Gérer l'accès aux fichiers via SMB

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/smb-admin/local-users-groups-concepts-concept.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Gérer l'accès aux fichiers via SMB . . . 1
Utilisez des utilisateurs et des groupes locaux pour l'authentification et l'autorisation . . . 1
Utilisation des utilisateurs et des groupes locaux par ONTAP . . . 1
Quels sont les privilèges locaux . . . 5
En savoir plus sur les groupes BUILTIN et les comptes d'administrateur local sur les serveurs ONTAP SMB . . . 7
Exigences relatives aux mots de passe des utilisateurs SMB ONTAP locaux . . . 7
Groupes BUILTIN prédéfinis et privilèges ONTAP SMB par défaut . . . 8
Activez ou désactivez la fonctionnalité utilisateurs et groupes locaux . . . 9
Gérez les comptes utilisateurs locaux . . . 12
Gérez des groupes locaux . . . 16
Gérer les privilèges locaux . . . 23
Configurer la vérification de la traverse de dérivation . . . 28
En savoir plus sur la configuration de la vérification de contournement de traversée ONTAP SMB . . . 28
Autoriser les utilisateurs ou les groupes à contourner la vérification de parcours du répertoire ONTAP SMB . . . 29
Interdire aux utilisateurs ou aux groupes de contourner la vérification de parcours du répertoire ONTAP SMB . . . 30
Affiche des informations sur la sécurité des fichiers et les stratégies d'audit . . . 31
En savoir plus sur l'affichage des politiques de sécurité et d'audit des fichiers ONTAP SMB . . . 31
Afficher des informations sur la sécurité des fichiers ONTAP SMB sur les volumes de style de sécurité NTFS . . . 32
Afficher des informations sur la sécurité des fichiers ONTAP SMB sur des volumes de style de sécurité mixte . . . 39
Afficher des informations sur la sécurité des fichiers ONTAP SMB sur les volumes de style de sécurité UNIX . . . 42
Commandes ONTAP pour afficher des informations sur les stratégies d'audit NTFS sur les volumes SMB FlexVol . . . 45
Commandes ONTAP pour afficher des informations sur les stratégies d'audit NFSv4 sur les volumes SMB FlexVol . . . 47
Découvrez comment afficher les informations sur la sécurité des fichiers SMB ONTAP et les politiques d'audit . . . 49
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 . . . 51
Commandes ONTAP pour la gestion de la sécurité des fichiers SMB NTFS, des stratégies d'audit NTFS et de Storage-Level Access Guard . . . 51
Commandes ONTAP pour définir la sécurité des fichiers et des dossiers SMB . . . 53
Découvrez les limites lors de l'utilisation des commandes ONTAP pour définir la sécurité des fichiers et des dossiers SMB . . . 53
Utilisez des descripteurs de sécurité pour appliquer la sécurité des fichiers et des dossiers ONTAP SMB . . . 53
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 . . . 54

Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande . . . 57
Configurez et appliquez des règles d'audit aux fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande . . . 65
En savoir plus sur la gestion des tâches de politique de sécurité ONTAP SMB . . . 73
Commandes ONTAP pour la gestion des descripteurs de sécurité NTFS sur les serveurs SMB . . . 74
Commandes ONTAP pour la gestion des entrées de contrôle d'accès NTFS DACL sur les serveurs SMB . . . 74
Commandes ONTAP pour la gestion des entrées de contrôle d'accès NTFS SACL sur les serveurs SMB . . . 75
Commandes ONTAP pour la gestion des politiques de sécurité SMB . . . 75
Commandes ONTAP pour la gestion des tâches de politique de sécurité SMB . . . 76
Commandes ONTAP pour la gestion des tâches de politique de sécurité SMB . . . 76
Configurez le cache des métadonnées pour les partages SMB . . . 77
En savoir plus sur la mise en cache des métadonnées ONTAP SMB . . . 77
Activer le cache de métadonnées ONTAP SMB . . . 77
Configurer la durée de vie des entrées du cache de métadonnées ONTAP SMB . . . 78
Gérer les verrous de fichier . . . 79
En savoir plus sur le verrouillage des fichiers SMB ONTAP entre les protocoles . . . 79
En savoir plus sur les bits en lecture seule ONTAP SMB . . . 80
La façon dont ONTAP diffère de Windows dans la gestion des verrous sur les composants de chemin de partage . . . 81
Afficher des informations sur les verrous SMB ONTAP . . . 81
Briser les verrous SMB ONTAP . . . 83
Surveiller l'activité des PME . . . 84
Afficher les informations de session ONTAP SMB . . . 84
Afficher des informations sur les fichiers SMB ONTAP ouverts . . . 88
Déterminer les statistiques, les objets et les compteurs disponibles sur les serveurs ONTAP SMB . . . 91
Afficher les statistiques ONTAP SMB . . . 95

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.
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`

Groupe prédéfini BUILTIN	Privilèges par défaut
`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`
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`*
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.

Les fonctions que vous recherchez…	Utilisez la commande…
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

Objet	Type d'accès	Droits d'accès	Où appliquer les autorisations
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 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`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les ACE existants dans les DACL NTFS	`vserver security file-directory ntfs dacl show`
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`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les stratégies de sécurité	`vserver security file-directory policy show`
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`

Les fonctions que vous recherchez…	Utilisez cette commande…
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.
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`
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`
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"

Informations sur le copyright

Copyright © 2026 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.