivantes sont affichées :

- Nom d'un vserver
- Nom de la règle d'accès central
- Description
- Heure de création
- Heure de modification
- Autorisations en cours
- Autorisations proposées
- Ressources cibles

Si vous souhaitez afficher des informations sur toutes les règles de stratégie d'accès central associées aux stratégies d'accès central…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Appliqué à un serveur CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Exemple

L'exemple suivant affiche les informations de toutes les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory :

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

L'exemple suivant affiche les informations de toutes les règles d'accès central associées aux règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Informations associées

- En savoir plus sur la sécurité d'accès aux fichiers pour les serveurs
- Affiche des informations sur les configurations GPO
- Afficher des informations sur les stratégies d'accès central

Commandes ONTAP pour la gestion des mots de passe des comptes d'ordinateur du serveur SMB

Vous devez connaître les commandes permettant de modifier, de réinitialiser et de désactiver les mots de passe, ainsi que de configurer des planifications de mises à jour automatiques. Vous pouvez également configurer une planification sur le serveur SMB pour la mettre à jour automatiquement.

Les fonctions que vous recherchez…	Utilisez cette commande…
Modifiez le mot de passe du compte de domaine lorsque ONTAP est synchronisé avec les services AD	`vserver cifs domain password change`
Réinitialisez le mot de passe du compte de domaine lorsque ONTAP n'est pas synchronisé avec les services AD	`vserver cifs domain password reset`
Configurez les serveurs SMB pour les changements de mot de passe de compte d'ordinateur automatique	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Désactivez les modifications de mot de passe de compte informatique automatique sur les serveurs SMB	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Pour en savoir plus, `vserver cifs domain password` consultez le "Référence de commande ONTAP".

Gérer les connexions du contrôleur de domaine

Affiche des informations sur les serveurs ONTAP SMB découverts

Vous pouvez afficher les informations relatives aux serveurs LDAP découverts et aux contrôleurs de domaine sur votre serveur CIFS.

Étape

1. Pour afficher les informations relatives aux serveurs découverts, entrez la commande suivante : `vserver cifs domain discovered-servers show`

Exemple

L'exemple suivant montre les serveurs découverts pour le SVM vs1 :

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informations associées

- Réinitialiser et redécouvrir les serveurs
- Arrêter ou démarrer les serveurs

Réinitialisez et redécouvrez les serveurs SMB ONTAP

La réinitialisation et la redécouverte des serveurs sur votre serveur CIFS permet au serveur CIFS de supprimer les informations stockées sur les serveurs LDAP et les contrôleurs de domaine. Après l'abandon des informations sur le serveur, le serveur CIFS acquiert de nouveau les informations actuelles sur ces serveurs externes. Cela peut être utile lorsque les serveurs connectés ne répondent pas correctement.

Étapes

1. Saisissez la commande suivante : `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Afficher les informations sur les nouveaux serveurs découverts : `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

Exemple

L'exemple suivant illustre la réinitialisation et la redécouverte des serveurs pour la machine virtuelle de stockage (SVM, anciennement Vserver) vs1 :

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informations associées

- Affiche des informations sur les serveurs découverts
- Arrêter ou démarrer les serveurs

Gérer la détection du contrôleur de domaine SMB ONTAP

À partir de ONTAP 9.3, vous pouvez modifier le processus par défaut par lequel les contrôleurs de domaine (DCS) sont détectés. Cela vous permet de limiter la détection à votre site ou à un pool de data centers préférés, ce qui peut entraîner des améliorations des performances en fonction de l'environnement.

Description de la tâche

Par défaut, le processus de découverte dynamique détecte tous les DCS disponibles, y compris tous les DCS préférés, tous les DCS du site local et tous les DCS distants. Cette configuration peut entraîner des temps de latence pour l'authentification et l'accès aux partages dans certains environnements. Si vous avez déjà déterminé le pool de DCS que vous souhaitez utiliser ou si les DCS distants sont insuffisants ou inaccessibles, vous pouvez changer la méthode de découverte.

Dans ONTAP 9.3 et versions ultérieures, le `discovery-mode` paramètre du `cifs domain discovered-servers` la commande vous permet de sélectionner l'une des options de découverte suivantes :

- Tous les DCS du domaine sont découverts.
- Seuls les DCS du site local sont découverts.

  Le `default-site` Le paramètre du serveur SMB peut être défini pour utiliser ce mode avec des LIFs qui ne sont pas attribuées à un site dans sites-et-services.

- La détection de serveur n'est pas effectuée, la configuration du serveur SMB dépend uniquement des DCS préférés.

  Pour utiliser ce mode, vous devez d'abord définir le DCS préféré pour le serveur SMB.

Avant de commencer

Vous devez avoir le niveau de privilège avancé.

Étape

1. Spécifiez l'option de découverte souhaitée : `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   Options du `mode` paramètre :

   - `all`

     Découvrez tous les DCS disponibles (par défaut).

   - `site`

     Limitez la détection de DC à votre site.

   - `none`

     Utilisez uniquement les DCS préférés sans effectuer de découverte.

Ajoutez vos contrôleurs de domaine SMB ONTAP préférés

ONTAP détecte automatiquement les contrôleurs de domaine via DNS. Vous pouvez éventuellement ajouter un ou plusieurs contrôleurs de domaine à la liste des contrôleurs de domaine privilégiés pour un domaine spécifique.

Description de la tâche

Si une liste de contrôleurs de domaine privilégiés existe déjà pour le domaine spécifié, la nouvelle liste est fusionnée avec la liste existante.

Étape

1. Pour ajouter à la liste des contrôleurs de domaine privilégiés, entrez la commande suivante : `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver` *`vserver_name`* Spécifie le nom de la machine virtuelle de stockage (SVM).

   `-domain` *`domain_name`* Spécifie le nom Active Directory complet du domaine auquel appartiennent les contrôleurs de domaine spécifiés.

   `-preferred-dc` *`IP_address`*,… indique une ou plusieurs adresses IP des contrôleurs de domaine préférés, en tant que liste délimitée par des virgules, par ordre de préférence.

Exemple

La commande suivante ajoute des contrôleurs de domaine 172.17.102.25 et 172.17.102.24 à la liste des contrôleurs de domaine préférés que le serveur SMB du SVM vs1 utilise pour gérer l'accès externe au domaine cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Informations associées

Commandes pour la gestion des contrôleurs de domaine privilégiés

Commandes ONTAP pour la gestion des contrôleurs de domaine SMB privilégiés

Vous devez connaître les commandes permettant d'ajouter, d'afficher et de supprimer les contrôleurs de domaine préférés.

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajouter un contrôleur de domaine préféré	`vserver cifs domain preferred-dc add`
Afficher les contrôleurs de domaine préférés	`vserver cifs domain preferred-dc show`
Supprimez un contrôleur de domaine préféré	`vserver cifs domain preferred-dc remove`

Pour en savoir plus, `vserver cifs domain preferred-dc` consultez le "Référence de commande ONTAP".

Informations associées

Ajouter des contrôleurs de domaine préférés

Activez les connexions chiffrées aux contrôleurs de domaine SMB ONTAP

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine.

Description de la tâche

ONTAP nécessite un cryptage pour les communications du contrôleur de domaine (DC) lorsque le système `-encryption-required-for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3.

Lorsque des communications DC cryptées sont requises, le `-smb2-enabled-for-dc-connections` L'option est ignorée, car ONTAP négocie uniquement les connexions SMB3. Si un DC ne prend pas en charge le SMB3 et le chiffrement, ONTAP ne se connecte pas avec lui.

Étape

1. Activer la communication chiffrée avec le DC : `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Utilisez des sessions null pour accéder au stockage dans des environnements non Kerberos

Utilisez les sessions NULL SMB ONTAP pour accéder au stockage dans des environnements non Kerberos

L'accès aux sessions null fournit des autorisations pour les ressources réseau, telles que les données du système de stockage, ainsi que pour les services basés sur les clients s'exécutant sous le système local. Une session null se produit lorsqu'un processus client utilise le compte "système" pour accéder à une ressource réseau. La configuration de session null est spécifique à l'authentification non Kerberos.

Découvrez comment les systèmes de stockage ONTAP SMB offrent un accès de session nulle

Comme les partages de session NULL ne nécessitent pas d'authentification, les clients qui ont besoin d'un accès de session nul doivent avoir leurs adresses IP mappées sur le système de stockage.

Par défaut, les clients de session null non mappés peuvent accéder à certains services système ONTAP, tels que l'énumération de partage, mais l'accès aux données du système de stockage est limité.

> ONTAP prend en charge les valeurs de paramètre de registre RestrictAnonymous de Windows avec `-restrict-anonymous` l'option. Cela vous permet de contrôler la mesure dans laquelle les utilisateurs nuls non mappés peuvent afficher ou accéder aux ressources système. Par exemple, vous pouvez désactiver l'énumération de partage et l'accès au partage IPC$ (le partage de tuyauterie nommé masqué). Pour en savoir plus sur `vserver cifs options modify` et et `vserver cifs options show` sur l' `–restrict-anonymous`option dans le "Référence de commande ONTAP".

Sauf configuration contraire, un client exécutant un processus local qui demande l'accès au système de stockage via une session nulle est membre uniquement de groupes non restrictifs, tels que « tout le monde ». Pour limiter l'accès à une session nulle aux ressources du système de stockage sélectionnées, vous pouvez créer un groupe auquel appartiennent tous les clients de session nulle. La création de ce groupe vous permet de limiter l'accès au système de stockage et de définir des autorisations de ressources du système de stockage qui s'appliquent spécifiquement aux clients de session nul.

ONTAP fournit une syntaxe de mappage dans le `vserver name-mapping` Ensemble de commandes permettant de spécifier l'adresse IP des clients autorisés à accéder aux ressources du système de stockage à l'aide d'une session utilisateur null. Une fois que vous avez créé un groupe pour les utilisateurs nuls, vous pouvez spécifier des restrictions d'accès pour les ressources du système de stockage et les autorisations de ressources qui s'appliquent uniquement aux sessions nulles. L'utilisateur null est identifié comme une connexion anonyme. Les utilisateurs null n'ont accès à aucun répertoire personnel.

Les autorisations d'utilisateur mappées sont accordées à tout utilisateur null accédant au système de stockage à partir d'une adresse IP mappée. Prenez les précautions appropriées pour empêcher tout accès non autorisé aux systèmes de stockage mappés avec des utilisateurs nuls. Pour une protection maximale, placez le système de stockage et tous les clients nécessitant un accès nul au système de stockage utilisateur sur un réseau distinct, afin d'éliminer la possibilité d'une adresse IP « couverture ».

Informations associées

Configurez les restrictions d'accès pour les utilisateurs anonymes

Accorder aux utilisateurs nuls l'accès aux partages de système de fichiers SMB ONTAP

Vous pouvez autoriser l'accès aux ressources de votre système de stockage par les clients de session null en attribuant un groupe à utiliser par les clients de session null et

en enregistrant les adresses IP des clients de session null à ajouter à la liste des clients autorisés à accéder aux données à l'aide de sessions null du système de stockage.

Étapes

1. Utilisez le `vserver name-mapping create` Commande permettant de mapper l'utilisateur null à un utilisateur Windows valide, avec un qualificateur IP.

   La commande suivante mappe l'utilisateur null à user1 avec un nom d'hôte valide google.com :

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   La commande suivante mappe l'utilisateur null à utilisateur1 avec une adresse IP valide 10.238.2.54/32 :

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. Utilisez le `vserver name-mapping show` commande pour confirmer le mappage de nom.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1       -                 10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. Utilisez le `vserver cifs options modify –win-name-for-null-user` Commande permettant d'attribuer l'appartenance à Windows à l'utilisateur nul.

   Cette option est applicable uniquement lorsqu'il existe un mappage de nom valide pour l'utilisateur nul.

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. Utilisez le `vserver cifs options show` Commande pour confirmer le mappage de l'utilisateur null à l'utilisateur ou au groupe Windows.

   ```
   vserver cifs options show

   Vserver :vs1

   Map Null User to Windows User of Group: user1
   ```

Gérer les alias NetBIOS des serveurs SMB

En savoir plus sur la gestion des alias NetBIOS pour les serveurs SMB ONTAP

Les alias NetBIOS sont des noms alternatifs pour votre serveur SMB que les clients SMB peuvent utiliser lors de la connexion au serveur SMB. La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs de fichiers d'origine.

Vous pouvez spécifier une liste d'alias NetBIOS lorsque vous créez le serveur SMB ou à tout moment après avoir créé le serveur SMB. Vous pouvez à tout moment ajouter ou supprimer des alias NetBIOS de la liste. Vous pouvez vous connecter au serveur SMB en utilisant l'un des noms de la liste d'alias NetBIOS.

Informations associées

Affiche des informations sur NetBIOS sur connexions TCP

Ajoutez des listes d'alias NetBIOS aux serveurs SMB ONTAP

Si vous souhaitez que les clients SMB se connectent au serveur SMB à l'aide d'un alias, vous pouvez créer une liste d'alias NetBIOS ou ajouter des alias NetBIOS à une liste existante d'alias NetBIOS.

Description de la tâche

- Le nom d'alias NetBIOS peut contenir jusqu'à 15 caractères.
- Vous pouvez configurer jusqu'à 200 alias NetBIOS sur le serveur SMB.
- Les caractères suivants ne sont pas autorisés :

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

Étapes

1. Ajoutez les alias NetBIOS:
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - Vous pouvez spécifier un ou plusieurs alias NetBIOS à l'aide d'une liste délimitée par des virgules.
   - Les alias NetBIOS spécifiés sont ajoutés à la liste existante.
   - Une nouvelle liste d'alias NetBIOS est créée si la liste est actuellement vide.
2. Vérifiez que les alias NetBIOS ont été correctement ajoutés : `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Informations associées

- Supprimer les alias NetBIOS de la liste pour les serveurs SMB
- Afficher la liste des alias NetBIOS pour les serveurs SMB

Supprimez les alias NetBIOS de la liste pour les serveurs SMB ONTAP

Si vous n'avez pas besoin d'alias NetBIOS spécifiques pour un serveur CIFS, vous pouvez supprimer ces alias NetBIOS de la liste. Vous pouvez également supprimer tous les alias NetBIOS de la liste.

Description de la tâche

Vous pouvez supprimer plusieurs alias NetBIOS à l'aide d'une liste délimitée par des virgules. Vous pouvez supprimer tous les alias NetBIOS d'un serveur CIFS en spécifiant - comme valeur pour le `-netbios -aliases` paramètre.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez supprimer…	Entrer…
Alias NetBIOS spécifiques dans la liste	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
Tous les alias NetBIOS de la liste	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Vérifiez que les alias NetBIOS spécifiés ont été supprimés : `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Affiche la liste des alias NetBIOS pour les serveurs SMB ONTAP

Vous pouvez afficher la liste des alias NetBIOS. Cela peut être utile lorsque vous voulez déterminer la liste des noms sur lesquels les clients SMB peuvent établir des connexions au serveur CIFS.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur…	Entrer…
Alias NetBIOS d'un serveur CIFS	`vserver cifs show -display-netbios -aliases`
La liste des alias NetBIOS dans le cadre des informations détaillées du serveur CIFS	`vserver cifs show -instance`

L'exemple suivant affiche des informations sur les alias NetBIOS d'un serveur CIFS :

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

L'exemple suivant affiche la liste des alias NetBIOS dans le cadre des informations détaillées du serveur CIFS :

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                      CIFS Server NetBIOS Name: CIFS_SERVER
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
               CIFS Server Administrative Status: up
                         CIFS Server Description:
                         List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Pour en savoir plus, `vserver cifs show` consultez le "Référence de commande ONTAP".

Informations associées

- Ajouter des listes d'alias NetBIOS aux serveurs

- Commandes pour la gestion des serveurs

Déterminez si les clients SMB ONTAP sont connectés à l'aide d'alias NetBIOS

Vous pouvez déterminer si les clients SMB sont connectés à l'aide d'alias NetBIOS et, si oui, quel alias NetBIOS est utilisé pour établir la connexion. Cela peut être utile lors du dépannage des problèmes de connexion.

Description de la tâche

Vous devez utiliser le `-instance` Paramètre pour afficher l'alias NetBIOS (le cas échéant) associé à une connexion SMB. Si le nom du serveur CIFS ou une adresse IP est utilisé pour établir la connexion SMB, la sortie de l' `NetBIOS Name` c'est – (tiret).

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez afficher les informations NetBIOS pour…	Entrer…
Connexions SMB	`vserver cifs session show -instance`
Connexions utilisant un alias NetBIOS spécifié :	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

L'exemple suivant affiche des informations sur l'alias NetBIOS utilisé pour établir la connexion SMB avec l'ID de session 1 :

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
          Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Gérer diverses tâches de serveur SMB

Arrêtez ou démarrez les serveurs SMB ONTAP

Vous pouvez arrêter le serveur CIFS sur un SVM, ce qui peut être utile lors d'opérations effectuées lorsque les utilisateurs n'accèdent pas aux données via les partages SMB. Vous pouvez redémarrer l'accès SMB en démarrant le serveur CIFS. En arrêtant le serveur CIFS, vous pouvez également modifier les protocoles autorisés sur la machine virtuelle de stockage (SVM).

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Arrêtez le serveur CIFS	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Démarrez le serveur CIFS
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` indique si la commande doit s'exécuter au premier plan ou en arrière-plan. Si vous ne

saisissez pas ce paramètre, il est défini sur `true`, et la commande est exécutée au premier plan.

2. Vérifiez que l'état administratif du serveur CIFS est correct à l'aide du `vserver cifs show` commande.

Exemple

Les commandes suivantes permettent de démarrer le serveur CIFS sur le SVM vs1 :

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Informations associées

- Affiche des informations sur les serveurs découverts
- Réinitialiser et redécouvrir les serveurs

Déplacez des serveurs SMB ONTAP vers différentes UO

Le processus de création du serveur CIFS utilise les unités organisationnelles (ou) CN=ordinateurs par défaut lors de la configuration, sauf si vous spécifiez une autre unité administrative. Après l'installation, vous pouvez déplacer les serveurs CIFS vers différents UO.

Étapes

1. Sur le serveur Windows, ouvrez l'arborescence **utilisateurs et ordinateurs Active Directory**.
2. Recherchez l'objet Active Directory pour la machine virtuelle de stockage (SVM).
3. Cliquez avec le bouton droit de la souris sur l'objet et sélectionnez **déplacer**.
4. Sélectionnez l'unité d'organisation que vous souhaitez associer à la SVM

Résultats

L'objet SVM est placé dans l'UO sélectionnée.

Modifiez le domaine DNS dynamique avant de déplacer les serveurs SMB ONTAP

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS du serveur SMB dans DNS lorsque vous déplacez le serveur SMB vers un autre domaine, vous devez modifier DNS dynamique (DDNS) sur la machine virtuelle de stockage (SVM) avant de déplacer le serveur SMB.

Avant de commencer

Les services de nom DNS doivent être modifiés sur le SVM afin d'utiliser le domaine DNS qui contient les enregistrements d'emplacement de service pour le nouveau domaine qui contiendra le compte ordinateur du serveur SMB. Si vous utilisez Secure DDNS, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory.

Description de la tâche

Bien que DDNS (si configuré sur la SVM) ajoute automatiquement les enregistrements DNS des LIFs de données au nouveau domaine, les enregistrements DNS du domaine d'origine ne sont pas automatiquement supprimés du serveur DNS d'origine. Vous devez les supprimer manuellement.

Pour effectuer les modifications DDNS avant de déplacer le serveur SMB, reportez-vous à la rubrique suivante :

"Configuration des services DNS dynamiques"

Rejoignez les SVM SMB ONTAP aux domaines Active Directory

Vous pouvez associer une machine virtuelle de stockage (SVM) à un domaine Active Directory sans supprimer le serveur SMB existant en modifiant le domaine à l'aide de `vserver cifs modify` commande. Vous pouvez rejoindre à nouveau le domaine actuel ou en rejoindre un nouveau.

Avant de commencer

- Le SVM doit déjà disposer d'une configuration DNS.
- La configuration DNS pour le SVM doit pouvoir représenter le domaine cible.

  Les serveurs DNS doivent contenir les enregistrements SRV (Service Location Records) pour les serveurs LDAP de domaine et de contrôleur de domaine.

Description de la tâche

- Le statut administratif du serveur CIFS doit être défini sur `down` pour continuer la modification du domaine Active Directory.
- Si la commande s'exécute correctement, l'état administratif est automatiquement défini sur `up`. Pour en savoir plus, `up` consultez le "Référence de commande ONTAP".
- Lorsque vous rejoignez un domaine, cette commande peut prendre plusieurs minutes.

Étapes

1. Relier le SVM au domaine du serveur CIFS : `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Pour en savoir plus, `vserver cifs modify` consultez le "Référence de commande ONTAP". Si vous devez reconfigurer le DNS pour le nouveau domaine, pour en savoir plus, `vserver dns modify` reportez-vous à la section "Référence de commande ONTAP".

   Pour créer un compte de machine Active Directory pour le serveur SMB, vous devez fournir le nom et le mot de passe d'un compte Windows disposant des privilèges suffisants pour ajouter des ordinateurs à l' `ou=` *`example`* `ou` conteneur dans le `*example*`domaine .com.

   À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous

recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

2. Vérifiez que le serveur CIFS se trouve dans le domaine Active Directory souhaité : `vserver cifs show`

Exemple

Dans l'exemple suivant, le serveur SMB « CIFSSERVER1 » sur le SVM vs1 rejoint le domaine example.com à l'aide de keytab Authentication :

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

Affiche des informations sur ONTAP SMB NetBIOS sur des connexions TCP

Vous pouvez afficher des informations sur les connexions NetBIOS sur TCP (NBT). Cela peut être utile lors du dépannage des problèmes liés au NetBIOS.

Étape

1. Utilisez le `vserver cifs nbtstat` Commande pour afficher les informations relatives à NetBIOS sur connexions TCP.

   Le service de noms NetBIOS (NNBNS) sur IPv6 n'est pas pris en charge.

Exemple

L'exemple suivant montre les informations relatives au service de nom NetBIOS affichées pour « cluster1 » :

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

Commandes ONTAP pour la gestion des serveurs SMB

Vous devez connaître les commandes pour créer, afficher, modifier, arrêter, démarrer, Et suppression des serveurs SMB. Il existe également des commandes permettant de réinitialiser et de redécouvrir les serveurs, de modifier ou de réinitialiser les mots de passe des comptes machine, de planifier des modifications pour les mots de passe des comptes machine et d'ajouter ou de supprimer des alias NetBIOS.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un serveur SMB	`vserver cifs create`
Affiche les informations relatives à un serveur SMB	`vserver cifs show`
Modifier un serveur SMB	`vserver cifs modify`

Déplacer un serveur SMB vers un autre domaine	`vserver cifs modify`
Arrêtez un serveur SMB	`vserver cifs stop`
Démarrez un serveur SMB	`vserver cifs start`
Supprimez un serveur SMB	`vserver cifs delete`
Réinitialisez et redécouvrez les serveurs pour le serveur SMB	`vserver cifs domain discovered-servers reset-servers`
Modifier le mot de passe du compte machine du serveur SMB	`vserver cifs domain password change`
Réinitialisez le mot de passe du compte machine du serveur SMB	`vserver cifs domain password change`
Planifier les modifications automatiques du mot de passe pour le compte machine du serveur SMB	`vserver cifs domain password schedule modify`
Ajoutez des alias NetBIOS pour le serveur SMB	`vserver cifs add-netbios-aliases`
Supprimez les alias NetBIOS du serveur SMB	`vserver cifs remove-netbios-aliases`

Pour en savoir plus, `vserver cifs` consultez le "Référence de commande ONTAP".

Informations associées

"Ce qui se passe pour les utilisateurs et les groupes locaux lors de la suppression des serveurs SMB"

Activez le service de nom NetBIOS SMB ONTAP

À partir de ONTAP 9, le service de noms NetBIOS (NBNS, parfois appelé Windows Internet Name Service ou WINS) est désactivé par défaut. Auparavant, les machines virtuelles de stockage compatibles CIFS (SVM) envoyaient des diffusions d'enregistrement de noms, même si WINS était activé sur un réseau. Pour limiter ces diffusions à des configurations où NBNS est nécessaire, vous devez activer explicitement NBNS pour les nouveaux serveurs CIFS.

Avant de commencer

- Si vous utilisez déjà NBNS et que vous effectuez une mise à niveau vers ONTAP 9, il n'est pas nécessaire d'effectuer cette tâche. NBNS continuera de fonctionner comme précédemment.
- NBNS est activé sur UDP (port 137).
- NBNS sur IPv6 n'est pas pris en charge.

Étapes

1. Définissez le niveau de privilège sur avancé.

```
set -privilege advanced
```

2. Activez NBNS sur un serveur CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Revenir au niveau de privilège admin.

```
set -privilege admin
```

Utilisez IPv6 pour l'accès SMB et les services SMB

En savoir plus sur la configuration SMB requise pour ONTAP pour IPv6

Avant de pouvoir utiliser IPv6 sur votre serveur SMB, vous devez connaître les versions de ONTAP et SMB qui la prennent en charge et les exigences de licence.

Conditions requises pour les licences ONTAP

Aucune licence spéciale n'est requise pour IPv6 lorsque SMB est sous licence. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Version requise du protocole SMB

- Pour les SVM, ONTAP prend en charge IPv6 sur toutes les versions du protocole SMB.

Le service de noms NetBIOS (NNBNS) sur IPv6 n'est pas pris en charge.

En savoir plus sur la prise en charge d'IPv6 avec accès SMB ONTAP et services CIFS

Si vous souhaitez utiliser IPv6 sur votre serveur CIFS, vous devez savoir comment ONTAP prend en charge IPv6 pour l'accès SMB et la communication réseau pour les services CIFS.

Prise en charge des serveurs et des clients Windows

ONTAP prend en charge les serveurs et clients Windows prenant en charge IPv6. La section suivante décrit la prise en charge du protocole IPv6 du serveur et du client Microsoft Windows :

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 et versions ultérieures prennent en charge IPv6 à la fois pour le partage de fichiers SMB et les services Active Directory, notamment les services DNS, LDAP, CLDAP et Kerberos.

Si les adresses IPv6 sont configurées, les versions Windows 7 et Windows Server 2008 et ultérieures utilisent IPv6 par défaut pour les services Active Directory. Les authentifications NTLM et Kerberos sur des connexions IPv6 sont prises en charge.

Tous les clients Windows pris en charge par ONTAP peuvent se connecter à des partages SMB à l'aide d'adresses IPv6.

Pour obtenir les informations les plus récentes sur les clients Windows pris en charge par ONTAP, reportez-vous au "Matrice d'interopérabilité".

Les domaines NT ne sont pas pris en charge pour IPv6.

Prise en charge supplémentaire de services CIFS

Outre la prise en charge IPv6 pour les partages de fichiers SMB et les services Active Directory, ONTAP prend en charge plusieurs protocoles :

- Services côté client, y compris les dossiers hors ligne, les profils itinérants, la redirection de dossiers et les versions précédentes
- Services côté serveur, y compris les répertoires locaux dynamiques (fonctionnalité Home Directory), les symlinks et les Widelinks, BranchCache, ODX, load des copies ODX, référencements automatiques des nœuds, Et versions précédentes
- Services de gestion de l'accès aux fichiers, y compris l'utilisation d'utilisateurs et de groupes Windows locaux pour le contrôle d'accès et la gestion des droits, la définition des autorisations de fichiers et des stratégies d'audit à l'aide de la CLI, le suivi de la sécurité, la gestion des verrous de fichiers et la surveillance de l'activité SMB
- Audit multiprotocole NAS
- FPolicy
- Partages disponibles en continu, protocole Witness et VSS distant (utilisés avec les configurations Hyper-V sur SMB)

Prise en charge du service d'authentification et du service de noms

La communication avec les services de noms suivants est prise en charge par IPv6 :

- Contrôleurs de domaine
- Serveurs DNS
- Serveurs LDAP
- Serveurs KDC
- Serveurs NIS

Découvrez comment les serveurs SMB ONTAP utilisent IPv6 pour se connecter à des serveurs externes

Pour créer une configuration qui répond à vos exigences, vous devez savoir comment les serveurs CIFS utilisent IPv6 lors de connexions à des serveurs externes.

- Sélection de l'adresse source

  Si une tentative de connexion à un serveur externe est effectuée, l'adresse source sélectionnée doit être

du même type que l'adresse de destination. Par exemple, si vous vous connectez à une adresse IPv6, la machine virtuelle de stockage (SVM) hébergeant le serveur CIFS doit disposer d'une LIF de données ou d'une LIF de gestion dont l'adresse IPv6 est à utiliser comme adresse source. De la même manière, en cas de connexion à une adresse IPv4, le SVM doit disposer d'une LIF de données ou d'une LIF de gestion qui possède une adresse IPv4 à utiliser comme adresse source.

- Pour les serveurs découverts dynamiquement à l'aide de DNS, la découverte de serveur s'effectue comme suit :
  - Si IPv6 est désactivé sur le cluster, seules les adresses des serveurs IPv4 sont découvertes.
  - Si IPv6 est activé sur le cluster, les adresses des serveurs IPv4 et IPv6 sont découvertes. L'un ou l'autre type peut être utilisé en fonction de l'adéquation du serveur auquel appartient l'adresse et de la disponibilité des LIF de gestion ou des données IPv6 ou IPv4.
    La découverte de serveurs dynamiques est utilisée pour découvrir les contrôleurs de domaine et leurs services associés, tels que LSA, NETLOGON, Kerberos et LDAP.
- Connectivité du serveur DNS

  Si le SVM utilise IPv6 lors de la connexion à un serveur DNS dépend de la configuration des services de noms DNS. Si les services DNS sont configurés pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration des services de noms DNS peut utiliser des adresses IPv4 afin que les connexions aux serveurs DNS continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration des services de noms DNS.

- Connectivité du serveur LDAP

  Si le SVM utilise IPv6 lors de la connexion à un serveur LDAP dépend de la configuration du client LDAP. Si le client LDAP est configuré pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration du client LDAP peut utiliser des adresses IPv4 pour que les connexions aux serveurs LDAP continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration du client LDAP.

  > La configuration du client LDAP est utilisée lors de la configuration de LDAP pour les services d'utilisateur, de groupe et de nom de groupe de réseau UNIX.

- Connectivité serveur NIS

  La question de savoir si le SVM utilise IPv6 lors de la connexion à un serveur NIS dépend de la configuration des services de nom NIS. Si les services NIS sont configurés pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration des services de noms NIS peut utiliser des adresses IPv4 pour que les connexions aux serveurs NIS continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration de services de noms NIS.

  > Les services de noms NIS sont utilisés pour stocker et gérer des objets de nom d'utilisateur, de groupe, de groupe et d'hôte UNIX.

Informations associées

- Activer IPv6 pour les serveurs
- Surveiller et afficher des informations sur les sessions IPv6

Activez IPv6 pour les serveurs SMB ONTAP

Les réseaux IPv6 ne sont pas activés lors de la configuration du cluster. Un administrateur de cluster doit activer IPv6 une fois l'installation du cluster terminée pour utiliser IPv6 pour SMB. Lorsque l'administrateur de cluster active IPv6, il est activé pour l'ensemble du cluster.

Étape

1. Activer IPv6 : `network options ipv6 modify -enabled true`

   IPv6 est activé. Les LIF de données IPv6 pour un accès SMB peuvent être configurées.

Informations associées

- Surveiller et afficher des informations sur les sessions IPv6
- "Visualiser le réseau à l'aide de System Manager"
- "Activation d'IPv6 sur le cluster"
- "options réseau ipv6 modifier"

Découvrez comment désactiver IPv6 pour les serveurs SMB ONTAP

Bien que IPv6 soit activé sur le cluster à l'aide d'une option réseau, vous ne pouvez pas désactiver IPv6 pour SMB en utilisant la même commande. En revanche, ONTAP désactive IPv6 lorsque l'administrateur de cluster désactive la dernière interface compatible IPv6 sur le cluster. Vous devez communiquer avec l'administrateur du cluster pour obtenir des informations sur la gestion de vos interfaces compatibles IPv6.

Informations associées

- "Visualiser le réseau ONTAP à l'aide de System Manager"

Surveiller et afficher des informations sur les sessions SMB IPv6 ONTAP

Vous pouvez contrôler et afficher des informations relatives aux sessions SMB connectées via les réseaux IPv6. Ces informations sont utiles pour déterminer quels clients se connectent à l'aide d'IPv6 ainsi que d'autres informations utiles sur les sessions SMB IPv6.

Étape

1. Effectuez l'action souhaitée :

Si vous voulez déterminer si…	Entrez la commande…
Les sessions SMB vers une machine virtuelle de stockage (SVM) sont connectées via IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`

Si vous voulez déterminer si…	Entrez la commande…
IPv6 est utilisé pour les sessions SMB via une adresse LIF spécifiée	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` *`LIF_IP_address`* Est l'adresse IPv6 de la LIF de données.

Configurez l'accès aux fichiers à l'aide de SMB

Configurer les styles de sécurité

Comment les styles de sécurité affectent l'accès aux données

Découvrez les styles de sécurité ONTAP pour PME et leurs effets

Il existe quatre styles de sécurité différents : UNIX, NTFS, mixte et unifié. Chaque style de sécurité a un effet différent sur la façon dont les autorisations sont traitées pour les données. Vous devez comprendre les différents effets pour vous assurer que vous sélectionnez le style de sécurité approprié à vos fins.

Il est important de comprendre que les styles de sécurité ne déterminent pas quels types de clients peuvent ou ne peuvent pas accéder aux données. Les styles de sécurité déterminent uniquement le type d'autorisations que ONTAP utilise pour contrôler l'accès aux données et le type de client pouvant modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu'ils s'authentifient et autorisent correctement) en raison de la nature multiprotocole de ONTAP. Toutefois, ONTAP utilise des autorisations UNIX que seuls les clients UNIX peuvent modifier à l'aide d'outils natifs.

Style de sécurité	Clients pouvant modifier des autorisations	Autorisations que les clients peuvent utiliser	Un style de sécurité efficace	Clients pouvant accéder aux fichiers
UNIX	NFS	Bits de mode NFSv3	UNIX	NFS et SMB
		Listes de contrôle d'accès NFSv4.x		
NTFS	PME	ALC NTFS	NTFS	
Mixte	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL.NFSv4		
		ALC NTFS	NTFS	
Unifiée (Pour Infinite volumes uniquement, dans ONTAP 9.4 et les versions antérieures.)	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL NFSv4.1		
		ALC NTFS	NTFS	

Les volumes FlexVol prennent en charge les styles de sécurité UNIX, NTFS et mixte. Lorsque le style de sécurité est mixte ou unifié, les autorisations effectives dépendent du type de client qui a modifié les autorisations pour la dernière fois, car les utilisateurs définissent le style de sécurité sur une base individuelle. Si le dernier client ayant modifié des autorisations était un client NFSv3, les autorisations sont des bits en mode UNIX NFSv3. Si le dernier client était un client NFSv4, les autorisations sont définies comme listes de contrôle d'accès NFSv4. Si le dernier client était un client SMB, les autorisations sont des listes de contrôle d'accès Windows NTFS.

La méthode de sécurité unifiée est uniquement disponible avec des volumes infinis, qui ne sont plus pris en charge dans ONTAP 9.5 et versions ultérieures. Pour plus d'informations, voir Présentation de la gestion des volumes FlexGroup.

Le `show-effective-permissions` paramètre avec le `vserver security file-directory` La commande vous permet d'afficher les autorisations effectives accordées à un utilisateur Windows ou UNIX sur le chemin de fichier ou de dossier spécifié. En outre, le paramètre facultatif `-share-name` vous permet d'afficher l'autorisation de partage effectif. Pour en savoir plus, `vserver security file-directory show-effective-permissions` consultez le "Référence de commande ONTAP".

> ONTAP définit au départ certaines autorisations de fichier par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité UNIX, mixte et unifié est UNIX et le type d'autorisation effectif est bits de mode UNIX (0755 sauf indication contraire) jusqu'à ce qu'un client soit configuré comme autorisé par le style de sécurité par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité NTFS est NTFS et dispose d'une liste de contrôle d'accès permettant un contrôle total à tous.

Informations associées

- "Référence de commande ONTAP"

Découvrez où et quand définir les styles de sécurité ONTAP SMB

Les styles de sécurité peuvent être définis sur les volumes FlexVol (volumes root ou de données) et les qtrees. Les styles de sécurité peuvent être définis manuellement au moment de la création, hérités automatiquement ou modifiés ultérieurement.

Choix des styles de sécurité SMB à utiliser sur les SVM ONTAP

Pour vous aider à choisir le style de sécurité à utiliser sur un volume, vous devez tenir compte de deux facteurs. Le facteur principal est le type d'administrateur qui gère le système de fichiers. Le facteur secondaire désigne le type d'utilisateur ou de service qui accède aux données du volume.

Lorsque vous configurez le style de sécurité sur un volume, vous devez tenir compte des besoins de votre environnement pour vous assurer que vous sélectionnez le meilleur style de sécurité et éviter les problèmes liés à la gestion des autorisations. Vous pouvez décider des considérations suivantes :

Style de sécurité	Choisissez si…
UNIX	• Le système de fichiers est géré par un administrateur UNIX. • La plupart des utilisateurs sont des clients NFS. • Une application accédant aux données utilise un utilisateur UNIX comme compte de service.
NTFS	• Le système de fichiers est géré par un administrateur Windows. • La majorité des utilisateurs sont des clients SMB. • Une application accédant aux données utilise un utilisateur Windows comme compte de service.
Mixte	Le système de fichiers est géré à la fois par les administrateurs et utilisateurs d'UNIX et de Windows, et il se compose de clients NFS et SMB.

En savoir plus sur l'héritage de style de sécurité SMB de ONTAP

Si vous ne spécifiez pas le style de sécurité lors de la création d'un nouveau volume FlexVol ou d'un qtree, il hérite de son style de sécurité de différentes manières.

Les styles de sécurité sont hérités de la manière suivante :

- Un volume FlexVol hérite du style de sécurité du volume root de son SVM contenant.
- Un qtree hérite du style de sécurité de son volume FlexVol.
- Un fichier ou un répertoire hérite du style de sécurité de son volume FlexVol ou qtree.

Découvrez comment conserver les autorisations UNIX pour les volumes ONTAP SMB FlexVol

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

Découvrez comment gérer les autorisations UNIX à l'aide de l'onglet sécurité Windows pour les serveurs SMB ONTAP

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtrees de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- Modification des autorisations UNIX

  Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

  Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- Modification des autorisations UNIX en autorisations NTFS

  Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

  Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

  Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

Configurer les styles de sécurité SMB sur les volumes root du SVM ONTAP

Il configure la style de sécurité du volume root de la machine virtuelle de stockage (SVM) afin de déterminer le type d'autorisations utilisées pour les données sur le volume root de la SVM.

Étapes

1. Utilisez le `vserver create` commande avec `-rootvolume-security-style` paramètre pour définir le style de sécurité.

   Les options possibles pour le style de sécurité du volume racine sont `unix`, `ntfs`, ou `mixed`.

2. Afficher et vérifier la configuration, y compris le style de sécurité du volume root du SVM que vous avez créé : `vserver show -vserver vserver_name`

Configurez les styles de sécurité SMB sur les volumes ONTAP FlexVol

Configurez le style de sécurité des volumes FlexVol afin de déterminer le type d'autorisations utilisées pour les données sur des volumes FlexVol de la machine virtuelle de stockage (SVM).

Étapes

1. Effectuez l'une des opérations suivantes :

Si le volume FlexVol…	Utilisez la commande…
N'existe pas encore	`volume create` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.
Existe déjà	`volume modify` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.

   Les options possibles pour le style de sécurité du volume FlexVol sont `unix`, `ntfs`, ou `mixed`.

   Si vous ne spécifiez pas de style de sécurité lors de la création d'un volume FlexVol, le volume hérite du style de sécurité du volume racine.

   Pour plus d'informations sur le `volume create` ou `volume modify` commandes, voir "Gestion du stockage logique".

2. Pour afficher la configuration, en incluant le style de sécurité du volume FlexVol que vous avez créé, entrez la commande suivante :

   ```
   volume show -volume volume_name -instance
   ```

Configurez les styles de sécurité SMB sur les qtrees ONTAP

Vous configurez le style de sécurité du volume qtree afin de déterminer le type d'autorisations utilisées pour les données sur des qtrees.

Étapes

1. Effectuez l'une des opérations suivantes :

Si le qtree…	Utilisez la commande…
N'existe pas encore	`volume qtree create` et inclure le `-security -style` paramètre pour spécifier le style de sécurité.
Existe déjà	`volume qtree modify` et inclure le `-security -style` paramètre pour spécifier le style de sécurité.

   Les options possibles pour la méthode de sécurité qtree sont `unix`, `ntfs`, ou `mixed`.

   Si vous ne spécifiez pas de style de sécurité lors de la création d'un qtree, le style de sécurité par défaut est `mixed`.

   Pour plus d'informations sur le `volume qtree create` ou `volume qtree modify` commandes, voir "Gestion du stockage logique".

2. Pour afficher la configuration, y compris le style de sécurité du qtree que vous avez créé, entrez la commande suivante : `volume qtree show -qtree qtree_name -instance`

Création et gestion des volumes de données dans les espaces de noms NAS

Découvrez comment créer et gérer des volumes de données SMB ONTAP dans les espaces de noms NAS

Pour gérer l'accès aux fichiers dans un environnement NAS, vous devez gérer les volumes et les points de jonction des données sur votre SVM (Storage Virtual machine). Cela inclut la planification de votre architecture d'espace de noms, la création de volumes avec ou sans points de jonction, le montage ou le démontage de volumes, et l'affichage des informations sur les volumes de données et les serveurs NFS ou les espaces de noms de serveurs CIFS.

Créez des volumes de données SMB ONTAP avec des points de jonction spécifiés

Vous pouvez spécifier le point de jonction lorsque vous créez un volume de données. Le volume ainsi obtenu est automatiquement monté au point de jonction et est immédiatement disponible pour la configuration pour l'accès NAS.

Avant de commencer

L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.

> Les caractères suivants ne peuvent pas être utilisés dans le chemin de jonction : * # " > < | ? \
>
> De plus, la longueur du chemin de jonction ne peut pas dépasser 255 caractères.

Étapes

1. Créer le volume avec un point de jonction : `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]}`

`-security-style {ntfs|unix|mixed} -junction-path junction_path`

Le chemin de jonction doit commencer par la racine (/) et peut contenir à la fois des répertoires et des volumes reliés. Il n'est pas nécessaire que la Junction path contienne le nom du volume. Les Junction paths sont indépendants du nom du volume.

La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Cependant, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données que vous créez. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

Le chemin de jonction n'est pas sensible à la casse ; `/ENG` est identique à `/eng`. Si vous créez un partage CIFS, Windows traite le chemin de jonction comme s'il est sensible à la casse. Par exemple, si la jonction est de `/ENG`, Le chemin d'un partage CIFS doit commencer par `/ENG`pas `/eng`.

De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

2. Vérifier que le volume a été créé avec le point de jonction souhaité : `volume show -vserver vserver_name -volume volume_name -junction`

Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Créez des volumes de données SMB ONTAP sans spécifier de points de jonction

Vous pouvez créer un volume de données sans spécifier de point de jonction. Le volume résultant n'est pas monté automatiquement et n'est pas disponible pour configurer l'accès NAS. Vous devez monter le volume avant de configurer les partages SMB ou les exportations NFS pour ce volume.

Avant de commencer

L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.

Étapes

1. Créer le volume sans point de jonction en utilisant la commande suivante : `volume create -vserver`

vserver_name -volume *volume_name* -aggregate *aggregate_name* -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}

La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Toutefois, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

2. Vérifier que le volume a été créé sans point de jonction : `volume show -vserver` *vserver_name* `-volume` *volume_name* `-junction`

Exemple

L'exemple suivant crée un volume nommé « sales » situé sur la SVM vs1 qui n'est pas monté à un point de jonction :

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Montez ou démontez des volumes SMB ONTAP existants dans l'espace de noms NAS

Un volume doit être monté sur le namespace NAS avant de pouvoir configurer l'accès des clients NAS aux données contenues dans les volumes SVM (Storage Virtual machine). Vous pouvez monter un volume sur un point de jonction s'il n'est pas actuellement monté. Vous pouvez également démonter des volumes.

Description de la tâche

Si vous démontez et mettez un volume hors ligne, toutes les données du point de jonction, y compris les données des volumes dont les points de jonction se trouvent dans l'espace de noms du volume non monté, sont inaccessibles aux clients NAS.

Pour interrompre l'accès client NAS à un volume, il ne suffit pas de démonter le volume. Vous devez mettre le volume hors ligne ou prendre d'autres mesures pour vous assurer que les caches de descripteur de fichier côté client sont invalidés. Pour plus d'informations, consultez l'article suivant de la base de connaissances : "Les clients NFSv3 ont toujours accès à un volume après avoir été supprimés du namespace dans ONTAP"

Lorsque vous démontez et mettez un volume hors ligne, les données du volume ne sont pas perdues. En outre, les règles d'exportation de volume et les partages SMB créés sur le volume ou sur des répertoires et des points de jonction au sein du volume démonté sont conservés. Si vous remontez le volume démonté, les clients NAS peuvent accéder aux données contenues dans le volume à l'aide des règles d'exportation et des partages SMB existants.

Étapes

1. Effectuez l'action souhaitée :

Les fonctions que vous recherchez…	Entrez les commandes…
Montez un volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Démonter un volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Vérifiez que le volume est dans l'état de montage souhaité :

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Exemples

L'exemple suivant monte un volume nommé « ventes » situé sur la SVM « vs1 » au point de jonction « /ventes » :

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

L'exemple suivant démonte et met hors ligne un volume nommé « `data' situé sur le SVM « vs1` » :

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Affiche les informations sur le point de jonction et le montage du volume SMB ONTAP

Vous pouvez afficher des informations sur les volumes montés pour les SVM et les points de jonction auxquels les volumes sont montés. Vous pouvez également déterminer quels volumes ne sont pas montés sur un point de jonction. Vous pouvez utiliser ces informations pour comprendre et gérer votre namespace SVM.

Étapes

1. Effectuez l'action souhaitée :

Si vous voulez afficher…	Entrez la commande…
Récapitulatif des informations sur les volumes montés et démontés sur le SVM	`volume show -vserver vserver_name -junction`
Informations détaillées sur les volumes montés et démontés sur le SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Informations spécifiques sur les volumes montés et démontés sur le SVM	a. Si nécessaire, vous pouvez afficher des champs valides pour l' `-fields` paramètre via la commande suivante : `volume show -fields ?` b. Afficher les informations souhaitées à l'aide de l' `-fields` paramètre : volume show -vserver_name -champs fieldname,…

Exemples

L'exemple suivant affiche un récapitulatif des volumes montés et démontés sur le SVM vs1 :

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

L'exemple suivant affiche des informations sur les champs spécifiés pour les volumes situés sur le SVM vs2 :

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurez les mappages de noms

En savoir plus sur la configuration des mappages de noms SMB de ONTAP

ONTAP fait appel au mappage de noms pour mapper les identités CIFS aux identités UNIX, les identités Kerberos aux identités UNIX et les identités UNIX aux identités CIFS. Il a besoin de ces informations pour obtenir les informations d'identification des utilisateurs et fournir un accès approprié aux fichiers, qu'ils se connectent à partir d'un client NFS ou d'un client CIFS.

Il existe deux exceptions lorsque vous n'avez pas besoin d'utiliser le mappage de noms :

- Vous configurez un environnement UNIX pur et ne prévoyez pas d'utiliser l'accès CIFS ou le style de sécurité NTFS sur les volumes.
- Vous configurez l'utilisateur par défaut à utiliser à la place.

  Dans ce scénario, le mappage de noms n'est pas nécessaire car au lieu de mapper chaque identifiant client individuel, toutes les informations d'identification client sont mappées au même utilisateur par défaut.

Notez que vous pouvez utiliser le mappage de noms uniquement pour les utilisateurs, pas pour les groupes.

Toutefois, vous pouvez mapper un groupe d'utilisateurs individuels à un utilisateur spécifique. Par exemple, vous pouvez mapper tous les utilisateurs AD qui commencent ou se terminent par le mot VENTES à un utilisateur UNIX spécifique et à l'UID de l'utilisateur.

En savoir plus sur le mappage de noms SMB de ONTAP

Lorsque ONTAP doit mapper les informations d'identification d'un utilisateur, il recherche tout d'abord un mappage existant dans la base de données de mappage de noms locaux et le serveur LDAP. Qu'elle vérifie un ou les deux et dans quel ordre est déterminé par la configuration du service de nom du SVM.

- Pour le mappage Windows à UNIX

  Si aucun mappage n'est trouvé, ONTAP vérifie si le nom d'utilisateur Windows minuscule est un nom d'utilisateur valide dans le domaine UNIX. Si cela ne fonctionne pas, il utilise l'utilisateur UNIX par défaut à condition qu'il soit configuré. Si l'utilisateur UNIX par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

- Pour le mappage d'UNIX à Windows

  Si aucun mappage n'est trouvé, ONTAP tente de trouver un compte Windows correspondant au nom UNIX dans le domaine SMB. Si cela ne fonctionne pas, il utilise l'utilisateur SMB par défaut, à condition qu'il soit configuré. Si l'utilisateur CIFS par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

Par défaut, les comptes machine sont mappés à l'utilisateur UNIX par défaut spécifié. Si aucun utilisateur UNIX par défaut n'est spécifié, les mappages de compte machine échouent.

- À partir de ONTAP 9.5, vous pouvez mapper des comptes machine à des utilisateurs autres que l'utilisateur UNIX par défaut.
- Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas mapper les comptes machine à d'autres utilisateurs.

  Même si des mappages de noms pour des comptes machine sont définis, les mappages sont ignorés.

En savoir plus sur les recherches multidomaines SMB de ONTAP pour les mappages de noms d'utilisateur UNIX vers Windows

ONTAP prend en charge les recherches multidomaine lors du mappage d'utilisateurs UNIX aux utilisateurs Windows. Tous les domaines de confiance découverts sont recherchés pour trouver des correspondances avec le modèle de remplacement jusqu'à

ce qu'un résultat correspondant soit renvoyé. Vous pouvez également configurer une liste de domaines de confiance préférés, qui est utilisée à la place de la liste de domaines de confiance découverts et est recherchée dans l'ordre jusqu'à ce qu'un résultat correspondant soit renvoyé.

La manière dont les approbations de domaine affectent les recherches de mappage de noms d'utilisateur UNIX à des noms d'utilisateur Windows

Pour comprendre le fonctionnement du mappage de noms d'utilisateur multidomaine, vous devez comprendre comment les approbations de domaine fonctionnent avec ONTAP. Les relations de confiance Active Directory avec le domaine personnel du serveur CIFS peuvent être une confiance bidirectionnelle ou l'un des deux types de fiducies unidirectionnelles, soit une confiance entrante, soit une confiance sortante. Le home domain est le domaine auquel le serveur CIFS du SVM appartient.

- *Confiance bidirectionnelle*

  Avec des approbations bidirectionnelles, les deux domaines se font confiance. Si le domaine de base du serveur CIFS possède une confiance bidirectionnelle avec un autre domaine, le domaine de base peut authentifier et autoriser un utilisateur appartenant au domaine de confiance et vice versa.

  Les recherches de mappage de noms d'utilisateur UNIX à Windows peuvent être effectuées uniquement sur les domaines avec des approbations bidirectionnelles entre le domaine principal et l'autre domaine.

- *Confiance sortante*

  Avec une confiance sortante, le domaine d'origine approuve l'autre domaine. Dans ce cas, le domaine home peut authentifier et autoriser un utilisateur appartenant au domaine de confiance sortant.

  Un domaine avec une confiance sortante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

- *Confiance entrante*

  Avec une confiance entrante, l'autre domaine approuve le domaine personnel du serveur CIFS. Dans ce cas, le domaine personnel ne peut pas authentifier ni autoriser un utilisateur appartenant au domaine de confiance entrant.

  Un domaine avec une confiance entrante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

Comment les caractères génériques (*) sont utilisés pour configurer les recherches multidomaines pour le mappage de noms

Les recherches de mappage de noms de domaines multiples sont facilitées par l'utilisation de caractères génériques dans la section domaine du nom d'utilisateur Windows. Le tableau suivant illustre comment utiliser des caractères génériques dans la partie domaine d'une entrée de mappage de nom pour activer les recherches multidomaine :

Motif	Remplacement	Résultat
racine	*\\administrateur	L'utilisateur UNIX « root » est mappé à l'utilisateur nommé « administrateur ». Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant nommé « administrateur » soit trouvé.
*	**	Les utilisateurs UNIX valides sont mappés aux utilisateurs Windows correspondants. Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant à ce nom soit trouvé. Le schéma ** n'est valide que pour le mappage de noms d'UNIX à Windows, pas l'inverse.

Mode d'exécution des recherches sur plusieurs noms de domaine

Vous pouvez choisir l'une des deux méthodes pour déterminer la liste des domaines approuvés utilisés pour les recherches de noms multidomaines :

- Utilisez la liste d'approbation bidirectionnelle automatiquement découverte compilée par ONTAP
- Utilisez la liste de domaines approuvés que vous compilez

Si un utilisateur UNIX est mappé à un utilisateur Windows avec un caractère générique utilisé pour la section domaine du nom d'utilisateur, l'utilisateur Windows est recherché dans tous les domaines approuvés comme suit :

- Si une liste de domaines de confiance est configurée, l'utilisateur Windows mappé est uniquement recherché dans cette liste de recherche, dans l'ordre.
- Si une liste préférée de domaines approuvés n'est pas configurée, l'utilisateur Windows est alors recherché dans tous les domaines de confiance bidirectionnels du domaine de départ.
- S'il n'existe pas de domaines de confiance bidirectionnellement pour le domaine personnel, l'utilisateur est recherché dans le domaine personnel.

Si un utilisateur UNIX est mappé à un utilisateur Windows sans section de domaine dans le nom d'utilisateur, l'utilisateur Windows est recherché dans le domaine personnel.

En savoir plus sur les règles de conversion de mappage de noms SMB ONTAP

Un système ONTAP conserve un ensemble de règles de conversion pour chaque SVM. Chaque règle se compose de deux éléments : un *pattern* et un *remplacement*. Les

conversions commencent au début de la liste appropriée et effectuent une substitution basée sur la première règle correspondante. Le motif est une expression régulière de style UNIX. Le remplacement est une chaîne contenant des séquences d'échappement représentant des sous-expressions du motif, comme dans UNIX `sed` programme.

Création du mappage de noms SMB ONTAP

Vous pouvez utiliser le `vserver name-mapping create` commande permettant de créer un mappage de noms. Vous utilisez les mappages de noms pour permettre aux utilisateurs Windows d'accéder aux volumes du style de sécurité UNIX et les inverser.

Description de la tâche

Par SVM, ONTAP prend en charge jusqu'à 12,500 mappages de noms dans chaque direction.

Étape

1. Créer un mappage de noms : `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > Les `-pattern` instructions et `-replacement` peuvent être formulées en tant qu'expressions régulières. Vous pouvez également utiliser l' `-replacement`instruction pour refuser explicitement un mappage à l'utilisateur en utilisant la chaîne de remplacement NULL `" "` (caractère d'espace). Pour en savoir plus, `vserver name-mapping create` consultez le "Référence de commande ONTAP".

   Lorsque des mappages entre Windows et UNIX sont créés, tous les clients SMB disposant de connexions ouvertes au système ONTAP au moment de la création des nouveaux mappages doivent se déconnecter et se reconnecter pour voir les nouveaux mappages.

Exemples

La commande suivante crée un nom de mappage sur le SVM nommé vs1. Le mappage est un mappage d'UNIX à Windows à la position 1 dans la liste des priorités. Le mappage mappe l'utilisateur UNIX johnd à l'utilisateur Windows ENG\johndoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Le mappage est un mappage de Windows à UNIX à la position 1 dans la liste des priorités. Dans ce cas, le motif et le remplacement incluent des expressions régulières. Le mapping mappe chaque utilisateur CIFS du domaine ENG aux utilisateurs du domaine LDAP associé avec la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Ici, le schéma inclut "`$"" comme élément du nom d'utilisateur Windows qui doit être échappé. Le mappage mappe l'utilisateur Windows ENG\ john$OPS à l'utilisateur UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configurez l'utilisateur SMB ONTAP par défaut

Vous pouvez configurer un utilisateur par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l'authentification des utilisateurs non mappés échoue, vous ne devez pas configurer un utilisateur par défaut.

Description de la tâche

Pour l'authentification CIFS, si vous ne souhaitez pas mapper chaque utilisateur Windows à un utilisateur UNIX individuel, vous pouvez spécifier un utilisateur UNIX par défaut.

Pour l'authentification NFS, si vous ne souhaitez pas mapper chaque utilisateur UNIX à un utilisateur Windows individuel, vous pouvez spécifier un utilisateur Windows par défaut.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Configurez l'utilisateur UNIX par défaut	`vserver cifs options modify -default -unix-user` *user_name*
Configurez l'utilisateur Windows par défaut	`vserver nfs modify -default-win-user` *user_name*

Commandes ONTAP pour la gestion des mappages de noms SMB

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un mappage de nom	`vserver name-mapping create`
Insérez un mappage de nom à une position spécifique	`vserver name-mapping insert`

Afficher les mappages de noms	`vserver name-mapping show`
Échange de la position de deux mappages de noms REMARQUE : un échange n'est pas autorisé lorsque le mappage-noms est configuré avec une entrée de qualificatif-ip.	`vserver name-mapping swap`
Modifier un mappage de noms	`vserver name-mapping modify`
Supprime un mappage de noms	`vserver name-mapping delete`
Valider le mappage de nom correct	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Pour en savoir plus, `vserver name-mapping` consultez le "Référence de commande ONTAP".

Configurez les recherches de mappage de noms-domaines multiples

Activez ou désactivez les recherches de mappage de noms multidomaines SMB ONTAP

Avec les recherches de mappage de noms multidomaine, vous pouvez utiliser un caractère générique (*) dans la partie domaine d'un nom Windows lors de la configuration du mappage de noms d'utilisateurs UNIX vers Windows. L'utilisation d'un caractère générique (*) dans la partie domaine du nom permet à ONTAP de rechercher tous les domaines ayant une confiance bidirectionnelle avec le domaine qui contient le compte ordinateur du serveur CIFS.

Description de la tâche

Comme alternative à la recherche de tous les domaines de confiance bidirectionnels, vous pouvez configurer une liste de domaines de confiance préférés. Lorsqu'une liste de domaines de confiance privilégiés est configurée, ONTAP utilise la liste de domaines de confiance préférée au lieu des domaines de confiance bidirectionnels découverts pour effectuer des recherches de mappage de noms multiples domaines.

- Les recherches de mappage de noms de domaines multiples sont activées par défaut.
- Cette option est disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Pour effectuer des recherches sur le mappage de noms de domaines multiples…	Entrez la commande…
Activé	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
Désactivé	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

Options de serveur disponibles

Réinitialisez et redécouvrez les domaines SMB ONTAP approuvés

Vous pouvez forcer la redécouverte de tous les domaines de confiance. Ceci peut être utile lorsque les serveurs de domaine approuvés ne répondent pas correctement ou que les relations de confiance ont changé. Seuls les domaines avec une confiance bidirectionnelle avec le domaine de base, qui est le domaine contenant le compte ordinateur du serveur CIFS, sont découverts.

Étape

1. Réinitialisez et redécouvrez des domaines de confiance à l'aide de `vserver cifs domain trusts rediscover` commande.

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

Informations associées

Affiche des informations sur les domaines de confiance découverts

Affiche des informations sur les domaines SMB ONTAP fiables découverts

Vous pouvez afficher des informations sur les domaines approuvés découverts pour le domaine personnel du serveur CIFS, qui est le domaine contenant le compte d'ordinateur du serveur CIFS. Cela peut être utile lorsque vous voulez savoir quels domaines de confiance sont découverts et comment ils sont ordonnés dans la liste domaine de confiance découvert.

Description de la tâche

Seuls les domaines avec des approbations bidirectionnelles avec le domaine de départ sont découverts. Étant donné que le contrôleur de domaine (DC) du domaine d'origine renvoie la liste des domaines de confiance dans un ordre déterminé par le DC, l'ordre des domaines dans la liste ne peut pas être prédit. En affichant la liste des domaines de confiance, vous pouvez déterminer l'ordre de recherche des recherches de mappage de noms de domaines multiples.

Les informations des domaines de confiance affichés sont regroupées par nœud et par SVM (Storage Virtual

machine).

Étape

1. Affiche des informations sur les domaines de confiance découverts à l'aide du `vserver cifs domain trusts show` commande.

```
vserver cifs domain trusts show -vserver vs1
```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

Informations associées

Réinitialiser et redécouvrir des domaines de confiance

Ajoutez, supprimez ou remplacez les domaines SMB ONTAP approuvés dans les listes préférées

Vous pouvez ajouter ou supprimer des domaines approuvés de la liste des domaines approuvés préférés pour le serveur SMB ou modifier la liste actuelle. Si vous configurez une liste de domaines de confiance privilégiés, cette liste est utilisée à la place des domaines de confiance bidirectionnels découverts lors de l'exécution de recherches sur le mappage de noms multidomaines.

Description de la tâche

- Si vous ajoutez des domaines approuvés à une liste existante, la nouvelle liste est fusionnée avec la liste existante et les nouvelles entrées sont placées à la fin Les domaines de confiance sont recherchés dans l'ordre dans lequel ils apparaissent dans la liste des domaines de confiance.
- Si vous supprimez des domaines de confiance de la liste existante et ne spécifiez pas de liste, la liste de domaines de confiance complète pour la machine virtuelle de stockage (SVM) spécifiée est supprimée.
- Si vous modifiez la liste existante des domaines approuvés, la nouvelle liste remplace la liste existante.

Vous devez entrer uniquement les domaines de confiance bidirectionnels dans la liste des domaines de confiance préférés. Même si vous pouvez entrer des domaines de confiance sortants ou entrants dans la liste de domaines préférés, ils ne sont pas utilisés lors de recherches de mappage de noms de domaines multiples. ONTAP ignore l'entrée du domaine unidirectionnel et passe au domaine de confiance bidirectionnel suivant dans la liste.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez effectuer les opérations suivantes avec la liste des domaines de confiance préférés…	Utilisez la commande…
Ajouter des domaines de confiance à la liste	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Supprimer des domaines de confiance de la liste	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modifier la liste existante	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Exemples

La commande suivante ajoute deux domaines de confiance (cifs1.example.com et cifs2.example.com) à la liste de domaines de confiance privilégiée utilisée par le SVM vs1 :

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

La commande suivante supprime deux domaines de confiance de la liste utilisée par le SVM vs1 :

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

La commande suivante modifie la liste de domaines approuvés utilisée par le SVM vs1. La nouvelle liste remplace la liste d'origine :

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Informations associées

Affiche des informations sur la liste de domaines de confiance préférée

Affiche des informations sur la liste de domaines SMB ONTAP de confiance préférée

Vous pouvez afficher des informations sur les domaines de confiance dans la liste des domaines de confiance préférés et l'ordre dans lequel ils sont recherchés si les recherches de mappage de noms de domaines multiples sont activées. Vous pouvez configurer une liste de domaines de confiance préférée comme alternative à l'utilisation de la liste de domaines de confiance automatiquement découverts.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur les éléments suivants…	Utilisez la commande…
Tous les domaines de confiance privilégiés dans le cluster regroupés par SVM (Storage Virtual machine)	`vserver cifs domain name-mapping-search show`
Tous les domaines fiables préférés pour un SVM spécifié	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

La commande suivante affiche des informations sur tous les domaines de confiance privilégiés sur le cluster :

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Informations associées

Ajouter, supprimer ou remplacer des domaines de confiance dans les listes préférées

Créez et configurez des partages SMB

En savoir plus sur la création et la configuration de partages SMB ONTAP

Avant que les utilisateurs et les applications n'accèdent aux données sur le serveur CIFS via SMB, vous devez créer et configurer des partages SMB, qui est un point d'accès nommé dans un volume. Vous pouvez personnaliser les partages en spécifiant des paramètres de partage et des propriétés de partage. Vous pouvez modifier un partage existant à tout moment.

Lorsque vous créez un partage SMB, ONTAP crée une liste de contrôle d'accès par défaut pour le partage avec les autorisations de contrôle total pour tous.

Les partages SMB sont liés au serveur CIFS sur la machine virtuelle de stockage (SVM). Les partages SMB sont supprimés si le SVM est supprimé ou si le serveur CIFS auquel il est associé est supprimé de la SVM. Si vous recréez le serveur CIFS sur le SVM, vous devez recréer les partages SMB.

Informations associées

- En savoir plus sur les utilisateurs et les groupes locaux
- "Configuration SMB pour Microsoft Hyper-V et SQL Server"
- Configurer le mappage de caractères pour la traduction des noms de fichiers sur les volumes

En savoir plus sur les partages SMB d'administration par défaut de ONTAP

Lorsque vous créez un serveur CIFS sur votre SVM (Storage Virtual machine), les partages administratifs par défaut sont automatiquement créés. Vous devez comprendre ce que sont ces partages par défaut et comment ils sont utilisés.

Lors de la création du serveur CIFS, ONTAP crée les partages administratifs par défaut suivants :

> Depuis ONTAP 9.8, le partage admin$ n'est plus créé par défaut.

- ipc$
- admin$ (ONTAP 9.7 et versions antérieures uniquement)
- c$

Les partages qui se terminent par le caractère $ étant des partages masqués, les partages administratifs par défaut ne sont pas visibles depuis mon ordinateur, mais vous pouvez les afficher à l'aide de dossiers partagés.

Utilisation des partages IPC$ et admin$ par défaut

Les partages ipc$ et admin$ sont utilisés par ONTAP et ne peuvent pas être utilisés par les administrateurs Windows pour accéder aux données résidant sur la SVM.

- part ipc$

  La part ipc$ est une ressource qui partage les canaux nommés qui sont essentiels à la communication entre les programmes. Le partage ipc$ est utilisé lors de l'administration à distance d'un ordinateur et lors de l'affichage des ressources partagées d'un ordinateur. Vous ne pouvez pas modifier les paramètres de partage, les propriétés de partage ou les listes de contrôle d'accès du partage ipc$. Vous ne pouvez pas non plus renommer ou supprimer le partage ipc$.

- Partage admin$ (ONTAP 9.7 et versions antérieures uniquement)

  > Depuis ONTAP 9.8, le partage admin$ n'est plus créé par défaut.

  Le partage admin$ est utilisé pendant l'administration à distance du SVM. Le chemin de cette ressource est toujours le chemin vers la racine SVM. Vous ne pouvez pas modifier les paramètres de partage, les propriétés de partage ou les listes de contrôle d'accès pour le partage admin$. Vous ne pouvez pas non plus renommer ou supprimer le partage admin$.

Utilisation du partage par défaut c$

Le partage c$ est un partage administratif que l'administrateur du cluster ou du SVM peut utiliser pour accéder au volume root du SVM et le gérer.

Voici les caractéristiques de la part c$:

- Le chemin pour ce partage est toujours le chemin vers le volume root du SVM et ne peut pas être modifié.
- La liste de contrôle d'accès par défaut pour le partage c$ est Administrator / Full Control.

  Cet utilisateur est le BULILTIN\Administrator. Par défaut, BUILTIN\Administrator peut mapper sur le partage et l'affichage, créer, modifier ou supprimer des fichiers et dossiers dans le répertoire racine mappé. Soyez prudent lorsque vous gérez des fichiers et des dossiers dans ce répertoire.

- Vous pouvez modifier l'ACL du partage c$.
- Vous pouvez modifier les paramètres de partage c$ et les propriétés de partage.
- Vous ne pouvez pas supprimer le partage c$.
- L'administrateur du SVM peut accéder au reste de l'espace de noms du SVM à partir du partage c$ mappé en croisant les jonctions de l'espace de noms.
- Le partage c$ est accessible à l'aide de la console de gestion Microsoft.

Informations associées

Configurer les autorisations de fichiers avancées à l'aide de l'onglet Sécurité Windows

En savoir plus sur les exigences de dénomination des partages SMB de ONTAP

Lors de la création de partages SMB sur votre serveur SMB, veillez à respecter les exigences de dénomination des partages ONTAP.

Les conventions de nom des partages pour ONTAP sont identiques à celles de Windows et doivent être respectées dans ce cas :

- Le nom de chaque partage doit être unique pour le serveur SMB.
- Les noms de partage ne sont pas sensibles à la casse.
- La longueur maximale du nom de partage est de 80 caractères.
- Les noms de partage Unicode sont pris en charge.
- Les noms de partage se terminant par le caractère $ sont des partages masqués.
- Pour ONTAP 9.7 et les versions antérieures, les partages administratifs admin$, ipc$ et c$ sont automatiquement créés sur chaque serveur CIFS et sont des noms de partage réservés. Depuis ONTAP 9.8, le partage admin$ n'est plus créé automatiquement.
- Lors de la création d'un partage, vous ne pouvez pas utiliser le nom de partage ONTAP_ADMIN$.
- Les noms de partage contenant des espaces sont pris en charge :
  - Vous ne pouvez pas utiliser un espace comme premier caractère ou comme dernier caractère dans un nom de partage.
  - Vous devez inclure des noms de partage contenant un espace entre guillemets.

    Les guillemets simples sont considérés comme faisant partie du nom du partage et ne peuvent pas être utilisés à la place des guillemets.

- Les caractères spéciaux suivants sont pris en charge lorsque vous nommez des partages SMB :

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- Les caractères spéciaux suivants ne sont pas pris en charge lorsque vous nommez des partages SMB :

```
** [ ] " / \ : ; | < > , ? * =
```

En savoir plus sur les exigences en matière de sensibilité aux cas des annuaires SMB de ONTAP lors de la création de partages dans un environnement multiprotocole

Si vous créez des partages dans un SVM où le schéma de nommage 8.3 est utilisé pour faire la distinction entre les noms de répertoire où il n'y a que des différences de cas entre les noms, vous devez utiliser le nom 8.3 du chemin de partage pour s'assurer que le client se connecte au chemin de répertoire souhaité.

Dans l'exemple suivant, deux répertoires nommés « testdir » et « TESTDIR » ont été créés sur un client Linux. La Junction path du volume contenant les répertoires est `/home`. La première sortie provient d'un client Linux et la seconde sortie provient d'un client SMB.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Lorsque vous créez un partage dans le second répertoire, vous devez utiliser le nom 8.3 dans le chemin du partage. Dans cet exemple, le chemin du partage vers le premier répertoire est `/home/testdir` et le chemin du partage vers le second répertoire est `/home/TESTDI~1`.

Utilisez les propriétés du partage SMB

Découvrez comment utiliser les propriétés de partage SMB de ONTAP

Vous pouvez personnaliser les propriétés des partages SMB.

Les propriétés de partage disponibles sont les suivantes :

Propriétés du partage	Description
`oplocks`	Cette propriété indique que le partage utilise des verrous opportunistes, également appelés mise en cache côté client.

Propriétés du partage	Description
`browsable`	Cette propriété permet aux clients Windows de parcourir le partage.
`showsnapshot`	Cette propriété indique que les instantanés peuvent être affichés et parcourus par les clients.
`changenotify`	Cette propriété indique que le partage prend en charge les demandes de notification des modifications. Pour les partages sur un SVM, il s'agit d'une propriété initiale par défaut.
`attributecache`	Cette propriété permet la mise en cache des attributs de fichier sur le partage SMB afin d'accélérer l'accès aux attributs. La valeur par défaut est de désactiver la mise en cache des attributs. Cette propriété ne doit être activée que si des clients se connectent à des partages sur SMB 1.0. Cette propriété de partage n'est pas applicable si les clients se connectent à des partages via SMB 2.x ou SMB 3.0.
`continuously-available`	Cette propriété permet aux clients SMB qui la prennent en charge d'ouvrir des fichiers de façon persistante. Les fichiers ouverts de cette façon sont protégés contre les événements perturbateurs, tels que le basculement et le rétablissement.
`branchcache`	Cette propriété spécifie que le partage permet aux clients de demander des hachages de BranchCache sur les fichiers de ce partage. Cette option n'est utile que si vous spécifiez « par partage » en mode de fonctionnement dans la configuration de BranchCache CIFS.
`access-based-enumeration`	Cette propriété spécifie que *accès basé sur Enumeration* (ABE) est activé sur ce partage. Les dossiers partagés filtrés PAR ABE sont visibles par un utilisateur en fonction des droits d'accès de cet utilisateur, empêchant l'affichage des dossiers ou d'autres ressources partagées que l'utilisateur ne dispose pas des droits d'accès.

Propriétés du partage	Description
`namespace-caching`	Cette propriété spécifie que les clients SMB qui se connectent à ce partage peuvent mettre en cache les résultats d'énumération de répertoire renvoyés par les serveurs CIFS, ce qui peut fournir de meilleures performances. Par défaut, les clients SMB 1 ne mettent pas en cache les résultats d'énumération des répertoires. Étant donné que les clients SMB 2 et SMB 3 mettent en cache les résultats d'énumération de répertoires par défaut, la spécification de cette propriété de partage n'offre des avantages en termes de performances que pour les connexions clients SMB 1.
`encrypt-data`	Cette propriété spécifie que le chiffrement SMB doit être utilisé lors de l'accès à ce partage. Les clients SMB qui ne prennent pas en charge le chiffrement lors de l'accès aux données SMB ne pourront pas accéder à ce partage.

Ajoutez ou supprimez des propriétés de partage sur les partages SMB ONTAP existants

Vous pouvez personnaliser un partage SMB existant en ajoutant ou en supprimant des propriétés de partage. Cela peut être utile si vous voulez modifier la configuration du partage pour répondre aux exigences changeantes de votre environnement.

Avant de commencer

Le partage dont vous souhaitez modifier les propriétés doit exister.

Description de la tâche

Instructions pour l'ajout de propriétés de partage :

- Vous pouvez ajouter une ou plusieurs propriétés de partage à l'aide d'une liste délimitée par des virgules.
- Toutes les propriétés de partage que vous avez précédemment spécifiées restent en vigueur.

  Les nouvelles propriétés ajoutées sont ajoutées à la liste existante des propriétés de partage.

- Si vous spécifiez une nouvelle valeur pour les propriétés de partage qui sont déjà appliquées au partage, la nouvelle valeur spécifiée remplace la valeur d'origine.
- Vous ne pouvez pas supprimer les propriétés de partage à l'aide de `vserver cifs share properties add` commande.

  Vous pouvez utiliser le `vserver cifs share properties remove` commande permettant de supprimer les propriétés de partage.

Consignes de suppression des propriétés de partage :

- Vous pouvez supprimer une ou plusieurs propriétés de partage à l'aide d'une liste délimitée par des virgules.

- Toutes les propriétés de partage que vous avez précédemment spécifiées mais que vous ne les supprimez pas restent en vigueur.

Étapes

1. Saisissez la commande appropriée :

Les fonctions que vous recherchez…	Entrez la commande…
Ajouter des propriétés de partage	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Supprimer les propriétés de partage	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Vérifiez les paramètres de propriété de partage : `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemples

La commande suivante ajoute la `showsnapshot` Partagez la propriété avec une part nommée « `khare1' » sur la SVM vs1 :

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

La commande suivante supprime le `browsable` Partagez des biens d'une part nommée « `sune2` » sur la SVM vs1 :

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Informations associées

Commandes de gestion des partages

Optimisez l'accès des utilisateurs SMB ONTAP avec le paramètre de partage de groupe de force

Lorsque vous créez un partage à partir de la ligne de commande ONTAP vers des données avec sécurité efficace UNIX, vous pouvez spécifier que tous les fichiers créés par les utilisateurs SMB de ce partage appartiennent au même groupe, appelé *force-group*, qui doit être un groupe prédéfini dans la base de données du groupe UNIX. L'utilisation d'un groupe de force facilite l'accès aux fichiers par les utilisateurs SMB appartenant à différents groupes.

La spécification d'un groupe de force n'est pertinente que si le partage est dans un qtree UNIX ou mixte. Il n'est pas nécessaire de définir un groupe de force pour les partages d'un volume NTFS ou d'un qtree, car l'accès aux fichiers de ces partages est déterminé par les autorisations Windows, et non par des GIDS UNIX.

Si un groupe de force a été spécifié pour un partage, les valeurs suivantes deviennent vraies pour le partage :

- Les moyennes entreprises qui accèdent à ce partage sont temporairement modifiées en GID du groupe force.

  Ce GID leur permet d'accéder aux fichiers de ce partage qui ne sont pas accessibles normalement avec leur GID ou leur UID principal.

- Tous les fichiers de ce partage créés par les utilisateurs SMB appartiennent au même groupe de force, quel que soit le GID principal du propriétaire du fichier.

Lorsque les utilisateurs SMB essaient d'accéder à un fichier créé par NFS, les principaux GID des utilisateurs SMB déterminent les droits d'accès.

La force-group n'affecte pas la façon dont les utilisateurs NFS accèdent aux fichiers dans ce partage. Un fichier créé par NFS acquiert le GID du propriétaire du fichier. La détermination des autorisations d'accès est basée sur l'UID et le GID principal de l'utilisateur NFS qui tente d'accéder au fichier.

L'utilisation d'un groupe de force facilite l'accès aux fichiers par les utilisateurs SMB appartenant à différents groupes. Par exemple, si vous souhaitez créer un partage pour stocker les pages Web de l'entreprise et donner un accès en écriture aux utilisateurs des départements Ingénierie et Marketing, vous pouvez créer un partage et donner accès en écriture à un groupe de force nommé « webgroupe1 ». En raison du groupe de force, tous les fichiers créés par les utilisateurs SMB de ce partage appartiennent au groupe « webgroupe1 ». En outre, les utilisateurs se voient automatiquement attribuer le GID du groupe « webgroupe1 » lorsqu'ils

accèdent au partage. Par conséquent, tous les utilisateurs peuvent écrire sur ce partage sans avoir à gérer les droits d'accès des utilisateurs dans les services Ingénierie et Marketing.

Informations associées

Créer des partages avec le paramètre de partage de groupe forcé

Créez des partages SMB ONTAP avec le paramètre de partage de groupe de force

Vous pouvez créer un partage SMB avec le paramètre de partage force-group si vous souhaitez que les utilisateurs SMB qui accèdent aux données sur des volumes ou des qtrees avec la sécurité de fichier UNIX soient considérés par ONTAP comme appartenant au même groupe UNIX.

Étape

1. Créez le partage SMB : `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Si le chemin UNC (`\\servername\sharename\filepath`) du partage contient plus de 256 caractères (à l'exclusion de la première «`\\`" Dans le chemin UNC), l'onglet **sécurité** de la boîte Propriétés de Windows n'est pas disponible. Il s'agit d'un problème de client Windows plutôt que d'un problème ONTAP. Pour éviter ce problème, ne créez pas de partages avec des chemins UNC de plus de 256 caractères.

   Si vous souhaitez supprimer le groupe de force après la création du partage, vous pouvez modifier le partage à tout moment et spécifier une chaîne vide ("") comme valeur pour le `-force-group-for -create` paramètre. Si vous supprimez le groupe de force en modifiant le partage, toutes les connexions existantes à ce partage continuent d'avoir le groupe de force précédemment défini comme GID principal.

Exemple

La commande suivante crée un partage « pages Web » accessible sur le Web dans le `/corp/companyinfo` Répertoire dans lequel tous les fichiers créés par les utilisateurs SMB sont affectés au groupe webgroupe1 :

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Informations associées

Optimiser l'accès des utilisateurs avec le paramètre de partage de groupe forcé

Afficher des informations sur les partages SMB ONTAP à l'aide de la console MMC

Vous pouvez afficher les informations relatives aux partages SMB sur votre SVM et effectuer certaines tâches de gestion à l'aide de la console de gestion Microsoft (MMC). Avant de pouvoir afficher les partages, vous devez connecter la MMC au SVM.

Description de la tâche

Vous pouvez effectuer les tâches suivantes sur les partages contenus dans les SVM à l'aide de MMC :

- Afficher les partages
- Afficher les sessions actives
- Afficher les fichiers ouverts
- Énumérer la liste des sessions, des fichiers et des connexions d'arborescence dans le système

- Fermez les fichiers ouverts dans le système
- Fermer les sessions ouvertes
- Création/gestion de partages

> Les vues affichées par les fonctionnalités précédentes sont propres à chaque nœud et non à chaque cluster. Par conséquent, lorsque vous utilisez le MMC pour vous connecter au nom d'hôte du serveur SMB (à savoir, cifs01.domain.local), vous êtes routé, selon la façon dont vous avez configuré DNS, vers une seule LIF au sein de votre cluster.

Les fonctions suivantes ne sont pas prises en charge dans MMC pour ONTAP :

- Création de nouveaux utilisateurs/groupes locaux
- Gestion/affichage des utilisateurs/groupes locaux existants
- Affichage des événements ou des journaux de performances
- Stockage
- Services et applications

Dans les cas où l'opération n'est pas prise en charge, vous pouvez être confrontés à une situation `remote procedure call failed` erreurs.

"FAQ : utilisation de Windows MMC avec ONTAP"

Étapes

1. Pour ouvrir Computer Management MMC sur n'importe quel serveur Windows, dans le **panneau de configuration**, sélectionnez **Outils d'administration** > **gestion de l'ordinateur**.
2. Sélectionnez **action** > **connexion à un autre ordinateur**.

   La boîte de dialogue Sélectionner un ordinateur s'affiche.

3. Tapez le nom du système de stockage ou cliquez sur **Parcourir** pour localiser le système de stockage.
4. Cliquez sur **OK**.

   La MMC se connecte à la SVM.

5. Dans le volet de navigation, cliquez sur **dossiers partagés** > **partages**.

   Une liste des partages sur le SVM est affichée dans le volet d'affichage droit.

6. Pour afficher les propriétés de partage d'un partage, double-cliquez sur le partage pour ouvrir la boîte de dialogue **Propriétés**.
7. Si vous ne pouvez pas vous connecter au système de stockage à l'aide de MMC, vous pouvez ajouter l'utilisateur au groupe BULTIN\Administrators ou BULTIN\Power Users en utilisant l'une des commandes suivantes sur le système de stockage :

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Commandes ONTAP pour la gestion des partages SMB

Vous utilisez le `vserver cifs share` et `vserver cifs share properties` Commandes pour gérer les partages SMB.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un partage SMB	`vserver cifs share create`
Affiche les partages SMB	`vserver cifs share show`
Modifiez un partage SMB	`vserver cifs share modify`
Supprime un partage SMB	`vserver cifs share delete`
Ajouter des propriétés de partage à un partage existant	`vserver cifs share properties add`
Supprimer les propriétés de partage d'un partage existant	`vserver cifs share properties remove`
Affiche des informations sur les propriétés de partage	`vserver cifs share properties show`

Pour en savoir plus, `vserver cifs` consultez le "Référence de commande ONTAP".

Sécurisez l'accès aux fichiers à l'aide des ACL de partage SMB

En savoir plus sur la gestion des listes de contrôle d'accès au niveau du partage SMB ONTAP

Vous pouvez modifier les listes de contrôle d'accès au niveau du partage pour accorder aux utilisateurs plus ou moins de droits d'accès au partage. Vous pouvez configurer les listes de contrôle d'accès au niveau du partage en utilisant soit des utilisateurs et des groupes Windows, soit des utilisateurs et des groupes UNIX.

Par défaut, la liste de contrôle d'accès au niveau du partage donne un contrôle total au groupe standard nommé Everyone. Le contrôle total dans la liste de contrôle d'accès signifie que tous les utilisateurs du domaine et tous les domaines de confiance ont un accès total au partage. Vous pouvez contrôler le niveau d'accès d'une liste de contrôle d'accès au niveau du partage à l'aide de la console de gestion Microsoft (MMC) sur un client Windows ou de la ligne de commande ONTAP. "Créer des listes de contrôle d'accès aux partages".

Les directives suivantes s'appliquent lorsque vous utilisez la console MMC :

- Les noms d'utilisateur et de groupe spécifiés doivent être des noms Windows.
- Vous ne pouvez spécifier que des autorisations Windows.

Les consignes suivantes s'appliquent lorsque vous utilisez la ligne de commande ONTAP :

- Les noms d'utilisateur et de groupe spécifiés peuvent être des noms Windows ou UNIX.

  Si un type d'utilisateur et de groupe n'est pas spécifié lors de la création ou de la modification des listes de contrôle d'accès, le type par défaut est utilisateurs et groupes Windows.

- Vous ne pouvez spécifier que des autorisations Windows.

Créez des listes de contrôle d'accès pour les partages SMB ONTAP

La configuration des autorisations de partage en créant des listes de contrôle d'accès (ACL) pour les partages SMB vous permet de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes.

Description de la tâche

Vous pouvez configurer les listes de contrôle d'accès au niveau du partage à l'aide des noms d'utilisateur ou de groupe Windows locaux ou de domaine ou des noms d'utilisateur ou de groupe UNIX.

Avant de créer une nouvelle liste de contrôle d'accès, vous devez supprimer la liste de contrôle d'accès de partage par défaut `Everyone / Full Control`, qui pose un risque pour la sécurité.

En mode Workgroup, le nom de domaine local est le nom du serveur SMB.

Étapes

1. Supprimez la liste de contrôle d'accès du partage par défaut : « vserver cifs share Access-control delete -vserver <vserver_name> -share <share_name> -user-or-group everyone »
2. Configurer la nouvelle liste de contrôle d'accès :

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un…	Entrez la commande…
Utilisateur Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Groupe Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un…	Entrez la commande…
Utilisateur UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
Groupe UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Vérifiez que la liste de contrôle d'accès appliquée au partage est correcte à l'aide de la `vserver cifs share access-control show` commande.

Exemple

La commande suivante donne `Change` Autorisations au groupe Windows "sales Team" pour la part "sales" sur le SVM "vs1.example.com":

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

La commande suivante donne `Read` l'autorisation au groupe UNIX « engineering » pour le partage « eng » sur le SVM « vs2.example.com » :

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$         BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng        engineering              unix-group  Read
```

Les commandes suivantes donnent `Change` l'autorisation au groupe Windows local nommé « Tiger Team » et `Full_Control` l'autorisation à l'utilisateur Windows local nommé « Sue Chang » pour le partage « datavol5 » sur le SVM « vs1 » :

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

Commandes ONTAP pour la gestion des listes de contrôle d'accès aux partages SMB

Vous devez connaître les commandes de gestion des listes de contrôle d'accès (ACL) SMB, notamment leur création, leur affichage, leur modification et leur suppression.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer une nouvelle liste de contrôle d'accès	`vserver cifs share access-control create`
Afficher les ACL	`vserver cifs share access-control show`
Modifier une ACL	`vserver cifs share access-control modify`
Supprimer une ACL	`vserver cifs share access-control delete`

Sécurisez l'accès aux fichiers grâce aux autorisations liées aux fichiers

Configurer les autorisations de fichiers NTFS avancées à l'aide de l'onglet Sécurité Windows pour les SVM SMB ONTAP

Vous pouvez configurer les autorisations de fichier NTFS standard sur les fichiers et les dossiers en utilisant l'onglet **sécurité Windows** de la fenêtre Propriétés Windows.

Avant de commencer

L'administrateur effectuant cette tâche doit disposer d'autorisations NTFS suffisantes pour modifier les autorisations sur les objets sélectionnés.

Description de la tâche

La configuration des autorisations de fichiers NTFS se fait sur un hôte Windows en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS. Ces tâches sont traitées automatiquement par l'interface graphique de Windows.

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Renseignez la boîte de dialogue **Map Network Drive** :

   a. Sélectionnez une lettre **lecteur**.

   b. Dans la zone **Folder**, saisissez le nom du serveur CIFS contenant le partage contenant les données auxquelles vous souhaitez appliquer les autorisations et le nom du partage.

      Si le nom de votre serveur CIFS est ""CIFS_SERVER"" et que votre partage est nommé "`hare1"", vous devez taper `\\CIFS_SERVER\share1`.

      > Vous pouvez spécifier l'adresse IP de l'interface de données du serveur CIFS au lieu du nom du serveur CIFS.

   c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez définir les autorisations de fichier NTFS.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.

   L'onglet **sécurité** affiche la liste des utilisateurs et des groupes pour lesquels les autorisations NTFS sont définies. La zone **autorisations pour** affiche une liste des autorisations Autoriser et refuser en vigueur pour chaque utilisateur ou groupe sélectionné.

6. Cliquez sur **Avancé**.

   La fenêtre Propriétés de Windows affiche des informations sur les autorisations de fichier existantes attribuées aux utilisateurs et aux groupes.

7. Cliquez sur **Modifier les autorisations**.

   La fenêtre autorisations s'ouvre.

8. Effectuez les opérations souhaitées :

Les fonctions que vous recherchez…	Procédez comme suit…
Configurez des autorisations NTFS avancées pour un nouvel utilisateur ou un nouveau groupe	a. Cliquez sur **Ajouter**. b. Dans la zone **Entrez le nom de l'objet à sélectionner**, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter. c. Cliquez sur **OK**.
Modifiez les autorisations NTFS avancées d'un utilisateur ou d'un groupe	a. Dans la zone **permissions Entries:**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier les autorisations avancées. b. Cliquez sur **Modifier**.
Supprimez les autorisations NTFS avancées pour un utilisateur ou un groupe	a. Dans la zone **permissions Entries:**, sélectionnez l'utilisateur ou le groupe à supprimer. b. Cliquez sur **Supprimer**. c. Passez à l'étape 13.

   Si vous ajoutez des autorisations NTFS avancées sur un nouvel utilisateur ou un nouveau groupe ou si vous modifiez les autorisations avancées NTFS sur un utilisateur ou un groupe existant, la zone entrée d'autorisation de <objet> s'ouvre.

9. Dans la zone **appliquer à**, sélectionnez la façon dont vous souhaitez appliquer cette entrée d'autorisation de fichier NTFS.

   Si vous configurez des autorisations de fichier NTFS sur un seul fichier, la case **appliquer à** n'est pas active. Le paramètre **appliquer à** est défini par défaut sur **cet objet uniquement**.

10. Dans la zone **permissions**, sélectionnez les cases **Autoriser** ou **refuser** pour les autorisations avancées que vous souhaitez définir sur cet objet.

- Pour autoriser l'accès spécifié, cochez la case **Autoriser**.
- Pour ne pas autoriser l'accès spécifié, cochez la case **Deny**.
  Vous pouvez définir des autorisations sur les droits avancés suivants :
- **Contrôle total**

  Si vous choisissez ce droit avancé, tous les autres droits avancés sont automatiquement choisis (autoriser ou refuser des droits).

- **Dossier traverse / fichier d'exécution**
- **Liste de dossiers / lecture de données**
- **Lire les attributs**
- **Lire les attributs étendus**
- **Créer des fichiers / écrire des données**
- **Créer des dossiers / ajouter des données**
- **Ecrire des attributs**
- **Ecrire des attributs étendus**
- **Supprimer des sous-dossiers et des fichiers**
- **Supprimer**
- **Autorisations de lecture**
- **Modifier les autorisations**
- * Prendre possession*

> Si l'une des zones d'autorisation avancée n'est pas sélectionnable, c'est parce que les autorisations sont héritées de l'objet parent.

11. Si vous souhaitez que les sous-dossiers et les fichiers de cet objet héritent de ces autorisations, cochez la case **appliquer ces autorisations aux objets et/ou aux conteneurs dans ce conteneur uniquement**.
12. Cliquez sur **OK**.
13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des autorisations NTFS, spécifiez le paramètre d'héritage de cet objet :

    - Sélectionnez la case **inclure les autorisations héritables dans la boîte parent** de cet objet.

      Il s'agit de la valeur par défaut.

    - Sélectionnez la case **remplacer toutes les autorisations d'objet enfant par des autorisations héritables de cet objet**.

      Ce paramètre n'est pas présent dans la zone autorisations si vous définissez des autorisations de fichier NTFS sur un seul fichier.

Soyez prudent lorsque vous sélectionnez ce paramètre. Ce paramètre supprime toutes les autorisations existantes sur tous les objets enfants et les remplace par les paramètres d'autorisation de cet objet. Vous pourriez supprimer par inadvertance les autorisations que vous ne souhaitez pas supprimer. Il est particulièrement important lorsque vous définissez des autorisations dans un volume mixte de style de sécurité ou qtree. Si les objets enfant ont un style de sécurité UNIX effectif, la propagation des autorisations NTFS à ces objets enfant entraîne le ONTAP changement de style de sécurité UNIX au style de sécurité NTFS, et toutes les autorisations UNIX sur ces objets enfants sont remplacées par des autorisations NTFS.

- Sélectionnez les deux cases.
- Sélectionnez aucune case.

14. Cliquez sur **OK** pour fermer la case **permissions**.
15. Cliquez sur **OK** pour fermer la case **Paramètres de sécurité avancés pour <objet>**.

Pour plus d'informations sur la définition des autorisations NTFS avancées, consultez votre documentation Windows.

Informations associées

- Créer des descripteurs de sécurité NTFS sur les serveurs
- Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité NTFS
- Affiche des informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes
- Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité UNIX

Commandes ONTAP pour les autorisations de fichiers SMB NTFS

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS sur les fichiers et les répertoires à l'aide de l'interface de ligne de commande ONTAP. Cela vous permet de configurer les autorisations d'accès aux fichiers NTFS sans avoir à vous connecter aux données à l'aide d'un partage SMB sur un client Windows.

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS.

Vous ne pouvez configurer les autorisations de fichier NTFS qu'à l'aide de la ligne de commande. Vous ne pouvez pas configurer les listes de contrôle d'accès NFSv4 en utilisant l'interface de ligne de commandes.

Étapes

1. Créez un descripteur de sécurité NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. Ajoutez des listes de contrôle d'accès discrétionnaire au descripteur de sécurité NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
```

```
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
{this-folder|sub-folders|files}
```

3. Créez une stratégie de sécurité de fichiers/répertoires.

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

En savoir plus sur les autorisations de fichiers UNIX fournissant un contrôle d'accès lors de l'accès aux fichiers sur les serveurs ONTAP SMB

Un volume FlexVol peut avoir l'un des trois types de style de sécurité suivants : NTFS, UNIX ou mixte. Vous pouvez accéder aux données via SMB quel que soit le style de sécurité. Cependant, des autorisations appropriées sur les fichiers UNIX sont nécessaires pour accéder aux données à l'aide de la sécurité effective d'UNIX.

Lorsque vous accédez aux données via SMB, plusieurs contrôles d'accès sont utilisés pour déterminer si un utilisateur est autorisé à effectuer une action demandée :

- Droits d'exportation

  La configuration des autorisations d'exportation pour l'accès SMB est facultative.

- Partager les autorisations
- Autorisations liées aux fichiers

  Les types d'autorisations de fichier suivants peuvent être appliqués aux données sur lesquelles l'utilisateur souhaite effectuer une action :

  - NTFS
  - ACL UNIX NFSv4
  - Bits mode UNIX

Pour les données avec des ACL NFSv4 ou des bits de mode UNIX définis, les autorisations de style UNIX sont utilisées afin de déterminer les droits d'accès aux fichiers aux données. L'administrateur du SVM doit définir l'autorisation appropriée pour garantir que les utilisateurs disposent des droits nécessaires pour effectuer l'action souhaitée.

> Les données d'un volume de type sécurité mixte peuvent avoir un style de sécurité NTFS ou UNIX. Si les données ont un style de sécurité UNIX effectif, les autorisations NFSv4 ou les bits du mode UNIX sont utilisés pour déterminer les droits d'accès aux fichiers aux données.

Accès sécurisé aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

En savoir plus sur la sécurité d'accès aux fichiers DAC pour les serveurs SMB ONTAP

Vous pouvez sécuriser l'accès à l'aide du contrôle d'accès dynamique et en créant des stratégies d'accès centrales dans Active Directory et en les appliquant aux fichiers et dossiers sur les SVM via des objets de stratégie de groupe appliqués (GPO, Applied Group Policy Objects). Vous pouvez configurer l'audit de manière à utiliser les événements d'activation de stratégie d'accès central pour voir les effets des modifications

apportées aux stratégies d'accès central avant de les appliquer.

Ajouts aux informations d'identification CIFS

Avant le contrôle d'accès dynamique, un identifiant CIFS incluait une identité de sécurité (de l'utilisateur) et une appartenance au groupe Windows. Avec le contrôle d'accès dynamique, trois autres types d'informations sont ajoutés à l'identité du périphérique, aux réclamations du périphérique et aux réclamations de l'utilisateur :

- Identité du périphérique

  Analogique des informations d'identité de l'utilisateur, à l'exception de l'identité et de l'appartenance au groupe de l'appareil à partir de lequel l'utilisateur se connecte.

- Réclamations de l'appareil

  Assertions sur un principal de sécurité de périphérique. Par exemple, un sinistre de périphérique peut être qu'il est membre d'une UO spécifique.

- Réclamations de l'utilisateur

  Assertions sur un principal de sécurité utilisateur. Par exemple, une réclamation d'utilisateur peut être que son compte AD est membre d'une unité d'organisation spécifique.

Politiques d'accès centralisé

Les stratégies d'accès centrales aux fichiers permettent aux organisations de déployer et de gérer de manière centralisée des stratégies d'autorisation qui incluent des expressions conditionnelles à l'aide de groupes d'utilisateurs, de revendications d'utilisateurs, de revendications de périphériques et de propriétés de ressources.

Par exemple, pour accéder aux données à fort impact sur l'entreprise, un utilisateur doit être un employé à plein temps et n'a accès qu'aux données à partir d'un périphérique géré. Les stratégies d'accès central sont définies dans Active Directory et distribuées aux serveurs de fichiers via le mécanisme GPO.

Mise en place centralisée des stratégies d'accès avec audit avancé

Les politiques d'accès central peuvent être « mises en service », auquel cas elles sont évaluées de manière « par quoi » lors des contrôles d'accès aux fichiers. Les résultats de ce qui se serait passé si la stratégie était en vigueur et la différence par rapport à ce qui est actuellement configuré sont consignés en tant qu'événement d'audit. De cette façon, les administrateurs peuvent utiliser les journaux d'événements d'audit pour étudier l'impact d'une modification de stratégie d'accès avant de mettre la stratégie en jeu. Après avoir évalué l'impact d'une modification de règle d'accès, la règle peut être déployée via des GPO sur les SVM souhaités.

Informations associées

- En savoir plus sur les GPO pris en charge
- En savoir plus sur l'application des objets de stratégie de groupe aux serveurs SMB
- Activer ou désactiver la prise en charge des GPO sur les serveurs
- Affiche des informations sur les configurations GPO
- Afficher des informations sur les stratégies d'accès central
- Afficher des informations sur les règles de stratégie d'accès central
- Configurer des politiques d'accès centralisées pour sécuriser les données sur les serveurs

- Afficher des informations sur la sécurité des serveurs
- "Audit et suivi de sécurité SMB et NFS"

Fonctionnalité DAC prise en charge pour les serveurs ONTAP SMB

Si vous souhaitez utiliser le contrôle d'accès dynamique (DAC) sur votre serveur CIFS, vous devez comprendre comment ONTAP prend en charge la fonctionnalité de contrôle d'accès dynamique dans les environnements Active Directory.

Pris en charge pour le contrôle d'accès dynamique

ONTAP prend en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Réclamations dans le système de fichiers	Les revendications sont des paires de nom et de valeur simples qui indiquent une certaine vérité sur un utilisateur. Les informations d'identification utilisateur contiennent des informations sur les sinistres, et les descripteurs de sécurité sur les fichiers peuvent effectuer des vérifications d'accès qui incluent des vérifications de sinistres. Les administrateurs peuvent ainsi mieux contrôler qui peut accéder aux fichiers.
Expressions conditionnelles pour les vérifications d'accès aux fichiers	Lors de la modification des paramètres de sécurité d'un fichier, les utilisateurs peuvent ajouter des expressions conditionnelles arbitrairement complexes au descripteur de sécurité du fichier. L'expression conditionnelle peut inclure des vérifications pour les sinistres.
Contrôle centralisé de l'accès aux fichiers via des règles d'accès centrales	Les stratégies d'accès central sont des types de listes de contrôle d'accès stockées dans Active Directory et peuvent être balisées vers un fichier. L'accès au fichier n'est accordé que si les contrôles d'accès du Security Descriptor sur disque et de la stratégie d'accès centrale balisée permettent l'accès.cela permet aux administrateurs de contrôler l'accès aux fichiers à partir d'un emplacement central (AD) sans avoir à modifier le Security Descriptor sur disque.
Mise en place de stratégies d'accès centrales	Ajoute la capacité d'essayer des changements de sécurité sans affecter l'accès réel aux fichiers, en "mettant en place" un changement aux politiques d'accès central, et en voyant l'effet de la modification dans un rapport d'audit.
Affichage d'informations sur la sécurité des règles d'accès centrales à l'aide de l'interface de ligne de commande de ONTAP	Étend le `vserver security file-directory show` commande pour afficher les informations sur les règles d'accès central appliquées.

Fonctionnalité	Commentaires
Suivi de la sécurité qui inclut les stratégies d'accès centralisé	Étend le `vserver security trace` famille de commandes permettant d'afficher les résultats qui incluent des informations sur les stratégies d'accès central appliquées.

Non pris en charge pour le contrôle d'accès dynamique

ONTAP ne prend pas en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Classification automatique des objets du système de fichiers NTFS	Il s'agit d'une extension de l'infrastructure de classification de fichiers Windows qui n'est pas prise en charge dans ONTAP.
Audit avancé autre que la mise en place de stratégies d'accès centrales	Seul le staging de stratégie d'accès central est pris en charge pour l'audit avancé.

En savoir plus sur l'utilisation de DAC et des politiques d'accès centralisées avec les serveurs ONTAP SMB

Vous devez garder à l'esprit certaines considérations lorsque vous utilisez le contrôle d'accès dynamique (DAC) et les règles d'accès central pour sécuriser les fichiers et dossiers sur les serveurs CIFS.

L'accès NFS peut être refusé à la racine si la règle de stratégie s'applique à l'utilisateur de domaine\administrateur

Dans certaines circonstances, l'accès NFS à la racine peut être refusé lorsque la sécurité de la stratégie d'accès centrale est appliquée aux données auxquelles l'utilisateur root tente d'accéder. Le problème se produit lorsque la stratégie d'accès central contient une règle appliquée au domaine\administrateur et que le compte racine est mappé au compte domaine\administrateur.

Au lieu d'appliquer une règle à l'utilisateur domaine/administrateur, vous devez appliquer la règle à un groupe avec des privilèges d'administration, tels que le groupe domaine/administrateurs. De cette façon, vous pouvez mapper root sur le compte domaine\administrateur sans que ce problème n'ait d'impact sur la racine.

Le groupe BUILTIN\Administrators du serveur CIFS a accès aux ressources lorsque la stratégie d'accès central appliquée n'est pas trouvée dans Active Directory

Il est possible que les ressources contenues dans le serveur CIFS aient des règles d'accès centrales qui leur sont appliquées, mais lorsque le serveur CIFS utilise le SID de la stratégie d'accès centrale pour tenter de récupérer des informations à partir d'Active Directory, le SID ne correspond à aucun SID de stratégie d'accès centrale existant dans Active Directory. Dans ces circonstances, le serveur CIFS applique la stratégie de restauration par défaut locale pour cette ressource.

La stratégie de récupération par défaut locale permet au groupe BUILTIN\Administrators du serveur CIFS d'accéder à cette ressource.

Activer ou désactiver DAC pour les serveurs ONTAP SMB

L'option qui vous permet d'utiliser le contrôle d'accès dynamique (DAC) pour sécuriser les objets sur votre serveur CIFS est désactivée par défaut. Vous devez activer cette option si vous souhaitez utiliser le contrôle d'accès dynamique sur votre serveur CIFS. Si vous décidez par la suite de ne pas utiliser le contrôle d'accès dynamique pour sécuriser les objets stockés sur le serveur CIFS, vous pouvez désactiver cette option.

Vous trouverez des informations sur la configuration du contrôle d'accès dynamique sur Active Directory dans la bibliothèque Microsoft TechNet.

"Microsoft TechNet : présentation des scénarios de contrôle d'accès dynamique"

Description de la tâche

Une fois le contrôle d'accès dynamique activé, le système de fichiers peut contenir des listes de contrôle d'accès avec des entrées liées au contrôle d'accès dynamique. Si le contrôle d'accès dynamique est désactivé, les entrées de contrôle d'accès dynamique actuelles seront ignorées et les nouvelles ne seront pas autorisées.

Cette option n'est disponible qu'au niveau de privilège avancé.

Étape

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que le contrôle d'accès dynamique soit…	Entrez la commande…
Activé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Désactivé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Revenir au niveau de privilège administrateur : `set -privilege admin`

Informations associées

Configurer des politiques d'accès centralisées pour sécuriser les données sur les serveurs

Gérer les ACL contenant les ACE DAC lorsque DAC est désactivé sur les serveurs SMB ONTAP

Si vous disposez de ressources dont les listes de contrôle d'accès sont appliquées avec les ACE de contrôle d'accès dynamique et que vous désactivez le contrôle d'accès dynamique sur la machine virtuelle de stockage (SVM), vous devez supprimer les ACE de contrôle d'accès dynamique avant de pouvoir gérer les ACE de contrôle d'accès non dynamique sur cette ressource.

Description de la tâche

Une fois le contrôle d'accès dynamique désactivé, vous ne pouvez pas supprimer les ACE existants de contrôle d'accès non dynamique ou ajouter de nouveaux ACE de contrôle d'accès non dynamique tant que

vous n’avez pas supprimé les ACE de contrôle d’accès dynamique existants.

Vous pouvez utiliser n’importe quel outil que vous utilisez normalement pour gérer les listes de contrôle d’accès pour effectuer ces étapes.

Étapes

1. Déterminez quels ACE de contrôle d’accès dynamique sont appliqués à la ressource.
2. Supprimez les ACE de contrôle d’accès dynamique de la ressource.
3. Ajoutez ou supprimez des ACE de contrôle d’accès non dynamiques comme vous le souhaitez de la ressource.

Configurer des politiques d’accès centralisées pour sécuriser les données sur les serveurs ONTAP SMB

Il existe plusieurs étapes à suivre pour sécuriser l’accès aux données sur le serveur CIFS à l’aide de stratégies d’accès centrales, notamment l’activation du contrôle d’accès dynamique (DAC) sur le serveur CIFS, la configuration de stratégies d’accès central dans Active Directory, l’application des règles d’accès central aux conteneurs Active Directory avec des GPO, Et activation des stratégies de groupe sur le serveur CIFS.

Avant de commencer

- L’Active Directory doit être configuré pour utiliser les stratégies d’accès central.
- Vous devez disposer d’un accès suffisant sur les contrôleurs de domaine Active Directory pour créer des stratégies d’accès centrales et pour créer et appliquer des GPO aux conteneurs contenant les serveurs CIFS.
- Vous devez disposer d’un accès administratif suffisant sur le SVM (Storage Virtual machine) pour exécuter les commandes nécessaires.

Description de la tâche

Les stratégies d’accès central sont définies et appliquées aux objets de stratégie de groupe (GPO, Group Policy Objects) d’Active Directory. Vous trouverez des informations sur la configuration des stratégies d’accès central sur Active Directory dans la bibliothèque Microsoft TechNet.

"Microsoft TechNet : scénario de stratégie d’accès centralisé"

Étapes

1. Activer le contrôle dynamique d’accès sur le SVM si celui-ci n’est pas déjà activé à l’aide de `vserver cifs options modify` commande.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Activez les objets de stratégie de groupe (GPO, Group policy objects) sur le serveur CIFS s’ils ne sont pas déjà activés à l’aide de l' `vserver cifs group-policy modify` commande.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Créez des règles d’accès centrales et des stratégies d’accès central sur Active Directory.
4. Créez un objet de stratégie de groupe (GPO) pour déployer les stratégies d’accès central sur Active Directory.
5. Appliquez l’objet GPO au conteneur où se trouve le compte d’ordinateur du serveur CIFS.

6. Mettre à jour manuellement les GPO appliqués au serveur CIFS à l'aide de `vserver cifs group-policy update` commande.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Vérifiez que la stratégie d'accès central GPO est appliquée aux ressources du serveur CIFS à l'aide de `vserver cifs group-policy show-applied` commande.

   L'exemple suivant montre que la stratégie de domaine par défaut comporte deux stratégies d'accès central appliquées au serveur CIFS :

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
         Hash Version Support for BranchCache: all-versions
     Security Settings:
         Event Audit and Event Log:
             Audit Logon Events: none
             Audit Object Access: success
             Log Retention Method: overwrite-as-needed
             Max Log Size: 16384
         File Security:
             /vol1/home
             /vol1/dir1
         Kerberos:
             Max Clock Skew: 5
             Max Ticket Age: 10
             Max Renew Age:  7
         Privilege Rights:
             Take Ownership: usr1, usr2
             Security Privilege: usr1, usr2
             Change Notify: usr1, usr2
         Registry Values:
             Signing Required: false
         Restrict Anonymous:
             No enumeration of SAM accounts: true
   ```

```
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
```

```
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Informations associées

- En savoir plus sur l'application des objets de stratégie de groupe aux serveurs SMB
- Affiche des informations sur les configurations GPO
- Afficher des informations sur les stratégies d'accès central
- Afficher des informations sur les règles de stratégie d'accès central
- Activer ou désactiver DAC pour les serveurs

Afficher des informations sur la sécurité DAC pour les serveurs SMB ONTAP

Vous pouvez afficher des informations sur la sécurité DAC (Dynamic Access Control) sur des volumes NTFS et sur des données avec la sécurité efficace NTFS sur des volumes de type sécurité mixtes. Cela comprend de l'information sur les ACE conditionnels, les ACE de ressources et les ACE de politique d'accès central. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver vserver_name -path path`
Avec détails étendus	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Où la sortie est affichée avec les SID de groupe et d'utilisateur	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`

Pour afficher les informations…	Saisissez la commande suivante…
A propos de la sécurité des fichiers et des répertoires pour les fichiers et les répertoires où le masque binaire hexadécimal est traduit en format texte	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Exemples

L'exemple suivant affiche les informations de sécurité du contrôle d'accès dynamique sur le chemin `/vol1` Au SVM vs1 :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                 File Inode Number: 112
                    Security Style: mixed
                   Effective Style: ntfs
                    DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                      Unix User Id: 0
                     Unix Group Id: 1
                    Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                       RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                       POLICY ID-All resources - No Write-
0x0-OI|CI
                                    DACL - ACEs
                                       ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                       ALLOW-Everyone-0x1f01ff-OI|CI
                                       ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Informations associées

- Affiche des informations sur les configurations GPO
- Afficher des informations sur les stratégies d'accès central
- Afficher des informations sur les règles de stratégie d'accès central

Considérations relatives à la restauration de DAC sur les serveurs SMB ONTAP

Vous devez savoir ce qui se passe lors du retour à une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique (DAC) et ce que vous devez faire avant et après le rétablissement.

Si vous souhaitez restaurer le cluster vers une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique et que le contrôle d'accès dynamique est activé sur une ou plusieurs machines virtuelles de stockage (SVM), vous devez effectuer les opérations suivantes avant le rétablissement :

- Vous devez désactiver le contrôle d'accès dynamique sur tous les SVM sur lesquels il est activé sur le cluster.
- Vous devez modifier toutes les configurations d'audit sur le cluster contenant le `cap-staging` type d'événement pour utiliser uniquement le `file-op` type d'événement.

Vous devez comprendre et agir sur certaines considérations importantes concernant la restauration des fichiers et dossiers avec les ACE Dynamic Access Control :

- Si le cluster est rétabli, les ACE de contrôle d'accès dynamique existants ne sont pas supprimés ; cependant, ils seront ignorés lors des vérifications d'accès aux fichiers.
- Comme les ACE de contrôle d'accès dynamique sont ignorés après réversion, l'accès aux fichiers change sur les fichiers avec les ACE de contrôle d'accès dynamique.

  Cela pourrait permettre aux utilisateurs d'accéder aux fichiers qu'ils ne pouvaient pas accéder ou ne pouvaient pas accéder aux fichiers qu'ils pouvaient auparavant.

- Vous devez appliquer des ACE de contrôle d'accès non dynamique aux fichiers concernés pour restaurer leur niveau de sécurité précédent.

  Cette opération peut être effectuée avant le rétablissement ou immédiatement après la fin de la nouvelle version.

> Les ACE de contrôle d'accès dynamique étant ignorés après la réversion, il n'est pas nécessaire de les supprimer lors de l'application d'ACE de contrôle d'accès non dynamique aux fichiers affectés. Toutefois, si vous le souhaitez, vous pouvez les supprimer manuellement.

Sécurisez l'accès SMB à l'aide de règles d'exportation

En savoir plus sur l'utilisation des politiques d'exportation avec l'accès ONTAP SMB

Si les export policy pour accès SMB sont activées sur le serveur SMB, les export policies sont utilisées lors du contrôle de l'accès aux volumes du SVM par les clients SMB. Pour accéder aux données, vous pouvez créer une export policy qui autorise l'accès SMB, puis associer la policy aux volumes contenant des partages SMB.

Une export policy applique une ou plusieurs règles qui lui permettent de spécifier les clients autorisés à accéder aux données et les protocoles d'authentification pris en charge pour l'accès en lecture seule et en lecture/écriture. Vous pouvez configurer des stratégies d'exportation afin d'autoriser l'accès via SMB à tous les clients, à un sous-réseau de clients ou à un client spécifique et autoriser l'authentification à l'aide de l'authentification Kerberos, de l'authentification NTLM ou des deux authentifications Kerberos et NTLM lors de la détermination de l'accès en lecture seule et en lecture/écriture aux données.

Après le traitement de toutes les règles d'exportation appliquées à l'export policy, ONTAP peut déterminer si le client dispose d'un accès et quel niveau d'accès. Les règles d'exportation s'appliquent aux ordinateurs clients et non aux utilisateurs et groupes Windows. Les règles d'exportation ne remplacent pas l'authentification et l'autorisation basées sur les utilisateurs et les groupes Windows. Les règles d'exportation offrent une autre couche de sécurité d'accès en plus des autorisations de partage et d'accès aux fichiers.

Vous associez exactement une export policy à chaque volume pour configurer l'accès client au volume. Chaque SVM peut contenir plusieurs export policy. Vous pouvez ainsi effectuer les opérations suivantes pour les SVM avec plusieurs volumes :

- Assigner différentes export policy à chaque volume du SVM pour le contrôle d'accès client individuel à chaque volume du SVM.
- Assigner la même export policy à plusieurs volumes du SVM pour un contrôle d'accès client identique sans avoir à créer de nouvelles export policy pour chaque volume.

Chaque SVM possède au moins une export policy appelée « default », qui ne contient aucune règle. Vous ne pouvez pas supprimer cette export-policy, mais vous pouvez la renommer ou la modifier. Par défaut, chaque volume du SVM est associé aux export policy par défaut. Si les export policy pour accès SMB sont désactivées sur le SVM, la « default » export policy n'a aucun impact sur l'accès SMB.

Vous pouvez configurer les règles fournissant l'accès aux hôtes NFS et SMB et associer cette règle à une export policy, qui peut ensuite être associée au volume qui contient des données auxquelles les hôtes NFS et SMB ont besoin d'accéder. Alternativement, s'il existe des volumes dans lesquels seuls les clients SMB ont besoin d'accéder, vous pouvez configurer une export policy avec des règles qui autorisent uniquement l'accès à l'aide du protocole SMB et qui utilisent uniquement Kerberos ou NTLM (ou les deux) pour l'authentification en lecture seule et l'accès en écriture. L'export policy est ensuite associée aux volumes pour lesquels seul l'accès SMB est souhaité.

Si les export policy pour SMB sont activées et qu'un client effectue une demande d'accès qui n'est pas autorisée par les export policy applicables, la requête échoue et un message d'autorisation refusée. Si un client ne correspond à aucune règle de l'export policy du volume, l'accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés. Ceci est vrai même si les autorisations de partage et de fichier autorisent autrement l'accès. Cela signifie que vous devez configurer votre export policy de manière à limiter les possibilités suivantes sur les volumes contenant des partages SMB :

- Autoriser l'accès à tous les clients ou au sous-ensemble de clients approprié
- Autoriser l'accès via SMB
- Autoriser un accès en lecture seule et en écriture approprié via l'authentification Kerberos ou NTLM (ou les deux)

Découvrez "configuration et gestion des export-policies".

En savoir plus sur les règles d'exportation SMB ONTAP

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client à un volume par rapport à des

paramètres spécifiques que vous configurez pour déterminer comment traiter les demandes d'accès client.

Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy. L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Vous pouvez configurer des règles d'exportation pour déterminer les autorisations d'accès client à l'aide des critères suivants :

- Protocole d'accès aux fichiers utilisé par le client envoyant la requête, par exemple, NFSv4 ou SMB.
- Identifiant client, par exemple, nom d'hôte ou adresse IP.

  La taille maximale du `-clientmatch` le champ est composé de 4096 caractères.

- Type de sécurité utilisé par le client pour l'authentification, par exemple Kerberos v5, NTLM ou AUTH_SYS.

Si une règle spécifie plusieurs critères, le client doit tous les correspondre pour que la règle s'applique.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée à l'aide du protocole NFSv3 et le client a l'adresse IP 10.1.17.37.

Bien que le protocole d'accès client corresponde, l'adresse IP du client se trouve dans un sous-réseau différent de celui spécifié dans la règle d'exportation. Par conséquent, la correspondance des clients échoue et cette règle ne s'applique pas à ce client.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée via le protocole NFSv4 et le client a l'adresse IP 10.1.16.54.

Le protocole d'accès client correspond et l'adresse IP du client se trouve dans le sous-réseau spécifié. Par conséquent, la correspondance du client a réussi et cette règle s'applique à ce client. Le client obtient un accès en lecture-écriture quel que soit son type de sécurité.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Par conséquent, les deux clients bénéficient d'un accès en lecture seule. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

Exemples de règles de politique d'exportation ONTAP qui restreignent ou autorisent l'accès via SMB

Les exemples montrent comment créer des règles d'export policy qui limitent ou autorisent l'accès via SMB sur un SVM dont les export policy pour l'accès SMB sont activées.

Les export policy pour accès SMB sont désactivées par défaut. Vous devez configurer des règles d'export policy qui limitent ou autorisent l'accès sur SMB uniquement si vous avez activé les export policy pour l'accès SMB.

Règle d'exportation pour l'accès SMB uniquement

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la politique: Cifs1
- Numéro d'index : 1
- Correspondance client : correspond uniquement aux clients sur le réseau 192.168.1.0/24
- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : aux clients utilisant l'authentification NTLM ou Kerberos
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Règle d'exportation pour les accès SMB et NFS

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 », qui dispose de la configuration suivante :

- Nom de la politique: Cifs1
- Numéro d'index : 2
- Correspondance client : correspond à tous les clients
- Protocole : accès SMB et NFS
- Accès en lecture seule : pour tous les clients
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos (NFS et SMB) ou NTLM (SMB)
- Mappage de l'ID utilisateur UNIX 0 (zéro) : mappé à l'ID utilisateur 65534 (qui correspond généralement au nom utilisateur personne)
- L'accès SUID et sgID permet

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Règle d'exportation pour accès SMB uniquement à l'aide de NTLM

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la stratégie : ntlm1
- Numéro d'index : 1
- Correspondance client : correspond à tous les clients
- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : uniquement aux clients utilisant NTLM
- Accès en lecture/écriture : uniquement aux clients utilisant NTLM

> Si vous configurez l'option lecture seule ou l'option lecture/écriture pour l'accès NTLM uniquement, vous devez utiliser des entrées basées sur l'adresse IP dans l'option de correspondance client. Autrement, vous recevez `access denied` erreurs. En effet, ONTAP utilise les noms de service Kerberos (SPN) lors de l'utilisation d'un nom d'hôte pour vérifier les droits d'accès du client. L'authentification NTLM ne prend pas en charge les noms SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Activer ou désactiver les politiques d'exportation ONTAP pour l'accès SMB

Vous pouvez activer ou désactiver les export policy pour l'accès SMB sur les SVM

(Storage Virtual machines). L'utilisation des règles d'exportation pour contrôler l'accès SMB aux ressources est facultative.

Avant de commencer

Les conditions suivantes sont requises pour l'activation des export policy pour SMB :

- Le client doit avoir un enregistrement "PTR" dans DNS avant de créer les règles d'exportation pour ce client.
- Un ensemble supplémentaire d'enregistrements « A » et « PTR » pour les noms d'hôtes est nécessaire si le SVM fournit l'accès aux clients NFS et si le nom d'hôte que vous souhaitez utiliser pour l'accès NFS est différent du nom du serveur CIFS.

Description de la tâche

Lors de la configuration d'un nouveau serveur CIFS sur votre SVM, l'utilisation des export policies pour l'accès SMB est désactivée par défaut. Vous pouvez activer des export policy pour l'accès SMB si vous souhaitez contrôler l'accès en fonction du protocole d'authentification, des adresses IP clientes ou des noms d'hôte. Vous pouvez activer ou désactiver des export policy pour l'accès SMB à tout moment.

L'activation des export policy pour CIFS/SMB dans un SVM compatible NFS permet à un client Linux d'utiliser `showmount -e` la commande sur le SVM afin de visualiser les Junction path de tous les volumes SMB avec les export policy rules associées.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activer ou désactiver les export-policies :
   - Activer les export-policies : `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled true`
   - Désactiver les export-policies : `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`
3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant permet d'utiliser les export policy pour contrôler l'accès des clients SMB aux ressources sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Sécurisez l’accès aux fichiers à l’aide de Storage-Level Access Guard

Découvrez l’accès sécurisé aux fichiers ONTAP SMB à l’aide de Storage-Level Access Guard

Outre la sécurisation de l’accès à l’aide de la sécurité native au niveau des fichiers et de l’exportation et du partage, vous pouvez configurer Storage-Level Access Guard, une troisième couche de sécurité appliquée par ONTAP au niveau du volume. Storage-Level Access Guard s’applique à l’accès à partir de tous les protocoles NAS vers l’objet de stockage auquel il est appliqué.

Seules les autorisations d’accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d’accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l’utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

Comportement de la protection d’accès au niveau du stockage

- Storage-Level Access Guard s’applique à tous les fichiers ou tous les répertoires d’un objet de stockage.

  Comme tous les fichiers ou répertoires d’un volume sont soumis aux paramètres Storage-Level Access Guard, l’héritage par propagation n’est pas requis.

- Vous pouvez configurer Storage-Level Access Guard pour qu’il s’applique aux fichiers uniquement, aux répertoires uniquement ou aux fichiers et répertoires d’un volume.
  - Sécurité des fichiers et des répertoires

    S’applique à chaque répertoire et fichier de l’objet de stockage. Il s’agit du paramètre par défaut.

  - Sécurité des fichiers

    S’applique à chaque fichier de l’objet de stockage. L’application de cette sécurité n’affecte pas l’accès aux répertoires ou leur audit.

  - Sécurité de l’annuaire

    S’applique à chaque répertoire de l’objet de stockage. L’application de cette sécurité n’affecte pas l’accès aux fichiers ou leur audit.

- Storage-Level Access Guard est utilisé pour restreindre les autorisations.

  Il ne vous donnera jamais d’autorisations d’accès supplémentaires.

- Si vous affichez les paramètres de sécurité d’un fichier ou d’un répertoire à partir d’un client NFS ou SMB, vous ne voyez pas la sécurité Storage-Level Access Guard.

  Elle est appliquée au niveau de l’objet de stockage et stockée dans les métadonnées utilisées afin de déterminer les autorisations efficaces.

- La sécurité au niveau du stockage ne peut pas être révoquée d’un client, même par un administrateur système (Windows ou UNIX).

  Il est conçu pour être modifié par les administrateurs de stockage uniquement.

- Vous pouvez appliquer Storage-Level Access Guard aux volumes dotés de NTFS ou d’un style de sécurité

mixte.

- Vous pouvez appliquer Storage-Level Access Guard aux volumes de style de sécurité UNIX, tant que le SVM contenant le volume a un serveur CIFS configuré.
- Lorsque les volumes sont montés sous un chemin de jonction de volume et que Storage-Level Access Guard est présent sur ce chemin, il ne sera pas propagé aux volumes montés sous celui-ci.
- Le descripteur de sécurité Storage-Level Access Guard est répliqué avec la réplication des données SnapMirror et avec la réplication SVM.
- Il existe une dispensation spéciale pour les scanners de virus.

  Un accès exceptionnel est autorisé à ces serveurs pour afficher des fichiers et des répertoires, même si Storage-Level Access Guard refuse l'accès à l'objet.

- Les notifications FPolicy ne sont pas envoyées si l'accès est refusé car la protection d'accès du niveau de stockage est disponible.

Ordre des contrôles d'accès

L'accès à un fichier ou à un répertoire est déterminé par l'effet combiné des autorisations d'exportation ou de partage, des autorisations Storage-Level Access Guard définies sur les volumes et des autorisations de fichier natif appliquées aux fichiers et/ou répertoires. Tous les niveaux de sécurité sont évalués pour déterminer les autorisations efficaces qu'un fichier ou un répertoire possède. Les contrôles d'accès de sécurité sont effectués dans l'ordre suivant :

1. Partage SMB ou autorisations au niveau des exportations NFS
2. Protection d'accès au niveau du stockage
3. Listes de contrôle d'accès aux fichiers/dossiers NTFS (ACL), listes de contrôle d'accès NFSv4 ou bits en mode UNIX

Cas d'utilisation de Storage-Level Access Guard

Storage-Level Access Guard fournit une sécurité supplémentaire au niveau du stockage, qui n'est pas visible du côté client. Par conséquent, il ne peut être révoqué par aucun des utilisateurs ou administrateurs de leur poste de travail. Dans certains cas, il est préférable de pouvoir contrôler l'accès au niveau de stockage.

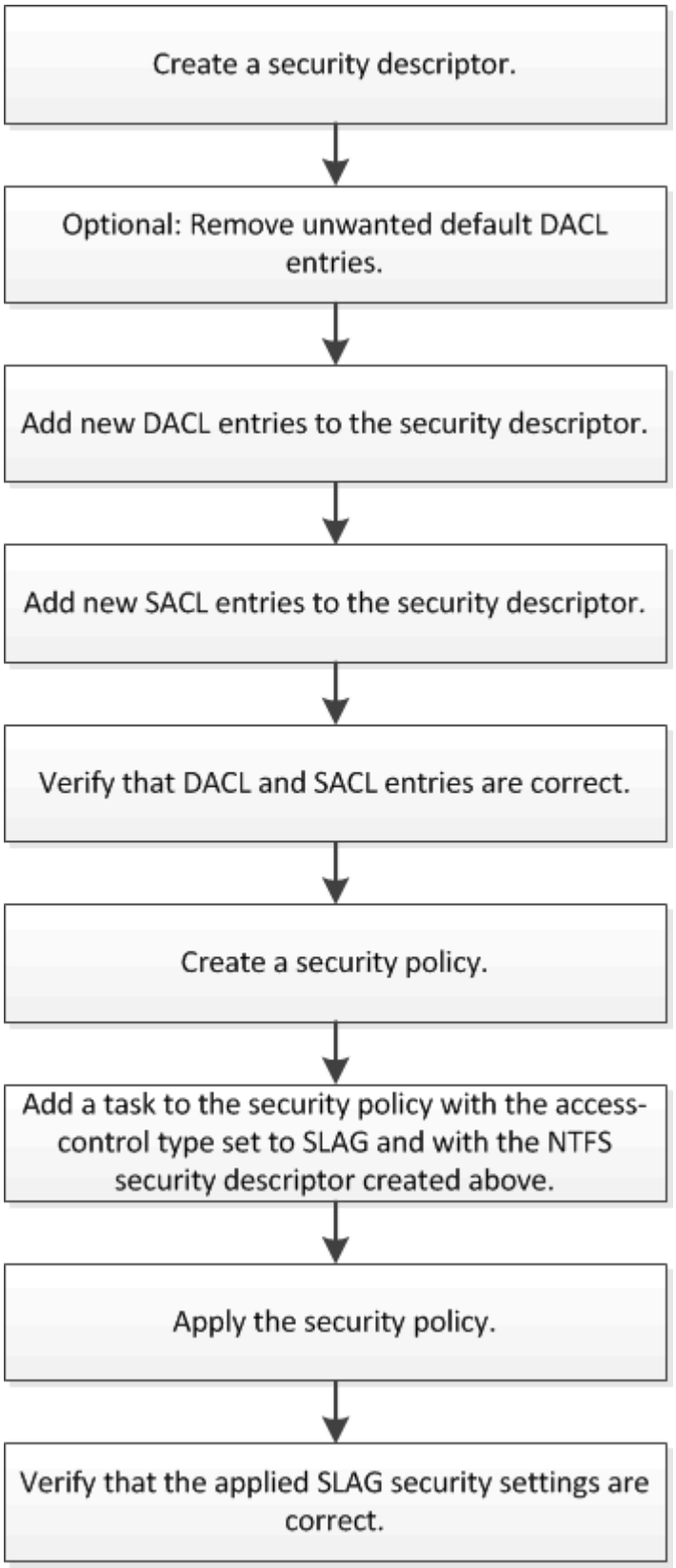
Les cas d'utilisation typiques de cette fonctionnalité sont les suivants :

- Protection de la propriété intellectuelle par l'audit et le contrôle de l'accès de tous les utilisateurs au niveau du stockage
- Stockage pour les entreprises de services financiers, y compris les services bancaires et les groupes de transactions
- Services publics avec stockage de fichiers distinct dans les différents départements
- Universités protégeant tous les fichiers des étudiants

Workflow de configuration pour Storage-Level Access Guard sur les serveurs ONTAP SMB

Le workflow de configuration de Storage-Level Access Guard (SLAG) utilise les mêmes commandes CLI de ONTAP que celles que vous utilisez pour configurer les autorisations d'accès aux fichiers NTFS et les stratégies d'audit. Au lieu de configurer l'accès aux

fichiers et aux répertoires sur une cible désignée, vous configurez LE SLAG sur le volume SVM (Storage Virtual machine) désigné.



Informations associées

Configurer Storage-Level Access Guard sur les serveurs

Configurer Storage-Level Access Guard sur les serveurs ONTAP SMB

Plusieurs étapes sont nécessaires pour configurer Storage-Level Access Guard sur un volume ou un qtree. Storage-Level Access Guard fournit un niveau de sécurité d'accès défini au niveau du stockage. Elle fournit une sécurité qui s'applique à tous les accès à partir de tous les protocoles NAS vers l'objet de stockage auquel il a été appliqué.

Étapes

1. Créez un descripteur de sécurité à l'aide du `vserver security file-directory ntfs create` commande.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Un descripteur de sécurité est créé avec les quatre entrées de contrôle d'accès DACL (ACE) suivantes :

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Si vous ne souhaitez pas utiliser les entrées par défaut lors de la configuration de Storage-Level Access Guard, vous pouvez les supprimer avant de créer et d'ajouter vos propres ACE au descripteur de sécurité.

2. Supprimez l'un des ACE DACL par défaut du descripteur de sécurité que vous ne souhaitez pas configurer avec la sécurité Storage-Level Access Guard :

a. Supprimez les ACE DACL indésirables à l'aide du `vserver security file-directory ntfs dacl remove` commande.

   Dans cet exemple, trois ACE DACL par défaut sont supprimés du descripteur de sécurité : BUILTIN\Administrators, BULTIN\Users et CRÉATEUR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Vérifiez que les ACE DACL que vous ne souhaitez pas utiliser pour la sécurité Storage-Level Access Guard sont supprimés du descripteur de sécurité à l'aide de `vserver security file-directory ntfs dacl show` commande.

   Dans cet exemple, la sortie de la commande vérifie que trois ACE DACL par défaut ont été supprimés du descripteur de sécurité, ne laissant que l'entrée ACE DACL par défaut du SYSTÈME/AUTORITÉ NT :

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Ajoutez une ou plusieurs entrées DACL à un descripteur de sécurité en utilisant le `vserver security file-directory ntfs dacl add` commande.

   Dans cet exemple, deux ACE DACL sont ajoutés au descripteur de sécurité :

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Ajoutez une ou plusieurs entrées SACL à un descripteur de sécurité à l'aide du `vserver security file-directory ntfs sacl add` commande.

   Dans cet exemple, deux ACE SACL sont ajoutés au descripteur de sécurité :

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   -access-type failure -account "example\Domain Users" -rights read -apply-to
   ```

```
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Vérifier que les ACE DACL et SACL sont correctement configurés à l'aide du `vserver security file-directory ntfs dacl show` et `vserver security file-directory ntfs sacl show` respectivement.

   Dans cet exemple, la commande suivante affiche des informations sur les entrées DACL pour le descripteur de sécurité "sd1":

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Dans cet exemple, la commande suivante affiche des informations sur les entrées SACL pour le descripteur de sécurité « `sd1' » :

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   files
   ```

6. Créez une stratégie de sécurité à l'aide de `vserver security file-directory policy create` commande.

   L'exemple suivant crée une politique nommée « politique 1 » :

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Vérifiez que la stratégie est correctement configurée à l'aide du `vserver security file-directory policy show` commande.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité en utilisant le `vserver security file-directory policy task add` commande avec `-access-control` paramètre défini sur `slag`.

   Même si une stratégie peut contenir plusieurs tâches Storage-Level Access Guard, vous ne pouvez pas configurer une stratégie pour contenir à la fois des tâches file-Directory et Storage-Level Access Guard. Une stratégie doit contenir soit toutes les tâches Storage-Level Access Guard, soit toutes les tâches du répertoire de fichiers.

   Dans cet exemple, une tâche est ajoutée à la politique nommée ""politie1"", qui est affectée au descripteur de sécurité "s1"". Il est affecté à l' `/datavol1` chemin avec le type de contrôle d'accès défini sur "`stable".

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Vérifiez que la tâche est correctement configurée à l'aide de l' `vserver security file-directory policy task show` commande.

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Appliquez la stratégie de sécurité de Storage-Level Access Guard à l'aide du `vserver security file-directory apply` commande.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    La tâche d'application de la stratégie de sécurité est planifiée.

11. Vérifiez que les paramètres de sécurité de Storage-Level Access Guard sont corrects à l'aide de l' `vserver security file-directory show` commande.

    Dans cet exemple, le résultat de la commande indique que la sécurité Storage-Level Access Guard a été appliquée au volume NTFS `/datavol1`. Bien que la DACL par défaut permettant un contrôle total à tout le monde reste, la sécurité de Storage-Level Access Guard limite (et vérifie) l'accès aux groupes définis dans les paramètres Storage-Level Access Guard.

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informations associées

- Commandes de gestion de la sécurité des fichiers NTFS, des stratégies d'audit NTFS et de Storage-Level Access Guard
- Workflow de configuration pour Storage-Level Access Guard sur les serveurs
- Afficher des informations sur Storage-Level Access Guard sur les serveurs
- Supprimer la protection d'accès au niveau du stockage sur les serveurs

Matrice SLAG efficace sur les serveurs ONTAP SMB

Vous pouvez configurer LE SCORIES sur un volume, un qtree ou les deux. La matrice DE SCORIES définit le volume ou qtree en tant que configuration SLAG applicable dans les différents scénarios répertoriés dans le tableau.

	SCORIES de volume dans un système AFS	SLAG de volume dans un snapshot	Qtree SCORIES dans un système AFS	SCORIES qtree dans un snapshot
Accès au volume dans un système de fichiers d'accès (AFS)	OUI	NON	S/O	S/O
Accès au volume dans un snapshot	OUI	NON	S/O	S/O
Accès au qtree dans un AFS (lorsque LE SCORIES est présent dans le qtree)	NON	NON	OUI	NON
Accès au qtree dans un AFS (lorsque LE SCORIES n'est pas présente dans le qtree)	OUI	NON	NON	NON
Accès qtree dans un snapshot (lorsque SLAG est présent dans le qtree AFS)	NON	NON	OUI	NON
Accès qtree dans un snapshot (lorsque SLAG n'est pas présent dans l'AFS qtree)	OUI	NON	NON	NON

Afficher des informations sur Storage-Level Access Guard sur les serveurs ONTAP SMB

La protection d'accès au niveau du stockage est une troisième couche de sécurité appliquée à un volume ou à un qtree. Les paramètres de Storage-Level Access Guard ne peuvent pas être affichés à l'aide de la fenêtre Propriétés de Windows. Vous devez utiliser l'interface de ligne de commande ONTAP pour afficher des informations sur la sécurité de Storage-Level Access Guard, que vous pouvez utiliser pour valider votre configuration ou pour résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès au volume ou qtree dont vous souhaitez afficher les informations de sécurité Storage-Level Access Guard. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

Étape

1. Afficher les paramètres de sécurité de Access Guard au niveau du stockage avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Avec détails étendus	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemples

L'exemple suivant présente les informations de sécurité Storage-Level Access Guard pour le volume de style de sécurité NTFS avec le chemin d'accès `/datavol1` Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

L’exemple suivant affiche les informations Storage-Level Access Guard sur le volume de style de sécurité mixte au niveau du chemin `/datavol5` Au SVM vs1. Le niveau supérieur de ce volume dispose d’une sécurité effective UNIX. Le volume est doté de la sécurité Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Supprimer la protection d'accès au niveau du stockage sur les serveurs SMB ONTAP

Vous pouvez supprimer Storage-Level Access Guard sur un volume ou qtree si vous ne souhaitez plus définir de sécurité d'accès au niveau du stockage. La suppression de Storage-Level Access Guard ne modifie pas ou ne supprime pas la sécurité des fichiers et répertoires NTFS standard.

Étapes

1. Vérifier que la protection d'accès au niveau du stockage est configurée à l'aide du volume ou qtree `vserver security file-directory show` commande.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Retirez le protecteur d'accès au niveau du stockage à l'aide du `vserver security file-directory remove-slag` commande.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Vérifiez que Storage-Level Access Guard a été supprimé du volume ou qtree en utilisant le `vserver security file-directory show` commande.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Gérer l’accès aux fichiers via SMB

Utilisez des utilisateurs et des groupes locaux pour l’authentification et l’autorisation

Utilisation des utilisateurs et des groupes locaux par ONTAP

En savoir plus sur les utilisateurs et les groupes SMB ONTAP locaux

Vous devez connaître les utilisateurs et les groupes locaux, ainsi que quelques informations de base à leur sujet, avant de déterminer si vous devez configurer et utiliser des utilisateurs et des groupes locaux dans votre environnement.

- **Utilisateur local**

  Un compte utilisateur avec un identifiant de sécurité unique (SID) qui n’a de visibilité que sur la machine virtuelle de stockage (SVM) sur laquelle elle est créée. Les comptes d’utilisateur locaux ont un ensemble d’attributs, y compris le nom d’utilisateur et le SID. Un compte utilisateur local s’authentifie localement sur le serveur CIFS à l’aide de l’authentification NTLM.

  Les comptes d’utilisateur ont plusieurs utilisations :

  - Permet d’accorder des privilèges *User Rights Management* à un utilisateur.
  - Permet de contrôler l’accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers détenues par la SVM.

- **Groupe local**

  Un groupe avec un SID unique n'a de visibilité que sur le SVM sur lequel il est créé. Les groupes contiennent un ensemble de membres. Les membres peuvent être des utilisateurs locaux, des utilisateurs de domaine, des groupes de domaines et des comptes de machine de domaine. Les groupes peuvent être créés, modifiés ou supprimés.

  Les groupes ont plusieurs utilisations :

  - Utilisé pour accorder des privilèges *User Rights Management* à ses membres.
  - Permet de contrôler l'accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers détenues par la SVM.
- **Domaine local**

  Domaine qui dispose de son étendue locale, limitée par le SVM. Le nom du domaine local est le nom du serveur CIFS. Les utilisateurs et groupes locaux sont contenus dans le domaine local.

- **Identificateur de sécurité (SID)**

  Un SID est une valeur numérique de longueur variable qui identifie les entités de sécurité de type Windows. Par exemple, un SID type prend le format suivant : s-1-5-21-3139654847-1303905135-2517279418-123456.

- **Authentification NTLM**

  Méthode de sécurité Microsoft Windows utilisée pour authentifier les utilisateurs sur un serveur CIFS.

- **Cluster Replicated database (RDB)**

  Base de données répliquée avec une instance sur chaque nœud d'un cluster. Les objets utilisateur et groupe locaux sont stockés dans le RDB.

Raisons de la création d'utilisateurs SMB ONTAP locaux et de groupes locaux

Il existe plusieurs raisons de créer des utilisateurs et des groupes locaux sur votre SVM (Storage Virtual machine). Par exemple, vous pouvez accéder à un serveur SMB à l'aide d'un compte d'utilisateur local si les contrôleurs de domaine (DCS) ne sont pas disponibles, vous pouvez utiliser des groupes locaux pour attribuer des privilèges ou si votre serveur SMB se trouve dans un groupe de travail.

Vous pouvez créer un ou plusieurs comptes utilisateur locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les utilisateurs de domaine ne sont pas disponibles.

  Les utilisateurs locaux sont requis dans les configurations de groupe de travail.

- Vous souhaitez pouvoir vous authentifier et vous connecter au serveur SMB si les contrôleurs de domaine ne sont pas disponibles.

  Les utilisateurs locaux peuvent s'authentifier auprès du serveur SMB en utilisant l'authentification NTLM lorsque le contrôleur de domaine est en panne, ou en cas de problèmes réseau empêchant votre serveur SMB de contacter le contrôleur de domaine.

- Vous souhaitez attribuer des privilèges *User Rights Management* à un utilisateur local.

  User Rights Management permet à un administrateur de serveurs SMB de contrôler les droits des utilisateurs et des groupes sur le SVM. Vous pouvez attribuer des privilèges à un utilisateur en lui attribuant des privilèges ou en faisant de l'utilisateur un membre d'un groupe local disposant de ces privilèges.

Vous pouvez créer un ou plusieurs groupes locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les groupes de domaines ne sont pas disponibles.

  Les groupes locaux ne sont pas requis dans les configurations de groupes de travail, mais ils peuvent être utiles pour gérer les privilèges d'accès pour les utilisateurs de groupes de travail locaux.

- Vous souhaitez contrôler l'accès aux ressources de fichiers et de dossiers à l'aide des groupes locaux pour le contrôle du partage et de l'accès aux fichiers.
- Vous souhaitez créer des groupes locaux avec des privilèges *User Rights Management* personnalisés.

  Certains groupes d'utilisateurs intégrés ont des privilèges prédéfinis. Pour attribuer un ensemble personnalisé de privilèges, vous pouvez créer un groupe local et attribuer les privilèges nécessaires à ce groupe. Vous pouvez ensuite ajouter des utilisateurs locaux, des utilisateurs de domaine et des groupes de domaines au groupe local.

Informations associées

- En savoir plus sur l'authentification des utilisateurs locaux
- Liste des privilèges pris en charge

En savoir plus sur l'authentification des utilisateurs SMB ONTAP locaux

Avant qu'un utilisateur local puisse accéder aux données sur un serveur CIFS, il doit créer une session authentifiée.

SMB étant basé sur une session, l'identité de l'utilisateur peut être déterminée une seule fois, lors de la première configuration de la session. Le serveur CIFS utilise l'authentification NTLM lors de l'authentification des utilisateurs locaux. Les fournisseurs de NTLMv1 et NTLMv2 sont tous deux pris en charge.

ONTAP utilise l'authentification locale dans trois cas d'utilisation. Chaque cas d'utilisation dépend du fait que la partie du domaine du nom d'utilisateur (au format DOMAINE\utilisateur) correspond au nom de domaine local du serveur CIFS (le nom du serveur CIFS) :

- La partie domaine correspond

  Les utilisateurs qui fournissent des informations d'identification d'utilisateur local lors de la demande d'accès aux données sont authentifiés localement sur le serveur CIFS.

- La partie du domaine ne correspond pas

  ONTAP tente d'utiliser l'authentification NTLM avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient. Si l'authentification réussit, la connexion est terminée. Si cela ne fonctionne pas, ce qui se passe ensuite dépend de la raison pour laquelle l'authentification n'a pas réussi.

  Par exemple, si l'utilisateur existe dans Active Directory mais que le mot de passe est incorrect ou expiré, ONTAP ne tente pas d'utiliser le compte d'utilisateur local correspondant sur le serveur CIFS. Au lieu de

cela, l'authentification échoue. Dans d'autres cas, ONTAP utilise le compte local correspondant sur le serveur CIFS, s'il existe, pour l'authentification, même si les noms de domaine NetBIOS ne correspondent pas. Par exemple, si un compte de domaine correspondant existe mais est désactivé, ONTAP utilise le compte local correspondant sur le serveur CIFS pour l'authentification.

- La partie domaine n'est pas spécifiée

  ONTAP tente d'abord l'authentification en tant qu'utilisateur local. Si l'authentification en tant qu'utilisateur local échoue, ONTAP authentifie l'utilisateur avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient.

Une fois l'authentification des utilisateurs locaux ou de domaine terminée, ONTAP crée un jeton d'accès complet, qui tient compte de l'appartenance et des privilèges des groupes locaux.

Pour plus d'informations sur l'authentification NTLM pour les utilisateurs locaux, consultez la documentation Microsoft Windows.

Informations associées

Activer ou désactiver l'authentification des utilisateurs locaux sur les serveurs

En savoir plus sur les jetons d'accès utilisateur ONTAP SMB

Lorsqu'un utilisateur mappe un partage, une session SMB authentifiée est établie et un jeton d'accès utilisateur est construit qui contient des informations sur l'utilisateur, l'appartenance au groupe de l'utilisateur et les privilèges cumulatifs, ainsi que l'utilisateur UNIX mappé.

À moins que la fonctionnalité ne soit désactivée, les informations d'utilisateur et de groupe locaux sont également ajoutées au jeton d'accès utilisateur. La manière dont les jetons d'accès sont créés dépend de la manière dont la connexion est destinée à un utilisateur local ou à un utilisateur de domaine Active Directory :

- Connexion de l'utilisateur local

  Bien que les utilisateurs locaux puissent être membres de groupes locaux différents, les groupes locaux ne peuvent pas être membres d'autres groupes locaux. Le jeton d'accès utilisateur local se compose d'une Union de tous les privilèges attribués aux groupes auxquels un utilisateur local particulier est membre.

- Connexion utilisateur du domaine

  Lorsqu'un utilisateur de domaine se connecte, ONTAP obtient un jeton d'accès utilisateur contenant le SID de l'utilisateur et les SID pour tous les groupes de domaine auxquels l'utilisateur est membre. ONTAP utilise l'Union du jeton d'accès d'utilisateur du domaine avec le jeton d'accès fourni par les membres locaux des groupes de domaine de l'utilisateur (le cas échéant), ainsi que tout privilège direct attribué à l'utilisateur du domaine ou à l'un de ses membres de groupe de domaine.

Pour les connexions utilisateur locales et de domaine, le GROUPE principal RID est également défini pour le jeton d'accès utilisateur. Le RID par défaut est `Domain Users` (RID 513). Vous ne pouvez pas modifier la valeur par défaut.

Le processus de mappage de noms Windows-to-UNIX et UNIX-to-Windows suit les mêmes règles pour les comptes locaux et de domaine.

Il n'y a pas de mappage automatique implicite d'un utilisateur UNIX vers un compte local. Si cela est nécessaire, une règle de mappage explicite doit être spécifiée à l'aide des commandes de mappage de noms existantes.

En savoir plus sur l'utilisation de SnapMirror sur les SVM SMB ONTAP contenant des groupes locaux

Notez les instructions lorsque vous configurez SnapMirror sur des volumes appartenant aux SVM contenant des groupes locaux.

Vous ne pouvez pas utiliser des groupes locaux dans des ACE appliqués à des fichiers, des répertoires ou des partages qui sont répliqués par SnapMirror vers une autre SVM. Si vous utilisez la fonctionnalité SnapMirror pour créer un miroir de reprise sur incident sur un volume situé sur un autre SVM et que le volume dispose d'une version ACE pour un groupe local, l'ACE n'est pas valide pour le miroir. Si les données sont répliquées sur un autre SVM, celles-ci se croisent efficacement et un autre domaine local. Les autorisations accordées aux utilisateurs et groupes locaux ne sont valides qu'au sein du périmètre de la SVM sur lequel ils ont été créés.

Découvrez les effets de la suppression des serveurs ONTAP SMB sur les utilisateurs et les groupes

L'ensemble par défaut des utilisateurs et groupes locaux est créé lors de la création d'un serveur CIFS et ils sont associés au serveur virtuel de stockage (SVM) qui héberge le serveur CIFS. Les administrateurs SVM peuvent créer à tout moment des utilisateurs et groupes locaux. Lorsque vous supprimez le serveur CIFS, vous devez connaître ce qui arrive aux utilisateurs et aux groupes locaux.

Les utilisateurs et groupes locaux sont associés à des SVM ; ils ne sont donc pas supprimés lorsque des serveurs CIFS sont supprimés pour des raisons de sécurité. Bien que les utilisateurs et groupes locaux ne soient pas supprimés lors de la suppression du serveur CIFS, ils sont masqués. Vous ne pouvez ni afficher ni gérer des utilisateurs et groupes locaux tant que vous n'avez pas recréés un serveur CIFS sur la SVM.

L'état d'administration du serveur CIFS n'affecte pas la visibilité des utilisateurs ou des groupes locaux.

Découvrez comment utiliser la console de gestion Microsoft avec les utilisateurs et groupes SMB ONTAP locaux

Vous pouvez afficher des informations sur les utilisateurs et groupes locaux à partir de la console de gestion Microsoft. Avec cette version de ONTAP, vous ne pouvez pas effectuer d'autres tâches de gestion pour les utilisateurs et groupes locaux à partir de la console de gestion Microsoft.

En savoir plus sur la restauration des clusters SMB ONTAP

Si vous prévoyez de restaurer le cluster à une version de ONTAP qui ne prend pas en charge les utilisateurs et groupes locaux, ainsi que les utilisateurs et groupes locaux utilisés pour gérer l'accès aux fichiers ou les droits des utilisateurs, vous devez tenir compte de certaines considérations.

- Pour des raisons de sécurité, les informations concernant les utilisateurs, groupes et privilèges locaux configurés ne sont pas supprimées lorsque ONTAP est rétabli sur une version qui ne prend pas en charge

les fonctionnalités des utilisateurs et des groupes locaux.

- Lors de la restauration d'une version majeure antérieure de ONTAP, ONTAP n'utilise pas d'utilisateurs et de groupes locaux pendant l'authentification et la création des informations d'identification.
- Les utilisateurs et groupes locaux ne sont pas supprimés des listes de contrôle d'accès aux fichiers et aux dossiers.
- Les demandes d'accès aux fichiers qui dépendent de l'accès sont refusées en raison des autorisations accordées aux utilisateurs ou groupes locaux.

  Pour autoriser l'accès, vous devez reconfigurer les autorisations d'accès aux fichiers afin d'autoriser l'accès en fonction des objets de domaine au lieu d'objets d'utilisateur et de groupe locaux.

Quels sont les privilèges locaux

Liste des privilèges SMB ONTAP pris en charge

ONTAP dispose d'un ensemble prédéfini de privilèges pris en charge. Certains groupes locaux prédéfinis ont certains de ces privilèges ajoutés par défaut. Vous pouvez également ajouter ou supprimer des privilèges des groupes prédéfinis ou créer de nouveaux utilisateurs ou groupes locaux et ajouter des privilèges aux groupes que vous avez créés ou aux utilisateurs et groupes de domaine existants.

Le tableau ci-dessous répertorie les privilèges pris en charge sur la machine virtuelle de stockage (SVM) et fournit la liste des groupes BUILTIN avec des privilèges attribués :

Nom de privilège	Paramètre de sécurité par défaut	Description
`SeTcbPrivilege`	Aucune	Faire partie du système d'exploitation
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Sauvegardez des fichiers et des répertoires, en remplaçant les listes de contrôle d'accès
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restaurez les fichiers et les répertoires, en remplaçant les listes de contrôle d'accès, définissez tout ID utilisateur ou groupe valide comme propriétaire du fichier
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Prendre possession de fichiers ou d'autres objets
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gérer les audits Cela inclut l'affichage, le vidage et l'effacement du journal de sécurité.

Nom de privilège	Paramètre de sécurité par défaut	Description
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Vérification de la traverse de dérivation Les utilisateurs disposant de ce privilège ne sont pas tenus d'avoir des autorisations traverse (x) pour traverser des dossiers, des liens symboliques ou des jonctions.

Informations associées

- En savoir plus sur l'attribution de privilèges
- En savoir plus sur la configuration de la vérification de contournement

En savoir plus sur l'attribution des privilèges SMB ONTAP

Vous pouvez attribuer des privilèges directement aux utilisateurs locaux ou aux utilisateurs du domaine. Vous pouvez également affecter des utilisateurs à des groupes locaux dont les privilèges attribués correspondent aux fonctions que vous souhaitez que ces utilisateurs disposent.

- Vous pouvez attribuer un ensemble de privilèges à un groupe que vous créez.

  Vous ajoutez ensuite un utilisateur au groupe disposant des privilèges que vous souhaitez que cet utilisateur dispose.

- Vous pouvez également attribuer des utilisateurs locaux et des utilisateurs de domaine à des groupes prédéfinis dont les privilèges par défaut correspondent aux privilèges que vous souhaitez accorder à ces utilisateurs.

Informations associées

- Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine
- Supprimez les privilèges des utilisateurs ou groupes locaux ou de domaine
- Réinitialisez les privilèges pour les utilisateurs et les groupes locaux ou de domaine
- En savoir plus sur la configuration de la vérification de contournement

En savoir plus sur les groupes BUILTIN et les comptes d'administrateur local sur les serveurs ONTAP SMB

Il y a certaines directives que vous devez garder à l'esprit lorsque vous utilisez les groupes BULTIN et le compte d'administrateur local. Par exemple, vous pouvez renommer le compte d'administrateur local, mais vous ne pouvez pas supprimer ce compte.

- Le compte Administrateur peut être renommé mais ne peut pas être supprimé.
- Le compte Administrateur ne peut pas être supprimé du groupe BULTIN\Administrators.
- Les groupes INTÉGRÉS peuvent être renommés mais ne peuvent pas être supprimés.

  Une fois le groupe BUILTIN renommé, un autre objet local peut être créé avec le nom connu ; cependant,

l'objet est affecté à un nouveau RID.

- Il n'y a pas de compte invité local.

Informations associées

Groupes et privilèges par défaut prédéfinis BUILTIN

Exigences relatives aux mots de passe des utilisateurs SMB ONTAP locaux

Par défaut, les mots de passe des utilisateurs locaux doivent répondre aux exigences de complexité. Les exigences de complexité des mots de passe sont similaires aux exigences définies dans la stratégie de sécurité Microsoft Windows *local*.

Le mot de passe doit répondre aux critères suivants :

- Doit comporter au moins six caractères
- Ne doit pas contenir le nom du compte d'utilisateur
- Doit contenir des caractères d'au moins trois des quatre catégories suivantes :
  - Caractères majuscules anglais (A à Z)
  - Caractères anglais minuscules (a à z)
  - Chiffres de base 10 (0 à 9)
  - Caractères spéciaux :

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Informations associées

- Configurer la complexité du mot de passe pour les utilisateurs locaux
- Afficher des informations sur les paramètres de sécurité du serveur
- Modifier les mots de passe des comptes utilisateur locaux

Groupes BUILTIN prédéfinis et privilèges ONTAP SMB par défaut

Vous pouvez affecter l'appartenance d'un utilisateur local ou d'un utilisateur de domaine à un ensemble prédéfini de groupes BUILTIN fourni par ONTAP. Les groupes prédéfinis ont des privilèges prédéfinis attribués.

Le tableau suivant décrit les groupes prédéfinis :

Groupe prédéfini BUILTIN	Privilèges par défaut
`BUILTIN\Administrators`RID 544 Lors de sa création initiale, le local `Administrator` Compte, avec UN RID de 500, est automatiquement fait membre de ce groupe. Lorsque l'ordinateur virtuel de stockage (SVM) est rejoint un domaine, le `domain\Domain Admins` le groupe est ajouté au groupe. Si le SVM laisse le domaine, le `domain\Domain Admins` le groupe est supprimé du groupe.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 Lors de sa création initiale, ce groupe n'a aucun membre. Les membres de ce groupe ont les caractéristiques suivantes : • Peut créer et gérer des utilisateurs et des groupes locaux. • Impossible d'ajouter eux-mêmes ou tout autre objet au `BUILTIN\Administrators` groupe.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Lors de sa création initiale, ce groupe n'a aucun membre. Les membres de ce groupe peuvent remplacer les autorisations de lecture et d'écriture sur des fichiers ou des dossiers s'ils sont ouverts avec l'intention de sauvegarde.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Lors de sa création initiale, ce groupe n'a pas de membres (outre les membres implicites) `Authenticated Users` groupe spécial). Lorsque le SVM est joint à un domaine, le `domain\Domain Users` le groupe est ajouté à ce groupe. Si le SVM laisse le domaine, le `domain\Domain Users` le groupe est supprimé de ce groupe.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Ce groupe inclut tous les utilisateurs, y compris les invités (mais pas les utilisateurs anonymes). Il s'agit d'un groupe implicite avec une adhésion implicite.	`SeChangeNotifyPrivilege`

Informations associées

- En savoir plus sur les groupes BUILTIN et les comptes d'administrateur local sur les serveurs

- Liste des privilèges pris en charge
- En savoir plus sur la configuration de la vérification de contournement

Activez ou désactivez la fonctionnalité utilisateurs et groupes locaux

En savoir plus sur les fonctionnalités des utilisateurs et des groupes SMB ONTAP locaux

Avant de pouvoir utiliser des utilisateurs et des groupes locaux pour contrôler l'accès aux données de style de sécurité NTFS, les fonctionnalités d'utilisateur et de groupe locaux doivent être activées. En outre, si vous souhaitez utiliser des utilisateurs locaux pour l'authentification SMB, la fonctionnalité d'authentification des utilisateurs locaux doit être activée.

Les fonctionnalités des utilisateurs et groupes locaux et l'authentification des utilisateurs locaux sont activées par défaut. Si elles ne sont pas activées, vous devez les activer avant de pouvoir configurer et utiliser des utilisateurs et des groupes locaux. Vous pouvez désactiver les fonctionnalités des utilisateurs et groupes locaux à tout moment.

En plus de désactiver explicitement la fonctionnalité des utilisateurs et groupes locaux, ONTAP désactive les fonctionnalités utilisateur et groupe locaux si un nœud du cluster est rétabli sur une version de ONTAP qui ne prend pas en charge cette fonctionnalité. Les fonctionnalités des utilisateurs et groupes locaux ne sont pas activées tant que tous les nœuds du cluster n'exécutent pas une version de ONTAP qui le prend en charge.

Informations associées

- Modifier les comptes utilisateur locaux
- Modifier les groupes locaux
- Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine

Activer ou désactiver les utilisateurs et groupes locaux sur les serveurs ONTAP SMB

Vous pouvez activer ou désactiver les utilisateurs et groupes locaux pour l'accès SMB sur des SVM (Storage Virtual machines). La fonctionnalité utilisateurs et groupes locaux est activée par défaut.

Description de la tâche

Vous pouvez utiliser des utilisateurs et des groupes locaux lors de la configuration des autorisations de partage SMB et de fichiers NTFS et, éventuellement, utiliser des utilisateurs locaux pour l'authentification lors de la création d'une connexion SMB. Pour utiliser les utilisateurs locaux pour l'authentification, vous devez également activer l'option d'authentification des utilisateurs et groupes locaux.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que les utilisateurs et les groupes locaux soient…	Entrez la commande…
Activé	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true`
Désactivé	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant permet aux utilisateurs et groupes locaux de la fonctionnalité sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Informations associées

- Activer ou désactiver l'authentification des utilisateurs locaux sur les serveurs
- Activez ou désactivez les comptes utilisateur locaux

Activer ou désactiver l'authentification des utilisateurs locaux sur les serveurs ONTAP SMB

Vous pouvez activer ou désactiver l'authentification des utilisateurs locaux pour l'accès SMB sur des SVM (Storage Virtual machines). La valeur par défaut est d'autoriser l'authentification des utilisateurs locaux, ce qui est utile lorsque la SVM ne peut pas contacter un contrôleur de domaine ou si vous choisissez de ne pas utiliser de contrôles d'accès au niveau des domaines.

Avant de commencer

La fonctionnalité utilisateurs et groupes locaux doit être activée sur le serveur CIFS.

Description de la tâche

Vous pouvez activer ou désactiver l'authentification des utilisateurs locaux à tout moment. Si vous souhaitez utiliser des utilisateurs locaux pour l'authentification lors de la création d'une connexion SMB, vous devez également activer l'option utilisateurs et groupes locaux du serveur CIFS.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que l'authentification locale soit…	Entrez la commande…
Activé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Désactivé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant active l'authentification utilisateur local sur le SVM vs1 :

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Informations associées

- En savoir plus sur l'authentification des utilisateurs locaux
- Activer ou désactiver les utilisateurs et groupes locaux sur les serveurs

Gérez les comptes utilisateurs locaux

Modifier les comptes utilisateurs SMB ONTAP locaux

Vous pouvez modifier un compte d'utilisateur local si vous souhaitez modifier le nom complet ou la description d'un utilisateur existant et si vous souhaitez activer ou désactiver le compte d'utilisateur. Vous pouvez également renommer un compte d'utilisateur local si le nom de l'utilisateur est compromis ou si un changement de nom est nécessaire à des fins administratives.

Les fonctions que vous recherchez…	Entrez la commande…
Modifier le nom complet de l'utilisateur local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-full-name text` Si le nom complet contient un espace, il doit être placé entre guillemets.
Modifier la description de l'utilisateur local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-description text` Si la description contient un espace, elle doit être placée entre guillemets.
Activez ou désactivez le compte utilisateur local	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	Renommez le compte d'utilisateur local

Exemple

L'exemple suivant renomme l'utilisateur local « CIFS_SERVER\sue » en « CIFS_SERVER\sue_New » sur la machine virtuelle de stockage (SVM, précédemment appelé vServer) vs1 :

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Activer ou désactiver les comptes d'utilisateurs SMB ONTAP locaux

Vous activez un compte utilisateur local si vous souhaitez que l'utilisateur puisse accéder aux données contenues dans la machine virtuelle de stockage (SVM) via une connexion SMB. Vous pouvez également désactiver un compte utilisateur local si vous ne souhaitez pas que cet utilisateur accède aux données des SVM via SMB.

Description de la tâche

Vous activez un utilisateur local en modifiant le compte utilisateur.

Étape

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Entrez la commande…
Activez le compte utilisateur	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`

Les fonctions que vous recherchez…	Entrez la commande…
Désactivez le compte utilisateur	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

Modifier les mots de passe des comptes utilisateurs SMB ONTAP locaux

Vous pouvez modifier le mot de passe du compte d'un utilisateur local. Cela peut être utile si le mot de passe de l'utilisateur est compromis ou si l'utilisateur a oublié le mot de passe.

Étape

1. Modifiez le mot de passe en effectuant l'action appropriée : `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Exemple

L'exemple suivant définit le mot de passe pour l'utilisateur local « CIFS_SERVER\sue » associé à une machine virtuelle de stockage (SVM, anciennement Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Informations associées

Configurer la complexité du mot de passe pour les utilisateurs locaux

Afficher des informations sur les paramètres de sécurité du serveur

Afficher des informations sur les utilisateurs locaux ONTAP SMB

Vous pouvez afficher une liste de tous les utilisateurs locaux sous forme de résumé. Si vous souhaitez déterminer les paramètres de compte configurés pour un utilisateur spécifique, vous pouvez afficher des informations détaillées sur le compte de cet utilisateur ainsi que les informations sur le compte de plusieurs utilisateurs. Ces informations peuvent vous aider à déterminer si vous devez modifier les paramètres d'un utilisateur et à résoudre les problèmes d'authentification ou d'accès aux fichiers.

Description de la tâche

Les informations relatives au mot de passe d'un utilisateur ne s'affichent jamais.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Affichage des informations relatives à tous les utilisateurs sur la machine virtuelle de stockage (SVM)	`vserver cifs users-and-groups local-user show -vserver vserver_name`
Affiche des informations détaillées sur le compte d'un utilisateur	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de la commande. Pour en savoir plus, `vserver cifs` consultez le "Référence de commande ONTAP".

Exemple

L'exemple suivant affiche les informations relatives à tous les utilisateurs locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

Afficher des informations sur les appartenances aux groupes SMB ONTAP pour les utilisateurs locaux

Vous pouvez afficher des informations sur les groupes locaux auxquels un utilisateur local appartient. Vous pouvez utiliser ces informations pour déterminer l'accès que l'utilisateur doit avoir aux fichiers et dossiers. Ces informations peuvent être utiles pour déterminer les droits d'accès que l'utilisateur doit posséder aux fichiers et dossiers ou pour résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous pouvez personnaliser la commande pour afficher uniquement les informations que vous souhaitez afficher.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Afficher les informations d'appartenance des utilisateurs locaux pour un utilisateur local spécifié	`vserver cifs users-and-groups local-user show-membership -user-name user_name`

Les fonctions que vous recherchez…	Entrez la commande…
Affiche les informations d'appartenance de l'utilisateur local pour le groupe local dont cet utilisateur local est membre	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Afficher les informations d'appartenance des utilisateurs aux utilisateurs locaux associés à une machine virtuelle de stockage (SVM) spécifiée	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Affiche des informations détaillées pour tous les utilisateurs locaux sur un SVM spécifié	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche les informations d'appartenance de tous les utilisateurs locaux sur le SVM vs1 ; l'utilisateur « CIFS_SERVER\Administrator » est membre du groupe « BUILTIN\Administrators » et « CIFS_SERVER\sue » est membre du groupe « CIFS_SERVER\g1 » :

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Supprimer les comptes utilisateurs SMB ONTAP locaux

Vous pouvez supprimer des comptes utilisateurs locaux de votre machine virtuelle de stockage (SVM) s'ils ne sont plus nécessaires pour l'authentification SMB locale sur le serveur CIFS ou pour déterminer les droits d'accès aux données contenues dans votre SVM.

Description de la tâche

Tenez compte des points suivants lors de la suppression d'utilisateurs locaux :

- Le système de fichiers n'est pas modifié.

  Les descripteurs de sécurité Windows sur les fichiers et les répertoires qui font référence à cet utilisateur ne sont pas ajustés.

- Toutes les références aux utilisateurs locaux sont supprimées des bases de données d'appartenance et de privilèges.
- Les utilisateurs standard bien connus tels que Administrateur ne peuvent pas être supprimés.

Étapes

1. Déterminez le nom du compte d'utilisateur local que vous souhaitez supprimer : `vserver cifs users-`

`and-groups local-user show -vserver vserver_name`

2. Supprimez l'utilisateur local : `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Vérifiez que le compte utilisateur est supprimé : `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemple

L'exemple suivant supprime l'utilisateur local « CIFS_SERVER\sue » associé à la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
```

Gérez des groupes locaux

Modifier les groupes SMB ONTAP locaux

Vous pouvez modifier les groupes locaux existants en modifiant la description d'un groupe local existant ou en renommant ce groupe.

Les fonctions que vous recherchez…	Utilisez la commande…
Modifier la description du groupe local	`vserver cifs users-and-groups local-group modify -vserver vserver_name -group-name group_name -description text` Si la description contient un espace, elle doit être placée entre guillemets.
Renommer le groupe local	`vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name`

Exemples

L'exemple suivant renomme le groupe local « CIFS_SERVER\engineering » en « CIFS_SERVER\engineering_New » :

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

L'exemple suivant modifie la description du groupe local « CIFS_SERVER\engineering » :

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Afficher des informations sur les groupes locaux ONTAP SMB

Vous pouvez afficher la liste de tous les groupes locaux configurés sur le cluster ou sur une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent être utiles pour résoudre les problèmes d'accès aux fichiers aux données contenues dans la SVM ou sur les problèmes liés aux droits d'utilisateur (privilège) sur la SVM.

Étape

1. Effectuez l'une des opérations suivantes :

Pour obtenir des informations sur…	Entrez la commande…
Tous les groupes locaux du cluster	`vserver cifs users-and-groups local-group show`
Tous les groupes locaux sur le SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de cette commande. Pour en savoir plus, `vserver cifs` consultez le "Référence de commande ONTAP".

Exemple

L'exemple suivant affiche les informations sur tous les groupes locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gérez l'appartenance au groupe SMB ONTAP local

Vous pouvez gérer l'appartenance à un groupe local en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et supprimant des groupes de domaines. Ceci est utile si vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe.

Description de la tâche

Directives pour l'ajout de membres à un groupe local :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial *Everyone*.
- Le groupe local doit exister avant de pouvoir y ajouter un utilisateur.
- L'utilisateur doit exister avant de pouvoir ajouter l'utilisateur à un groupe local.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, Data ONTAP doit pouvoir résoudre le nom en SID.

Directives pour le retrait de membres d'un groupe local :

- Vous ne pouvez pas supprimer des membres du groupe spécial *Everyone*.
- Le groupe dont vous souhaitez supprimer un membre doit exister.
- ONTAP doit pouvoir résoudre les noms des membres que vous souhaitez supprimer du groupe vers un SID correspondant.

Étape

1. Ajouter ou supprimer un membre d'un groupe.

Les fonctions que vous recherchez…	Utilisez ensuite la commande…
Ajouter un membre à un groupe	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à ajouter au groupe local spécifié.
Supprimer un membre d'un groupe	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à supprimer du groupe local spécifié.

L'exemple suivant ajoute un utilisateur local « `SMB_SERVER\sue` » et un groupe de domaine « AD_DOM\dom_eng »au groupe local « `SMB_SERVER\engineering' » sur la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

L'exemple suivant supprime les utilisateurs locaux « `SMB_SERVER\sue` » et « `SMB_SERVER\james` du groupe local « `SMB_SERVER\engineering' » sur la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informations associées

Affiche des informations sur les membres des groupes locaux

Afficher les informations ONTAP SMB sur les membres des groupes locaux

Vous pouvez afficher la liste de tous les membres des groupes locaux configurés sur le cluster ou sur une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent être utiles pour résoudre les problèmes d'accès aux fichiers ou de droits d'utilisateur (privilèges).

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur…	Entrez la commande…
Membres de tous les groupes locaux du cluster	`vserver cifs users-and-groups local-group show-members`
Membres de tous les groupes locaux sur le SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche les informations sur les membres de tous les groupes locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Supprimer les groupes SMB ONTAP locaux

Vous pouvez supprimer un groupe local de la machine virtuelle de stockage (SVM) s'il n'est plus nécessaire pour déterminer les droits d'accès aux données associées à ce SVM ou s'il n'est plus nécessaire d'attribuer des droits d'utilisateur de SVM (privilèges) aux membres du groupe.

Description de la tâche

Lors de la suppression de groupes locaux, tenez compte des points suivants :

- Le système de fichiers n'est pas modifié.

  Les descripteurs de sécurité Windows sur les fichiers et les répertoires faisant référence à ce groupe ne sont pas ajustés.

- Si le groupe n'existe pas, une erreur est renvoyée.
- Le groupe *Everyone* spécial ne peut pas être supprimé.
- Les groupes intégrés tels que *BUILTIN\Administrators BUILTIN\Users* ne peuvent pas être supprimés.

Étapes

1. Déterminer le nom du groupe local que vous souhaitez supprimer en affichant la liste des groupes locaux sur la SVM : `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Supprimez le groupe local : `vserver cifs users-and-groups local-group delete -vserver`

vserver_name -group-name *group_name*

3. Vérifiez que le groupe est supprimé : `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemple

L'exemple suivant supprime le groupe local « CIFS_SERVER\sales » associé à la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Mettre à jour les noms d'utilisateurs et de groupes du domaine SMB ONTAP dans les bases de données locales

Vous pouvez ajouter des utilisateurs et des groupes de domaine aux groupes locaux d'un serveur CIFS. Ces objets de domaine sont enregistrés dans des bases de données locales sur le cluster. Si un objet domaine est renommé, les bases de données locales doivent être mises à jour manuellement.

Description de la tâche

On doit préciser le nom de la machine virtuelle de stockage (SVM) sur laquelle vous souhaitez mettre à jour les noms de domaine.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'action appropriée :

Si vous souhaitez mettre à jour les utilisateurs et les groupes du domaine et…	Utilisez cette commande…
Affiche les utilisateurs et groupes du domaine mis à jour avec succès et dont la mise à jour a échoué	`vserver cifs users-and-groups update-names -vserver vserver_name`
Afficher les utilisateurs et groupes du domaine mis à jour avec succès	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Afficher uniquement les utilisateurs et les groupes du domaine qui n'ont pas été mis à jour	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Supprimez toutes les informations d'état concernant les mises à jour	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant met à jour les noms des utilisateurs et groupes de domaine associés à la machine virtuelle de stockage (SVM, anciennement Vserver) vs1. Pour la dernière mise à jour, une chaîne de noms dépendante doit être mise à jour :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Gérer les privilèges locaux

Ajouter des privilèges aux utilisateurs ou groupes locaux ou de domaine ONTAP SMB

Vous pouvez gérer les droits d'utilisateur pour les utilisateurs ou groupes locaux ou de domaine en ajoutant des privilèges. Les privilèges ajoutés remplacent les privilèges par défaut attribués à l'un de ces objets. Cela vous permet de renforcer la sécurité en vous permettant de personnaliser les privilèges d'un utilisateur ou d'un groupe.

Avant de commencer

L'utilisateur ou le groupe local ou de domaine auquel les privilèges seront ajoutés doit déjà exister.

Description de la tâche

L'ajout d'un privilège à un objet remplace les privilèges par défaut pour cet utilisateur ou ce groupe. L'ajout d'un privilège ne supprime pas les privilèges précédemment ajoutés.

Lorsque vous ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine, vous devez garder à l'esprit les éléments suivants :

- Vous pouvez ajouter un ou plusieurs privilèges.
- Lors de l'ajout de privilèges à un utilisateur ou à un groupe de domaine, ONTAP peut valider l'utilisateur ou le groupe du domaine en contactant le contrôleur de domaine.

  La commande peut échouer si ONTAP n'est pas en mesure de contacter le contrôleur de domaine.

Étapes

1. Ajoutez un ou plusieurs privilèges à un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or -group-name name -privileges _privilege_[,...]`
2. Vérifiez que les privilèges souhaités sont appliqués à l'objet : `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemple

L'exemple suivant ajoute les privilèges « `Enregistrer TcbPrivilege' » et « `Enregistrer OwnershipPrivilege » à l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

Supprimer les privilèges des utilisateurs ou groupes locaux ou de domaine ONTAP SMB

Vous pouvez gérer les droits d'utilisateur pour les utilisateurs ou groupes locaux ou de

domaine en supprimant les privilèges. Cela vous permet de renforcer la sécurité en vous permettant de personnaliser le nombre maximal de privilèges dont disposent les utilisateurs et les groupes.

Avant de commencer

L'utilisateur ou le groupe local ou de domaine dont les privilèges seront supprimés doit déjà exister.

Description de la tâche

Vous devez garder à l'esprit les éléments suivants lorsque vous supprimez des privilèges des utilisateurs ou groupes locaux ou de domaine :

- Vous pouvez supprimer un ou plusieurs privilèges.
- Lors de la suppression de privilèges d'un utilisateur ou d'un groupe de domaines, ONTAP peut valider l'utilisateur ou le groupe de domaines en contactant le contrôleur de domaine.

  La commande peut échouer si ONTAP n'est pas en mesure de contacter le contrôleur de domaine.

Étapes

1. Supprimer un ou plusieurs privilèges d'un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or -group-name _name_ -privileges _privilege_[,...]`
2. Vérifiez que les privilèges souhaités ont été supprimés de l'objet : `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemple

L'exemple suivant supprime les privilèges « `Enregistrer TcbPrivilege' » et « `Saba OwnershipPrivilege » de l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue      -
```

Réinitialiser les privilèges des utilisateurs et groupes locaux ou de domaine ONTAP SMB

Vous pouvez réinitialiser les privilèges des utilisateurs et groupes locaux ou de domaine.

Cela peut s'avérer utile lorsque vous avez apporté des modifications aux privilèges d'un utilisateur ou d'un groupe local ou de domaine et que ces modifications ne sont plus nécessaires ou souhaitées.

Description de la tâche

La réinitialisation des privilèges d'un utilisateur ou groupe local ou de domaine supprime toutes les entrées de privilèges de cet objet.

Étapes

1. Réinitialisez les privilèges sur un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. Vérifiez que les privilèges sont réinitialisés sur l'objet : `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemples

L'exemple suivant réinitialise les privilèges de l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, anciennement appelée Vserver) vs1. Par défaut, les utilisateurs normaux ne disposent pas de privilèges associés à leurs comptes :

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

L'exemple suivant réinitialise les privilèges du groupe « BUILTIN\Administrators », supprimant ainsi l'entrée de privilège :

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Afficher des informations sur les remplacements de privilèges SMB ONTAP

Vous pouvez afficher des informations sur les privilèges personnalisés attribués à des comptes ou groupes d'utilisateurs locaux ou de domaine. Ces informations vous aident à déterminer si les droits d'utilisateur souhaités sont appliqués.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur…	Entrez cette commande…
Privilèges personnalisés pour tous les utilisateurs et groupes locaux et du domaine sur la machine virtuelle de stockage (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Privilèges personnalisés pour un domaine spécifique ou un utilisateur et groupe local sur le SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de cette commande. Pour en savoir plus, `vserver cifs users-and-groups privilege show` consultez le "Référence de commande ONTAP".

Exemple

La commande suivante affiche tous les privilèges explicitement associés aux utilisateurs et groupes locaux ou de domaine pour le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------  --------------------   ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configurer la vérification de la traverse de dérivation

En savoir plus sur la configuration de la vérification de contournement de traversée ONTAP SMB

La vérification du contournement de la traverse est un droit utilisateur (également appelé *Privilege*) qui détermine si un utilisateur peut traverser tous les répertoires du chemin d'accès à un fichier, même si l'utilisateur ne dispose pas des autorisations sur le répertoire de parcours. Vous devez comprendre ce qui se passe lors de l'autorisation ou de la désautorisation de la vérification transversale et comment configurer la vérification de dérivation pour les utilisateurs sur les machines virtuelles de stockage (SVM).

Que se passe-t-il lors de l'autorisation ou de la désautorisation du contrôle de la traverse de dérivation

- Si l'accès est autorisé, lorsqu'un utilisateur tente d'accéder à un fichier, ONTAP ne vérifie pas l'autorisation traverse pour les répertoires intermédiaires lorsqu'il détermine s'il faut accorder ou refuser l'accès au fichier.
- S'il n'est pas autorisé, ONTAP vérifie l'autorisation traverse (exécution) pour tous les répertoires du chemin d'accès au fichier.

  Si l'un des répertoires intermédiaires ne dispose pas de l'autorisation « X » (traverse), ONTAP refuse l'accès au fichier.

Configurer la vérification de la traverse de dérivation

Vous pouvez configurer la vérification de contournement via l'interface de ligne de commande ONTAP ou en configurant des règles de groupe Active Directory avec ce droit d'utilisateur.

Le `SeChangeNotifyPrivilege` privilège contrôle si les utilisateurs sont autorisés à contourner la vérification transversale.

- L'ajout aux utilisateurs ou groupes SMB locaux sur le SVM, ou aux utilisateurs ou groupes de domaine permet de contourner la vérification transversale.
- L'élimination de ce groupe ou des utilisateurs SMB locaux sur le SVM, ou des utilisateurs ou groupes de domaine permet de contourner la vérification des traversent.

Par défaut, les groupes BUILTIN suivants sur le SVM ont le droit de contourner le contrôle de la traverse :

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`

- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Si vous ne souhaitez pas autoriser les membres de l'un de ces groupes à contourner la vérification de la traverse, vous devez supprimer ce privilège du groupe.

Lors de la configuration de la vérification de dérivation des utilisateurs et groupes SMB locaux sur le SVM, il faut garder ce qui suit à l'aide de l'interface de ligne de commande :

- Si vous souhaitez autoriser les membres d'un groupe local ou de domaine personnalisé à contourner la vérification transversale, vous devez ajouter le `SeChangeNotifyPrivilege` privilège de ce groupe.
- Si vous souhaitez autoriser un utilisateur local ou de domaine individuel à contourner la vérification de la traverse et que cet utilisateur n'est pas membre d'un groupe avec ce privilège, vous pouvez ajouter `SeChangeNotifyPrivilege` privilège de ce compte utilisateur.
- Vous pouvez désactiver la vérification de contournement pour les utilisateurs ou groupes locaux ou de domaine en supprimant le `SeChangeNotifyPrivilege` privilège à tout moment.

> Pour désactiver la vérification des trvers de contournement pour les utilisateurs ou groupes locaux ou de domaine spécifiés, vous devez également supprimer le `SeChangeNotifyPrivilege` privilège du `Everyone` groupe.

Informations associées

- Permet aux utilisateurs ou aux groupes de contourner la vérification de la traverse du répertoire
- Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire
- Configurer le mappage de caractères pour la traduction des noms de fichiers sur les volumes
- Créer des listes de contrôle d'accès aux partages
- Sécurisez l'accès aux fichiers à l'aide de Storage-Level Access Guard
- Liste des privilèges pris en charge
- Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine

Autoriser les utilisateurs ou les groupes à contourner la vérification de parcours du répertoire ONTAP SMB

Si vous souhaitez qu'un utilisateur puisse parcourir tous les répertoires du chemin d'accès à un fichier, même si l'utilisateur ne dispose pas des autorisations sur un répertoire de parcours, vous pouvez ajouter le `SeChangeNotifyPrivilege` Privilège pour les utilisateurs ou groupes SMB locaux sur des SVM (Storage Virtual machine). Par défaut, les utilisateurs peuvent contourner la vérification par passage de répertoire.

Avant de commencer

- Un serveur SMB doit être existant sur le SVM.
- L'option serveur SMB des utilisateurs et groupes locaux doit être activée.
- Utilisateur ou groupe local ou de domaine auquel `SeChangeNotifyPrivilege` le privilège sera ajouté doit déjà exister.

Description de la tâche

Lors de l'ajout de privilèges à un utilisateur ou à un groupe de domaine, ONTAP peut valider l'utilisateur ou le groupe du domaine en contactant le contrôleur de domaine. La commande peut échouer si ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Activer la vérification de la traverse de dérivation en ajoutant le `SeChangeNotifyPrivilege` privilège d'un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   La valeur pour le `-user-or-group-name` il s'agit d'un utilisateur ou d'un groupe local, ou d'un utilisateur ou d'un groupe de domaines.

2. Vérifiez que la vérification de la dérivation transversale est activée pour l'utilisateur ou le groupe spécifié : `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemple

La commande suivante permet aux utilisateurs qui appartiennent au groupe « EXEMPLE\eng » de contourner la vérification de la traverse de répertoire en ajoutant le `SeChangeNotifyPrivilege` privilège du groupe :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Informations associées

Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire

Interdire aux utilisateurs ou aux groupes de contourner la vérification de parcours du répertoire ONTAP SMB

Si vous ne souhaitez pas qu'un utilisateur traverse tous les répertoires du chemin d'accès à un fichier car l'utilisateur ne dispose pas des autorisations sur le répertoire de parcours, vous pouvez supprimer le `SeChangeNotifyPrivilege` Privilège des utilisateurs ou groupes SMB locaux sur des SVM (Storage Virtual machine).

Avant de commencer

L'utilisateur ou le groupe local ou de domaine dont les privilèges seront supprimés doit déjà exister.

Description de la tâche

Lors de la suppression de privilèges d'un utilisateur ou d'un groupe de domaines, ONTAP peut valider l'utilisateur ou le groupe de domaines en contactant le contrôleur de domaine. La commande peut échouer si ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Interdire la vérification de la traverse de dérivation : `vserver cifs users-and-groups privilege`

`remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

La commande supprime le `SeChangeNotifyPrivilege` privilège de l'utilisateur ou groupe local ou de domaine que vous spécifiez avec la valeur pour le `-user-or-group-name name` paramètre.

2. Vérifiez que le contrôle de la traverse de dérivation de l'utilisateur ou du groupe spécifié est désactivé : `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemple

La commande suivante empêche les utilisateurs appartenant au groupe « EXEMPLE\eng » de contourner la vérification de la traverse de répertoire :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          -
```

Informations associées

Permet aux utilisateurs ou aux groupes de contourner la vérification de la traverse du répertoire

Affiche des informations sur la sécurité des fichiers et les stratégies d'audit

En savoir plus sur l'affichage des politiques de sécurité et d'audit des fichiers ONTAP SMB

Vous pouvez afficher des informations sur la sécurité des fichiers dans les fichiers et les répertoires contenus dans les volumes des SVM (Storage Virtual machine). Vous pouvez afficher des informations sur les règles d'audit sur les volumes FlexVol. Si configuré, vous pouvez afficher des informations sur les paramètres de sécurité Storage-Level Access Guard et Dynamic Access Control sur les volumes FlexVol.

Affichage des informations relatives à la sécurité des fichiers

Vous pouvez afficher les informations relatives à la sécurité des fichiers appliquées aux données contenues dans des volumes et des qtrees (pour les volumes FlexVol) avec les styles de sécurité suivants :

- NTFS
- UNIX

- Mixte

Affichage des informations relatives aux stratégies d'audit

Vous pouvez afficher des informations sur les règles d'audit pour l'audit des événements d'accès sur les volumes FlexVol sur les protocoles NAS suivants :

- SMB (toutes les versions)
- NFSv4.x

Affichage d'informations sur la sécurité de Storage-Level Access Guard (SLAG)

La sécurité de la protection d'accès au niveau du stockage peut être appliquée sur des volumes FlexVol et des objets qtree avec les styles de sécurité suivants :

- NTFS
- Mixte
- UNIX (si un serveur CIFS est configuré sur le SVM qui contient le volume)

Affichage d'informations sur la sécurité du contrôle d'accès dynamique (DAC)

La sécurité du contrôle d'accès dynamique peut être appliquée à un objet au sein d'un volume FlexVol avec les styles de sécurité suivants :

- NTFS
- Mixte (si l'objet dispose d'une sécurité NTFS effective)

Informations associées

- Découvrez l'accès sécurisé aux fichiers à l'aide de Storage-Level Access Guard
- Afficher des informations sur Storage-Level Access Guard sur les serveurs

Afficher des informations sur la sécurité des fichiers ONTAP SMB sur les volumes de style de sécurité NTFS

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur les volumes de style de sécurité NTFS, notamment le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les attributs DOS. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Étant donné que les volumes et les qtrees de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux fichiers, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.
- Les valeurs de sortie ACL sont affichées pour les fichiers et les dossiers avec la sécurité NTFS.
- Étant donné que la sécurité Storage-Level Access Guard peut être configurée sur le volume racine ou

qtree, le résultat d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois les listes de contrôle d'accès standard des fichiers et les listes de contrôle d'accès Storage-Level Access Guard.

- La sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin de fichier ou de répertoire donné.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver vserver_name -path path`
Avec détails étendus	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/vol4` Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

L'exemple suivant affiche les informations de sécurité avec des masques étendus sur le chemin `/data/engineering` Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
```

```
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...0 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...1 .... .... .... .... .... =
Synchronize
                            .... .... .... 1... .... .... .... .... =
Write Owner
                            .... .... .... .1.. .... .... .... .... =
Write DAC
                            .... .... .... ..1. .... .... .... .... =
Read Control
                            .... .... .... ...1 .... .... .... .... =
Delete
                            .... .... .... .... .... ...1 .... .... =
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...1 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

L’exemple suivant affiche des informations de sécurité, y compris des informations de sécurité Storage-Level Access Guard, pour le volume avec le chemin d’accès `/datavol1` Au SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informations associées

- Affiche des informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes
- Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité UNIX

Afficher des informations sur la sécurité des fichiers ONTAP SMB sur des volumes de style de sécurité mixte

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur des volumes de style de sécurité mixtes, y compris le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les qtrees et volumes de style de sécurité mixtes peuvent contenir certains fichiers et dossiers qui utilisent des autorisations de fichier UNIX, soit les bits de mode ou les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.
- Le niveau supérieur d'un volume de type sécurité mixte peut avoir une sécurité efficace UNIX ou NTFS.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec sécurité NTFS ou NFSv4.

  Ce champ est vide pour les fichiers et les répertoires utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois les autorisations de fichiers UNIX et les listes de contrôle d'accès Storage-Level Access Guard.
- Si le chemin entré dans la commande est de données avec la sécurité effective NTFS, la sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin de fichier ou de répertoire donné.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver vserver_name -path path`
Avec détails étendus	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/projects` Dans le SVM vs1 sous forme de masque étendu. Ce chemin de sécurité mixte possède une sécurité efficace UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

L’exemple suivant affiche les informations de sécurité relatives au chemin d’accès `/data` Au SVM vs1. Ce chemin de sécurité mixte dispose d’une sécurité NTFS efficace.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

L'exemple suivant affiche les informations de sécurité relatives au volume sur le chemin d'accès `/datavol5` Au SVM vs1. Le niveau supérieur de ce volume de type sécurité mixte dispose d'une sécurité effective UNIX. Le volume est doté de la sécurité Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Informations associées

- Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité NTFS
- Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité UNIX

Afficher des informations sur la sécurité des fichiers ONTAP SMB sur les volumes de style de sécurité UNIX

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur les volumes de style de sécurité UNIX, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et

groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité de fichier ou de répertoire. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité UNIX n'utilisent que les autorisations de fichier UNIX, soit les bits de mode, soit les listes de contrôle d'accès NFSv4 lors de la détermination des droits d'accès aux fichiers.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec la sécurité NFSv4.

  Ce champ est vide pour les fichiers et les répertoires utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent pas dans le cas des descripteurs de sécurité NFSv4.

  Ils ne sont utiles que pour les descripteurs de sécurité NTFS.

- Étant donné que la sécurité Storage-Level Access Guard est prise en charge sur un volume UNIX ou qtree si un serveur CIFS est configuré sur le SVM, le résultat peut contenir des informations relatives à la sécurité Storage-Level Access Guard appliquée au volume ou au qtree spécifié dans le `-path` paramètre.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Avec détails étendus	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/home` Au SVM vs1 :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/home` Au SVM vs1 sous forme de masque étendu :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                        Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Informations associées

- Afficher des informations sur la sécurité des fichiers sur les volumes de style sécurisé
- Affiche des informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes

Commandes ONTAP pour afficher des informations sur les stratégies d'audit NTFS sur les volumes SMB FlexVol

Vous pouvez afficher des informations sur les stratégies d'audit NTFS sur les volumes FlexVol, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les listes de contrôle d'accès système. Vous pouvez utiliser les résultats pour valider votre configuration de sécurité ou pour résoudre les problèmes d'audit.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux fichiers ou dossiers dont vous souhaitez afficher les informations d'audit. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité NTFS utilisent uniquement des listes de contrôle d'accès au système NTFS pour les stratégies d'audit.
- Les règles d'audit NTFS peuvent être appliquées aux fichiers et dossiers d'un volume de style de sécurité mixte avec la sécurité efficace NTFS.

  Les volumes et qtrees de style de sécurité mixtes peuvent contenir certains fichiers et répertoires qui utilisent des autorisations de fichier UNIX, soit les bits de mode, soit les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.

- Le niveau supérieur d'un volume de style de sécurité mixte peut avoir une sécurité efficace sous UNIX ou NTFS et peut-être ne pas contenir des CLS NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois le fichier régulier et le dossier SACLs NFSv4 et les SACLs NTFS Storage-Level Access Guard.
- Si le chemin entré dans la commande est celui des données avec la sécurité effective NTFS, la sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin d'accès au fichier ou au répertoire donné.
- Lorsque vous affichez des informations de sécurité sur les fichiers et les dossiers avec la sécurité efficace NTFS, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.

  Les fichiers et dossiers de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux fichiers.

- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers disposant de la sécurité NTFS ou NFSv4.

  Ce champ est vide pour les fichiers et les dossiers utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.

Étape

1. Afficher les paramètres de stratégie d'audit de fichier et de répertoire avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver vserver_name -path path`
En tant que liste détaillée	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemples

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin `/corp` Au SVM vs1. Le chemin dispose d'une sécurité NTFS efficace. Le descripteur de sécurité NTFS contient à la fois une entrée RACL RÉUSSIE/ÉCHEC.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin `/datavol1` Au SVM vs1. Le chemin contient à la fois des fichiers standard et des SACL de dossier et des SALC de Storage-Level Access Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Commandes ONTAP pour afficher des informations sur les stratégies d'audit NFSv4 sur les volumes SMB FlexVol

Vous pouvez afficher des informations sur les stratégies d'audit NFSv4 sur les volumes FlexVol à l'aide de l'interface de ligne de commande ONTAP, notamment les styles de

sécurité et les styles de sécurité efficaces, les autorisations appliquées, ainsi que les informations sur les listes de contrôle d'accès système (SACL). Vous pouvez utiliser les résultats pour valider votre configuration de sécurité ou pour résoudre les problèmes d'audit.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux fichiers ou aux répertoires dont vous souhaitez afficher les informations d'audit. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité UNIX n'utilisent que les règles d'audit NFSv4.
- Les fichiers et les répertoires d'un volume mixte de style de sécurité UNIX peuvent appliquer des règles d'audit NFSv4.

  Les volumes et qtrees de style de sécurité mixtes peuvent contenir certains fichiers et répertoires qui utilisent des autorisations de fichier UNIX, soit les bits de mode, soit les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.

- Le niveau supérieur d'un volume de type sécurité mixte peut présenter une sécurité efficace sous UNIX ou NTFS et peut-être ne pas contenir des CLS NFSv4.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec sécurité NTFS ou NFSv4.

  Ce champ est vide pour les fichiers et les dossiers utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois le fichier NFSv4 régulier et le répertoire SACLs et les SACLs NTFS Storage-Level Access Guard.
- Étant donné que la sécurité Storage-Level Access Guard est prise en charge sur un volume UNIX ou qtree si un serveur CIFS est configuré sur le SVM, le résultat peut contenir des informations relatives à la sécurité Storage-Level Access Guard appliquée au volume ou au qtree spécifié dans le `-path` paramètre.

Étapes

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver vserver_name -path path`
Avec détails étendus	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/lab` Au SVM vs1. Ce chemin de style de sécurité UNIX dispose d'un SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Découvrez comment afficher les informations sur la sécurité des fichiers SMB ONTAP et les politiques d'audit

Vous pouvez utiliser le caractère générique (*) pour afficher des informations sur la sécurité des fichiers et les stratégies d'audit de tous les fichiers et répertoires sous un chemin donné ou un volume racine.

Le caractère générique (**) peut être utilisé comme dernier sous-composant d'un chemin d'accès de répertoire donné, sous lequel vous souhaitez afficher les informations de tous les fichiers et répertoires. Si vous souhaitez afficher les informations d'un fichier ou d'un répertoire donné nommé "*"**, vous devez alors indiquer le chemin complet à l'intérieur de guillemets doubles ("``"*"``").

Exemple

La commande suivante avec le caractère générique affiche les informations relatives à tous les fichiers et répertoires sous le chemin d'accès `/1/` Du SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

La commande suivante affiche les informations d’un fichier nommé "*" sous le chemin d’accès `/vol1/a` Du SVM vs1. Le chemin est entouré de guillemets doubles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 1002
          Unix Group Id: 65533
         Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Gérez la sécurité des fichiers NTFS, les règles d'audit NTFS et Storage-Level Access Guard sur les SVM à l'aide de l'interface de ligne de commande

Commandes ONTAP pour la gestion de la sécurité des fichiers SMB NTFS, des stratégies d'audit NTFS et de Storage-Level Access Guard

Vous pouvez gérer la sécurité des fichiers NTFS, les règles d'audit NTFS et Storage-Level Access Guard sur les SVM de stockage virtuels à l'aide de l'interface de ligne de commande.

Vous pouvez gérer les règles de sécurité et d'audit des fichiers NTFS des clients SMB ou à l'aide de l'interface de ligne de commande. Toutefois, l'utilisation de la CLI pour configurer les stratégies de sécurité des fichiers et d'audit supprime la nécessité d'utiliser un client distant pour gérer la sécurité des fichiers. L'utilisation de l'interface de ligne de commande permet de réduire considérablement le temps nécessaire à l'application de la sécurité sur de nombreux fichiers et dossiers à l'aide d'une seule commande.

Vous pouvez configurer Storage-Level Access Guard, qui est une autre couche de sécurité appliquée par ONTAP aux volumes de SVM. Storage-Level Access Guard s'applique aux accès de tous les protocoles NAS à l'objet de stockage auquel Storage-Level Access Guard est appliqué.

Storage-Level Access Guard peut être configuré et géré uniquement à partir de l'interface de ligne de commande ONTAP. Vous ne pouvez pas gérer les paramètres Storage-Level Access Guard à partir des clients SMB. De plus, si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne verrez pas la sécurité Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX). Par conséquent, Storage-Level Access Guard offre une couche supplémentaire de sécurité pour

l'accès aux données, qui est défini et géré de façon indépendante par l'administrateur du stockage.

> Bien que seules les autorisations d'accès NTFS soient prises en charge pour Storage-Level Access Guard, ONTAP peut effectuer des vérifications de sécurité pour l'accès via NFS aux données sur les volumes où Storage-Level Access Guard est appliqué si l'utilisateur UNIX mappe avec un utilisateur Windows sur le SVM propriétaire du volume.

Volumes de sécurité NTFS

Tous les fichiers et dossiers contenus dans des volumes et qtrees de style de sécurité NTFS bénéficient d'une sécurité efficace. Vous pouvez utiliser le `vserver security file-directory` Famille de commandes permettant d'implémenter les types de sécurité suivants sur les volumes de style de sécurité NTFS :

- Autorisations liées aux fichiers et stratégies d'audit pour les fichiers et les dossiers contenus dans le volume
- Sécurité Access Guard du niveau de stockage sur les volumes

Volumes de sécurité mixtes

Les qtrees et volumes de style de sécurité mixtes peuvent contenir certains fichiers et dossiers disposant d'une sécurité effective UNIX et utiliser des autorisations de fichiers UNIX, soit les bits de mode, soit les listes de contrôle d'accès NFSv4.x et les règles d'audit NFSv4.x, ainsi que certains fichiers et dossiers disposant d'une sécurité efficace NTFS, et utilisant les autorisations d'accès aux fichiers NTFS et les règles d'audit. Vous pouvez utiliser le `vserver security file-directory` famille de commandes pour appliquer les types de sécurité suivants aux données de style de sécurité mixte :

- Autorisations liées aux fichiers et règles d'audit sur les fichiers et les dossiers avec le style de sécurité effectif NTFS dans le volume mixte ou le qtree
- Access Guard au niveau du stockage pour les volumes NTFS et UNIX

Volumes de style de sécurité UNIX

Les volumes et les qtrees de style de sécurité UNIX contiennent des fichiers et des dossiers qui disposent d'une sécurité effective UNIX (soit les bits de mode, soit les ACL NFSv4.x). Si vous souhaitez utiliser le, vous devez garder à l'esprit les éléments suivants `vserver security file-directory` Famille de commandes pour implémenter la sécurité sur des volumes de type sécurité UNIX :

- Le `vserver security file-directory` Les familles de commandes ne peuvent pas être utilisées pour gérer la sécurité des fichiers UNIX et les règles d'audit sur les volumes et les qtrees de style de sécurité UNIX.
- Vous pouvez utiliser le `vserver security file-directory` Gamme de commandes permettant de configurer Storage-Level Access Guard sur des volumes de style de sécurité UNIX, à condition que le SVM avec le volume cible contienne un serveur CIFS.

Informations associées

- En savoir plus sur l'affichage des politiques de sécurité et d'audit des fichiers
- Créer des descripteurs de sécurité NTFS sur les serveurs
- Commandes pour configurer et appliquer des politiques d'audit aux fichiers et dossiers
- Découvrez l'accès sécurisé aux fichiers à l'aide de Storage-Level Access Guard

Commandes ONTAP pour définir la sécurité des fichiers et des dossiers SMB

Puisque vous pouvez appliquer et gérer la sécurité des fichiers et des dossiers localement sans l'intervention d'un client distant, vous pouvez réduire considérablement le temps nécessaire pour définir la sécurité en bloc sur un grand nombre de fichiers ou de dossiers.

Vous pouvez utiliser l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers dans les cas d'utilisation suivants :

- Stockage de fichiers dans les grands environnements d'entreprise, tels que le stockage de fichiers dans les répertoires locaux
- Migration des données
- Changement de domaine Windows
- Standardisation des règles de sécurité des fichiers et d'audit sur l'ensemble des systèmes de fichiers NTFS

Découvrez les limites lors de l'utilisation des commandes ONTAP pour définir la sécurité des fichiers et des dossiers SMB

Vous devez connaître certaines limites lorsque vous utilisez l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers.

- Le `vserver security file-directory` La famille de commandes ne prend pas en charge la configuration des listes de contrôle d'accès NFSv4.

  Vous pouvez uniquement appliquer des descripteurs de sécurité NTFS aux fichiers et dossiers NTFS.

Utilisez des descripteurs de sécurité pour appliquer la sécurité des fichiers et des dossiers ONTAP SMB

Les descripteurs de sécurité contiennent les listes de contrôle d'accès qui déterminent les actions qu'un utilisateur peut effectuer sur les fichiers et les dossiers, et ce qui est vérifié lorsqu'un utilisateur accède à des fichiers et à des dossiers.

- **Autorisations**

  Les autorisations sont autorisées ou refusées par le propriétaire d'un objet et déterminent les actions qu'un objet (utilisateurs, groupes ou objets informatiques) peut exécuter sur des fichiers ou dossiers spécifiés.

- **Descripteurs de sécurité**

  Les descripteurs de sécurité sont des structures de données contenant des informations de sécurité qui définissent les autorisations associées à un fichier ou à un dossier.

- **Listes de contrôle d'accès (ACL)**

  Les listes de contrôle d'accès sont les listes contenues dans un descripteur de sécurité qui contiennent des informations sur les actions que les utilisateurs, les groupes ou les objets informatiques peuvent exécuter sur le fichier ou le dossier auquel le descripteur de sécurité est appliqué. Le Security Descriptor peut contenir les deux types de listes de contrôle d'accès suivants :

  - Listes de contrôle d'accès discrétionnaire (DACL)

    - Listes de contrôle d’accès au système (SACL)
- * Listes de contrôle d’accès discrétionnaire (listes DACL)*

  Les DACL contiennent la liste des SID pour les utilisateurs, les groupes et les objets d’ordinateur qui sont autorisés ou refusés à effectuer des actions sur des fichiers ou des dossiers. Les listes DALC contiennent au moins zéro entrée de contrôle d’accès (ACE).

- **Listes de contrôle d’accès au système (SACL)**

  Les SACL contiennent la liste des PEID pour les utilisateurs, les groupes et les objets d’ordinateur pour lesquels des événements d’audit réussis ou échoués sont consignés. Les SACL contiennent au moins zéro entrée de contrôle d’accès (ACE).

- **Entrées de contrôle d’accès (ACE)**

  Ces sont des entrées individuelles dans DACL ou SACL :

    - Une entrée de contrôle d’accès DACL spécifie les droits d’accès autorisés ou refusés pour certains utilisateurs, groupes ou objets d’ordinateur.
    - Une entrée de contrôle d’accès SACL spécifie les événements succès ou échec à consigner lors de l’audit des actions spécifiées effectuées par des utilisateurs, des groupes ou des objets d’ordinateur particuliers.
- **Héritage des autorisations**

  L’héritage des autorisations décrit comment les autorisations définies dans les descripteurs de sécurité sont propagées à un objet à partir d’un objet parent. Seules les autorisations héritables sont héritées par des objets enfants. Lorsque vous définissez des autorisations sur l’objet parent, vous pouvez décider si les dossiers, sous-dossiers et fichiers peuvent les hériter avec "'appliquer à `this-folder`, `sub-folders`, et `fichierss".

Informations associées

- "Audit et suivi de sécurité SMB et NFS"
- Commandes pour configurer et appliquer des politiques d’audit aux fichiers et dossiers

En savoir plus sur l’application de stratégies de répertoire de fichiers qui utilisent des utilisateurs ou des groupes SMB locaux sur la destination de reprise après sinistre ONTAP SVM

Si la configuration de votre politique de répertoire de fichiers utilise des utilisateurs ou des groupes locaux dans le Security Descriptor ou les entrées DACL ou SACL, vous devez garder à l’esprit avant d’appliquer les stratégies de répertoires de fichiers sur la destination de reprise après incident SVM (Storage Virtual machine) en configuration de suppression d’ID.

Il est possible de configurer une configuration de reprise sur incident pour un SVM où le SVM source sur le cluster source réplique les données et la configuration depuis le SVM source vers un SVM destination sur un cluster de destination.

Vous pouvez configurer l’un des deux types de reprise après incident des SVM :

- Identité préservée

  Avec cette configuration, l’identité du SVM et du serveur CIFS est préservée.

- Identité rejetée

  Avec cette configuration, l'identité du SVM et du serveur CIFS n'est pas conservée Dans ce scénario, le nom du SVM et du serveur CIFS sur le SVM de destination est différent de celui du SVM et du nom du serveur CIFS sur le SVM source.

Instructions pour les configurations éliminées par identité

Dans une configuration définie par l'identité, pour une source SVM qui contient des configurations utilisateur, groupe et privilège local, le nom du domaine local (nom du serveur CIFS local) doit être modifié afin de correspondre au nom du serveur CIFS sur la destination du SVM. Par exemple, si le nom du SVM source est « vs1 » et que le nom du serveur CIFS est « CIFS1 », et que le nom du SVM de destination est « vs1_dst » et que le nom du serveur CIFS est « CIFS1_DST », le nom de domaine local d'un utilisateur local nommé « DST CI1\user1 » est automatiquement modifié sur la SVM « destination » :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Même si les noms d'utilisateur et de groupe locaux sont automatiquement modifiés dans les bases de données des utilisateurs et des groupes locaux, les noms d'utilisateurs ou de groupes locaux ne sont pas automatiquement modifiés dans les configurations des stratégies de répertoires de fichiers (règles configurées sur la CLI à l'aide de l' `vserver security file-directory` famille de commande).

Par exemple, pour « vs1 », si vous avez configuré une entrée DACL où le `-account` Le paramètre est défini sur « CIFS1\user1 », le paramètre n'est pas automatiquement modifié sur le SVM de destination pour refléter le nom du serveur CIFS de destination.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Vous devez utiliser le `vserver security file-directory modify` Commandes permettant de modifier manuellement le nom du serveur CIFS sur le nom du serveur CIFS de destination.

Composants de configuration de la stratégie de répertoire de fichiers contenant des paramètres de compte

Il existe trois composants de configuration de stratégie de répertoire de fichiers qui peuvent utiliser des paramètres pouvant contenir des utilisateurs ou des groupes locaux :

- Descripteur de sécurité

  Vous pouvez éventuellement spécifier le propriétaire du descripteur de sécurité et le groupe principal du propriétaire du descripteur de sécurité. Si le Security Descriptor utilise un utilisateur ou groupe local pour les entrées propriétaire et groupe principal, vous devez modifier le Security Descriptor afin d'utiliser le SVM destination dans le nom du compte. Vous pouvez utiliser le `vserver security file-directory ntfs modify` commande permettant de modifier les noms de compte si nécessaire.

- Entrées DACL

  Chaque entrée DACL doit être associée à un compte. Vous devez modifier tout DACL qui utilisent des comptes utilisateur ou groupe locaux pour utiliser le nom de SVM de destination. Étant donné que vous ne pouvez pas modifier le nom du compte pour les entrées DACL existantes, vous devez supprimer toutes les entrées DACL avec des utilisateurs ou des groupes locaux des descripteurs de sécurité, créer de nouvelles entrées DACL avec les noms de compte de destination corrigés et associer ces nouvelles entrées DACL aux descripteurs de sécurité appropriés.

- Entrées SACL

  Chaque entrée SACL doit être associée à un compte. Vous devez modifier les CLS qui utilisent des

comptes utilisateur ou groupe locaux pour utiliser le nom de SVM de destination. Comme vous ne pouvez pas modifier le nom du compte pour les entrées SACL existantes, vous devez supprimer les entrées SACL avec des utilisateurs ou des groupes locaux des descripteurs de sécurité, créer de nouvelles entrées SACL avec les noms de compte de destination corrigés et associer ces nouvelles entrées SACL aux descripteurs de sécurité appropriés.

Vous devez apporter les modifications nécessaires aux utilisateurs ou groupes locaux utilisés dans la configuration de la stratégie de répertoire de fichiers avant d'appliquer la stratégie. Sinon, la tâche d'application échoue.

Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande

Créer des descripteurs de sécurité NTFS sur les serveurs ONTAP SMB

La création d'un Security Descriptor (politique de sécurité des fichiers) NTFS constitue la première étape de configuration et d'application des listes de contrôle d'accès (ACL) NTFS aux fichiers et dossiers résidant sur les SVM (Storage Virtual machines). Vous pouvez associer le descripteur de sécurité au chemin du fichier ou du dossier dans une tâche de stratégie.

Description de la tâche

Vous pouvez créer des descripteurs de sécurité NTFS pour les fichiers et les dossiers résidant dans des volumes de style de sécurité NTFS ou pour les fichiers et dossiers résidant sur des volumes de type sécurité mixtes.

Par défaut, lorsqu'un descripteur de sécurité est créé, quatre entrées de contrôle d'accès (ACE) de liste de contrôle d'accès discrétionnaire (DACL) sont ajoutées à ce descripteur de sécurité. Les quatre ACE par défaut sont les suivants :

Objet	Type d'accès	Droits d'accès	Où appliquer les autorisations
INTÉGRÉ\administrateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
INTÉGRÉ\utilisateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
PROPRIÉTAIRE DU CRÉATEUR	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
AUTORITÉ NT\SYSTÈME	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Propriétaire du Security Descriptor
- Groupe principal du propriétaire

- Indicateurs de contrôle bruts

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Pour en savoir plus, consultez le "Référence de commande ONTAP".

Ajouter des entrées de contrôle d'accès NTFS DACL aux descripteurs de sécurité NTFS sur les serveurs SMB ONTAP

L'ajout d'entrées de contrôle d'accès (ACE) DACL (liste de contrôle d'accès discrétionnaire) au descripteur de sécurité NTFS est la deuxième étape de la configuration et de l'application des listes de contrôle d'accès NTFS à un fichier ou à un dossier. Chaque entrée identifie quel objet est autorisé ou refusé à accéder et définit ce que l'objet peut ou ne peut pas faire pour les fichiers ou dossiers définis dans ACE.

Description de la tâche

Vous pouvez ajouter un ou plusieurs ACE au DACL du Security Descriptor.

Si le descripteur de sécurité contient un DACL contenant des ACE existants, la commande ajoute le nouveau ACE au DACL. Si le descripteur de sécurité ne contient pas de DACL, la commande crée le DACL et y ajoute le nouveau ACE.

Vous pouvez éventuellement personnaliser les entrées DACL en spécifiant les droits que vous souhaitez autoriser ou refuser pour le compte spécifié dans `-account` paramètre. Il existe trois méthodes mutuellement exclusives de définition des droits :

- Droits
- Droits avancés
- Droits bruts (privilège avancé)

> Si vous ne spécifiez pas de droits pour l'entrée DACL, la valeur par défaut est de définir les droits sur `Full Control`.

Vous pouvez personnaliser les entrées DACL en spécifiant la manière d'appliquer l'héritage.

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Étapes

1. Ajouter une entrée DACL à un descripteur de sécurité : `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Vérifier que l'entrée DACL est correcte : `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
Security Descriptor Name: sd1
             Allow or Deny: deny
         Account Name or SID: DOMAIN\joe
               Access Rights: full-control
  Advanced Access Rights: -
                   Apply To: this-folder
               Access Rights: full-control
```

Pour en savoir plus, `vserver security file-directory ntfs dacl` consultez le "Référence de commande ONTAP".

Créer des politiques de sécurité ONTAP SMB

La création d'une politique de sécurité des fichiers pour les SVM représente la troisième étape de la configuration et de l'application de ces ACL à un fichier ou dossier. Une règle agit comme un conteneur pour différentes tâches, où chaque tâche est une entrée unique qui peut être appliquée à des fichiers ou des dossiers. Vous pouvez ajouter des tâches à la stratégie de sécurité ultérieurement.

Description de la tâche

Les tâches que vous ajoutez à une stratégie de sécurité contiennent des associations entre le descripteur de sécurité NTFS et les chemins de fichier ou de dossier. Vous devez donc associer la politique de sécurité à chaque SVM (qui contient des volumes de style de sécurité NTFS ou des volumes de type sécurité mixtes).

Étapes

1. Création d'une stratégie de sécurité : `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver vs1
   ```

2. Vérifiez la stratégie de sécurité : `vserver security file-directory policy show`

   ```
   vserver security file-directory policy show
     Vserver          Policy Name
    ------------     --------------
       vs1              policy1
   ```

Ajouter des tâches à la politique de sécurité ONTAP SMB

La création et l'ajout d'une tâche policy à une policy de sécurité constitue la quatrième étape de la configuration et de l'application de ACL à des fichiers ou dossiers des SVM. Lorsque vous créez la tâche de stratégie, vous associez la tâche à une stratégie de sécurité. Vous pouvez ajouter une ou plusieurs entrées de tâche à une stratégie de

sécurité.

Description de la tâche

La stratégie de sécurité est un conteneur pour une tâche. Une tâche fait référence à une opération unique qui peut être effectuée par une stratégie de sécurité pour les fichiers ou dossiers avec NTFS ou la sécurité mixte (ou à un objet de volume si vous configurez Storage-Level Access Guard).

Il existe deux types de tâches :

- Tâches de fichier et de répertoire

  Permet de spécifier les tâches qui appliquent des descripteurs de sécurité aux fichiers et dossiers spécifiés. Les ACL appliquées via les tâches de fichier et de répertoire peuvent être gérées avec les clients SMB ou l'interface de ligne de commande ONTAP.

- Tâches de Storage-Level Access Guard

  Permet de spécifier les tâches qui appliquent des descripteurs de sécurité Storage-Level Access Guard à un volume spécifié. Les listes de contrôle d'accès appliquées via les tâches Storage-Level Access Guard peuvent être gérées uniquement via l'interface de ligne de commande ONTAP.

Une tâche contient des définitions pour la configuration de sécurité d'un fichier (ou d'un dossier) ou d'un ensemble de fichiers (ou de dossiers). Chaque tâche d'une stratégie est identifiée de manière unique par le chemin. Il ne peut y avoir qu'une seule tâche par chemin au sein d'une même stratégie. Une stratégie ne peut pas avoir d'entrées de tâche en double.

Instructions pour l'ajout d'une tâche à une stratégie :

- Il peut y avoir un maximum de 10,000 entrées de tâches par stratégie.
- Une stratégie peut contenir une ou plusieurs tâches.

  Même si une stratégie peut contenir plusieurs tâches, vous ne pouvez pas configurer une stratégie pour contenir à la fois des tâches de répertoire de fichiers et de Storage-Level Access Guard. Une stratégie doit contenir soit toutes les tâches Storage-Level Access Guard, soit toutes les tâches du répertoire de fichiers.

- Storage-Level Access Guard est utilisé pour restreindre les autorisations.

  Il ne vous donnera jamais d'autorisations d'accès supplémentaires.

Lorsque vous ajoutez des tâches aux stratégies de sécurité, vous devez spécifier les quatre paramètres requis suivants :

- Nom du SVM
- Nom de la règle
- Chemin
- Descripteur de sécurité à associer au chemin d'accès

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Type de sécurité
- Mode de propagation

- Position de l'index
- Type de contrôle d'accès

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Étapes

1. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité : `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` est la valeur par défaut de l' `-access-control` paramètre. La définition du type de contrôle d'accès lors de la configuration des tâches d'accès aux fichiers et aux répertoires est facultative.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Vérifiez la configuration de la tâche de stratégie : `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Pour en savoir plus, `vserver security file-directory policy task` consultez le "Référence de commande ONTAP".

Appliquer les politiques de sécurité ONTAP SMB

L'application d'une politique de sécurité des fichiers aux SVM est la dernière étape de la création et de l'application de ces ACL NTFS aux fichiers ou aux dossiers.

Description de la tâche

Vous pouvez appliquer les paramètres de sécurité définis dans la stratégie de sécurité aux fichiers et dossiers NTFS résidant au sein de volumes FlexVol (NTFS ou style de sécurité mixte).

Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Lorsqu'une stratégie de sécurité et les listes de contrôle d'accès discrétionnaire associées sont appliquées, toutes les listes de contrôle d'accès discrétionnaire existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Étape

1. Appliquer une politique de sécurité : `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   La tâche d'application de la politique est planifiée et l'ID de la tâche est renvoyé.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Surveiller les tâches de politique de sécurité SMB ONTAP

Lorsque vous appliquez la stratégie de sécurité aux serveurs virtuels de stockage (SVM), vous pouvez surveiller la progression de la tâche en surveillant la tâche de stratégie de sécurité. Ceci est utile si vous voulez vérifier que l'application de la politique de sécurité a réussi. Ceci est également utile si vous avez un travail de longue durée où vous appliquez la sécurité en bloc à un grand nombre de fichiers et de dossiers.

Description de la tâche

Pour afficher des informations détaillées sur une tâche de stratégie de sécurité, vous devez utiliser le `-instance` paramètre.

Étape

1. Surveillez la tâche de stratégie de sécurité : `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Vérifier la sécurité des fichiers SMB ONTAP

Vous pouvez vérifier les paramètres de sécurité des fichiers pour confirmer que les fichiers ou les dossiers de la machine virtuelle de stockage (SVM) à laquelle vous avez appliqué la stratégie de sécurité disposent des paramètres souhaités.

Description de la tâche

Vous devez fournir le nom de la SVM qui contient les données et le chemin d'accès au fichier et aux dossiers sur lesquels vous souhaitez vérifier les paramètres de sécurité. Vous pouvez utiliser l'option `-expand-mask` paramètre pour afficher des informations détaillées sur les paramètres de sécurité.

Étape

1. Afficher les paramètres de sécurité des fichiers et dossiers : `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   -expand-mask true
   ```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
```

```
                           .... .... .... ..0. = Group Defaulted
                           .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
                             .... .... .... .... .... ...1 .... .... =
Write Attributes
                             .... .... .... .... .... .... 1... .... =
Read Attributes
                             .... .... .... .... .... .... .1.. .... =
Delete Child
                             .... .... .... .... .... .... ..1. .... =
Execute
                             .... .... .... .... .... .... ...1 .... =
Write EA
                             .... .... .... .... .... .... .... 1... =
Read EA
                             .... .... .... .... .... .... .... .1.. =
Append
                             .... .... .... .... .... .... .... ..1. =
Write
                             .... .... .... .... .... .... .... ...1 =
Read
```

```
                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Configurez et appliquez des règles d'audit aux fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande

Commandes ONTAP pour configurer et appliquer des stratégies d'audit SMB aux fichiers et dossiers NTFS

Lorsque vous utilisez l'interface de ligne de commande ONTAP, vous devez effectuer

plusieurs étapes pour appliquer des règles d'audit aux fichiers et dossiers NTFS. Tout d'abord, vous créez un descripteur de sécurité NTFS et ajoutez des CLS au descripteur de sécurité. Ensuite, vous créez une stratégie de sécurité et ajoutez des tâches de stratégie. Vous appliquez ensuite la politique de sécurité sur une machine virtuelle de stockage (SVM).

Description de la tâche

Après avoir appliqué la stratégie de sécurité, vous pouvez surveiller la tâche de stratégie de sécurité, puis vérifier les paramètres de la stratégie d'audit appliquée.

> Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Informations associées

- Découvrez l'accès sécurisé aux fichiers à l'aide de Storage-Level Access Guard
- Découvrez les limites lors de l'utilisation de commandes pour définir la sécurité des fichiers et des dossiers SMB
- Utilisez des descripteurs de sécurité pour appliquer la sécurité des fichiers et des dossiers
- "Audit et suivi de sécurité SMB et NFS"
- Créer des descripteurs de sécurité NTFS sur les serveurs

Créer des descripteurs de sécurité NTFS sur les serveurs ONTAP SMB

La création d'une règle d'audit NTFS est la première étape de la configuration et de l'application des listes de contrôle d'accès (ACL) NTFS aux fichiers et dossiers qui résident au sein des SVM. Vous associerez le descripteur de sécurité au chemin du fichier ou du dossier dans une tâche de stratégie.

Description de la tâche

Vous pouvez créer des descripteurs de sécurité NTFS pour les fichiers et les dossiers résidant dans des volumes de style de sécurité NTFS ou pour les fichiers et dossiers résidant sur des volumes de type sécurité mixtes.

Par défaut, lorsqu'un descripteur de sécurité est créé, quatre entrées de contrôle d'accès (ACE) de liste de contrôle d'accès discrétionnaire (DACL) sont ajoutées à ce descripteur de sécurité. Les quatre ACE par défaut sont les suivants :

Objet	Type d'accès	Droits d'accès	Où appliquer les autorisations
INTÉGRÉ\administrateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
INTÉGRÉ\utilisateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers

Objet	Type d'accès	Droits d'accès	Où appliquer les autorisations
PROPRIÉTAIRE DU CRÉATEUR	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
AUTORITÉ NT\SYSTÈME	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Propriétaire du Security Descriptor
- Groupe principal du propriétaire
- Indicateurs de contrôle bruts

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Étapes

1. Si vous souhaitez utiliser les paramètres avancés, définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Créez un Security Descriptor: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. Vérifiez que la configuration du descripteur de sécurité est correcte : `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Si vous êtes au niveau de privilège avancé, revenez au niveau de privilège admin : `set -privilege admin`

Ajouter des entrées de contrôle d'accès NTFS SACL aux descripteurs de sécurité NTFS sur les serveurs SMB ONTAP

L'ajout d'entrées de contrôle d'accès (ACE) SACL (System Access Control list) au descripteur de sécurité NTFS est la deuxième étape de création des politiques d'audit NTFS pour les fichiers ou les dossiers des SVM. Chaque entrée identifie l'utilisateur ou le

groupe que vous souhaitez auditer. L'entrée SACL définit si vous souhaitez auditer les tentatives d'accès réussies ou échouées.

Description de la tâche

Vous pouvez ajouter un ou plusieurs ACE au SACL du descripteur de sécurité.

Si le descripteur de sécurité contient une SACL comportant des ACE existants, la commande ajoute la nouvelle ACE à la SACL. Si le descripteur de sécurité ne contient pas de SACL, la commande crée la SACL et y ajoute la nouvelle ACE.

Vous pouvez configurer les entrées SACL en spécifiant les droits que vous souhaitez auditer pour les événements de réussite ou d'échec du compte spécifié dans `-account` paramètre. Il existe trois méthodes mutuellement exclusives de définition des droits :

- Droits
- Droits avancés
- Droits bruts (privilège avancé)

> Si vous ne spécifiez pas de droits pour l'entrée SACL, le paramètre par défaut est `Full Control`.

Vous pouvez personnaliser des entrées SACL en spécifiant la façon d'appliquer l'héritage à l' `apply to` paramètre. Si vous ne spécifiez pas ce paramètre, la valeur par défaut est d'appliquer cette entrée SACL à ce dossier, sous-dossiers et fichiers.

Étapes

1. Ajoutez une entrée SACL à un descripteur de sécurité : `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Vérifiez que l'entrée SACL est correcte : `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                              Vserver: vs1
                   Security Descriptor Name: sd1
         Access type for Specified Access Rights: failure
                        Account Name or SID: DOMAIN\joe
                              Access Rights: full-control
                     Advanced Access Rights: -
                                   Apply To: this-folder
                              Access Rights: full-control
```

Créer des politiques de sécurité ONTAP SMB

La création d'une policy d'audit pour les SVM (Storage Virtual machines) constitue la troisième étape de la configuration et de l'application de ces ACL à un fichier ou à un dossier. Une règle agit comme un conteneur pour différentes tâches, où chaque tâche est une entrée unique qui peut être appliquée à des fichiers ou des dossiers. Vous pouvez ajouter des tâches à la stratégie de sécurité ultérieurement.

Description de la tâche

Les tâches que vous ajoutez à une stratégie de sécurité contiennent des associations entre le descripteur de sécurité NTFS et les chemins de fichier ou de dossier. Par conséquent, vous devez associer la stratégie de sécurité à chaque SVM (Storage Virtual machine) (contenant des volumes de style de sécurité NTFS ou des volumes de type sécurité mixtes).

Étapes

1. Création d'une stratégie de sécurité : `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Vérifiez la stratégie de sécurité : `vserver security file-directory policy show`

```
            vserver security file-directory policy show
               Vserver          Policy Name
             ------------     --------------
                 vs1              policy1
```

Ajouter des tâches à la politique de sécurité ONTAP SMB

La création et l'ajout d'une tâche policy à une policy de sécurité constitue la quatrième étape de la configuration et de l'application de ACL à des fichiers ou dossiers des SVM. Lorsque vous créez la tâche de stratégie, vous associez la tâche à une stratégie de sécurité. Vous pouvez ajouter une ou plusieurs entrées de tâche à une stratégie de sécurité.

Description de la tâche

La stratégie de sécurité est un conteneur pour une tâche. Une tâche fait référence à une opération unique qui peut être effectuée par une stratégie de sécurité pour les fichiers ou dossiers avec NTFS ou la sécurité mixte (ou à un objet de volume si vous configurez Storage-Level Access Guard).

Il existe deux types de tâches :

- Tâches de fichier et de répertoire

  Permet de spécifier les tâches qui appliquent des descripteurs de sécurité aux fichiers et dossiers spécifiés. Les ACL appliquées via les tâches de fichier et de répertoire peuvent être gérées avec les clients SMB ou l'interface de ligne de commande ONTAP.

- Tâches de Storage-Level Access Guard

  Permet de spécifier les tâches qui appliquent des descripteurs de sécurité Storage-Level Access Guard à un volume spécifié. Les listes de contrôle d'accès appliquées via les tâches Storage-Level Access Guard peuvent être gérées uniquement via l'interface de ligne de commande ONTAP.

Une tâche contient des définitions pour la configuration de sécurité d'un fichier (ou d'un dossier) ou d'un ensemble de fichiers (ou de dossiers). Chaque tâche d'une stratégie est identifiée de manière unique par le chemin. Il ne peut y avoir qu'une seule tâche par chemin au sein d'une même stratégie. Une stratégie ne peut pas avoir d'entrées de tâche en double.

Instructions pour l'ajout d'une tâche à une stratégie :

- Il peut y avoir un maximum de 10,000 entrées de tâches par stratégie.
- Une stratégie peut contenir une ou plusieurs tâches.

  Même si une stratégie peut contenir plusieurs tâches, vous ne pouvez pas configurer une stratégie pour contenir à la fois des tâches de répertoire de fichiers et de Storage-Level Access Guard. Une stratégie doit contenir soit toutes les tâches Storage-Level Access Guard, soit toutes les tâches du répertoire de fichiers.

- Storage-Level Access Guard est utilisé pour restreindre les autorisations.

  Il ne vous donnera jamais d'autorisations d'accès supplémentaires.

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Type de sécurité
- Mode de propagation
- Position de l'index
- Type de contrôle d'accès

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Étapes

1. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité : `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` est la valeur par défaut de l' `-access-control` paramètre. La définition du type de contrôle d'accès lors de la configuration des tâches d'accès aux fichiers et aux répertoires est facultative.

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
-index-num 1 -access-control file-directory
```

2. Vérifiez la configuration de la tâche de stratégie : `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Pour en savoir plus, `vserver security file-directory policy task` consultez le "Référence de commande ONTAP".

Appliquer les politiques de sécurité ONTAP SMB

L'application d'une règle d'audit aux SVM constitue la dernière étape de création et d'application des listes de contrôle d'accès NTFS aux fichiers ou dossiers.

Description de la tâche

Vous pouvez appliquer les paramètres de sécurité définis dans la stratégie de sécurité aux fichiers et dossiers NTFS résidant au sein de volumes FlexVol (NTFS ou style de sécurité mixte).

> Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Lorsqu'une stratégie de sécurité et les listes de contrôle d'accès discrétionnaire associées sont appliquées, toutes les listes de contrôle d'accès discrétionnaire existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Étape

1. Appliquer une politique de sécurité : `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   La tâche d'application de la politique est planifiée et l'ID de la tâche est renvoyé.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Surveiller les tâches de politique de sécurité SMB ONTAP

Lorsque vous appliquez la stratégie de sécurité aux serveurs virtuels de stockage (SVM), vous pouvez surveiller la progression de la tâche en surveillant la tâche de stratégie de sécurité. Ceci est utile si vous voulez vérifier que l'application de la politique de sécurité a réussi. Ceci est également utile si vous avez un travail de longue durée où vous appliquez la sécurité en bloc à un grand nombre de fichiers et de dossiers.

Description de la tâche

Pour afficher des informations détaillées sur une tâche de stratégie de sécurité, vous devez utiliser le `-instance` paramètre.

Étape

1. Surveillez la tâche de stratégie de sécurité : `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

Vérifier les politiques d'audit ONTAP SMB

Vous pouvez vérifier la stratégie d'audit pour confirmer que les fichiers ou les dossiers de la machine virtuelle de stockage (SVM) à laquelle vous avez appliqué la stratégie de sécurité disposent des paramètres de sécurité d'audit souhaités.

Description de la tâche

Vous utilisez le `vserver security file-directory show` commande permettant d'afficher les informations relatives aux règles d'audit. Vous devez fournir le nom de la SVM qui contient les données et le chemin d'accès aux données dont vous souhaitez afficher les informations de la politique d'audit de fichier ou de dossier.

Étape

1. Afficher les paramètres de stratégie d'audit : `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Exemple

La commande suivante affiche les informations de la politique d'audit appliquées au chemin "/corp" du SVM vs1. Le chemin a à la fois UN SUCCÈS et une entrée SACL SUCCÈS/ÉCHEC qui lui est appliquée :

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

En savoir plus sur la gestion des tâches de politique de sécurité ONTAP SMB

Si une tâche de stratégie de sécurité existe, dans certaines circonstances, vous ne pouvez pas modifier cette stratégie de sécurité ou les tâches affectées à cette stratégie. Vous devez comprendre dans quelles conditions vous pouvez ou ne pouvez pas modifier les stratégies de sécurité pour que toute tentative de modification de la stratégie soit réussie. Les modifications apportées à la stratégie comprennent l'ajout, la suppression ou la modification de tâches affectées à la stratégie et la suppression ou la modification de celle-ci.

Vous ne pouvez pas modifier une stratégie de sécurité ou une tâche affectée à cette stratégie si un travail existe pour cette stratégie et que ce travail se trouve dans les États suivants :

- Le travail est en cours d'exécution ou en cours d'exécution.
- Le travail est suspendu.
- Le travail reprend et est en cours d'exécution.
- Si le travail attend le basculement vers un autre nœud.

Dans les circonstances suivantes, si une tâche existe pour une stratégie de sécurité, vous pouvez modifier avec succès cette stratégie de sécurité ou une tâche affectée à cette stratégie :

- La tâche de stratégie est arrêtée.
- La tâche de stratégie s'est terminée avec succès.

Commandes ONTAP pour la gestion des descripteurs de sécurité NTFS sur les serveurs SMB

Il existe des commandes ONTAP spécifiques pour gérer les descripteurs de sécurité. Vous pouvez créer, modifier, supprimer et afficher des informations sur les descripteurs de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer des descripteurs de sécurité NTFS	`vserver security file-directory ntfs create`
Modifiez les descripteurs de sécurité NTFS existants	`vserver security file-directory ntfs modify`
Affiche des informations sur les descripteurs de sécurité NTFS existants	`vserver security file-directory ntfs show`
Supprimez les descripteurs de sécurité NTFS	`vserver security file-directory ntfs delete`

Pour en savoir plus, `vserver security file-directory ntfs` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des entrées de contrôle d'accès NTFS DACL sur les serveurs SMB

Il existe des commandes ONTAP spécifiques pour la gestion des entrées de contrôle d'accès DACL (ACE). Vous pouvez ajouter des ACE aux listes de contrôle d'accès NTFS à tout moment. Vous pouvez également gérer les listes de contrôle d'accès NTFS existantes en modifiant, supprimant et affichant des informations sur les ACE dans les listes de contrôle d'accès.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez des ACE et ajoutez-les dans les listes de contrôle d'accès NTFS	`vserver security file-directory ntfs dacl add`
Modifier les ACE existants dans les listes de contrôle d'accès NTFS	`vserver security file-directory ntfs dacl modify`
Affiche des informations sur les ACE existants dans les DACL NTFS	`vserver security file-directory ntfs dacl show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Supprimez les ACE existants des listes de contrôle d'accès NTFS	`vserver security file-directory ntfs dacl remove`

Pour en savoir plus, `vserver security file-directory ntfs dacl` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des entrées de contrôle d'accès NTFS SACL sur les serveurs SMB

Il existe des commandes ONTAP spécifiques pour gérer les entrées de contrôle d'accès SACL (ACE). Vous pouvez ajouter des ACE aux CLS NTFS à tout moment. Vous pouvez également gérer les SALC NTFS existants en modifiant, supprimant et affichant des informations sur les ACE dans les SACL.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez des ACE et ajoutez-les aux CLS NTFS	`vserver security file-directory ntfs sacl add`
Modifier les ACE existants dans les SACL NTFS	`vserver security file-directory ntfs sacl modify`
Affiche des informations sur les ACE existants dans les CLS NTFS	`vserver security file-directory ntfs sacl show`
Supprimez les ACE existants des SACL NTFS	`vserver security file-directory ntfs sacl remove`

Pour en savoir plus, `vserver security file-directory ntfs sacl` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des politiques de sécurité SMB

Il existe des commandes ONTAP spécifiques pour gérer les stratégies de sécurité. Vous pouvez afficher des informations sur les règles et supprimer les règles. Vous ne pouvez pas modifier une stratégie de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer des stratégies de sécurité	`vserver security file-directory policy create`
Affiche des informations sur les stratégies de sécurité	`vserver security file-directory policy show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Supprimer des stratégies de sécurité	`vserver security file-directory policy delete`

Pour en savoir plus, `vserver security file-directory policy` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des tâches de politique de sécurité SMB

Il existe des commandes ONTAP permettant d'ajouter, de modifier, de supprimer et d'afficher des informations relatives aux tâches de la stratégie de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajouter des tâches de stratégie de sécurité	`vserver security file-directory policy task add`
Modifier les tâches de stratégie de sécurité	`vserver security file-directory policy task modify`
Afficher des informations sur les tâches de stratégie de sécurité	`vserver security file-directory policy task show`
Supprimer les tâches de stratégie de sécurité	`vserver security file-directory policy task remove`

Pour en savoir plus, `vserver security file-directory policy task` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des tâches de politique de sécurité SMB

Des commandes ONTAP permettent d'interrompre, de reprendre, d'arrêter et d'afficher des informations sur les tâches de stratégie de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Interrompre les tâches de stratégie de sécurité	`vserver security file-directory job pause -vserver vserver_name -id integer`
Reprendre les tâches de stratégie de sécurité	`vserver security file-directory job resume -vserver vserver_name -id integer`
Affiche des informations sur les tâches de stratégie de sécurité	`vserver security file-directory job show -vserver vserver_name` Vous pouvez déterminer l'ID d'un travail à l'aide de cette commande.

Les fonctions que vous recherchez…	Utilisez cette commande…
Arrêtez les tâches de stratégie de sécurité	`vserver security file-directory job stop -vserver vserver_name -id integer`

Pour en savoir plus, `vserver security file-directory job` consultez le "Référence de commande ONTAP".

Configurez le cache des métadonnées pour les partages SMB

En savoir plus sur la mise en cache des métadonnées ONTAP SMB

La mise en cache des métadonnées permet la mise en cache des attributs de fichier sur les clients SMB 1.0 pour un accès plus rapide aux attributs des fichiers et des dossiers. Vous pouvez activer ou désactiver la mise en cache des attributs par partage. Vous pouvez également configurer le temps de mise en service des entrées mises en cache si la mise en cache des métadonnées est activée. La configuration de la mise en cache des métadonnées n'est pas nécessaire si les clients se connectent aux partages SMB 2.x ou SMB 3.0.

Lorsqu'il est activé, le cache de métadonnées SMB stocke les données d'attribut de chemin et de fichier pendant un temps limité. Ceci peut améliorer les performances SMB des clients SMB 1.0 avec des charges de travail communes.

Pour certaines tâches, SMB crée un trafic important, pouvant inclure plusieurs requêtes identiques pour les métadonnées des chemins d'accès et des fichiers. Vous pouvez réduire le nombre de requêtes redondantes et améliorer les performances des clients SMB 1.0 en utilisant la mise en cache de métadonnées SMB pour récupérer les informations du cache.

> Même si cela est peu probable, il est possible que le cache de métadonnées transmette des informations obsolètes aux clients SMB 1.0. Si votre environnement ne peut pas se permettre ce risque, vous ne devez pas activer cette fonctionnalité.

Activer le cache de métadonnées ONTAP SMB

Vous pouvez améliorer les performances SMB des clients SMB 1.0 en activant le cache de métadonnées SMB. Par défaut, la mise en cache des métadonnées SMB est désactivée.

Étape

1. Effectuez l'action souhaitée :

Les fonctions que vous recherchez…	Entrez la commande…
Activez la mise en cache des métadonnées SMB lorsque vous créez un partage	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`

Les fonctions que vous recherchez…	Entrez la commande…
Activez la mise en cache des métadonnées SMB sur un partage existant	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Informations associées

- Configurer la durée de vie des entrées du cache de métadonnées
- Ajouter ou supprimer des propriétés de partage sur des partages existants

Configurer la durée de vie des entrées du cache de métadonnées ONTAP SMB

Vous pouvez configurer la durée de vie des entrées du cache de métadonnées SMB afin d'optimiser les performances du cache de métadonnées SMB dans votre environnement. La valeur par défaut est 10 secondes.

Avant de commencer

Vous devez avoir activé la fonctionnalité de cache de métadonnées SMB. Si le cache des métadonnées SMB n'est pas activé, le paramètre TTL du cache SMB n'est pas utilisé.

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez configurer la durée de vie des entrées du cache de métadonnées SMB lorsque vous…	Entrez la commande…
Créer un partage	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]`
Modifier un partage existant	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]`

Vous pouvez spécifier d'autres options et propriétés de configuration de partage lorsque vous créez ou modifiez des partages. Pour en savoir plus, `vserver cifs share` consultez le "Référence de commande ONTAP".

Gérer les verrous de fichier

En savoir plus sur le verrouillage des fichiers SMB ONTAP entre les protocoles

Le verrouillage de fichier est une méthode utilisée par les applications client pour empêcher un utilisateur d'accéder à un fichier précédemment ouvert par un autre

utilisateur. Le mode de verrouillage des fichiers par ONTAP dépend du protocole du client.

Si le client est un client NFS, les verrouillages sont consultatifs ; si le client est un client SMB, les verrous sont obligatoires.

En raison des différences entre les verrouillages de fichiers NFS et SMB, un client NFS peut ne pas accéder à un fichier précédemment ouvert par une application SMB.

Ce qui suit se produit lorsqu'un client NFS tente d'accéder à un fichier verrouillé par une application SMB :

- Dans les volumes mixtes ou NTFS, les opérations de manipulation de fichiers telles que `rm`, `rmdir`, et `mv` Peut entraîner l'échec de l'application NFS.
- Les opérations de lecture et d'écriture NFS sont refusées par les modes SMB Deny-read et deny-write open, respectivement.
- Les opérations d'écriture NFS échouent lorsque la plage d'écriture du fichier est verrouillée par un bytelock SMB exclusif.
- Dissocier
  - Pour les systèmes de fichiers NTFS, les opérations de suppression SMB et CIFS sont prises en charge.

    Le fichier sera supprimé après la dernière fermeture.
  - Les opérations de liaison NFS ne sont pas prises en charge.

    Elle n'est pas prise en charge car les sémantiques NTFS et SMB sont requises et l'opération dernière suppression-fermeture n'est pas prise en charge pour NFS.
  - Pour les systèmes de fichiers UNIX, l'opération de liaison est prise en charge.

    Il est pris en charge car la sémantique NFS et UNIX est requise.
- Renommer
  - Pour les systèmes de fichiers NTFS, si le fichier de destination est ouvert depuis SMB ou CIFS, le fichier de destination peut être renommé.
  - Le renommage NFS n'est pas pris en charge.

    Elle n'est pas prise en charge car NTFS et la sémantique SMB sont requises.

Dans les volumes de style de sécurité UNIX, les opérations de dissociation NFS et de renommage ignorent l'état du verrouillage SMB et permettent l'accès au fichier. Toutes les autres opérations NFS sur des volumes de type sécurité UNIX respectent l'état de verrouillage SMB.

En savoir plus sur les bits en lecture seule ONTAP SMB

Le bit de lecture seule est défini fichier par fichier pour indiquer si un fichier est inscriptible (désactivé) ou en lecture seule (activé).

Les clients SMB qui utilisent Windows peuvent définir un bit en lecture seule par fichier. Les clients NFS ne définissent pas de bit en lecture seule par fichier, car les clients NFS ne disposent d'aucune opération de protocole utilisant un bit en lecture seule par fichier.

ONTAP peut définir un bit en lecture seule sur un fichier lorsqu'un client SMB utilisant Windows crée ce fichier. ONTAP peut également définir un bit en lecture seule lorsqu'un fichier est partagé entre les clients NFS et les clients SMB. Certains logiciels, lorsqu'ils sont utilisés par des clients NFS et SMB, nécessitent l'activation du bit en lecture seule.

Pour que ONTAP garde les autorisations appropriées en lecture et écriture sur un fichier partagé entre les clients NFS et les clients SMB, il traite le bit en lecture seule conformément aux règles suivantes :

- NFS traite tous les fichiers dont le bit de lecture seule est activé comme s'il n'a pas de bits d'autorisation d'écriture activés.
- Si un client NFS désactive tous les bits d'autorisation d'écriture et qu'au moins un de ces bits avait été précédemment activé, ONTAP active le bit en lecture seule pour ce fichier.
- Si un client NFS active un bit d'autorisation d'écriture, ONTAP désactive le bit en lecture seule pour ce fichier.
- Si le bit de lecture seule d'un fichier est activé et qu'un client NFS tente de détecter les autorisations pour le fichier, les bits d'autorisation du fichier ne sont pas envoyés au client NFS. ONTAP envoie les bits d'autorisation au client NFS avec les bits d'autorisation d'écriture masqués.
- Si le bit de lecture seule d'un fichier est activé et qu'un client SMB désactive le bit de lecture seule, ONTAP active le bit d'autorisation d'écriture du propriétaire pour le fichier.
- Les fichiers dont le bit de lecture seule est activé sont accessibles en écriture uniquement par root.

Le bit en lecture seule interagit avec les bits de mode ACL et Unix des manières suivantes :

Lorsque le bit de lecture seule est défini sur un fichier :

- Aucune modification n'est apportée à la liste de contrôle d'accès (ACL) pour ce fichier. Les clients NFS verront la même liste de contrôle d'accès qu'avant la définition du bit de lecture seule.
- Tous les bits du mode Unix qui autorisent l'accès en écriture au fichier sont ignorés.
- Les clients NFS et SMB peuvent lire le fichier, mais ils ne peuvent pas le modifier.
- Les ACL et les bits du mode UNIX sont ignorés au profit du bit de lecture seule. Cela signifie que même si l'ACL autorise l'accès en écriture, le bit de lecture seule empêche toute modification.

Lorsque le bit de lecture seule n'est pas défini sur un fichier :

- ONTAP détermine l'accès en fonction des bits de mode ACL et UNIX.
  - Si l'ACL ou les bits du mode UNIX refusent l'accès en écriture, les clients NFS et SMB ne peuvent pas modifier le fichier.
  - Si ni les bits de mode ACL ni les bits de mode UNIX ne refusent l'accès en écriture, les clients NFS et SMB peuvent modifier le fichier.

Les modifications des autorisations liées aux fichiers sont immédiatement appliquées aux clients SMB, mais elles peuvent ne pas être immédiatement appliquées aux clients NFS si le client NFS active la mise en cache des attributs.

La façon dont ONTAP diffère de Windows dans la gestion des verrous sur les composants de chemin de partage

Contrairement à Windows, ONTAP ne verrouille pas chaque composant du chemin d'accès à un fichier ouvert lorsque le fichier est ouvert. Ce comportement affecte également les chemins de partage SMB.

Étant donné que ONTAP ne verrouille pas chaque composant du chemin d'accès, il est possible de renommer un composant de chemin au-dessus du fichier ou du partage ouvert, ce qui peut causer des problèmes pour certaines applications ou peut rendre le chemin de partage dans la configuration SMB invalide. Cela peut rendre le partage inaccessible.

Pour éviter les problèmes causés par la modification du nom des composants du chemin d'accès, vous pouvez appliquer des paramètres de sécurité qui empêchent les utilisateurs ou les applications de renommer les répertoires critiques.

Afficher des informations sur les verrous SMB ONTAP

Vous pouvez afficher des informations sur les verrous de fichier en cours, y compris les types de verrous qui sont conservés et l'état de verrouillage, les détails sur les verrous de plage d'octets, les modes de verrouillage de sharelock, les verrous de délégation et les verrous opportunistes, et si les verrous sont ouverts avec des poignées durables ou persistantes.

Description de la tâche

L'adresse IP du client ne peut pas être affichée pour les verrouillages établis via NFS V4 ou NFS v4.1.

Par défaut, la commande affiche des informations relatives à tous les verrouillages. Vous pouvez utiliser les paramètres de la commande pour afficher des informations sur les verrous d'une machine virtuelle de stockage (SVM) spécifique ou pour filtrer les résultats de la commande par d'autres critères.

Le `vserver locks show` la commande affiche des informations sur quatre types de verrous :

- Les verrous de plage d'octets, qui verrouillent uniquement une partie d'un fichier.
- Verrous de partage, qui verrouillent les fichiers ouverts.
- Verrouillages opportunistes, qui contrôlent la mise en cache côté client sur SMB.
- Des délégations qui contrôlent la mise en cache côté client sur NFSv4.x.

En spécifiant des paramètres facultatifs, vous pouvez déterminer des informations importantes sur chaque type de verrou. Pour en savoir plus, `vserver locks show` consultez le "Référence de commande ONTAP".

Étape

1. Affiche des informations sur les verrous à l'aide de `vserver locks show` commande.

Exemples

L'exemple suivant présente un récapitulatif des informations relatives à un verrouillage NFSv4 sur un fichier avec le chemin d'accès `/vol1/file1`. Le mode d'accès de sharelock est Write-deny_none et le verrou a été accordé avec la délégation d'écriture :

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

L'exemple suivant affiche des informations détaillées sur le verrou SMB d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un descripteur durable est accordé sur le fichier avec un mode d'accès à verrouillage de partage Write-Deny_none à un client dont l'adresse IP est 10.3.1.3. Un oplock de location est accordé avec un niveau de oplock de lot :

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
```

```
                    Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Briser les verrous SMB ONTAP

Lorsque des verrous de fichier empêchent l'accès client aux fichiers, vous pouvez afficher des informations sur les verrous actuellement mis en attente, puis interrompre des verrous spécifiques. Les applications de débogage sont des exemples de scénarios dans lesquels vous devrez peut-être interrompre les verrous.

Description de la tâche

```
`vserver locks break`La commande n'est disponible qu'au niveau de
privilège avancé et supérieur. Pour en savoir plus, `vserver locks break`
consultez le link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-
break.html["Référence de commande ONTAP"^].
```

Étapes

1. Pour trouver les informations dont vous avez besoin pour interrompre un verrouillage, utilisez le `vserver locks show` commande.

   Pour en savoir plus, `vserver locks show` consultez le "Référence de commande ONTAP".

2. Définissez le niveau de privilège sur avancé : `set -privilege advanced`

3. Effectuez l'une des opérations suivantes :

Si vous voulez rompre un verrou en spécifiant…	Entrez la commande…
Le nom du SVM, le nom du volume, le nom de la LIF et le chemin de fichier	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
L'ID de verrouillage	`vserver locks break -lockid UUID`

4. Retour au niveau de privilège admin : `set -privilege admin`

Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Surveiller l'activité des PME

Afficher les informations de session ONTAP SMB

Vous pouvez afficher des informations sur les sessions SMB établies, notamment la connexion SMB et l'ID de session ainsi que l'adresse IP du poste de travail à l'aide de la session. Vous pouvez afficher des informations sur la version du protocole SMB de la session et le niveau de protection disponible en continu, ce qui vous aide à déterminer si cette session prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher les informations de toutes les sessions de votre SVM sous forme récapitulative. Cependant, dans de nombreux cas, la quantité de sortie renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs :

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie des champs que vous choisissez.

  Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les sessions SMB établies.
- Vous pouvez utiliser le `-fields` ou le `-instance` paramètre seul ou associé à d'autres paramètres facultatifs.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
Pour toutes les sessions sur le SVM sous forme résumée	`vserver cifs session show -vserver vserver_name`
Sur un ID de connexion spécifié	`vserver cifs session show -vserver vserver_name -connection-id integer`

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
À partir d'une adresse IP de poste de travail spécifiée	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Sur une adresse IP LIF spécifiée	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Sur un nœud spécifié	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	D'un utilisateur Windows spécifié
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Avec un mécanisme d'authentification spécifié
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Avec une version de protocole spécifiée	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== La protection et SMB Multichannel sont disponibles en continu uniquement pour les sessions SMB 3.0 et ultérieures. Pour afficher leur statut sur toutes les sessions de qualification, vous devez spécifier ce paramètre avec la valeur définie sur `SMB3` ou ultérieure. ====
Avec un niveau spécifié de protection disponible en continu	`vserver cifs session show -vserver vserver_name -continuously-available {No

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
Yes	Partial}`  [NOTE] ==== Si l'état disponible en continu est de `Partial`, cela signifie que la session contient au moins un fichier ouvert en continu disponible, mais que la session contient certains fichiers qui ne sont pas ouverts avec une protection disponible en continu. Vous pouvez utiliser le `vserver cifs sessions file show` commande permettant de déterminer quels fichiers de la session établie ne sont pas ouverts avec une protection disponible en continu. ====
Avec un état de session de signature SMB spécifié	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Exemples

La commande suivante affiche les informations relatives aux sessions sur le SVM vs1 établies à partir d'un poste de travail avec l'adresse IP 10.1.1.1 :

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

La commande suivante affiche des informations détaillées pour les sessions avec protection disponible en continu sur le SVM vs1. La connexion a été établie à l'aide du compte de domaine.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
          Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

La commande suivante affiche les informations relatives aux sessions sur une session utilisant SMB 3.0 et SMB Multichannel sur le SVM vs1. Dans l'exemple, l'utilisateur connecté à ce partage à un client SMB 3.0 en utilisant l'adresse IP du LIF ; par conséquent, le mécanisme d'authentification par défaut est NTLMv2. La connexion doit se faire à l'aide de l'authentification Kerberos pour se connecter à une protection disponible en continu.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                 NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informations associées

Affichage des informations relatives aux fichiers SMB ouverts

Afficher des informations sur les fichiers SMB ONTAP ouverts

Vous pouvez afficher des informations sur les fichiers SMB ouverts, notamment la connexion SMB et l'ID de session, le volume hôte, le nom du partage et le chemin du partage. Vous pouvez afficher des informations sur le niveau de protection disponible en continu d'un fichier, ce qui permet de déterminer si un fichier ouvert est dans un état qui prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher des informations sur les fichiers ouverts dans une session SMB établie. Les informations affichées sont utiles lorsque vous devez déterminer les informations de session SMB pour des fichiers particuliers dans une session SMB.

Par exemple, si vous disposez d'une session SMB où certains fichiers ouverts sont ouverts avec une protection disponible en continu et certains ne sont pas ouverts avec une protection disponible en continu (valeur pour le `-continuously-available` champ dans `vserver cifs session show` la sortie de la commande est `Partial`), vous pouvez déterminer quels fichiers ne sont pas disponibles en continu à l'aide de cette commande.

Vous pouvez afficher les informations de tous les fichiers ouverts sur des sessions SMB établies sur des SVM

(Storage Virtual machines) sous forme de récapitulatif à l'aide de `vserver cifs session file show` commande sans paramètres facultatifs.

Cependant, dans de nombreux cas, la quantité de production renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque vous souhaitez afficher des informations pour un petit sous-ensemble de fichiers ouverts uniquement.

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie sur les champs de votre choix.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les fichiers SMB ouverts.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
Sur le SVM sous forme résumée	`vserver cifs session file show -vserver vserver_name`
Sur un nœud spécifié	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	Sur un ID de fichier spécifié
`vserver cifs session file show -vserver vserver_name -file-id integer`	Sur un ID de connexion SMB spécifié
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Sur un ID de session SMB spécifié
`vserver cifs session file show -vserver vserver_name -session-id integer`	Sur l'agrégat d'hébergement spécifié
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Sur le volume spécifié
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	Sur le partage SMB spécifié

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
`vserver cifs session file show -vserver vserver_name -share share_name`	Sur le chemin SMB spécifié
`vserver cifs session file show -vserver vserver_name -path path`	Avec le niveau spécifié de protection disponible en continu
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Si l'état disponible en continu est de `No`, cela signifie que ces fichiers ouverts ne peuvent pas être rétablis sans interruption à partir du basculement et du rétablissement. Ils ne peuvent pas non plus récupérer d'une relocalisation générale entre les partenaires dans une relation de haute disponibilité. ====
Avec l'état reconnecté spécifié	`vserver cifs session file show -vserver vserver_name -reconnected {No

D'autres paramètres facultatifs peuvent être utilisés pour affiner les résultats de sortie. Pour en savoir plus, `vserver cifs session file show` consultez le "Référence de commande ONTAP".

Exemples

L'exemple suivant affiche les informations sur les fichiers ouverts sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

L'exemple suivant affiche des informations détaillées sur les fichiers SMB ouverts avec l'ID de fichier 82 sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informations associées

Afficher les informations de session

Déterminer les statistiques, les objets et les compteurs disponibles sur les serveurs ONTAP SMB

Avant d'obtenir des informations sur les statistiques de hachage CIFS, SMB, d'audit et de BranchCache, ainsi que sur les performances, vous devez connaître les objets et compteurs disponibles, à partir desquels vous pouvez obtenir des données.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez déterminer…	Entrer…
Les objets disponibles	`statistics catalog object show`
Objets spécifiques disponibles	`statistics catalog object show -object object_name`
Quels compteurs sont disponibles	`statistics catalog counter show -object object_name`

Pour en savoir plus sur `statistics catalog object show`, y compris les objets et les compteurs disponibles, consultez le "Référence de commande ONTAP".

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemples

La commande suivante affiche la description des objets statistiques sélectionnés relatifs à l'accès CIFS et SMB au cluster, comme s'il s'affiche au niveau de privilège avancé :

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

La commande suivante affiche des informations sur certains compteurs de `cifs` objet tel qu'il apparaît au

niveau de privilège avancé :

Cet exemple n’affiche pas tous les compteurs disponibles pour le `cifs` objet ; la sortie est tronquée.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Informations associées

- Affiche les statistiques
- "compteur de catalogue de statistiques afficher l'objet"

- "les statistiques commencent"

Afficher les statistiques ONTAP SMB

Vous pouvez afficher plusieurs statistiques, notamment des statistiques sur CIFS et SMB, l'audit et des hachages de BranchCache, pour surveiller les performances et diagnostiquer les problèmes.

Avant de commencer

Vous devez avoir collecté des échantillons de données à l'aide du `statistics start` et `statistics stop` commandes avant de pouvoir afficher les informations relatives aux objets.

En savoir plus sur `statistics start` et `statistics stop` dans le "Référence de commande ONTAP" .

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Pour afficher les statistiques de…	Entrer…
Toutes les versions de SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x et SMB 3.0	`statistics show -object smb2`
Sous-système CIFS du nœud	`statistics show -object nblade_cifs`
Audit multiprotocole	`statistics show -object audit_ng`
Service de hachage BranchCache	`statistics show -object hashd`
DNS dynamique	`statistics show -object ddns_update`

   Pour en savoir plus, `statistics show` consultez le "Référence de commande ONTAP".

3. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

- Déterminer quelles statistiques, quels objets et quels compteurs sont disponibles sur les serveurs
- Contrôle des statistiques de session signées SMB
- Afficher les statistiques de BranchCache
- Utilisez les statistiques pour surveiller l'activité de renvoi automatique des nœuds
- "Configuration SMB pour Microsoft Hyper-V et SQL Server"
- "Configuration du contrôle des performances"

Déploiement des services basés sur les clients SMB

Utilisez les fichiers hors ligne pour permettre la mise en cache des fichiers pour une utilisation hors ligne

En savoir plus sur l'utilisation de fichiers hors ligne pour permettre la mise en cache des fichiers ONTAP SMB pour une utilisation hors ligne

ONTAP prend en charge la fonctionnalité de fichiers hors ligne Microsoft, ou *mise en cache côté client*, qui permet de mettre les fichiers en cache sur l'hôte local pour une utilisation hors ligne. Les utilisateurs peuvent utiliser la fonctionnalité fichiers hors ligne pour continuer à travailler sur des fichiers même lorsqu'ils sont déconnectés du réseau.

Vous pouvez spécifier si les documents et programmes utilisateur Windows sont automatiquement mis en cache sur un partage ou si les fichiers doivent être sélectionnés manuellement pour la mise en cache. La mise en cache manuelle est activée par défaut pour les nouveaux partages. Les fichiers mis hors ligne sont synchronisés avec le disque local du client Windows. La synchronisation a lieu lorsque la connectivité réseau à un partage de système de stockage spécifique est restaurée.

Étant donné que les fichiers et dossiers hors ligne conservent les mêmes autorisations d'accès que la version des fichiers et dossiers enregistrés sur le serveur CIFS, l'utilisateur doit disposer des autorisations suffisantes sur les fichiers et dossiers enregistrés sur le serveur CIFS pour effectuer des actions sur les fichiers et dossiers hors ligne.

Lorsque l'utilisateur et une autre personne du réseau modifient le même fichier, l'utilisateur peut enregistrer la version locale du fichier sur le réseau, conserver l'autre version ou enregistrer les deux. Si l'utilisateur conserve les deux versions, un nouveau fichier avec les modifications de l'utilisateur local est enregistré localement et le fichier mis en cache est écrasé par des modifications de la version du fichier enregistré sur le serveur CIFS.

Vous pouvez configurer des fichiers hors ligne par partage à l'aide des paramètres de configuration du partage. Vous pouvez choisir l'une des quatre configurations de dossiers hors ligne lorsque vous créez ou modifiez des partages :

- Pas de mise en cache

  Désactive la mise en cache côté client pour le partage. Les fichiers et les dossiers ne sont pas automatiquement mis en cache localement sur les clients et les utilisateurs ne peuvent pas choisir de mettre en cache des fichiers ou des dossiers localement.

- Mise en cache manuelle

  Permet la sélection manuelle des fichiers à mettre en cache sur le partage. Il s'agit du paramètre par défaut. Par défaut, aucun fichier ni dossier n'est mis en cache sur le client local. Les utilisateurs peuvent choisir les fichiers et dossiers qu'ils souhaitent mettre en cache localement pour une utilisation hors ligne.

- Mise en cache automatique des documents

  Permet de mettre automatiquement en cache les documents utilisateur sur le partage. Seuls les fichiers et les dossiers accessibles sont mis en cache localement.

- Mise en cache automatique des programmes

  Permet de mettre automatiquement en cache les programmes et les documents utilisateur sur le partage. Seuls les fichiers, les dossiers et les programmes accessibles sont mis en cache localement. De plus, ce

paramètre permet au client d'exécuter des exécutables mis en cache localement, même lorsqu'il est connecté au réseau.

Pour plus d'informations sur la configuration des fichiers hors ligne sur les serveurs et les clients Windows, consultez la bibliothèque Microsoft TechNet.

Informations associées

- Utilisation de profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur CIFS associé à la SVM
- En savoir plus sur l'utilisation de la redirection de dossiers pour stocker des données sur des serveurs
- Découvrez comment utiliser BranchCache pour mettre en cache le contenu partagé dans une succursale
- "Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

En savoir plus sur les exigences d'utilisation des fichiers SMB ONTAP hors ligne

Avant de pouvoir utiliser la fonctionnalité Microsoft Offline Files avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

Les versions d'ONTAP prennent en charge les fichiers hors ligne.

Version requise du protocole SMB

Pour le SVM (Storage Virtual machine), ONTAP prend en charge les fichiers hors ligne dans toutes les versions de SMB.

Configuration requise pour le client Windows

Le client Windows doit prendre en charge les fichiers hors ligne.

Pour obtenir les informations les plus récentes sur les clients Windows prenant en charge la fonctionnalité fichiers hors ligne, reportez-vous à la matrice d'interopérabilité.

"mysupport.netapp.com/matrix"

Directives pour le déploiement de fichiers SMB ONTAP hors ligne

Il existe certaines directives importantes que vous devez comprendre lorsque vous déployez des fichiers hors ligne sur des partages de répertoire personnel qui possèdent le `showsnapshot` propriété de partage définie sur les répertoires d'accueil.

Si la `showsnapshot` propriété de partage est définie sur un partage de répertoire de base sur lequel des fichiers hors ligne sont configurés, les clients Windows mettent en cache tous les snapshots sous le `~snapshot` dossier du répertoire de base de l'utilisateur.

Les clients Windows mettent en cache tous les snapshots sous le répertoire de base si l'une des conditions suivantes est vraie :

- L'utilisateur rend le répertoire personnel disponible hors ligne à partir du client.

Le contenu du `~snapshot` le dossier du répertoire personnel est inclus et rendu disponible hors ligne.

- L'utilisateur configure la redirection de dossier pour rediriger un dossier tel que `My Documents` À la racine d'un répertoire local résidant sur le partage CIFS Server.

  Certains clients Windows peuvent rendre automatiquement le dossier redirigé hors ligne. Si le dossier est redirigé vers la racine du répertoire de base, le `~snapshot` le dossier est inclus dans le contenu hors ligne mis en cache.

> Les déploiements de fichiers hors ligne où le `~snapshot` dossier est inclus dans les fichiers hors ligne doivent être évités. Les snapshots du `~snapshot` dossier contiennent toutes les données du volume au moment où ONTAP a créé le snapshot. Par conséquent, la création d'une copie hors ligne du dossier consomme une `~snapshot` quantité importante de stockage local sur le client, consomme de la bande passante réseau pendant la synchronisation des fichiers hors ligne et augmente le temps nécessaire à la synchronisation des fichiers hors ligne.

Commandes ONTAP pour configurer la prise en charge des fichiers SMB hors ligne

Vous pouvez configurer la prise en charge des fichiers hors ligne à l'aide de l'interface de ligne de commandes ONTAP en spécifiant l'un des quatre paramètres de fichier hors ligne lorsque vous créez des partages SMB ou en modifiant à tout moment des partages SMB existants. La prise en charge des fichiers manuels hors ligne est le paramètre par défaut.

Description de la tâche

Lors de la configuration de la prise en charge des fichiers hors ligne, vous pouvez choisir l'un des quatre paramètres de fichiers hors ligne suivants :

Réglage	Description
`none`	Interdire aux clients Windows de mettre en cache les fichiers sur ce partage.
`manual`	Permet aux utilisateurs des clients Windows de sélectionner manuellement les fichiers à mettre en cache.
`documents`	Permet aux clients Windows de mettre en cache les documents utilisateur qui sont utilisés par l'utilisateur pour l'accès hors ligne.
`programs`	Permet aux clients Windows de mettre en cache les programmes utilisés par l'utilisateur pour l'accès hors ligne. Les clients peuvent utiliser les fichiers de programme mis en cache en mode hors ligne, même si le partage est disponible.

Vous ne pouvez choisir qu'un seul paramètre de fichier hors ligne. Si vous modifiez un paramètre de fichiers hors ligne sur un partage SMB existant, le nouveau paramètre de fichiers hors ligne remplace le paramètre d'origine. Les autres paramètres de configuration et propriétés de partage SMB existants ne sont ni supprimés

ni remplacés. Ils restent en vigueur jusqu'à ce qu'ils soient explicitement supprimés ou modifiés.

Étapes

1. Effectuez l'action appropriée :

Si vous souhaitez configurer des fichiers hors ligne sur…	Entrez la commande…
Un nouveau partage SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Un partage SMB existant
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Vérifiez que la configuration du partage SMB est correcte : `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemple

La commande suivante crée un partage SMB nommé "data1" avec des fichiers hors ligne définis sur `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

La commande suivante modifie un partage SMB existant nommé "data1" en changeant le paramètre fichiers hors ligne sur `manual` et ajout de valeurs pour le masque de création de mode fichier et répertoire :

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informations associées

Ajouter ou supprimer des propriétés de partage sur des partages existants

Configurer la prise en charge des fichiers hors ligne sur les partages SMB ONTAP à l'aide de la console MMC de gestion de l'ordinateur

Si vous souhaitez autoriser les utilisateurs à mettre en cache des fichiers localement pour une utilisation hors ligne, vous pouvez configurer la prise en charge des fichiers hors ligne à l'aide de la console MMC gestion de l'ordinateur (Microsoft Management Console).

Étapes

1. Pour ouvrir la console MMC sur votre serveur Windows, dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur l'icône de l'ordinateur local, puis sélectionnez **gérer**.
2. Dans le panneau de gauche, sélectionnez **Computer Management**.
3. Sélectionnez **action** > **connexion à un autre ordinateur**.

   La boîte de dialogue Sélectionner un ordinateur s'affiche.

4. Tapez le nom du serveur CIFS ou cliquez sur **Browse** pour localiser le serveur CIFS.

   Si le nom du serveur CIFS est identique au nom d'hôte SVM (Storage Virtual machine), tapez le nom du

SVM. Si le nom du serveur CIFS est différent du nom d'hôte du SVM, tapez le nom du serveur CIFS.

5. Cliquez sur **OK**.
6. Dans l'arborescence de la console, cliquez sur **Outils système** > **dossiers partagés**.
7. Cliquez sur **partages**.
8. Dans le volet des résultats, cliquez avec le bouton droit de la souris sur le partage.
9. Cliquez sur **Propriétés**.

   Les propriétés du partage sélectionné s'affichent.

10. Dans l'onglet **général**, cliquez sur **Paramètres hors ligne**.

    La boîte de dialogue Paramètres hors ligne s'affiche.

11. Configurez les options de disponibilité hors ligne selon les besoins.
12. Cliquez sur **OK**.

Utilisez les profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur SMB associé à la SVM

En savoir plus sur l'utilisation des profils itinérants pour stocker les profils utilisateur ONTAP SMB de manière centralisée

ONTAP prend en charge le stockage des profils itinérants Windows sur un serveur CIFS associé à la machine virtuelle de stockage (SVM). La configuration des profils itinérants d'utilisateurs offre des avantages à l'utilisateur, tels que la disponibilité automatique des ressources, quel que soit l'endroit où l'utilisateur se connecte. Les profils itinérants simplifient également l'administration et la gestion des profils utilisateur.

Les profils utilisateur itinérants présentent les avantages suivants :

- Disponibilité automatique des ressources

  Le profil unique d'un utilisateur est automatiquement disponible lorsque cet utilisateur se connecte à n'importe quel ordinateur du réseau exécutant Windows 8, Windows 7, Windows 2000 ou Windows XP. Les utilisateurs n'ont pas besoin de créer de profil sur chaque ordinateur qu'ils utilisent sur un réseau.

- Remplacement simplifié de l'ordinateur

  Étant donné que toutes les informations de profil de l'utilisateur sont conservées séparément sur le réseau, le profil de l'utilisateur peut être facilement téléchargé sur un nouvel ordinateur de remplacement. Lorsque l'utilisateur se connecte au nouvel ordinateur pour la première fois, la copie du profil de l'utilisateur est copiée sur le nouvel ordinateur.

Informations associées

- En savoir plus sur l'utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne
- En savoir plus sur l'utilisation de la redirection de dossiers pour stocker des données sur des serveurs

En savoir plus sur les exigences d'utilisation des profils SMB ONTAP itinérants

Avant de pouvoir utiliser les profils itinérants de Microsoft avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

ONTAP prend en charge les profils itinérants.

Version requise du protocole SMB

Pour le serveur virtuel de stockage (SVM), ONTAP prend en charge les profils itinérants sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser les profils itinérants, le client Windows doit prendre en charge cette fonctionnalité.

Pour obtenir les dernières informations sur les clients Windows qui prennent en charge les profils itinérants, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

Configurer les profils SMB ONTAP itinérants via la console MMC Utilisateurs et ordinateurs Active Directory

Si vous souhaitez rendre automatiquement le profil d'un utilisateur disponible lorsque cet utilisateur se connecte à n'importe quel ordinateur du réseau, vous pouvez configurer des profils itinérants via le composant logiciel enfichable MMC utilisateurs et ordinateurs Active Directory. Si vous configurez des profils itinérants sur Windows Server, vous pouvez utiliser le Centre d'administration Active Directory.

Étapes

1. Sur le serveur Windows, ouvrez la MMC utilisateurs et ordinateurs Active Directory (ou le Centre d'administration Active Directory sur les serveurs Windows).
2. Recherchez l'utilisateur pour lequel vous souhaitez configurer un profil d'itinérance.
3. Cliquez avec le bouton droit de la souris sur l'utilisateur et cliquez sur **Propriétés**.
4. Dans l'onglet **profil**, entrez le chemin du profil vers le partage où vous souhaitez stocker le profil d'itinérance de l'utilisateur, suivi de `%username%`.

   Par exemple, un chemin de profil peut être le suivant : `\\vs1.example.com\profiles\%username%`. La première fois qu'un utilisateur se connecte, `%username%` est remplacé par le nom de l'utilisateur.

   > Dans le chemin `\\vs1.example.com\profiles\%username%`, `profiles` Est le nom de partage d'un partage sur SVM (Storage Virtual machine) vs1 qui dispose de droits de contrôle total pour tous.

5. Cliquez sur **OK**.

Utiliser la redirection de dossiers pour stocker des données sur un serveur SMB

Découvrez comment utiliser la redirection de dossiers pour stocker des données sur les serveurs ONTAP SMB

ONTAP prend en charge la redirection de dossiers Microsoft, qui permet aux utilisateurs ou aux administrateurs de rediriger le chemin d'un dossier local vers un emplacement sur le serveur CIFS. Il apparaît comme si les dossiers redirigés sont stockés sur le client Windows local, même si ces données sont stockées dans un partage SMB.

La redirection de dossiers s'adresse principalement aux entreprises qui ont déjà déployé des répertoires locaux et qui souhaitent maintenir la compatibilité avec leur environnement de home Directory existant.

- `Documents`, `Desktop`, et `Start Menu` sont des exemples de dossiers que vous pouvez rediriger.
- Les utilisateurs peuvent rediriger les dossiers à partir de leur client Windows.
- Les administrateurs peuvent configurer et gérer de façon centralisée la redirection de dossiers en configurant des GPO dans Active Directory.
- Si les administrateurs ont configuré des profils itinérants, la redirection de dossiers permet aux administrateurs de diviser les données utilisateur à partir des données de profil.
- Les administrateurs peuvent utiliser la redirection de dossiers et les fichiers hors ligne ensemble pour rediriger le stockage des données des dossiers locaux vers le serveur CIFS, tout en permettant aux utilisateurs de mettre le contenu en cache localement.

Informations associées

- En savoir plus sur l'utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne
- Utilisation de profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur CIFS associé à la SVM

En savoir plus sur les exigences d'utilisation de la redirection de dossiers SMB ONTAP

Avant de pouvoir utiliser la redirection de dossiers de Microsoft avec votre serveur CIFS, vous devez connaître les versions de ONTAP et SMB et les clients Windows qui prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

ONTAP prend en charge la redirection de dossiers Microsoft.

Version requise du protocole SMB

Pour le serveur virtuel de stockage (SVM), ONTAP prend en charge la redirection de dossiers de Microsoft sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser la redirection de dossier de Microsoft, le client Windows doit prendre en charge cette fonctionnalité.

Pour obtenir les dernières informations sur les clients Windows prenant en charge la redirection de dossiers, consultez la matrice d'interopérabilité.

"mysupport.netapp.com/matrix"

Configurer la redirection de dossier SMB ONTAP à l'aide des propriétés Windows

Vous pouvez configurer la redirection de dossiers à l'aide de la fenêtre Propriétés de Windows. L'avantage de cette méthode est que l'utilisateur Windows peut configurer la redirection de dossiers sans l'aide de l'administrateur SVM.

Étapes

1. Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le dossier que vous souhaitez rediriger vers un partage réseau.
2. Cliquez sur **Propriétés**.

   Les propriétés du partage sélectionné s'affichent.

3. Dans l'onglet **raccourci**, cliquez sur **cible** et spécifiez le chemin d'accès à l'emplacement réseau où vous souhaitez rediriger le dossier sélectionné.

   Par exemple, si vous souhaitez rediriger un dossier vers le `data` dossier dans un répertoire personnel mappé sur `Q:\`, spécifiez `Q:\data` comme cible.

4. Cliquez sur **OK**.

   Pour plus d'informations sur la configuration des dossiers hors ligne, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

En savoir plus sur l'accès au répertoire ONTAP ~snapshot à partir des clients Windows à l'aide de SMB 2.x

La méthode que vous utilisez pour accéder au `~snapshot` répertoire à partir de clients Windows utilisant SMB 2.x diffère de celle utilisée pour SMB 1.0. Vous devez comprendre comment accéder au `~snapshot` répertoire lorsque vous utilisez des connexions SMB 2.x pour accéder aux données stockées dans les snapshots.

L'administrateur du SVM contrôle si les utilisateurs des clients Windows peuvent afficher et accéder à l' `~snapshot` répertoire sur un partage en activant ou désactivant le `showsnapshot` partager la propriété en utilisant les commandes du vserver cifs share properties familles.

Lorsque la `showsnapshot` propriété de partage est désactivée, un utilisateur d'un client Windows utilisant SMB 2.x ne peut pas afficher le `~snapshot` répertoire et ne peut pas accéder aux snapshots dans le `~snapshot` répertoire, même lorsque vous saisissez manuellement le chemin d'accès au `~snapshot` répertoire ou à des snapshots spécifiques dans le répertoire.

Lorsque le `showsnapshot` La propriété partager est activée, un utilisateur sur un client Windows utilisant SMB 2.x ne peut toujours pas afficher `~snapshot` répertoire soit à la racine du partage, soit dans une jonction ou un répertoire sous la racine du partage. Toutefois, après la connexion à un partage, l'utilisateur peut accéder au système masqué `~snapshot` en ajoutant manuellement le répertoire `\~snapshot` à la fin du chemin de partage. Le masqué `~snapshot` le répertoire est accessible à partir de deux points d'entrée :

- À la racine du partage
- À chaque point de jonction de l'espace de partage

Le masqué `~snapshot` le répertoire n'est pas accessible à partir de sous-répertoires non-jonctions dans le partage.

Exemple

Avec la configuration indiquée dans l'exemple suivant, un utilisateur d'un client Windows avec une connexion SMB 2.x au partage « eng » peut accéder à l' `~snapshot` en ajoutant manuellement le répertoire `\~snapshot` au chemin de partage à la racine du partage et à chaque point de jonction du chemin. Le masqué `~snapshot` le répertoire est accessible à partir des trois chemins suivants :

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Restaurez des fichiers et des dossiers à l'aide des versions précédentes

En savoir plus sur la récupération des fichiers et dossiers ONTAP SMB à l'aide des versions précédentes

La possibilité d'utiliser les versions précédentes de Microsoft s'applique aux systèmes de fichiers qui prennent en charge les instantanés sous une forme ou une autre et qui les ont activés. La technologie Snapshot fait partie intégrante de ONTAP. Les utilisateurs peuvent récupérer des fichiers et des dossiers à partir de snapshots à partir de leur client Windows en utilisant la fonction versions précédentes de Microsoft.

La fonctionnalité versions précédentes permet aux utilisateurs de parcourir les snapshots ou de restaurer des données à partir d'un snapshot sans l'intervention d'un administrateur de stockage. Les versions précédentes ne peuvent pas être configurées. Elle est toujours activée. Si l'administrateur du stockage a rendu des instantanés disponibles sur un partage, l'utilisateur peut utiliser les versions précédentes pour effectuer les tâches suivantes :

- Restaurer les fichiers supprimés par inadvertance.
- Récupération après écrasement accidentel d'un fichier.
- Comparer les versions du fichier pendant le fonctionnement.

Les données stockées dans les snapshots sont en lecture seule. Les utilisateurs doivent enregistrer une copie d'un fichier à un autre emplacement pour apporter des modifications au fichier. Les snapshots sont régulièrement supprimés. Par conséquent, les utilisateurs doivent créer des copies des fichiers contenus dans les versions précédentes s'ils souhaitent conserver indéfiniment une version précédente d'un fichier.

Exigences ONTAP SMB pour l'utilisation des versions précédentes de Microsoft

Avant de pouvoir utiliser les versions précédentes avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows le prennent en charge. Vous devez également connaître les exigences relatives aux paramètres de snapshot.

Configuration requise pour la version ONTAP

Prend en charge les versions précédentes.

Version requise du protocole SMB

Pour les machines virtuelles de stockage (SVM), ONTAP prend en charge les versions précédentes sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser les versions précédentes pour accéder aux données dans les instantanés, le client Windows doit prendre en charge cette fonctionnalité.

Pour obtenir les dernières informations sur les clients Windows prenant en charge les versions précédentes, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

Configuration requise pour les paramètres de snapshot

Pour utiliser les versions précédentes afin d'accéder aux données des instantanés, une stratégie d'instantanés activée doit être associée au volume contenant les données, les clients doivent pouvoir accéder aux données d'instantanés et des instantanés doivent exister.

Afficher et gérer les données de snapshot ONTAP SMB avec l'onglet Versions précédentes de Windows

Les utilisateurs des ordinateurs clients Windows peuvent utiliser l'onglet versions précédentes de la fenêtre Propriétés de Windows pour restaurer les données stockées dans les snapshots sans avoir à faire appel à l'administrateur de la machine virtuelle de stockage (SVM).

Description de la tâche

L'onglet versions précédentes permet uniquement d'afficher et de gérer les données des snapshots des données stockées sur le SVM si l'administrateur a activé les snapshots sur le volume contenant le partage et si l'administrateur configure le partage pour afficher les snapshots.

Étapes

1. Dans l'Explorateur Windows, affichez le contenu du lecteur mappé des données stockées sur le serveur CIFS.
2. Cliquez avec le bouton droit de la souris sur le fichier ou le dossier du lecteur réseau mappé dont vous souhaitez afficher ou gérer les snapshots.
3. Cliquez sur **Propriétés**.

   Les propriétés du fichier ou dossier sélectionné s'affichent.

4. Cliquez sur l'onglet **versions précédentes**.

   La liste des instantanés disponibles du fichier ou dossier sélectionné s'affiche dans la zone versions de dossier. Les snapshots répertoriés sont identifiés par le préfixe du nom du snapshot et l'horodatage de création.

5. Dans la zone **versions de dossier:**, cliquez avec le bouton droit de la souris sur la copie du fichier ou du dossier que vous souhaitez gérer.
6. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Procédez comme suit…
Afficher les données de cet instantané	Cliquez sur **Ouvrir**.
Créez une copie des données à partir de cet instantané	Cliquez sur **Copier**.

   Les données des snapshots sont en lecture seule. Si vous souhaitez apporter des modifications aux fichiers et dossiers répertoriés dans l'onglet versions précédentes, vous devez enregistrer une copie des fichiers et dossiers que vous souhaitez modifier à un emplacement inscriptible et apporter des modifications aux copies.

7. Une fois la gestion des données de snapshot terminée, fermez la boîte de dialogue **Propriétés** en cliquant sur **OK**.

   Pour plus d'informations sur l'utilisation de l'onglet versions précédentes pour afficher et gérer les données d'instantané, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Déterminer si les snapshots ONTAP SMB sont disponibles pour une utilisation dans les versions précédentes

Vous pouvez afficher les instantanés à partir de l'onglet versions précédentes uniquement si une règle de snapshot activée est appliquée au volume contenant le partage et si la configuration du volume autorise l'accès aux instantanés. La détermination de la disponibilité des instantanés est utile lorsque vous aidez un utilisateur à accéder aux versions précédentes.

Étapes

1. Déterminez si les snapshots automatiques sont activés sur le volume sur lequel résident les données de

partage et si les clients ont accès aux répertoires de snapshots : `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

Le résultat affiche la politique de snapshot associée au volume, si l'accès au répertoire de snapshots client est activé et le nombre de snapshots disponibles.

2. Déterminez si la règle de snapshot associée est activée : `volume snapshot policy show -policy policy-name`
3. Répertorier les instantanés disponibles : `volume snapshot show -volume volume_name`

   Pour plus d'informations sur la configuration et la gestion des stratégies d'instantanés et des planifications d'instantanés, reportez-vous à la section "La protection des données".

Exemple

L'exemple suivant affiche des informations sur les règles de snapshot associées au volume nommé « data1 » qui contient les données partagées et les snapshots disponibles sur « data1 ».

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Informations associées

- Créer des configurations d'instantanés pour permettre l'accès aux versions précédentes
- "Protection des données"

Créer des configurations de snapshots ONTAP SMB pour permettre l'accès aux versions précédentes

La fonctionnalité versions précédentes est toujours disponible, à condition que l'accès client aux instantanés soit activé et que des instantanés existent. Si votre configuration de snapshot ne répond pas à ces exigences, vous pouvez créer une configuration de snapshot.

Étapes

1. Si aucune règle de snapshot n'est associée au volume contenant le partage auquel vous souhaitez autoriser l'accès aux versions précédentes, associez une règle de snapshot au volume et activez-la à l'aide de la `volume modify` commande.

   Pour en savoir plus, `volume modify` consultez le "Référence de commande ONTAP".

2. Activez l'accès aux snapshots à l'aide de la `volume modify` commande pour définir l' `-snap -dir`option sur `true`.

   Pour en savoir plus, `volume modify` consultez le "Référence de commande ONTAP".

3. Vérifiez que les stratégies de snapshot sont activées et que l'accès aux répertoires de snapshots est activé à l'aide des `volume show` commandes et `volume snapshot policy show`.

   Pour en savoir plus sur `volume show` et `volume snapshot policy show` dans le "Référence de commande ONTAP".

   Pour plus d'informations sur la configuration et la gestion des stratégies d'instantanés et des planifications d'instantanés, reportez-vous à la section "La protection des données".

Informations associées

"Protection des données"

En savoir plus sur la restauration des répertoires des versions précédentes contenant des jonctions SMB ONTAP

Vous devez garder à l'esprit certaines consignes lorsque vous utilisez les versions précédentes pour restaurer des dossiers contenant des points de jonction.

Lorsque vous utilisez les versions précédentes pour restaurer des dossiers comportant des dossiers enfants qui sont des points de jonction, la restauration peut échouer avec un `Access Denied` erreur.

Vous pouvez déterminer si le dossier que vous essayez de restaurer contient une jonction à l'aide de l' `vol show` commande avec `-parent` option. Vous pouvez également utiliser le `vserver security trace` commandes permettant de créer des journaux détaillés sur les problèmes d'accès aux fichiers et aux dossiers.

Informations associées

Création et gestion des volumes de données dans les espaces de noms NAS

Déployez les services basés sur serveur SMB

Gérer les répertoires locaux

En savoir plus sur l'activation des répertoires personnels dynamiques sur les serveurs ONTAP SMB

Les home directories ONTAP vous permettent de configurer un partage SMB qui correspond à différents répertoires en fonction de l'utilisateur qui se connecte à celui-ci et d'un ensemble de variables. Au lieu de créer des partages distincts pour chaque utilisateur, vous pouvez configurer un partage avec quelques paramètres de home Directory afin de définir la relation d'un utilisateur entre un point d'entrée (le partage) et le home Directory (un répertoire sur la SVM).

Un utilisateur connecté en tant qu'utilisateur invité ne dispose pas d'un répertoire personnel et ne peut pas accéder aux répertoires d'accueil d'autres utilisateurs. Il existe quatre variables qui déterminent la manière dont un utilisateur est mappé à un répertoire :

- **Nom de partage**

  Il s'agit du nom du partage que vous créez et auquel l'utilisateur se connecte. Vous devez définir la propriété du répertoire personnel pour ce partage.

  Le nom du partage peut utiliser les noms dynamiques suivants :

  - `%w` (Nom d'utilisateur Windows de l'utilisateur)
  - `%d` (Nom de domaine Windows de l'utilisateur)
  - `%u` (Nom d'utilisateur UNIX mappé de l'utilisateur)
    Pour que le nom du partage soit unique dans tous les répertoires d'accueil, le nom du partage doit contenir soit/`%w` ou le `%u` variable. Le nom du partage peut contenir les deux `%d` et le/`%w` variable (par exemple, `%d`/`%w`), ou le nom du partage peut contenir une partie statique et une partie variable (par exemple, home_/`%w`).
- **Chemin de partage**

  Il s'agit du chemin relatif, défini par le partage, et donc associé à l'un des noms de partage, qui est ajouté à chaque chemin de recherche pour générer le chemin d'accès complet du home Directory de l'utilisateur, à partir de la racine de la SVM. Il peut être statique (par exemple, `home`), dynamique (par exemple, `%w`), ou une combinaison des deux (par exemple, `eng/%w`).
- **Chemins de recherche**

  Il s'agit de l'ensemble des chemins absolus depuis la racine du SVM que vous spécifiez qui dirigent la recherche ONTAP pour les répertoires locaux. Vous pouvez spécifier un ou plusieurs chemins de recherche à l'aide de la `vserver cifs home-directory search-path add` commande. Si vous spécifiez plusieurs chemins de recherche, ONTAP les essaie dans l'ordre spécifié jusqu'à ce qu'il trouve un chemin valide. Pour en savoir plus, `vserver cifs home-directory search-path add` consultez le "Référence de commande ONTAP".
- **Répertoire**

  Il s'agit du répertoire de base de l'utilisateur que vous créez pour l'utilisateur. Le nom du répertoire est généralement le nom de l'utilisateur. Vous devez créer le répertoire personnel dans l'un des répertoires définis par les chemins de recherche.

Prenons l'exemple de la configuration suivante :

- Utilisateur : John Smith
- Domaine utilisateur : acme
- Nom d'utilisateur: Jsmith
- Nom du SVM : vs1
- Nom de partage du répertoire de base n°1 : Home_ `%w` - chemin de partage : `%w`
- Nom de partage du répertoire racine #2 : `%w` - chemin de partage : `%d/%w`
- Chemin de recherche n°1 : `/vol0home/home`

- Chemin de recherche n°2 : `/vol1home/home`
- Chemin de recherche n°3 : `/vol2home/home`
- Home Directory : `/vol1home/home/jsmith`

Scénario 1 : l'utilisateur se connecte à `\\vs1\home_jsmith`. Ceci correspond au premier nom de partage du répertoire racine et génère le chemin relatif `jsmith`. ONTAP recherche désormais un répertoire nommé `jsmith` en vérifiant chaque chemin de recherche dans l'ordre suivant :

- `/vol0home/home/jsmith` n'existe pas ; passer au chemin de recherche n°2.
- `/vol1home/home/jsmith` existe ; par conséquent, le chemin de recherche #3 n'est pas coché ; l'utilisateur est maintenant connecté à son répertoire de base.

Scénario 2 : l'utilisateur se connecte à `\\vs1\jsmith`. Ceci correspond au deuxième nom de partage du répertoire de base et génère le chemin relatif `acme/jsmith`. ONTAP recherche désormais un répertoire nommé `acme/jsmith` en vérifiant chaque chemin de recherche dans l'ordre suivant :

- `/vol0home/home/acme/jsmith` n'existe pas ; passer au chemin de recherche n°2.
- `/vol1home/home/acme/jsmith` n'existe pas ; passer au chemin de recherche #3.
- `/vol2home/home/acme/jsmith` n'existe pas ; le répertoire personnel n'existe pas ; la connexion échoue donc.

Partages de répertoires locaux

Ajouter des partages de répertoire personnel ONTAP SMB

Si vous souhaitez utiliser la fonction de répertoire de base SMB, vous devez ajouter au moins un partage avec la propriété de répertoire de base incluse dans les propriétés de partage.

Description de la tâche

Vous pouvez créer un partage de répertoire personnel au moment de la création du partage en utilisant le `vserver cifs share create` vous pouvez également modifier un partage existant en un partage de répertoire personnel à tout moment à l'aide de l' `vserver cifs share modify` commande.

Pour créer un partage de répertoire personnel, vous devez inclure le `homedirectory` valeur dans le `-share-properties` lorsque vous créez ou modifiez un partage. Vous pouvez spécifier le nom du partage et le chemin du partage à l'aide de variables développées dynamiquement lorsque les utilisateurs se connectent à leurs répertoires locaux. Les variables disponibles que vous pouvez utiliser dans le chemin sont `%w`, `%d`, et `%u`, Correspondant respectivement au nom d'utilisateur Windows, au domaine et au nom d'utilisateur UNIX mappé.

Étapes

1. Ajouter un partage de répertoire de base :
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

   `-share-name` *`share-name`* spécifie le nom de partage du répertoire racine.

En plus de contenir l'une des variables requises, si le nom du partage contient l'une des chaînes littérales `%w`, `%u`, ou `%d`, Vous devez faire précéder la chaîne littérale d'un caractère % (pourcentage) pour empêcher ONTAP de traiter la chaîne littérale comme une variable (par exemple, `%%w`).

- Le nom du partage doit contenir soit le `%w` ou le `%u` variable.
- Le nom du partage peut également contenir le `%d` variable (par exemple, `%d/%w`) ou une partie statique dans le nom du partage (par exemple, home1_/`%w`).
- Si le partage est utilisé par les administrateurs pour se connecter aux répertoires d'accueil d'autres utilisateurs ou pour permettre aux utilisateurs de se connecter aux répertoires d'accueil d'autres utilisateurs, le modèle de nom de partage dynamique doit être précédé d'un tilde (~).

  Le `vserver cifs home-directory modify` est utilisé pour activer cet accès en configurant le `-is-home-dirs-access-for-admin-enabled` option à `true`) ou en définissant l'option avancée `-is-home-dirs-access-for-public-enabled` à `true`.

`-path path` spécifie le chemin relatif vers le répertoire de base.

`-share-properties homedirectory[,…]` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.

1. Vérifiez que vous avez correctement ajouté le partage du répertoire personnel à l'aide de l' `vserver cifs share show` commande.

Exemple

La commande suivante crée un partage de répertoire personnel nommé `%w`. Le `oplocks`, `browsable`, et `changenotify` les propriétés de partage sont définies en plus de la configuration du `homedirectory` propriété de partage.

> Cet exemple n'affiche pas les valeurs de sortie de tous les partages du SVM. La sortie est tronquée.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Informations associées

- Ajouter des chemins de recherche de répertoire personnel
- Exigences et directives pour l'utilisation des références automatiques de nœuds sur les serveurs

- Gérer l’accessibilité aux répertoires personnels des utilisateurs

En savoir plus sur les exigences uniques en matière de nom d’utilisateur ONTAP SMB pour les partages de répertoire personnel

Veillez à attribuer des noms d’utilisateur uniques lors de la création de partages de répertoires locaux à l’aide de l' `%w` (Nom d’utilisateur Windows) ou `%u` (Nom d’utilisateur UNIX) variables permettant de générer des partages de façon dynamique. Le nom du partage est mappé sur votre nom d’utilisateur.

Deux problèmes peuvent survenir lorsqu’un nom de partage statique et un nom d’utilisateur sont identiques :

- Lorsque l’utilisateur répertorie les partages sur un cluster utilisant le `net view` commande : deux partages portant le même nom d’utilisateur sont affichés.
- Lorsque l’utilisateur se connecte à ce nom de partage, l’utilisateur est toujours connecté au partage statique et ne peut pas accéder au partage de répertoire personnel portant le même nom.

Par exemple, il y a un partage nommé « administrateur » et vous avez un nom d’utilisateur Windows « administrateur ». Si vous créez un partage de répertoire personnel et vous connectez à ce partage, vous êtes connecté au partage statique « administrateur » et non à votre partage de répertoire personnel « administrateur ».

Vous pouvez résoudre le problème avec les noms de partage en double en suivant l’une des étapes suivantes :

- Renommer le partage statique de sorte qu’il n’entre plus en conflit avec le partage du répertoire personnel de l’utilisateur.
- Donner à l’utilisateur un nouveau nom d’utilisateur pour qu’il n’entre plus en conflit avec le nom du partage statique.
- Création d’un partage CIFS home Directory avec un nom statique tel que « home » au lieu d’utiliser le `%w` paramètre pour éviter les conflits avec les noms des partages.

Découvrez ce qui arrive aux noms de partage de répertoire personnel statiques ONTAP SMB après la mise à niveau

Les noms de partage de répertoire racine doivent contenir soit le `%w` ou le `%u` variable dynamique. Vous devez savoir ce qui arrive aux noms de partage de répertoire personnel statiques après la mise à niveau vers une version de ONTAP avec la nouvelle exigence.

Si votre configuration de répertoire personnel contient des noms de partage statiques et que vous effectuez une mise à niveau vers ONTAP, les noms de partage de répertoire personnel statique ne sont pas modifiés et sont toujours valides. Cependant, vous ne pouvez pas créer de nouveaux partages de répertoire personnel qui ne contiennent ni `%w` ou `%u` variable.

Le fait de demander que l’une de ces variables soit incluse dans le nom de partage du répertoire de base de l’utilisateur garantit que chaque nom de partage est unique dans la configuration du répertoire de base. Si vous le souhaitez, vous pouvez modifier les noms de partage des répertoires d’accueil statiques en noms contenant l’un ou l’autre `%w` ou `%u` variable.

Ajouter des chemins de recherche de répertoire personnel ONTAP SMB

Si vous souhaitez utiliser les home directories ONTAP SMB, vous devez ajouter au moins un chemin de recherche de répertoire personnel.

Description de la tâche

Vous pouvez ajouter un chemin de recherche de répertoire personnel à l'aide de la `vserver cifs home-directory search-path add` commande.

Le `vserver cifs home-directory search-path add` la commande vérifie le chemin d'accès spécifié dans `-path` option pendant l'exécution de la commande. Si le chemin spécifié n'existe pas, la commande génère un message vous invitant à continuer. Votre choix `y` ou `n`. Si vous le souhaitez `y` Pour continuer, ONTAP crée le chemin de recherche. Toutefois, vous devez créer la structure du répertoire avant de pouvoir utiliser le chemin de recherche dans la configuration du répertoire racine. Si vous choisissez de ne pas continuer, la commande échoue ; le chemin de recherche n'est pas créé. Vous pouvez ensuite créer la structure du répertoire de chemins d'accès et réexécuter le `vserver cifs home-directory search-path add` commande.

Étapes

1. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.

Exemple

L'exemple suivant ajoute le chemin `/home1` Vers la configuration home Directory sur le SVM vs1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

L'exemple suivant tente d'ajouter le chemin d'accès `/home2` Vers la configuration home Directory sur le SVM vs1. Le chemin d'accès n'existe pas. Le choix est de ne pas continuer.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Informations associées

Ajouter des partages de répertoire personnel

Créer des configurations de répertoire personnel ONTAP SMB à l'aide des variables %w et %d

Vous pouvez créer une configuration de répertoire personnel à l'aide de l' `%w` et `%d` variables. Les utilisateurs peuvent ensuite se connecter à leur partage personnel à l'aide de partages créés de manière dynamique.

Étapes

1. Créer un qtree pour contenir les home directories de l'utilisateur : `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vérifier que le qtree utilise le style de sécurité approprié : `volume qtree show`
3. Si le qtree n'utilise pas le style de sécurité souhaité, modifiez le style de sécurité à l'aide de `volume qtree security` commande.
4. Ajouter un partage de répertoire de base : `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

   `-share-name %w` spécifie le nom de partage du répertoire racine. ONTAP crée dynamiquement le nom du partage lorsque chaque utilisateur se connecte à son répertoire de base. Le nom du partage sera sous la forme *Windows_user_name*.

   `-path %d/%w` spécifie le chemin relatif vers le répertoire de base. Le chemin relatif est créé de façon dynamique au fur et à mesure que chaque utilisateur se connecte à son répertoire de départ et sera sous la forme *domain/Windows_user_name*.

   `-share-properties homedirectory[,…]+` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.
5. Vérifiez que le partage dispose de la configuration souhaitée à l'aide du `vserver cifs share show` commande.
6. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Spécifie le SVM activé sur CIFS sur lequel ajouter le chemin de recherche.

   `-path` *`path`* spécifie le chemin absolu du répertoire vers le chemin de recherche.
7. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.
8. Pour les utilisateurs disposant d'un home Directory, créez un répertoire correspondant dans le qtree ou le volume désigné pour contenir des home directories.

   Par exemple, si vous avez créé un qtree avec le chemin d'accès du groupe `/vol/vol1/users` et le nom d'utilisateur dont vous souhaitez créer le répertoire est mydomain\user1, vous devez créer un répertoire avec le chemin suivant : `/vol/vol1/users/mydomain/user1`.

   Si vous avez créé un volume nommé « home1 » monté à `/home1`, vous créeriez un répertoire avec le chemin suivant : `/home1/mydomain/user1`.

9. Vérifiez qu'un utilisateur peut se connecter avec succès au partage d'accueil en mappant un lecteur ou en vous connectant à l'aide du chemin UNC.

   Par exemple, si l'utilisateur mydomain\user1 souhaite se connecter au répertoire créé à l'étape 8 situé sur le SVM vs1, l'utilisateur 1 se connecte à l'aide du chemin UNC `\\vs1\user1`.

Exemple

Dans l'exemple suivant, les commandes permettent de créer une configuration de home Directory avec les paramètres suivants :

- Le nom du partage est %w.
- Le chemin relatif du répertoire d'accueil est %d/%w.
- Le chemin de recherche utilisé pour contenir les répertoires locaux, `/home1`, Est un volume configuré avec le style de sécurité NTFS.
- La configuration est créée sur le SVM vs1.

Vous pouvez utiliser ce type de configuration de répertoire personnel lorsque les utilisateurs accèdent à leurs répertoires personnels à partir d'hôtes Windows. Vous pouvez également utiliser ce type de configuration lorsque les utilisateurs accèdent à leurs répertoires personnels à partir d'hôtes Windows et UNIX et que l'administrateur du système de fichiers utilise des utilisateurs et des groupes Windows pour contrôler l'accès au système de fichiers.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                     Vserver: vs1
                       Share: %w
     CIFS Server NetBIOS Name: VS1
                        Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Informations associées

- Configurez les répertoires d'accueil à l'aide de la variable %u
- En savoir plus sur les configurations supplémentaires du répertoire personnel
- Afficher des informations sur les chemins d'accès aux répertoires personnels des utilisateurs

Configurer les répertoires personnels ONTAP SMB à l'aide de la variable %u

Vous pouvez créer une configuration de répertoire personnel dans laquelle vous désignez le nom du partage à l'aide de l' `%w` variable mais vous utilisez `%u` variable pour désigner le chemin relatif vers le partage du répertoire racine. Les utilisateurs peuvent ensuite se connecter à leur partage d'origine à l'aide de partages dynamiques créés à l'aide de leur nom d'utilisateur Windows sans connaître le nom ou le chemin réel du répertoire d'accueil.

Étapes

1. Créer un qtree pour contenir les home directories de l'utilisateur : `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vérifier que le qtree utilise le style de sécurité approprié : `volume qtree show`
3. Si le qtree n'utilise pas le style de sécurité souhaité, modifiez le style de sécurité à l'aide de `volume qtree security` commande.
4. Ajouter un partage de répertoire de base : `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

   `-share-name %w` spécifie le nom de partage du répertoire racine. Le nom du partage est créé dynamiquement lorsque chaque utilisateur se connecte à son répertoire de départ et se présente sous la forme *Windows_user_name*.

   > Vous pouvez également utiliser le `%u` variable pour le `-share-name` option. Cela crée un chemin de partage relatif qui utilise le nom d'utilisateur UNIX mappé.

   `-path %u` spécifie le chemin relatif vers le répertoire de base. Le chemin relatif est créé dynamiquement au fur et à mesure que chaque utilisateur se connecte à son répertoire de départ et se présente sous la forme *mappé_UNIX_user_name*.

   > La valeur de cette option peut également contenir des éléments statiques. Par exemple : `eng/%u`.

   `-share-properties homedirectory\[,...\]` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.
5. Vérifiez que le partage dispose de la configuration souhaitée à l'aide du `vserver cifs share show` commande.
6. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Spécifie le SVM activé sur CIFS sur lequel ajouter le chemin de recherche.

   `-path path` spécifie le chemin absolu du répertoire vers le chemin de recherche.
7. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.
8. Si l'utilisateur UNIX n'existe pas, créez l'utilisateur UNIX à l'aide de `vserver services unix-user create` commande.

   > Le nom d'utilisateur UNIX auquel vous associez le nom d'utilisateur Windows doit exister avant le mappage de l'utilisateur.
9. Créer un mappage de nom pour l'utilisateur Windows auprès de l'utilisateur UNIX à l'aide de la commande suivante : `vserver name-mapping create -vserver vserver_name -direction win-unix`

```
-priority integer -pattern windows_user_name -replacement unix_user_name
```

> Si des mappages de noms existent déjà et mappent des utilisateurs Windows aux utilisateurs UNIX, vous n'avez pas besoin d'effectuer l'étape de mappage.

Le nom d'utilisateur Windows est mappé sur le nom d'utilisateur UNIX correspondant. Lorsque l'utilisateur Windows se connecte à son partage de répertoire personnel, il se connecte à un répertoire personnel créé dynamiquement avec un nom de partage qui correspond à son nom d'utilisateur Windows sans avoir à savoir que le nom de répertoire correspond au nom d'utilisateur UNIX.

10. Pour les utilisateurs disposant d'un home Directory, créez un répertoire correspondant dans le qtree ou le volume désigné pour contenir des home directories.

    Par exemple, si vous avez créé un qtree avec le chemin d'accès du groupe `/vol/vol1/users` Et le nom d'utilisateur UNIX mappé de l'utilisateur dont vous souhaitez créer le répertoire est « unixuser1 », vous devez créer un répertoire avec le chemin suivant : `/vol/vol1/users/unixuser1`.

    Si vous avez créé un volume nommé « home1 » monté à `/home1`, vous créeriez un répertoire avec le chemin suivant : `/home1/unixuser1`.

11. Vérifiez qu'un utilisateur peut se connecter avec succès au partage d'accueil en mappant un lecteur ou en vous connectant à l'aide du chemin UNC.

    Par exemple, si l'utilisateur mydomain\user1 est mappé sur l'utilisateur UNIX unixuser1 et souhaite se connecter au répertoire créé à l'étape 10 situé sur le SVM vs1, l'utilisateur 1 se connecte à l'aide du chemin UNC `\\vs1\user1`.

Exemple

Dans l'exemple suivant, les commandes permettent de créer une configuration de home Directory avec les paramètres suivants :

- Le nom du partage est %w.
- Le chemin relatif du répertoire d'accueil est %U.
- Le chemin de recherche utilisé pour contenir les répertoires locaux, `/home1`, Est un volume configuré avec le style de sécurité UNIX.
- La configuration est créée sur le SVM vs1.

Vous pouvez utiliser ce type de configuration de répertoire personnel lorsque les utilisateurs accèdent à leurs répertoires personnels à partir des hôtes Windows ou Windows et UNIX et que l'administrateur de système de fichiers utilise des utilisateurs et des groupes UNIX pour contrôler l'accès au système de fichiers.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Informations associées

- Créer des configurations de répertoire personnel à l'aide des variables %w et %d
- En savoir plus sur les configurations supplémentaires du répertoire personnel
- Afficher des informations sur les chemins d'accès aux répertoires personnels des utilisateurs

En savoir plus sur les configurations supplémentaires du répertoire personnel ONTAP SMB

Vous pouvez créer d'autres configurations de home Directory à l'aide du `%w`, `%d`, et `%u` variables, qui vous permettent de personnaliser la configuration du répertoire personnel pour répondre à vos besoins.

Vous pouvez créer un certain nombre de configurations de répertoire personnel en utilisant une combinaison de variables et de chaînes statiques dans les noms de partage et les chemins de recherche. Le tableau suivant fournit des exemples illustrant la création de différentes configurations de répertoires locaux :

Chemins d'accès créés lors de `/vol1/user` contient les répertoires locaux…	**Partager, commande…**
Pour créer un chemin de partage `\\vs1\~win_username` qui dirige l'utilisateur vers `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Pour créer un chemin de partage `\\vs1\win_username` qui dirige l'utilisateur vers `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Pour créer un chemin de partage `\\vs1\win_username` qui dirige l'utilisateur vers `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Pour créer un chemin de partage `\\vs1\unix_username` qui dirige l'utilisateur vers `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Commandes ONTAP pour la gestion des chemins de recherche SMB

Il existe des commandes ONTAP spécifiques permettant de gérer les chemins de recherche pour les configurations du home Directory SMB. Par exemple, il existe des commandes permettant d'ajouter, de supprimer et d'afficher les informations relatives aux chemins de recherche. Il existe également une commande permettant de modifier l'ordre du chemin de recherche.

Les fonctions que vous recherchez…	**Utilisez cette commande…**
Ajouter un chemin de recherche	`vserver cifs home-directory search-path add`
Afficher les chemins de recherche	`vserver cifs home-directory search-path show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Modifier l'ordre du chemin de recherche	`vserver cifs home-directory search-path reorder`
Supprimer un chemin de recherche	`vserver cifs home-directory search-path remove`

Pour en savoir plus, `vserver cifs home-directory search-path` consultez le "Référence de commande ONTAP".

Afficher des informations sur les chemins d'accès aux répertoires personnels des utilisateurs ONTAP SMB

Vous pouvez afficher le chemin d'accès au home Directory d'un utilisateur SMB sur la machine virtuelle de stockage (SVM), que vous pouvez utiliser si plusieurs chemins de home Directory CIFS sont configurés et que vous souhaitez voir quel chemin contient le home Directory de l'utilisateur.

Étape

1. Afficher le chemin du répertoire racine à l'aide de la `vserver cifs home-directory show-user` commande.

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  ----------------------
   vs1          user1                /home/user1
   ```

Informations associées

Gérer l'accessibilité aux répertoires personnels des utilisateurs

Gérer l'accessibilité aux répertoires personnels des utilisateurs ONTAP SMB

Par défaut, le répertoire personnel d'un utilisateur est accessible uniquement par cet utilisateur. Pour les partages dont le nom dynamique du partage est précédé d'un tilde (~), vous pouvez activer ou désactiver l'accès aux répertoires d'accueil des utilisateurs par les administrateurs Windows ou par tout autre utilisateur (accès public).

Avant de commencer

Les partages de home Directory sur la machine virtuelle de stockage (SVM) doivent être configurés avec des noms de partage dynamiques précédés d'un tilde (~). Les cas suivants illustrent les conditions de dénomination des partages :

Nom de partage du répertoire racine	Exemple de commande pour se connecter au partage
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Étape

1. Effectuez l'action appropriée :

Si vous souhaitez activer ou désactiver l'accès aux répertoires d'accueil des utilisateurs à…	Entrez les informations suivantes…
Administrateurs Windows	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` La valeur par défaut est `true`.
Tout utilisateur (accès public)	a. Définissez le niveau de privilège sur avancé : `set -privilege advanced` b. Activer ou désactiver l'accès : `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public-enabled {true

L'exemple suivant permet l'accès public aux répertoires locaux des utilisateurs :

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Informations associées

Afficher des informations sur les chemins d'accès aux répertoires personnels des utilisateurs

Configurez l'accès client SMB aux liens symboliques UNIX

En savoir plus sur la fourniture d'un accès client ONTAP SMB aux liens symboliques UNIX

Un lien symbolique est un fichier créé dans un environnement UNIX qui contient une référence à un autre fichier ou répertoire. Si un client accède à un lien symbolique, le client est redirigé vers le fichier ou répertoire cible auquel le lien symbolique fait référence. ONTAP prend en charge les liens symboliques relatifs et absolus, y compris les liens filaires (liens absolus avec des cibles en dehors du système de fichiers local).

ONTAP permet aux clients SMB de suivre des liens symboliques UNIX configurés sur la SVM. Cette fonction est facultative et vous pouvez la configurer par partage à l'aide de `-symlink-properties` de la `vserver cifs share create` avec l'un des paramètres suivants :

- Accès en lecture/écriture
- Activé avec accès en lecture seule
- Désactivé en masquant les liens symboliques des clients SMB
- Désactivé sans accès aux liens symboliques des clients SMB

Si vous activez des liens symboliques sur un partage, les liens symboliques relatifs fonctionnent sans configuration supplémentaire.

Si vous activez des liens symboliques sur un partage, les liens symboliques absolus ne fonctionnent pas immédiatement. Vous devez d'abord créer un mappage entre le chemin UNIX du lien symbolique et le chemin SMB de destination. Lors de la création de mappages de liens symboliques absolus, vous pouvez spécifier s'il s'agit d'un lien local ou d'un *widelink* ; les liens vers des systèmes de fichiers sur d'autres périphériques de stockage ou des liens vers des systèmes de fichiers hébergés dans des SVM distincts sur le même système ONTAP. Lorsque vous créez un lien, il doit inclure les informations que le client doit suivre, c'est-à-dire que vous créez un point de reanalyse pour que le client puisse découvrir le point de jonction du répertoire. Si vous créez un lien symbolique absolu vers un fichier ou un répertoire en dehors du partage local mais que vous définissez la localité sur local, ONTAP n'autorise pas l'accès à la cible.

> Si un client tente de supprimer un lien symbolique local (absolu ou relatif), seul le lien symbolique est supprimé, pas le fichier ou le répertoire cible. Toutefois, si un client tente de supprimer un lien vers le fil, il peut supprimer le fichier ou le répertoire cible auquel le lien vers le fil vers le fil. ONTAP n'a pas le contrôle sur cela, car le client peut explicitement ouvrir le fichier ou le répertoire cible en dehors du SVM et le supprimer.

- **Analyse des points et des services de système de fichiers ONTAP**

  Un *reparse point* est un objet système de fichiers NTFS qui peut éventuellement être stocké sur des volumes avec un fichier. Les points de reanalyse permettent aux clients SMB de recevoir des services de système de fichiers améliorés ou étendus lorsqu'ils travaillent avec des volumes de style NTFS. Les points de réanalyse se composent d'étiquettes standard identifiant le type de point de réanalyse et le contenu du point de réanalyse pouvant être récupéré par les clients SMB pour un traitement ultérieur par le client. Parmi les types d'objets disponibles pour la fonctionnalité étendue du système de fichiers, ONTAP met en œuvre la prise en charge des liens symboliques NTFS et des points de jonction de répertoire à l'aide de balises de point de reparse. Les clients SMB qui ne peuvent pas comprendre le contenu d'un point de reanalyse le ignorent et ne fournissent pas le service étendu de système de fichiers que le point de reanalyse peut activer.

- **Prise en charge des points de jonction de répertoire et de ONTAP pour les liens symboliques**

  Les points de jonction de répertoire sont des emplacements au sein d'une structure de répertoire de système de fichiers qui peuvent faire référence à des emplacements de remplacement où les fichiers sont stockés, soit sur un chemin différent (liens symboliques), soit sur un périphérique de stockage distinct (liens filaires). Les serveurs ONTAP SMB exposent les points de jonction de répertoire aux clients Windows sous forme de points de reanalyse, ce qui permet aux clients capables d'obtenir le contenu du point de reanalyse à partir de ONTAP lorsqu'un point de jonction de répertoire est en cours de traitement. Ils peuvent ainsi naviguer et se connecter à différents chemins ou périphériques de stockage comme s'ils faisaient partie du même système de fichiers.

- **Activation de la prise en charge wdelink à l'aide des options de point de réanalyse**

L'`-is-use-junctions-as-reparse-points-enabled`option est activée par défaut dans ONTAP 9. L'option d'activation des informations est configurable pour chaque protocole, car tous les clients SMB ne prennent pas en charge les liens étendus. Cela permet aux administrateurs de gérer les clients SMB pris en charge ou non. Vous devez activer cette option. `-widelink-as-reparse-point-versions` pour chaque protocole client qui accède au partage à l'aide de liens larges ; la valeur par défaut est SMB1.

Informations associées

- "Applications de sauvegarde Windows et liens symboliques de style Unix"
- "Documentation Microsoft : analyse des points"

Limites lors de la configuration des liens symboliques UNIX pour l'accès SMB ONTAP

Vous devez connaître certaines limites lors de la configuration de liens symboliques UNIX pour l'accès SMB.

Limite	Description
45	Longueur maximale du nom de serveur CIFS que vous pouvez spécifier lors de l'utilisation d'un FQDN pour le nom du serveur CIFS. Vous pouvez également spécifier le nom du serveur CIFS sous la forme d'un nom NetBIOS, limité à 15 caractères.
80	Longueur maximale du nom de partage.
256	Longueur maximale du chemin UNIX que vous pouvez spécifier lors de la création d'un lien symbolique ou lors de la modification du chemin UNIX d'un lien symbolique existant.le chemin UNIX doit commencer par un ""/" (slash) and end with a "/». Les barres obliques de début et de fin font partie de la limite de 256 caractères.
256	Longueur maximale du chemin CIFS que vous pouvez spécifier lors de la création d'un lien symbolique ou lors de la modification du chemin CIFS d'un lien symbolique existant.le chemin CIFS doit commencer par « »/" (slash) and end with a "/». Les barres obliques de début et de fin font partie de la limite de 256 caractères.

Informations associées

Créer des mappages de liens symboliques pour les partages

Contrôler les publicités DFS automatiques sur les serveurs SMB ONTAP

Une option de serveur CIFS contrôle la manière dont les fonctionnalités DFS sont annoncées aux clients SMB lors de la connexion aux partages. Étant donné que ONTAP utilise des référencements DFS lorsque les clients accèdent aux liens symboliques via SMB, vous devez savoir quel est l'impact lorsque cette option est désactivée ou activée.

Une option de serveur CIFS détermine si les serveurs CIFS annoncent automatiquement qu'ils sont compatibles DFS pour les clients SMB. Par défaut, cette option est activée et le serveur CIFS annonce toujours que DFS est capable pour les clients SMB (même lors de la connexion à des partages où l'accès aux liens symboliques est désactivé). Si vous voulez que le serveur CIFS annonce qu'il est compatible avec les clients uniquement lorsqu'ils se connectent à des partages où l'accès aux liens symboliques est activé, vous pouvez désactiver cette option.

Vous devez savoir ce qui se passe lorsque cette option est désactivée :

- Les configurations de partage des liens symboliques ne sont pas modifiées.
- Si le paramètre de partage est défini pour autoriser l'accès à la liaison symbolique (accès en lecture/écriture ou accès en lecture seule), le serveur CIFS transmet les fonctionnalités DFS aux clients se connectant à ce partage.

  Les connexions client et l'accès aux liens symboliques se poursuivent sans interruption.

- Si le paramètre de partage est défini sur ne pas autoriser l'accès aux liens symboliques (soit en désactivant l'accès, soit si la valeur du paramètre de partage est nulle), le serveur CIFS n'annonce pas les capacités DFS aux clients se connectant à ce partage.

  Comme les clients disposent d'informations en cache sur lesquelles le serveur CIFS prend en charge DFS et qu'il n'est plus publicitaire qu'il est, les clients connectés à des partages où l'accès à la liaison symbolique est désactivé risquent de ne pas pouvoir accéder à ces partages une fois que l'option de serveur CIFS est désactivée. Une fois l'option désactivée, vous devrez peut-être redémarrer les clients connectés à ces partages, ce qui vous permettra de supprimer les informations mises en cache.

Ces modifications ne s'appliquent pas aux connexions SMB 1.0.

Configurer la prise en charge des liens symboliques UNIX sur les partages SMB ONTAP

Vous pouvez configurer la prise en charge des liens symboliques UNIX sur les partages SMB en spécifiant un paramètre de propriété de partage de liens symboliques lorsque vous créez des partages SMB ou en modifiant à tout moment des partages SMB existants. La prise en charge des liens symboliques UNIX est activée par défaut. Vous pouvez également désactiver la prise en charge des liens symboliques UNIX sur un partage.

Description de la tâche

Lors de la configuration de la prise en charge des liens symboliques UNIX pour les partages SMB, vous pouvez choisir l'un des paramètres suivants :

Réglage	Description
`enable` (OBSOLÈTE*)	Indique que les liens symboliques sont activés pour l'accès en lecture/écriture.
`read_only` (OBSOLÈTE*)	Indique que les symlinks sont activés pour l'accès en lecture seule. Ce paramètre ne s'applique pas aux boutons de mode. L'accès Widelink est toujours en lecture-écriture.
`hide` (OBSOLÈTE*)	Spécifie que les clients SMB ne peuvent pas voir les symlinks.
`no-strict-security`	Spécifie que les clients suivent des symlinks en dehors des limites de partage.
`symlinks`	Indique que les symlinks sont activés localement pour l'accès en lecture/écriture. Les annonces DFS ne sont pas générées même si l'option CIFS `is-advertise-dfs-enabled` est défini sur `true`. Il s'agit du paramètre par défaut.
`symlinks-and-widelinks`	Spécifie que les liens symlinks locaux et les widelinks pour l'accès en lecture-écriture. Les annonces DFS sont générées pour les symlinks locaux et les widelinks, même si l'option CIFS `is-advertise-dfs-enabled` est défini sur `false`.
`disable`	Spécifie que les liens symlinks et les liens de fil sont désactivés. Les annonces DFS ne sont pas générées même si l'option CIFS `is-advertise-dfs-enabled` est défini sur `true`.
`""` (nul, non défini)	Désactive les liens symboliques sur le partage.
– (non défini)	Désactive les liens symboliques sur le partage.

*Les paramètres *enable*, *hide* et *read-only* sont obsolètes et peuvent être supprimés dans une version future de ONTAP.

Étapes

1. Configurer ou désactiver la prise en charge des liens symboliques :

Si c'est…	Entrer…
Un nouveau partage SMB	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable

Si c’est…	Entrer…
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Un partage SMB existant
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Vérifiez que la configuration du partage SMB est correcte : `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemple

La commande suivante crée un partage SMB nommé "data1" avec la configuration de lien symbolique UNIX définie sur `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informations associées

Créer des mappages de liens symboliques pour les partages

Créer des mappages de liens symboliques pour les partages SMB ONTAP

Vous pouvez créer des mappages de liens symboliques UNIX pour les partages SMB. Vous pouvez soit créer un lien symbolique relatif, qui fait référence au fichier ou au dossier par rapport à son dossier parent, soit créer un lien symbolique absolu, qui fait référence au fichier ou au dossier à l'aide d'un chemin absolu.

Description de la tâche

Les Widelinks ne sont pas accessibles à partir de clients Mac OS X si vous utilisez SMB 2.x. Lorsqu'un utilisateur tente de se connecter à un partage à l'aide de liens de liaison d'un client Mac OS X, la tentative échoue. Toutefois, vous pouvez utiliser des liens de mode avec les clients Mac OS X si vous utilisez SMB 1.

Étapes

1. Pour créer des mappages de liens symboliques pour les partages SMB : `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` Spécifie le nom de la machine virtuelle de stockage (SVM).

`-unix-path path` Spécifie le chemin UNIX. Le chemin UNIX doit commencer par une barre oblique (`/`) et doit se terminer par une barre oblique (`/`).

`-share-name share_name` Spécifie le nom du partage SMB à mapper.

`-cifs-path path` Spécifie le chemin CIFS. Le chemin CIFS doit commencer par une barre oblique (`/`) et doit se terminer par une barre oblique (`/`).

`-cifs-server server_name` Spécifie le nom du serveur CIFS. Le nom du serveur CIFS peut être spécifié sous la forme d'un nom DNS (par exemple, mynetwork.cifs.server.com), d'une adresse IP ou d'un nom NetBIOS. Le nom NetBIOS peut être déterminé à l'aide du `vserver cifs show` commande. Si ce paramètre facultatif n'est pas spécifié, la valeur par défaut est le nom NetBIOS du serveur CIFS local.

`-locality local|free|widelink}` spécifie s'il faut créer un lien local, un lien libre ou un lien symbolique étendu. Un lien symbolique local correspond au partage SMB local. Un lien symbolique libre peut être mappé n'importe où sur le serveur SMB local. Un lien symbolique étendu correspond à n'importe quel partage SMB du réseau. Si vous ne spécifiez pas ce paramètre facultatif, la valeur par défaut est `local`.

`-home-directory true false}` indique si le partage cible est un répertoire de base. Même si ce paramètre est facultatif, vous devez définir ce paramètre sur `true` lorsque le partage cible est configuré en tant que répertoire de base. La valeur par défaut est `false`.

Exemple

La commande suivante crée un mappage de lien symbolique sur le SVM nommé vs1. Il a le chemin UNIX `/src/`, Le nom de partage SMB "SOUCE", le chemin CIFS `/mycompany/source/`, Et l'adresse IP 123.123.123.123 du serveur CIFS, et c'est un lien de type widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Informations associées

Configurer la prise en charge des liens symboliques UNIX sur les partages

Commandes ONTAP pour la gestion des mappages de liens symboliques SMB

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de liens symboliques.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un mappage de lien symbolique	`vserver cifs symlink create`
Affiche des informations sur les mappages de liens symboliques	`vserver cifs symlink show`
Modifier un mappage de lien symbolique	`vserver cifs symlink modify`

Les fonctions que vous recherchez…	Utilisez cette commande…
Supprimer un mappage de lien symbolique	`vserver cifs symlink delete`

Pour en savoir plus, `vserver cifs symlink` consultez le "Référence de commande ONTAP".

Applications de sauvegarde Windows et liens symboliques de style Unix sur les serveurs ONTAP SMB

Lorsqu'une application de sauvegarde s'exécutant sous Windows rencontre un lien symbolique de style Unix (symlink), le lien est suivi et les données sont sauvegardées. Depuis ONTAP 9.15.1, vous avez la possibilité de sauvegarder les liens symboliques au lieu des données. Cette fonctionnalité est entièrement prise en charge avec les volumes ONTAP FlexGroup et FlexVols.

Présentation

Avant de modifier la façon dont ONTAP gère les liens symboliques au cours d'une opération de sauvegarde Windows, vous devez connaître les avantages, les concepts clés et les options de configuration.

Avantages

Lorsque cette fonction est désactivée ou indisponible, chaque lien symbolique est parcouru et les données auxquelles elle est liée sont sauvegardées. C'est pourquoi il est parfois possible de sauvegarder des données inutiles et, dans certains cas, l'application risque de se retrouver en boucle. La sauvegarde des liens symboliques permet d'éviter ces problèmes. Et comme les fichiers symlink sont très petits par rapport aux données dans la plupart des cas, les sauvegardes prennent moins de temps. La réduction des opérations d'E/S permet également d'améliorer les performances globales du cluster.

Environnement de serveur Windows

Cette fonction est prise en charge pour les applications de sauvegarde s'exécutant sous Windows. Vous devez comprendre les aspects techniques pertinents de l'environnement avant de l'utiliser.

Attributs étendus

Windows prend en charge les attributs étendus (EA) qui forment collectivement des métadonnées supplémentaires éventuellement associées aux fichiers. Ces attributs sont utilisés par diverses applications, telles que le sous-système Windows pour Linux, comme décrit à la section "Autorisations de fichier pour WSL". Les applications peuvent demander des attributs étendus pour chaque fichier lors de la lecture de données à partir de ONTAP.

Les liens symboliques sont renvoyés dans les attributs étendus lorsque la fonction est activée. Par conséquent, une application de sauvegarde doit fournir une prise en charge EA standard utilisée pour stocker les métadonnées. Certains utilitaires Windows prennent en charge et conservent les attributs étendus. Toutefois, si le logiciel de sauvegarde ne prend pas en charge la sauvegarde et la restauration des attributs étendus, il ne conservera pas les métadonnées associées à chaque fichier et ne traitera pas correctement les liens symboliques.

Configuration Windows

Les applications de sauvegarde exécutées sur un serveur Microsoft Windows peuvent bénéficier d'un privilège spécial leur permettant de contourner la sécurité normale des fichiers. Pour ce faire, vous devez généralement ajouter les applications au groupe opérateurs de sauvegarde. Les applications peuvent ensuite sauvegarder et restaurer les fichiers selon les besoins, ainsi que réaliser d'autres opérations système connexes. Le protocole

SMB utilisé par les applications de sauvegarde est subtils changements qui peuvent être détectés par ONTAP lors de la lecture et de l'écriture des données.

De formation

La fonction de sauvegarde de lien symbolique a plusieurs exigences, notamment :

- Votre cluster exécute ONTAP 9.15.1 ou une version ultérieure.
- Application de sauvegarde Windows bénéficiant de privilèges de sauvegarde spéciaux.
- L'application de sauvegarde doit également prendre en charge les attributs étendus et les demander pendant les opérations de sauvegarde.
- La fonctionnalité de sauvegarde ONTAP symlink est activée pour le SVM de données applicable.

Options de configuration

Outre l'interface de ligne de commandes de ONTAP, vous pouvez également gérer cette fonctionnalité via l'API REST. Voir "Nouveautés de l'API REST ONTAP et de l'automatisation" pour plus d'informations. La configuration déterminant la façon dont ONTAP traite les symlinks de style Unix doit être effectuée séparément pour chaque SVM.

Activez la fonction de sauvegarde de lien symbolique dans ONTAP

Une option de configuration a été ajoutée à une commande CLI existante avec ONTAP 9.15.1. Vous pouvez utiliser cette option pour activer ou désactiver le traitement des liens symboliques de style Unix.

Avant de commencer

Passez en revue le de base De formation. Par ailleurs :

- Être capable de porter vos privilèges d'interface de ligne de commandes au niveau avancé.
- Déterminer le SVM de données à modifier Le SVM `vs1` est utilisé dans la commande exemple.

Étapes

1. Définissez le niveau de privilège avancé.

```
set privilege advanced
```

2. Activer la sauvegarde du fichier symlink.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Utilisez BranchCache pour mettre en cache le contenu du partage SMB dans une succursale

Découvrez comment utiliser BranchCache pour mettre en cache le contenu du partage SMB ONTAP dans une succursale

BranchCache a été développé par Microsoft afin de permettre la mise en cache du contenu sur les ordinateurs locaux pour les clients. L'implémentation par ONTAP de BranchCache permet de réduire l'utilisation du réseau étendu (WAN) et de réduire le

temps de réponse d'accès lorsque les utilisateurs d'une succursale accèdent au contenu stocké sur des serveurs virtuels de stockage (SVM) avec SMB.

Si vous configurez BranchCache, les clients Windows BranchCache récupèrent le contenu du SVM, puis le mettent en cache sur un ordinateur au sein de la succursale. Si un autre client BranchCache du bureau de succursale demande le même contenu, le SVM procède d'abord à l'authentification et autorise l'utilisateur à demander. La SVM détermine ensuite si le contenu en cache est toujours à jour et, le cas échéant, elle envoie les métadonnées client relatives au contenu en cache. Le client utilise ensuite les métadonnées pour récupérer le contenu directement à partir du cache local.

Informations associées

En savoir plus sur l'utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne

Exigences et directives

En savoir plus sur la prise en charge des versions ONTAP SMB BranchCache

Notez bien les versions de BranchCache prises en charge par ONTAP.

ONTAP prend en charge BranchCache 1 et le BranchCache 2 optimisé :

- Lorsque vous configurez BranchCache sur le serveur SMB pour le serveur de stockage virtuel (SVM), vous pouvez activer BranchCache 1, BranchCache 2 ou toutes les versions.

  Par défaut, toutes les versions sont activées.

- Si vous n'activez que BranchCache 2, les ordinateurs clients Windows du bureau distant doivent prendre en charge BranchCache 2.

  Seuls les clients SMB 3.0 ou version ultérieure prennent en charge BranchCache 2.

Pour plus d'informations sur les versions de BranchCache, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

En savoir plus sur les exigences de prise en charge du protocole réseau ONTAP SMB

Pour implémenter ONTAP BranchCache, vous devez connaître les exigences en matière de protocoles réseau.

Vous pouvez implémenter la fonction ONTAP BranchCache sur des réseaux IPv4 et IPv6 à l'aide de SMB 2.1 ou version ultérieure.

Tous les serveurs CIFS et les succursales qui participent à l'implémentation de BranchCache doivent activer le protocole SMB 2.1 ou version ultérieure. Avec SMB 2.1, les extensions de protocole permettent à un client de participer à un environnement de BranchCache. Il s'agit de la version minimale du protocole SMB qui prend en charge BranchCache. SMB 2.1 prend en charge BranchCache version 1.

Si vous souhaitez utiliser BranchCache version 2, SMB 3.0 est la version minimale prise en charge. SMB 3.0 doit être activé sur tous les serveurs CIFS et les succursales qui participent à une implémentation de BranchCache 2.

Si vous disposez de bureaux distants où certains clients prennent uniquement en charge SMB 2.1 et que certains clients prennent en charge SMB 3.0, vous pouvez implémenter une configuration de BranchCache sur le serveur CIFS, qui prend en charge la mise en cache de BranchCache 1 et BranchCache 2.

Même si la fonctionnalité de BranchCache de Microsoft prend en charge l'utilisation des protocoles HTTP/HTTPS et SMB comme protocoles d'accès aux fichiers, ONTAP BranchCache ne prend en charge que SMB.

En savoir plus sur les exigences de version des hôtes ONTAP SMB et Windows

Avant de configurer BranchCache, les hôtes Windows du ONTAP et des succursales doivent répondre à certaines exigences de version.

Avant de configurer BranchCache, vous devez vérifier que la version de ONTAP est compatible avec le cluster et les clients des succursales participantes et prennent en charge SMB 2.1 ou version ultérieure, et prend en charge la fonctionnalité BranchCache. Si vous configurez le mode cache hébergé, vous devez également vous assurer que vous utilisez un hôte pris en charge pour le serveur de cache.

BranchCache 1 est pris en charge sur les versions ONTAP et hôtes Windows suivantes :

- Serveur de contenu : serveur virtuel de stockage (SVM) avec ONTAP
- Serveur de cache : Windows Server 2008 R2 ou Windows Server 2012 ou version ultérieure
- Poste ou client : Windows 7 Enterprise, Windows 7 Édition intégrale, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 ou version ultérieure

BranchCache 2 est pris en charge sur les versions ONTAP et les hôtes Windows suivants :

- Serveur de contenu : SVM avec ONTAP
- Serveur de cache : Windows Server 2012 ou version ultérieure
- Poste ou client : Windows 8 ou Windows Server 2012 ou version ultérieure

Découvrez les raisons pour lesquelles ONTAP SMB invalide les hachages BranchCache

Pour planifier votre configuration de BranchCache, ONTAP permet de déterminer les raisons pour lesquelles des hachages sont validés. Elle vous aide à choisir le mode de fonctionnement à configurer et à choisir les partages qui permettent d'activer BranchCache.

ONTAP doit gérer BranchCache pour vérifier que des hachages sont valides. Si un hachage n'est pas valide, ONTAP invalide le hachage et calcule un nouveau hachage la prochaine fois que le contenu est demandé, en supposant que BranchCache est toujours activé.

Des hachages de ONTAP valident les données pour les raisons suivantes :

- La clé de serveur est modifiée.

  Si la clé du serveur est modifiée, ONTAP invalide tous les hachages du magasin de hachage.

- Le hachage est transféré depuis le cache, car la taille maximale du magasin de hachage de BranchCache a été atteinte.

Il s'agit d'un paramètre ajustable et peut être modifié pour répondre à vos exigences métier.

- Un fichier est modifié via un accès SMB ou NFS.
- Un fichier pour lequel des hachages sont calculés est restauré à l'aide de l' `snap restore` commande.
- Un volume qui contient des partages SMB qui sont activés pour BranchCache est restauré à l'aide du `snap restore` commande.

En savoir plus sur le choix de l'emplacement du magasin de hachage ONTAP SMB

Lors de la configuration de BranchCache, vous pouvez choisir l'emplacement de stockage des hachages et la taille du magasin de hachage. Comprendre les instructions à suivre lors du choix de l'emplacement et de la taille du magasin de hachage peut vous aider à planifier la configuration de BranchCache sur un SVM compatible CIFS.

- Vous devez localiser le magasin de hachage sur un volume où les mises à jour atime sont autorisées.

  Le temps d'accès sur un fichier de hachage est utilisé pour conserver les fichiers fréquemment utilisés dans le magasin de hachage. Si les mises à jour atime sont désactivées, l'heure de création est utilisée à cette fin. Il est préférable d'utiliser atime pour suivre les fichiers fréquemment utilisés.

- Vous ne pouvez pas stocker des hachages sur des systèmes de fichiers en lecture seule, tels que les destinations SnapMirror et les volumes SnapLock.
- Si la taille maximale du magasin de hachage est atteinte, des hachages plus anciens sont vidés pour faire de la place à de nouveaux hachages.

  Vous pouvez augmenter la taille maximale du magasin de hachage pour réduire la quantité de hachages vidés du cache.

- Si le volume sur lequel vous stockez des hachages est indisponible ou saturé, ou si une communication interne au cluster pose un problème, là où le service de BranchCache ne peut pas récupérer les informations de hachage, les services de BranchCache ne sont pas disponibles.

  Le volume peut être indisponible parce qu'il est hors ligne ou parce que l'administrateur du stockage a spécifié un nouvel emplacement pour le magasin de hachage.

  Cela ne cause pas de problèmes d'accès aux fichiers. Si l'accès au magasin de hachage est entravé, ONTAP renvoie une erreur définie par Microsoft au client, ce qui entraîne la demande du client concernant le fichier à l'aide de la requête de lecture SMB normale.

Informations associées

- Configurer BranchCache sur les serveurs
- Modifier les configurations de BranchCache sur les partages

En savoir plus sur les recommandations ONTAP SMB BranchCache

Avant de configurer BranchCache, il est important de tenir compte de certaines recommandations lorsque vous décidez des partages SMB que vous souhaitez activer la mise en cache de BranchCache.

Veillez à respecter les recommandations suivantes lorsque vous décidez du mode d'exploitation à utiliser et des partages SMB pour activer BranchCache :

- Grâce à la mise en cache à distance des données, BranchCache est moins bénéfique.
- Les services de BranchCache sont avantageux pour les partages contenant du contenu de fichier, réutilisé par plusieurs clients distants ou par du contenu de fichier accessible de manière répétée par un seul utilisateur distant.
- Envisagez d'activer la mise en cache pour du contenu en lecture seule, comme les données des snapshots et des destinations SnapMirror.

Configurer BranchCache

En savoir plus sur la configuration d'ONTAP SMB BranchCache

Vous pouvez configurer BranchCache sur votre serveur SMB à l'aide des commandes ONTAP. Pour implémenter BranchCache, vous devez également configurer vos clients et, éventuellement, vos serveurs de cache hébergés dans les succursales où vous souhaitez mettre en cache le contenu.

Si vous configurez BranchCache pour permettre la mise en cache partage par partage, vous devez activer BranchCache sur les partages SMB pour lesquels vous souhaitez fournir des services de mise en cache de BranchCache.

Conditions requises pour la configuration d'ONTAP SMB BranchCache

Une fois que vous avez atteint certains prérequis, vous pouvez configurer BranchCache.

Les exigences suivantes doivent être respectées avant de configurer BranchCache sur le serveur CIFS pour le SVM :

- ONTAP doit être installé sur tous les nœuds du cluster.
- CIFS doit être sous licence et un serveur SMB doit être configuré. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.
- La connectivité réseau IPv4 ou IPv6 doit être configurée.
- Pour BranchCache 1, SMB 2.1 ou version ultérieure doit être activé.
- Pour BranchCache 2, SMB 3.0 doit être activé et les clients Windows distants doivent prendre en charge BranchCache 2.

Configurer BranchCache sur les serveurs SMB ONTAP

Vous pouvez configurer BranchCache pour fournir des services de BranchCache sur la base de chaque partage. Vous pouvez également configurer BranchCache pour activer automatiquement la mise en cache sur tous les partages SMB.

Description de la tâche

Vous pouvez configurer BranchCache sur des SVM.

- Vous pouvez créer une configuration de BranchCache pour tous les partages si vous souhaitez proposer des services de mise en cache pour tout le contenu contenu contenu contenu contenu dans tous les partages SMB sur le serveur CIFS.
- Vous pouvez créer une configuration de BranchCache par partage si vous souhaitez proposer des services

de mise en cache pour le contenu contenu contenu hébergé dans des partages SMB sélectionnés sur le serveur CIFS.

Vous devez spécifier les paramètres suivants lors de la configuration de BranchCache :

Paramètres requis	Description
Nom du SVM	BranchCache est configuré pour chaque SVM. Vous devez spécifier sur quel SVM compatible CIFS vous souhaitez configurer le service de BranchCache.
Chemin vers magasin de hachage	Les hachages de BranchCache sont stockés dans des fichiers réguliers sur le volume du SVM. Vous devez spécifier le chemin d'accès à un répertoire existant dans lequel ONTAP doit stocker les données de hachage.le chemin de hachage BranchCache doit être accessible en lecture-écriture. Les chemins en lecture seule, tels que les répertoires de snapshots, ne sont pas autorisés. Vous pouvez stocker les données de hachage dans un volume contenant d'autres données ou créer un volume distinct pour stocker les données de hachage. Si le SVM est une source de reprise d'activité du SVM, le chemin de hachage ne peut pas se trouver sur le volume root. En effet, le volume racine n'est pas répliqué vers la destination de reprise après incident. Le chemin de hachage peut contenir des blancs et des caractères de nom de fichier valides.

Vous pouvez éventuellement spécifier les paramètres suivants :

Paramètres facultatifs	Description
Versions prises en charge	ONTAP prend en charge BranchCache 1 et 2. Vous pouvez activer la version 1, la version 2 ou les deux versions. La valeur par défaut est d'activer les deux versions.

Paramètres facultatifs	Description
Taille maximale du magasin de hachage	Vous pouvez spécifier la taille à utiliser pour le magasin de données de hachage. Si les données de hachage dépassent cette valeur, ONTAP supprime des hachages plus anciens pour faire de la place à des hachages plus récents. La taille par défaut du magasin de hachage est de 1 Go. BranchCache fonctionne plus efficacement si des hachages ne sont pas éliminés de manière trop agressive. Si vous déterminez que les hachages sont fréquemment ignorés car le magasin de hachage est plein, vous pouvez augmenter la taille du magasin de hachage en modifiant la configuration de BranchCache.
Clé du serveur	Vous pouvez spécifier une clé de serveur utilisée par le service BranchCache pour empêcher les clients d'imiter le serveur BranchCache. Si vous ne spécifiez pas de clé de serveur, une clé est générée de manière aléatoire lors de la création de la configuration de BranchCache. Vous pouvez définir la clé du serveur à une valeur spécifique. Ainsi, si plusieurs serveurs fournissent des données de BranchCache pour les mêmes fichiers, les clients peuvent utiliser des hachages à partir de n'importe quel serveur à l'aide de la même clé de serveur. Si la clé du serveur contient des espaces, vous devez inclure la clé du serveur entre guillemets.
Mode de fonctionnement	Par défaut, BranchCache est activé par partage. • Pour créer une configuration de BranchCache dans laquelle vous activez BranchCache par partage, vous pouvez soit spécifier ce paramètre facultatif, soit `per-share`. • Pour activer automatiquement BranchCache sur tous les partages, vous devez définir le mode de fonctionnement sur `all-shares`.

Étapes

1. SMB 2.1 et 3.0 si nécessaire :
   a. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
   b. Vérifier les paramètres du SVM SMB configurés pour déterminer si toutes les versions nécessaires de SMB sont activées : `vserver cifs options show -vserver` *`vserver_name`*
   c. Si nécessaire, activez SMB 2.1 : `vserver cifs options modify -vserver` *`vserver_name`* `-smb2-enabled true`

      La commande active SMB 2.0 et SMB 2.1.

   d. Si nécessaire, activez SMB 3.0 : `vserver cifs options modify -vserver` *`vserver_name`*

```
-smb3-enabled true
```

e. Retour au niveau de privilège admin : `set -privilege admin`

2. Configurer BranchCache : `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   Le chemin de stockage de hachage spécifié doit exister et doit résider sur un volume géré par la SVM. Le chemin doit également être situé sur un volume accessible en lecture-écriture. La commande échoue si le chemin d'accès est en lecture seule ou n'existe pas.

   Si vous souhaitez utiliser la même clé de serveur pour d'autres configurations de BranchCache du SVM, enregistrez la valeur que vous entrez pour la clé du serveur. La clé du serveur n'apparaît pas lorsque vous affichez des informations sur la configuration de BranchCache.

3. Vérifiez que la configuration de BranchCache est correcte : `vserver cifs branchcache show -vserver vserver_name`

Exemples

Les commandes suivantes vérifient que SMB 2.1 et 3.0 sont activées et configurent BranchCache pour activer automatiquement la mise en cache sur tous les partages SMB sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Les commandes suivantes vérifient que SMB 2.1 et 3.0 sont activées, configurent BranchCache pour permettre la mise en cache par partage sur le SVM vs1 et vérifient la configuration de BranchCache :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informations associées

- En savoir plus sur la prise en charge des versions de BranchCache
- En savoir plus sur la configuration de BranchCache au bureau distant
- Créez un partage SMB compatible BranchCache
- Activer BranchCache sur les partages existants
- Modifier les configurations de BranchCache sur les partages
- En savoir plus sur la désactivation de BranchCache sur les partages
- Supprimer la configuration BranchCache sur les partages

En savoir plus sur la configuration de BranchCache au bureau distant dans ONTAP SMB

Une fois BranchCache configuré sur le serveur SMB, vous devez installer et configurer BranchCache sur les ordinateurs clients et, éventuellement, sur les serveurs de mise en cache de votre bureau distant. Microsoft fournit des instructions pour configurer BranchCache dans le bureau distant.

Les instructions de configuration des clients des succursales et, éventuellement, des serveurs de mise en cache pour utiliser BranchCache sont disponibles sur le site Web Microsoft BranchCache.

"Microsoft BranchCache Docs : nouveautés"

Configurez des partages SMB compatibles avec BranchCache

En savoir plus sur la configuration des partages SMB ONTAP compatibles BranchCache

Une fois que vous avez configuré BranchCache sur le serveur SMB et dans la succursale, vous pouvez activer BranchCache sur des partages SMB contenant du contenu que vous souhaitez autoriser les clients des succursales à mettre en cache.

La mise en cache de BranchCache peut être activée sur tous les partages SMB sur le serveur SMB ou sur la base du partage par partage.

- Si vous activez BranchCache sur le partage à partage, vous pouvez activer BranchCache pendant la création du partage ou en modifiant les partages existants.

  Si vous activez la mise en cache sur un partage SMB existant, ONTAP commence des hachages de calcul et envoie des métadonnées aux clients demandant du contenu dès que vous activez BranchCache sur ce partage.

- Les clients qui disposent d'une connexion SMB existante vers un partage n'bénéficient pas de la prise en charge de BranchCache si ce partage est ensuite activé.

  ONTAP annonce la prise en charge de BranchCache pour un partage au moment de la configuration de la session SMB. Les clients qui ont déjà établi des sessions lorsque BranchCache est activé doivent se déconnecter, puis se reconnecter pour utiliser le contenu mis en cache pour ce partage.

> Si BranchCache sur un partage SMB est ensuite désactivé, ONTAP arrête d'envoyer les métadonnées au client demandeur. Un client qui a besoin de données l'extrait directement du serveur de contenu (serveur SMB).

Créer des partages SMB ONTAP compatibles avec BranchCache

Vous pouvez activer BranchCache sur un partage SMB lors de la création du partage en configurant le `branchcache` propriété de partage.

Description de la tâche

- Si BranchCache est activé sur le partage SMB, le partage doit disposer de la configuration des fichiers hors ligne pour la mise en cache manuelle.

  Il s'agit du paramètre par défaut lorsque vous créez un partage.

- Vous pouvez également spécifier d'autres paramètres de partage facultatifs lorsque vous créez le partage avec BranchCache.
- Vous pouvez définir le `branchcache` Propriété sur un partage, même si BranchCache n'est pas configuré et activé sur le serveur virtuel de stockage (SVM).

  Toutefois, si vous souhaitez que le partage offre du contenu en cache, vous devez configurer et activer BranchCache sur le SVM.

- Puisqu'aucune propriété de partage par défaut n'est appliquée au partage lorsque vous utilisez le `-share -properties` paramètre, vous devez spécifier toutes les autres propriétés de partage que vous souhaitez

appliquer au partage en plus de `branchcache` partager la propriété à l'aide d'une liste délimitée par des virgules.

- Pour en savoir plus, `vserver cifs share create` consultez le "Référence de commande ONTAP".

Étape

1. Création d'un partage SMB compatible avec BranchCache :
   `vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,…]`
2. Vérifiez que la propriété de partage BranchCache est définie sur le partage SMB à l'aide du `vserver cifs share show` commande.

Exemple

La commande suivante crée un partage SMB avec fonction de BranchCache nommé « data » avec le chemin d'accès de `/data` Sur la SVM vs1. Par défaut, le paramètre fichiers hors ligne est défini sur `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informations associées

Désactiver BranchCache sur un seul partage

Activer BranchCache sur les partages SMB ONTAP existants

Vous pouvez activer BranchCache sur un partage SMB existant en ajoutant le `branchcache` partager la propriété dans la liste existante des propriétés de partage.

Description de la tâche

- Si BranchCache est activé sur le partage SMB, le partage doit disposer de la configuration des fichiers hors ligne pour la mise en cache manuelle.

  Si le paramètre fichiers hors ligne du partage existant n'est pas défini sur mise en cache manuelle, vous devez le configurer en modifiant le partage.

- Vous pouvez définir le `branchcache` Propriété sur un partage, même si BranchCache n'est pas configuré et activé sur le serveur virtuel de stockage (SVM).

  Toutefois, si vous souhaitez que le partage offre du contenu en cache, vous devez configurer et activer BranchCache sur le SVM.

- Lorsque vous ajoutez le `branchcache` la propriété de partage sur le partage, les paramètres de partage existants et les propriétés de partage sont conservés.

  La propriété de partage BranchCache est ajoutée à la liste existante des propriétés de partage. Pour en savoir plus, `vserver cifs share properties add` consultez le "Référence de commande ONTAP".

Étapes

1. Si nécessaire, configurez le paramètre de partage de fichiers hors ligne pour la mise en cache manuelle :
   a. Déterminez ce que le paramètre de partage de fichiers hors ligne est défini à l'aide de l' `vserver cifs share show` commande.
   b. Si le paramètre de partage de fichiers hors ligne n'est pas défini sur manuel, remplacez-le par la valeur requise : `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Activer BranchCache sur un partage SMB existant : `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Vérifiez que la propriété de partage BranchCache est définie sur le partage SMB : `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemple

La commande suivante permet d'activer BranchCache sur un partage SMB existant nommé « data2 » avec le chemin d'accès de `/data2` Sur la SVM vs1 :

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informations associées

- Ajouter ou supprimer des propriétés de partage sur des partages existants
- Désactiver BranchCache sur un seul partage

Modifier les configurations de BranchCache sur les partages SMB ONTAP

Vous pouvez modifier la configuration du service de BranchCache sur les SVM, notamment la modification du chemin du répertoire du magasin de hachage, la taille maximale du répertoire, le mode de fonctionnement et les versions de BranchCache prises en charge. Vous pouvez également augmenter la taille du volume contenant le magasin de hachage.

Étapes

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Entrez les informations suivantes…
Modifier la taille du répertoire du magasin de hachage	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Augmentez la taille du volume contenant le magasin de hachage	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Si le volume contenant le magasin de hachage se remplit, vous pourrez peut-être augmenter la taille du volume. Vous pouvez spécifier la nouvelle taille du volume comme un nombre suivi d'une désignation d'unité. En savoir plus sur "Gestion des volumes FlexVol"	Modifiez le chemin du répertoire du magasin de hachage

Les fonctions que vous recherchez…	Entrez les informations suivantes…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Si le SVM est une source de reprise d'activité du SVM, le chemin de hachage ne peut pas se trouver sur le volume root. En effet, le volume racine n'est pas répliqué vers la destination de reprise après incident. Le chemin de hachage BranchCache peut contenir des blancs et des caractères de nom de fichier valides. Si vous modifiez le chemin de hachage, `-flush -hashes` Est un paramètre requis qui spécifie si vous souhaitez que ONTAP affleure les hachages à partir de l'emplacement de magasin de hachage d'origine. Vous pouvez définir les valeurs suivantes pour le `-flush-hashes` paramètre : **Si vous spécifiez `true`, ONTAP supprime les hachages dans l'emplacement d'origine et crée de nouveaux hachages à l'emplacement du nouveau, car les nouvelles demandes sont effectuées par des clients compatibles BranchCache.** Si vous spécifiez `false`, les hachages ne sont pas vidés. + Dans ce cas, vous pouvez choisir de réutiliser les hachages existants ultérieurement en retrouvant le chemin du magasin de hachage à l'emplacement d'origine.
Changer le mode de fonctionnement	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share	all-shares	disable}` Lors de la modification du mode de fonctionnement, vous devez connaître les éléments suivants : **ONTAP annonce la prise en charge de BranchCache pour un partage lors de la configuration de la session SMB.** Les clients qui ont déjà établi des sessions lorsque BranchCache est activé doivent se déconnecter, puis se reconnecter pour utiliser le contenu mis en cache pour ce partage.
Modifier la prise en charge de BranchCache	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable	v2-enable	enable-all}`

2. Vérifiez les modifications de configuration à l'aide de la `vserver cifs branchcache show` commande.

Afficher des informations sur les configurations BranchCache sur les partages SMB ONTAP

Vous pouvez afficher des informations sur les configurations de BranchCache sur les SVM (Storage Virtual machines), qui peuvent être utilisées lors de la vérification d'une configuration ou lors de la détermination des paramètres actuels avant de modifier une configuration.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher…	Entrez cette commande…
Récapitulatif des informations sur les configurations de BranchCache sur tous les SVM	`vserver cifs branchcache show`
Informations détaillées sur la configuration d'un SVM spécifique	`vserver cifs branchcache show -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche des informations sur la configuration de BranchCache sur le SVM vs1 :

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

Modifier la clé du serveur ONTAP SMB BranchCache

Il est possible de modifier la clé du serveur de BranchCache en modifiant la configuration de BranchCache sur le serveur virtuel de stockage (SVM) et en indiquant une clé de serveur différente.

Description de la tâche

Vous pouvez définir la clé du serveur à une valeur spécifique. Ainsi, si plusieurs serveurs fournissent des données de BranchCache pour les mêmes fichiers, les clients peuvent utiliser des hachages à partir de n'importe quel serveur à l'aide de la même clé de serveur.

Lorsque vous modifiez la clé du serveur, vous devez également vider le cache de hachage. Après avoir effectué des hachages, ONTAP crée des hachages de nouvelles demandes des clients compatibles avec BranchCache.

Étapes

1. Modifiez la clé du serveur à l'aide de la commande suivante : `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   Lors de la configuration d'une nouvelle clé de serveur, vous devez également spécifier `-flush-hashes` et définissez la valeur sur `true`.

2. Vérifiez que la configuration de BranchCache est correcte à l'aide du `vserver cifs branchcache show` commande.

Exemple

L'exemple suivant définit une nouvelle clé de serveur qui contient des espaces et purge le cache de hachage sur la SVM vs1 :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informations associées

Découvrez les raisons pour lesquelles ONTAP invalide les hachages BranchCache

Précalculer les hachages BranchCache sur les chemins SMB ONTAP spécifiés

Vous pouvez configurer le service de BranchCache pour précalculer les hachages pour un seul fichier, un répertoire ou tous les fichiers d'une structure de répertoires. Cette fonctionnalité est utile pour calculer des hachages de données dans un partage de BranchCache pendant les heures creuses.

Description de la tâche

Si vous souhaitez collecter un échantillon de données avant d'afficher les statistiques de hachage, vous devez utiliser le `statistics start` et en option `statistics stop` commandes.

- Vous devez spécifier la machine virtuelle de stockage (SVM) et le chemin d'accès sur lequel vous souhaitez précalculer les hachages.
- Vous devez également indiquer si vous voulez que des hachages soient calculés de manière récursive.
- Si vous souhaitez calculer des hachages de façon récursive, le service BranchCache traverse l'intégralité de l'arborescence du répertoire sous le chemin spécifié et calcule des hachages pour chaque objet éligible.

  En savoir plus sur `statistics start` et `statistics stop` dans le "Référence de commande

ONTAP" .

Étapes

1. Des hachages de pré-calcul si vous le souhaitez :

Si vous voulez précalculer des hachages sur…	Entrez la commande…
Un seul fichier ou répertoire	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Récursivement sur tous les fichiers d'une structure de répertoires	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Vérifiez que des hachages sont calculés à l'aide de l' `statistics` commande :

   a. Affiche les statistiques du `hashd` Objet sur l'instance SVM souhaitée : `statistics show -object hashd -instance vserver_name`

   b. Vérifiez que le nombre de hachages créés augmente en répétant la commande.

   Pour en savoir plus, `statistics show` consultez le "Référence de commande ONTAP".

Exemples

L'exemple suivant crée des hachages sur le chemin d'accès `/data` Et sur tous les fichiers et sous-répertoires contenus dans la SVM vs1 :

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Informations associées

- "Configuration du contrôle des performances"

Vider les hachages du magasin de hachage ONTAP SMB SVM BranchCache

Vous pouvez vider toutes les hachages en cache du magasin de hachage BranchCache sur la machine virtuelle de stockage (SVM). Cette fonction est utile si vous avez modifié la configuration de BranchCache du bureau de succursale. Par exemple, si vous avez récemment reconfiguré le mode de mise en cache de la mise en cache distribuée au mode de mise en cache hébergée, vous devrez vider le magasin de hachage.

Description de la tâche

Après avoir effectué des hachages, ONTAP crée des hachages de nouvelles demandes des clients compatibles avec BranchCache.

Étape

1. Rincez les hachages à partir du magasin de hachage BranchCache : `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Afficher les statistiques ONTAP SMB BranchCache

Vous pouvez afficher des statistiques de BranchCache, notamment, afin d'identifier le niveau de mise en cache efficace, déterminer si votre configuration fournit du contenu mis en cache aux clients et déterminer si les fichiers de hachage ont été supprimés pour prendre de l'espace pour les données de hachage les plus récentes.

Description de la tâche

Le `hashd` L'objet statistique contient des compteurs qui fournissent des informations statistiques sur les hachages de BranchCache. Le `cifs` L'objet statistique contient des compteurs qui fournissent des informations statistiques sur l'activité liée à BranchCache. Vous pouvez collecter et afficher les informations relatives à ces objets au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Afficher les compteurs liés à BranchCache à l'aide du `statistics catalog counter show` commande.

   ```
   cluster1::*> statistics catalog counter show -object hashd

   Object: hashd
       Counter                     Description
   ```

```
    --------------------------
-------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
```

```
It
                                  does not include attempts to fetch hash
data
                                  that has not yet been generated.
    branchcache_hash_fetch_ok     Total number of times a request to fetch
hash
                                  data succeeded.
    branchcache_hash_sent_bytes   Total number of bytes sent to clients
                                  requesting hashes.
    branchcache_missing_hash_bytes
                                  Total number of bytes of data that had
to be
                                  read by the client because the hash for
that
                                  content was not available on the server.
    ....Output truncated....
```

Pour en savoir plus, `statistics catalog counter show` consultez le "Référence de commande ONTAP".

3. Collectez les statistiques liées à BranchCache à l'aide du `statistics start` et `statistics stop` commandes.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

En savoir plus sur `statistics start` et `statistics stop` dans le "Référence de commande ONTAP" .

4. Afficher les statistiques de BranchCache collectées à l'aide de `statistics show` commande.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

Pour en savoir plus, `statistics show` consultez le "Référence de commande ONTAP".

5. Retour au niveau de privilège admin : `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Informations associées

- Affiche les statistiques
- "Configuration du contrôle des performances"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

En savoir plus sur la prise en charge ONTAP SMB pour les objets de stratégie de groupe BranchCache

ONTAP BranchCache prend en charge les objets de stratégie de groupe (GPO) de BranchCache, ce qui permet une gestion centralisée de certains paramètres de configuration de BranchCache. Deux GPO sont utilisés pour BranchCache, la publication Hash pour BranchCache et la prise en charge de la version Hash pour BranchCache.

- **Publication Hash pour BranchCache**

  La publication Hash pour BranchCache de BranchCache correspond à `-operating-mode` paramètre. Lors des mises à jour de GPO, cette valeur est appliquée aux objets SVM (Storage Virtual machine) contenus dans l'unité organisationnelle à laquelle s'applique la stratégie de groupe.

- **Prise en charge de la version de hachage pour BranchCache**

  La prise en charge de la version de hachage pour BranchCache correspond au `-versions` paramètre. Lors des mises à jour de GPO, cette valeur est appliquée aux objets SVM contenus dans l'unité organisationnelle à laquelle la politique de groupe s'applique.

Informations associées

En savoir plus sur l'application des objets de stratégie de groupe aux serveurs SMB

Afficher des informations sur les objets de stratégie de groupe ONTAP SMB BranchCache

Vous pouvez afficher des informations sur la configuration GPO (Group Policy Object) du serveur CIFS pour déterminer si des GPO de BranchCache sont définis pour le domaine auquel le serveur CIFS appartient et, le cas échéant, quels sont les paramètres autorisés. Vous pouvez également déterminer si les paramètres GPO de BranchCache sont appliqués au serveur CIFS.

Description de la tâche

Bien qu'un paramètre GPO soit défini au sein du domaine auquel le serveur CIFS appartient, il n'est pas nécessairement appliqué à l'unité organisationnelle contenant la machine virtuelle de stockage (SVM) compatible CIFS. Le paramètre GPO appliqué est le sous-ensemble de tous les GPO définis qui sont appliqués à la SVM compatible CIFS. Les paramètres BranchCache appliqués via les GPO remplacent les paramètres appliqués via l'interface CLI.

Étapes

1. Affichez le paramètre GPO de BranchCache défini pour le domaine Active Directory à l'aide du `vserver cifs group-policy show-defined` commande.

   Cet exemple n'affiche pas tous les champs de sortie disponibles pour la commande. La sortie est tronquée.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Affichez le paramètre GPO de BranchCache appliqué au serveur CIFS à l'aide de `vserver cifs group-policy show-applied` commande. ``

> Cet exemple n'affiche pas tous les champs de sortie disponibles pour la commande. La sortie est tronquée.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Informations associées

- Activer ou désactiver la prise en charge des GPO sur les serveurs
- "vserver cifs group-policy show-defined"
- "vserver cifs group-policy show-applied"

Désactiver BranchCache sur les partages SMB

En savoir plus sur la désactivation de BranchCache sur les partages SMB ONTAP

Si vous ne souhaitez pas fournir de services de mise en cache de BranchCache sur certains partages SMB, mais que vous pouvez ensuite fournir des services de mise en cache, vous pouvez désactiver BranchCache sur le partage à partager. Si BranchCache est configuré pour assurer la mise en cache sur tous les partages, mais que vous souhaitez désactiver temporairement tous les services de mise en cache, vous pouvez modifier la configuration de BranchCache afin d'arrêter la mise en cache automatique sur tous les partages.

Si BranchCache sur un partage SMB est ensuite désactivé après son activation, ONTAP arrête d'envoyer les métadonnées au client qui demande. Client qui a besoin de données la récupère directement depuis le serveur de contenu (serveur CIFS sur la machine virtuelle de stockage (SVM)).

Informations associées

En savoir plus sur la configuration des partages compatibles BranchCache

Désactiver BranchCache sur un seul partage SMB ONTAP

Si vous ne souhaitez pas offrir de services de mise en cache sur certains partages qui proposaient déjà du contenu en cache, vous pouvez désactiver BranchCache sur un partage SMB existant.

Étape

1. Saisissez la commande suivante : `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   La propriété de partage BranchCache est supprimée. Les autres propriétés de partage appliquées restent en vigueur.

Exemple

La commande suivante désactive BranchCache sur un partage SMB existant nommé « data2 » :

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Arrêter la mise en cache automatique sur tous les partages SMB ONTAP

Si votre configuration de BranchCache permet automatiquement la mise en cache de tous les partages SMB sur chaque serveur virtuel de stockage (SVM), vous pouvez modifier la configuration de BranchCache afin d'arrêter automatiquement la mise en cache du contenu pour tous les partages SMB.

Description de la tâche

Pour arrêter la mise en cache automatique sur tous les partages SMB, il est possible de basculer le mode d'exploitation de BranchCache vers la mise en cache par partage.

Étapes

1. Configurer BranchCache pour arrêter la mise en cache automatique sur tous les partages SMB : `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Vérifiez que la configuration de BranchCache est correcte : `vserver cifs branchcache show -vserver vserver_name`

Exemple

La commande suivante modifie la configuration de BranchCache sur le serveur de stockage virtuel (SVM, précédemment appelé vServer) vs1 pour arrêter la mise en cache automatique sur tous les partages SMB :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Désactivation ou activation de BranchCache sur le SVM

Découvrez ce qui se passe lorsque vous désactivez ou réactivez BranchCache sur les serveurs SMB ONTAP

Si vous avez déjà configuré BranchCache, mais que vous ne souhaitez pas que les clients des succursales utilisent le contenu en cache, vous pouvez désactiver la mise en cache sur le serveur CIFS. Vous devez savoir ce qui se passe lorsque vous désactivez BranchCache.

Lorsque vous désactivez BranchCache, ONTAP ne calcule plus de hachages et n'envoie plus les métadonnées au client qui demande. Toutefois, l'accès aux fichiers n'est pas interrompu. Par la suite, lorsque des clients compatibles avec BranchCache demandent des informations de métadonnées pour le contenu auquel ils doivent accéder, ONTAP répond par une erreur définie par Microsoft, ce qui entraîne l'envoi d'une seconde demande par le client, demandant le contenu réel. En réponse à la demande de contenu, le serveur

CIFS envoie le contenu réel stocké sur la machine virtuelle de stockage (SVM).

Une fois que BranchCache est désactivé sur le serveur CIFS, les partages SMB n'annoncent pas les fonctionnalités de BranchCache. Pour accéder aux données lors de nouvelles connexions SMB, les clients font des requêtes SMB en lecture standard.

Vous pouvez réactiver BranchCache sur le serveur CIFS à tout moment.

- Comme le magasin de hachage n'est pas supprimé lorsque vous désactivez BranchCache, ONTAP peut utiliser les hachages stockés pour répondre aux demandes de hachage après la réactivation de BranchCache, à condition que le hachage demandé soit toujours valide.
- Tout client qui a établi des connexions SMB vers des partages compatibles avec BranchCache au cours de la désactivation de BranchCache n'est pas pris en charge si BranchCache est ensuite réactivé.

  En effet, ONTAP annonce la prise en charge de BranchCache pour un partage au moment de la configuration de la session SMB. Les clients qui ont établi des sessions vers des partages compatibles BranchCache alors que ce dernier était désactivé doivent se déconnecter et se reconnecter pour utiliser le contenu en cache pour ce partage.

> Si vous ne souhaitez pas enregistrer le magasin de hachage après avoir désactivé BranchCache sur un serveur CIFS, vous pouvez le supprimer manuellement. Si vous réactivez BranchCache, vous devez vous assurer que le répertoire du magasin de hachage existe. Une fois que BranchCache est activé à nouveau, les partages compatibles avec BranchCache publicité des fonctionnalités de BranchCache. ONTAP crée de nouvelles hachages lorsque de nouvelles demandes sont faites par des clients compatibles avec BranchCache.

Désactiver ou activer BranchCache sur les partages SMB ONTAP

Vous pouvez désactiver BranchCache sur le serveur virtuel de stockage (SVM) en changeant le mode d'exploitation BranchCache en `disabled`. Vous pouvez activer BranchCache à tout moment en modifiant le mode d'exploitation afin d'offrir soit des services de BranchCache par partage, soit automatiquement pour tous les partages.

Étapes

1. Exécutez la commande appropriée :

Les fonctions que vous recherchez…	Puis entrez les informations suivantes…
Désactivez BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Activez BranchCache par partage	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
Activez BranchCache pour tous les partages	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Vérifiez que le mode de fonctionnement de BranchCache est configuré avec le paramètre souhaité : `vserver cifs branchcache show -vserver vserver_name`

Exemple

L'exemple suivant désactive BranchCache sur le SVM vs1 :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Supprimez la configuration de BranchCache sur les SVM

Découvrez ce qui se passe lorsque vous supprimez la configuration BranchCache sur les partages SMB ONTAP

Si vous avez déjà configuré BranchCache, mais que vous ne souhaitez pas que le serveur de stockage virtuel (SVM) puisse continuer à fournir du contenu en cache, vous pouvez supprimer la configuration de BranchCache sur le serveur CIFS. Vous devez connaître ce qui se passe lorsque vous supprimez la configuration.

Lorsque vous supprimez la configuration, ONTAP supprime du cluster les informations de configuration du SVM et arrête le service de BranchCache. Vous pouvez choisir si ONTAP doit supprimer le magasin de hachage sur la SVM.

La suppression de la configuration de BranchCache n'interrompt pas l'accès des clients compatibles avec BranchCache. Par la suite, lorsque les clients compatibles avec BranchCache demandent des informations de métadonnées sur les connexions SMB existantes pour du contenu déjà mis en cache, ONTAP répond par une erreur définie par Microsoft, ce qui entraîne l'envoi par le client d'une seconde demande, demandant le contenu réel. En réponse à la demande de contenu, le serveur CIFS envoie le contenu réel stocké sur le SVM

Une fois la configuration de BranchCache supprimée, les partages SMB n'annoncent pas les fonctionnalités de BranchCache. Pour accéder au contenu qui n'avait pas encore été mis en cache par de nouvelles connexions SMB, les clients effectuent des requêtes SMB en lecture standard.

Supprimer la configuration BranchCache sur les partages SMB ONTAP

La commande que vous utilisez pour supprimer le service de BranchCache sur le serveur de stockage virtuel (SVM) diffère selon que vous souhaitez supprimer ou conserver des hachages existants.

Étape

1. Exécutez la commande appropriée :

Les fonctions que vous recherchez…	Puis entrez les informations suivantes…
Supprimez la configuration de BranchCache et supprimez des hachages existants	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Supprimez la configuration de BranchCache, mais conservez des hachages existants	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Exemple

L'exemple suivant supprime la configuration de BranchCache sur le SVM vs1 et supprime toutes les hachages existants :

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Découvrez ce qui arrive à ONTAP SMB BranchCache lors de la restauration

Il est important de comprendre ce qui se passe lorsque vous restaurez ONTAP vers une version qui ne prend pas en charge BranchCache.

- Lorsque vous restaurez vers une version d'ONTAP qui ne prend pas en charge BranchCache, les partages SMB n'publient pas de fonctionnalités de BranchCache pour les clients compatibles avec BranchCache. Ainsi, les clients ne demandent pas d'informations de hachage.

  À la place, ils demandent le véritable contenu à l'aide de demandes de lecture SMB normales. En réponse à la demande de contenu, le serveur SMB envoie le contenu réel qui est stocké sur la machine virtuelle de stockage (SVM).

- Lorsqu'un nœud qui héberge un magasin de hachage est rétabli dans une version qui ne prend pas en charge BranchCache, l'administrateur du stockage doit restaurer manuellement la configuration de BranchCache à l'aide d'une commande imprimée pendant la restauration.

  Cette commande supprime la configuration de BranchCache et des hachages.

  Une fois la restauration terminée, l'administrateur du stockage peut supprimer manuellement le répertoire qui contient le magasin de hachage si nécessaire.

Informations associées

Supprimer la configuration BranchCache sur les partages

Améliorez les performances de la copie à distance Microsoft

Découvrez les améliorations des performances de copie à distance Microsoft sur les serveurs SMB ONTAP

Microsoft Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le

transfert direct de données au sein d'un périphérique de stockage compatible ou entre ces périphériques, sans transférer les données via l'ordinateur hôte.

ONTAP prend en charge ODX à la fois pour les protocoles SMB et SAN. La source peut être un serveur CIFS ou une LUN et la destination peut être un serveur CIFS ou une LUN.

Dans les transferts de fichiers non ODX, les données sont lues à partir de la source et transférées sur le réseau vers l'ordinateur client. L'ordinateur client transfère les données via le réseau vers la destination. En résumé, l'ordinateur client lit les données à partir de la source et les écrit vers la destination. Grâce aux transferts de fichiers ODX, les données sont copiées directement de la source vers la destination.

Les copies déchargées d'ODX étant effectuées directement entre le stockage source et le stockage de destination, les performances sont considérablement améliorées. Les avantages obtenus en termes de performances comprennent l'accélération du délai de copie entre la source et la destination, la réduction de l'utilisation des ressources (CPU, mémoire) sur le client et la réduction de l'utilisation de la bande passante E/S du réseau.

Dans les environnements SMB, cette fonctionnalité n'est disponible que lorsque le client et le serveur de stockage prennent en charge SMB 3.0 et la fonctionnalité ODX. Dans les environnements SAN, cette fonctionnalité n'est disponible que lorsque le client et le serveur de stockage prennent en charge la fonctionnalité ODX. Les ordinateurs clients qui prennent en charge ODX et où ODX est activé automatiquement et de manière transparente utilisent le transfert de fichiers déchargées lors du déplacement ou de la copie des fichiers. ODX est utilisé par glisser-déposer des fichiers via l'Explorateur Windows ou utiliser des commandes de copie de fichier en ligne de commande, ou bien si une application client génère des demandes de copie de fichiers.

Informations associées

- Découvrez comment améliorer le temps de réponse des clients en fournissant des références automatiques de nœuds avec la localisation automatique
- "Configuration SMB pour Microsoft Hyper-V et SQL Server"

En savoir plus sur ODX sur les serveurs SMB ONTAP

L'allègement de la charge de copies (ODX) utilise un mécanisme basé sur des jetons pour la lecture et l'écriture des données dans et entre des serveurs CIFS compatibles avec ODX. Au lieu d'acheminer les données via l'hôte, le serveur CIFS envoie un petit jeton qui représente les données au client. Le client ODX présente ce token au serveur de destination, qui peut ensuite transférer les données représentées par ce token de la source vers la destination.

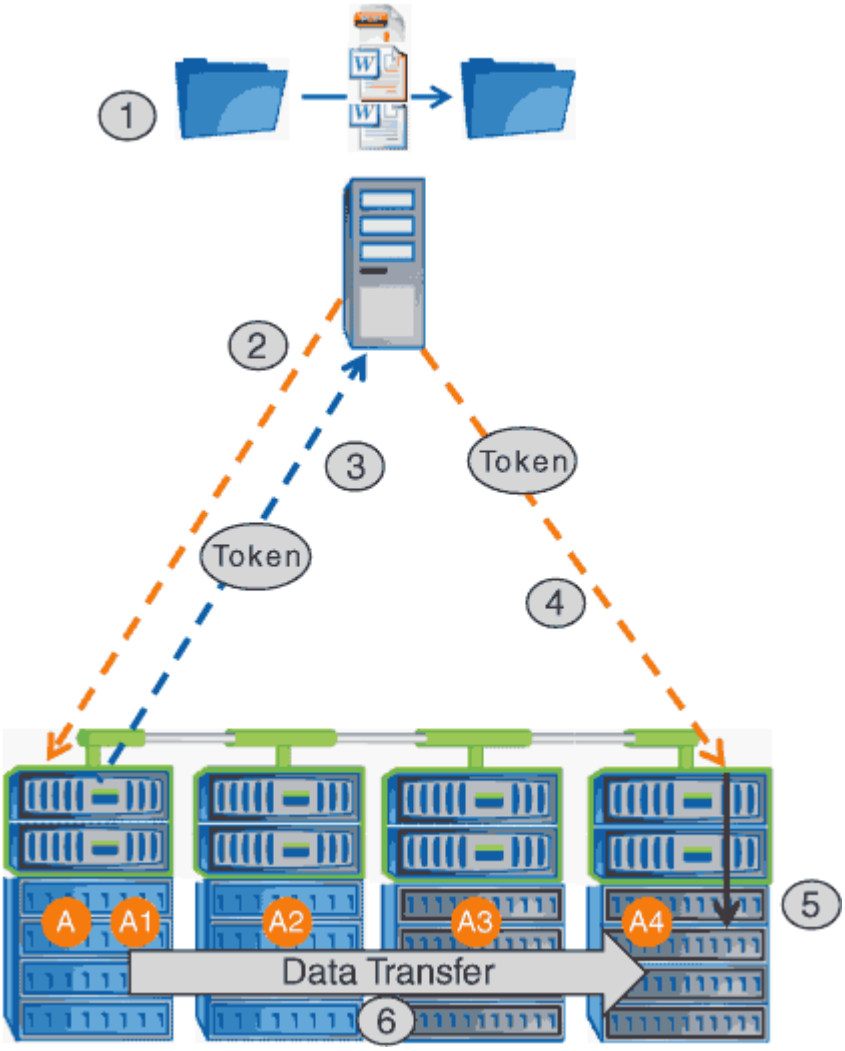
Lorsqu'un client ODX apprend que le serveur CIFS prend en charge ODX, il ouvre le fichier source et demande un jeton au serveur CIFS. Après l'ouverture du fichier de destination, le client utilise le jeton pour demander au serveur de copier les données directement de la source vers la destination.

> La source et la destination peuvent se trouver sur le même SVM (Storage Virtual machine) ou sur différents SVM, selon le cadre de l'opération de copie.

Ce token sert de représentation des données à un point dans le temps. Par exemple, lorsque vous copiez des données entre des emplacements de stockage, un token représentant un segment de données est renvoyé au client requérant, que le client copie vers la destination, ce qui élimine la nécessité de copier les données sous-jacentes via le client.

ONTAP prend en charge les jetons représentant 8 Mo de données. Des copies ODX de plus de 8 Mo sont effectuées à l'aide de plusieurs jetons, chaque jeton représentant 8 Mo de données.

La figure suivante décrit les étapes du processus de copie d'ODX :



1. Un utilisateur copie ou déplace un fichier à l'aide de l'Explorateur Windows, d'une interface de ligne de commande ou dans le cadre d'une migration d'un serveur virtuel, ou une application crée des copies ou des déplacements de fichiers.
2. Le client compatible ODX convertit automatiquement cette demande de transfert en requête d'ODX.

   La demande ODX envoyée au serveur CIFS contient une demande de jeton.
3. Si ODX est activé sur le serveur CIFS et que la connexion est via SMB 3.0, le serveur CIFS génère un jeton, qui est une représentation logique des données sur la source.
4. Le client reçoit un jeton représentant les données et l'envoie avec la demande d'écriture au serveur CIFS de destination.

   Il s'agit des seules données copiées sur le réseau de la source vers le client, puis du client vers la destination.
5. Ce jeton est fourni au sous-système de stockage.
6. La SVM effectue en interne la copie ou déplacement.

Si le fichier copié ou déplacé dépasse 8 Mo, plusieurs jetons sont nécessaires pour effectuer la copie. Les étapes 2 à 6 ont été effectuées selon les besoins pour compléter la copie.

> En cas de défaillance de la copie ODX déchargée, l'opération de copie ou de déplacement retourne aux lectures et écritures traditionnelles de la copie ou du déplacement. De même, si le serveur CIFS de destination ne prend pas en charge ODX ou ODX est désactivé, l'opération de copie ou de déplacement retourne aux opérations classiques de lecture et d'écriture pour la copie ou de déplacement.

Conditions requises pour l'utilisation d'ODX sur les serveurs ONTAP SMB

Avant de pouvoir utiliser ODX pour la réduction des déchargements de copies avec votre machine virtuelle de stockage (SVM), vous devez prendre en compte certaines exigences.

Configuration requise pour la version ONTAP

Les versions d'ONTAP prennent en charge ODX pour la réduction des copies.

Conditions requises pour la version SMB

- ONTAP prend en charge ODX avec SMB 3.0 et versions ultérieures.
- SMB 3.0 doit être activé sur le serveur CIFS pour que ODX puisse être activé :
  - L'activation d'ODX active également SMB 3.0, si elle n'est pas déjà activée.
  - La désactivation de SMB 3.0 désactive également ODX.

Configuration requise pour le serveur et le client Windows

Avant de pouvoir utiliser ODX pour la réduction des tâches de copie, le client Windows doit prendre en charge cette fonctionnalité.

Le "Matrice d'interopérabilité NetApp"Contient les informations les plus récentes sur les clients Windows pris en charge.

Besoins en termes de volume

- Les volumes source doivent être d'au moins 1.25 Go.
- Si vous utilisez des volumes compressés, le type de compression doit être adaptatif et seule la taille de groupe de compression de 8 Ko est prise en charge.

  Le type de compression secondaire n'est pas pris en charge.

Directives d'utilisation d'ODX sur les serveurs ONTAP SMB

Avant de pouvoir utiliser ODX pour l'allègement de la charge des copies, vous devez prendre connaissance des instructions. Par exemple, vous devez connaître les types de volumes que vous pouvez utiliser ODX, et connaître les considérations d'ODX au sein du cluster et entre clusters.

Règles relatives aux volumes

- ODX ne peut pas être utilisé pour l'allègement de la charge des copies avec les configurations de volume suivantes :
  - La taille du volume source est inférieure à 1.25 Go

    La taille du volume doit être supérieure ou égale à 1.25 Go pour utiliser ODX.

  - Volumes en lecture seule

    ODX n'est pas utilisé pour les fichiers et les dossiers résidant dans des miroirs de partage de charge ou dans des volumes de destination SnapMirror ou SnapVault.

  - Si le volume source n'est pas dédupliqué
- Les copies ODX sont prises en charge uniquement pour les copies intra-cluster.

  Vous ne pouvez pas utiliser ODX pour copier des fichiers ou des dossiers vers un volume d'un autre cluster.

Autres lignes directrices

- Dans les environnements SMB, pour utiliser ODX pour l'allègement de la charge des copies, les fichiers doivent être d'une taille supérieure ou égale à 256 Ko.

  Les fichiers plus petits sont transférés à l'aide d'une opération de copie traditionnelle.

- La fonctionnalité de déchargement des copies d'ODX utilise la déduplication dans le cadre du processus de copie.

  Si vous ne souhaitez pas que la déduplication s'exécute sur les volumes SVM lors de la copie ou du déplacement de données, vous devez désactiver la décharge des copies ODX sur ce SVM.

- L'application qui effectue le transfert de données doit être écrite pour prendre en charge ODX.

  Les opérations applicatives prenant en charge ODX sont les suivantes :

  - Les opérations de gestion Hyper-V, telles que la création et la conversion de disques durs virtuels (VHD), la gestion de snapshots et la copie de fichiers entre des machines virtuelles
  - Opérations de l'Explorateur Windows
  - Commandes de copie Windows PowerShell
  - Commandes de copie de l'invite de commande Windows

    Robocopy à l'invite de commandes Windows prend en charge ODX.

    > Les applications doivent être exécutées sur des serveurs Windows ou des clients prenant en charge ODX.

  +
  Pour plus d'informations sur les applications ODX prises en charge sur les serveurs et clients Windows, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Cas d'utilisation d'ODX sur les serveurs ONTAP SMB

Vous devez tenir compte des cas d'utilisation d'ODX sur des SVM afin de pouvoir déterminer dans quelles circonstances ODX vous fournit des avantages en matière de performances.

Par défaut, les serveurs et clients Windows qui prennent en charge ODX utilisent la fonction d'allègement de la charge des copies pour copier des données sur des serveurs distants. Si le serveur ou le client Windows ne prend pas en charge ODX, ou si l'allègement de la charge des copies ODX échoue à tout moment, l'opération de copie ou de déplacement retourne aux lectures et écritures classiques pour la copie ou le déplacement.

Les cas d'utilisation suivants prennent en charge l'utilisation de copies et de déplacements d'ODX :

- Intra-volume

  Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volume, même nœud, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

  Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

- Inter-cluster

  Les LUN source et de destination se trouvent sur des volumes différents, sur différents nœuds, sur l'ensemble des clusters. Ceci n'est pris en charge que pour SAN et ne fonctionne pas pour CIFS.

Il existe d'autres cas d'utilisation spéciaux :

- Dans l'implémentation de ONTAP ODX, vous pouvez utiliser ODX pour copier des fichiers entre des partages SMB et des disques virtuels connectés FC ou iSCSI.

  Vous pouvez utiliser Windows Explorer, l'interface de ligne de commande Windows ou PowerShell, Hyper-V ou d'autres applications prenant en charge ODX pour copier ou déplacer des fichiers de manière transparente à l'aide de l'allègement de la charge des copies ODX entre les partages SMB et les LUN connectés, à condition que les partages SMB et les LUN soient sur le même cluster.

- Hyper-V fournit des cas d'utilisation supplémentaires pour la décharge de copies ODX :
  - Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.

    Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.
  - Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
  - L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.

> Pour tirer parti des cas d'utilisation liés au délestage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Activer ou désactiver ODX sur les serveurs ONTAP SMB

Vous pouvez activer ou désactiver ODX sur des SVM. Par défaut, est d'activer la prise en charge de l'allègement de la charge des copies (ODX) si SMB 3.0 est également activé.

Avant de commencer

SMB 3.0 doit être activé.

Description de la tâche

Si vous désactivez SMB 3.0, ONTAP désactive également SMB ODX. Si vous réactivez SMB 3.0, vous devez réactiver manuellement SMB ODX.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que l'allègement de la charge des copies ODX soit…	Entrez la commande…
Activé	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Désactivé	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant active la décharge de la copie ODX sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Informations associées

Options de serveur disponibles

Améliorer le temps de réponse des clients en fournissant des référencements de nœuds automatiques SMB avec Auto Location

Découvrez comment améliorer le temps de réponse des clients en fournissant des références automatiques de nœuds ONTAP SMB avec localisation automatique

Auto Location utilise les référencements automatiques des nœuds SMB pour augmenter les performances des clients SMB sur les machines virtuelles de stockage (SVM). Les référencements automatiques du nœud reconnectent automatiquement le client demandeur à une LIF sur le SVM du nœud qui héberge le volume dans lequel résident les données, ce qui peut améliorer les temps de réponse du client.

Lorsqu'un client SMB se connecte à un partage SMB hébergé sur le SVM, il peut se connecter à l'aide d'une LIF qui se trouve sur un nœud qui ne possède pas les données demandées. Le nœud auquel le client est connecté accède aux données détenues par un autre nœud via le réseau de cluster. Le client peut bénéficier de temps de réponse plus rapides si la connexion SMB utilise une LIF située sur le nœud contenant les données demandées :

- ONTAP fournit cette fonctionnalité à l'aide des référencements Microsoft DFS pour informer les clients SMB qu'un fichier ou dossier demandé dans l'espace de noms est hébergé quelque part.

  Un nœud fait une recommandation lorsqu'il détermine qu'il existe une LIF de SVM sur le nœud qui contient les données.

- Les référencements de nœuds automatiques sont pris en charge pour les adresses IP LIF IPv4 et IPv6.
- Les renvois sont effectués en fonction de l'emplacement de la racine du partage auquel le client est connecté.
- Le renvoi se produit pendant la négociation avec les PME.

  Le renvoi est effectué avant l'établissement de la connexion. Après que ONTAP désigne le client SMB au nœud cible, la connexion est établie et le client accède aux données via le chemin LIF référencé à partir de ce point. Les clients accèdent ainsi plus rapidement aux données et évitent toute communication supplémentaire avec le cluster.

Si un partage couvre plusieurs points de jonction et que certaines des jonctions sont vers les volumes contenus sur les autres nœuds, les données du partage sont réparties sur plusieurs nœuds. Étant donné que ONTAP fournit des référencements locaux à la racine du partage, ONTAP doit utiliser le réseau cluster pour récupérer les données contenues dans ces volumes non locaux. Avec ce type d'architecture de namespace, les référencements automatiques des nœuds ne peuvent pas être significatifs pour les performances.

Si le nœud qui héberge les données ne dispose pas de LIF disponible, ONTAP établit la connexion en utilisant la LIF choisie par le client. Une fois qu'un fichier est ouvert par un client SMB, il continue à accéder au fichier via la même connexion référencée.

Si, pour une raison quelconque, le serveur CIFS ne peut pas faire de recommandation, le service SMB ne subit aucune perturbation. La connexion SMB est établie comme si les référencements de nœuds automatiques n'étaient pas activés.

Informations associées

Amélioration des performances de la copie à distance Microsoft

Exigences et directives pour l'utilisation des références automatiques de nœuds sur les serveurs ONTAP SMB

Avant de pouvoir utiliser les référencements de nœud automatiques SMB, également appelés *autolocalisation*, vous devez connaître certaines exigences, y compris les versions de ONTAP qui prennent en charge la fonctionnalité. Vous devez également connaître les versions du protocole SMB prises en charge et d'autres directives spéciales.

Version ONTAP et conditions requises pour les licences

- Tous les nœuds du cluster doivent exécuter une version de ONTAP qui prend en charge les référencements de nœuds automatiques.
- Les Widelinks doivent être activés sur un partage SMB pour utiliser l'autolocalisation.
- CIFS doit être sous licence et un serveur SMB doit exister sur les SVM. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Version requise du protocole SMB

- Pour les SVM, ONTAP prend en charge les référencements de nœuds automatiques sur toutes les versions de SMB.

Exigences des clients PME

Tous les clients Microsoft pris en charge par ONTAP prennent en charge les référencements automatiques des nœuds SMB.

La matrice d'interopérabilité contient les dernières informations sur les clients Windows pris en charge par ONTAP.

"Matrice d'interopérabilité NetApp"

Configuration requise pour Data LIF

Si vous souhaitez utiliser une LIF de données comme référence potentielle pour les clients SMB, vous devez créer des LIF de données avec NFS et CIFS activés.

Les référencements de nœuds automatiques peuvent ne fonctionner que si le nœud cible contient des LIFs de données qui sont activées uniquement pour le protocole NFS ou uniquement pour le protocole SMB.

Si cette exigence n'est pas respectée, l'accès aux données n'est pas affecté. Le client SMB mappe le partage à l'aide de la LIF d'origine que le client a utilisée pour se connecter à la SVM.

Exigences d'authentification NTLM lors de la connexion SMB référencée

L'authentification NTLM doit être autorisée sur le domaine contenant le serveur CIFS et sur les domaines contenant des clients qui souhaitent utiliser des référencements de nœud automatiques.

Lors d'une recommandation, le serveur SMB renvoie une adresse IP au client Windows. Étant donné que l'authentification NTLM est utilisée lors de la connexion à l'aide d'une adresse IP, l'authentification Kerberos n'est pas réalisée pour les connexions mentionnées.

Cela se produit car le client Windows ne peut pas créer le nom principal de service utilisé par Kerberos (qui est de la forme `service/NetBIOS name` et `service/FQDN`), ce qui signifie que le client ne peut pas demander un ticket Kerberos au service.

Instructions pour l'utilisation de renvois de nœuds automatiques avec la fonction home Directory

Lorsque les partages sont configurés avec la propriété de partage de répertoire personnel activée, il peut y avoir un ou plusieurs chemins de recherche de répertoire racine configurés pour une configuration de répertoire personnel. Les chemins de recherche peuvent pointer vers les volumes contenus dans chaque nœud contenant des volumes du SVM. Les clients reçoivent une recommandation et, si une LIF de données locale active est disponible, connectez-vous via une LIF référencée qui est locale au home Directory de l'utilisateur.

Il existe des directives lorsque les clients SMB 1.0 accèdent aux home directories dynamiques avec l'activation automatique des référencements de nœuds. En effet, les clients SMB 1.0 nécessitent le renvoi automatique de nœud avant d'avoir été authentifiés, c'est-à-dire avant que le serveur SMB ait le nom de l'utilisateur. Cependant, l'accès au répertoire local SMB fonctionne correctement pour les clients SMB 1.0 si les instructions suivantes sont vraies :

- Les répertoires locaux SMB sont configurés pour utiliser des noms simples, tels que "%W" (nom d'utilisateur Windows) ou "%u" (nom d'utilisateur UNIX mappé), et non des noms de style de nom de domaine, tels que "`%d\%W `" (nom-domaine\nom-utilisateur).
- Lors de la création de partages de répertoires locaux CIFS, les noms de partages de répertoire racine CIFS sont configurés avec des variables ("`%W"" ou "`%u""), et non avec des noms statiques, tels que ""HOME"".

Pour les clients SMB 2.x et SMB 3.0, il n'y a pas de directives spéciales lors de l'accès aux répertoires locaux en utilisant des référencements de nœuds automatiques.

Instructions relatives à la désactivation des référencements de nœuds automatiques sur les serveurs CIFS avec les connexions existantes désignées

Si vous désactivez les référencements de nœuds automatiques après l'activation de l'option, les clients actuellement connectés à une LIF référencée conservent la connexion référencée. Étant donné que ONTAP utilise les référencements DFS comme mécanisme pour les référencements automatiques des nœuds SMB,

les clients peuvent même se reconnecter au LIF référencé après que vous avez désactivé l'option jusqu'à ce que le renvoi DFS mis en cache du client pour les connexions mentionnées soit trop court. Cela est vrai même dans le cas d'une restauration vers une version de ONTAP qui ne prend pas en charge les référencements de nœuds automatiques. Les clients continuent d'utiliser les référencements jusqu'à ce que la référence DFS soit hors du cache du client.

La géolocalisation automatique utilise les référencements automatiques des nœuds SMB pour augmenter les performances des clients SMB en orientant les clients vers la LIF sur le nœud qui possède le volume de données d'un SVM. Lorsqu'un client SMB se connecte à un partage SMB hébergé sur un SVM, il peut se connecter à l'aide d'une LIF sur un nœud qui ne détient pas les données demandées et utilise un réseau d'interconnexion de cluster pour récupérer les données. Le client peut bénéficier de temps de réponse plus rapides si la connexion SMB utilise une LIF située sur le nœud contenant les données demandées.

ONTAP fournit cette fonctionnalité à l'aide des référencements DFS (système de fichiers distribués Microsoft) pour informer les clients SMB qu'un fichier ou dossier demandé dans l'espace de noms est hébergé quelque part. Un nœud fait une recommandation lorsqu'il détermine qu'il existe une LIF de SVM sur le nœud qui contient les données. Les renvois sont effectués en fonction de l'emplacement de la racine du partage auquel le client est connecté.

Le renvoi se produit pendant la négociation avec les PME. Le renvoi est effectué avant l'établissement de la connexion. Après que ONTAP désigne le client SMB au nœud cible, la connexion est établie et le client accède aux données via le chemin LIF référencé à partir de ce point. Les clients accèdent ainsi plus rapidement aux données et évitent toute communication supplémentaire avec le cluster.

Instructions pour l'utilisation de renvois de nœuds automatiques avec des clients Mac OS

Les clients Mac OS X ne prennent pas en charge les renvois de nœuds automatiques SMB, même si le système d'exploitation Mac prend en charge le système de fichiers distribué (DFS, Distributed File System) de Microsoft. Les clients Windows effectuent une demande de recommandation DFS avant de se connecter à un partage SMB. ONTAP fournit une référence à une LIF de données située sur le même nœud qui héberge les données requises, ce qui entraîne une amélioration des temps de réponse du client. Bien que le système d'exploitation Mac prend en charge DFS, les clients Mac OS ne se comportent pas exactement comme les clients Windows dans cette zone.

Informations associées

- En savoir plus sur l'activation des répertoires personnels dynamiques sur les serveurs
- "Gestion du réseau"
- "Matrice d'interopérabilité NetApp"

Prise en charge des références automatiques de nœuds ONTAP SMB

Avant d'activer les référencements automatiques des nœuds SMB, sachez que certaines fonctionnalités ONTAP ne prennent pas en charge les référencements.

- Les types de volumes suivants ne prennent pas en charge les référencements automatiques des nœuds SMB :
  - Membres en lecture seule d'un miroir de partage de charge
  - Volume de destination d'un miroir de protection des données
- Les référencements des nœuds ne bougent pas parallèlement à un déplacement LIF.

  Lorsqu'un client utilise une connexion référencée sur une connexion SMB 2.x ou SMB 3.0 et qu'une LIF de données se déplace sans interruption, le client continue d'utiliser la même connexion référencée, même si

la LIF n'est plus locale des données.

- Les référencements de nœuds ne se déplacent pas parallèlement à un déplacement des volumes.

  Lorsqu'un client utilise une connexion référencée sur une connexion SMB et qu'un déplacement de volume se produit, le client continue à utiliser la même connexion référencée, même si le volume n'est plus situé sur le même nœud que la LIF de données.

Activer ou désactiver les références automatiques de nœuds ONTAP SMB

Vous pouvez activer les référencements automatiques des nœuds SMB pour augmenter les performances d'accès des clients SMB. Vous pouvez désactiver les référencements automatiques des nœuds si vous ne souhaitez pas que ONTAP fait des référencements aux clients SMB.

Avant de commencer

Un serveur CIFS doit être configuré et exécuté sur la machine virtuelle de stockage (SVM).

Description de la tâche

La fonctionnalité de référencements automatiques des nœuds SMB est désactivée par défaut. Vous pouvez activer ou désactiver cette fonctionnalité sur chaque SVM si nécessaire.

Cette option est disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activez ou désactivez les référencements automatiques des nœuds SMB si nécessaire :

Si vous voulez que les référencements automatiques des nœuds SMB soient…	Saisissez la commande suivante…
Activé	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Désactivé	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   Le paramètre d'option prend effet pour les nouvelles sessions SMB. Les clients avec une connexion existante peuvent utiliser le renvoi de nœud uniquement lorsque leur expiration de délai de cache existant expire.

3. Basculer vers le niveau de privilège admin : `set -privilege admin`

Informations associées

Options de serveur disponibles

Utiliser les statistiques pour surveiller l'activité de référencement automatique des nœuds ONTAP SMB

Pour déterminer le nombre de connexions SMB mentionnées, vous pouvez surveiller

l'activité de renvoi automatique des nœuds à l'aide du `statistics` commande. En surveillant les référencements, vous pouvez déterminer dans quelle mesure les référencements automatiques localise des connexions sur des nœuds hébergeant les partages et si vous devez redistribuer vos LIFs de données pour fournir un meilleur accès local aux partages sur le serveur CIFS.

Description de la tâche

Le `cifs` Objet fournit plusieurs compteurs au niveau de privilèges avancés qui sont utiles lors du suivi des référencements automatiques des nœuds SMB :

- `node_referral_issued`

  Nombre de clients ayant été aiguillage vers le nœud racine du partage après que le client ait connecté via une LIF hébergée par un nœud différent du nœud racine du partage.

- `node_referral_local`

  Nombre de clients connectés via une LIF hébergée par le même nœud qui héberge la racine du partage. L'accès local offre généralement des performances optimales.

- `node_referral_not_possible`

  Nombre de clients qui n'ont pas été aiguillage vers le nœud hébergeant la racine du partage après connexion à une LIF hébergée par un nœud différent du nœud racine du partage. En effet, une LIF de données actives pour le nœud racine du partage n'a pas été trouvée.

- `node_referral_remote`

  Nombre de clients connectés via une LIF hébergée par un nœud différent du nœud qui héberge la racine du partage. L'accès à distance peut affecter les performances.

Vous pouvez surveiller les statistiques de référence automatique des nœuds sur votre SVM en collectant et en affichant les données d'une période donnée (échantillon). Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison peut vous aider à identifier les tendances en matière de performances.

Pour évaluer et utiliser les informations que vous recueillez à partir du `statistics` command, vous devez comprendre la distribution des clients dans vos environnements.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Afficher les statistiques de référence de nœud automatique à l'aide du `statistics` commande.

   Cet exemple affiche les statistiques d'aiguillage automatique des nœuds en recueillant et en visualisant les données d'une période d'échantillonnage :

   a. Lancez la collection : `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Attendez que le délai de collecte souhaité s'écoule.

c. Arrêter la collection : `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

En savoir plus sur `statistics start` et `statistics stop` dans le "Référence de commande ONTAP" .

d. Afficher les statistiques de référence automatique des nœuds : `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                                  Value
    ---------------------------- --------------------------
    node_name                                               node1
    node_referral_issued                                        0
    node_referral_local                                         1
    node_referral_not_possible                                  2
    node_referral_remote                                        2
    ...

    node_name                                               node2
    node_referral_issued                                        2
    node_referral_local                                         1
    node_referral_not_possible                                  0
    node_referral_remote                                        2
    ...
```

Le résultat affiche des compteurs pour tous les nœuds participant au SVM vs1. Pour plus de clarté, seuls les champs de sortie liés aux statistiques de renvoi automatique de nœud sont fournis dans l'exemple.

Pour en savoir plus, `statistics show` consultez le "Référence de commande ONTAP".

3. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

- Affiche les statistiques
- "Configuration du contrôle des performances"

Surveiller les informations de référence automatique des nœuds ONTAP SMB côté client à l'aide d'un client Windows

Pour déterminer les références faites du point de vue du client, vous pouvez utiliser Windows `dfsutil.exe` informatique.

Le kit Remote Server Administration Tools (RSAT) disponible avec les clients Windows 7 et versions ultérieures contient le `dfsutil.exe` informatique. Cet utilitaire vous permet d'afficher des informations sur le contenu du cache de référence ainsi que des informations sur chaque référence que le client utilise actuellement. Vous pouvez également utiliser l'utilitaire pour effacer le cache de référence du client. Pour plus d'informations, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Sécurité des dossiers sur les partages dotés d'une énumération basée sur l'accès

Fournir la sécurité des dossiers ONTAP SMB sur les partages avec une énumération basée sur l'accès

Lorsque l'énumération basée sur l'accès (ABE) est activée sur un partage SMB, les utilisateurs qui n'ont pas l'autorisation d'accéder à un dossier ou un fichier contenu dans le partage (que ce soit par le biais de restrictions d'autorisation individuelles ou de groupe) ne voient pas cette ressource partagée affichée dans leur environnement, bien que le partage lui-même reste visible.

Les propriétés de partage conventionnelles vous permettent de spécifier quels utilisateurs (individuellement ou en groupes) ont l'autorisation d'afficher ou de modifier les fichiers ou dossiers contenus dans le partage. Cependant, elles ne vous permettent pas de contrôler si les dossiers ou les fichiers contenus dans le partage sont visibles pour les utilisateurs qui ne disposent pas de l'autorisation d'y accéder. Cela peut poser des problèmes si les noms de ces dossiers ou fichiers dans le partage décrivent des informations sensibles, telles que les noms des clients ou des produits en cours de développement.

L'énumération basée sur l'accès (ABE) étend les propriétés de partage pour inclure l'énumération des fichiers et dossiers dans le partage. ABE vous permet donc de filtrer l'affichage des fichiers et dossiers dans le partage en fonction des droits d'accès des utilisateurs. C'est-à-dire que le partage lui-même est visible pour tous les utilisateurs, mais les fichiers et les dossiers du partage peuvent être affichés ou masqués par les utilisateurs désignés. En plus de protéger les informations sensibles sur votre lieu de travail, ABE vous permet de simplifier l'affichage de grandes structures de répertoires pour le bénéfice des utilisateurs qui n'ont pas besoin d'accéder à toute votre gamme de contenus. Par exemple, le partage lui-même est visible pour tous les utilisateurs, mais les fichiers et dossiers du partage peuvent être affichés ou masqués.

Découvrez "Impact sur les performances lors de l'utilisation d'une énumération basée sur SMB/CIFS".

Activer ou désactiver l'énumération basée sur l'accès sur les partages SMB ONTAP

Vous pouvez activer ou désactiver l'énumération basée sur l'accès (ABE) sur les partages SMB afin d'autoriser ou d'empêcher les utilisateurs de voir les ressources partagées qu'ils ne disposent pas des autorisations d'accès.

Description de la tâche

Par défaut, ABE est désactivé.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activer ABE sur un nouveau partage	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Vous pouvez spécifier des paramètres de partage facultatifs supplémentaires et des propriétés de partage supplémentaires lorsque vous créez un partage SMB. Pour en savoir plus, `vserver cifs share create` consultez le "Référence de commande ONTAP".
Activer ABE sur un partage existant	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Les propriétés de partage existantes sont conservées. La propriété partage ABE est ajoutée à la liste existante des propriétés de partage.
Désactivez ABE sur un partage existant	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Les autres propriétés de partage sont conservées. Seule la propriété partage ABE est supprimée de la liste des propriétés de partage.

2. Vérifiez que la configuration du partage est correcte à l'aide du `vserver cifs share show` commande.

Exemples

L'exemple suivant crée un partage ABE SMB nommé "sales" avec un chemin de `/sales` Sur la SVM vs1. Le partage est créé avec `access-based-enumeration` en tant que propriété de partage :

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

L'exemple suivant ajoute le `access-based-enumeration` Partagez la propriété dans un partage SMB nommé "data2":

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Informations associées

Ajouter ou supprimer des propriétés de partage sur des partages existants

Activer ou désactiver l'énumération basée sur l'accès à partir d'un client Windows sur les partages SMB ONTAP

Vous pouvez activer ou désactiver l'énumération basée sur l'accès (ABE) sur des partages SMB à partir d'un client Windows, ce qui vous permet de configurer ce paramètre de partage sans avoir à vous connecter au serveur CIFS.

Le `abecmd` Utilitaire non disponible dans les nouvelles versions de Windows Server et des clients Windows. Elle a été publiée dans le cadre de Windows Server 2008. Le support de Windows Server 2008 a pris fin le 14 janvier 2020.

Étapes

1. À partir d'un client Windows prenant en charge ABE, entrez la commande suivante : `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Pour plus d'informations sur le `abecmd` Consultez la documentation de votre client Windows.

Dépendances de nommage des fichiers et des répertoires NFS et SMB

En savoir plus sur les dépendances de nommage des fichiers et des répertoires ONTAP NFS et SMB

Les conventions d'appellation des fichiers et des répertoires dépendent à la fois des systèmes d'exploitation des clients réseau et des protocoles de partage de fichiers, en plus des paramètres de langue sur le cluster ONTAP et les clients.

Le système d'exploitation et les protocoles de partage de fichiers déterminent ce qui suit :

- Caractères un nom de fichier peut utiliser
- Sensibilité à la casse d'un nom de fichier

ONTAP prend en charge les caractères multi-octets dans les noms de fichier, de répertoire et de qtree, en fonction de la version de ONTAP utilisée.

En savoir plus sur les caractères valides pour les noms de fichiers ou de répertoires ONTAP SMB

Si vous accédez à un fichier ou à un répertoire à partir de clients ayant différents systèmes d'exploitation, vous devez utiliser des caractères valides dans les deux systèmes d'exploitation.

Par exemple, si vous utilisez UNIX pour créer un fichier ou un répertoire, n'utilisez pas de deux-points (:) dans le nom car le deux-points n'est pas autorisé dans les noms de fichiers ou de répertoires MS-DOS. Comme les restrictions sur les caractères valides varient d'un système d'exploitation à l'autre, consultez la documentation de votre système d'exploitation client pour plus d'informations sur les caractères interdits.

Sensibilité à la casse des noms de fichiers et de répertoires ONTAP SMB dans un environnement multiprotocole

Les noms de fichiers et de répertoires sont sensibles à la casse pour les clients NFS et non sensibles à la casse, mais ils préservent la casse pour les clients SMB. Vous devez comprendre les implications dans un environnement multiprotocole et les actions nécessaires lorsque vous spécifiez le chemin lors de la création des partages SMB et lors de l'accès aux données au sein des partages.

Si un client SMB crée un répertoire nommé `testdir`, Les clients SMB et NFS affichent le nom de fichier comme `testdir`. Toutefois, si un utilisateur SMB tente par la suite de créer un nom de répertoire `TESTDIR`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un répertoire nommé `TESTDIR`, Les clients NFS et SMB affichent le nom du répertoire différemment,

comme suit :

- Sur les clients NFS, vous voyez les deux noms de répertoire tels qu'ils ont été créés, par exemple `testdir` et `TESTDIR`, car les noms de répertoire sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour faire la distinction entre les deux répertoires. Un répertoire porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux répertoires supplémentaires.
  - Sur les clients SMB, vous voyez `testdir` et `TESTDI~1`.
  - ONTAP crée le `TESTDI~1` nom du répertoire pour différencier les deux répertoires.

    Dans ce cas, vous devez utiliser le nom 8.3 lorsque vous spécifiez un chemin de partage lors de la création ou de la modification d'un partage sur un SVM (Storage Virtual machine).

De la même manière pour les fichiers, si un client SMB crée `test.txt`, Les clients SMB et NFS affichent le nom de fichier comme `text.txt`. Toutefois, si un utilisateur SMB tente par la suite de le créer `Test.txt`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un fichier nommé `Test.txt`, Les clients NFS et SMB affichent le nom de fichier différemment, comme suit :

- Sur les clients NFS, les deux noms de fichiers sont ceux qu'ils ont créés, `test.txt` et `Test.txt`, car les noms de fichiers sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour distinguer les deux fichiers. Un fichier porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux fichiers supplémentaires.
  - Sur les clients SMB, vous voyez `test.txt` et `TEST~1.TXT`.
  - ONTAP crée le `TEST~1.TXT` nom de fichier pour différencier les deux fichiers.

> Si vous avez activé ou modifié le mappage de caractères à l'aide des commandes Vserver CIFS Character-mapping, une recherche Windows sensible à la casse devient normalement sensible à la casse.

En savoir plus sur la création de noms de fichiers et de répertoires ONTAP SMB

ONTAP crée et conserve deux noms pour les fichiers ou les répertoires de tout répertoire ayant accès à partir d'un client SMB : le nom long et le nom d'origine au format 8.3.

Pour les noms de fichier ou de répertoire dépassant le nom de huit caractères ou la limite d'extension de trois caractères (pour les fichiers), ONTAP génère un nom de format 8.3 comme suit :

- Il tronque le nom de fichier ou de répertoire d'origine à six caractères, si le nom dépasse six caractères.
- Il ajoute un tilde (~) et un nombre, un à cinq, aux noms de fichier ou de répertoire qui ne sont plus uniques après être tronqués.

  S'il manque des nombres parce qu'il y a plus de cinq noms similaires, il crée un nom unique qui n'a aucune relation avec le nom original.
- Dans le cas des fichiers, il tronque l'extension du nom de fichier à trois caractères.

Par exemple, si un client NFS crée un fichier nommé `specifications.html`, Le nom de fichier au format 8.3 créé par ONTAP est `specif~1.htm`. Si ce nom existe déjà, ONTAP utilise un numéro différent à la fin du nom du fichier. Par exemple, si un client NFS crée un autre fichier nommé `specifications_new.html`, le

format 8.3 de `specifications_new.html` est `specif~2.htm`.

En savoir plus sur les noms de fichiers, de répertoires et de qtree multi-octets ONTAP SMB

À partir de ONTAP 9.5, la prise en charge des noms codés UTF-8 de 4 octets permet la création et l'affichage des noms de fichier, de répertoire et d'arborescence qui incluent des caractères supplémentaires Unicode à l'extérieur du plan multilingue de base (BMP). Dans les versions précédentes, ces caractères supplémentaires ne s'affichent pas correctement dans les environnements multiprotocoles.

Pour activer la prise en charge des noms codés UTF-8 à 4 octets, un nouveau code de langue *utf8mb4* est disponible pour l' `vserver` et `volume` familles de commandement.

Vous devez créer un volume de l'une des manières suivantes :

- Réglage du volume `-language` explicitement option : `volume create -language utf8mb4 {…}`
- Hériter du volume `-language` Option d'un SVM qui a été créé avec ou modifié pour l'option : `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- Dans ONTAP 9.6 et les versions antérieures, vous ne pouvez pas modifier les volumes existants pour le support utf8mb4 ; vous devez créer un nouveau volume prêt pour utf8mb4, puis migrer les données à l'aide d'outils de copie basés sur le client.

  Vous pouvez mettre à jour les SVM pour la prise en charge de utf8mb4, mais les volumes existants conservent leurs codes de langue d'origine.

  Si vous utilisez ONTAP 9.7P1 ou une version ultérieure, vous pouvez modifier les volumes existants pour utf8mb4 avec une demande de support. Pour plus d'informations, voir "Est-il possible de modifier la langue du volume après sa création dans ONTAP ?".

- À partir de ONTAP 9.8, vous pouvez utiliser le `[-language <Language code>]` Paramètre permettant de changer le langage de volume de *.UTF-8 à utf8mb4. Pour modifier la langue d'un volume, contactez "Support NetApp".

> Les noms de LUN portant des caractères UTF-8 de 4 octets ne sont pas pris en charge actuellement.

- Les données de caractères Unicode sont généralement représentées dans les applications de systèmes de fichiers Windows utilisant le format de transformation Unicode 16 bits (UTF-16) et dans les systèmes de fichiers NFS utilisant le format de transformation Unicode 8 bits (UTF-8).

  Dans les versions antérieures à ONTAP 9.5, les noms, y compris les caractères supplémentaires UTF-16 créés par les clients Windows, étaient correctement affichés sur d'autres clients Windows mais n'étaient pas traduits correctement en UTF-8 pour les clients NFS. De même, les noms comportant des caractères supplémentaires UTF-8 par les clients NFS créés n'ont pas été correctement traduits en UTF-16 pour les clients Windows.

- Lorsque vous créez des noms de fichier sur des systèmes exécutant ONTAP 9.4 ou une version antérieure contenant des caractères supplémentaires valides ou non valides, ONTAP rejette le nom de fichier et renvoie une erreur de nom de fichier non valide.

  Pour éviter ce problème, utilisez uniquement des caractères BMP dans les noms de fichiers et évitez d'utiliser des caractères supplémentaires, ou mettez à niveau vers ONTAP 9.5 ou version ultérieure.

À partir de ONTAP 9, les caractères Unicode sont autorisés dans les noms de qtree.

- Vous pouvez utiliser le `volume qtree` Famille de commandes ou System Manager pour définir ou modifier les noms des qtree.
- Les noms des qtrees peuvent inclure des caractères multi-octets au format Unicode, comme les caractères japonais et chinois.
- Dans les versions antérieures à ONTAP 9.5, seuls les caractères BMP (c'est-à-dire ceux qui pouvaient être représentés en 3 octets) étaient pris en charge.

> Dans les versions antérieures à ONTAP 9.5, le Junction-path du volume parent du qtree peut contenir des noms de qtree et de répertoire avec des caractères Unicode. Le `volume show` La commande affiche ces noms correctement lorsque le volume parent a un paramètre de langue UTF-8. Cependant, si la langue du volume parent n'est pas l'un des paramètres de langue UTF-8, certaines parties du chemin de jonction sont affichées à l'aide d'un nom de remplacement NFS numérique.

- Dans les versions 9.5 et ultérieures, les noms des qtree prennent en charge des caractères de 4 octets, à condition que le qtree se trouve dans un volume activé pour utf8m4.

Configurer le mappage de caractères pour la traduction des noms de fichiers ONTAP SMB sur les volumes

Les clients NFS peuvent créer des noms de fichiers contenant des caractères non valides pour les clients SMB et certaines applications Windows. Vous pouvez configurer le mappage de caractères pour la conversion de noms de fichiers sur des volumes pour permettre aux clients SMB d'accéder aux fichiers avec des noms NFS qui ne seraient autrement pas valides.

Description de la tâche

Lorsque les fichiers créés par des clients NFS sont accessibles par des clients SMB, ONTAP recherche le nom du fichier. Si le nom n'est pas un nom de fichier SMB valide (par exemple, s'il comporte un caractère «`:`") inclus, ONTAP renvoie le nom de fichier 8.3 qui est conservé pour chaque fichier. Cependant, cela cause des problèmes pour les applications qui codent des informations importantes dans des noms de fichiers longs.

Par conséquent, si vous partagez un fichier entre des clients sur des systèmes d'exploitation différents, vous devez utiliser des caractères dans les noms de fichiers valides dans les deux systèmes d'exploitation.

Cependant, si vous avez des clients NFS qui créent des noms de fichier contenant des caractères qui ne sont pas des noms de fichier valides pour les clients SMB, vous pouvez définir une carte qui convertit les caractères NFS non valides en caractères Unicode acceptés par SMB et certaines applications Windows. Par exemple, cette fonctionnalité prend en charge les applications CATIA MCAD et Mathematica, ainsi que d'autres applications qui ont cette exigence.

Vous pouvez configurer le mappage de caractères sur une base volume par volume.

Lors de la configuration du mappage de caractères sur un volume, vous devez garder à l'esprit les éléments suivants :

- Le mappage de caractères n'est pas appliqué à travers les points de jonction.

  Vous devez configurer explicitement le mappage de caractères pour chaque volume de jonction.

- Vous devez vous assurer que les caractères Unicode utilisés pour représenter des caractères non valides ou illégaux sont des caractères qui n'apparaissent normalement pas dans les noms de fichiers ; sinon, des mappages indésirables se produisent.

  Par exemple, si vous essayez de mapper un deux-points (:) à un tiret (-) mais que le tiret (-) a été utilisé correctement dans le nom de fichier, un client Windows essayant d'accéder à un fichier nommé ""a-b" aurait sa demande mappée au nom NFS de ""a:b" (pas le résultat souhaité).

- Après l'application du mappage de caractères, si le mappage contient toujours un caractère Windows non valide, ONTAP revient aux noms de fichier Windows 8.3.
- Dans les notifications FPolicy, les journaux d'audit NAS et les messages de suivi de sécurité, les noms de fichiers mappés sont affichés.
- Lors de la création d'une relation SnapMirror de type DP, le mappage de caractères du volume source n'est pas répliqué sur le volume DP de destination.
- Sensibilité à la casse : comme les noms Windows mappés se transforment en noms NFS, la recherche des noms suit la sémantique NFS. Ainsi, les recherches NFS sont sensibles à la casse. Cela signifie que les applications qui accèdent aux partages mappés ne doivent pas se fier au comportement non sensible à la casse de Windows. Cependant, le nom 8.3 est disponible, et cela n'est pas sensible à la casse.
- Mappages partiels ou non valides : après le mappage d'un nom pour revenir aux clients faisant une énumération de répertoire (« dir »), le nom Unicode obtenu est vérifié pour la validité de Windows. Si ce nom contient toujours des caractères non valides ou s'il n'est pas valide pour Windows (par exemple, il se termine par "." ou vierge), le nom 8.3 est renvoyé à la place du nom non valide.

Étape

1. Configurer le mappage de caractères : +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

Le mappage se compose d'une liste de paires de caractères source-cible séparées par «»:». Les caractères sont des caractères Unicode saisis à l'aide de chiffres hexadécimaux. Par exemple : 3C:E03C. +

La première valeur de chaque `mapping_text` La paire séparée par deux-points est la valeur hexadécimale du caractère NFS que vous souhaitez traduire, et la seconde est la valeur Unicode utilisée par SMB. Les paires de mappage doivent être uniques (un mappage un-à-un doit exister).

- Mappage de source +

Le tableau suivant montre le jeu de caractères Unicode autorisé pour le mappage de source :

+

Caractère Unicode	Caractère imprimé	Description
0x01-0x19	Sans objet	Caractères de contrôle sans impression
0x5C		Barre oblique inversée
0x3A	:	Deux-points

Caractère Unicode	Caractère imprimé	Description
0x2A	*	Astérisque
0x3F	?	Point d'interrogation
0x22	«	Devis
0x3C	<	Inférieur à
0x3E	>	Supérieur à
0x7C		
Ligne verticale	0xb1	±

- Mappage de cible

  Vous pouvez spécifier des caractères cibles dans la « zone d'utilisation privée » d'Unicode dans la plage suivante : U+E0000…U+F8FF.

Exemple

La commande suivante crée un mappage de caractères pour un volume nommé « `dates' » sur la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Informations associées

En savoir plus sur la création et la gestion des volumes de données dans les espaces de noms

Commandes ONTAP pour la gestion des mappages de caractères pour la traduction des noms de fichiers SMB

Vous pouvez gérer le mappage de caractères en créant, en modifiant, en affichant des informations sur et en supprimant des mappages de caractères de fichiers utilisés pour la conversion de noms de fichiers SMB sur des volumes FlexVol.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer de nouveaux mappages de caractères de fichier	`vserver cifs character-mapping create`
Affiche des informations sur les mappages de caractères de fichier	`vserver cifs character-mapping show`
Modifier les mappages de caractères de fichier existants	`vserver cifs character-mapping modify`
Supprimer les mappages de caractères de fichier	`vserver cifs character-mapping delete`

Pour en savoir plus, `vserver cifs character-mapping` consultez le "Référence de commande ONTAP".

Informations associées

Configurer le mappage de caractères pour la traduction des noms de fichiers sur les volumes

Offrez un accès client S3 aux données NAS

En savoir plus sur la prise en charge multiprotocole ONTAP S3

Depuis ONTAP 9.12.1, vous pouvez activer les clients exécutant le protocole S3 pour accéder aux données qui sont servies aux clients qui utilisent les protocoles NFS et SMB sans nouveau formatage. Ainsi, les données NAS peuvent continuer à être servies aux clients NAS, tout en présentant les données d'objet aux clients S3 qui exécutent des applications S3 (par exemple, le data mining et l'intelligence artificielle).

La fonctionnalité multiprotocole S3 répond à deux cas d'utilisation :

1. Accès aux données NAS existantes à l'aide de clients S3

   Si vos données existantes ont été créées à l'aide de clients NAS traditionnels (NFS ou SMB) et se trouvent sur des volumes NAS (volumes FlexVol ou FlexGroup), vous pouvez utiliser des outils d'analyse sur les clients S3 pour accéder à ces données.

2. Stockage back-end pour les clients modernes capables d'exécuter des E/S avec les protocoles NAS et S3

   Vous pouvez fournir un accès intégré pour des applications telles que Spark et Kafka qui peuvent lire et écrire les mêmes données à l'aide des protocoles NAS et S3.

Fonctionnement de la prise en charge multiprotocole S3

La prise en charge multiprotocole de ONTAP vous permet de présenter le même jeu de données sous la forme d'une hiérarchie de fichiers ou d'objets dans un compartiment. Pour ce faire, ONTAP crée des « compartiments NAS S3 » qui permettent aux clients S3 de créer, lire, supprimer et énumérer des fichiers dans le stockage NAS à l'aide de requêtes d'objets S3. Ce mappage est conforme à la configuration de sécurité NAS, en observant les autorisations d'accès aux fichiers et aux répertoires ainsi qu'en écrivant dans la piste d'audit de sécurité si nécessaire.

Ce mappage est effectué en présentant une hiérarchie de répertoires NAS spécifiée comme un compartiment S3. Chaque fichier de la hiérarchie de répertoires est représenté comme un objet S3 dont le nom est relatif à partir du répertoire mappé vers le bas, avec des limites de répertoire représentées par le caractère de barre oblique ('/').

Les utilisateurs ONTAP-Defined S3 peuvent accéder à ce stockage, tel que régi par les politiques de compartiment définies pour le compartiment qui correspond au répertoire NAS. Pour que cela soit possible, des mappages doivent être définis entre les utilisateurs S3 et SMB/NFS. Les informations d'identification de l'utilisateur SMB/NFS seront utilisées pour la vérification des autorisations NAS et incluses dans tous les enregistrements d'audit résultant de ces accès.

Lorsqu'un fichier est créé par des clients SMB ou NFS, il est immédiatement placé dans un répertoire, et donc visible aux clients, avant l'écriture des données. Les clients S3 s'attendent à une sémantique différente, où le nouvel objet n'est pas visible dans le namespace tant que toutes ses données n'ont pas été écrites. Le mappage de S3 sur le stockage NAS crée des fichiers avec la sémantique S3, afin de rendre les fichiers invisibles en externe jusqu'à la fin de la commande de création S3.

Protection des données par compartiments NAS S3

Les « compartiments » NAS S3 sont simplement des mappages des données NAS pour les clients S3, ils ne sont pas des compartiments S3 standard. Par conséquent, il n'est pas nécessaire de protéger les compartiments NAS S3 à l'aide de la fonctionnalité NetApp SnapMirror S3. À la place, vous pouvez protéger les volumes contenant des compartiments NAS S3 à l'aide de la réplication asynchrone de volume SnapMirror. La fonction SnapMirror synchrone et la reprise d'activité SVM ne sont pas prises en charge.

À partir de ONTAP 9.14.1, les compartiments NAS S3 sont pris en charge dans les agrégats en miroir et sans miroir pour les configurations MetroCluster IP et FC.

En savoir plus sur "Réplication asynchrone SnapMirror".

Audit des compartiments NAS S3

Les compartiments NAS S3 ne sont pas des compartiments S3 classiques. L'audit S3 ne peut donc pas être configuré pour l'audit de l'accès. En savoir plus sur "Audit S3".

Cependant, les fichiers et les répertoires NAS mappés dans des compartiments NAS S3 peuvent être audités pour les événements d'accès à l'aide de procédures d'audit ONTAP conventionnelles. Les opérations S3 peuvent ainsi déclencher des événements d'audit NAS, à l'exception de ce qui suit :

- Si l'accès client S3 est refusé par la configuration de la règle S3 (groupe ou règle de compartiment), l'audit NAS pour l'événement n'est pas lancé. En effet, les autorisations S3 sont vérifiées avant la vérification des audits des SVM.
- Si le fichier cible d'une requête GET S3 est de taille 0, le contenu 0 est renvoyé à la demande GET et l'accès en lecture n'est pas consigné.
- Si le fichier cible d'une requête GET S3 se trouve dans un dossier pour lequel l'utilisateur n'a pas d'autorisation « traverse », la tentative d'accès échoue et l'événement n'est pas enregistré.

Découvrez "Audit des événements NAS sur les SVM".

Téléchargement partitionné des objets

À partir de ONTAP 9.16.1, le téléchargement partitionné des objets est pris en charge dans les compartiments NAS S3 lorsque "équilibrage avancé de la capacité" est activé sur le volume FlexGroup sous-jacent.

Le téléchargement partitionné des objets sur le stockage de fichiers NAS permet à un client protocole S3 de télécharger un objet volumineux en tant que parties plus petites. Le téléchargement partitionné des objets présente les avantages suivants :

- Il permet de télécharger des objets en parallèle.
- En cas d'échec du téléchargement ou de pause, seules les pièces qui n'ont pas encore été téléchargées devront être téléchargées. Le téléchargement de l'objet entier n'a pas besoin d'être redémarré.
- Si la taille de l'objet n'est pas connue à l'avance (par exemple, lorsqu'un objet volumineux est toujours en cours d'écriture), les clients peuvent commencer à télécharger immédiatement des parties de l'objet et terminer le téléchargement après la création de l'objet entier.

> Les objets à plusieurs pièces dans les compartiments NAS S3 doivent être alignés dans des tailles de pièce de 1 Mo. Par exemple, une pièce peut être de 4 Mo ou 4 Go ou d'une taille similaire. Une pièce ne peut pas utiliser des tailles de sous-Mo, telles que 4,5 Mo ou 4000,5 Mo.

Le téléchargement partitionné prend en charge les actions S3 suivantes :

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (à partir de ONTAP 9.17.1)
- CreateMultipartUpload

  À partir d' ONTAP 9.17.1, CreateMultipartUpload prend en charge le balisage et les paires clé/valeur de métadonnées utilisateur.

- ListMultipartUpload
- UploadPart

> L'OPTION OBTENIR par référence (« Numéro de pièce=xx ») n'est pas prise en charge dans les compartiments NAS S3. L'objet complet sera renvoyé à la place.

Interopérabilité S3 et NAS

Sauf mention contraire, les compartiments NAS ONTAP S3 prennent en charge les fonctionnalités NAS standard et S3.

La fonctionnalité NAS n'est pas prise en charge par les compartiments NAS S3

Un niveau de capacité FabricPool

Les compartiments NAS S3 ne peuvent pas être configurés en tant que Tier de capacité pour FabricPool.

Les actions et fonctionnalités S3 ne sont pas prises en charge par les compartiments NAS S3 pour le moment

Actions

- ByPassGovernanceRetention
- DeleteBuckeLifecycleConfiguration
- GetBucketLifecycleConfiguration
- GetBucketObjectLockConfiguration
- GetBucketVersioning

- GetObjectRetention
- ListBucketVersioning
- ListObjectVersions
- PutBucketLifecycleConfiguration
- PutBuckeVersioning
- PutObjectLockConfiguration
- PutObjectRetention

Ces actions S3 ne sont pas prises en charge spécifiquement lors de l'utilisation de S3 dans des compartiments NAS S3. Lors de l'utilisation de compartiments S3 natifs, ces actions sont "pris en charge normalement".

Métadonnées d'utilisateur AWS

- À partir d' ONTAP 9.17.1, prise en charge des métadonnées avec des objets en plusieurs parties.
- À partir d' ONTAP 9.16.1, prise en charge des métadonnées avec des objets à art unique.
- Pour ONTAP 9.15.1 et les versions antérieures, les paires de valeurs clés reçues dans le cadre des métadonnées utilisateur S3 ne sont pas stockées sur le disque avec les données d'objet.
- Pour ONTAP 9.15.1 et les versions antérieures, les en-têtes de requête avec le préfixe "x-amz-meta" sont ignorés.

Balises AWS

- À partir d' ONTAP 9.17.1, prise en charge des balises avec des objets en plusieurs parties.
- À partir d' ONTAP 9.16.1, prise en charge des balises avec des objets à art unique.
- Pour ONTAP 9.15.1 et les versions antérieures sur les requêtes PUT object et Multipart Initiate, les en-têtes avec le préfixe « x-amz-tagging » sont ignorés.
- Pour ONTAP 9.15.1 et les versions antérieures, les demandes de mise à jour des balises sur un fichier existant (put, GET et Delete requetes with the ?tagging query-string) sont rejetées avec une erreur.

Gestion des versions

Il n'est pas possible de spécifier la gestion des versions dans la configuration du mappage des compartiments.

- Les demandes qui incluent des spécifications de version non nulles (versionID=xyz query-string) reçoivent des réponses d'erreur.
- Les demandes visant à affecter l'état de gestion des versions d'un compartiment sont rejetées avec des erreurs.

En savoir plus sur les exigences de données NAS pour l'accès client ONTAP S3

Il est important de comprendre qu'il existe des incompatibilités inhérentes lors du mappage des fichiers NAS et des répertoires pour l'accès S3. Il peut être nécessaire d'ajuster la hiérarchie des fichiers NAS avant de les transférer à l'aide de compartiments NAS S3.

Un compartiment NAS S3 fournit un accès S3 à un répertoire NAS en effectuant le mappage de ce répertoire à l'aide de la syntaxe du compartiment S3, et les fichiers de l'arborescence sont considérés comme des objets.

Les noms d'objet sont les chemins d'accès délimités par des barres obliques des fichiers par rapport au répertoire spécifié dans la configuration du compartiment S3.

Ce mappage impose une certaine exigence lorsque les fichiers et les répertoires sont gérés à l'aide de compartiments NAS S3 :

- Les noms S3 sont limités à 1024 octets. Les fichiers dont les chemins d'accès sont plus longs ne sont donc pas accessibles via S3.
- Les noms de fichiers et de répertoires sont limités à 255 caractères, de sorte qu'un nom d'objet ne peut pas comporter plus de 255 caractères consécutifs non-slash ('/')
- Un chemin SMB délimité par des caractères de barre oblique inverse («\') apparaîtra à s3 comme un nom d'objet contenant des caractères de barre oblique («/ »).
- Certaines paires de noms d'objets S3 légaux ne peuvent pas coexister dans l'arborescence de répertoires NAS mappée. Par exemple, les noms d'objet S3 légal "part1/part2" et "part1/part2/part3" correspondent à des fichiers qui ne peuvent pas exister simultanément dans l'arborescence du répertoire NAS, "part1/part2" étant un fichier du premier nom et un répertoire de l'autre.
  - Si "part1/part2" est un fichier existant, la création S3 de "part1/part2/part3" échouera.
  - Si "part1/part2/part3" est un fichier existant, la création ou la suppression S3 de "part1/part2" échouera.
  - La création d'objet S3 correspondant au nom d'un objet existant remplace l'objet existant (dans des compartiments sans version). La gestion est assurée dans le NAS, mais la correspondance est obligatoire. Les exemples ci-dessus ne peuvent pas entraîner la suppression de l'objet existant car les noms entrent en collision et ne correspondent pas.

Alors qu'un magasin d'objets est conçu pour prendre en charge un grand nombre de noms arbitraires, une structure d'annuaire NAS peut rencontrer des problèmes de performance si un très grand nombre de noms sont placés dans un répertoire. En particulier, les noms sans barre oblique ('/') dans ces caractères seront tous placés dans le répertoire racine du mappage NAS. Les applications qui utilisent de manière intensive les noms qui ne sont pas « compatibles avec le NAS » seraient mieux hébergées dans un compartiment de magasin d'objets réel plutôt que dans un mappage NAS.

Activer l'accès au protocole S3 aux données NAS sur une SVM ONTAP

L'activation de l'accès au protocole S3 consiste à s'assurer qu'un SVM compatible avec NAS répond aux mêmes exigences qu'un serveur compatible S3, notamment l'ajout d'un serveur de magasin d'objets et la vérification des exigences en matière de réseau et d'authentification.

Pour les nouvelles installations ONTAP, il est recommandé d'activer l'accès par le protocole S3 à un SVM après sa configuration afin d'assurer le service des données NAS aux clients. Pour en savoir plus sur la configuration du protocole NAS, voir :

- "Configuration NFS"
- "Configuration SMB"

Avant de commencer

Les éléments suivants doivent être configurés avant d'activer le protocole S3 :

- Les licences existent pour le protocole S3 et les protocoles NAS souhaités (NFS, SMB ou les deux).
- Un SVM est configuré pour les protocoles NAS souhaités.

- Les serveurs NFS et/ou SMB existent.
- DNS et tous les autres services requis sont configurés.
- Les données NAS sont exportées ou partagées vers les systèmes clients.

Description de la tâche

Un certificat d'autorité de certification (CA) est nécessaire pour activer le trafic HTTPS des clients S3 vers le SVM compatible avec S3. Les certificats CA provenant de trois sources peuvent être utilisés :

- Nouveau certificat auto-signé ONTAP sur le SVM.
- Certificat ONTAP signé automatiquement sur le SVM.
- Un certificat tiers.

Vous pouvez utiliser les mêmes LIF de données pour le compartiment S3/NAS que pour le service des données NAS. Si des adresses IP spécifiques sont requises, reportez-vous à la section "Création de LIF de données". Une règle de données de service S3 est nécessaire pour activer le trafic de données S3 sur les LIF. Vous pouvez modifier la règle de service existante de la SVM afin d'inclure S3.

Lorsque vous créez le serveur objet S3, vous devez préparer le nom du serveur S3 en tant que nom de domaine complet (FQDN) que les clients utiliseront pour l'accès S3. Le FQDN du serveur S3 ne doit pas commencer par un nom de compartiment.

System Manager

1. Activez S3 sur une machine virtuelle de stockage avec les protocoles NAS configurés.
   a. Cliquez sur **stockage > Storage VMs**, sélectionnez une VM de stockage compatible NAS, cliquez sur Paramètres, puis cliquez sous S3.
   b. Sélectionnez le type de certificat. Que vous sélectionniez un certificat généré par le système ou l'un de vos propres certificats, il sera nécessaire d'accéder au client.
   c. Saisissez les interfaces réseau.
2. Si vous avez sélectionné le certificat généré par le système, les informations de certificat s'affichent lorsque la création de la nouvelle machine virtuelle de stockage est confirmée. Cliquez sur **Download** et enregistrez-le pour accéder au client.
   - La clé secrète ne s'affiche plus.
   - Si vous avez besoin de nouveau des informations de certificat : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.

CLI

1. Vérifier que le protocole S3 est autorisé sur la SVM :
   `vserver show -fields allowed-protocols`
2. Enregistrer le certificat de clé publique pour ce SVM.
   Si vous avez besoin d'un nouveau certificat auto-signé ONTAP, reportez-vous à la section "Créer et installer un certificat d'autorité de certification sur le SVM".
3. Mettre à jour la stratégie de données de service
   a. Afficher la politique de données de service pour la SVM
      `network interface service-policy show -vserver svm_name`

      Pour en savoir plus, `network interface service-policy show` consultez le "Référence de commande ONTAP".

   b. Ajoutez le `data-core` et `data-s3-server services` s'ils ne sont pas présents.
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. Vérifier que les LIF de données du SVM répondent à vos exigences :
   `network interface show -vserver svm_name`

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

5. Création du serveur S3 :
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Vous pouvez spécifier des options supplémentaires lors de la création du serveur S3 ou à tout moment ultérieurement.

- HTTPS est activé par défaut sur le port 443. Vous pouvez modifier le numéro de port à l'aide de l'option -Secure-Listener-port.
  Lorsque HTTPS est activé, des certificats CA sont requis pour une intégration correcte avec

SSL/TLS. À partir de ONTAP 9.15.1, TLS 1.3 est pris en charge avec le stockage objet S3.

- HTTP est désactivé par défaut ; lorsqu'il est activé, le serveur écoute le port 80. Vous pouvez l'activer avec l'option -is-http-enabled ou modifier le numéro de port avec l'option -port d'écoute.
  Lorsque HTTP est activé, toutes les demandes et réponses sont envoyées en clair sur le réseau.

1. Vérifiez que S3 est configuré comme vous le souhaitez :
   `vserver object-store-server show`

Exemple
La commande suivante vérifie les valeurs de configuration de tous les serveurs de stockage objet :
`cluster1::> vserver object-store-server show`

```
Vserver: vs1

                     Object Store Server Name: s3.example.com
                         Administrative State: up
                       Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
            Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Informations associées

- "service d'ajout de stratégie de service d'interface réseau"

Créer un bucket NAS ONTAP S3

Un bucket NAS S3 est un mappage entre un nom de bucket S3 et un chemin NAS. Les buckets NAS S3 permettent de fournir un accès S3 à toute partie d'un espace de noms SVM contenant des volumes et une structure de répertoires existants.

Avant de commencer

- Un serveur d'objets S3 est configuré dans une SVM contenant des données NAS.
- Les données NAS sont conformes à la "Exigences en matière d'accès client S3".

Description de la tâche

Vous pouvez configurer les compartiments NAS S3 pour spécifier tout ensemble de fichiers et de répertoires dans le répertoire racine de la SVM.

Vous pouvez également définir des règles de compartiment qui permettent ou non l'accès aux données NAS selon n'importe quelle combinaison de ces paramètres :

- Fichiers et répertoires
- Autorisations utilisateur et groupe
- Opérations S3

Il peut par exemple s'avérer nécessaire de définir des règles de compartiment distinctes pour accorder l'accès aux données en lecture seule à un grand groupe d'utilisateurs, tandis qu'un groupe limité peut effectuer des opérations sur un sous-ensemble de ces données.

À partir d' ONTAP 9.17.1, vous pouvez lier directement un bucket NAS S3 à un volume plutôt qu'au chemin de jonction. Par défaut, un bucket S3 sur un volume NAS est associé à un chemin de jonction, qui peut être modifié à tout moment par un administrateur ONTAP . Ces modifications peuvent perturber le fonctionnement du bucket S3. À partir d' ONTAP 9.17.1, vous pouvez utiliser l'option `-is-nas-path-mutable false` option avec le `vserver object-store-server bucket create` Commande dans l'interface de ligne de commande ONTAP pour permettre la liaison du compartiment NAS S3 à un volume. Par défaut, `-is-nas-path-mutable` est réglé sur `true` .

Étant donné que les « buckets » NAS S3 sont des mappages et non des buckets S3, les propriétés suivantes des buckets S3 standard ne s'appliquent pas aux buckets NAS S3.

- **aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-group**
  Aucun volume ou qtree n'est créé lors de la configuration des compartiments NAS S3.
- **role \ is -protected \ is -protected-on-ontap \ is -protected-on-cloud** + Les buckets NAS S3 ne sont pas protégés ou mis en miroir à l'aide de SnapMirror S3, mais utilisent plutôt la protection SnapMirror standard disponible à la granularité du volume.
- **Versionnage-state** + les volumes NAS disposent généralement de la technologie snapshot permettant d'enregistrer différentes versions. Cependant, la gestion de version n'est pas disponible dans les compartiments NAS S3.
- **utilisation logique \ nombre-objets**
  Des statistiques équivalentes sont disponibles pour les volumes NAS via les commandes de volume.
- **objets multiparties** + À partir d' ONTAP 9.16.1, les objets multiparties sont pris en charge dans les buckets NAS S3 lorsque "équilibrage avancé de la capacité" est activé sur le volume FlexGroup sous-jacent. L'équilibrage de capacité avancé ne peut être activé que sur les volumes FlexGroup . Il ne peut pas être activé sur les volumes FlexVol .

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP pour créer un bucket NAS.

System Manager

Ajoutez un nouveau compartiment NAS S3 sur une machine virtuelle de stockage compatible NAS.

1. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
2. Entrez un nom pour le compartiment NAS S3 et sélectionnez la machine virtuelle de stockage, ne saisissez pas de taille, puis cliquez sur **plus d'options**.
3. Entrez un nom de chemin d'accès valide ou cliquez sur Parcourir pour le sélectionner dans une liste de noms de chemin valides.
   Lorsque vous entrez un chemin d'accès valide, les options qui ne sont pas pertinentes pour la configuration du NAS S3 sont masquées.
4. Si vous avez déjà mappé des utilisateurs S3 aux utilisateurs NAS et aux groupes créés, vous pouvez configurer leurs autorisations, puis cliquez sur **Enregistrer**.
   Vous devez avoir déjà mappé des utilisateurs S3 à des utilisateurs NAS avant de configurer les autorisations de cette étape.

Sinon, cliquez sur **Save** pour terminer la configuration du compartiment NAS S3.

CLI

1. Créez un bucket NAS S3 dans une SVM contenant des systèmes de fichiers NAS.
   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
   true|false [-comment <text>]
   ```

   Exemple 1 : Créer un bucket NAS S3

   ```
   cluster1::> vserver object-store-server bucket create -bucket testbucket
   -type nas -path /vol1
   ```

   Exemple 2 : créer un bucket NAS S3 et lier le bucket à un volume

   ```
   vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
   -type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
   ```

Activer les utilisateurs du client ONTAP S3

Pour permettre aux utilisateurs du client S3 d'accéder aux données NAS, vous devez mapper les noms d'utilisateur S3 aux utilisateurs NAS correspondants, puis leur accorder l'autorisation d'accéder aux données NAS à l'aide des stratégies de service de compartiment.

Avant de commencer

Les noms d'utilisateur pour l'accès client (utilisateurs clients LINUX/UNIX, Windows et S3) doivent déjà exister.

Notez que certaines fonctionnalités de S3 sont "Non pris en charge par les compartiments NAS S3".

Description de la tâche

Le mappage d'un nom d'utilisateur S3 avec un utilisateur LINUX/UNIX ou Windows correspondant permet de vérifier les autorisations sur les fichiers NAS qui doivent être honorés lors de l'accès à ces fichiers par des

clients S3. Les mappages S3 vers NAS sont spécifiés en fournissant un nom d'utilisateur S3 *Pattern*, qui peut être exprimé sous la forme d'un nom unique ou d'une expression régulière POSIX, et un nom d'utilisateur LINUX/UNIX ou Windows *Replace*.

En l'absence de mappage de nom, le mappage de nom par défaut sera utilisé, où le nom d'utilisateur S3 lui-même sera utilisé comme nom d'utilisateur UNIX et nom d'utilisateur Windows. Vous pouvez modifier les mappages de noms d'utilisateur UNIX et Windows par défaut avec l' `vserver object-store-server modify` commande.

Seule la configuration locale de mappage de noms est prise en charge ; LDAP n'est pas prise en charge.

Une fois que les utilisateurs S3 sont mappés aux utilisateurs NAS, vous pouvez accorder des autorisations aux utilisateurs spécifiant les ressources (répertoires et fichiers) auxquelles ils ont accès et les actions qu'ils sont autorisés ou non à y effectuer.

System Manager

1. Créez des mappages de noms locaux pour les clients UNIX ou Windows (ou les deux).
   a. Cliquez sur **stockage > compartiments**, puis sélectionnez la machine virtuelle de stockage compatible S3/NAS.
   b. Sélectionnez **Paramètres**, puis cliquez sur → **mappage de noms** (sous **utilisateurs et groupes hôtes**).
   c. Dans les mosaïques **S3 à Windows** ou **S3 à UNIX** (ou les deux), cliquez sur **Ajouter**, puis entrez les noms d'utilisateur **Pattern** (S3) et **Replacement** (NAS) souhaités.
2. Création d'une politique de compartiment pour fournir un accès client
   a. Cliquez sur **stockage > compartiments**, cliquez sur ⋮ en regard du compartiment S3 souhaité, puis cliquez sur **Modifier**.
   b. Cliquez sur **Ajouter** et indiquez les valeurs souhaitées.
      - **Principal** - fournir des noms d'utilisateur S3 ou utiliser la valeur par défaut (tous les utilisateurs).
      - **Effet** - sélectionnez **Autoriser** ou **refuser**.
      - **Actions** - Entrez des actions pour ces utilisateurs et ressources. L'ensemble des opérations de ressources que le serveur de magasin d'objets prend actuellement en charge pour les compartiments NAS S3 sont : GetObject, PutObject, DeleteObject, ListBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBuckeLocation, GetBucketVersioning, PutBuckeVersioning et ListBuckeVersions. Les caractères génériques sont acceptés pour ce paramètre.
      - **Ressources** - Entrez les chemins de dossier ou de fichier dans lesquels les actions sont autorisées ou refusées, ou utilisez les valeurs par défaut (répertoire racine du compartiment).

CLI

1. Créez des mappages de noms locaux pour les clients UNIX ou Windows (ou les deux).
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - numéro de priorité pour l'évaluation de la cartographie; saisissez 1 ou 2.
   - `-pattern` - Un nom d'utilisateur S3 ou une expression régulière
   - `-replacement` - un nom d'utilisateur windows ou unix

Exemples

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. Création d'une politique de compartiment pour fournir un accès client
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - indique si l'accès est autorisé ou refusé lorsqu'un utilisateur demande une action.

- `-action <Action>, …` - indique les opérations de ressources autorisées ou refusées. L'ensemble des opérations de ressources que le serveur de magasin d'objets prend actuellement en charge pour les compartiments NAS S3 sont les suivantes : GetObject, PutObject, DeleteObject, ListBucket, GetBuckeAcl, GetObjectAcl et GetBuckeLocation. Les caractères génériques sont acceptés pour ce paramètre.
- `-principal <Objectstore Principal>, …` - valide l'utilisateur demandant un accès par rapport aux utilisateurs ou aux groupes du serveur de magasin d'objets spécifiés dans ce paramètre.
  - Un groupe de serveurs de stockage d'objets est spécifié en ajoutant un groupe de préfixe/ au nom du groupe.
  - `-principal` - (le caractère de trait d'union) donne accès à tous les utilisateurs.
- `-resource <text>, …` - spécifie le compartiment, le dossier ou l'objet pour lequel les autorisations d'autorisation/de refus sont définies. Les caractères génériques sont acceptés pour ce paramètre.
- `[-sid <SID>]` - spécifie un commentaire texte facultatif pour l'instruction de stratégie de compartiment de serveur de magasin d'objets.

Exemples

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Configuration SMB pour Microsoft Hyper-V et SQL Server

Présentation de la configuration SMB pour Microsoft Hyper-V et SQL Server

Les fonctionnalités de ONTAP assurent la continuité de l'activité pour deux applications Microsoft sur le protocole SMB : Microsoft Hyper-V et Microsoft SQL Server.

Vous devez appliquer ces procédures pour implémenter une continuité de l'activité SMB dans les circonstances suivantes :

- L'accès de base aux fichiers du protocole SMB a été configuré.
- Vous souhaitez activer les partages de fichiers SMB 3.0 ou version ultérieure résidant sur les SVM pour stocker les objets suivants :
  - Fichiers de machines virtuelles Hyper-V.
  - Bases de données système SQL Server

Informations associées

Pour plus d'informations sur la technologie ONTAP et l'interaction avec les services externes, voir les rapports techniques (TR) : ** "Rapport technique de NetApp 4172 : Microsoft Hyper-V sur SMB 3.0 avec les meilleures

pratiques de ONTAP" "Rapport technique NetApp 4369 : meilleures pratiques pour Microsoft SQL Server et SnapManager 7.2 for SQL Server avec clustered Data ONTAP"

Configuration de ONTAP pour Microsoft Hyper-V et SQL Server sur les solutions SMB

Vous pouvez utiliser les partages de fichiers SMB 3.0 et versions ultérieures disponibles en permanence pour stocker les fichiers des machines virtuelles Hyper-V ou les bases de données du système SQL Server et les bases de données des utilisateurs sur des volumes résidant dans des SVM, tout en assurant la continuité de l'activité à la fois pour les événements planifiés et non planifiés.

Microsoft Hyper-V sur SMB

Pour créer une solution Hyper-V sur SMB, vous devez d'abord configurer ONTAP afin de fournir des services de stockage aux serveurs Microsoft Hyper-V. En outre, vous devez également configurer les clusters Microsoft (s'ils utilisent une configuration en cluster), les serveurs Hyper-V, les connexions SMB 3.0 disponibles en continu vers les partages hébergés par le serveur CIFS, et, éventuellement, les services de sauvegarde pour protéger les fichiers de machines virtuelles stockés sur les volumes de SVM.

Les serveurs Hyper-V doivent être configurés sur Windows 2012 Server ou version ultérieure. Les configurations de serveur Hyper-V autonomes et en cluster sont toutes deux prises en charge.

- Pour plus d'informations sur la création de clusters Microsoft et de serveurs Hyper-V, consultez le site Web de Microsoft.
- SnapManager for Hyper-V est une application basée sur hôte qui facilite des services de sauvegarde rapides basés sur des copies Snapshot. Elle est conçue pour s'intégrer aux configurations Hyper-V sur SMB.

  Pour plus d'informations sur l'utilisation de SnapManager avec les configurations Hyper-V sur SMB, voir le *SnapManager for Hyper-V installation and Administration Guide*.

Microsoft SQL Server sur SMB

Pour créer une solution SQL Server sur SMB, vous devez d'abord configurer ONTAP afin de fournir des services de stockage pour l'application Microsoft SQL Server. En outre, vous devez également configurer les clusters Microsoft (en cas d'utilisation d'une configuration en cluster). Vous devez ensuite installer et configurer SQL Server sur les serveurs Windows et créer des connexions SMB 3.0 disponibles en continu vers les partages hébergés par le serveur CIFS. Vous pouvez choisir de configurer les services de sauvegarde pour protéger les fichiers de base de données stockés sur des volumes SVM.

SQL Server doit être installé et configuré sur Windows 2012 Server ou version ultérieure. Les configurations autonomes et en cluster sont prises en charge.

- Pour plus d'informations sur la création de clusters Microsoft et l'installation et la configuration de SQL Server, consultez le site Web de Microsoft.
- Le plug-in SnapCenter pour Microsoft SQL Server est une application basée sur hôte qui facilite des services de sauvegarde rapides basés sur des snapshots, conçus pour s'intégrer aux configurations SQL Server sur SMB.

Pour plus d'informations sur l'utilisation du plug-in SnapCenter pour Microsoft SQL Server, consultez le "Plug-in SnapCenter pour Microsoft SQL Server" documentation :

Continuité de l'activité pour Hyper-V et SQL Server over SMB

En termes de continuité de l'activité pour Hyper-V et SQL Server over SMB

La continuité de l'activité pour Hyper-V et SQL Server over SMB se réfère à la combinaison de fonctionnalités permettant aux serveurs d'application et aux machines virtuelles ou bases de données contenues de rester en ligne et d'assurer une disponibilité continue au cours de nombreuses tâches administratives. Cela inclut les temps d'indisponibilité planifiés et non planifiés de l'infrastructure de stockage.

La continuité de l'activité pour les serveurs applicatifs via SMB est prise en charge :

- Takeover et Giveback planifiées
- Basculement non planifié
- Mise à niveau
- Transfert d'agrégats planifié (ARL)
- Migration et basculement de LIF
- Déplacement de volume planifié

Protocoles qui garantissent la continuité de l'activité sur SMB

Outre la commercialisation de SMB 3.0, Microsoft a lancé de nouveaux protocoles qui fournissent les fonctionnalités nécessaires à la continuité de l'activité pour Hyper-V et SQL Server over SMB.

ONTAP utilise ces protocoles pour assurer la continuité de l'activité des serveurs applicatifs sur SMB :

- SMB 3.0
- Témoin

Concepts clés de la continuité de l'activité pour Hyper-V et SQL Server sur SMB

Avant de configurer la solution Hyper-V ou SQL Server sur SMB, certains concepts relatifs à la continuité de l'activité doivent être abordés.

- **Partage disponible en continu**

  Partage SMB 3.0 avec la propriété de partage disponible en continu. Les clients qui se connectent via des partages disponibles en permanence peuvent survivre aux événements perturbateur tels que le basculement, le rétablissement et le transfert d'agrégats.

- **Nœud**

  Un contrôleur unique membre d'un cluster. Pour faire la distinction entre les deux nœuds d'une paire SFO, un nœud est parfois appelé *local node* et l'autre nœud est parfois appelé *Partner node* ou *remote node*. Le propriétaire principal du stockage est le nœud local. Le propriétaire secondaire, qui prend le contrôle du

stockage en cas de défaillance du propriétaire principal, est le nœud partenaire. Chaque nœud est le principal propriétaire de son stockage et du secondaire pour le stockage de son partenaire.

- **Transfert d'agrégats sans interruption**

  Capacité à déplacer un agrégat entre les nœuds partenaires au sein d'une paire SFO dans un cluster sans interrompre les applications client.

- **Basculement sans interruption**

  Voir *Takeover*.

- **Migration de LIF sans interruption**

  La possibilité d'effectuer une migration de LIF sans interrompre les applications client qui sont connectées au cluster via cette LIF. Pour les connexions SMB, cette opération est uniquement possible pour les clients qui se connectent via SMB 2.0 ou version ultérieure.

- * Continuité de l'activité*

  La possibilité d'effectuer les principales opérations de gestion et de mise à niveau ONTAP, et de résister aux défaillances de nœud sans interrompre les applications client. Ce terme fait référence à la collecte de fonctionnalités de basculement sans interruption, de mise à niveau sans interruption et de migration dans son ensemble.

- * Mise à niveau sans interruption*

  Capacité à mettre à niveau le matériel ou les logiciels des nœuds sans perturber les applications.

- **Déplacement de volume sans interruption**

  La capacité de déplacer librement un volume au sein du cluster sans interrompre les applications qui utilisent ce volume. Pour les connexions SMB, toutes les versions de SMB prennent en charge le déplacement de volumes sans interruption.

- **Poignées permanentes**

  Propriété de SMB 3.0 qui permet aux connexions disponibles en continu de se reconnecter de façon transparente au serveur CIFS en cas de déconnexion. Tout comme les poignées durables, les poignées permanentes sont conservées par le serveur CIFS pendant un certain temps après la perte de la communication avec le client connecté. Toutefois, les pointeurs permanents bénéficient d'une résilience supérieure à celle des poignées durables. En plus de donner au client la possibilité de récupérer la poignée dans une fenêtre de 60 secondes après reconnexion, le serveur CIFS refuse l'accès à tout autre client demandant l'accès au fichier pendant cette fenêtre de 60 secondes.

  Des informations relatives aux pointeurs permanents sont mises en miroir sur le stockage persistant du partenaire SFO, qui permet aux clients disposant de pointeurs permanents déconnectés de récupérer les pointeurs durables après un événement où le partenaire SFO est propriétaire du stockage du nœud. En plus d'assurer la continuité de l'activité en cas de déplacement de LIF (dont la prise en charge est durable), des pointeurs permanents assurent la continuité de l'activité pendant le basculement, le rétablissement et le transfert d'agrégats.

- **OFS-retour**

  Retour d'agrégats à leurs locaux lors d'une récupération après un événement de basculement.

- **Paire SFO**

  Si l'un des deux nœuds cesse de fonctionner, une paire de nœuds dont les contrôleurs sont configurés pour transmettre des données les uns aux autres. Selon le modèle du système, les deux contrôleurs peuvent se trouver dans un seul châssis ou les contrôleurs peuvent se trouver dans un châssis distinct. Appelé paire HA dans un cluster à deux nœuds.

- * Prise de contrôle*

  Processus par lequel le partenaire prend le contrôle du stockage en cas de défaillance du propriétaire principal de ce stockage. Dans le cadre du SFO, le basculement et le basculement sont synonymes.

La fonctionnalité SMB 3.0 prend en charge la continuité de l'activité sur les partages SMB

SMB 3.0 apporte une fonctionnalité essentielle qui permet la continuité de l'activité pour les partages Hyper-V et SQL Server sur SMB. Cela inclut le `continuously-available` Partagez la propriété et un type de descripteur de fichier appelé *persistent handle* qui permettent aux clients SMB de récupérer l'état ouvert du fichier et de rétablir de façon transparente les connexions SMB.

Des pointeurs permanents peuvent être accordés aux clients compatibles SMB 3.0 qui se connectent à un partage avec l'ensemble de propriétés de partage disponible en continu. Si la session SMB est déconnectée, le serveur CIFS conserve les informations relatives à l'état de descripteur permanent. Le serveur CIFS bloque les autres requêtes client pendant la période de 60 secondes pendant laquelle le client est autorisé à se reconnecter, ce qui permet au client avec le descripteur permanent de récupérer le descripteur après une déconnexion du réseau. Les clients avec pointeurs permanents peuvent se reconnecter en utilisant l'une des LIF de données sur la machine virtuelle de stockage (SVM), en reconnectant via la même LIF ou via une autre LIF.

Le transfert, le basculement et le rétablissement d'agrégats s'effectuent tous entre les paires SFO. Pour gérer de manière transparente la déconnexion et la reconnexion des sessions avec des fichiers dotés de pointeurs permanents, le nœud partenaire conserve une copie de toutes les informations de verrouillage de descripteur permanent. Que l'événement soit planifié ou non, le partenaire SFO peut gérer les reconnexions de la poignée persistante sans interruption. Grâce à cette nouvelle fonctionnalité, les connexions SMB 3.0 au serveur CIFS peuvent basculer en toute transparence vers une autre LIF de données affectée à la SVM, selon les temps d'événements perturbateurs.

Bien que l'utilisation de pointeurs permanents permette au serveur CIFS de basculer en toute transparence sur des connexions SMB 3.0, en cas de défaillance, l'application Hyper-V bascule vers un autre nœud du cluster Windows Server, le client n'a aucun moyen de récupérer les descripteurs de fichiers de ces pointeurs déconnectés. Dans ce scénario, les descripteurs de fichier à l'état déconnecté peuvent potentiellement bloquer l'accès à l'application Hyper-V s'il est redémarré sur un autre nœud. « Failover Clustering » fait partie de SMB 3.0 qui répond à ce scénario en fournissant un mécanisme permettant d'invalider des pointeurs obsolètes en conflit. Grâce à ce mécanisme, un cluster Hyper-V peut restaurer rapidement les données en cas de panne des nœuds de cluster Hyper-V.

Comment le protocole Witness traite l'amélioration du basculement transparent

Le protocole Witness propose des fonctionnalités de basculement client améliorées pour les partages SMB 3.0 disponibles en continu (partages CA). Témoin facilite le basculement plus rapide car il évite toute période de restauration de basculement LIF. Cette notification avertit les serveurs d'applications lorsqu'un nœud est indisponible sans

nécessiter l’attente de la connexion SMB 3.0.

Le basculement est transparent, car les applications s’exécutant sur le client ne savent pas qu’un basculement a eu lieu. Si Witness n’est pas disponible, le basculement s’effectue toujours avec succès, mais le basculement sans Witness s’avère moins efficace.

Le basculement amélioré par témoin est possible lorsque les conditions suivantes sont respectées :

- Il ne peut être utilisé qu’avec des serveurs CIFS compatibles SMB 3.0 sur lesquels SMB 3.0 est activé.
- Les partages doivent utiliser SMB 3.0 avec l’ensemble de propriétés de partage de disponibilité continue.
- Le partenaire SFO du nœud sur lequel les serveurs d’applications sont connectés doit disposer d’au moins une LIF de données opérationnelles attribuée au SVM (Storage Virtual machine) qui héberge les données des serveurs applicatifs.

> Le protocole Witness fonctionne entre les paires SFO. Étant donné que les LIF peuvent migrer vers n’importe quel nœud du cluster, n’importe quel nœud peut avoir besoin d’être le témoin de son partenaire SFO. Le protocole Witness ne peut pas permettre le basculement rapide des connexions SMB sur un nœud donné si le SVM hébergeant les données des serveurs d’applications ne dispose pas d’une LIF de données active sur le nœud partenaire. Par conséquent, chaque nœud du cluster doit disposer d’au moins une LIF de données pour chaque SVM hébergeant l’une de ces configurations.

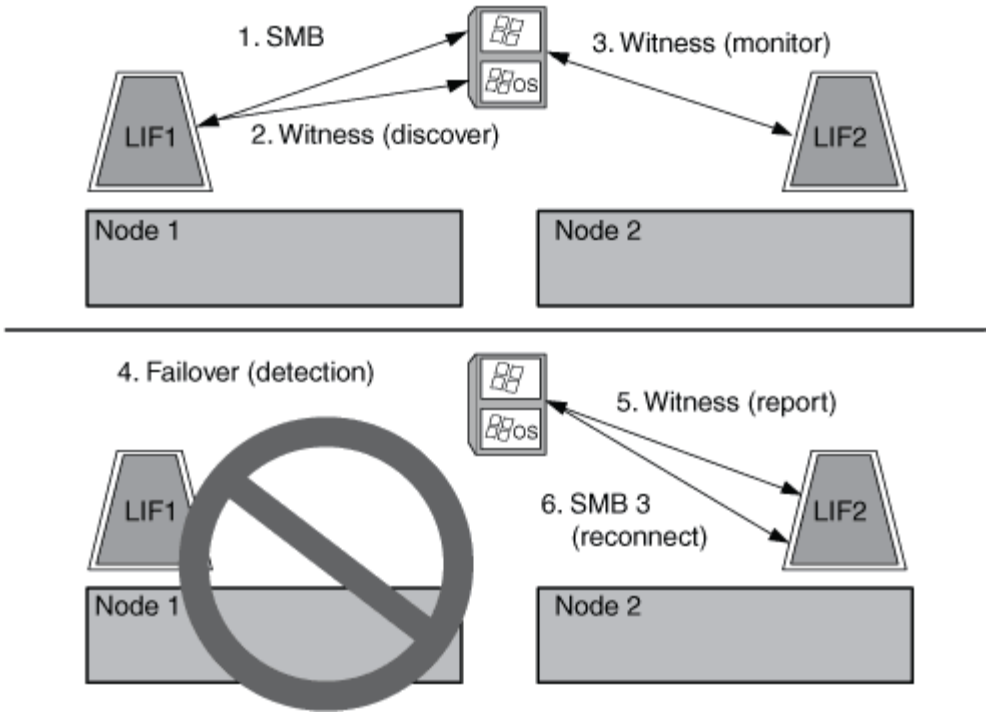
- Les serveurs d’applications doivent se connecter au serveur CIFS en utilisant le nom du serveur CIFS stocké dans DNS au lieu d’utiliser des adresses IP LIF individuelles.

Fonctionnement du protocole Witness

ONTAP implémente le protocole Witness en utilisant le partenaire SFO d’un nœud comme témoin. En cas de défaillance, le partenaire détecte rapidement la panne et en informe le client SMB.

Le protocole Witness fournit un basculement amélioré à l’aide du processus suivant :

1. Lorsque le serveur d’applications établit une connexion SMB disponible en continu pour Node1, le serveur CIFS informe le serveur d’applications que Witness est disponible.
2. Le serveur d’application demande les adresses IP du serveur Witness à partir du nœud 1 et reçoit une liste des adresses IP LIF de données Node2 (le partenaire SFO) attribuées à la machine virtuelle de stockage (SVM).
3. Le serveur d’application choisit l’une des adresses IP, crée une connexion témoin à Node2 et s’enregistre pour être averti si la connexion disponible en continu sur Node1 doit être déplacé.
4. Si un événement de basculement se produit sur le nœud 1, Witness simplifie les événements de basculement, mais n’est pas impliqué dans le rétablissement.
5. Témoin détecte l’événement de basculement et informe le serveur d’application via la connexion Witness que la connexion SMB doit passer à Node2.
6. Le serveur d’application déplace la session SMB sur Node2 et restaure la connexion sans interruption de l’accès client.



Partage de sauvegardes avec VSS distant

Présentation de VSS distant pour les sauvegardes basées sur le partage

Vous pouvez utiliser VSS distant pour effectuer des sauvegardes basées sur les partages des fichiers de machines virtuelles Hyper-V stockés sur un serveur CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) est une extension de l'infrastructure Microsoft VSS existante. Avec Remote VSS, Microsoft a étendu l'infrastructure VSS pour prendre en charge la copie Shadow des partages SMB. De plus, des applications serveur telles qu'Hyper-V peuvent stocker des fichiers VHD sur des partages de fichiers SMB. Avec ces extensions, il est possible d'effectuer des clichés instantanés cohérents avec les applications pour les machines virtuelles qui stockent des données et des fichiers de configuration sur des partages.

Concepts de VSS distant

Vous devez connaître certains concepts requis pour comprendre l'utilisation de VSS distant (Volume Shadow Copy Service) par les services de sauvegarde avec des configurations Hyper-V sur SMB.

- **VSS (Volume Shadow Copy Service)**

  Technologie Microsoft utilisée pour effectuer des copies de sauvegarde ou des snapshots de données sur un volume spécifique à un point dans le temps spécifique. VSS coordonne entre les serveurs de données, les applications de sauvegarde et les logiciels de gestion du stockage afin d'assurer la création et la gestion de sauvegardes cohérentes.

- **VSS distant (Remote Volume Shadow Copy Service)**

  Technologie Microsoft utilisée pour créer des copies de sauvegarde basées sur les partages de données qui sont cohérentes avec les données à un point spécifique dans le temps où les données sont accessibles via les partages SMB 3.0. Également connu sous le nom *Volume Shadow Copy Service*.

- **Copie fantôme**

  Un jeu de données dupliqué contenu dans le partage à un instant bien défini dans le temps. Des clichés instantanés sont utilisés pour créer des sauvegardes ponctuelles cohérentes des données, permettant ainsi au système ou aux applications de continuer à mettre à jour les données sur les volumes d'origine.

- **Ensemble de copies ombré**

  Collection d'une ou plusieurs clichés instantanés, chaque copie fantôme correspondant à un partage. Les clichés instantanés dans un jeu de clichés instantanés représentent tous les partages qui doivent être sauvegardés dans la même opération. Le client VSS de l'application VSS-enabled identifie les clichés instantanés à inclure dans l'ensemble.

- **Shadow Copy set Automatic Recovery**

  La partie du processus de sauvegarde pour les applications de sauvegarde VSS distantes dans lesquelles le répertoire de réplica contenant les clichés instantanés est cohérent à un point dans le temps. Au début de la sauvegarde, le client VSS de l'application déclenche l'application pour qu'elle prenne des points de contrôle logiciels sur les données planifiées pour la sauvegarde (les fichiers de la machine virtuelle dans le cas d'Hyper-V). Le client VSS autorise alors les applications à continuer. Une fois le jeu de clichés instantanés créé, Remote VSS rend le jeu de clichés instantanés inscriptible et expose la copie inscriptible aux applications. L'application prépare le jeu de clichés instantanés pour la sauvegarde en effectuant une restauration automatique à l'aide du point de contrôle du logiciel précédemment effectué. La récupération automatique place les clichés instantanés dans un état cohérent en détournant les modifications apportées aux fichiers et répertoires depuis la création du point de contrôle. La restauration automatique est une étape facultative pour les sauvegardes VSS.

- **ID de copie fantôme**

  GUID qui identifie de manière unique une copie en double.

- **ID jeu de copies ombré**

  GUID qui identifie de manière unique une collection d'ID de copie en double sur le même serveur.

- **SnapManager pour Hyper-V**

  Logiciel qui automatise et simplifie les opérations de sauvegarde et de restauration pour Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V utilise VSS distant avec restauration automatique pour sauvegarder des fichiers Hyper-V sur des partages SMB.

Informations associées

Concepts clés de la continuité de l'activité pour Hyper-V et SQL Server sur SMB

Partage de sauvegardes avec VSS distant

Exemple de structure de répertoire utilisée par VSS distant

VSS distant traverse la structure de répertoire qui stocke les fichiers de machine virtuelle Hyper-V lorsqu'il crée des clichés instantanés. Il est important de comprendre la structure de répertoires appropriée afin de pouvoir créer des sauvegardes de fichiers de machines virtuelles.

Une structure de répertoire prise en charge pour la création réussie de clichés instantanés est conforme aux

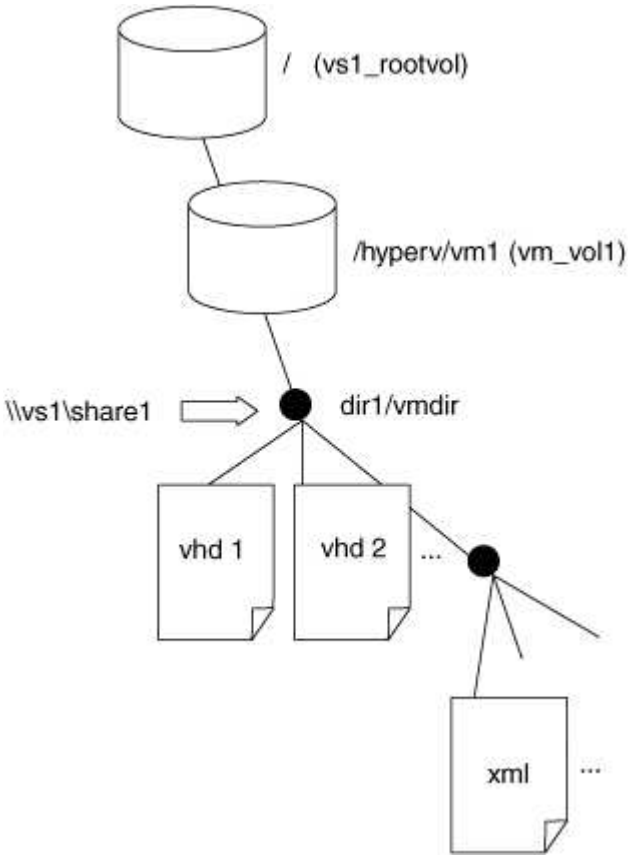
exigences suivantes :

- Seuls les répertoires et les fichiers réguliers sont présents dans la structure de répertoires utilisée pour stocker les fichiers de la machine virtuelle.

  La structure du répertoire ne contient pas de jonctions, de liens ou de fichiers non réguliers.

- Tous les fichiers d'une machine virtuelle résident dans un même partage.
- La structure de répertoire utilisée pour stocker les fichiers de la machine virtuelle ne dépasse pas la profondeur configurée dans le répertoire de clichés instantanés.
- Le répertoire racine du partage contient uniquement des fichiers ou des répertoires de machine virtuelle.

Dans l'illustration suivante, le volume nommé vm_vol1 est créé avec un point de jonction à `/hyperv/vm1` Sur la machine virtuelle de stockage (SVM) vs1. Les sous-répertoires contenant les fichiers de la machine virtuelle sont créés sous le point de jonction. Les fichiers de machine virtuelle du serveur Hyper-V sont accessibles sur share1 qui a le chemin `/hyperv/vm1/dir1/vmdir`. Le service Shadow Copy crée des clichés instantanés de tous les fichiers de la machine virtuelle qui sont contenus dans la structure de répertoires sous share1 (jusqu'à la profondeur configurée dans le répertoire Shadow Copy).



Comment SnapManager for Hyper-V gère les sauvegardes VSS distantes pour Hyper-V sur SMB

Vous pouvez utiliser SnapManager for Hyper-V pour gérer les services de sauvegarde VSS distants. Les avantages du service géré de sauvegarde SnapManager for Hyper-V sont nombreux, car il permet de créer des ensembles de sauvegarde peu gourmands en espace.

Les optimisations vers SnapManager pour les sauvegardes gérées Hyper-V sont les suivantes :

- L’intégration de SnapDrive avec ONTAP permet d’optimiser les performances lors de la détection de l’emplacement de partage SMB.

  ONTAP fournit à SnapDrive le nom du volume où réside le partage.

- SnapManager for Hyper-V spécifie la liste des fichiers de machine virtuelle dans les partages SMB que le service Shadow Copy doit copier.

  En fournissant une liste ciblée de fichiers de machine virtuelle, le service de clichés instantanés n’a pas besoin de créer de clichés instantanés de tous les fichiers du partage.

- La machine virtuelle de stockage (SVM) conserve les snapshots de SnapManager pour Hyper-V à utiliser pour les restaurations.

  Il n’y a pas de phase de sauvegarde. La sauvegarde est le snapshot compact.

SnapManager for Hyper-V fournit des fonctionnalités de sauvegarde et de restauration pour HyperV sur SMB, en utilisant le processus suivant :

1. Préparation de l’opération de copie en double

   Le client VSS de l’application SnapManager pour Hyper-V configure le jeu de clichés instantanés. Le client VSS collecte des informations sur les partages à inclure dans le jeu de clichés instantanés et fournit ces informations à ONTAP. Un ensemble peut contenir une ou plusieurs clichés instantanés et une copie en double correspond à un partage.

2. Création du jeu de clichés instantanés (si la restauration automatique est utilisée)

   Pour chaque partage inclus dans le jeu de clichés instantanés, ONTAP crée une copie « shadow » et rend la copie « shadow Copy » accessible en écriture.

3. Exposition du jeu de clichés instantanés

   Une fois que ONTAP a créé les clichés instantanés, ils sont exposés à SnapManager for Hyper-V de sorte que les enregistreurs VSS de l’application peuvent effectuer une restauration automatique.

4. Restauration automatique du jeu de clichés instantanés

   Au cours de la création du jeu de clichés instantanés, il y a une période pendant laquelle des modifications actives sont apportées aux fichiers inclus dans le jeu de sauvegardes. Les VSS writer de l’application doivent mettre à jour les clichés instantanés pour s’assurer qu’ils sont dans un état complètement cohérent avant la sauvegarde.

   La méthode d’exécution de la restauration automatique est spécifique à l’application. VSS distant n’est pas impliqué dans cette phase.

5. Finalisation et nettoyage du jeu de clichés instantanés

   Le client VSS informe ONTAP après la fin de la restauration automatique. Le jeu de copies « shadow » est en lecture seule, puis prêt pour la sauvegarde. Lors de l’utilisation de SnapManager pour Hyper-V pour la sauvegarde, les fichiers d’un snapshot deviennent la sauvegarde. Par conséquent, pour la phase de sauvegarde, un snapshot est créé pour chaque volume contenant des partages dans le jeu de sauvegarde. Une fois la sauvegarde terminée, le jeu de clichés instantanés est supprimé du serveur CIFS.

Comment l’allègement de la charge des copies d’ODX est utilisé avec Hyper-V et SQL Server sur des partages SMB

Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le transfert direct de données au sein d’un périphérique de stockage compatible ou entre ces périphériques, sans transférer les données via l’ordinateur hôte. Le allègement de la charge des copies ONTAP ODX présente des avantages en termes de performances lors des opérations de copie sur votre serveur applicatif plutôt que sur une installation SMB.

Dans les transferts de fichiers non ODX, les données sont lues à partir du serveur CIFS source et sont transférées sur le réseau vers l’ordinateur client. L’ordinateur client transfère les données via le réseau vers le serveur CIFS de destination. En résumé, l’ordinateur client lit les données à partir de la source et les écrit vers la destination. Grâce aux transferts de fichiers ODX, les données sont copiées directement de la source vers la destination.

Les copies déchargées d’ODX étant effectuées directement entre le stockage source et le stockage de destination, les performances sont considérablement améliorées. Les avantages obtenus en termes de performances comprennent l’accélération du délai de copie entre la source et la destination, la réduction de l’utilisation des ressources (CPU, mémoire) sur le client et la réduction de l’utilisation de la bande passante E/S du réseau.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
Les cas d'utilisation suivants prennent en charge l'utilisation de copies
et de déplacements d'ODX :
```

- Intra-volume

  Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volumes, même nœud, même machine virtuelle de stockage (SVM)

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

  Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

Les cas d’utilisation spécifiques pour l’allègement de la charge des copies d’ODX avec les solutions Hyper-V

sont les suivants :

- Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.

  Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.

- Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
- L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.

> Pour tirer parti des cas d'utilisation liés au délestage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Voici quelques cas d'utilisation spécifiques des copies ODX utilisées par les solutions SQL Server :

- Vous pouvez utiliser l'allègement de la charge des copies d'ODX pour exporter et importer des bases de données SQL Server entre des partages SMB mappés ou entre des partages SMB et des LUN iSCSI connectés au sein du même cluster.
- L'allègement de la charge de copies (ODX) est utilisé pour les exportations et les importations de bases de données si le stockage source et cible est situé sur le même cluster.

Configuration requise et considérations

Conditions requises pour le ONTAP et les licences

Vous devez connaître certaines exigences en matière de licences et de ONTAP lors de la création de solutions SQL Server ou Hyper-V sur SMB afin de garantir la continuité de l'activité sur les SVM.

Configuration requise pour la version ONTAP

- Hyper-V sur SMB

  ONTAP prend en charge la continuité de l'activité sur les partages SMB pour Hyper-V exécutés sous Windows 2012 ou version ultérieure.

- SQL Server sur SMB

  ONTAP prend en charge la continuité de l'activité sur les partages SMB pour SQL Server 2012 ou une version ultérieure fonctionnant sous Windows 2012 ou version ultérieure.

Pour obtenir les dernières informations sur les versions prises en charge de ONTAP, Windows Server et SQL Server pour assurer la continuité de l'activité sur les partages SMB, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

Licences requises

Les licences suivantes sont requises :

- CIFS
- FlexClone (pour Hyper-V sur SMB uniquement)

  Cette licence est requise si Remote VSS est utilisé pour les sauvegardes. Le service Shadow Copy utilise FlexClone pour créer des copies instantanées de fichiers qui sont ensuite utilisés lors de la création d'une sauvegarde.

  Une licence FlexClone est facultative si vous utilisez une méthode de sauvegarde qui n'utilise pas VSS distant.

La licence FlexClone est incluse dans "ONTAP One". Si vous n'avez pas ONTAP One, vous devez "vérifiez que les licences requises sont installées", et, si nécessaire, "installez-les".

Exigences LIF relatives au réseau et aux données

Vous devez connaître certaines exigences LIF de réseau et de données lors de la création de configurations SQL Server ou Hyper-V sur SMB afin de garantir la continuité de l'activité).

Exigences en matière de protocoles réseau

- Les réseaux IPv4 et IPv6 sont pris en charge.
- SMB 3.0 ou version ultérieure requis.

  SMB 3.0 apporte les fonctionnalités nécessaires pour créer les connexions SMB disponibles en continu nécessaires à la continuité de l'activité.

- Les serveurs DNS doivent contenir des entrées qui mappent le nom du serveur CIFS aux adresses IP attribuées aux LIF de données sur la machine virtuelle de stockage (SVM).

  Les serveurs d'applications Hyper-V ou SQL Server font en général plusieurs connexions sur plusieurs LIF de données lors de l'accès aux fichiers de machines virtuelles ou de bases de données. Pour garantir la fonctionnalité appropriée, les serveurs d'applications doivent établir ces connexions SMB en utilisant le nom du serveur CIFS au lieu de créer plusieurs connexions à plusieurs adresses IP uniques.

  Témoin exige également l'utilisation du nom DNS du serveur CIFS au lieu d'adresses IP LIF individuelles.

  Depuis ONTAP 9.4, SMB Multichannel permet d'améliorer le débit et la tolérance aux pannes des configurations Hyper-V et SQL Server sur SMB. Pour ce faire, vous devez avoir plusieurs cartes réseau 1G, 10G ou plus grandes déployées sur le cluster et les clients.

Configuration requise pour Data LIF

- La SVM hébergeant le serveur d'application sur la solution SMB doit disposer d'au moins une LIF de données opérationnelles sur chaque nœud du cluster.

  Les LIFs de données SVM peuvent basculer vers d'autres ports de données du cluster, y compris les nœuds qui n'hébergent pas actuellement les données accessibles par les serveurs applicatifs. De plus, comme le nœud Witness est toujours le partenaire SFO d'un nœud sur lequel le serveur d'applications est

connecté, chaque nœud du cluster est un nœud potentiel Witness.

- Les LIF de données ne doivent pas être configurées pour rétablir automatiquement ces données.

  Après un événement de basculement ou de rétablissement, vous devez rétablir manuellement les LIF de données sur leurs ports de rattachement.

- Toutes les adresses IP de la LIF de données doivent disposer d'une entrée dans DNS et toutes les entrées doivent se résoudre au nom du serveur CIFS.

  Les serveurs d'applications doivent se connecter aux partages SMB à l'aide du nom du serveur CIFS. Ne configurez pas les serveurs d'application pour établir des connexions en utilisant les adresses IP de LIF.

- Si le nom du serveur CIFS est différent du nom du SVM, les entrées DNS doivent être résolus sur le nom du serveur CIFS.

Exigences en termes de volumes et de serveurs SMB pour Hyper-V sur SMB

Vous devez tenir compte de certaines exigences en matière de volume et de serveur SMB lors de la création de configurations Hyper-V sur SMB afin de garantir la continuité de l'activité.

Configuration requise pour les serveurs SMB

- SMB 3.0 doit être activé.

  Cette option est activée par défaut.

- L'option de serveur CIFS utilisateur UNIX par défaut doit être configurée avec un compte utilisateur UNIX valide.

  Les serveurs d'applications utilisent le compte machine lors de la création d'une connexion SMB. Comme tout accès SMB nécessite que l'utilisateur Windows soit correctement mappé à un compte d'utilisateur UNIX ou au compte d'utilisateur UNIX par défaut, ONTAP doit pouvoir mapper le compte machine du serveur d'applications sur le compte d'utilisateur UNIX par défaut.

- Les référencements de nœuds automatiques doivent être désactivés (cette fonctionnalité est désactivée par défaut).

  Si vous souhaitez utiliser les référencements de nœuds automatiques pour l'accès aux données autres que les fichiers des machines Hyper-V, vous devez créer un SVM distinct pour ces données.

- L'authentification Kerberos et NTLM doit être autorisée dans le domaine auquel le serveur SMB appartient.

  ONTAP ne fait pas la promotion du service Kerberos pour VSS distant ; par conséquent, le domaine doit être défini pour autoriser NTLM.

- La fonctionnalité Shadow Copy doit être activée.

  Cette fonctionnalité est activée par défaut.

- Le compte de domaine Windows utilisé par le service de copie instantanée lors de la création de copies en double doit être membre du groupe local BULILTIN\Administrators ou BULILTIN\Backup Operators du serveur SMB.

Besoins en termes de volume

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

  Pour fournir des NDO aux serveurs d'applications utilisant des connexions SMB disponibles en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume de type sécurité NTFS et l'utiliser directement pour les NDO sur des partages SMB. Si vous modifiez un volume de style de sécurité mixte en volume de style de sécurité NTFS et que vous envisagez de l'utiliser pour les NDO sur des partages SMB, vous devez placer manuellement une ACL en haut du volume et propager cette ACL à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Pour que les opérations de copie en mode « shadow » aient réussi, vous devez disposer de suffisamment d'espace disponible sur le volume.

  L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Besoins en volume et serveur SMB pour SQL Server sur SMB

Pour assurer la continuité de l'activité, vous devez tenir compte des exigences en matière de volumes et de serveurs SMB lors de la création de configurations SQL Server sur SMB.

Configuration requise pour les serveurs SMB

- SMB 3.0 doit être activé.

  Cette option est activée par défaut.

- L'option de serveur CIFS utilisateur UNIX par défaut doit être configurée avec un compte utilisateur UNIX valide.

  Les serveurs d'applications utilisent le compte machine lors de la création d'une connexion SMB. Comme tout accès SMB nécessite que l'utilisateur Windows soit correctement mappé à un compte d'utilisateur UNIX ou au compte d'utilisateur UNIX par défaut, ONTAP doit pouvoir mapper le compte machine du serveur d'applications sur le compte d'utilisateur UNIX par défaut.

  En outre, SQL Server utilise un utilisateur de domaine comme compte de service SQL Server. Le compte de service doit également être mappé à l'utilisateur UNIX par défaut.

- Les référencements de nœuds automatiques doivent être désactivés (cette fonctionnalité est désactivée par défaut).

  Si vous souhaitez utiliser les référencements de nœuds automatiques pour l'accès aux données autres

que les fichiers de bases de données SQL Server, vous devez créer un SVM distinct pour ces données.

- Le privilège SeSecurityPrivilege doit être attribué au compte utilisateur Windows utilisé pour installer SQL Server sur ONTAP.

  Ce privilège est attribué au groupe local BULTILTIN\Administrators du serveur SMB.

Besoins en termes de volume

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

  Pour fournir des NDO aux serveurs d'applications utilisant des connexions SMB disponibles en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume de type sécurité NTFS et l'utiliser directement pour les NDO sur des partages SMB. Si vous modifiez un volume de style de sécurité mixte en volume de style de sécurité NTFS et que vous envisagez de l'utiliser pour les NDO sur des partages SMB, vous devez placer manuellement une ACL en haut du volume et propager cette ACL à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Bien que le volume contenant les fichiers de base de données puisse contenir des jonctions, SQL Server ne traverse pas les jonctions lors de la création de la structure du répertoire de base de données.
- Pour que les opérations de sauvegarde du plug-in SnapCenter pour Microsoft SQL Server réussissent, vous devez disposer de suffisamment d'espace disponible sur le volume.

  Le volume sur lequel les fichiers de base de données SQL Server résident doit être suffisamment grand pour contenir la structure du répertoire de base de données et tous les fichiers contenus résidant dans le partage.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Exigences de partage constamment disponibles et considérations pour Hyper-V sur SMB

Vous devez connaître certaines exigences et considérations relatives à la configuration de partages disponibles en continu pour les configurations Hyper-V sur SMB qui prennent en charge la continuité de l'activité.

Exigences en matière de partage

- Les partages utilisés par les serveurs d'applications doivent être configurés avec le jeu de propriétés disponible en continu.

  Les serveurs d'application qui se connectent aux partages disponibles en permanence sont dotés de pointeurs permanents qui leur permettent de se reconnecter sans interruption aux partages SMB et de récupérer les verrouillages de fichiers après des événements perturbateurs, tels que le basculement, le rétablissement et le transfert d'agrégats.

- Si vous souhaitez utiliser les services de sauvegarde Remote VSS-enabled, vous ne pouvez pas placer de

fichiers Hyper-V dans des partages contenant des jonctions.

Dans le cas de la récupération automatique, la création de clichés instantanés échoue si une jonction est détectée lors du déplacement du partage. Dans le cas non auto-Recovery, la création de la copie en double ne échoue pas, mais la jonction ne pointe en rien.

- Si vous souhaitez utiliser les services de sauvegarde Remote VSS-enabled avec auto-Recovery, vous ne pouvez pas placer les fichiers Hyper-V dans des partages contenant les éléments suivants :
  - Symlinks, liens rigides ou widelinks
  - Fichiers non standard

    La création de la copie en double échoue si des liens ou des fichiers non standard se trouvent dans le partage vers copie en double. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

  - Pour que les opérations de clichés instantanés réussisse, vous devez disposer d'un espace disponible suffisant sur le volume (pour Hyper-V sur SMB uniquement).

    L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.
- Les propriétés de partage suivantes ne doivent pas être définies sur les partages disponibles en continu utilisés par les serveurs d'applications :
  - Répertoire de base
  - Mise en cache des attributs
  - BranchCache

Considérations

- Les quotas sont pris en charge par les partages disponibles en permanence.
- La fonctionnalité suivante n'est pas prise en charge pour les configurations Hyper-V sur SMB :
  - Audit
  - FPolicy
- L'analyse antivirus n'est pas réalisée sur les partages SMB avec le `continuously-availability` paramètre défini sur `Yes`.

Exigences en matière de partages disponibles en permanence et considérations pour SQL Server sur SMB

Vous devez connaître certaines exigences et considérations relatives à la configuration de partages disponibles en continu pour les configurations SQL Server sur SMB qui prennent en charge la continuité de l'activité.

Exigences en matière de partage

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

  Pour assurer la continuité de l'activité des serveurs applicatifs en utilisant des connexions SMB disponibles

en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume NTFS de type sécurité, et l'utiliser directement pour la continuité de l'activité sur les partages SMB. Si vous remplacez un volume de style de sécurité mixte par un volume de style de sécurité NTFS et que vous prévoyez de l'utiliser pour assurer la continuité des opérations sur des partages SMB, vous devez placer manuellement une liste de contrôle d'accès en haut du volume et la propager à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Les partages utilisés par les serveurs d'applications doivent être configurés avec le jeu de propriétés disponible en continu.

  Les serveurs d'application qui se connectent aux partages disponibles en permanence sont dotés de pointeurs permanents qui leur permettent de se reconnecter sans interruption aux partages SMB et de récupérer les verrouillages de fichiers après des événements perturbateurs, tels que le basculement, le rétablissement et le transfert d'agrégats.

- Bien que le volume contenant les fichiers de base de données puisse contenir des jonctions, SQL Server ne traverse pas les jonctions lors de la création de la structure du répertoire de base de données.
- Pour que les opérations du plug-in SnapCenter pour Microsoft SQL Server réussissent, vous devez disposer de suffisamment d'espace disponible sur le volume.

  Le volume sur lequel les fichiers de base de données SQL Server résident doit être suffisamment grand pour contenir la structure du répertoire de base de données et tous les fichiers contenus résidant dans le partage.

- Les propriétés de partage suivantes ne doivent pas être définies sur les partages disponibles en continu utilisés par les serveurs d'applications :
  - Répertoire de base
  - Mise en cache des attributs
  - BranchCache

Partager des considérations

- Les quotas sont pris en charge par les partages disponibles en permanence.
- La fonctionnalité suivante n'est pas prise en charge dans les configurations SQL Server sur SMB :
  - Audit
  - FPolicy
- L'analyse antivirus n'est pas réalisée sur les partages SMB avec le `continuously-availability` ensemble de propriétés de partage.

Considérations relatives à VSS distant pour les configurations Hyper-V sur SMB

Vous devez tenir compte de certains éléments à prendre en compte lors de l'utilisation de solutions de sauvegarde Remote VSS-enabled pour les configurations Hyper-V over SMB.

Considérations générales de VSS distant

- Un maximum de 64 partages peut être configuré par serveur d'applications Microsoft.

  L'opération de copie en double échoue si plus de 64 partages se trouvent dans un jeu de clichés instantanés. Il s'agit d'une condition requise par Microsoft.

- Un seul jeu de clichés instantanés actif par serveur CIFS est autorisé.

  Une opération de copie en double échouera si une opération de copie en double est en cours sur le même serveur CIFS. Il s'agit d'une condition requise par Microsoft.

- Aucune jonction n'est autorisée dans la structure de répertoire sur laquelle VSS distant crée une copie en double.
  - Dans le cas de la restauration automatique, la création de clichés instantanés échouera si une jonction est rencontrée lors du déplacement du partage.
  - Dans le cas de restauration non automatique, la création de clichés instantanés ne échoue pas, mais la jonction ne pointe en rien.

Considérations relatives à la VSS distante qui ne s'appliquent qu'aux clichés instantanés avec restauration automatique

Certaines limites s'appliquent uniquement aux clichés instantanés avec restauration automatique.

- Une profondeur maximale de répertoire de cinq sous-répertoires est autorisée pour la création de clichés instantanés.

  Il s'agit de la profondeur du répertoire sur laquelle le service Shadow Copy crée un jeu de sauvegarde Shadow Copy. La création de clichés instantanés échoue si les répertoires contenant un fichier de machine virtuelle sont imbriqués de plus de cinq niveaux. Cela permet de limiter la traversée de répertoire lors du clonage du partage. La profondeur maximale de répertoire peut être modifiée à l'aide d'une option de serveur CIFS.

- La quantité d'espace disponible sur le volume doit être adéquate.

  L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy.

- Aucun lien ou fichier non régulier n'est autorisé dans la structure de répertoires sur laquelle VSS distant crée une copie en double.

  La création de la copie en double échoue si des liens ou des fichiers non standard se trouvent dans le partage vers la copie en double. Le processus de clonage ne les prend pas en charge.

- Les répertoires ne sont pas autorisés à ACL NFSv4.

  Bien que la création de clichés instantanés conserve les listes de contrôle d'accès NFSv4 sur les fichiers, les listes de contrôle d'accès NFSv4 sur les répertoires sont perdues.

- Un maximum de 60 secondes est autorisé à créer un jeu de clichés instantanés.

  Les spécifications Microsoft permettent de créer le jeu de clichés instantanés pendant 60 secondes au maximum. Si le client VSS ne peut pas créer l'ensemble de clichés instantanés dans ce délai, l'opération de copie en double échoue ; ceci limite donc le nombre de fichiers dans un jeu de clichés instantanés. Le nombre réel de fichiers ou de machines virtuelles pouvant être inclus dans un jeu de sauvegardes varie ;

ce nombre dépend de nombreux facteurs et doit être déterminé pour chaque environnement du client.

Conditions d'allègement de la charge des copies d'ODX pour SQL Server et Hyper-V sur SMB

L'allègement de la charge des copies (ODX) doit être activé pour migrer les fichiers de machines virtuelles ou pour exporter et importer les fichiers de base de données directement depuis la source vers l'emplacement de stockage de destination, sans envoyer de données par le biais des serveurs applicatifs. Certaines exigences sont à prendre en compte lors de l'utilisation de l'allègement de la charge des copies d'ODX avec les solutions SQL Server et Hyper-V sur SMB.

L'utilisation de l'allègement de la charge des copies (ODX) offre des performances importantes. Cette option de serveur CIFS est activée par défaut.

- SMB 3.0 doit être activé pour utiliser l'allègement de la charge des copies (ODX).
- Les volumes source doivent être d'au moins 1.25 Go.
- La déduplication doit être activée sur les volumes utilisés avec l'allègement de la charge des copies.
- Si vous utilisez des volumes compressés, le type de compression doit être adaptatif et seule la taille de groupe de compression de 8 Ko est prise en charge.

  Le type de compression secondaire n'est pas pris en charge
- Pour utiliser le délestage des copies ODX pour migrer des invités Hyper-V dans et entre les disques, les serveurs Hyper-V doivent être configurés pour utiliser des disques SCSI.

  La valeur par défaut consiste à configurer des disques IDE, mais l'allègement de charge des copies d'ODX ne fonctionne pas lorsque les invités sont migrés si des disques sont créés à l'aide de disques IDE.

Recommandations concernant les configurations SQL Server et Hyper-V sur SMB

Pour être certain que vos configurations SQL Server et Hyper-V sur SMB sont robustes et opérationnelles, vous devez connaître les meilleures pratiques recommandées lors de la configuration des solutions.

Recommandations générales

- Séparez les fichiers du serveur d'applications des données générales de l'utilisateur.

  Si possible, consacrer un SVM complet et son stockage aux données du serveur d'applications.
- Pour obtenir les meilleures performances, n'activez pas la signature SMB sur les SVM utilisés pour stocker les données du serveur d'applications.
- Pour des performances optimales et une meilleure tolérance aux pannes, SMB Multichannel permet de fournir plusieurs connexions entre ONTAP et les clients au cours d'une seule session SMB.
- Ne créez pas de partages disponibles en permanence sur d'autres partages que ceux utilisés dans la configuration Hyper-V ou SQL Server sur SMB.
- Désactiver l'alerte de modification sur les partages utilisés pour la disponibilité continue.
- N'effectuez pas de déplacement de volume simultanément au transfert d'agrégats (ARL), car les phases

de l'ARL sont suspendues.

- Pour les solutions Hyper-V sur SMB, utilisez des disques iSCSI invités lors de la création de machines virtuelles en cluster. Partagée `.VHDX` Les fichiers ne sont pas pris en charge par Hyper-V sur SMB dans les partages ONTAP SMB.

Planifiez la configuration Hyper-V ou SQL Server sur SMB

Renseignez la fiche technique de configuration des volumes

Cette fiche fournit un moyen simple d'enregistrer les valeurs nécessaires lors de la création de volumes pour les configurations SQL Server et Hyper-V sur SMB.

Pour chaque volume, vous devez spécifier les informations suivantes :

- Nom de la machine virtuelle de stockage (SVM)

  Le nom du SVM est identique pour tous les volumes.

- Nom du volume
- Nom de l'agrégat

  Vous pouvez créer des volumes sur des agrégats situés sur n'importe quel nœud du cluster.

- Taille
- Un chemin de jonction

Lorsque vous créez des volumes utilisés pour stocker des données de serveur d'applications, vous devez garder à l'esprit les éléments suivants :

- Si le volume racine n'a pas de style de sécurité NTFS, vous devez spécifier le style de sécurité comme NTFS lorsque vous créez le volume.

  Par défaut, les volumes héritent du style de sécurité du volume root du SVM.

- Les volumes doivent être configurés avec la garantie d'espace du volume par défaut.
- Vous pouvez éventuellement configurer le paramètre de gestion de l'espace de dimensionnement automatique.
- Vous devez définir l'option qui détermine la réserve d'espace de snapshot sur `0`.
- La politique de snapshot appliquée au volume doit être désactivée.

  Si la politique de snapshot du SVM est désactivée, il n'est pas nécessaire de spécifier une politique de snapshot pour les volumes. Les volumes héritent de la policy Snapshot pour le SVM. Si la politique de snapshot de la SVM n'est pas désactivée et qu'elle est configurée pour créer des snapshots, vous devez spécifier une politique de snapshot au niveau du volume, et cette politique doit être désactivée. Les sauvegardes basées sur le service Shadow Copy et les sauvegardes SQL Server gèrent la création et la suppression de snapshots.

- Vous ne pouvez pas configurer de miroirs de partage de charge pour les volumes.

Les chemins de jonction sur lesquels vous prévoyez de créer des partages que les serveurs d'applications doivent être choisis de sorte qu'aucun volume relié par jonction ne se trouve sous le point d'entrée du partage.

Par exemple, si vous souhaitez stocker des fichiers de machine virtuelle sur quatre volumes nommés « vol1 », « vol2 », « vol3 » et « vol4 », vous pouvez créer l'espace de noms indiqué dans l'exemple. Vous pouvez ensuite créer des partages pour les serveurs d'applications aux chemins suivants : `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, et `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Types d'information	Valeurs
Volume 1 : nom du volume, agrégat, taille, Junction path	
Volume 2 : nom du volume, agrégat, taille, chemin de jonction	
Volume 3 : nom du volume, agrégat, taille, chemin de jonction	
Volume 4 : nom du volume, agrégat, taille, chemin de jonction	
Volume 5 : nom du volume, agrégat, taille, chemin de jonction	
Volume 6 : nom du volume, agrégat, taille, chemin de jonction	
Volumes supplémentaires : nom du volume, agrégat, taille, Junction path	

Remplissez la fiche de configuration du partage SMB

Cette fiche vous permet d'enregistrer les valeurs dont vous avez besoin lors de la création de partages SMB disponibles en continu pour les configurations SQL Server et Hyper-V sur SMB.

Informations sur les propriétés des partages SMB et les paramètres de configuration

Pour chaque partage, vous devez spécifier les informations suivantes :

- Nom de la machine virtuelle de stockage (SVM)

  Le nom du SVM est identique pour tous les partages

- Nom de partage
- Chemin
- Propriétés du partage

  Vous devez configurer les deux propriétés de partage suivantes :

  ◦ `oplocks`

  ◦ `continuously-available`

Les propriétés de partage suivantes ne doivent pas être définies :

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  ◦ Les symlinks doivent être désactivés (la valeur de l' `-symlink-properties` le paramètre doit être nul [""]).

Informations sur les chemins de partage

Si vous utilisez VSS distant pour sauvegarder les fichiers Hyper-V, il est important de choisir les chemins de partage à utiliser lors des connexions SMB des serveurs Hyper-V vers les emplacements de stockage dans lesquels sont stockés les fichiers des machines virtuelles. Bien que les partages peuvent être créés à tout moment dans l'espace de noms, les chemins pour les partages utilisés par les serveurs Hyper-V ne doivent pas contenir de volumes reliés. Les opérations de copie en double ne peuvent pas être effectuées sur des chemins de partage qui contiennent des points de jonction.

SQL Server ne peut pas traverser les jonctions lors de la création de la structure du répertoire de la base de données. Vous ne devez pas créer de chemins de partage pour SQL Server contenant des points de jonction.

Par exemple, si vous souhaitez stocker des fichiers de machine virtuelle ou de base de données sur des volumes « vol1 », « vol2 », « vol3 » et « vol4 », vous devez créer des partages pour les serveurs d'applications aux chemins suivants : `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, et `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Bien que vous puissiez créer des partages sur le `/data1` et les `/data2` chemins pour la gestion administrative, ne configurez pas les serveurs d'applications pour qu'ils utilisent ces partages pour stocker des données.

Fiche de planification

Types d'information	Valeurs
Volume 1 : nom du partage SMB et chemin	
Volume 2 : nom et chemin du partage SMB	
Volume 3 : nom et chemin du partage SMB	
Volume 4 : nom et chemin du partage SMB	
Volume 5 : nom et chemin du partage SMB	
Volume 6 : nom et chemin du partage SMB	
Volume 7 : nom et chemin du partage SMB	
Volumes supplémentaires : noms et chemins de partage SMB	

Créez des configurations ONTAP pour la continuité de l'activité avec Hyper-V et SQL Server over SMB

Créez des configurations ONTAP pour la continuité de l'activité grâce à la présentation Hyper-V et SQL Server sur SMB

Vous devez effectuer plusieurs étapes de configuration ONTAP pour préparer les installations Hyper-V et SQL Server qui assurent la continuité de l'activité sur SMB.

Avant de créer la configuration ONTAP pour la continuité de l'activité avec Hyper-V et SQL Server sur SMB, les tâches suivantes doivent être effectuées :

- Les services de temps doivent être configurés sur le cluster.
- La mise en réseau doit être configurée pour le SVM.
- Le SVM doit être créé.
- Les interfaces LIF de données doivent être configurées sur le SVM.
- DNS doit être configuré sur le SVM.
- Les services de noms souhaités doivent être configurés pour la SVM.
- Le serveur SMB doit être créé.

Informations associées

Vérifier que les authentifications Kerberos et NTLMv2 sont autorisées (Hyper-V sur les partages SMB)

La continuité de l'activité pour Hyper-V over SMB requiert que le serveur CIFS d'un SVM de données et le serveur Hyper-V autorisent l'authentification Kerberos et NTLMv2. Vous devez vérifier les paramètres du serveur CIFS et des serveurs Hyper-V qui contrôlent les méthodes d'authentification autorisées.

Description de la tâche

L'authentification Kerberos est requise lors de la mise en place d'une connexion de partage disponible en continu. Une partie du processus VSS distant utilise l'authentification NTLMv2. Par conséquent, les connexions utilisant les deux méthodes d'authentification doivent être prises en charge dans les configurations Hyper-V sur SMB.

Les paramètres suivants doivent être configurés pour autoriser l'authentification Kerberos et NTLMv2 :

- Les export policy pour SMB doivent être désactivées sur le serveur virtuel de stockage (SVM).

Les authentifications Kerberos et NTLMv2 sont toujours activées sur les SVM, mais les règles d'exportation peuvent être utilisées pour limiter l'accès en fonction de la méthode d'authentification.

Les export policy pour SMB sont facultatives et désactivées par défaut. Si les règles d'exportation sont désactivées, l'authentification Kerberos et NTLMv2 sont autorisées par défaut sur un serveur CIFS.

- Le domaine auquel le serveur CIFS et les serveurs Hyper-V appartiennent doit autoriser l'authentification Kerberos et NTLMv2.

L'authentification Kerberos est activée par défaut sur les domaines Active Directory. Toutefois, l'authentification NTLMv2 peut être refusée, en utilisant des paramètres de stratégie de sécurité ou des stratégies de groupe.

Étapes

1. Effectuer les opérations suivantes pour vérifier que les export policies sont désactivée sur le SVM:
   a. Définissez le niveau de privilège sur avancé :

      ```
      set -privilege advanced
      ```

   b. Vérifiez que le `-is-exportpolicy-enabled` L'option de serveur CIFS est définie sur `false`:

      ```
      vserver cifs options show -vserver vserver_name -fields vserver,is-
      exportpolicy-enabled
      ```

   c. Retour au niveau de privilège admin :

      ```
      set -privilege admin
      ```

2. Si les export policy pour SMB ne sont pas désactivées, désactivez-les :

   ```
   vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled
   false
   ```

3. Vérifiez que les authentifications NTLMv2 et Kerberos sont autorisées dans le domaine.

   Pour plus d'informations sur la détermination des méthodes d'authentification autorisées dans le domaine, consultez la bibliothèque Microsoft TechNet.

4. Si le domaine n'autorise pas l'authentification NTMLv2, activez l'authentification NTLMv2 en utilisant l'une des méthodes décrites dans la documentation Microsoft.

Exemple

Les commandes suivantes vérifient que les export policies pour SMB sont désactivées sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

Vérifiez que les comptes de domaine correspondent à l'utilisateur UNIX par défaut dans ONTAP

Hyper-V et SQL Server utilisent des comptes de domaine pour créer des connexions SMB à des partages disponibles en continu. Pour réussir la création de la connexion, le compte d'ordinateur doit être mappé avec un utilisateur UNIX. Le moyen le plus pratique pour y parvenir est de mapper le compte d'ordinateur à l'utilisateur UNIX par défaut.

Description de la tâche

Hyper-V et SQL Server utilisent les comptes d'ordinateur de domaine pour créer des connexions SMB. En outre, SQL Server utilise un compte d'utilisateur de domaine comme compte de service qui établit également des connexions SMB.

Lorsque vous créez une machine virtuelle de stockage (SVM), ONTAP crée automatiquement l'utilisateur par défaut nommé `pcuser` (avec un UID de `65534`) et le groupe nommé `pcuser` (avec un GID de `65534`), et ajoute l'utilisateur par défaut au `pcuser` groupe. Si vous configurez une solution Hyper-V sur SMB sur un SVM existant avant de mettre à niveau le cluster vers Data ONTAP 8.2, l'utilisateur et le groupe par défaut risquent de ne pas exister. Dans le cas contraire, vous devez les créer avant de configurer l'utilisateur UNIX par défaut du serveur CIFS.

Étapes

1. Déterminez s'il existe un utilisateur UNIX par défaut :

```
vserver cifs options show -vserver <vserver_name>
```

2. Si l'option utilisateur par défaut n'est pas définie, déterminez si un utilisateur UNIX peut être désigné comme utilisateur UNIX par défaut :

```
vserver services unix-user show -vserver <vserver_name>
```

3. Si l'option utilisateur par défaut n'est pas définie et qu'aucun utilisateur UNIX ne peut être désigné comme utilisateur UNIX par défaut, créez le groupe par défaut et l'utilisateur UNIX par défaut, puis ajoutez l'utilisateur par défaut au groupe.
4. Le groupe par défaut reçoit généralement le nom de groupe « pcuser » Le GID attribué au groupe doit être `65534`.
   a. Créez le groupe par défaut :

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. Créez l'utilisateur par défaut et ajoutez l'utilisateur par défaut au groupe par défaut :

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. Vérifiez que l'utilisateur par défaut et le groupe par défaut sont correctement configurés :

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

5. Si l'utilisateur par défaut du serveur CIFS n'est pas configuré, effectuez les opérations suivantes :
   a. Configurez l'utilisateur par défaut :

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

   b. Vérifiez que l'utilisateur UNIX par défaut est configuré correctement :

```
vserver cifs options show -vserver <vserver_name>
```

6. Pour vérifier que le compte de l'ordinateur du serveur d'application correspond correctement à l'utilisateur par défaut, mappez un disque sur un partage résidant sur le SVM et confirmez que l'utilisateur Windows correspond au mappage utilisateur UNIX à l'aide de `vserver cifs session show` commande.

   Pour en savoir plus, `vserver cifs options` consultez le "Référence de commande ONTAP".

Exemple

Les commandes suivantes déterminent que l'utilisateur par défaut du serveur CIFS n'est pas défini, mais déterminent que le `pcuser` utilisateur et `pcuser` groupe existe. Le `pcuser` l'utilisateur est affecté comme utilisateur par défaut du serveur CIFS sur SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser
```

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Vérifier que le style de sécurité du volume root du SVM est défini sur NTFS

Pour assurer la continuité de l'activité pour Hyper-V et SQL Server sur SMB, des volumes doivent être créés avec le style de sécurité NTFS. Comme le style de sécurité du volume root est appliqué par défaut aux volumes créés sur la machine virtuelle de stockage (SVM), le style de sécurité du volume root doit être défini sur NTFS.

Description de la tâche

- Vous pouvez spécifier le style de sécurité du volume root au moment de la création de la SVM.
- Si le SVM n'est pas créé avec le volume root défini sur le style de sécurité NTFS, vous pouvez changer le style de sécurité plus tard en utilisant le `volume modify` commande.

Étapes

1. Déterminer la méthode de sécurité actuelle du volume root du SVM :

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. Si le volume racine n'est pas un volume de style de sécurité NTFS, remplacez le style de sécurité par NTFS :

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. Vérifier que le volume root du SVM est défini sur le style de sécurité NTFS :

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Exemple

Les commandes suivantes vérifient que le style de sécurité du volume root est NTFS sur le SVM vs1 :

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Vérifiez que les options requises pour les serveurs CIFS sont configurées

Vous devez vérifier que les options des serveurs CIFS requis sont activées et configurées conformément aux exigences de continuité de l'activité pour Hyper-V et SQL Server sur SMB.

Description de la tâche

- SMB 2.x et SMB 3.0 doivent être activés.
- L'allègement de la charge des copies (ODX) doit être activé pour que l'allègement de la performance des copies soit délesté.
- Les services VSS Shadow Copy doivent être activés si la solution Hyper-V sur SMB utilise des services de sauvegarde VSS distants (Hyper-V uniquement).

Étapes

1. Vérifier que les options des serveurs CIFS requis sont activées sur la machine virtuelle de stockage (SVM) :
   a. Définissez le niveau de privilège sur avancé :

      `set -privilege advanced`

   b. Saisissez la commande suivante :

      `vserver cifs options show -vserver *vserver_name*`

      Les options suivantes doivent être définies sur `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Hyper-V uniquement)
2. Si l'une des options n'est pas définie sur `true`, effectuez les opérations suivantes :
   a. Réglez-les sur `true` à l'aide du `vserver cifs options modify` commande.

b. Vérifiez que les options sont définies sur `true` à l'aide du `vserver cifs options show` commande.

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

Les commandes suivantes vérifient que les options requises pour la configuration Hyper-V sur SMB sont activées sur le SVM vs1. Dans l'exemple, l'allègement de la charge des copies (ODX) doit être activé pour répondre aux exigences des options.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

Configurez SMB Multichannel pour des performances et une redondance optimales

Depuis ONTAP 9.4, vous pouvez configurer SMB Multichannel pour fournir plusieurs connexions entre ONTAP et les clients dans une seule session SMB. L'amélioration du débit et de la tolérance aux pannes pour les configurations Hyper-V et SQL Server sur SMB.

Avant de commencer

La fonctionnalité SMB Multichannel ne peut être utilisée que lorsque les clients négocient avec SMB 3.0 ou une version ultérieure. SMB 3.0 et versions ultérieures sont activés par défaut sur le serveur ONTAP SMB.

Description de la tâche

Les clients SMB détectent et utilisent automatiquement plusieurs connexions réseau si une configuration

adéquate est identifiée sur le cluster ONTAP.

Le nombre de connexions simultanées dans une session SMB dépend des cartes réseau que vous avez déployées :

- **NIC 1G sur le client et le cluster ONTAP**

  Le client établit une connexion par carte réseau et lie la session à toutes les connexions.

- **Cartes réseau 10G et de capacité supérieure sur le client et le cluster ONTAP**

  Le client établit jusqu'à quatre connexions par carte réseau et lie la session à toutes les connexions. Le client peut établir des connexions sur plusieurs cartes réseau 10G et supérieures.

Vous pouvez également modifier les paramètres suivants (privilège avancé) :

- `-max-connections-per-session`

  Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut est 32 connexions.

  Si vous souhaitez activer plus de connexions que la configuration par défaut, vous devez effectuer des ajustements comparables à la configuration client, qui possède également une valeur par défaut de 32 connexions.

- `-max-lifs-per-session`

  Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut est 256 interfaces réseau.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Activez SMB Multichannel sur le serveur SMB :

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Vérifiez que ONTAP signale les sessions SMB multicanaux :

```
vserver cifs session show
```

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

L'exemple suivant affiche les informations relatives à toutes les sessions SMB, affichant plusieurs connexions pour une seule session :

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

L'exemple suivant affiche des informations détaillées sur une session SMB avec l'ID-session 1 :

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Création de volumes de données NTFS

Vous devez créer des volumes de données NTFS sur la machine virtuelle de stockage (SVM) avant de pouvoir configurer les partages disponibles en continu pour une utilisation avec Hyper-V ou SQL Server sur les serveurs d'applications SMB. Utilisez la fiche de configuration des volumes pour créer vos volumes de données.

Description de la tâche

Vous pouvez utiliser des paramètres facultatifs pour personnaliser un volume de données. Pour plus d'informations sur la personnalisation des volumes, reportez-vous à la section "Gestion du stockage logique".

Lorsque vous créez vos volumes de données, vous ne devez pas créer de points de jonction au sein d'un volume contenant les éléments suivants :

- Hyper-V Files pour lesquels ONTAP crée des clichés instantanés
- Fichiers de base de données SQL Server sauvegardés à l'aide de SQL Server

> Si vous créez par inadvertance un volume utilisant un style de sécurité mixte ou UNIX, vous ne pouvez pas le remplacer par un volume de style de sécurité NTFS, puis l'utiliser directement pour créer des partages disponibles en continu pour assurer la continuité de l'activité. La continuité de l'activité pour Hyper-V et SQL Server over SMB ne fonctionne pas correctement, sauf si les volumes utilisés dans la configuration sont créés en tant que volumes de sécurité NTFS.vous devez supprimer le volume et recréer le volume avec le style de sécurité NTFS, Vous pouvez également mapper le volume sur un hôte Windows et appliquer une liste de contrôle d'accès en haut du volume et propager la liste de contrôle d'accès à tous les fichiers et dossiers du volume.

Étapes

1. Créez le volume de données en entrant la commande appropriée :

Si vous souhaitez créer un volume dans un SVM où le root volume Security style…	Entrez la commande…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Pas NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path`

2. Vérifiez que la configuration de volume est correcte :

```
volume show -vserver vserver_name -volume volume_name
```

Créer des partages SMB disponibles en permanence

Une fois les volumes de données créés, vous pouvez créer les partages disponibles en continu que les serveurs d'applications utilisent pour accéder aux fichiers de la machine virtuelle et de configuration Hyper-V ainsi qu'aux fichiers de la base de données SQL Server. Vous devez utiliser la fiche de configuration du partage lors de la création des partages SMB.

Étapes

1. Afficher des informations sur les volumes de données existants et leurs Junction paths :

   volume show -vserver *vserver_name* -junction

2. Créer un partage SMB disponible en continu :

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - Vous pouvez éventuellement ajouter un commentaire à la configuration du partage.
   - Par défaut, la propriété de partage de fichiers hors ligne est configurée sur le partage et est définie sur `manual`.
   - ONTAP crée le partage avec l'autorisation de partage par défaut Windows de `Everyone` / `Full Control`.

3. Répétez l'étape précédente pour tous les partages de la fiche de configuration du partage.
4. Vérifiez que votre configuration est correcte à l'aide du `vserver cifs share show` commande.
5. Configurez les autorisations de fichiers NTFS sur les partages disponibles en permanence en mappant un lecteur sur chaque partage et en configurant les autorisations de fichiers à l'aide de la fenêtre **Propriétés Windows**.

Exemple

Les commandes suivantes créent un partage disponible en continu nommé « data2 » sur la machine virtuelle de stockage (SVM, précédemment appelé vServer) vs1. Les symlinks sont désactivés en définissant l' `-symlink` paramètre à `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Ajoutez le privilège SeSecurityPrivilege au compte d'utilisateur (pour SQL Server des partages SMB)

Le compte d'utilisateur de domaine utilisé pour installer le serveur SQL doit être affecté au privilège "`SteSecurityPrivilege" pour effectuer certaines actions sur le serveur CIFS qui exigent des privilèges non attribués par défaut aux utilisateurs de domaine.

Avant de commencer

Le compte de domaine utilisé pour installer SQL Server doit déjà exister.

Description de la tâche

Lors de l'ajout du privilège au compte du programme d'installation de SQL Server, ONTAP peut valider le compte en contactant le contrôleur de domaine. La commande peut échouer si ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Ajoutez le privilège "S`SecurityPrivilege" :

vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

La valeur pour le `-user-or-group-name` Paramètre est le nom du compte utilisateur de domaine utilisé pour l'installation de SQL Server.

2. Vérifiez que le privilège est appliqué au compte :

vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Exemple

La commande suivante ajoute le privilège "SteSecurityPrivilege" au compte du programme d'installation de SQL Server dans le domaine D'EXEMPLE pour la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

Configurer la profondeur du répertoire de copie « shadow » VSS (pour les partages Hyper-V sur SMB)

Vous pouvez également configurer la profondeur maximale des répertoires dans les partages SMB sur lesquels vous souhaitez créer des clichés instantanés. Ce paramètre est utile si vous souhaitez contrôler manuellement le niveau maximal de sous-répertoires sur lesquels ONTAP doit créer des clichés instantanés.

Avant de commencer

La fonction VSS Shadow Copy doit être activée.

Description de la tâche

La valeur par défaut est de créer des clichés instantanés pour un maximum de cinq sous-répertoires. Si la valeur est définie sur `0`, ONTAP crée des clichés instantanés pour tous les sous-répertoires.

> Bien que vous puissiez spécifier que la profondeur du répertoire du jeu de clichés instantanés inclut plus de cinq sous-répertoires ou tous les sous-répertoires, Microsoft a besoin que la création du jeu de clichés instantanés soit terminée dans les 60 secondes. La création d'un jeu de clichés instantanés échoue s'il ne peut pas être terminé dans ce délai. La profondeur du répertoire de copie en double que vous choisissez ne doit pas entraîner le dépassement du délai de création.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Définissez la profondeur du répertoire de copie fantôme VSS au niveau souhaité :

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
integer

vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Gérez les configurations Hyper-V et SQL Server sur SMB

Configurez les partages existants pour assurer la disponibilité sans interruption

Vous pouvez modifier les partages existants pour devenir des partages disponibles en permanence que les serveurs d'applications Hyper-V et SQL Server utilisent pour accéder sans interruption aux fichiers de configuration et des machines virtuelles Hyper-V et aux fichiers de base de données SQL Server.

Description de la tâche

Vous ne pouvez pas utiliser un partage existant comme partage disponible en continu pour assurer la continuité de l'activité avec des serveurs applicatifs sur SMB si le partage présente les caractéristiques suivantes :

- Si le `homedirectory` la propriété partager est définie sur ce partage
- Si le partage contient des symlinks ou des widelinks activés
- Si le partage contient des volumes sous la racine du partage

Vous devez vérifier que les deux paramètres de partage suivants sont correctement définis :

- Le `-offline-files` le paramètre est défini sur l'un ou l'autre `manual` (valeur par défaut) ou `none`.
- Les symlinks doivent être désactivés.

Les propriétés de partage suivantes doivent être configurées :

- `continuously-available`
- `oplocks`

Les propriétés de partage suivantes ne doivent pas être définies. S'ils sont présents dans la liste des propriétés de partage actuelles, ils doivent être supprimés du partage disponible en continu :

- `attributecache`
- `branchcache`

Étapes

1. Afficher les paramètres de partage actuels et la liste actuelle des propriétés de partage configurées :

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Si nécessaire, modifiez les paramètres de partage pour désactiver les liens symboliques et définissez les fichiers hors ligne sur manuel à l'aide de la `vserver cifs share modify` commande.
   - Vous pouvez désactiver les symlinks en définissant la valeur de l' `-symlink` paramètre à `""`.
   - Vous pouvez définir le `-offline-files` paramètre au réglage correct en spécifiant `manual`.
3. Ajoutez la `continuously-available` propriété de partage et, si nécessaire, la `oplocks` propriété de partage :

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   Si le `oplocks` la propriété de partage n'est pas déjà définie, vous devez l'ajouter avec `continuously-available` propriété de partage.

4. Supprimez toutes les propriétés de partage qui ne sont pas prises en charge sur les partages disponibles en continu :

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   Vous pouvez supprimer une ou plusieurs propriétés de partage en spécifiant les propriétés de partage avec une liste délimitée par des virgules.

5. Vérifiez que le `-symlink` et `-offline-files` les paramètres sont correctement réglés :

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Vérifiez que la liste des propriétés de partage configurées est correcte :

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Exemples

L'exemple suivant montre comment configurer un partage existant nommé « share1 » sur la machine virtuelle de stockage (SVM) « vs1 » pour les NDO avec un serveur d'application sur SMB :

- Les liens symboliques sont désactivés sur le partage en définissant le `-symlink` paramètre sur `""`.
- Le `-offline-file` le paramètre est modifié et défini sur `manual`.
- Le `continuously-available` la propriété de partage est ajoutée au partage.

- Le `oplocks` la propriété de partage figure déjà dans la liste des propriétés de partage ; il n'est donc pas nécessaire de l'ajouter.
- Le `attributecache` la propriété de partage est supprimée du partage.
- Le `browsable` La propriété de partage est facultative pour un partage disponible en continu utilisé pour les NDO avec des serveurs d'application sur SMB et est conservée comme une des propriétés de partage.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Activez ou désactivez les clichés instantanés VSS pour les sauvegardes Hyper-V sur SMB

Si vous utilisez une application de sauvegarde VSS pour sauvegarder les fichiers de machine virtuelle Hyper-V stockés sur des partages SMB, la copie Shadow VSS doit être activée. Vous pouvez désactiver la copie « shadow Copy VSS » si vous n'utilisez pas d'applications de sauvegarde « VSS Aware ». La valeur par défaut est d'activer la copie fantôme VSS.

Description de la tâche

Vous pouvez activer ou désactiver les clichés instantanés VSS à tout moment.

Étapes

1. Définissez le niveau de privilège sur avancé :

   `set -privilege advanced`

2. Effectuez l'une des opérations suivantes :

Si vous voulez que les clichés instantanés VSS soient…	Entrez la commande…
Activé	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true`**
Désactivé	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false`**

3. Retour au niveau de privilège admin :

   `set -privilege admin`

Exemple

Les commandes suivantes permettent d'activer les clichés instantanés VSS sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Utilisez les statistiques pour surveiller l'activité Hyper-V et SQL Server sur SMB

Déterminez les objets statistiques et les compteurs disponibles dans ONTAP

Avant d'obtenir des informations sur les statistiques de hachage CIFS, SMB, d'audit et de BranchCache, ainsi que sur les performances, vous devez connaître les objets et compteurs disponibles, à partir desquels vous pouvez obtenir des données.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Si vous voulez déterminer…	Entrer…
Les objets disponibles	`statistics catalog object show`
Objets spécifiques disponibles	`statistics catalog object show -object` *`object_name`*
Quels compteurs sont disponibles	`statistics catalog counter show -object` *`object_name`*

   En savoir plus sur `statistics catalog object show` et `statistics catalog counter show` dans le "Référence de commande ONTAP" .

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Exemples

La commande suivante affiche la description des objets statistiques sélectionnés relatifs à l'accès CIFS et SMB au cluster, comme s'il s'affiche au niveau de privilège avancé :

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

La commande suivante affiche des informations sur certains compteurs de `cifs` objet tel qu'il apparaît au niveau de privilège avancé :

> Cet exemple n'affiche pas tous les compteurs disponibles pour le `cifs` objet ; la sortie est tronquée.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Pour en savoir plus, `statistics start` consultez le "Référence de commande ONTAP".

Affiche les statistiques SMB dans ONTAP

Vous pouvez afficher différentes statistiques SMB pour surveiller les performances et diagnostiquer les problèmes.

Étapes

1. Utilisez le `statistics start` et en option `statistics stop` commandes pour collecter un échantillon de données.
2. Effectuez l'une des opérations suivantes :

Pour afficher les statistiques de…	Saisissez la commande suivante…
Toutes les versions de SMB	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x et SMB 3.0	**`statistics show -object smb2`**
Sous-système SMB du nœud	**`statistics show -object nblade_cifs`**

Informations associées

- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Vérifiez que la configuration permet la continuité de l'activité

Utilisez le contrôle de l'état de l'intégrité pour déterminer si l'état de la continuité de l'activité fonctionne correctement

Le contrôle de l'état fournit des informations relatives à l'état du système sur le cluster. Le contrôle de l'état surveille les configurations Hyper-V et SQL Server sur SMB pour assurer la continuité de l'activité pour les serveurs applicatifs. Si l'état est dégradé, vous pouvez afficher des détails sur le problème, y compris la cause probable et les actions de récupération recommandées.

Il y a plusieurs moniteurs de santé. ONTAP contrôle à la fois l'état global du système et l'état de santé des personnes. Le contrôle de l'état de connectivité des nœuds contient le sous-système CIFS-NDO Le contrôle dispose d'un ensemble de règles d'intégrité qui déclenchent des alertes si certaines conditions physiques peuvent entraîner des interruptions et, si une condition de perturbation existe, génère des alertes et fournit des informations sur les actions correctives à mettre en œuvre. Pour les configurations NDO sur SMB, des alertes sont générées dans les deux conditions suivantes :

L'ID d'alerte	Gravité	Condition
HaNotReadyCifsNdo_Alert	Majeur	Un ou plusieurs fichiers hébergés par un volume dans un agrégat du nœud ont été ouverts via un partage SMB disponible en continu, avec la promesse de persistance en cas de défaillance. Cependant, la relation de haute disponibilité avec le partenaire n'est pas configurée ou n'est pas saine.
NoStandbyLifCifsNdo_Alert	Mineur	Le SVM (Storage Virtual machine) transmet activement les données via SMB via un nœud, et les fichiers SMB sont ouverts de manière continue sur des partages disponibles. Cependant, son nœud partenaire n'expose pas de LIF de données actives pour la SVM.

Affichez l'état de l'opération sans interruption grâce à la surveillance de l'état du système

Vous pouvez utiliser le `system health` Commandes permettant d'afficher des informations relatives à l'état global du cluster et à l'état de santé du sous-système CIFS-NDO, de répondre aux alertes, de configurer les alertes futures et d'afficher des informations sur la configuration du contrôle de l'état.

Étapes

1. Surveillez l'état de l'état de santé en effectuant l'action appropriée :

Si vous voulez afficher…	Entrez la commande…
L'état d'intégrité du système, qui reflète l'état global des moniteurs d'état individuels	**system health status show**
Informations sur l'état de santé du sous-système CIFS-NDO	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Afficher des informations sur la configuration de la surveillance des alertes CIFS-NDO en effectuant les actions appropriées :

Pour afficher des informations sur…	Entrez la commande…
La configuration et l'état du contrôle de l'état du sous-système CIFS-NDO, tels que les nœuds contrôlés, l'état d'initialisation et l'état	**system health config show -subsystem CIFS-NDO**

Pour afficher des informations sur…	Entrez la commande…
CIFS-NDO signale qu'un contrôle de l'état peut générer	**system health alert definition show -subsystem CIFS-NDO**
Règles de contrôle de l'état de la CONTINUITÉ de l'ACTIVITÉ CIFS qui déterminent la date d'émission des alertes	**system health policy definition show -monitor node-connect**

Utilisez le `-instance` paramètre pour afficher des informations détaillées.

Exemples

Le résultat suivant affiche des informations sur l'état d'intégrité global du cluster et le sous-système CIFS-NDO :

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                  Subsystem: CIFS-NDO
                     Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                       Node: node2
  Subsystem Refresh Interval: 5m
```

Le résultat suivant affiche des informations détaillées sur la configuration et l'état du contrôle de l'état du sous-système CIFS-NDO :

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
            Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
            Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Vérifiez la configuration du partage SMB disponible en continu

Pour prendre en charge la continuité de l'activité, les partages SMB Hyper-V et SQL Server doivent être configurés en tant que partages disponibles en continu. En outre, vous devez vérifier certains autres paramètres de partage. Vérifiez que les partages sont correctement configurés pour assurer la continuité de l'activité des serveurs applicatifs en cas d'événements planifiés ou non.

Description de la tâche

Vous devez vérifier que les deux paramètres de partage suivants sont correctement définis :

- Le `-offline-files` le paramètre est défini sur l'un ou l'autre `manual` (valeur par défaut) ou `none`.
- Les symlinks doivent être désactivés.

Pour garantir la continuité de l'activité, les propriétés de partage suivantes doivent être définies :

- `continuously-available`
- `oplocks`

Les propriétés de partage suivantes ne doivent pas être définies :

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Étapes

1. Vérifiez que les fichiers hors ligne sont définis sur `manual` ou `disabled` et que les symlinks sont désactivés :

   vserver cifs shares show -vserver *vserver_name*

2. Vérifiez que les partages SMB sont configurés pour une disponibilité continue :

   vserver cifs shares properties show -vserver *vserver_name*

Exemples

L'exemple suivant présente le paramètre de partage d'un partage nommé « `sunre1' » sur la machine virtuelle de stockage (SVM, anciennement appelée Vserver) vs1. Les fichiers hors ligne sont définis sur `manual` et les symlinks sont désactivés (désignés par un tiret dans le `Symlink Properties` sortie de champ) :

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

L'exemple suivant affiche les propriétés de partage d'un partage nommé «`sunre1'» sur la SVM vs1 :

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

Vérifiez l'état du LIF

Même si vous configurez des SVM (Storage Virtual machines) avec des configurations Hyper-V et SQL Server over SMB pour avoir des LIF sur chaque nœud d'un cluster, au cours des opérations quotidiennes, certaines LIF peuvent être déplacées vers des ports sur un autre nœud. Vous devez vérifier le statut de la LIF et prendre les mesures correctives nécessaires.

Description de la tâche

Pour assurer la prise en charge transparente et sans interruption de l'activité, chaque nœud d'un cluster doit disposer d'au moins une LIF pour le SVM et toutes les LIF doivent être associées à un port de rattachement. Si certaines des LIFs configurées ne sont actuellement pas associées à leur port de base, vous devez résoudre un problème de port, puis rétablir les LIF sur leur port de base.

Étapes

1. Afficher les informations relatives aux LIFs configurées pour le SVM :

   network interface show -vserver *vserver_name*

   Dans cet exemple, « lites1 » n'est pas situé sur le port d'attache.

```
network interface show -vserver vs1
```

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node2      e0d
false
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

2. Si certaines des LIFs ne se trouvent pas sur leurs ports de home, effectuez les opérations suivantes :

   a. Pour chaque LIF, déterminez ce que le port de base de la LIF est :

   network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

   network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

   ```
   vserver lif  home-node  home-port
   ------- ---- ---------- ---------
   vs1     lif1 node1      e0d
   ```

   b. Pour chaque LIF, déterminez si le port de base de la LIF est active :

   network port show -node *node_name* -port *port* -fields port,link

   ```
   network port show -node node1 -port e0d -fields port,link
   ```

   ```
   node       port link
   ---------- ---- ----
   node1      e0d  up
   ```

   Dans cet exemple, « lie1 » doit être remigré vers son port d'origine, `node1:e0d`.

   Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

3. Si l'une des interfaces réseau du port de attache à laquelle les LIFs doivent être associées n'est pas dans `up` l'état, résolvez le problème afin que ces interfaces fonctionnent. Pour en savoir plus, `up` consultez le "Référence de commande ONTAP".

4. Si besoin, rerestaurez les LIF sur leurs ports de base :

   network interface revert -vserver *vserver_name* -lif *lif_name*

   network interface revert -vserver vs1 -lif lif1

   Pour en savoir plus, `network interface revert` consultez le "Référence de commande ONTAP".

5. Vérifier que chaque nœud du cluster dispose d'une LIF active pour le SVM :

   network interface show -vserver *vserver_name*

   network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Déterminez si les sessions SMB sont disponibles en continu

Affiche les informations relatives aux sessions SMB

Vous pouvez afficher des informations sur les sessions SMB établies, notamment la connexion SMB et l'ID de session ainsi que l'adresse IP du poste de travail à l'aide de la session. Vous pouvez afficher des informations sur la version du protocole SMB de la session et son niveau de protection disponible en continu, ce qui vous aide à déterminer si cette session prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher les informations de toutes les sessions de votre SVM sous forme récapitulative. Cependant, dans de nombreux cas, la quantité de sortie renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs :

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie des champs que vous choisissez.

  Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les sessions SMB établies.
- Vous pouvez utiliser le `-fields` ou le `-instance` paramètre seul ou associé à d'autres paramètres facultatifs.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
Pour toutes les sessions sur le SVM sous forme résumée	**vserver cifs session show -vserver *vserver_name***
Sur un ID de connexion spécifié	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
À partir d'une adresse IP de poste de travail spécifiée	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Sur une adresse IP LIF spécifiée	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Sur un nœud spécifié	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	D'un utilisateur Windows spécifié
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* Le format de `user_name` est `[domain]\user`.	Avec un mécanisme d'authentification spécifié

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism La valeur pour `-auth -mechanism` peut être l'une des suivantes : • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Avec une version de protocole spécifiée

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version La valeur pour `-protocol-version` peut être l'une des suivantes : • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Avec un niveau spécifié de protection disponible en continu

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
vserver cifs session show -vserver *vserver_name* -continuously -available *continuously_available_protection_level* La valeur pour `-continuously -available` peut être l'une des suivantes : • `No` • `Yes` • `Partial`	Avec un état de session de signature SMB spécifié

Exemples

La commande suivante affiche les informations relatives aux sessions sur le SVM vs1 établies à partir d'un poste de travail avec l'adresse IP 10.1.1.1 :

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

ouvert en continu

La commande suivante affiche des informations détaillées pour les sessions avec protection disponible en continu sur le SVM vs1. La connexion a été établie à l'aide du compte de domaine.

disponible

mais que

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                      Node: node1
                   Vserver: vs1
                Session ID: 1
              Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
             Windows User: DOMAIN\SERVER1$
                UNIX User: pcuser
              Open Shares: 1
               Open Files: 1
               Open Other: 0
            Connected Time: 10m 43s
                 Idle Time: 1m 19s
          Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

sont pas ouverts avec une protection disponible en continu.

La commande suivante affiche les informations relatives aux sessions sur une session utilisant SMB 3.0 et SMB Multichannel sur le SVM vs1. Dans l'exemple, l'utilisateur connecté à ce partage à un client SMB 3.0 en utilisant l'adresse IP du LIF ; par conséquent, le mécanisme d'authentification par défaut est NTLMv2. La connexion doit se faire à l'aide de l'authentification Kerberos pour se connecter à une protection disponible en

continu.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
             **Connection IDs: 3151272607,31512726078,3151272609
           Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
               Connected Time: 6m 22s
                    Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Affiche des informations sur les fichiers SMB ouverts dans ONTAP

Vous pouvez afficher des informations sur les fichiers SMB ouverts, notamment la connexion SMB et l'ID de session, le volume hôte, le nom du partage et le chemin du partage. Vous pouvez également afficher des informations sur le niveau de protection disponible en continu d'un fichier, ce qui permet de déterminer si un fichier ouvert est dans un état qui prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher des informations sur les fichiers ouverts dans une session SMB établie. Les informations affichées sont utiles lorsque vous devez déterminer les informations de session SMB pour des fichiers particuliers dans une session SMB.

Par exemple, si vous disposez d'une session SMB où certains fichiers ouverts sont ouverts avec une protection disponible en continu et certains ne sont pas ouverts avec une protection disponible en continu (valeur pour le `-continuously-available` champ dans `vserver cifs session show` la sortie de la commande est `Partial`), vous pouvez déterminer quels fichiers ne sont pas disponibles en continu à l'aide de cette commande.

Vous pouvez afficher les informations de tous les fichiers ouverts sur des sessions SMB établies sur des SVM (Storage Virtual machines) sous forme de récapitulatif à l'aide de `vserver cifs session file show` commande sans paramètres facultatifs.

Cependant, dans de nombreux cas, la quantité de production renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque vous souhaitez afficher des informations pour un petit sous-ensemble de fichiers ouverts uniquement.

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie sur les champs de votre choix.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les fichiers SMB ouverts.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
Sur le SVM sous forme résumée	**vserver cifs session file show -vserver *vserver_name***
Sur un nœud spécifié	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Sur un ID de fichier spécifié
vserver cifs session file show -vserver *vserver_name* -file-id integer	Sur un ID de connexion SMB spécifié
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Sur un ID de session SMB spécifié
vserver cifs session file show -vserver *vserver_name* -session-id integer	Sur l'agrégat d'hébergement spécifié
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	Sur le volume spécifié
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	Sur le partage SMB spécifié

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
vserver cifs session file show -vserver *vserver_name* -share *share_name*	Sur le chemin SMB spécifié
vserver cifs session file show -vserver *vserver_name* -path *path*	Avec le niveau spécifié de protection disponible en continu
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* La valeur pour `-continuously-available` peut être l'une des suivantes : • `No` • `Yes` Si l'état disponible en continu est de `No`, cela signifie que ces fichiers ouverts ne peuvent pas être rétablis sans interruption à partir du basculement et du rétablissement. Ils ne peuvent pas non plus récupérer d'une relocalisation générale entre les partenaires dans une relation de haute disponibilité.	Avec l'état reconnecté spécifié

D'autres paramètres facultatifs peuvent être utilisés pour affiner les résultats de sortie. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Exemples

L'exemple suivant affiche les informations sur les fichiers ouverts sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

L'exemple suivant affiche des informations détaillées sur les fichiers SMB ouverts avec l'ID de fichier 82 sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                Node: node1
             Vserver: vs1
             File ID: 82
       Connection ID: 104617
          Session ID: 1
           File Type: Regular
           Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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