



Audit des événements NAS sur les SVM

ONTAP 9

NetApp
September 12, 2024

Sommaire

Audit des événements NAS sur les SVM	1
Audit et suivi de sécurité SMB et NFS	1
Fonctionnement de l'audit	2
Exigences et considérations relatives à l'audit	5
Restrictions quant à la taille des enregistrements d'audit sur les fichiers intermédiaires	6
Formats du journal des événements d'audit pris en charge	7
Affiche les journaux d'événements d'audit	7
Événements SMB pouvant être audités	8
Les événements d'accès aux fichiers et aux répertoires NFS pouvant être vérifiés	14
Planification de la configuration d'audit	15
Créer une configuration d'audit de fichier et de répertoire sur les SVM	22
Configuration des règles d'audit des fichiers et des dossiers	25
Affiche des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires	30
Les événements de modification de l'interface de ligne de commande peuvent être audités	37
Gérer les configurations d'audit	44
Dépanner les problèmes d'espace des volumes liés à l'audit et au staging	49

Audit des événements NAS sur les SVM

Audit et suivi de sécurité SMB et NFS

Grâce à ONTAP, vous pouvez utiliser les fonctions d'audit de l'accès aux fichiers disponibles pour les protocoles SMB et NFS, comme l'audit natif et la gestion des règles de fichiers via FPolicy.

Vous devez concevoir et implémenter l'audit des événements d'accès aux fichiers SMB et NFS dans les circonstances suivantes :

- L'accès de base aux fichiers des protocoles SMB et NFS a été configuré.
- Vous souhaitez créer et gérer une configuration d'audit à l'aide de l'une des méthodes suivantes :
 - Fonctionnalité ONTAP native
 - Serveurs FPolicy externes

Audit des événements NAS sur les SVM

L'audit des événements NAS est une mesure de sécurité qui vous permet de suivre et de consigner certains événements SMB et NFS sur des serveurs virtuels de stockage (SVM). Cela vous permet de suivre les problèmes de sécurité potentiels et de prouver toute violation de la sécurité. Vous pouvez également définir et auditer les stratégies d'accès central Active Directory pour voir quel serait le résultat de leur mise en œuvre.

Événements SMB

Vous pouvez auditer les événements suivants :

- Événements d'accès aux fichiers et aux dossiers SMB

Vous pouvez auditer les événements d'accès aux fichiers et aux dossiers SMB sur des objets stockés sur des volumes FlexVol appartenant aux SVM activés à l'audit.

- Événements de connexion et de déconnexion SMB

Vous pouvez auditer les événements de connexion et de déconnexion SMB des serveurs SMB sur les SVM.

- Événements d'activation de stratégie d'accès central

Vous pouvez auditer l'accès effectif des objets sur les serveurs SMB à l'aide des autorisations appliquées à l'aide des règles d'accès centrales proposées. L'audit par la mise en place de stratégies d'accès central vous permet de voir quels sont les effets des stratégies d'accès central avant leur déploiement.

L'audit du staging des règles d'accès central est configuré à l'aide des GPO Active Directory. Cependant, la configuration d'audit du SVM doit être configurée pour auditer les événements de staging des règles d'accès central.

Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, les événements de staging de stratégie d'accès central ne sont générés que si le contrôle d'accès dynamique est activé. Le contrôle d'accès dynamique est activé par le biais d'une option de serveur SMB. Elle n'est pas activée par défaut.

Événements NFS

Vous pouvez auditer les événements de fichier et de répertoire à l'aide des ACL NFSv4 sur des objets stockés sur les SVM.

Fonctionnement de l'audit

Concepts d'audit de base

Pour comprendre l'audit dans ONTAP, vous devez connaître certains concepts d'audit de base.

- **Fichiers de transfert**

Les fichiers binaires intermédiaires sur les nœuds individuels où les enregistrements d'audit sont stockés avant la consolidation et la conversion. Les fichiers de staging sont contenus dans des volumes de staging.

- **Volume de transfert**

Volume dédié créé par ONTAP pour stocker les fichiers de transfert. Il existe un volume intermédiaire par agrégat. Les volumes de sauvegarde sont partagés par toutes les machines virtuelles de stockage (SVM) activées par les audits, ce qui permet de stocker des enregistrements d'audit de l'accès aux données pour les volumes de données de cet agrégat particulier. Les enregistrements d'audit de chaque SVM sont stockés dans un répertoire distinct dans le volume intermédiaire.

Les administrateurs de cluster peuvent afficher des informations sur les volumes intermédiaires, mais la plupart des autres opérations de volume ne sont pas autorisées. Seul ONTAP peut créer des volumes intermédiaires. ONTAP attribue automatiquement un nom aux volumes intermédiaires. Tous les noms de volumes de staging commencent par MDV_aud_ Suivi par l'UUID de l'agrégat contenant ce volume intermédiaire (par exemple : MDV_aud_1d0131843d4811e296fc123478563412.)

- **Volumes système**

Un volume FlexVol qui contient des métadonnées spéciales, telles que les métadonnées pour les journaux d'audit des services de fichiers. Le SVM d'administration possède des volumes système qui sont visibles sur l'ensemble du cluster. Les volumes de staging sont un type de volume système.

- **Tâche de consolidation**

Tâche créée lorsque l'audit est activé. Cette tâche longue durée sur chaque SVM enregistre les enregistrements d'audit dans des fichiers intermédiaires dans les nœuds membres de la SVM. Cette tâche fusionne les enregistrements d'audit dans un ordre chronologique trié, puis les convertit en un format de journal d'événements lisible par l'utilisateur spécifié dans la configuration d'audit, soit au format de fichier EVTX soit au format XML. Les journaux d'événements convertis sont stockés dans le répertoire du journal des événements d'audit spécifié dans la configuration d'audit du SVM.

Fonctionnement du processus d'audit ONTAP

Le processus d'audit de ONTAP est différent du processus d'audit de Microsoft. Avant de configurer l'audit, vous devez comprendre le fonctionnement du processus d'audit ONTAP.

Les enregistrements d'audit sont initialement stockés dans des fichiers intermédiaires binaires sur des nœuds individuels. En cas d'audit sur un SVM, chaque nœud membre conserve les fichiers temporaires pour ce SVM. Ils sont régulièrement consolidés et convertis en journaux d'événements lisibles par l'utilisateur, qui sont stockés dans le répertoire du journal des événements d'audit de la SVM.

Processus lors de l'audit sur un SVM

L'audit peut uniquement être activé sur les SVM. Lorsque l'administrateur du stockage active l'audit sur le SVM, le sous-système d'audit vérifie si les volumes intermédiaires sont présents. Un volume de transfert doit exister pour chaque agrégat qui contient des volumes de données détenus par le SVM. Le sous-système d'audit crée tous les volumes de staging nécessaires s'ils n'existent pas.

Le sous-système d'audit effectue également d'autres tâches préalables avant l'activation de l'audit :

- Le sous-système d'audit vérifie que le chemin du répertoire des journaux est disponible et ne contient pas de symlinks.

Le répertoire log doit déjà exister sous la forme d'un chemin au sein du namespace du SVM. Il est recommandé de créer un nouveau volume ou qtree pour conserver les fichiers journaux d'audit. Le sous-système d'audit n'affecte pas d'emplacement de fichier journal par défaut. Si le chemin d'accès au répertoire du journal spécifié dans la configuration d'audit n'est pas un chemin valide, la création de la configuration d'audit échoue avec le message `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` erreur.

La création de la configuration échoue si le répertoire existe mais contient des symlinks.

- L'audit planifie la tâche de consolidation.

Une fois cette tâche planifiée, l'audit est activé. La configuration d'audit du SVM et les fichiers journaux sont conservés lors d'un redémarrage ou si les serveurs NFS ou SMB sont arrêtés ou redémarrés.

Consolidation du journal des événements

La consolidation des journaux est une tâche planifiée qui s'exécute régulièrement jusqu'à ce que l'audit soit désactivé. Lorsque l'audit est désactivé, la tâche de consolidation vérifie que tous les journaux restants sont consolidés.

Audit garanti

L'audit est garanti par défaut. ONTAP garantit l'enregistrement de tous les événements d'accès aux fichiers vérifiables (tels que spécifiés par les ACL de règles d'audit configurées), même si un nœud n'est pas disponible. Une opération de fichier demandé ne peut pas être effectuée tant que l'enregistrement d'audit pour cette opération n'est pas enregistré dans le volume intermédiaire du stockage persistant. Si les enregistrements d'audit ne peuvent pas être archivés sur le disque dans les fichiers de transfert, soit en raison d'un espace insuffisant, soit en raison d'autres problèmes, les opérations client sont refusées.



Un administrateur ou un utilisateur de compte disposant d'un niveau de privilège peut contourner l'opération de journalisation d'audit de fichiers en utilisant le SDK de gestion NetApp ou les API REST. Vous pouvez déterminer si des actions ont été effectuées à l'aide du SDK de gestion NetApp ou des API REST en consultant les journaux de l'historique des commandes stockés dans le `audit.log` fichier.

Pour plus d'informations sur les journaux d'audit de l'historique des commandes, reportez-vous à la section « gestion de la journalisation d'audit pour les activités de gestion » du ["Administration du système"](#).

Processus de consolidation lorsqu'un nœud n'est pas disponible

Si un nœud contenant des volumes appartenant à un SVM dont l'audit est activé n'est pas disponible, le comportement de la tâche de consolidation d'audit dépend si le partenaire SFO (ou le partenaire HA dans le cas d'un cluster à deux nœuds) est disponible :

- Si le volume intermédiaire est disponible via le partenaire SFO, les volumes intermédiaires déclarés en dernier sur le nœud sont analysés et la consolidation s'effectue normalement.
- Si le partenaire SFO n'est pas disponible, la tâche crée un fichier journal partiel.

Lorsqu'un nœud est inaccessible, la tâche de consolidation consolide les enregistrements d'audit depuis les autres nœuds disponibles de ce SVM. Pour identifier qu'elle n'est pas terminée, la tâche ajoute le suffixe `.partial` au nom du fichier consolidé.

- Une fois le nœud indisponible disponible, les enregistrements d'audit de ce nœud sont consolidés avec les enregistrements d'audit des autres nœuds à ce moment-là.
- Tous les enregistrements d'audit sont conservés.

Rotation du journal des événements

Les fichiers journaux d'événements d'audit sont pivotés lorsqu'ils atteignent une taille de journal de seuil configurée ou dans une planification configurée. Lorsqu'un fichier journal d'événements est pivoté, la tâche de consolidation planifiée renomme d'abord le fichier actif converti en fichier d'archive horodaté, puis crée un nouveau fichier journal d'événements converti actif.

Processus lorsque l'audit est désactivé sur le SVM

Lorsque l'audit est désactivé sur le SVM, la tâche de consolidation est déclenchée une dernière fois. Tous les enregistrements d'audit en attente et enregistrés sont consignés dans un format lisible par l'utilisateur. Les journaux d'événements stockés dans le répertoire du journal des événements ne sont pas supprimés lorsque l'audit est désactivé sur le SVM et sont disponibles pour l'affichage.

Une fois que tous les fichiers de données intermédiaires existants pour ce SVM sont consolidés, la tâche de consolidation est supprimée de la planification. La désactivation de la configuration d'audit de la SVM ne supprime pas la configuration d'audit. Un administrateur du stockage peut réactiver les audits à tout moment.

La tâche de consolidation d'audit, qui est créée lorsque l'audit est activé, surveille la tâche de consolidation et la recrée si la tâche de consolidation se ferme en raison d'une erreur. Les utilisateurs ne peuvent pas supprimer le travail de consolidation d'audit.

Exigences et considérations relatives à l'audit

Avant de configurer et d'activer l'audit sur votre serveur virtuel de stockage (SVM), vous devez connaître certaines exigences et considérations.

- Le nombre maximal de SVM pouvant être auditer dépend de votre version de ONTAP :

Version ONTAP	Maximum
9.8 et versions antérieures	50
9.9.1 et versions ultérieures	400

- L'audit n'est pas lié aux licences SMB ou NFS.

Vous pouvez configurer et activer l'audit même si les licences SMB et NFS ne sont pas installées sur le cluster.

- L'audit NFS prend en charge les ACE de sécurité (type U).
- Pour l'audit NFS, il n'y a pas de mappage entre les bits de mode et les ACE d'audit.

Lors de la conversion des ACL en bits de mode, les ACE d'audit sont ignorés. Lors de la conversion des bits de mode en listes de contrôle d'accès, les ACE d'audit ne sont pas générés.

- Le répertoire spécifié dans la configuration d'audit doit exister.

S'il n'existe pas, la commande de création de la configuration d'audit échoue.

- Le répertoire spécifié dans la configuration d'audit doit satisfaire aux exigences suivantes :

- Le répertoire ne doit pas contenir de liens symboliques.

Si le répertoire spécifié dans la configuration d'audit contient des liens symboliques, la commande permettant de créer la configuration d'audit échoue.

- Vous devez spécifier le répertoire à l'aide d'un chemin d'accès absolu.

Vous ne devez pas spécifier de chemin relatif, par exemple, `/vs1/././`.

- L'audit dépend de l'espace disponible dans les volumes de transfert.

Vous devez connaître et planifier l'espace suffisant pour les volumes intermédiaires des agrégats contenant des volumes audités.

- L'audit dépend de l'espace disponible dans le volume contenant le répertoire dans lequel les journaux d'événements convertis sont stockés.

Vous devez connaître et disposer d'un plan vous assurant que l'espace disponible dans les volumes utilisés pour stocker les journaux d'événements est suffisant. Vous pouvez spécifier le nombre de journaux d'événements à conserver dans le répertoire d'audit en utilisant le `-rotate-limit` paramètre lors de la création d'une configuration d'audit, qui peut vous aider à vérifier que l'espace disponible pour les journaux d'événements du volume est suffisant.

- Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, le contrôle d'accès dynamique doit être activé

pour générer des événements de staging de stratégie d'accès central.

Le contrôle d'accès dynamique n'est pas activé par défaut.

Considérations relatives à l'espace des agrégats lors de l'activation des audits

Lorsqu'une configuration d'audit est créée et que l'audit est activé sur au moins une machine virtuelle de stockage (SVM) du cluster, le sous-système d'audit crée des volumes intermédiaires sur tous les agrégats existants et sur tous les nouveaux agrégats créés. Vous devez tenir compte de certaines considérations relatives à l'espace des agrégats lorsque vous activez l'audit sur le cluster.

La création d'un volume de transfert peut échouer en raison de l'absence de disponibilité de l'espace dans un agrégat. Cela peut se produire si vous créez une configuration d'audit et que les agrégats existants ne disposent pas d'espace suffisant pour contenir le volume d'activation.

Assurez-vous de disposer de suffisamment d'espace sur les agrégats existants pour les volumes intermédiaires avant d'activer l'audit sur une SVM.

Restrictions quant à la taille des enregistrements d'audit sur les fichiers intermédiaires

La taille d'un enregistrement d'audit sur un fichier temporaire ne peut pas être supérieure à 32 Ko.

Lorsque de grands enregistrements d'audit peuvent se produire

De grands enregistrements d'audit peuvent se produire lors de l'audit de gestion dans l'un des scénarios suivants :

- Ajout ou suppression d'utilisateurs à ou à partir de groupes comportant un grand nombre d'utilisateurs.
- Ajout ou suppression d'une liste de contrôle d'accès de partage de fichiers (ACL) sur un partage de fichiers avec un grand nombre d'utilisateurs de partage de fichiers.
- Autres scénarios.

Désactivez l'audit de gestion pour éviter ce problème. Pour ce faire, modifiez la configuration de l'audit et supprimez ce qui suit de la liste des types d'événements d'audit :

- partage de fichiers
- compte utilisateur
- groupe-de-sécurité
- autorisation-stratégie-modification

Après suppression, ils ne seront pas audités par le sous-système d'audit des services de fichiers.

Les effets des enregistrements d'audit trop importants

- Si la taille d'un enregistrement d'audit est trop importante (plus de 32 Ko), l'enregistrement d'audit n'est pas créé et le sous-système d'audit génère un message de système de gestion des événements (EMS) similaire à ce qui suit :


```
File Services Auditing subsystem failed the operation or truncated an audit record because it was greater than max_audit_record_size value. Vserver UUID=%s, event_id=%u, size=%u
```

Si l'audit est garanti, l'opération de fichier échoue car son enregistrement d'audit ne peut pas être créé.

- Si la taille de l'enregistrement d'audit est supérieure à 9,999 octets, le même message EMS est affiché. Un enregistrement d'audit partiel est créé avec une valeur de clé plus élevée manquante.
- Si l'enregistrement d'audit dépasse 2,000 caractères, le message d'erreur suivant s'affiche au lieu de la valeur réelle :

```
The value of this field was too long to display.
```

Formats du journal des événements d'audit pris en charge

Les formats de fichiers pris en charge pour les journaux d'événements d'audit convertis sont EVTX et XML formats de fichiers.

Vous pouvez spécifier le type de format de fichier lorsque vous créez la configuration d'audit. Par défaut, ONTAP convertit les journaux binaires en EVTX format de fichier.

Affiche les journaux d'événements d'audit

Vous pouvez utiliser les journaux d'événements d'audit pour déterminer si vous disposez de la sécurité adéquate des fichiers et si des tentatives d'accès incorrectes aux fichiers et aux dossiers ont été effectuées. Vous pouvez afficher et traiter les journaux d'événements d'audit enregistrés dans le EVTX ou XML formats de fichiers.

- EVTX format de fichier

Vous pouvez ouvrir le converti EVTX L'événement d'audit se connecte en tant que fichiers enregistrés à l'aide de Microsoft Event Viewer.

Vous pouvez utiliser deux options pour afficher les journaux d'événements à l'aide de l'Observateur d'événements :

- Vue générale

Les informations communes à tous les événements sont affichées pour l'enregistrement d'événement. Dans cette version de ONTAP, les données spécifiques à l'événement pour l'enregistrement d'événement ne sont pas affichées. Vous pouvez utiliser la vue détaillée pour afficher des données spécifiques à un événement.

- Vue détaillée

Une vue conviviale et une vue XML sont disponibles. La vue conviviale et la vue XML affichent à la fois les informations communes à tous les événements et les données spécifiques à l'événement pour l'enregistrement d'événement.

- XML format de fichier

Vous pouvez afficher et traiter XML auditer les journaux d'événements sur des applications tierces prenant en charge le XML format de fichier. Les outils de visualisation XML peuvent être utilisés pour afficher les journaux d'audit à condition que vous ayez le schéma XML et des informations sur les définitions des champs XML. Pour plus d'informations sur le schéma XML et les définitions, reportez-vous au "[Référence de schéma d'audit ONTAP](#)".

Mode d'affichage des journaux d'audit actifs à l'aide de l'Observateur d'événements

Si le processus de consolidation d'audit est exécuté sur le cluster, le processus de consolidation ajoute de nouveaux enregistrements au fichier journal d'audit actif pour les serveurs virtuels de stockage (SVM) activés par audit. Ce journal d'audit actif est accessible et ouvert via un partage SMB dans Microsoft Event Viewer.

En plus d'afficher les enregistrements d'audit existants, Event Viewer dispose d'une option de rafraîchissement qui vous permet d'actualiser le contenu dans la fenêtre de la console. Si les journaux nouvellement ajoutés peuvent être consultés dans l'Observateur d'événements, cela dépend de l'activation ou non des oplocks sur le partage utilisé pour accéder au journal d'audit actif.

Paramètre oplocks sur le partage	Comportement
Activé	Event Viewer ouvre le journal qui contient les événements qui y sont écrits jusqu'à ce point dans le temps. L'opération d'actualisation n'actualise pas le journal avec de nouveaux événements ajoutés par le processus de consolidation.
Désactivé	Event Viewer ouvre le journal qui contient les événements qui y sont écrits jusqu'à ce point dans le temps. L'opération d'actualisation actualise le journal avec de nouveaux événements ajoutés par le processus de consolidation.



Ces informations ne s'appliquent que pour EVTX journaux d'événements. XML Les journaux d'événements peuvent être affichés via SMB dans un navigateur ou via NFS à l'aide d'un éditeur ou d'un visualiseur XML.

Événements SMB pouvant être audités

Événements SMB pouvant être audités

ONTAP peut auditer certains événements SMB, notamment certains événements d'accès aux fichiers et aux dossiers, certains événements de connexion et de déconnexion, et des événements d'activation des règles d'accès central. Savoir quels événements d'accès peuvent être audités est utile pour interpréter les résultats des journaux d'événements.

Les événements SMB supplémentaires suivants peuvent être audités dans ONTAP 9.2 et versions ultérieures :

ID D'ÉVÉNEMENT (EVT/EVTX)	Événement	Description	Catégorie
---------------------------	-----------	-------------	-----------

4670	Les autorisations d'objet ont été modifiées	ACCÈS AUX OBJETS : autorisations modifiées.	Accès aux fichiers
4907	Les paramètres d'audit d'objet ont été modifiés	ACCÈS À L'OBJET : paramètres d'audit modifiés.	Accès aux fichiers
4913	La stratégie d'accès à Object Central a été modifiée	ACCÈS À L'OBJET : BOUCHON MODIFIÉ.	Accès aux fichiers

Les événements SMB suivants peuvent être audités dans ONTAP 9.0 et versions ultérieures :

ID D'ÉVÉNEMENT (EVT/EVTX)	Événement	Description	Catégorie
540/4624	Un compte a été connecté avec succès	CONNEXION/DÉCONNEXION : connexion réseau (SMB).	Connexion et déconnexion
529/4625	Impossible de se connecter à un compte	CONNEXION/DÉCONNEXION : nom d'utilisateur inconnu ou mot de passe incorrect.	Connexion et déconnexion
530/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE de SESSION : restriction de l'heure de connexion au compte.	Connexion et déconnexion
531/4625	Impossible de se connecter à un compte	CONNEXION/DÉCONNEXION : compte actuellement désactivé.	Connexion et déconnexion
532/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : le compte utilisateur a expiré.	Connexion et déconnexion
533/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : l'utilisateur ne peut pas se connecter à cet ordinateur.	Connexion et déconnexion
534/4625	Impossible de se connecter à un compte	OUVERTURE DE SESSION/DÉCONNEXION : l'utilisateur n'a pas accordé de type de connexion ici.	Connexion et déconnexion
535/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : le mot de passe de l'utilisateur a expiré.	Connexion et déconnexion

537/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE de SESSION : la connexion a échoué pour des raisons autres que ci-dessus.	Connexion et déconnexion
539/4625	Impossible de se connecter à un compte	OUVERTURE DE SESSION/DÉCONNEXION : compte verrouillé.	Connexion et déconnexion
538/4634	Un compte a été déconnecté	OUVERTURE/FERMETURE DE SESSION : déconnexion de l'utilisateur local ou réseau.	Connexion et déconnexion
560/4656	Ouvrir objet/Créer objet	ACCÈS EN MODE OBJET : objet (fichier ou répertoire) ouvert.	Accès aux fichiers
563/4659	Ouvrez l'objet avec l'intention de supprimer	ACCÈS AUX OBJETS : un descripteur d'objet (fichier ou répertoire) a été demandé avec l'intention de supprimer.	Accès aux fichiers
564/4660	Supprimer l'objet	ACCÈS OBJET : supprimer l'objet (fichier ou répertoire). ONTAP génère cet événement lorsqu'un client Windows tente de supprimer l'objet (fichier ou répertoire).	Accès aux fichiers
567/4663	Lire objet/Ecrire objet/obtenir attributs d'objet/définir attributs d'objet	ACCÈS AUX OBJETS : tentative d'accès aux objets (lecture, écriture, obtenir l'attribut, définir l'attribut). Remarque : pour cet événement, ONTAP vérifie uniquement la première opération de lecture SMB et la première opération d'écriture SMB (succès ou échec) sur un objet. Cela empêche ONTAP de créer un nombre excessif d'entrées de journal lorsqu'un seul client ouvre un objet et effectue de nombreuses opérations de lecture ou d'écriture successives sur le même objet.	Accès aux fichiers
NA/4664	Lien dur	ACCÈS À L'OBJET : tentative de création d'un lien dur.	Accès aux fichiers

NA/4818	La politique d'accès central proposée n'accorde pas les mêmes autorisations d'accès que la politique d'accès central actuelle	ACCÈS AUX OBJETS : transfert de la stratégie d'accès central.	Accès aux fichiers
Na/NA - ID d'événement Data ONTAP 9999	Renommer l'objet	ACCÈS OBJET : objet renommé. Il s'agit d'un événement ONTAP. Windows ne prend actuellement pas en charge cet événement en tant qu'événement unique.	Accès aux fichiers
Na/NA Data ONTAP ID d'événement 9998	Dissocier l'objet	ACCÈS AUX OBJETS : objet non lié. Il s'agit d'un événement ONTAP. Windows ne prend actuellement pas en charge cet événement en tant qu'événement unique.	Accès aux fichiers

Informations supplémentaires sur l'événement 4656

Le `HandleID` dans l'audit XML event contient le descripteur de l'objet (fichier ou répertoire) accédé. Le `HandleID` La balise de l'événement EVT 4656 contient des informations différentes selon que l'événement ouvert permet de créer un nouvel objet ou d'ouvrir un objet existant :

- Si l'événement ouvert est une demande ouverte pour créer un nouvel objet (fichier ou répertoire), le `HandleID` La balise dans l'événement XML d'audit affiche un vide `HandleID` (par exemple : `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>`).

Le `HandleID` Est vide car la demande OUVERTE (pour la création d'un nouvel objet) est auditée avant la création réelle de l'objet et avant qu'un descripteur n'existe. Les événements audités suivants pour le même objet ont le bon descripteur d'objet dans le `HandleID` balise :

- Si l'événement ouvert est une demande ouverte d'ouverture d'un objet existant, l'événement d'audit aura le descripteur affecté à cet objet dans le `HandleID` balise (par exemple : `<Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>`).

Déterminez le chemin complet de l'objet vérifié

Le chemin d'accès de l'objet imprimé dans `<ObjectName>` la balise d'un enregistrement d'audit contient le nom du volume (entre parenthèses) et le chemin relatif de la racine du volume contenant. Si vous voulez déterminer le chemin complet de l'objet vérifié, y compris le chemin de jonction, il y a certaines étapes que vous devez suivre.

Étapes

1. Déterminez ce que correspond le nom du volume et le chemin relatif de l'objet vérifié en consultant le `<ObjectName>` balise dans l'événement d'audit.

Dans cet exemple, le nom du volume est "data1" et le chemin relatif vers le fichier est `/dir1/file.txt:`

```
<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
```

2. En utilisant le nom du volume déterminé à l'étape précédente, déterminez ce qu'est la Junction path du volume contenant l'objet vérifié :

Dans cet exemple, le nom du volume est "data1" et le chemin de jonction du volume contenant l'objet vérifié est /data/data1:

```
volume show -junction -volume data1
```

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Language	Active		
vs1	data1	en_US.UTF-8	true	/data/data1	RW_volume

3. Déterminez le chemin d'accès complet à l'objet vérifié en ajoutant le chemin d'accès relatif trouvé dans le <ObjectName> marquez la junction path du volume.

Dans cet exemple la Junction path du volume :

```
/data/data1/dir1/file.txt
```

Considérations relatives à l'audit des liens symlinks et des liens matériels

Il y a certaines considérations que vous devez garder à l'esprit lors de l'audit des liens symlinks et des liens matériels.

Un enregistrement d'audit contient des informations sur l'objet en cours d'audit, y compris le chemin d'accès à l'objet vérifié, qui est identifié dans le `ObjectName` balise : Vous devez savoir comment les chemins pour les liens symlinks et les liens rigides sont enregistrés dans le `ObjectName` balise :

Symlinks

Un symlink est un fichier avec un inode séparé qui contient un pointeur vers l'emplacement d'un objet de destination, appelé cible. Lors de l'accès à un objet via une symlink, ONTAP interprète automatiquement la symlink et suit le chemin canonique réel de protocole indépendant vers l'objet cible dans le volume.

Dans l'exemple de sortie suivant, il y a deux symlinks, tous deux pointant vers un fichier nommé `target.txt`. Un des symlinks est un symlink relatif et un est un symlink absolu. Si l'un des symlinks est vérifié, le `ObjectName` la balise de l'événement d'audit contient le chemin d'accès au fichier `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Liens matériels

Un lien dur est une entrée de répertoire qui associe un nom à un fichier existant sur un système de fichiers. Le lien matériel pointe vers l'emplacement d'inode du fichier d'origine. De la même manière que ONTAP interprète les symlinks, ONTAP interprète le lien rigide et suit le chemin canonique réel vers l'objet cible dans le volume. Lorsque l'accès à un objet de lien rigide est vérifié, l'événement d'audit enregistre ce chemin canonique absolu dans l' `ObjectName` marquez plutôt que le chemin du lien dur.

Points à prendre en compte lors de l'audit des autres flux de données NTFS

Vous devez garder à l'esprit certaines considérations lors de l'audit des fichiers avec les autres flux de données NTFS.

L'emplacement d'un objet vérifié est enregistré dans un enregistrement d'événement à l'aide de deux balises, le `ObjectName` tag (le chemin) et le `HandleID` étiquette (la poignée). Pour identifier correctement les demandes de flux en cours de journalisation, vous devez connaître les enregistrements ONTAP dans ces champs pour les flux de données alternatifs NTFS :

- EVTX ID : 4656 événements (ouvrir et créer des événements d'audit)
 - Le chemin du flux de données secondaire est enregistré dans le `ObjectName` balise :
 - La poignée du flux de données alternatif est enregistrée dans le `HandleID` balise :
- EVTX ID : 4663 événements (tous les autres événements d'audit, tels que lecture, écriture, getattr, etc.)
 - Le chemin du fichier de base, et non le flux de données secondaire, est enregistré dans le `ObjectName` balise :
 - La poignée du flux de données alternatif est enregistrée dans le `HandleID` balise :

Exemple

L'exemple suivant illustre comment identifier EVTX ID : 4663 événements pour d'autres flux de données à l'aide de l' `HandleID` balise : Même si le `ObjectName` la balise (chemin) enregistrée dans l'événement d'audit de lecture correspond au chemin du fichier de base, le `HandleID` la balise peut être utilisée pour identifier l'événement comme enregistrement d'audit pour le flux de données secondaire.

Les noms des fichiers de flux prennent le format `base_file_name:stream_name`. Dans cet exemple, le `dir1` le répertoire contient un fichier de base avec un autre flux de données ayant les chemins suivants :

```
/dir1/file1.txt  
/dir1/file1.txt:stream1
```



La sortie dans l'exemple d'événement suivant est tronquée comme indiqué ; la sortie n'affiche pas toutes les balises de sortie disponibles pour les événements.

Pour un EVTX ID 4656 (événement d'audit ouvert), la sortie de l'enregistrement d'audit du flux de données secondaire enregistre le nom du flux de données alternatif dans le `ObjectName` tag :

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\(data1\);/dir1/file1.txt:stream1</Data>
  **
  [...]
</EventData>
</Event>
- <Event>

```

Pour un EVT-X ID 4663 (lecture d'événement d'audit), la sortie de l'enregistrement d'audit du même flux de données alternatif enregistre le nom du fichier de base dans le `ObjectName` marqué, cependant, la poignée dans le `HandleID` tag est la poignée du flux de données alternatif et peut être utilisé pour mettre en corrélation cet événement avec l'autre flux de données :

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\(data1\);/dir1/file1.txt</Data> **
  [...]
</EventData>
</Event>
- <Event>

```

Les événements d'accès aux fichiers et aux répertoires NFS pouvant être vérifiés

ONTAP peut auditer certains événements d'accès aux fichiers et aux répertoires NFS.

Savoir quels événements d'accès peuvent être audités est utile lors de l'interprétation des résultats des journaux d'événements d'audit convertis.

Vous pouvez auditer les événements d'accès au répertoire et aux fichiers NFS suivants :

- LECTURE
- LA TRANSPARENCE
- FERMER
- READDIR
- ÉCRITURE
- DÉFINIR
- CRÉATION
- LIEN
- OPENATTR
- DÉPOSER
- GETATTR
- LA VÉRIFICATION
- NVÉRIFIER
- RENOMMER

Pour effectuer un audit fiable des événements DE RENOMMAGE NFS, vous devez définir des ACE d'audit sur les répertoires au lieu de fichiers car les autorisations de fichier ne sont pas vérifiées pour une opération DE RENOMMAGE si les autorisations de répertoire sont suffisantes.

Planification de la configuration d'audit

Avant de configurer l'audit sur les SVM (Storage Virtual machines), vous devez connaître les options de configuration disponibles et planifier les valeurs à définir pour chaque option. Ces informations peuvent vous aider à configurer la configuration d'audit qui répond aux besoins de votre entreprise.

Certains paramètres de configuration sont communs à toutes les configurations d'audit.

En outre, certains paramètres peuvent être utilisés pour spécifier les méthodes utilisées lors de la rotation des journaux d'audit consolidés et convertis. Vous pouvez spécifier l'une des trois méthodes suivantes lorsque vous configurez l'audit :

- Rotation des journaux en fonction de la taille du journal

Il s'agit de la méthode par défaut utilisée pour faire pivoter les journaux.

- Rotation des journaux en fonction d'un planning
- Rotation des journaux en fonction de la taille du journal et du planning (quel que soit l'événement qui se produit en premier)



Au moins une des méthodes de rotation du log doit toujours être définie.

Paramètres communs à toutes les configurations d'audit

Vous devez spécifier deux paramètres requis lors de la création de la configuration d'audit. Il existe également trois paramètres facultatifs que vous pouvez spécifier :

Type d'information	Option	Obligatoire	Inclure	Vos valeurs
<i>Nom du SVM</i> Nom du SVM sur lequel créer la configuration d'audit. Le SVM doit déjà exister.	<code>-vserver vserver_name</code>	Oui.	Oui.	
<i>Chemin de destination du journal</i> Spécifie le répertoire dans lequel les journaux d'audit convertis sont stockés, généralement un volume dédié ou un qtree. Le chemin doit déjà exister dans le namespace du SVM. Le chemin d'accès peut comporter jusqu'à 864 caractères et doit avoir des autorisations de lecture/écriture. Si le chemin n'est pas valide, la commande audit de configuration échoue. Si le SVM est une source de reprise après incident du SVM, le chemin de destination du journal ne peut pas se trouver sur le volume root. En effet, le contenu du volume racine n'est pas répliqué vers la destination de reprise après incident. Vous ne pouvez pas utiliser un volume FlexCache comme destination du journal (ONTAP 9.7 et versions ultérieures).	<code>-destination text</code>	Oui.	Oui.	

<p><i>Catégories d'événements à auditer</i></p> <p>Spécifie les catégories d'événements à auditer. Les catégories d'événements suivantes peuvent être auditées :</p> <ul style="list-style-type: none"> • Événements d'accès aux fichiers (SMB et NFSv4) • Événements de connexion et de déconnexion SMB • Événements d'activation de stratégie d'accès central <p>Les événements de transfert de stratégie d'accès central sont disponibles à partir des domaines Active Directory de Windows 2012.</p> <ul style="list-style-type: none"> • Événements de catégorie de partage de fichiers • Audit des événements de modification de règle • Événements locaux de gestion de compte utilisateur • Événements de gestion de groupe de sécurité • Événements de modification de la politique d'autorisation <p>La valeur par défaut consiste à auditer l'accès aux fichiers et les événements de connexion et de déconnexion SMB.</p> <p>Remarque : avant de pouvoir spécifier <code>cap-staging</code> En tant que catégorie d'événement, un serveur SMB doit exister sur le SVM. Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, les événements de staging de stratégie d'accès central ne sont générés que si le contrôle d'accès dynamique est activé. Le contrôle d'accès dynamique est activé par le biais d'une option de serveur SMB. Elle n'est pas activée par défaut.</p>	<p><code>-events {file-ops</code></p>	<p><code>cifs- logon- logoff</code></p>	<p><code>cap- staging</code></p>	<p><code>file- share</code></p>
---	---------------------------------------	---	--------------------------------------	-------------------------------------

audit-policy-change	user-account	security-group	authorization-policy-change}	Non
		<p><i>Format de sortie du fichier journal</i></p> <p>Déterminez le format de sortie des journaux d'audit. Le format de sortie peut être spécifique à ONTAP XML Ou Microsoft Windows EVTX format du journal. Par défaut, le format de sortie est EVTX.</p>	-format {xml	evtx}

Non			<p><i>Limite de rotation des fichiers journaux</i></p> <p>Déterminer le nombre de fichiers journaux d'audit à conserver avant de faire pivoter le fichier journal le plus ancien vers l'extérieur. Par exemple, si vous saisissez une valeur de 5, les cinq derniers fichiers journaux sont conservés.</p> <p>Valeur de 0 indique que tous les fichiers journaux sont conservés. La valeur par défaut est 0.</p>	<p>-rotate -limit integer</p>
-----	--	--	--	---------------------------------------

Paramètres utilisés pour déterminer quand faire pivoter les journaux d'événements d'audit

Faire pivoter les journaux en fonction de la taille du journal

La valeur par défaut consiste à faire pivoter les journaux d'audit en fonction de la taille.

- La taille du journal par défaut est de 100 Mo
- Si vous souhaitez utiliser la méthode de rotation du journal par défaut et la taille du journal par défaut, vous n'avez pas besoin de configurer de paramètres spécifiques pour la rotation du journal.
- Si vous souhaitez faire pivoter les journaux d'audit en fonction d'une taille de journal seule, utilisez la commande suivante pour annuler la définition du `-rotate-schedule-minute` paramètre : `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

Si vous ne souhaitez pas utiliser la taille de journal par défaut, vous pouvez configurer le `-rotate-size` paramètre pour spécifier une taille de journal personnalisée :

Type d'information	Option	Obligatoire	Inclure	Vos valeurs
<i>Limite de taille du fichier journal</i> Détermine la limite de taille du fichier journal d'audit.	<code>-rotate-size {integer[KO]</code>	MO	GO	TO

Faire pivoter les journaux en fonction d'un horaire

Si vous choisissez de faire pivoter les journaux d'audit en fonction d'un planning, vous pouvez programmer la rotation du journal en utilisant les paramètres de rotation basés sur le temps dans n'importe quelle combinaison.

- Si vous utilisez une rotation basée sur le temps, le `-rotate-schedule-minute` paramètre obligatoire.
- Tous les autres paramètres de rotation basés sur le temps sont facultatifs.
- Le planning de rotation est calculé en utilisant toutes les valeurs liées au temps.

Par exemple, si vous spécifiez uniquement le `-rotate-schedule-minute` paramètre, les fichiers journaux d'audit sont pivotés en fonction des minutes spécifiées pour tous les jours de la semaine, pendant toutes les heures sur tous les mois de l'année.

- Si vous spécifiez uniquement un ou deux paramètres de rotation basés sur le temps (par exemple, `-rotate-schedule-month` et `-rotate-schedule-minutes`), les fichiers journaux pivotent en fonction des valeurs de minutes que vous avez spécifiées tous les jours de la semaine, pendant toutes les heures, mais seulement pendant les mois spécifiés.

Par exemple, vous pouvez préciser que le journal d'audit doit être tourné pendant les mois janvier, mars et août tous les lundis, mercredis et samedis à 10 h 30

- Si vous spécifiez des valeurs pour les deux `-rotate-schedule-dayofweek` et `-rotate-schedule-day`, ils sont considérés indépendamment.

Par exemple, si vous spécifiez `-rotate-schedule-dayofweek` Comme vendredi et `-rotate-schedule-day` Comme 13, les registres de vérification seront ensuite tournés tous les vendredis et les

13ème jours du mois spécifié, pas seulement tous les vendredis du 13ème.

- Si vous souhaitez faire pivoter les journaux d'audit en fonction d'une planification seule, utilisez la commande suivante pour annuler la définition du `-rotate-size` paramètre : `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Vous pouvez utiliser la liste suivante de paramètres d'audit disponibles pour déterminer les valeurs à utiliser pour configurer un planning pour les rotations du journal d'événements d'audit :

Type d'information	Option	Obligatoire	Inclure	Vos valeurs
<i>Horaire de rotation du journal : mois</i> Détermine le calendrier mensuel de rotation des journaux d'audit. Les valeurs valides sont January à December, et all. Par exemple, vous pouvez indiquer que le journal d'audit doit être pivoté pendant les mois janvier, mars et août.	<code>-rotate-schedule-month</code> <code>chron_month</code>	Non		
<i>Horaire de rotation du journal : jour de la semaine</i> Détermine le calendrier quotidien (jour de la semaine) pour la rotation des journaux d'audit. Les valeurs valides sont Sunday à Saturday, et all. Par exemple, vous pouvez préciser que le journal d'audit doit être tourné le mardi et le vendredi, ou pendant tous les jours d'une semaine.	<code>-rotate-schedule</code> <code>-dayofweek</code> <code>chron_dayofweek</code>	Non		
<i>Horaire de rotation du journal : jour</i> Détermine le jour du mois de la rotation du journal d'audit. Les valeurs valides vont de 1 à 31. Par exemple, vous pouvez indiquer que le journal d'audit doit être tourné les 10e et 20e jours d'un mois, ou tous les jours d'un mois.	<code>-rotate-schedule-day</code> <code>chron_dayofmonth</code>	Non		

<p><i>Horaires de rotation du journal : heure</i></p> <p>Détermine le planning horaire pour la rotation du journal d'audit.</p> <p>Les valeurs valides vont de 0 de minuit à 23 (11 h 00). Spécification <code>all</code> fait pivoter les journaux d'audit toutes les heures. Par exemple, vous pouvez spécifier que le journal d'audit doit être tourné à 6 (6 h) et 18 (6 h).</p>	<p><code>-rotate-schedule-hour</code> <code>chron_hour</code></p>	Non		
<p><i>Horaires de rotation du journal : minute</i></p> <p>Détermine la planification des minutes pour la rotation du journal d'audit.</p> <p>Les valeurs valides vont de 0 à 59. Par exemple, vous pouvez indiquer que le journal d'audit doit être pivoté à la 30e minute.</p>	<p><code>-rotate-schedule-minute</code> <code>chron_minute</code></p>	Oui, si vous configurez une rotation de journal basée sur un planning, sinon non		

Faire pivoter les journaux en fonction de la taille du journal et de l'horaire

Vous pouvez choisir de faire pivoter les fichiers journaux en fonction de la taille du journal et d'une planification en définissant les deux `-rotate-size` paramètre et paramètres de rotation basés sur le temps dans n'importe quelle combinaison. Par exemple : si `-rotate-size` Est défini sur 10 Mo et `-rotate-schedule-minute` Est défini sur 15, les fichiers journaux pivotent lorsque la taille du fichier journal atteint 10 Mo ou la 15e minute de chaque heure (selon la première éventualité).

Créer une configuration d'audit de fichier et de répertoire sur les SVM

Créez la configuration d'audit

La création d'une configuration d'audit de fichier et de répertoire sur votre SVM (Storage Virtual machine) comprend les options de configuration disponibles, la planification de la configuration, puis la configuration et l'activation de la configuration. Vous pouvez ensuite afficher des informations sur la configuration d'audit pour confirmer que la configuration résultante est la configuration souhaitée.

Avant de pouvoir commencer l'audit des événements de fichiers et de répertoires, vous devez créer une configuration d'audit sur la machine virtuelle de stockage (SVM).

Avant de commencer

Si vous prévoyez de créer une configuration d'audit pour la mise en attente des règles d'accès central, un serveur SMB doit exister sur le SVM.



- Bien que vous puissiez activer le staging de stratégie d'accès central dans la configuration d'audit sans activer le contrôle d'accès dynamique sur le serveur SMB, les événements de staging de stratégie d'accès central ne sont générés que si le contrôle d'accès dynamique est activé.

Le contrôle d'accès dynamique est activé par le biais d'une option de serveur SMB. Elle n'est pas activée par défaut.

- Si les arguments d'un champ d'une commande ne sont pas valides, par exemple des entrées non valides pour les champs, des entrées dupliquées et des entrées non existantes, la commande échoue avant la phase d'audit.

Ces échecs ne génèrent pas d'enregistrement d'audit.

Description de la tâche

Si le SVM est une source de reprise d'activité du SVM, le chemin de destination ne peut pas se trouver sur le volume root.

Étape

1. À l'aide des informations de la fiche de planification, créez la configuration d'audit pour faire pivoter les journaux d'audit en fonction de la taille du journal ou d'une planification :

Si vous souhaitez faire pivoter les journaux d'audit en...	Entrer...
Taille du journal	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]]`
Un planning	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Exemples

L'exemple suivant crée une configuration d'audit qui vérifie les opérations de fichiers et les événements de connexion et de déconnexion SMB (par défaut) à l'aide de la rotation basée sur la taille. Le format du journal est EVTX (valeur par défaut). Les journaux sont stockés dans le `/audit_log` répertoire. La taille limite du fichier journal est de 200 MB. Les journaux pivotent lorsqu'ils atteignent 200 Mo de taille :

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log  
-rotate-size 200MB
```

L'exemple suivant crée une configuration d'audit qui vérifie les opérations de fichiers et les événements de connexion et de déconnexion SMB (par défaut) à l'aide de la rotation basée sur la taille. Le format du journal est EVTX (valeur par défaut). Les journaux sont stockés dans le /cifs_event_logs répertoire. La taille limite du fichier journal est de 100 MB (valeur par défaut) et la limite de rotation du journal est 5:

```
cluster1::> vservers audit create -vservers vs1 -destination  
/cifs_event_logs -rotate-limit 5
```

L'exemple suivant crée une configuration d'audit qui audite les opérations de fichiers, les événements de connexion et de déconnexion CIFS, ainsi que les événements d'activation de stratégie d'accès central à l'aide d'une rotation basée sur le temps. Le format du journal est EVTX (valeur par défaut). Les journaux d'audit sont pivotés tous les mois, à 12:30 tous les jours de la semaine. La limite de rotation du log est de 5:

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log  
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-  
account,security-group,authorization-policy-change,cap-staging -rotate  
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour  
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Informations associées

- ["Activation de l'audit sur le SVM"](#)
- ["Vérifiez la configuration de l'audit"](#)

Activation de l'audit sur le SVM

Une fois la configuration d'audit terminée, vous devez activer l'audit sur la machine virtuelle de stockage (SVM).

Avant de commencer

La configuration d'audit SVM doit déjà exister.

Description de la tâche

Lorsqu'une configuration SVM Disaster Recovery ID rebuter est démarrée en premier (une fois l'initialisation de SnapMirror terminée) et que le SVM dispose d'une configuration d'audit, ONTAP désactive automatiquement la configuration d'audit. L'audit est désactivé sur le SVM en lecture seule pour empêcher le remplissage des volumes de transit. Vous pouvez activer l'audit uniquement après la rupture de la relation SnapMirror et la SVM est read-write.

Étapes

1. Activer l'audit sur le SVM :

```
vservers audit enable -vservers vservers_name
```

```
vserver audit enable -vserver vs1
```

Informations associées

- ["Créez la configuration d'audit"](#)
- ["Vérifiez la configuration de l'audit"](#)

Vérifiez la configuration de l'audit

Une fois la configuration d'audit terminée, vous devez vérifier que l'audit est correctement configuré et activé.

Étapes

1. Vérifiez la configuration de l'audit :

```
vserver audit show -instance -vserver vserver_name
```

La commande suivante s'affiche sous forme de liste toutes les informations de configuration d'audit pour la machine virtuelle de stockage (SVM) vs1 :

```
vserver audit show -instance -vserver vs1
```

```
Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evtv
Log File Size Limit: 200MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

Informations associées

- ["Créez la configuration d'audit"](#)
- ["Activation de l'audit sur le SVM"](#)

Configuration des règles d'audit des fichiers et des dossiers

Configuration des règles d'audit des fichiers et des dossiers

L'implémentation de l'audit sur les événements d'accès aux fichiers et aux dossiers est

un processus en deux étapes. Vous devez d'abord créer et activer une configuration d'audit sur les serveurs virtuels de stockage (SVM). Ensuite, vous devez configurer des stratégies d'audit sur les fichiers et dossiers que vous souhaitez surveiller. Vous pouvez configurer des stratégies d'audit pour surveiller les tentatives d'accès réussies et échouées.

Vous pouvez configurer les règles d'audit SMB et NFS. Les règles d'audit SMB et NFS diffèrent entre les exigences de configuration et les fonctionnalités d'audit.

Si les stratégies d'audit appropriées sont configurées, ONTAP surveille les événements d'accès SMB et NFS comme spécifié dans les règles d'audit uniquement si les serveurs SMB ou NFS sont exécutés.

Configurez les règles d'audit sur les répertoires et les fichiers de style de sécurité NTFS

Avant de pouvoir auditer les opérations de fichiers et de répertoires, vous devez configurer des stratégies d'audit sur les fichiers et répertoires pour lesquels vous souhaitez collecter les informations d'audit. Cela permet en plus de configurer et d'activer la configuration d'audit. Vous pouvez configurer les stratégies d'audit NTFS en utilisant l'onglet sécurité Windows ou l'interface de ligne de commande ONTAP.

Configuration des stratégies d'audit NTFS à l'aide de l'onglet sécurité de Windows

Vous pouvez configurer les stratégies d'audit NTFS sur les fichiers et les répertoires en utilisant l'onglet **sécurité Windows** de la fenêtre Propriétés Windows. Il s'agit de la même méthode utilisée lors de la configuration de stratégies d'audit sur des données résidant sur un client Windows, qui vous permet d'utiliser la même interface graphique que celle que vous êtes habitué à utiliser.

Avant de commencer

L'audit doit être configuré sur la machine virtuelle de stockage (SVM) qui contient les données auxquelles vous appliquez des listes de contrôle d'accès système (SACL).

Description de la tâche

La configuration des stratégies d'audit NTFS se fait en ajoutant des entrées aux SACL NTFS associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS. Ces tâches sont traitées automatiquement par l'interface graphique de Windows. Le descripteur de sécurité peut contenir des listes de contrôle d'accès discrétionnaire (DACL) pour l'application d'autorisations d'accès aux fichiers et aux dossiers, des listes SACL pour l'audit des fichiers et des dossiers, ou des listes SACL et des listes DACL.

Pour définir les stratégies d'audit NTFS à l'aide de l'onglet sécurité Windows, procédez comme suit sur un hôte Windows :

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Complétez la boîte **Map Network Drive** :
 - a. Sélectionnez une lettre **lecteur**.
 - b. Dans la zone **Folder**, saisissez le nom du serveur SMB qui contient le partage, en tenant les données à auditer et le nom du partage.

Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

Si votre nom de serveur SMB est "SMB_SERVER" et que votre partage est nommé "share1", vous devez entrer \\SMB_SERVER\share1.

c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez activer l'accès d'audit.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.
6. Cliquez sur **Avancé**.
7. Sélectionnez l'onglet **Audit**.
8. Effectuez les opérations souhaitées :

Si vous voulez	Procédez comme suit
Configuration de l'audit pour un nouvel utilisateur ou un nouveau groupe	<ol style="list-style-type: none">a. Cliquez sur Ajouter.b. Dans la zone entrer le nom de l'objet à sélectionner, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter.c. Cliquez sur OK.
Supprimer l'audit d'un utilisateur ou d'un groupe	<ol style="list-style-type: none">a. Dans la zone entrer le nom de l'objet à sélectionner, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer.b. Cliquez sur Supprimer.c. Cliquez sur OK.d. Ignorer le reste de cette procédure.
Modifier l'audit d'un utilisateur ou d'un groupe	<ol style="list-style-type: none">a. Dans la zone entrer le nom de l'objet à sélectionner, sélectionnez l'utilisateur ou le groupe que vous souhaitez modifier.b. Cliquez sur Modifier.c. Cliquez sur OK.

Si vous configurez l'audit sur un utilisateur ou un groupe ou si vous modifiez l'audit sur un utilisateur ou un groupe existant, la zone entrée d'audit pour <objet> s'ouvre.

9. Dans la case **appliquer à**, sélectionnez la façon dont vous souhaitez appliquer cette entrée d'audit.

Vous pouvez sélectionner l'une des options suivantes :

- **Ce dossier, sous-dossiers et fichiers**
- **Ce dossier et sous-dossiers**

- **Ce dossier uniquement**
- **Ce dossier et fichiers**
- **Sous-dossiers et fichiers uniquement**
- **Sous-dossiers uniquement**
- **Fichiers uniquement** Si vous configurez l'audit sur un seul fichier, la case **appliquer à** n'est pas active. Le paramètre de case **appliquer à** est défini par défaut sur **cet objet uniquement**.



Étant donné que l'audit utilise les ressources de l'SVM, sélectionnez uniquement le niveau minimal qui fournit les événements d'audit qui répondent à vos exigences de sécurité.

10. Dans la case **Access**, sélectionnez ce que vous voulez auditer et si vous voulez auditer les événements réussis, les événements d'échec, ou les deux.

- Pour auditer les événements réussis, cochez la case succès.
- Pour auditer les événements d'échec, cochez la case échec.

Sélectionnez uniquement les actions à surveiller pour répondre à vos exigences de sécurité. Pour plus d'informations sur ces événements auditable, consultez votre documentation Windows. Vous pouvez auditer les événements suivants :

- **Contrôle total**
- **Dossier traverse / fichier d'exécution**
- **Liste de dossiers / lecture de données**
- **Lire les attributs**
- **Lire les attributs étendus**
- **Créer des fichiers / écrire des données**
- **Créer des dossiers / ajouter des données**
- **Ecrire des attributs**
- **Ecrire des attributs étendus**
- **Supprimer des sous-dossiers et des fichiers**
- **Supprimer**
- **Autorisations de lecture**
- **Modifier les autorisations**
- * Prendre possession*

11. Si vous ne souhaitez pas que le paramètre d'audit se propage aux fichiers et dossiers suivants du conteneur d'origine, sélectionnez la case **appliquer ces entrées d'audit aux objets et/ou aux conteneurs dans ce conteneur uniquement**.

12. Cliquez sur **appliquer**.

13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des entrées d'audit, cliquez sur **OK**.

La zone entrée d'audit pour <objet> se ferme.

14. Dans la zone **Audit**, sélectionnez les paramètres d'héritage de ce dossier.

Sélectionnez uniquement le niveau minimal qui fournit les événements d'audit qui répondent à vos

exigences de sécurité. Vous pouvez choisir l'une des options suivantes :

- Sélectionnez l'option inclure les entrées d'audit héritées de la boîte parent de cet objet.
- Sélectionnez remplacer toutes les entrées d'audit héritées sur tous les descendants avec des entrées d'audit héritées de cet objet.
- Sélectionnez les deux cases.
- Sélectionnez aucune case. Si vous définissez des SACLs sur un seul fichier, la boîte remplacer toutes les entrées d'audit héritées sur tous les descendants avec des entrées d'audit héritables de cet objet n'est pas présente dans la zone Audit.

15. Cliquez sur **OK**.

La zone Audit se ferme.

Configuration des règles d'audit NTFS à l'aide de l'interface de ligne de commande ONTAP

Vous pouvez configurer des stratégies d'audit sur des fichiers et des dossiers à l'aide de l'interface de ligne de commande ONTAP. Cela vous permet de configurer les stratégies d'audit NTFS sans avoir à vous connecter aux données à l'aide d'un partage SMB sur un client Windows.

Vous pouvez configurer les règles d'audit NTFS en utilisant le `vserver security file-directory` famille de commande.

Vous pouvez uniquement configurer les SACLs NTFS à l'aide de l'interface de ligne de commande. La configuration des SACLs NFSv4 n'est pas prise en charge avec cette famille de commandes ONTAP. Consultez les pages man pour plus d'informations sur l'utilisation de ces commandes pour configurer et ajouter des SACLs NTFS aux fichiers et dossiers.

Configurer l'audit pour les fichiers et répertoires de style de sécurité UNIX

Vous configurez l'audit des répertoires et des fichiers de style de sécurité UNIX en ajoutant des ACE d'audit aux listes de contrôle d'accès NFSv4.x. Cela vous permet de surveiller certains événements d'accès aux fichiers et aux répertoires NFS à des fins de sécurité.

Description de la tâche

Pour NFSv4.x, les ACE discrétionnaires et système sont tous deux stockés dans la même liste de contrôle d'accès. Ils ne sont pas stockés dans des listes de contrôle d'accès (DACL) et des listes de contrôle d'accès (SACL) distinctes. Par conséquent, vous devez faire preuve de prudence lorsque vous ajoutez des ACE d'audit à une liste de contrôle d'accès existante pour éviter d'écraser et de perdre une liste de contrôle d'accès existante. L'ordre dans lequel vous ajoutez les ACE d'audit à une liste de contrôle d'accès existante n'a aucune importance.

Étapes

1. Récupérez la liste de contrôle d'accès existante pour le fichier ou le répertoire à l'aide de la `nfs4_getfacl` ou une commande équivalente.

Pour plus d'informations sur la manipulation des listes de contrôle d'accès, consultez les pages de manuels de votre client NFS.

2. Ajoutez les ACE d'audit souhaités.

3. Appliquez la liste de contrôle d'accès mise à jour au fichier ou au répertoire à l'aide de la `nfs4_setfacl` ou une commande équivalente.

Affiche des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires

Affiche des informations sur les stratégies d'audit à l'aide de l'onglet sécurité Windows

Vous pouvez afficher des informations sur les stratégies d'audit qui ont été appliquées aux fichiers et aux répertoires à l'aide de l'onglet sécurité de la fenêtre Propriétés de Windows. Cette méthode est identique à celle utilisée pour les données résidant sur un serveur Windows. Elle permet aux clients d'utiliser la même interface graphique qu'ils sont habitués.

Description de la tâche

L'affichage des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires vous permet de vérifier que les listes de contrôle d'accès système (SACL) appropriées sont définies sur les fichiers et dossiers spécifiés.

Pour afficher des informations sur les listes de contrôle d'application qui ont été appliquées aux fichiers et dossiers NTFS, procédez comme suit sur un hôte Windows.

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Renseignez la boîte de dialogue **Map Network Drive** :
 - a. Sélectionnez une lettre **lecteur**.
 - b. Dans la zone **Folder**, saisissez l'adresse IP ou le nom du serveur SMB de la machine virtuelle de stockage (SVM) contenant le partage contenant à la fois les données que vous souhaitez auditer et le nom du partage.

Si votre nom de serveur SMB est "SMB_SERVER" et que votre partage est nommé "share1", vous devez entrer `\\SMB_SERVER\share1`.



Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

- c. Cliquez sur **Terminer**.

Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous affichez les informations d'audit.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire et sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.
6. Cliquez sur **Avancé**.
7. Sélectionnez l'onglet **Audit**.

8. Cliquez sur **Continuer**.

La boîte de dialogue Audit s'ouvre. La boîte de dialogue **Auditing Entries** affiche un récapitulatif des utilisateurs et des groupes auxquels des SACL sont appliquées.

9. Dans la zone **Auditing Entries**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez afficher les entrées SACL.

10. Cliquez sur **Modifier**.

L'entrée Audit pour <Object> s'ouvre.

11. Dans la zone **Access**, affichez les CLS actuelles appliquées à l'objet sélectionné.

12. Cliquez sur **Annuler** pour fermer l'entrée **Audit pour <objet>**.

13. Cliquez sur **Annuler** pour fermer la case **Audit**.

Affiche des informations sur les règles d'audit NTFS sur les volumes FlexVol à l'aide de l'interface de ligne de commande

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 ces informations pour valider votre configuration de sécurité ou résoudre les problèmes d'audit.

Description de la tâche

L'affichage des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires vous permet de vérifier que les listes de contrôle d'accès système (SACL) appropriées sont définies sur les fichiers et dossiers spécifiés.

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	<code>vserver security file-directory show -vserver vserver_name -path path</code>
En tant que liste détaillée	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

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

```

Moyens d'afficher des informations sur la sécurité des fichiers et les stratégies 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 particulier nommé "", vous devez fournir le chemin complet à l'intérieur des 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::> vservers security file-directory show -vservers 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
```

Les événements de modification de l'interface de ligne de commande peuvent être audités

Les événements de modification de la CLI pouvant être audités

ONTAP peut auditer certains événements de modification de l'interface de ligne de commandes, notamment certains événements de partage SMB, certains événements de stratégie d'audit, certains événements de groupe de sécurité local, des événements de groupe d'utilisateurs locaux et des événements de politique d'autorisation. Il est utile de savoir quels événements de modification peuvent être audités lors de l'interprétation des résultats des journaux d'événements.

Vous pouvez gérer les événements de modification de l'interface de ligne de commande d'audit des machines virtuelles de stockage (SVM) en faisant tourner manuellement les journaux d'audit, en activant ou désactivant l'audit, en affichant des informations sur l'audit des événements de modification, en modifiant l'audit des événements et en supprimant les événements d'audit des modifications.

En tant qu'administrateur, si vous exécutez une commande pour modifier la configuration relative aux événements SMB-share, local user-group, local Security-group, autorisation-policy et audit-policy, un enregistrement génère et l'événement correspondant est vérifié :

Catégorie d'audit	Événements	ID d'événement	Exécuter cette commande...
Audit Mhost	modification de règles	[4719] Configuration d'audit modifiée	`vserver audit disable`
enable	modify`	partage de fichiers	[5142] le partage réseau a été ajouté
vserver cifs share create	[5143] le partage réseau a été modifié	vserver cifs share modify`vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] partage réseau supprimé	vserver cifs share delete
Audit	compte utilisateur	[4720] utilisateur local créé	vserver cifs users-and-groups local-user create vserver services name-service unix-user create
[4722] utilisateur local activé	`vserver cifs users-and-groups local-user create	modify`	[4724] Réinitialisation du mot de passe de l'utilisateur local
vserver cifs users-and-groups local-user set-password	[4725] utilisateur local désactivé	`vserver cifs users-and-groups local-user create	modify`
[4726] utilisateur local supprimé	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738] modification de l'utilisateur local	vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify
[4781] utilisateur local Renommer	vserver cifs users-and-groups local-user rename	groupe-de-sécurité	[4731] Groupe de sécurité local créé
vserver cifs users-and-groups local-group create vserver services name-service unix-group create	[4734] Groupe de sécurité local supprimé	vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete	[4735] Groupe de sécurité local modifié

<code>`vserver cifs users-and-groups local-group rename</code>	<code>modify` vserver services name-service unix-group modify</code>	[4732] utilisateur ajouté au groupe local	<code>vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser</code>
[4733] utilisateur supprimé du groupe local	<code>vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser</code>	autorisation-stratégie-modification	[4704] droits d'utilisateur attribués
<code>vserver cifs users-and-groups privilege add-privilege</code>	[4705] droits d'utilisateur supprimés	<code>`vserver cifs users-and-groups privilege remove-privilege</code>	<code>reset-privilege`</code>

Gérer un événement de partage de fichiers

Lorsqu'un événement de partage de fichiers est configuré pour un SVM (Storage Virtual machine) et qu'un audit est activé, des événements d'audit sont générés. Les événements de partage de fichiers sont générés lorsque le partage réseau SMB est modifié à l'aide de `vserver cifs share` commandes associées

Les événements de partage de fichiers avec les id-événements 5142, 5143 et 5144 sont générés lorsqu'un partage réseau SMB est ajouté, modifié ou supprimé pour la SVM. La configuration du partage réseau SMB est modifiée à l'aide du `cifs share access control create|modify|delete` commandes.

L'exemple suivant affiche un événement de partage de fichiers avec l'ID 5143 est généré lorsqu'un objet de partage appelé « `audit_dest` » est créé :

```

netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID 5142
    EventName Share Object Added
    ...
    ...
    ShareName audit_dest
    SharePath /audit_dest
    ShareProperties oplocks;browsable;changenotify;show-previous-versions;
    SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;;FA;;;WD)

```

Gestion de l'événement audit-policy-change

Lorsqu'un événement d'audit-policy-change est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés. Les événements audit-règle-modification sont générés lorsqu'une règle d'audit est modifiée à l'aide de `vserver audit` commandes associées

L'événement audit-policy-change avec l'ID-événement 4719 est généré chaque fois qu'une stratégie d'audit est désactivée, activée ou modifiée et aide à identifier quand un utilisateur tente de désactiver l'audit pour couvrir les pistes. Il est configuré par défaut et requiert un privilège de diagnostic pour être désactivé.

L'exemple suivant montre un événement de modification de règle d'audit avec l'ID 4719 généré lorsqu'un audit est désactivé :

```

netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID 4719
    EventName Audit Disabled
    ...
    ...
    SubjectUserName admin
    SubjectUserSid 65533-1001
    SubjectDomainName ~
    SubjectIP console
    SubjectPort

```

Gérer un événement de compte utilisateur

Lorsqu'un événement de compte utilisateur est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements du compte utilisateur avec les id-événements 4720, 4722, 4724, 4725, 4726, 4738 et 4781 sont générés lorsqu'un utilisateur SMB ou NFS local est créé ou supprimé du système, le compte d'utilisateur local est activé, désactivé ou modifié et le mot de passe de l'utilisateur SMB local est réinitialisé ou modifié. Les événements du compte utilisateur sont générés lorsqu'un compte utilisateur est modifié à l'aide de `vserver cifs users-and-groups <local user>` et `vserver services name-service <unix user>` commandes.

L'exemple suivant montre un événement de compte d'utilisateur avec l'ID 4720 généré lors de la création d'un utilisateur SMB local :

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4720
  EventName Local Cifs User Created
  ...
  ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

L'exemple suivant affiche un événement de compte utilisateur avec l'ID 4781 généré lorsque l'utilisateur SMB local créé dans l'exemple précédent est renommé :

```

netapp-clus1::*> vservers cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~

```

Gérer l'événement de groupe de sécurité

Lorsqu'un événement de groupe de sécurité est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements du groupe de sécurité avec les id-événements 4731, 4732, 4733, 4734 et 4735 sont générés lorsqu'un groupe SMB ou NFS local est créé ou supprimé du système et que l'utilisateur local est ajouté ou supprimé du groupe. Les événements groupe-sécurité sont générés lorsqu'un compte utilisateur est modifié à l'aide de `vservers cifs users-and-groups <local-group>` et `vservers services name-service <unix-group>` commandes.

L'exemple suivant montre un événement de groupe de sécurité avec l'ID 4731 généré lors de la création d'un groupe de sécurité UNIX local :

```

netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~

```

Gérer l'événement autorisation-stratégie-modification

Lorsque l'événement autorisation-policy-change est configuré pour une machine virtuelle de stockage (SVM) et qu'un audit est activé, des événements d'audit sont générés.

Les événements autorisation-policy-change avec les id-événements 4704 et 4705 sont générés chaque fois que les droits d'autorisation sont accordés ou révoqués pour un utilisateur SMB et un groupe SMB. Les événements autorisation-stratégie-modification sont générés lorsque les droits d'autorisation sont affectés ou révoqués à l'aide de `vserver cifs users-and-groups privilege` commandes associées

L'exemple suivant affiche un événement de stratégie d'autorisation avec l'ID 4704 généré lorsque les droits d'autorisation d'un groupe d'utilisateurs SMB sont affectés :

```

netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS

```

Gérer les configurations d'audit

Rotation manuelle des journaux d'événements d'audit

Avant de pouvoir afficher les journaux d'événements d'audit, ils doivent être convertis en formats lisibles par l'utilisateur. Si vous souhaitez afficher les journaux des événements d'une machine virtuelle de stockage (SVM) spécifique avant que ONTAP ne fasse automatiquement pivoter le journal, vous pouvez faire tourner manuellement les journaux des événements d'audit sur un SVM.

Étape

1. Faites pivoter les journaux d'événements d'audit à l'aide de `vserver audit rotate-log` commande.

```
vserver audit rotate-log -vserver vs1
```

Le journal des événements d'audit est enregistré dans le répertoire du journal des événements d'audit SVM au format spécifié par la configuration d'audit (XML ou EVTX), et peut être consulté à l'aide de l'application appropriée.

Activation et désactivation de l'audit sur les SVM

Vous pouvez activer ou désactiver l'audit sur les serveurs virtuels de stockage (SVM). Vous pouvez désactiver l'audit des fichiers et des répertoires temporairement. Vous pouvez activer l'audit à tout moment (si une configuration d'audit existe).

Ce dont vous avez besoin

Avant de pouvoir activer l'audit sur le SVM, la configuration d'audit du SVM doit déjà exister.

"Créez la configuration d'audit"

Description de la tâche

La désactivation de l'audit ne supprime pas la configuration d'audit.

Étapes

1. Exécutez la commande appropriée :

Si vous voulez que l'audit soit...	Entrez la commande...
Activé	<code>vserver audit enable -vserver vserver_name</code>
Désactivé	<code>vserver audit disable -vserver vserver_name</code>

2. Vérifiez que l'audit est dans l'état souhaité :

```
vserver audit show -vserver vserver_name
```

Exemples

L'exemple suivant permet l'audit du SVM vs1 :

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
            Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 10
```

L'exemple suivant désactive l'audit pour SVM vs1 :

```
cluster1::> vserver audit disable -vserver vs1

Vserver: vs1
Auditing state: false
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
Log Format: evtv
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 10
```

Affiche des informations sur les configurations d'audit

Vous pouvez afficher des informations sur les configurations d'audit. Les informations peuvent vous aider à déterminer si la configuration est celle que vous souhaitez mettre en place pour chaque SVM. Les informations affichées vous permettent également de vérifier si une configuration d'audit est activée.

Description de la tâche

Vous pouvez afficher des informations détaillées sur les configurations d'audit sur tous les SVM. Vous pouvez également personnaliser les informations affichées dans le résultat en spécifiant des paramètres facultatifs. Si vous ne spécifiez aucun des paramètres facultatifs, les éléments suivants s'affichent :

- Nom du SVM auquel s'applique la configuration d'audit
- État d'audit, qui peut être `true` ou `false`

Si l'état d'audit est `true`, l'audit est activé. Si l'état d'audit est `false`, l'audit est désactivé.

- Catégories d'événements à vérifier
- Format du journal d'audit
- Répertoire cible dans lequel le sous-système d'audit stocke les journaux d'audit consolidés et convertis

Étape

1. Affiche des informations sur la configuration d'audit à l'aide du `vserver audit show` commande.

Pour plus d'informations sur l'utilisation de la commande, consultez les pages de manuels.

Exemples

L'exemple suivant affiche un résumé de la configuration d'audit de tous les SVM :


```
cluster1::> vserver audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	file-ops	evtx	/audit_log

L'exemple suivant affiche, sous forme de liste, toutes les informations de configuration d'audit de tous les SVM :


```
cluster1::> vserver audit show -instance
```

```
                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
            Log Format: evtx
        Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 0
```

Commandes permettant de modifier les configurations d'audit

Si vous souhaitez modifier un paramètre d'audit, vous pouvez modifier la configuration actuelle à tout moment, notamment modifier le chemin d'accès du journal et le format du journal, modifier les catégories d'événements à auditer, enregistrer automatiquement les fichiers journaux et spécifier le nombre maximal de fichiers journaux à enregistrer.

Les fonctions que vous recherchez...	Utilisez cette commande...
Modifiez le chemin de destination du journal	<code>vserver audit modify</code> avec le <code>-destination</code> paramètre

Modifier la catégorie d'événements à auditer	vserver audit modify avec le <code>-events</code> paramètre <div>  <div> <p>Pour auditer les événements de transfert des règles d'accès central, l'option du serveur SMB Dynamic Access Control (DAC) doit être activée sur le serveur SVM (Storage Virtual machine).</p> </div> </div>
Modifiez le format du journal	vserver audit modify avec le <code>-format</code> paramètre
Activation des sauvegardes automatiques en fonction de la taille du fichier journal interne	vserver audit modify avec le <code>-rotate-size</code> paramètre
Activation des sauvegardes automatiques en fonction d'un intervalle de temps	vserver audit modify avec le <code>-rotate-schedule-month</code> , <code>-rotate-schedule-dayofweek</code> , <code>-rotate-schedule-day</code> , <code>-rotate-schedule-hour</code> , et <code>-rotate-schedule-minute</code> paramètres
Spécification du nombre maximal de fichiers journaux enregistrés	vserver audit modify avec le <code>-rotate-limit</code> paramètre

Supprimer une configuration d'audit

Vous ne souhaitez plus auditer les événements de fichier et de répertoire sur la machine virtuelle de stockage (SVM) et ne souhaitez pas conserver une configuration d'audit sur la SVM, vous pouvez supprimer la configuration d'audit.

Étapes

1. Désactivez la configuration d'audit :

```
vserver audit disable -vserver vserver_name
vserver audit disable -vserver vs1
```

2. Supprimer la configuration d'audit :

```
vserver audit delete -vserver vserver_name
vserver audit delete -vserver vs1
```

Comprenez les implications du rétablissement du cluster

Si vous prévoyez de restaurer le cluster, sachez que le processus de restauration suivi par la ONTAP est exécuté lors de l'audit de serveurs virtuels de stockage (SVM) dans le

cluster. Vous devez effectuer certaines actions avant de revenir en retour.

Restauration vers une version d'ONTAP qui ne prend pas en charge l'audit des événements de connexion et de déconnexion SMB et des événements de mise en attente des règles d'accès central

La prise en charge de l'audit des événements de connexion et de déconnexion SMB et de l'activation des règles d'accès central commence avec clustered Data ONTAP 8.3. Si vous rétablissez une version de ONTAP qui ne prend pas en charge ces types d'événements et que vous disposez de configurations d'audit qui surveillent ces types d'événements, vous devez modifier la configuration d'audit de ces SVM activés par audit avant de procéder à un rétablissement. Vous devez modifier la configuration de manière à ce que seuls les événements file-op soient audités.

Dépanner les problèmes d'espace des volumes liés à l'audit et au staging

Des problèmes peuvent survenir lorsqu'il n'y a pas suffisamment d'espace sur les volumes d'activation ou sur le volume contenant les journaux d'événements d'audit. Si l'espace est insuffisant, les nouveaux enregistrements d'audit ne peuvent pas être créés, ce qui empêche les clients d'accéder aux données et les demandes d'accès échouent. Vous devez savoir comment résoudre ces problèmes d'espace de volume.

Résolution des problèmes d'espace liés aux volumes du journal des événements

Si les volumes contenant des fichiers journaux d'événements sont à court d'espace, l'audit ne peut pas convertir les enregistrements de journal en fichiers journaux. Cela entraîne des échecs d'accès client. Vous devez savoir comment résoudre les problèmes d'espace liés aux volumes des journaux d'événements.

- En affichant les informations sur l'utilisation et la configuration des volumes et des agrégats, les administrateurs du cluster et des serveurs virtuels de stockage peuvent déterminer si l'espace disponible est insuffisant.
- En cas de manque d'espace dans les volumes contenant les journaux d'événements, les administrateurs du SVM et du cluster peuvent résoudre ces problèmes d'espace en supprimant certains fichiers journaux d'événements ou en augmentant la taille du volume.



Si l'agrégat contenant le volume du journal des événements est plein, la taille de l'agrégat doit être augmentée avant que vous puissiez augmenter la taille du volume. Seul un administrateur de cluster peut augmenter la taille d'un agrégat.

- Le chemin de destination des fichiers journaux d'événements peut être modifié en répertoire sur un autre volume en modifiant la configuration d'audit.



L'accès aux données est refusé dans les cas suivants :

- Le répertoire de destination est supprimé.
- La limite de fichier d'un volume, qui héberge le répertoire de destination, atteint son niveau maximal.

En savoir plus sur :

- "Afficher des informations sur les volumes et augmenter leur taille".
- "Afficher des informations sur les agrégats et la gestion des agrégats".

Résoudre les problèmes d'espace liés aux volumes de transfert

Si l'un des volumes contenant des fichiers de transfert de votre machine virtuelle de stockage (SVM) manque d'espace, l'audit ne peut pas écrire les enregistrements des journaux dans les fichiers intermédiaires. Cela entraîne des échecs d'accès client. Pour résoudre ce problème, vous devez déterminer si certains volumes de transit utilisés dans le SVM sont pleins en affichant des informations sur l'utilisation du volume.

Si le volume contenant les fichiers journaux d'événements consolidés dispose de suffisamment d'espace, mais que l'espace occupé par les clients est insuffisant, les volumes intermédiaires risquent de manquer d'espace. L'administrateur du SVM doit vous contacter pour déterminer si l'espace des volumes intermédiaires contenant des fichiers de transfert pour la SVM est insuffisant. Le sous-système d'audit génère un événement EMS si les événements d'audit ne peuvent pas être générés en raison d'un espace insuffisant dans un volume de staging. Le message suivant s'affiche : `No space left on device`. Seul vous pouvez afficher les informations relatives aux volumes de transfert ; les administrateurs du SVM ne le peuvent pas.

Tous les noms de volumes de staging commencent par `MDV_aud_` Suivi par l'UUID de l'agrégat contenant ce volume intermédiaire. L'exemple suivant montre quatre volumes système sur le SVM admin, qui ont été automatiquement créés lors de la création d'une configuration d'audit des services de fichiers pour un SVM de données dans le cluster :

```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
Used%						
-----	-----	-----	-----	----	-----	-----

cluster1	MDV_aud_1d0131843d4811e296fc123478563412					
		aggr0	online	RW	5GB	4.75GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412					
		root_vs0	online	RW	5GB	4.75GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412					
		aggr1	online	RW	5GB	4.75GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412					
		aggr2	online	RW	5GB	4.75GB
5%						

4 entries were displayed.

Si l'espace disponible dans les volumes de transfert est insuffisant, vous pouvez résoudre les problèmes d'espace en augmentant la taille du volume.



Si l'agrégat contenant le volume intermédiaire est saturé, vous devez augmenter la taille de l'agrégat avant de pouvoir augmenter la taille du volume. Seul vous pouvez augmenter la taille d'un agrégat. Les administrateurs du SVM ne le peuvent pas.

Si un ou plusieurs agrégats ont un espace disponible inférieur à 2 Go (dans ONTAP 9.14.1 et versions antérieures) ou 5 Go (à partir de ONTAP 9.15.1), la création de l'audit du SVM échoue. Lorsque la création d'un audit SVM échoue, les volumes de transit qui ont été créés sont supprimés.

Informations sur le copyright

Copyright © 2024 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 DÉLICTELLE (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.