Sécurité et chiffrement des données

ONTAP 9

NetApp
April 24, 2024

Sommaire

Sécurité et chiffrement des données

Présentation de la gestion de la sécurité avec System Manager

Depuis ONTAP 9.7, vous pouvez gérer la sécurité du cluster avec System Manager.

System Manager vous permet d'utiliser des méthodes standard ONTAP pour sécuriser l'accès des clients et des administrateurs au stockage et vous protéger contre les virus. Des technologies avancées sont disponibles pour le chiffrement des données au repos et WORM.

Si vous utilisez System Manager classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à "System Manager Classic (ONTAP 9.0 à 9.7)"

Analyse antivirus

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur le système de stockage afin de protéger vos données contre les virus ou tout autre code malveillant. L'analyse antivirus ONTAP, appelée *Vscan*, associe le meilleur logiciel antivirus tiers à des fonctionnalités ONTAP, vous offrant ainsi la flexibilité nécessaire pour contrôler quels fichiers sont analysés et à quel moment.

Le cryptage

ONTAP propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

Stockage WORM

SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM_ (Write Once, Read Many) pour conserver les fichiers stratégiques sous une forme non modifiée aux fins réglementaires et de gouvernance.

Protégez-vous contre les ransomware

Présentation de la protection autonome contre les ransomwares

Depuis ONTAP 9.10.1, la fonctionnalité ARP (autonome ransomware protection) utilise l'analyse des workloads dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive les activités anormales qui pourraient indiquer une attaque par ransomware.

Lorsqu'une attaque est suspectée, ARP crée également de nouvelles copies Snapshot, en plus de la protection existante à partir de copies Snapshot planifiées.

Licences et activation

ARP requiert une licence. ARP est disponible avec le "Licence ONTAP ONE". Si vous ne disposez pas de la licence ONTAP One, d'autres licences sont disponibles pour utiliser ARP, qui varient selon votre version de ONTAP.

Versions d'ONTAP	Licence
ONTAP 9.11.1 et versions ultérieures	Protection contre les ransomwares
ONTAP 9.10.1	MT_EK_MGMT (gestion des clés mutualisée)

- Si vous effectuez une mise à niveau vers ONTAP 9.11.1 ou version ultérieure et que ARP est déjà configuré sur votre système, vous n'avez pas besoin d'acheter la nouvelle licence anti-ransomware. Pour les nouvelles configurations ARP, la nouvelle licence est requise.
- Si vous effectuez une restauration depuis ONTAP 9.11.1 ou une version ultérieure vers ONTAP 9.10.1 et que vous avez activé ARP avec la licence anti-ransomware, un message d'avertissement s'affiche et vous devrez peut-être reconfigurer ARP. "Découvrez le rétablissement ARP".

Vous pouvez configurer le protocole ARP par volume à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

Stratégie ONTAP de protection contre les ransomwares

Une stratégie efficace de détection des ransomwares doit inclure plus d'une couche de protection unique

On pourrait comparer les caractéristiques de sécurité d'un véhicule. Vous ne vous fiez pas à une seule fonction, telle qu'une ceinture de sécurité, pour vous protéger complètement en cas d'accident. Les sacs gonflables, les freins antiblocage et l'avertissement de collision avant sont tous des dispositifs de sécurité supplémentaires qui permettront d'obtenir un meilleur résultat. La protection contre les ransomwares doit être vue de la même manière.

Tandis que ONTAP inclut des fonctionnalités comme FPolicy, les copies Snapshot, SnapLock et Active IQ Digital Advisor pour vous protéger contre les attaques par ransomware, les informations suivantes se concentrent sur la fonctionnalité intégrée ARP avec des fonctionnalités de machine learning.

Pour en savoir plus sur les autres fonctionnalités anti-ransomware d'ONTAP, consultez la page "Tr-4572 : solution NetApp pour ransomware"

Ce que le protocole ARP détecte

Le protocole ARP est conçu pour vous protéger contre les attaques par déni de service où l'attaquant conserve ses données jusqu'au paiement d'une rançon. ARP propose une détection anti-ransomware basée sur :

- Identification des données entrantes comme cryptées ou en texte clair.
- Les analyses, qui détectent
  - **Entropy**: Une évaluation du caractère aléatoire des données dans un fichier
  - **Types d'extension de fichier** : extension non conforme au type d'extension normal
  - **File IOPS** : une augmentation de l'activité de volume anormale avec le chiffrement des données (à partir de ONTAP 9.11.1)

ARP peut détecter la propagation de la plupart des attaques par ransomware après le chiffrement d'un petit nombre de fichiers uniquement, l'action automatique pour protéger les données et vous avertir qu'une attaque suspectée a lieu.

> Aucun système de détection ou de prévention par ransomware ne peut garantir la sécurité en cas d'attaque par ransomware. Bien qu'il soit possible qu'une attaque ne soit pas détectée, ARP agit comme une couche supplémentaire importante de défense si un logiciel antivirus ne parvient pas à détecter une intrusion.

Modes d'apprentissage et actifs

ARP a deux modes :

- **Apprentissage** (ou mode de fonctionnement à sec)
- **Actif** (ou mode « activé »)

Lorsque vous activez ARP, il s'exécute en *mode d'apprentissage*. En mode apprentissage, le système ONTAP développe un profil d'alerte basé sur les zones analytiques : entropie, types d'extension de fichier et IOPS de fichier. Après avoir exécuté ARP en mode d'apprentissage pendant suffisamment de temps pour évaluer les caractéristiques de la charge de travail, vous pouvez passer en mode actif et commencer à protéger vos données. Une fois que le protocole ARP est passé en mode actif, ONTAP crée des copies Snapshot ARP pour protéger les données en cas de détection d'une menace.

Il est recommandé de laisser ARP en mode d'apprentissage pendant 30 jours. À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur, qui peut se produire avant 30 jours.

En mode actif, si une extension de fichier est marquée comme anormale, vous devez évaluer l'alerte. Vous pouvez agir sur l'alerte pour protéger vos données ou marquer l'alerte comme un faux positif. Le fait de marquer une alerte comme un faux positif met à jour le profil d'alerte. Par exemple, si l'alerte est déclenchée par une nouvelle extension de fichier et que vous marquez l'alerte comme un faux positif, vous ne recevrez pas d'alerte la prochaine fois que l'extension de fichier sera observée. La commande `security anti-ransomware volume workload-behavior show` affiche les extensions de fichier qui ont été détectées dans le volume. (Si vous exécutez cette commande très tôt en mode d'apprentissage et qu'elle affiche une représentation précise des types de fichiers, vous ne devez pas utiliser ces données comme base pour passer en mode actif, car ONTAP collecte toujours d'autres metrics.)

À partir de ONTAP 9.11.1, vous pouvez personnaliser les paramètres de détection pour ARP. Pour plus d'informations, voir Gérer les paramètres de détection d'attaque ARP.

Évaluation des menaces et copies Snapshot ARP

En mode actif, ARP évalue la probabilité de menace en fonction des données entrantes mesurées par rapport aux analyses apprises. Une mesure est attribuée lorsque ARP détecte une menace :

- **Faible** : la première détection d'une anomalie dans le volume (par exemple, une nouvelle extension de fichier est observée dans le volume).
- **Modéré**: Plusieurs fichiers avec la même extension de fichier jamais vu-avant sont observés.
  - Dans ONTAP 9.10.1, le seuil de remontée à modéré est de 100 fichiers ou plus. À partir de ONTAP 9.11.1, la quantité du fichier peut être modifiée ; sa valeur par défaut est 20.

En cas de menace faible, ONTAP détecte une anomalie et crée une copie Snapshot du volume pour créer le meilleur point de restauration. ONTAP ajoute au nom de la copie snapshot ARP le préfixe `Anti-ransomware-backup` pour le rendre facilement identifiable, par exemple `Anti_ransomware_backup.2022-12-20_1248`.

La menace passe au niveau modéré après l'exécution d'un rapport d'analytique par ONTAP qui détermine si

l'anomalie correspond à un profil de ransomware. Les menaces qui restent au niveau bas sont consignées et visibles dans la section **événements** de System Manager. Lorsque la probabilité d'attaque est modérée, ONTAP génère une notification EMS vous invitant à évaluer la menace. ONTAP n'envoie pas d'alertes en cas de menaces faibles, mais à partir de ONTAP 9.14.1, vous pouvez le faire modifier les paramètres des alertes. Pour plus d'informations, voir Réagir à une activité anormale.

Vous pouvez afficher des informations sur une menace, quel que soit le niveau, dans la section **événements** de System Manager ou avec le `security anti-ransomware volume show` commande.

Les copies Snapshot ARP sont conservées pendant au moins deux jours. À partir de ONTAP 9.11.1, vous pouvez modifier les paramètres de rétention. Pour plus d'informations, voir Modifiez les options des copies Snapshot.

Comment récupérer des données dans ONTAP après une attaque par ransomware

Lorsqu'une attaque est suspectée, le système prend une copie Snapshot du volume à ce moment-là et verrouille cette copie. Si l'attaque est confirmée ultérieurement, le volume peut être restauré à l'aide de la copie ARP Snapshot.

La suppression des copies Snapshot verrouillées ne peut pas être effectuée par des moyens normaux. Cependant, si vous décidez plus tard de marquer l'attaque comme un faux positif, la copie verrouillée sera supprimée.

En connaissant les fichiers affectés et l'heure de l'attaque, il est possible de restaurer de manière sélective les fichiers affectés à partir de plusieurs copies Snapshot, plutôt que de simplement restaurer le volume entier vers l'une des copies Snapshot.

ARP s'appuie donc sur la technologie de protection des données et de reprise après incident ONTAP éprouvée pour répondre aux attaques par ransomware. Pour plus d'informations sur la récupération de données, reportez-vous aux rubriques suivantes.

- "Restauration à partir de copies Snapshot (System Manager)"
- "Restauration de fichiers à partir de copies Snapshot (interface de ligne de commandes)"
- "Restauration intelligente par ransomware"

Cas d'utilisation et considérations relatives à la protection autonome contre les ransomwares

La protection anti-ransomware autonome (ARP) est disponible pour les charges de travail NAS à partir de ONTAP 9.10.1. Avant de déployer ARP, vous devez connaître les utilisations recommandées et les configurations prises en charge, ainsi que les implications en termes de performances.

Configurations prises en charge et non prises en charge

Lorsque vous décidez d'utiliser ARP, il est important de vous assurer que la charge de travail de votre volume est adaptée à ARP et qu'elle répond aux configurations système requises.

Charges de travail adaptées

ARP est adapté pour :

- Les bases de données sur le stockage NFS

- Répertoires locaux Windows ou Linux

  Comme les utilisateurs pouvaient créer des fichiers avec des extensions qui n'ont pas été détectées pendant la période d'apprentissage, les risques de faux positifs sont plus élevés dans cette charge de travail.

- Images et vidéos

  Par exemple, les dossiers médicaux et les données EDA

Charges de travail non adaptées

ARP n'est pas adapté pour :

- Les workloads comportant une fréquence élevée de création ou de suppression de fichiers (des centaines de milliers de fichiers en quelques secondes, par exemple des workloads de test/développement).
- La détection des menaces par ARP dépend de sa capacité à reconnaître une augmentation inhabituelle de l'activité de création, de renommage ou de suppression de fichiers. Si l'application elle-même est la source de l'activité des fichiers, elle ne peut pas être efficacement distinguée de l'activité des ransomware.
- Charges de travail où l'application ou l'hôte chiffre les données.
  ARP dépend de la distinction des données entrantes comme chiffrées ou non chiffrées. Si l'application elle-même est en train de chiffrer les données, l'efficacité de la fonction est réduite. Toutefois, la fonction peut toujours fonctionner en fonction de l'activité du fichier (supprimer, écraser ou créer, ou créer ou renommer avec une nouvelle extension de fichier) et du type de fichier.

Configurations compatibles

ARP est disponible pour les volumes NFS et SMB dans les systèmes ONTAP sur site à partir de ONTAP 9.10.1.

La prise en charge d'autres configurations et types de volumes est disponible dans les versions ONTAP suivantes :

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes protégés avec SnapMirror asynchrone	✓	✓	✓		
SVM protégé avec SnapMirror asynchrone (reprise après incident SVM)	✓	✓	✓		
Mobilité des données des SVM (`vserver migrate`)	✓	✓	✓		
Volumes FlexGroup	✓	✓			

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Vérification multi-administrateurs	✓	✓			

Interopérabilité SnapMirror et ARP

À partir de ONTAP 9.12.1, ARP est pris en charge sur les volumes de destination SnapMirror asynchrones. ARP est **non** pris en charge avec SnapMirror Synchronous.

Si un volume source SnapMirror est compatible ARP, le volume de destination SnapMirror acquiert automatiquement l'état de configuration ARP (apprentissage, activation, etc.), les données d'entraînement ARP et le snapshot créé par ARP du volume source. Aucune activation explicite n'est requise.

Alors que le volume de destination se compose de copies Snapshot RO (lecture seule), aucun traitement ARP n'est effectué sur ses données. Toutefois, lorsque le volume de destination SnapMirror est converti en lecture-écriture (RW), ARP est automatiquement activé sur le volume de destination converti en RW. Le volume de destination ne nécessite pas de procédure d'apprentissage supplémentaire en plus de ce qui est déjà enregistré sur le volume source.

Dans ONTAP 9.10.1 et 9.11.1, SnapMirror ne transfère pas l'état de configuration ARP, les données d'entraînement et les copies Snapshot des volumes source vers les volumes de destination. Ainsi, lorsque le volume de destination SnapMirror est converti en RW, ARP sur le volume de destination doit être explicitement activé en mode apprentissage une fois la conversion terminée.

ARP et machines virtuelles

ARP est pris en charge avec les machines virtuelles (VM). La détection ARP se comporte différemment pour les modifications à l'intérieur et à l'extérieur de la machine virtuelle. ARP n'est pas recommandé pour les workloads avec des fichiers fortement entropie dans la machine virtuelle.

Modifications en dehors de la VM

ARP peut détecter les modifications d'extension de fichier sur un volume NFS en dehors de la machine virtuelle si une nouvelle extension entre dans le volume chiffré ou si une extension de fichier change. Les modifications d'extension de fichier détectables sont les suivantes :

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

Modifications au sein de la machine virtuelle

Si l'attaque par ransomware cible la machine virtuelle et les fichiers à l'intérieur de la machine virtuelle sont modifiés sans effectuer de modifications à l'extérieur de la machine virtuelle, ARP détecte la menace si l'entropie par défaut de la machine virtuelle est faible (par exemple, fichiers .txt, .docx ou .mp4). Bien que ARP crée un instantané de protection dans ce scénario, il ne génère pas d'alerte de menace car les extensions de fichiers en dehors de la machine virtuelle n'ont pas été falsifiées.

Si, par défaut, les fichiers sont à haute entropie (par exemple, les fichiers .gzip ou protégés par mot de passe), les capacités de détection d'ARP sont limitées. ARP peut toujours prendre des snapshots proactifs dans cette instance, cependant aucune alerte ne sera déclenchée si les extensions de fichier n'ont pas été falsifiées en externe.

Configurations non prises en charge

ARP n'est pas pris en charge dans les configurations système suivantes :

- Les environnements ONTAP S3
- Environnements SAN

ARP ne prend pas en charge les configurations de volume suivantes :

- Volumes FlexGroup (dans ONTAP 9.10.1 à 9.12.1. À partir de ONTAP 9.13.1, les volumes FlexGroup sont pris en charge)
- Volumes FlexCache (ARP est pris en charge sur les volumes FlexVol d'origine, mais pas sur les volumes de cache)
- Les volumes hors ligne
- Volumes SAN uniquement
- Volumes SnapLock
- SnapMirror synchrone
- SnapMirror asynchrone (non pris en charge uniquement dans ONTAP 9.10.1 et 9.11.1) SnapMirror asynchrone est pris en charge à partir de ONTAP 9.12.1. Pour plus d'informations, voir [snapmirror].)
- Volumes restreints
- Volumes root des VM de stockage
- Volumes des machines virtuelles de stockage arrêtées

Considérations relatives aux performances ARP et à la fréquence

Le protocole ARP peut avoir un impact minimal sur les performances du système, mesuré en débit et en pic d'IOPS. L'impact de la fonctionnalité ARP dépend des charges de travail de volume spécifiques. Pour les charges de travail courantes, les limites de configuration suivantes sont recommandées :

Caractéristiques de la charge de travail	Limite de volume recommandée par nœud	Dégradation des performances lorsque la limite de volume par nœud est dépassée :[*]
Ces données intensives en lecture ou compressées peuvent être compressées.	150	4 % des IOPS maximales

Caractéristiques de la charge de travail	Limite de volume recommandée par nœud	Dégradation des performances lorsque la limite de volume par nœud est dépassée :[*]
Des opérations d'écriture intensives et des données ne peuvent pas être compressées.	60	10 % des IOPS maximales

Pass:[*] les performances du système ne sont pas dégradées au-delà de ces pourcentages, quel que soit le nombre de volumes ajoutés au-delà des limites recommandées.

L'analyse ARP étant exécutée selon une séquence prioritaire, à mesure que le nombre de volumes protégés augmente, l'analyse s'exécute moins souvent sur chaque volume.

Vérification multiadministrateur avec volumes protégés par ARP

À partir de ONTAP 9.13.1, vous pouvez activer la vérification multiadministrateur (MAV) pour une sécurité supplémentaire avec ARP. MAV s'assure qu'au moins deux administrateurs authentifiés sont requis pour désactiver ARP, mettre en pause ARP ou marquer une attaque suspecte comme faux positif sur un volume protégé. Découvrez comment "Activez MAV pour les volumes protégés par ARP".

Vous devez définir des administrateurs pour un groupe MAV et créer des règles MAV pour le `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, et `security anti-ransomware volume attack clear-suspect` Commandes ARP à protéger. Chaque administrateur du groupe MAV doit approuver chaque nouvelle demande de règle et "Ajoutez à nouveau la règle MAV" Dans les paramètres MAV.

Depuis ONTAP 9.14.1, ARP propose des alertes pour la création d'un instantané ARP et pour l'observation d'une nouvelle extension de fichier. Les alertes pour ces événements sont désactivées par défaut. Les alertes peuvent être définies au niveau du volume ou des SVM. Vous pouvez créer des règles MAV au niveau du SVM à l'aide de `security anti-ransomware vserver event-log modify` ou au niveau du volume avec `security anti-ransomware volume event-log modify`.

Étapes suivantes

- "Activation de la protection autonome contre les ransomwares"
- "Activez MAV pour les volumes protégés par ARP"

Activation de la protection autonome contre les ransomwares

Depuis ONTAP 9.10.1, la protection autonome contre les ransomwares (ARP) peut être activée sur les volumes nouveaux ou existants. Vous commencez par activer ARP en mode d'apprentissage, dans lequel le système analyse la charge de travail pour caractériser le comportement normal. Vous pouvez activer ARP sur un volume existant ou créer un nouveau volume et activer ARP depuis le début.

Description de la tâche

Vous devez toujours activer le protocole ARP au départ en mode d'apprentissage (ou d'exécution à sec). Le démarrage en mode actif peut entraîner des rapports faux positifs excessifs.

Il est recommandé de laisser ARP fonctionner en mode d'apprentissage pendant au moins 30 jours. À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur, qui peut se produire avant 30 jours. Pour plus d'informations, voir "Modes d'apprentissage et

actifs".

> Dans les volumes existants, les modes d'apprentissage et actif s'appliquent uniquement aux données nouvellement écrites, et non aux données existantes du volume. Les données existantes ne sont pas analysées et analysées, car les caractéristiques du trafic de données normal antérieur sont présumées basées sur les nouvelles données une fois que le volume est activé pour ARP.

Avant de commencer

- Une VM de stockage (SVM) doit être activée pour NFS ou SMB (ou les deux).
- Le licence correcte Doit être installé pour votre version ONTAP.
- Vous devez avoir une charge de travail NAS avec des clients configurés.
- Le volume sur lequel vous souhaitez définir ARP doit être protégé et doit avoir un actif "chemin de jonction".
- Le volume doit être rempli à moins de 100 %.
- Il est recommandé de configurer le système EMS pour envoyer des notifications par e-mail, qui incluront des notifications d'activité ARP. Pour plus d'informations, voir "Configurez les événements EMS pour envoyer des notifications par e-mail".
- À partir de la version ONTAP 9.13.1, il est recommandé d'activer la vérification multiadministrateur afin que deux administrateurs d'utilisateurs authentifiés ou plus soient requis pour la configuration ARP (Autonomous ransomware protection). Pour plus d'informations, voir "Activez la vérification multiadministrateur".

Activez ARP

Vous pouvez activer le protocole ARP à l'aide de System Manager ou de l'interface de ligne de commande ONTAP.

System Manager

Étapes

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume à protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé en mode apprentissage dans la zone **anti-ransomware**.
3. Lorsque la période d'apprentissage est terminée, passez ARP en mode actif.

   > À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur. C'est possible "Désactivez ce paramètre sur la machine virtuelle de stockage associée" si vous souhaitez contrôler manuellement le mode d'apprentissage en mode actif.

   a. Sélectionnez **stockage > volumes**, puis sélectionnez le volume prêt pour le mode actif.
   b. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **basculer** en mode actif dans la zone anti-ransomware.
4. Vous pouvez vérifier l'état ARP du volume dans la zone **anti-ransomware**.

   Pour afficher l'état ARP de tous les volumes : dans le volet **volumes**, sélectionnez **Afficher/Masquer**, puis assurez-vous que l'état **anti-ransomware** est vérifié.

CLI

Le processus d'activation de ARP avec l'interface de ligne de commande diffère si vous l'activez sur un volume existant par rapport à un nouveau volume.

Activez ARP sur un volume existant

1. Modifiez un volume existant pour activer la protection par ransomware en mode d'apprentissage :

   ```
   security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
   ```

   Si vous utilisez ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif soit effectué automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, modifier le paramètre au niveau du SVM sur tous les volumes associés :

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Lorsque la période d'apprentissage est terminée, modifiez le volume protégé pour passer en mode actif si ce n'est pas déjà fait automatiquement :

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   Vous pouvez également passer en mode actif à l'aide de la commande modifier le volume :

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Vérifiez l'état ARP du volume.

   ```
   security anti-ransomware volume show
   ```

Activez ARP sur un nouveau volume

1. Créez un volume avec la protection anti-ransomware activée avant le provisionnement des données.

   ```
   volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size
   nn -anti-ransomware-state dry-run -junction-path /path_name
   ```

   Si vous utilisez ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif soit effectué automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, modifier le paramètre au niveau du SVM sur tous les volumes associés :

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Lorsque la période d'apprentissage est terminée, modifiez le volume protégé pour passer en mode actif si ce n'est pas déjà fait automatiquement :

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   Vous pouvez également passer en mode actif à l'aide de la commande modifier le volume :

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Vérifiez l'état ARP du volume.

   ```
   security anti-ransomware volume show
   ```

Activez la protection autonome par défaut contre les ransomwares dans les nouveaux volumes

Depuis ONTAP 9.10.1, vous pouvez configurer des machines virtuelles de stockage (SVM) de manière à ce que les nouveaux volumes soient activés par défaut pour le mode d'apprentissage ARP (autonome ransomware protection).

Description de la tâche

Par défaut, de nouveaux volumes sont créés avec ARP en mode désactivé. Vous pouvez modifier ce paramètre dans System Manager et via l'interface de ligne de commandes. Les volumes activés par défaut sont définis sur ARP en mode d'apprentissage (ou d'exécution à sec).

ARP ne sera activé que sur les volumes créés dans le SVM après avoir modifié le paramètre. ARP ne sera pas activé sur les volumes existants. Découvrez comment "Activez ARP dans un volume existant".

À partir de ONTAP 9.13.1, l'apprentissage adaptatif a été ajouté à l'analyse ARP et le passage du mode d'apprentissage au mode actif s'effectue automatiquement. Pour plus d'informations, voir "Modes d'apprentissage et actifs".

Avant de commencer

- Le licence correcte Doit être installé pour votre version ONTAP.
- Le volume doit être rempli à moins de 100 %.

- Les chemins de jonction doivent être actifs.
- À partir de la version ONTAP 9.13.1, il est recommandé d'activer la vérification multiadministrateur afin que deux administrateurs d'utilisateurs authentifiés minimum soient requis pour les opérations anti-ransomware. "En savoir plus >>".

Basculez ARP du mode d'apprentissage au mode actif

À partir de la ONTAP 9.13.1, l'apprentissage adaptatif a été ajouté à l'analyse ARP. Le passage du mode d'apprentissage au mode actif s'effectue automatiquement. La décision autonome prise par ARP de passer automatiquement du mode d'apprentissage au mode actif est basée sur les paramètres de configuration des options suivantes :

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

Après 30 jours d'apprentissage, un volume passe automatiquement en mode actif même si une ou plusieurs de ces conditions ne sont pas satisfaites. Autrement dit, si le commutateur automatique est activé, le volume passe en mode actif au bout de 30 jours maximum. La valeur maximale de 30 jours est fixe et non modifiable.

Pour plus d'informations sur les options de configuration ARP, y compris les valeurs par défaut, reportez-vous au "Référence de commande ONTAP".

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour activer le protocole ARP par défaut.

System Manager

1. Sélectionnez **Storage > Storage VM**, puis sélectionnez la VM de stockage contenant les volumes que vous souhaitez protéger avec ARP.
2. Accédez à l'onglet **Paramètres**. Sous **sécurité**, localisez la mosaïque **anti-ransomware**, puis sélectionnez
3. Cochez la case pour activer ARP pour les volumes NAS. Cochez la case supplémentaire pour activer ARP sur tous les volumes NAS éligibles de la machine virtuelle de stockage.

> Si vous avez effectué une mise à niveau vers ONTAP 9.13.1, le **passage automatique du mode apprentissage au mode actif après un apprentissage suffisant** est activé automatiquement. Cela permet à ARP de déterminer l'intervalle de la période d'apprentissage optimale et d'automatiser le passage en mode actif. Désactivez le paramètre si vous souhaitez passer manuellement en mode actif.

CLI

1. Modifier un SVM existant pour activer ARP par défaut dans les nouveaux volumes :
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   Au niveau de l'interface de ligne de commandes, vous pouvez également créer un nouveau SVM avec ARP activé par défaut pour les nouveaux volumes.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   Si vous avez mis à niveau vers ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif s'effectue automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, utilisez la commande suivante :

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

Mettez en pause la protection autonome contre les ransomwares pour exclure les événements des charges de travail de l'analyse

Si vous attendez des événements inhabituels des charges de travail, vous pouvez suspendre et reprendre temporairement l'analyse ARP (autonome ransomware protection) à tout moment.

À partir de ONTAP 9.13.1, vous pouvez activer la vérification multiadministrateur (MAV) de sorte que deux administrateurs d'utilisateurs authentifiés ou plus soient requis pour interrompre le protocole ARP. "En savoir plus >>".

Description de la tâche

Lors d'une pause ARP, aucun événement n'est enregistré et aucune action n'est en cours pour les nouvelles écritures. Toutefois, le processus d'analytique continue pour les journaux précédents en arrière-plan.

N’utilisez pas la fonction de désactivation ARP pour interrompre l’analyse. Ceci désactive ARP sur le volume et toutes les informations existantes concernant le comportement de la charge de travail apprise sont perdues. Cela nécessiterait un redémarrage de la période d’apprentissage.

Étapes

Vous pouvez utiliser System Manager ou l’interface de ligne de commandes de ONTAP pour interrompre le protocole ARP.

System Manager

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume sur lequel vous souhaitez mettre en pause ARP.
2. Dans l'onglet **sécurité** de la vue d'ensemble des volumes, sélectionnez **Pause anti-ransomware** dans la zone **anti-ransomware**.

> À partir de ONTAP 9.13.1, si vous utilisez MAV pour protéger vos paramètres ARP, l'opération de pause vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. "L'approbation doit être reçue de tous les administrateurs" Associé au groupe d'approbation MAV ou l'opération échouera.

CLI

1. Suspendre ARP sur un volume :

   ```
   security anti-ransomware volume pause -vserver svm_name -volume vol_name
   ```

2. Pour reprendre le traitement, utilisez `resume` paramètre.

   ```
   security anti-ransomware volume resume -vserver svm_name -volume vol_name
   ```

3. **Si vous utilisez MAV (disponible avec ARP à partir de ONTAP 9.13.1) pour protéger vos paramètres ARP,** l'opération de pause vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. L'approbation doit être reçue de tous les administrateurs associés au groupe d'approbation MAV, faute de quoi l'opération échouera.

   Si vous utilisez MAV et qu'une opération de pause attendue nécessite des approbations supplémentaires, chaque approbateur de groupe MAV effectue les opérations suivantes :

   a. Afficher la demande :

      ```
      security multi-admin-verify request show
      ```

   b. Approuver la demande :

      ```
      security multi-admin-verify request approve -index[number returned from show request]
      ```

      La réponse du dernier approbateur de groupe indique que le volume a été modifié et que l'état du protocole ARP est mis en pause.

      Si vous utilisez MAV et que vous êtes un approbateur de groupe MAV, vous pouvez rejeter une demande d'opération de pause :

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Gérez les paramètres de détection des attaques par protection anti-ransomware autonome

À partir de la version ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des ransomwares sur un volume spécifique optimisé par la protection anti-ransomware autonome et signaler une augmentation connue sous le nom d'activité de fichier normale. Le réglage des paramètres de détection permet d'améliorer la précision des rapports en fonction de votre charge de travail de volume spécifique.

Fonctionnement de la détection des attaques

Lorsque la protection anti-ransomware autonome (ARP) est en mode d'apprentissage, elle développe des valeurs de base pour les comportements de volume. Il s'agit d'entropie, d'extensions de fichiers et, à partir de ONTAP 9.11.1, d'IOPS. Ces données de base sont utilisées pour évaluer les menaces de ransomware. Pour plus d'informations sur ces critères, reportez-vous à la section Ce que le protocole ARP détecte.

Dans ONTAP 9.10.1, ARP émet un avertissement s'il détecte les deux conditions suivantes :

- plus de 20 fichiers avec des extensions de fichier qui n'ont pas été observées précédemment dans le volume
- données d'entropie élevées

À partir de ONTAP 9.11.1, ARP émet un avertissement de menace si *seule* une condition est remplie. Par exemple, si plus de 20 fichiers avec des extensions de fichier qui n'ont pas été observées précédemment dans le volume sont observés dans une période de 24 heures, ARP catégorise ceci comme une menace *indépendamment* de l'entropie observée. (Les valeurs de fichier 24 heures et 20 sont des valeurs par défaut, qui peuvent être modifiées.)

À partir de ONTAP 9.14.1, vous pouvez configurer des alertes lorsque ARP observe une nouvelle extension de fichier et lorsque ARP crée un instantané. Pour plus d'informations, voir [modify-alerts]

Certains volumes et charges de travail requièrent des paramètres de détection différents. Par exemple, votre volume ARP peut héberger de nombreux types d'extensions de fichiers. Dans ce cas, vous pouvez modifier le nombre de seuils pour les extensions de fichiers jamais vues à un nombre supérieur à la valeur par défaut de 20 ou désactiver les avertissements basés sur des extensions de fichiers jamais vues. À partir de ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des attaques afin qu'ils s'adaptent mieux à vos workloads spécifiques.

Modifier les paramètres de détection d'attaque

Selon les comportements attendus de votre volume ARP, vous pouvez modifier les paramètres de détection d'attaque.

Étapes

1. Afficher les paramètres de détection d'attaque existants :

   ```
   security anti-ransomware volume attack-detection-parameters show -vserver
   svm_name -volume volume_name
   ```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                                Vserver Name : vs1
                                                 Volume Name : vol1
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                  Is Detection Based on File Create Rate? : true
                  Is Detection Based on File Rename Rate? : true
                  Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24
```

2. Tous les champs affichés peuvent être modifiés avec des valeurs booléennes ou entières. Pour modifier un champ, utilisez `security anti-ransomware volume attack-detection-parameters modify` commande.

   Pour obtenir la liste complète des paramètres, reportez-vous à la section "Référence de commande ONTAP".

Signaler les surtensions connues

ARP continue de modifier les valeurs de base pour les paramètres de détection, même en mode actif. Si vous connaissez des surtensions dans votre activité de volume—des surtensions ou une surtension qui est caractéristique d'une nouvelle normale—vous devriez la signaler comme sûre. La déclaration manuelle de ces surtensions comme étant sûres contribue à améliorer la précision des évaluations des menaces d'ARP.

Signaler une surtension ponctuelle

1. Si une surtension ponctuelle se produit dans des circonstances connues et que vous souhaitez que ARP signale une surtension similaire dans des circonstances futures, éliminez la poussée du comportement de la charge de travail :

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   svm_name -volume volume_name
   ```

Modifier la surtension de la ligne de base

1. Si une surtension signalée doit être considérée comme un comportement normal de l'application, signalez-la en tant que telle pour modifier la valeur de surtension de la ligne de base.

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver svm_name -volume volume_name
   ```

Configurez les alertes ARP

Depuis ONTAP 9.14.1, ARP vous permet de spécifier des alertes pour deux événements ARP :

- Observation de la nouvelle extension de fichier sur un volume
- Création d'un instantané ARP

Les alertes liées à ces deux événements peuvent être définies sur des volumes individuels ou pour l'ensemble du SVM. Si vous activez des alertes pour le SVM, les paramètres d'alerte ne sont hérités que par les volumes créés après l'activation de l'alerte. Par défaut, les alertes ne sont activées sur aucun volume.

Les alertes d'événements peuvent être contrôlées par une vérification multiadministrateur. Pour plus d'informations, voir Vérification multiadministrateur avec volumes protégés par ARP.

System Manager

Définir des alertes pour un volume

1. Accédez à **volumes**. Sélectionnez le volume individuel pour lequel vous souhaitez modifier les paramètres.
2. Sélectionnez l'onglet **sécurité**, puis **Paramètres de sécurité des événements**.
3. Pour recevoir des alertes pour **Nouvelle extension de fichier détectée** et **instantané de ransomware créé**, sélectionnez le menu déroulant sous l'en-tête **gravité**. Modifiez le paramètre de **ne pas générer l'événement** à **Avis**.
4. Sélectionnez **Enregistrer**.

Définir des alertes pour un SVM

1. Naviguer jusqu'à **Storage VM** puis sélectionner le SVM pour lequel vous voulez activer les paramètres.
2. Sous la rubrique **sécurité**, repérez la carte **anti-ransomware**. Sélectionnez ⋮ Puis **Modifier la gravité des événements ransomware**.
3. Pour recevoir des alertes pour **Nouvelle extension de fichier détectée** et **instantané de ransomware créé**, sélectionnez le menu déroulant sous l'en-tête **gravité**. Modifiez le paramètre de **ne pas générer l'événement** à **Avis**.
4. Sélectionnez **Enregistrer**.

CLI

Définir des alertes pour un volume

- Pour définir des alertes pour une nouvelle extension de fichier :

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- Pour définir des alertes pour la création d'un instantané ARP :

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confirmez vos paramètres à l'aide du `anti-ransomware volume event-log show` commande.

Définir des alertes pour un SVM

- Pour définir des alertes pour une nouvelle extension de fichier :

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- Pour définir des alertes pour la création d'un instantané ARP :

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confirmez vos paramètres à l'aide du `security anti-ransomware vserver event-log show` commande.

Plus d'informations

- "Apprenez à comprendre les attaques de protection anti-ransomware autonomes et le snapshot de protection anti-ransomware autonome"

Réagir à une activité anormale

Lorsque la protection autonome contre les attaques par ransomware (ARP) détecte une activité anormale dans un volume protégé, elle émet un avertissement. Vous devez évaluer la notification pour déterminer si l'activité est acceptable (faux positif) ou si une attaque semble malveillante.

Description de la tâche

ARP affiche une liste des fichiers suspects lorsqu'il détecte une combinaison de données entropie élevée, une activité de volume anormale avec chiffrement des données et des extensions de fichier inhabituelles.

Lorsque l'avertissement est émis, vous pouvez répondre en marquant l'activité du fichier de l'une des deux façons suivantes :

- **Faux positif**

  Le type de fichier identifié est attendu dans votre charge de travail et peut être ignoré.

- **Attaque potentielle par ransomware**

  Le type de fichier identifié est inattendu dans votre charge de travail et doit être traité comme une attaque potentielle.

Dans les deux cas, la surveillance normale reprend après la mise à jour et la suppression des avis. ARP enregistre votre évaluation dans le profil d'évaluation des menaces, en utilisant votre choix pour surveiller les activités de fichiers suivantes.

Dans le cas d'une attaque suspectée, vous devez déterminer s'il s'agit d'une attaque, y répondre si c'est le cas et restaurer les données protégées avant d'effacer les notifications. "En savoir plus sur la manière de procéder à une reprise après une attaque par ransomware".

> Si vous restaurez un volume entier, il n'y a pas d'avis à effacer.

Avant de commencer

ARP doit être exécuté en mode actif.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour répondre à une tâche anormale.

System Manager

1. Lorsque vous recevez une notification d'activité anormale, suivez le lien ou naviguez jusqu'à l'onglet **sécurité** de l'aperçu **volumes**.

   Les avertissements s'affichent dans le volet **vue d'ensemble** du menu **Events**.

2. Lorsqu'un message "activité de volume anormale détectée" s'affiche, consultez les fichiers suspects.

   Dans l'onglet **sécurité**, sélectionnez **Afficher les types de fichiers suspects**.

3. Dans la boîte de dialogue **types de fichiers suspects**, examinez chaque type de fichier et marquez-le comme "Faux positif" ou "attaque par ransomware potentielle".

Si vous avez sélectionné cette valeur…	Prendre cette action…
Faux positif	Sélectionnez **mettre à jour** et **Effacer les types de fichiers suspects** pour enregistrer votre décision et reprendre la surveillance ARP normale. À partir de ONTAP 9.13.1, si vous utilisez MAV pour protéger vos paramètres ARP, l'opération Effacer-suspect vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. "L'approbation doit être reçue de tous les administrateurs" Associé au groupe d'approbation MAV ou l'opération échouera.
Attaques par ransomware potentielles	Répondez aux attaques et restaurez les données protégées. Sélectionnez ensuite **Update** et **Clear suspect File types** pour enregistrer votre décision et reprendre la surveillance ARP normale. Il n'existe aucun type de fichier suspect à effacer si vous avez restauré un volume entier.

CLI

1. Lorsque vous recevez une notification d'attaque par ransomware suspectée, vérifiez l'heure et la gravité de l'attaque :

   `security anti-ransomware volume show -vserver` *`svm_name`* `-volume` *`vol_name`*

   Sortie d'échantillon :

   ```
   Vserver Name: vs0
   Volume Name: vol1
   State: enabled
   Attack Probability: moderate
   Attack Timeline: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

   Vous pouvez également vérifier les messages EMS :

```
event log show -message-name callhome.arw.activity.seen
```

2. Générez un rapport d'attaque et notez l'emplacement de sortie :

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   Sortie d'échantillon :

   ```
   Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
   "vs0:vol1/"
   ```

3. Afficher le rapport sur un système client d'administration. Par exemple :

   ```
   [root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

   19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
   20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
   21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
   ```

4. Suivez l'une des actions suivantes en fonction de votre évaluation des extensions de fichier :

   - Faux positif

     Entrez la commande suivante pour enregistrer votre décision, en ajoutant la nouvelle extension à la liste de ceux autorisés et en redonnant une surveillance anti-ransomware normale :
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     Utilisez l'un des paramètres suivants pour identifier les extensions :
     `[-seq-no integer]` Numéro de séquence du fichier dans la liste des suspects.
     `[-extension text, … ]` Extensions de fichier
     `[-start-time date_time -end-time date_time]` Heures de début et de fin pour la plage de fichiers à effacer, sous la forme "MM/JJ/AAAA HH:MM:SS".

   - Attaque par ransomware potentielle

     Répondez à l'attaque et "Récupérez les données à partir de l'instantané de sauvegarde créé par ARP". Une fois les données récupérées, entrez la commande suivante pour enregistrer votre décision et reprendre la surveillance ARP normale :

     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive false`

     Utilisez l'un des paramètres suivants pour identifier les extensions :
     `[-seq-no integer]` Numéro de séquence du fichier dans la liste des suspects
     `[-extension text, … ]` Extension de fichier
     `[-start-time date_time -end-time date_time]` Heures de début et de fin pour la plage de fichiers à effacer, sous la forme "MM/JJ/AAAA HH:MM:SS".

Il n'existe aucun type de fichier suspect à effacer si vous avez restauré un volume entier. L'instantané de sauvegarde créé par ARP sera supprimé et le rapport d'attaque sera effacé.

5. Si vous utilisez MAV et un attendu `clear-suspect` L'opération nécessite des approbations supplémentaires, chaque approbateur de groupe MAV effectue les opérations suivantes :

   a. Afficher la demande :

   ```
   security multi-admin-verify request show
   ```

   b. Approuver la demande de reprise de la surveillance anti-ransomware classique :

   ```
   security multi-admin-verify request approve -index[number returned from show request]
   ```

   La réponse du dernier approbateur de groupe indique que le volume a été modifié et qu'un faux positif est enregistré.

6. Si vous utilisez MAV et que vous êtes un approbateur de groupe MAV, vous pouvez également rejeter une demande claire-suspecte :

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Plus d'informations

- "Base de connaissances : comprendre les attaques de protection anti-ransomware autonomes et le snapshot de protection anti-ransomware autonome".

Restaurez les données après une attaque par ransomware

La protection anti-ransomware autonome (ARP) crée des copies Snapshot nommées `Anti_ransomware_backup` lorsqu'il détecte une menace potentielle de ransomware. Vous pouvez utiliser l'une de ces copies snapshot ARP ou une autre copie Snapshot de votre volume pour restaurer les données.

Description de la tâche

Si le volume possède des relations SnapMirror, répliquez manuellement toutes les copies miroir du volume immédiatement après la restauration à partir d'une copie Snapshot. Cette opération risque d'entraîner des copies miroir inutilisables qui doivent d'être supprimées et recréées.

Pour effectuer une restauration à partir d'une copie Snapshot autre que le `Anti_ransomware_backup` Instantané après l'identification d'une attaque système, vous devez d'abord libérer l'instantané ARP.

Si aucune attaque système n'a été signalée, vous devez d'abord restaurer à partir du `Anti_ransomware_backup` La copie Snapshot effectue ensuite une restauration ultérieure du volume à partir de la copie Snapshot de votre choix.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour restaurer vos données.

System Manager

Restauration après une attaque système

1. Pour effectuer une restauration à partir de l'instantané ARP, passez à l'étape 2. Pour effectuer une restauration à partir d'une copie Snapshot antérieure, vous devez d'abord libérer le verrouillage de l'instantané ARP.
   a. Sélectionnez **stockage > volumes**.
   b. Sélectionnez **sécurité** puis **Afficher les types de fichiers suspects**
   c. Marquez les fichiers comme « Faux positif » .
   d. Sélectionnez **mettre à jour** et **Effacer les types de fichiers suspects**
2. Afficher les copies Snapshot dans des volumes :

   Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.

3. Sélectionnez ⋮ En regard de la copie Snapshot que vous souhaitez restaurer, puis de **Restore**.

Restaurez si aucune attaque système n'a été identifiée

1. Afficher les copies Snapshot dans des volumes :

   Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.

2. Sélectionnez ⋮ ils choisissent le `Anti_ransomware_backup` Snapshot.
3. Sélectionnez **Restaurer**.
4. Revenez au menu **copies Snapshot**, puis choisissez la copie Snapshot que vous souhaitez utiliser. Sélectionnez **Restaurer**.

CLI

Restauration après une attaque système

1. Pour effectuer une restauration à partir de la copie ARP Snapshot, passez à l'étape 2. Pour restaurer des données à partir de copies Snapshot antérieures, vous devez libérer le verrouillage de l'instantané ARP.

   > Si vous utilisez la, vous devez libérer la fonctionnalité anti-ransomware SnapLock avant de restaurer vos données à partir de copies Snapshot antérieures `volume snap restore` comme décrit ci-dessous. Si vous restaurez des données à l'aide de Flex Clone, de Single File Snap Restore ou d'autres méthodes, cela n'est pas nécessaire.

   Marquer l'attaque comme « faux positif » et « suspect clair » :
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   Utilisez l'un des paramètres suivants pour identifier les extensions :
   `[-seq-no` *`integer`*`]` Numéro de séquence du fichier dans la liste des suspects.
   `[-extension` *`text`*`, … ]` Extensions de fichier
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Heures de début et de fin pour la plage de fichiers à effacer, sous la forme "MM/JJ/AAAA HH:MM:SS".

2. Lister les copies Snapshot dans un volume :

```
volume snapshot show -vserver SVM -volume volume
```

L'exemple suivant montre les copies Snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Restaurer le contenu d'un volume à partir d'une copie Snapshot :

   ```
   volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
   ```

   L'exemple suivant restaure le contenu de `vol1`:

   ```
   cluster1::> volume snapshot restore -vserver vs0 -volume vol1
   -snapshot daily.2013-01-25_0010
   ```

Restaurez si aucune attaque système n'a été identifiée

1. Lister les copies Snapshot dans un volume :

   ```
   volume snapshot show -vserver SVM -volume volume
   ```

   L'exemple suivant montre les copies Snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                 State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurer le contenu d'un volume à partir d'une copie Snapshot :

   `volume snapshot restore -vserver SVM -volume volume -snapshot snapshot`

   L'exemple suivant restaure le contenu de `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

3. Répétez les étapes 1 et 2 pour restaurer le volume à l'aide de la copie Snapshot souhaitée.

Plus d'informations

- "Base de connaissances : prévention des ransomwares et restauration dans ONTAP"

Modifiez les options des copies Snapshot automatiques

Depuis la version ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes pour contrôler les paramètres de conservation des copies Snapshot ARP (Autonomous ransomware protection) qui sont générées automatiquement en réponse à des attaques de ransomware suspectées.

Avant de commencer

Vous pouvez uniquement modifier les options ARP snapshots sur une SVM de nœud.

Étapes

1. Pour afficher tous les paramètres de copie snapshot ARP actuels, entrez :
   `vserver options -vserver svm_name arw*`

   > Le `vserver options` commande est une commande masquée. Pour afficher la page man, entrez `man vserver options` Sur l'interface de ligne de commandes de ONTAP.

2. Pour afficher les paramètres de copie snapshot ARP actuels sélectionnés, entrez :
   `vserver options -vserver svm_name -option-name arw_setting_name`
3. Pour modifier les paramètres de copie snapshot ARP, entrez :
   `vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

   Les paramètres suivants peuvent être modifiés :

Réglage ARW	Description
arw.snap.max.count	Spécifie le nombre maximal de copies snapshot ARP pouvant exister dans un volume à tout moment. Les anciennes copies sont supprimées pour garantir que le nombre total de copies snapshot ARP se situe dans cette limite spécifiée.
arw.snap.create.interval.hours	Spécifie l'intervalle *en heures* entre les copies snapshot ARP. Une nouvelle copie Snapshot est créée lorsqu'une attaque est suspectée et que la copie créée précédemment est antérieure à l'intervalle spécifié.
arw.snap.normal.retain.interval.hours	Spécifie la durée *en heures* pendant laquelle une copie snapshot ARP est conservée. Lorsqu'une copie snapshot ARP devient cet ancien, toute autre copie Snapshot ARP créée avant la dernière copie pour atteindre cet âge est supprimée. Aucune copie snapshot ARP ne peut être antérieure à cette durée.
arw.snap.max.retain.interval.days	Spécifie la durée maximale *en jours* pendant laquelle une copie snapshot ARP peut être conservée. Toute copie snapshot ARP antérieure à cette durée sera supprimée si aucune attaque n'a été signalée sur le volume. + L'intervalle de rétention maximal pour les copies snapshot ARP est ignoré si une menace modérée est détectée. La copie snapshot ARP créée en réponse à la menace est conservée jusqu'à ce que vous ayez répondu à la menace. Le marquage d'une menace comme faux positif entraîne la suppression des copies Snapshot ARP sur le volume.
arw.snap.create.interval.hours.post.max.count	Spécifie l'intervalle *en heures* entre les copies snapshot ARP lorsque le volume contient déjà le nombre maximal de copies snapshot ARP. Lorsque le nombre maximum est atteint, une copie snapshot ARP est supprimée pour faire place à une nouvelle copie. La nouvelle vitesse de création de copie Snapshot ARP peut être réduite pour conserver l'ancienne copie à l'aide de cette option. Si le volume contient déjà un nombre maximal de copies snapshot ARP, cet intervalle spécifié dans cette option est utilisé pour la création de la copie Snapshot ARP suivante, au lieu de arw.snap.create.interval.hours.
arw.surge.snap.interval.days	Spécifie l'intervalle *en jours* entre les copies snapshot de surtension ARP. ONTAP crée une copie snapshot ARP en cas de surcharge du trafic d'E/S et lorsque la dernière copie Snapshot ARP créée est antérieure à l'intervalle spécifié. Cette option spécifie également la période de rétention *in Day* pour un instantané de surtension ARP.

Protection contre les virus

Présentation de la configuration antivirus

Vscan est une solution d'analyse antivirus développée par NetApp qui permet aux clients de protéger leurs données contre toute compromission par des virus ou d'autres codes malveillants.

Vscan effectue des analyses antivirus lorsque les clients accèdent aux fichiers via SMB. Vous pouvez configurer Vscan pour scanner à la demande ou selon une planification. Vous pouvez interagir avec Vscan en utilisant l'interface de ligne de commande (CLI) ONTAP ou les interfaces de programmation d'applications (API) ONTAP.

Informations associées

"Solutions partenaires Vscan"

À propos de la protection antivirus NetApp

À propos de l'analyse antivirus NetApp

Vscan est une solution d'analyse antivirus développée par NetApp qui permet aux clients de protéger leurs données contre toute compromission par des virus ou d'autres codes malveillants. Il associe un logiciel antivirus fourni par le partenaire aux fonctionnalités de ONTAP pour offrir aux clients la flexibilité dont ils ont besoin pour gérer l'analyse des fichiers.

Fonctionnement de l'analyse antivirus

Les systèmes de stockage délèguent des opérations d'analyse à des serveurs externes hébergeant le logiciel antivirus de fournisseurs tiers.

En fonction du mode d'analyse actif, ONTAP envoie des demandes d'analyse lorsque les clients accèdent aux fichiers via SMB (on-Access) ou accèdent à des fichiers dans des emplacements spécifiques, selon une planification ou immédiatement (on-Demand).

- Vous pouvez utiliser *On-Access scan* pour rechercher des virus lorsque les clients ouvrent, lisent, renomment ou ferment des fichiers sur SMB. Les opérations sur les fichiers sont suspendues jusqu'à ce que le serveur externe indique l'état d'analyse du fichier. Si le fichier a déjà été numérisé, ONTAP autorise l'opération de fichier. Dans le cas contraire, il demande un scan à partir du serveur.

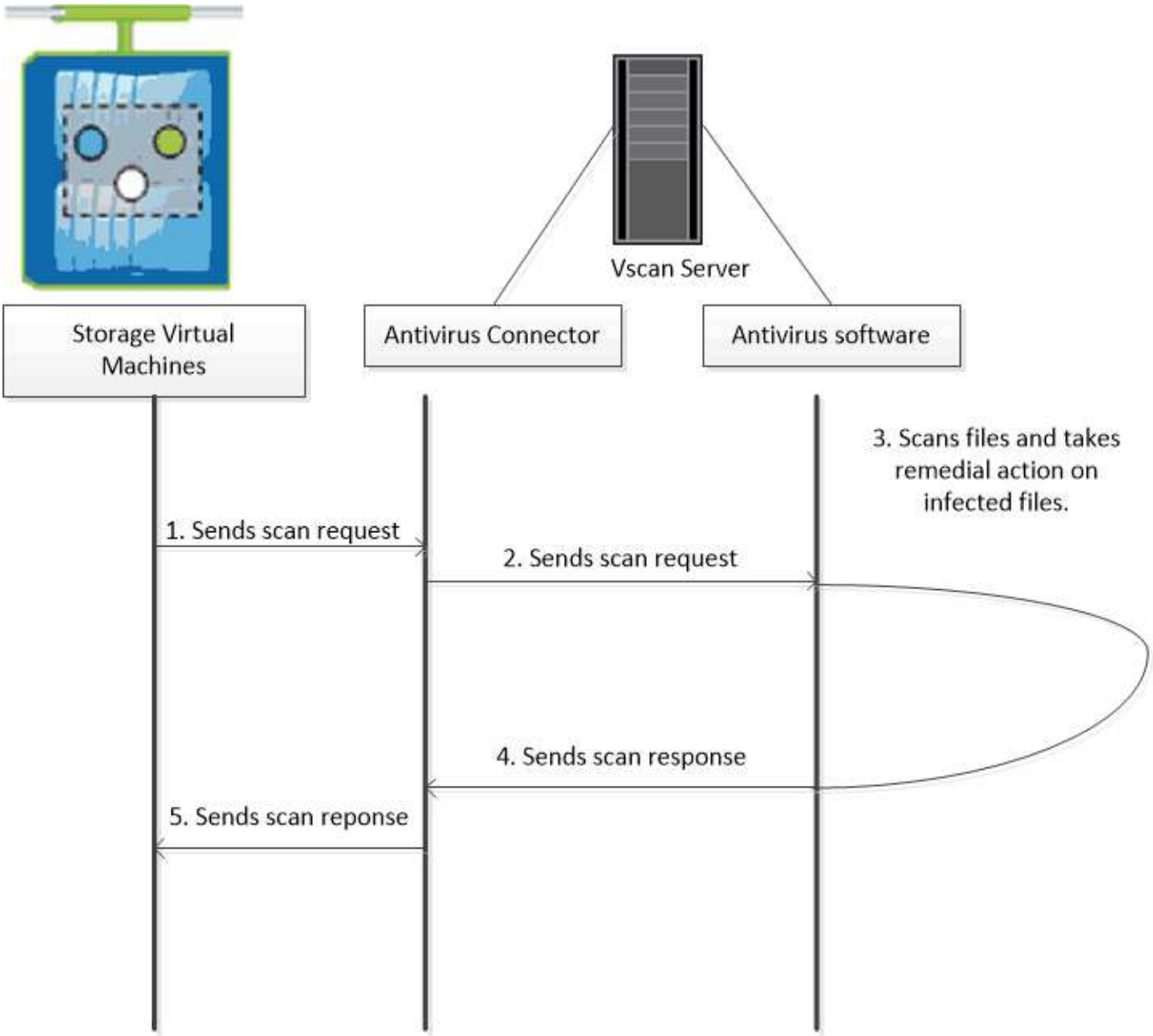
  L'analyse lors de l'accès n'est pas prise en charge par NFS.

- Vous pouvez utiliser *On-Demand scan* pour vérifier immédiatement ou selon un planning les fichiers à la recherche de virus. Nous recommandons que les analyses à la demande ne s'exécutent qu'en dehors des heures de pointe pour éviter de surcharger l'infrastructure AV existante, qui est normalement dimensionnée pour l'analyse à l'accès. Le serveur externe met à jour l'état d'analyse des fichiers vérifiés afin de réduire la latence d'accès aux fichiers par rapport à SMB. S'il y a eu des modifications de fichier ou des mises à jour de version de logiciel, il demande une nouvelle analyse de fichier à partir du serveur externe.

  Vous pouvez utiliser l'analyse à la demande pour n'importe quel chemin du namespace du SVM, même pour les volumes exportés uniquement via NFS.

Il est généralement possible d'activer les modes d'analyse à la fois on-Access et on-Demand sur une SVM. Dans les deux modes, le logiciel antivirus effectue des actions correctives sur les fichiers infectés en fonction des paramètres de votre logiciel.

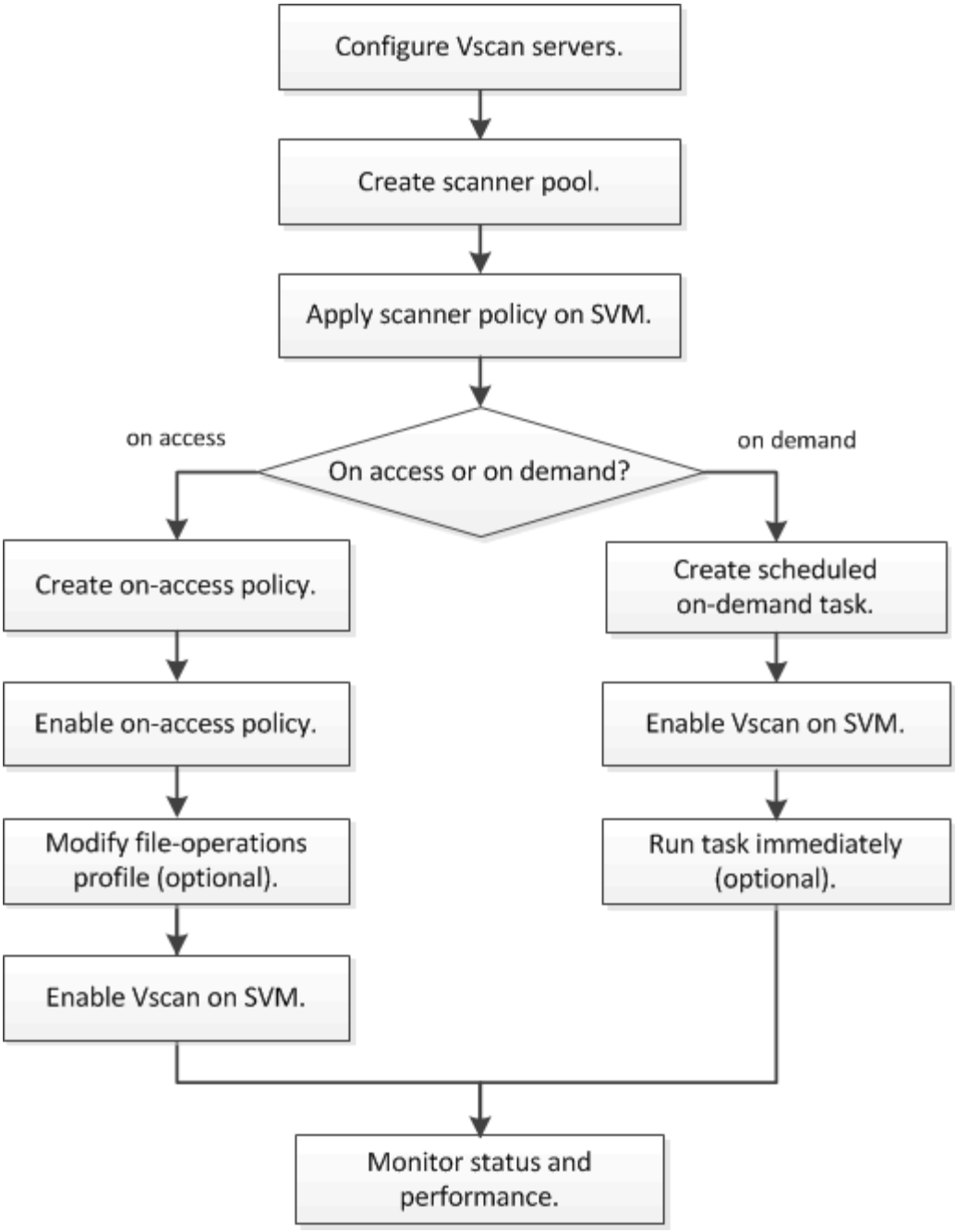
Le connecteur antivirus ONTAP, fourni par NetApp et installé sur le serveur externe, gère la communication entre le système de stockage et le logiciel antivirus.



Workflow d'analyse de virus

Vous devez créer un pool de scanner et appliquer une politique de scanner avant de pouvoir activer la numérisation. Il est généralement possible d'activer les modes d'analyse à la fois on-Access et on-Demand sur une SVM.

Vous devez avoir terminé la configuration CIFS.



Étapes suivantes

- Créer un pool de scanner sur un seul cluster
- Appliquer une politique scanner sur un seul cluster
- Création d'une règle on-Access

Architecture antivirus

L'architecture antivirus NetApp se compose du logiciel du serveur Vscan et des paramètres associés.

Logiciel du serveur Vscan

Vous devez installer ce logiciel sur le serveur Vscan.

- **ONTAP antivirus Connector**

  Il s'agit d'un logiciel fourni par NetApp qui gère les communications de demande et de réponse de scan entre les SVM et le logiciel antivirus. Il peut être exécuté sur une machine virtuelle, mais pour optimiser les performances, il convient d'utiliser une machine physique. Vous pouvez télécharger ce logiciel sur le site du support NetApp (vous devez disposer d'un identifiant).

- **Logiciel antivirus**

  Il s'agit d'un logiciel fourni par un partenaire qui analyse les fichiers à la recherche de virus ou d'autres codes malveillants. Lors de la configuration du logiciel, vous spécifiez les actions correctives à effectuer sur les fichiers infectés.

Paramètres du logiciel Vscan

Vous devez configurer ces paramètres logiciels sur le serveur Vscan.

- **Scanner pool**

  Ce paramètre définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. Il définit également une période de temporisation de la demande de scan, après laquelle la requête de scan est envoyée à un autre serveur Vscan si un serveur est disponible.

  > Vous devez définir la période de temporisation dans le logiciel antivirus sur le serveur Vscan à cinq secondes de moins que le délai d'expiration de la demande de scan-pool. Cela permet d'éviter les situations dans lesquelles l'accès aux fichiers est retardé ou refusé car le délai d'expiration du logiciel est supérieur au délai d'expiration de la demande d'analyse.

- **Utilisateur privilégié**

  Ce paramétrage est un compte utilisateur de domaine qu'un serveur Vscan utilise pour se connecter à la SVM. Le compte doit figurer dans la liste des utilisateurs privilégiés du scanner pool.

- **Politique du scanner**

  Ce paramètre détermine si un scanner pool est actif. Les règles de scanner sont définies par le système ; vous ne pouvez donc pas créer de règles de scanner personnalisées. Seules les trois règles suivantes sont disponibles :

  - `Primary` indique que le pool de scanner est actif.
  - `Secondary` Précise que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
  - `Idle` indique que le pool de scanner est inactif.

- **Politique sur accès**

  Ce paramètre définit la portée d'une analyse à l'accès. Vous pouvez spécifier la taille maximale du fichier à numériser, les extensions de fichier et les chemins à inclure dans la numérisation, ainsi que les extensions de fichier et les chemins à exclure de la numérisation.

  Par défaut, seuls les volumes en lecture-écriture sont analysés. Vous pouvez spécifier des filtres qui permettent la numérisation de volumes en lecture seule ou qui limitent la numérisation aux fichiers ouverts avec l'accès d'exécution :

- `scan-ro-volume` permet d'analyser les volumes en lecture seule.
- `scan-execute-access` limite la numérisation aux fichiers ouverts avec l'accès d'exécution.

> « Exécuter l'accès » est différent de « Exécuter l'autorisation ». Un client donné aura « accès à l'exécution » sur un fichier exécutable uniquement si le fichier a été ouvert avec « intention d'exécution ».

Vous pouvez définir le `scan-mandatory` Option désactivée pour spécifier que l'accès aux fichiers est autorisé lorsqu'aucun serveur Vscan n'est disponible pour l'analyse antivirus. En mode On-Access, vous pouvez choisir parmi les deux options mutuellement exclusives suivantes :

- Obligatoire : avec cette option, Vscan tente de livrer la demande de scan au serveur jusqu'à expiration du délai. Si la demande d'analyse n'est pas acceptée par le serveur, la demande d'accès client est refusée.
- Non obligatoire : avec cette option, Vscan permet toujours l'accès client, qu'un serveur Vscan soit disponible ou non pour l'analyse antivirus.

- **Tâche à la demande**

  Ce paramètre définit l'étendue d'une acquisition à la demande. Vous pouvez spécifier la taille maximale du fichier à numériser, les extensions de fichier et les chemins à inclure dans la numérisation, ainsi que les extensions de fichier et les chemins à exclure de la numérisation. Les fichiers des sous-répertoires sont analysés par défaut.

  Vous utilisez une planification cron pour spécifier quand la tâche s'exécute. Vous pouvez utiliser le `vserver vscan on-demand-task run` commande permettant d'exécuter la tâche immédiatement.

- **Profil d'opérations fichier Vscan (analyse sur accès uniquement)**

  Le `vscan-fileop-profile` paramètre pour le `vserver cifs share create` Définit les opérations de fichier SMB qui déclenchent l'analyse antivirus. Par défaut, le paramètre est défini sur `standard`, Qui est la meilleure pratique de NetApp. Vous pouvez ajuster ce paramètre si nécessaire lors de la création ou de la modification d'un partage SMB :

  - `no-scan` spécifie que les analyses antivirus ne sont jamais déclenchées pour le partage.
  - `standard` indique que les analyses antivirus sont déclenchées par les opérations ouvrir, fermer et renommer.
  - `strict` spécifie que les analyses antivirus sont déclenchées par les opérations d'ouverture, de lecture, de fermeture et de renommage.

    Le `strict` le profil offre une sécurité améliorée dans les situations où plusieurs clients accèdent simultanément à un fichier. Si un client ferme un fichier après avoir écrit un virus, et que le même fichier reste ouvert sur un deuxième client, `strict` assure qu'une opération de lecture sur le second client déclenche une analyse avant la fermeture du fichier.

    Veillez à restreindre le `strict` le profil des partages contenant des fichiers que vous prévoyez sera accessible simultanément. Étant donné que ce profil génère davantage de demandes d'analyse, il peut avoir un impact sur les performances.

  - `writes-only` spécifie que les analyses de virus ne sont déclenchées que lorsque les fichiers modifiés sont fermés.

Depuis `writes-only` génère moins de demandes d'analyse, ce qui améliore généralement les performances.

Si vous utilisez ce profil, le scanner doit être configuré pour supprimer ou mettre en quarantaine les fichiers infectés irréparables, afin qu'ils ne soient pas accessibles. Si, par exemple, un client ferme un fichier après l'écriture d'un virus, et que le fichier n'est pas réparé, supprimé ou mis en quarantaine, tout client qui accède au fichier `without` écrire à elle sera infecté.

> Si une application client effectue une opération de renommage, le fichier est fermé avec le nouveau nom et n'est pas analysé. Si de telles opérations posent un problème de sécurité dans votre environnement, vous devez utiliser le `standard` ou `strict` profil.

Solutions partenaires Vscan

NetApp collabore avec Trellix, Symantec, Trend micro et Sentinel One afin de proposer des solutions anti-malware et anti-virus de pointe basées sur la technologie ONTAP Vscan. Ces solutions vous aident à rechercher des programmes malveillants dans les fichiers et à corriger les fichiers affectés.

Comme le montre le tableau ci-dessous, les informations d'interopérabilité pour Trellix, Symantec et Trend micro sont conservées dans la matrice d'interopérabilité NetApp. Les détails sur l'interopérabilité de Trellix et Symantec sont également disponibles sur les sites Web des partenaires. Les informations d'interopérabilité pour Sentinel One et les autres nouveaux partenaires seront conservées par le partenaire sur son site Web.

En tant que partenaire	Documentation de la solution	Détails sur l'interopérabilité
Trellix (anciennement McAfee)	"Documentation produit Trellix"	• "Matrice d'interopérabilité NetApp" • "Plates-formes prises en charge pour la protection du stockage Endpoint Security (trellix.com)"
Symantec	"Symantec protection Engine 9.0.0"	• "Matrice d'interopérabilité NetApp" • "Matrice de prise en charge des périphériques partenaires certifiés avec Symantec protection Engine (SPE) pour le stockage en réseau (NAS) 9.x.x." • "Matrice de prise en charge des périphériques partenaires certifiés avec Symantec protection Engine (SPE) pour le stockage en réseau (NAS) 8.x (broadcom.com)"

En tant que partenaire	Documentation de la solution	Détails sur l'interopérabilité
Trend micro	"Guide de démarrage de Trend micro ServerProtect for Storage 6.0"	"Matrice d'interopérabilité NetApp"
Sentinel One	• "Sécurité des données du cloud de singularité de SentinelOne" • "Assistance SentinelOne" Ce lien requiert une connexion utilisateur. Vous pouvez demander l'accès à Sentinel One.	Instinct profond

Installation et configuration du serveur Vscan

Installation et configuration du serveur Vscan

Configurez un ou plusieurs serveurs Vscan pour vous assurer que les fichiers de votre système sont analysés pour détecter d'éventuels virus. Suivez les instructions fournies par votre fournisseur pour installer et configurer le logiciel antivirus sur le serveur.

Suivez les instructions du fichier README fourni par NetApp pour installer et configurer ONTAP antivirus Connector. Vous pouvez également suivre les instructions du "Installez la page ONTAP antivirus Connector".

> Pour les configurations de reprise après incident et MetroCluster, vous devez installer et configurer des serveurs Vscan distincts pour les clusters ONTAP principal/local et secondaire/partenaire.

Configuration logicielle requise pour l'antivirus

- Pour plus d'informations sur la configuration requise pour le logiciel antivirus, reportez-vous à la documentation du fournisseur.
- Pour plus d'informations sur les fournisseurs, les logiciels et les versions pris en charge par Vscan, voir le "Solutions partenaires Vscan" page.

Conditions requises pour ONTAP antivirus Connector

- Vous pouvez télécharger ONTAP antivirus Connector à partir de la page **Téléchargement de logiciels** du site de support NetApp. "Téléchargements NetApp : logiciels"
- Pour plus d'informations sur les versions de Windows prises en charge par le connecteur antivirus ONTAP et les conditions d'interopérabilité, voir "Solutions partenaires Vscan".

> Vous pouvez installer différentes versions de serveurs Windows pour différents serveurs Vscan dans un cluster.

- .NET 3.0 ou version ultérieure doit être installé sur le serveur Windows.
- SMB 2.0 doit être activé sur le serveur Windows.

Installez ONTAP antivirus Connector

Installer le ONTAP antivirus Connector sur le serveur Vscan pour permettre la communication entre le système exécutant ONTAP et le serveur Vscan. Une fois ONTAP antivirus Connector installé, le logiciel antivirus peut communiquer avec un ou plusieurs SVM.

Description de la tâche

- Voir la "Solutions partenaires Vscan" Page pour plus d'informations sur les protocoles pris en charge, les versions de logiciels des fournisseurs antivirus, les versions de ONTAP, les conditions d'interopérabilité et les serveurs Windows.
- .NET 4.5.1 ou version ultérieure doit être installé.
- ONTAP antivirus Connector peut s'exécuter sur une machine virtuelle. Toutefois, pour de meilleures performances, NetApp recommande l'utilisation d'une machine virtuelle dédiée à l'analyse antivirus.
- SMB 2.0 doit être activé sur le serveur Windows sur lequel vous installez et exécutez ONTAP antivirus Connector.

Avant de commencer

- Téléchargez le fichier d'installation de ONTAP antivirus Connector à partir du site de support et enregistrez-le dans un répertoire de votre disque dur.
- Vérifiez que vous répondez aux exigences requises pour installer ONTAP antivirus Connector.
- Vérifiez que vous disposez des privilèges d'administrateur pour installer l'antivirus Connector.

Étapes

1. Démarrez l'assistant d'installation de l'antivirus Connector en exécutant le fichier d'installation approprié.
2. Sélectionnez *Suivant*. La boîte de dialogue dossier de destination s'ouvre.
3. Sélectionnez *Next* pour installer l'antivirus Connector dans le dossier qui est répertorié ou sélectionnez *change* pour l'installer dans un autre dossier.
4. La boîte de dialogue informations d'identification du service Windows du connecteur AV ONTAP s'ouvre.
5. Entrez vos informations d'identification de service Windows ou sélectionnez **Ajouter** pour sélectionner un utilisateur. Pour un système ONTAP, cet utilisateur doit être un utilisateur de domaine valide et doit exister dans la configuration scanner pool de la SVM.
6. Sélectionnez **Suivant**. La boîte de dialogue prêt à installer le programme s'ouvre.
7. Sélectionnez **installer** pour commencer l'installation ou sélectionnez **Précédent** si vous souhaitez modifier les paramètres.
   Une boîte de dialogue d'état s'ouvre et indique la progression de l'installation, suivie de la boîte de dialogue Assistant InstallShield terminé.
8. Cochez la case configurer les LIFs ONTAP si vous souhaitez poursuivre la configuration des LIFs de données ou de gestion ONTAP.
   Vous devez configurer au moins une LIF de données ou de gestion ONTAP avant d'utiliser ce serveur Vscan.
9. Cochez la case Afficher le journal **Windows installer** si vous souhaitez afficher les journaux d'installation.
10. Sélectionnez **Terminer** pour terminer l'installation et fermer l'assistant InstallShield.
    L'icône **Configure ONTAP LIFs** est enregistrée sur le bureau pour configurer les LIFs ONTAP.
11. Ajouter un SVM au antivirus Connector.
    Vous pouvez ajouter un SVM à l'antivirus Connector en ajoutant une LIF de gestion ONTAP, interrogée sur

la liste des LIFs de données, ou en configurant directement la LIF de données.
Si la LIF de gestion ONTAP est configurée, vous devez également fournir les informations d'interrogation et les informations d'identification du compte admin ONTAP.

- Vérifier que la LIF de management ou l'adresse IP du SVM est Enabled for `management-https`. Cela n'est pas nécessaire lorsque vous configurez uniquement les LIFs de données.
- Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système `/api/network/ip/interfaces` API REST.
  Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "création d'un rôle de connexion de sécurité" et "création d'une connexion de sécurité" Pages de manuel ONTAP.

> Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration. Pour plus d'informations, reportez-vous à la section "connexion de sécurité domaine-tunnel créer" ONTAP ou utilisez `/api/security/acccounts` et `/api/security/roles` API REST pour configurer le compte et le rôle admin

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**.
2. Dans la boîte de dialogue Configure ONTAP LIFs, sélectionnez le type de configuration préféré, puis effectuez les actions suivantes :

Pour créer ce type de LIF…	Procédez comme suit…
LIF de données	a. Définissez « rôle » sur « données ». b. Définissez « protocole de données » sur « cifs ». c. Définissez la « politique de pare-feu » sur « données ». d. Définissez « stratégie de service » sur « fichiers-données-par-défaut ».
LIF de management	a. Définir « rôle* sur « données » b. Définissez « protocole de données » sur « aucun ». c. Définissez la « politique de pare-feu » sur « gestion ». d. Définissez « stratégie de service » sur « gestion par défaut ».

En savoir plus sur "Création d'une LIF".

Après avoir créé une LIF, entrer la LIF de données ou de gestion ou l'adresse IP du SVM que vous souhaitez ajouter. Vous pouvez également entrer dans la LIF de cluster management. Si vous spécifiez la LIF de cluster management, tous les SVM au sein de ce cluster qui servent SMB peuvent utiliser le serveur Vscan.

> Lorsque l'authentification Kerberos est requise pour les serveurs Vscan, chaque LIF de données du SVM doit avoir un nom DNS unique, et vous devez enregistrer ce nom en tant que nom principal du serveur (SPN) avec Windows Active Directory. Lorsqu'un nom DNS unique n'est pas disponible pour chaque LIF de données ou enregistré en tant que SPN, le serveur Vscan utilise le mécanisme NT LAN Manager pour l'authentification. Si vous ajoutez ou modifiez les noms DNS et les SPN après la connexion du serveur Vscan, vous devez redémarrer le service antivirus Connector sur le serveur Vscan pour appliquer les modifications.

3. Pour configurer une LIF de gestion, entrez la durée d'interrogation en secondes. La durée de l'interrogation est la fréquence à laquelle l'antivirus Connector recherche des modifications des SVM ou de la configuration LIF du cluster. L'intervalle d'interrogation par défaut est de 60 secondes.
4. Entrez le nom et le mot de passe du compte admin ONTAP pour configurer une LIF de gestion.
5. Cliquez sur **Test** pour vérifier la connectivité et l'authentification. L'authentification est uniquement vérifiée pour une configuration LIF de management.
6. Cliquez sur **mettre à jour** pour ajouter la LIF à la liste des LIFs à interroger ou à se connecter.
7. Cliquez sur **Enregistrer** pour enregistrer la connexion au registre.
8. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre. Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Voir la "Configurez la page ONTAP antivirus Connector" pour les options de configuration.

Configurer ONTAP antivirus Connector

Configurer ONTAP antivirus Connector pour spécifier un ou plusieurs SVM (Storage Virtual machines) auxquels vous souhaitez vous connecter en entrant dans la LIF de gestion ONTAP, en interrotant qu'information et les informations d'identification du compte d'administrateur ONTAP, ou simplement dans la LIF de données. Vous pouvez également modifier les détails d'une connexion SVM ou supprimer une connexion SVM. Par défaut, ONTAP antivirus Connector utilise les API REST pour récupérer la liste des LIFs de données si le LIF de management ONTAP est configuré.

Modifier le détail d'une connexion SVM

Vous pouvez mettre à jour les détails d'une connexion SVM (Storage Virtual machine), qui a été ajoutée à l'antivirus Connector, en modifiant la LIF de gestion ONTAP et les informations d'interrogation. Une fois ajoutées, les LIF de données ne peuvent pas être mises à jour. Pour mettre à jour les LIF de données, vous devez d'abord les supprimer, puis les ajouter de nouveau avec la nouvelle LIF ou adresse IP.

Avant de commencer

Vérifiez que vous avez créé un compte d'utilisateur pour l'application HTTP et que vous avez attribué un rôle ayant (au moins en lecture seule) accès au système `/api/network/ip/interfaces` API REST.
Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la section "création d'un rôle de connexion de sécurité" et le "création d'une connexion de sécurité" commandes.
Vous pouvez également utiliser l'utilisateur du domaine en tant que compte en ajoutant un SVM de tunnel d'authentification pour une SVM d'administration.
Pour plus d'informations, reportez-vous à la section "connexion de sécurité domaine-tunnel créer" Page de manuel ONTAP.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner l'adresse IP du SVM, puis cliquer sur **Update**.
3. Mettez à jour les informations, si nécessaire.
4. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
5. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers une importation de registre ou un fichier d'exportation de registre.
   Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Retirer une connexion SVM du connecteur antivirus

Si vous n'avez plus besoin d'une connexion SVM, vous pouvez la supprimer.

Étapes

1. Cliquez avec le bouton droit de la souris sur l'icône **configurer ONTAP LIFs**, qui a été enregistrée sur votre bureau lorsque vous avez terminé l'installation du connecteur antivirus, puis sélectionnez **Exécuter en tant qu'administrateur**. La boîte de dialogue Configure ONTAP LIFs s'ouvre.
2. Sélectionner une ou plusieurs adresses IP de SVM, puis cliquer sur **Supprimer**.
3. Cliquez sur **Enregistrer** pour mettre à jour les détails de la connexion dans le registre.
4. Cliquez sur **Exporter** si vous souhaitez exporter la liste des connexions vers un fichier d'importation de registre ou d'exportation de registre.
   Ceci est utile si plusieurs serveurs Vscan utilisent le même ensemble de LIFs de gestion ou de données.

Résoudre les problèmes

Avant de commencer

Lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet droit.

Vous pouvez activer ou désactiver les journaux antivirus Connector à des fins de diagnostic. Par défaut, ces journaux sont désactivés. Pour améliorer les performances, vous devez conserver les journaux du connecteur antivirus désactivés et les activer uniquement pour les événements critiques.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector :
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Créez des valeurs de registre en fournissant le type, le nom et les valeurs indiqués dans le tableau suivant :

Type	Nom	Valeurs
Chaîne	Chemin de traçabilité	c:\avshim.log

   Cette valeur de registre peut être n'importe quel autre chemin valide.

4. Créez une autre valeur de registre en fournissant le type, le nom, les valeurs et les informations de journalisation indiquées dans le tableau suivant :

Type	Nom	Journalisation critique	Journalisation intermédiaire	Journalisation détaillée
DWORD	TRACELEVEL	1	2 ou 3	4

   Cela active les journaux antivirus Connector qui sont enregistrés à la valeur de chemin fournie dans TracePath à l'étape 3.

5. Désactivez les journaux du connecteur antivirus en supprimant les valeurs de registre que vous avez créées aux étapes 3 et 4.
6. Créez une autre valeur de registre de type "MULTI_SZ" avec le nom "LogRotation" (sans guillemets). Dans « LogRotation »,
   Indiquez « logFileSize:1 » comme entrée pour la taille de rotation (où 1 représente 1 Mo) et dans la ligne suivante, indiquez « logFileCount:5 » comme
   entrée pour la limite de rotation (5 est la limite).

   > Ces valeurs sont facultatives. Si elles ne sont pas fournies, les valeurs par défaut des fichiers 20 Mo et 10 sont utilisées respectivement pour la taille de rotation et la limite de rotation. Les valeurs entières fournies ne fournissent pas de valeurs décimales ou de fraction. Si vous indiquez des valeurs supérieures aux valeurs par défaut, les valeurs par défaut sont utilisées à la place.

7. Pour désactiver la rotation du journal configurée par l'utilisateur, supprimez les valeurs de registre que vous avez créées à l'étape 6.

Bannière personnalisable

Une bannière personnalisée vous permet de placer une déclaration juridiquement contraignante et une clause de non-responsabilité d'accès au système dans la fenêtre *Configure ONTAP LIF API*.

Étape

1. Modifiez la bannière par défaut en mettant à jour le contenu de l' `banner.txt` dans le répertoire d'installation, puis en enregistrant les modifications.
   Vous devez rouvrir la fenêtre configurer l'API LIF ONTAP pour voir les modifications reflétées dans la bannière.

Activer le mode Eo (Extended Ordinance)

Vous pouvez activer et désactiver le mode Extended Ordinance (EO) pour un fonctionnement sécurisé.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, localisez la sous-clé suivante pour ONTAP antivirus Connector :
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Dans le volet de droite, créez une nouvelle valeur de registre de type "DWORD" avec le nom "EO_mode" (sans guillemets) et la valeur "1" (sans guillemets) pour activer le mode EO ou la valeur "0" (sans

guillemets) pour désactiver le mode EO.

> Par défaut, si l' `EO_Mode` L'entrée de registre est absente, le mode EO est désactivé. Lorsque vous activez le mode EO, vous devez configurer à la fois le serveur syslog externe et l'authentification mutuelle des certificats.

Configurez le serveur syslog externe

Avant de commencer

Notez que lorsque vous créez des valeurs de registre dans cette procédure, utilisez le volet de droite.

Étapes

1. Sélectionnez **Démarrer**, tapez "regedit" dans la zone de recherche, puis sélectionnez `regedit.exe` Dans la liste programmes.
2. Dans **Éditeur du Registre**, créez la sous-clé suivante pour ONTAP antivirus Connector pour la configuration syslog :
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Créez une valeur de registre en fournissant le type, le nom et la valeur, comme indiqué dans le tableau suivant :

Type	Nom	Valeur
DWORD	syslog_enabled	1 ou 0

   Veuillez noter qu'une valeur « 1 » active le syslog et qu'une valeur « 0 » le désactive.

4. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Hôte_syslog

   Indiquez l'adresse IP ou le nom de domaine de l'hôte syslog pour le champ valeur.

5. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Syslog_port

   Indiquez le numéro de port sur lequel le serveur syslog s'exécute dans le champ valeur.

6. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom
REG_SZ	Protocole_syslog

Saisissez le protocole utilisé sur le serveur syslog, soit « tcp », soit « udp », dans le champ valeur.

7. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	JOURNAL_CRIT	LOG_NOTICE	INFO_JOURNAL	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Créez une autre valeur de registre en fournissant les informations comme indiqué dans le tableau suivant :

Type	Nom	Valeur
DWORD	syslog_tls	1 ou 0

Notez qu'une valeur « 1 » active syslog avec TLS (transport Layer Security) et une valeur « 0 » désactive syslog avec TLS.

Assurez-vous qu'un serveur syslog externe configuré fonctionne correctement

- Si la clé est absente ou a une valeur nulle :
  - Le protocole par défaut est « tcp ».
  - Le port par défaut est "514" pour "tcp/udp" et par défaut "6514" pour TLS.
  - Par défaut, le niveau syslog est 5 (LOG_NOTICE).
- Vous pouvez confirmer que syslog est activé en vérifiant que le système `syslog_enabled` la valeur est « 1 ». Lorsque le `syslog_enabled` La valeur est "1", vous devriez pouvoir vous connecter au serveur distant configuré, que le mode EO soit activé ou non.
- Si le mode EO est réglé sur « 1 » et que vous modifiez le `syslog_enabled` valeur comprise entre « 1 » et « 0 », ce qui suit s'applique :
  - Vous ne pouvez pas démarrer le service si syslog n'est pas activé en mode EO.
  - Si le système fonctionne dans un état stable, un avertissement s'affiche indiquant que syslog ne peut pas être désactivé en mode EO et que syslog est fermement défini sur « 1 », que vous pouvez voir dans le registre. Si cela se produit, vous devez d'abord désactiver le mode EO, puis désactiver syslog.
- Si le serveur syslog ne peut pas fonctionner correctement lorsque le mode EO et syslog sont activés, le service s'arrête. Ceci peut se produire pour l'une des raisons suivantes :
  - Un hôte syslog_non valide ou non configuré.
  - Un protocole non valide, hormis UDP ou TCP, est configuré.
  - Un numéro de port n'est pas valide.
- Dans le cas d'une configuration TCP ou TLS sur TCP, si le serveur n'écoute pas le port IP, la connexion échoue et le service s'arrête.

Configurer l'authentification de certificat mutuel X.509

L'authentification mutuelle basée sur certificat X.509 est possible pour la communication SSL (Secure Sockets Layer) entre l'antivirus Connector et ONTAP dans le chemin de gestion. Si le mode EO est activé et que le certificat n'est pas trouvé, le connecteur AV se termine. Effectuez la procédure suivante sur l'antivirus Connector :

Étapes

1. Le connecteur antivirus recherche le certificat client du connecteur antivirus et le certificat de l'autorité de certification du serveur NetApp dans le chemin d'accès au répertoire à partir duquel le connecteur antivirus exécute le répertoire d'installation. Copiez les certificats dans ce chemin de répertoire fixe.
2. Intégrez le certificat client et sa clé privée au format PKCS12 et nommez-le « AV_client.P12 ».
3. Assurez-vous que le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat du serveur NetApp est au format PEM (Privacy Enhanced Mail) et nommé ONTAP_CA.pem. Placez-le dans le répertoire d'installation de l'antivirus Connector. Sur le système NetApp ONTAP, installez le certificat de l'autorité de certification (ainsi que toute autorité de signature intermédiaire jusqu'à l'autorité de certification racine) utilisé pour signer le certificat client pour le connecteur antivirus à « ONTAP » en tant que certificat de type « client-ca ».

Configurer les scanner pool

Présentation de la configuration des scanner pool

Un scanner pool définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. Une politique scanner détermine si un pool de scanner est actif.

> Si vous utilisez une export policy sur un serveur SMB, vous devez ajouter chaque serveur Vscan à la export policy.

Créer un pool de scanner sur un seul cluster

Un scanner pool définit les serveurs Vscan et les utilisateurs privilégiés qui peuvent se connecter aux SVM. On peut créer un pool de scanner pour un SVM individuel ou pour tous les SVM d'un cluster.

Ce dont vous avez besoin

- Les SVM et les serveurs Vscan doivent se trouver dans le même domaine ou dans des domaines de confiance.
- Pour les scanner-pool définis pour un SVM individuel, vous devez avoir configuré ONTAP antivirus Connector avec la LIF de management du SVM ou la LIF de donnée du SVM.
- Pour les scanner-pool définis pour tous les SVM d'un cluster, vous devez avoir configuré ONTAP antivirus Connector avec la LIF cluster management.
- La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan utilise pour se connecter à la SVM.
- Une fois le scanner pool configuré, vérifiez l'état de la connexion aux serveurs.

Étapes

1. Créer un pool de scanner :

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Spécifier un SVM de données pour un pool défini pour un SVM individuel et spécifier un SVM d'administration du cluster pour un pool défini pour tous les SVM d'un cluster.

- Spécifiez une adresse IP ou un FQDN pour chaque nom d'hôte de serveur Vscan.
- Spécifiez le domaine et le nom d'utilisateur pour chaque utilisateur privilégié.
  Pour obtenir la liste complète des options, consultez la page man de la commande.

  La commande suivante crée un pool de scanner nommé `SP` sur le `vs1` SVM :

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Vérifiez que le scanner pool a été créé :

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails de `SP` scanner pool :

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                   Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

   Vous pouvez également utiliser le `vserver vscan scanner-pool show` Commande pour afficher tous les scanner pool d'un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Créer des pools de scanner dans les configurations MetroCluster

Il faut créer des pools de scanner primaires et secondaires sur chaque cluster dans une configuration MetroCluster, ce qui correspond aux SVM principal et secondaire sur le cluster.

Ce dont vous avez besoin

- Les SVM et les serveurs Vscan doivent se trouver dans le même domaine ou dans des domaines de confiance.

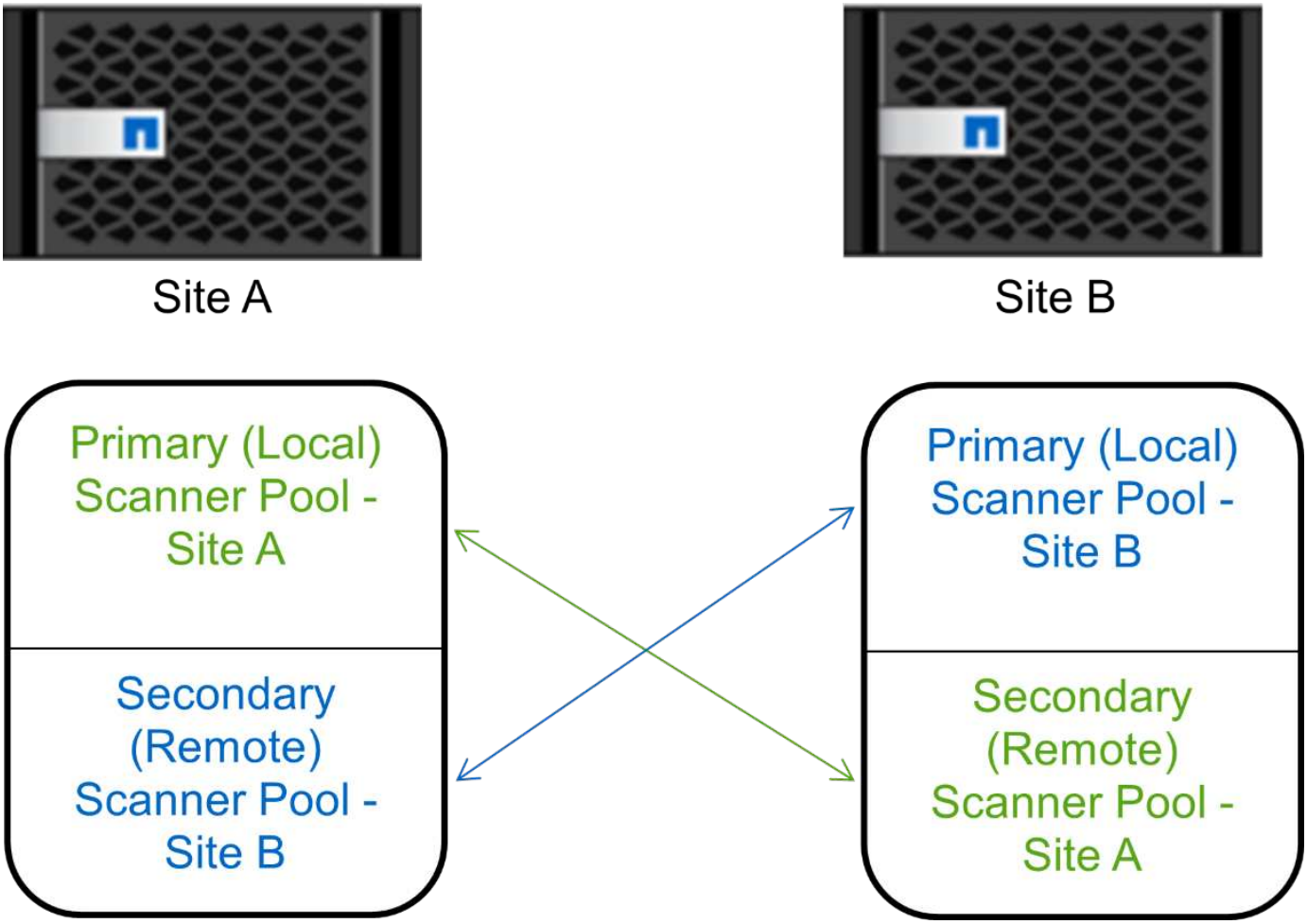
- Pour les scanner-pool définis pour un SVM individuel, vous devez avoir configuré ONTAP antivirus Connector avec la LIF de management du SVM ou la LIF de donnée du SVM.
- Pour les scanner-pool définis pour tous les SVM d'un cluster, vous devez avoir configuré ONTAP antivirus Connector avec la LIF cluster management.
- La liste des utilisateurs privilégiés doit inclure le compte d'utilisateur de domaine que le serveur Vscan utilise pour se connecter à la SVM.
- Une fois le scanner pool configuré, vérifiez l'état de la connexion aux serveurs.

Description de la tâche

Les configurations MetroCluster protègent les données grâce à la mise en œuvre de deux clusters en miroir séparés physiquement. Chaque cluster réplique de manière synchrone les données et la configuration SVM de l'autre. Un SVM principal sur le cluster local diffuse des données lorsque le cluster est en ligne. Un SVM secondaire situé sur le cluster local transmet des données lorsque le cluster distant est hors ligne.

Cela signifie que vous devez créer des scanner pools principal et secondaire sur chaque cluster d'une configuration MetroCluster. Le pool secondaire devient actif lorsque le cluster commence à transmettre des données depuis le SVM secondaire. Pour la reprise sur incident, la configuration est similaire à celle de MetroCluster.

Cette figure présente une configuration MetroCluster/DR classique.



Étapes

1. Créer un pool de scanner :

`vserver vscan scanner-pool create -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`* `-hostnames` *`Vscan_server_hostnames`* `-privileged-users` *`privileged_users`*

- Spécifier un SVM de données pour un pool défini pour un SVM individuel et spécifier un SVM d'administration du cluster pour un pool défini pour tous les SVM d'un cluster.
- Spécifiez une adresse IP ou un FQDN pour chaque nom d'hôte de serveur Vscan.
- Spécifiez le domaine et le nom d'utilisateur pour chaque utilisateur privilégié.

  On doit créer tous les scanner pool depuis le cluster contenant le SVM principal.

  Pour obtenir la liste complète des options, consultez la page man de la commande.

  Les commandes suivantes créent des scanner pool principal et secondaire sur chaque cluster en configuration MetroCluster :

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Vérifiez que les scanner pool ont été créés :

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails du scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                   Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

Vous pouvez également utiliser le `vserver vscan scanner-pool show` Commande pour afficher tous les scanner pool d'un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Appliquer une politique scanner sur un seul cluster

Une politique scanner détermine si un pool de scanner est actif. On doit activer un scanner pool avant que les serveurs Vscan qu'il définit puissent se connecter à une SVM.

Description de la tâche

- Vous ne pouvez appliquer qu'une seule politique scanner à un pool de scanner.
- Si vous avez créé un pool de scanner pour tous les SVM d'un cluster, vous devez appliquer une scanner policy sur chaque SVM individuellement.

Étapes

1. Appliquer une politique scanner :

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Une politique scanner peut avoir l'une des valeurs suivantes :

   - `Primary` indique que le pool de scanner est actif.
   - `Secondary` Spécifie que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
   - `Idle` indique que le pool de scanner est inactif.

   L'exemple suivant montre que le pool de scanner est nommé `SP` sur le `vs1` Le SVM est actif :

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. Vérifiez que le pool de scanner est actif :

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails de `SP` scanner pool :

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                   Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

   Vous pouvez utiliser le `vserver vscan scanner-pool show-active` Commande pour afficher les scanner pool actifs sur un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man de la commande.

Appliquez les politiques de scanner dans les configurations MetroCluster

Une politique scanner détermine si un pool de scanner est actif. Vous devez appliquer une scanner policy aux scanner pool principal et secondaire sur chaque cluster dans une configuration MetroCluster.

Description de la tâche

- Vous ne pouvez appliquer qu'une seule politique scanner à un pool de scanner.
- Si vous avez créé un pool de scanner pour tous les SVM d'un cluster, vous devez appliquer une scanner policy sur chaque SVM individuellement.
- Pour les configurations MetroCluster et de reprise après incident, vous devez appliquer une stratégie scanner à chaque pool de scanner du cluster local et distant.
- Dans la règle que vous créez pour le cluster local, vous devez spécifier le cluster local dans le `cluster` paramètre. Dans la stratégie que vous créez pour le cluster distant, vous devez spécifier le cluster distant dans `cluster` paramètre. Le cluster distant peut alors prendre le contrôle des opérations d'analyse antivirus en cas d'incident.

Étapes

1. Appliquer une politique scanner :

`vserver vscan scanner-pool apply-policy -vserver` *`data_SVM`* `-scanner-pool` *`scanner_pool`* `-scanner-policy primary|secondary|idle -cluster` *`cluster_to_apply_policy_on`*

Une politique scanner peut avoir l'une des valeurs suivantes :

- `Primary` indique que le pool de scanner est actif.
- `Secondary` Spécifie que le pool de scanner est actif uniquement si aucun des serveurs Vscan du pool de scanner principal n'est connecté.
- `Idle` indique que le pool de scanner est inactif.

> Vous devez appliquer toutes les scanner policy à partir du cluster qui contient la SVM principale.

Les commandes suivantes appliquent des scanner policy aux scanner pool principal et secondaire sur chaque cluster de la configuration MetroCluster :

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Vérifiez que le pool de scanner est actif :

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails du scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

Vous pouvez utiliser le `vserver vscan scanner-pool show-active` Commande pour afficher les scanner pool actifs sur un SVM. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Commandes pour la gestion des scanner pool

Vous pouvez modifier et supprimer des pools de scanner et gérer des utilisateurs privilégiés et des serveurs Vscan pour un pool de scanner. Vous pouvez également afficher des informations récapitulatives sur le pool de scanner.

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Modifier un pool de scanner	`vserver vscan scanner-pool modify`
Supprimer un pool de scanner	`vserver vscan scanner-pool delete`
Ajouter des utilisateurs privilégiés à un pool de scanner	`vserver vscan scanner-pool privileged-users add`
Supprimer des utilisateurs privilégiés d'un pool de scanner	`vserver vscan scanner-pool privileged-users remove`
Ajout de serveurs Vscan à un pool de scanner	`vserver vscan scanner-pool servers add`
Supprimer les serveurs Vscan d'un pool de scanner	`vserver vscan scanner-pool servers remove`
Afficher le résumé et les détails d'un pool de scanner	`vserver vscan scanner-pool show`
Afficher les utilisateurs privilégiés d'un pool de scanner	`vserver vscan scanner-pool privileged-users show`

Afficher les serveurs Vscan pour tous les pools de scanner	`vserver vscan scanner-pool servers show`

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

Configurer la numérisation à l'accès

Création d'une règle on-Access

Une règle On-Access définit l'étendue d'une analyse on-Access. On peut créer une on-Access policy pour un SVM individuel ou pour tous les SVM d'un cluster. Si vous avez créé une on-Access policy pour tous les SVM d'un cluster, vous devez activer la politique sur chaque SVM individuellement.

Description de la tâche

- Vous pouvez spécifier la taille maximale du fichier à numériser, les extensions de fichier et les chemins à inclure dans la numérisation, ainsi que les extensions de fichier et les chemins à exclure de la numérisation.
- Vous pouvez définir le `scan-mandatory` Option désactivée pour spécifier que l'accès aux fichiers est autorisé lorsqu'aucun serveur Vscan n'est disponible pour l'analyse antivirus.
- Par défaut, ONTAP crée une on-Access policy nommée « default_CIFS » et l'active pour tous les SVM d'un cluster.
- Tout fichier admissible à l'exclusion de numérisation en fonction du `paths-to-exclude`, `file-ext-to-exclude`, ou `max-file-size` les paramètres ne sont pas pris en compte pour l'acquisition, même si l' `scan-mandatory` l'option est activée. (Cochez cette case "dépannage" pour les problèmes de connectivité liés au `scan-mandatory` option.)
- Par défaut, seuls les volumes en lecture-écriture sont analysés. Vous pouvez spécifier des filtres qui permettent la numérisation de volumes en lecture seule ou qui limitent la numérisation aux fichiers ouverts avec l'accès d'exécution.
- L'analyse antivirus n'est pas effectuée sur un partage SMB pour lequel le paramètre disponible en continu est défini sur Oui.
- Voir la "Architecture antivirus" Pour plus d'informations sur le profil *Vscan file-Operations*.
- Vous pouvez créer un maximum de dix (10) règles d'accès par SVM. Toutefois, vous ne pouvez activer qu'une seule stratégie d'accès à la fois.
  - Vous pouvez exclure un maximum de cent (100) chemins et extensions de fichiers de l'analyse antivirus dans une stratégie d'accès.
- Quelques recommandations d'exclusion de fichiers :
  - Pensez à exclure les fichiers volumineux (la taille de fichier peut être spécifiée) de l'analyse antivirus car ils peuvent entraîner un temps de réponse lent ou des délais de requête d'analyse pour les utilisateurs CIFS. La taille de fichier par défaut pour l'exclusion est de 2 Go.
  - Pensez à exclure les extensions de fichier telles que `.vhd` et `.tmp` car les fichiers avec ces extensions peuvent ne pas être appropriés pour la numérisation.
  - Pensez à exclure les chemins de fichiers tels que le répertoire de quarantaine ou les chemins dans lesquels seuls les disques durs virtuels ou les bases de données sont stockés.
  - Vérifiez que toutes les exclusions sont spécifiées dans la même stratégie, car une seule stratégie peut

être activée à la fois. NetApp recommande vivement de disposer du même ensemble d'exclusions que celui spécifié dans le moteur antivirus.

- Une stratégie d'accès est requise pour un analyse à la demande. Pour éviter la numérisation à l'accès, vous devez définir `-scan-files-with-no-ext` pour faux et `-file-ext-to-exclude` à * pour exclure tous les postes.

Étapes

1. Création d'une règle on-Access :

   `vserver vscan on-access-policy create -vserver` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`policy_name`* `-protocol CIFS -max-file-size` *`max_size_of_files_to_scan`* `-filters [scan-ro-volume,][scan-execute-access] -file-ext-to-include` *`extensions_of_files_to_include`* `-file-ext-to-exclude` *`extensions_of_files_to_exclude`* `-scan-files-with-no-ext true|false -paths-to -exclude` *`paths_of_files_to_exclude`* `-scan-mandatory on|off`

   - Spécifier un SVM de données pour une politique définie pour un SVM individuel, un SVM d'administration du cluster pour une politique définie pour tous les SVM d'un cluster.
   - Le `-file-ext-to-exclude` le réglage remplace le `-file-ext-to-include` réglage.
   - Réglez `-scan-files-with-no-ext` à vrai pour numériser des fichiers sans extensions.
     La commande suivante crée une on-Access policy nommée `Policy1` sur le `vs1` SVM :

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include “mp*”,"tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. Vérifiez que la stratégie on-Access a été créée : `vserver vscan on-access-policy show -instance` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`name`*

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails de `Policy1` règle :

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Activez une stratégie on-Access

Une règle On-Access définit l'étendue d'une analyse on-Access. Vous devez activer une on-Access policy sur un SVM avant que ses fichiers ne puissent être analysés.

Si vous avez créé une on-Access policy pour tous les SVM d'un cluster, vous devez activer la politique sur chaque SVM individuellement. Vous ne pouvez activer qu'une seule stratégie à la fois sur un SVM.

Étapes

1. Activer une stratégie on-Access :

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   La commande suivante active une on-Access policy nommée `Policy1` sur le `vs1` SVM :

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. Vérifiez que la stratégie on-Access est activée :

   `vserver vscan on-access-policy show -instance` *`data_SVM`* `-policy-name` *`policy_name`*

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails de `Policy1` règle d'accès :

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Modifier le profil des opérations-fichiers Vscan pour un partage SMB

Le profil _Vscan opérations-fichiers_pour un partage SMB définit les opérations sur le partage qui peuvent déclencher le scan. Par défaut, le paramètre est défini sur `standard`. Vous pouvez régler le paramètre si nécessaire lors de la création ou de la modification d'un partage SMB.

Voir la "Architecture antivirus" Pour plus d'informations sur le profil *Vscan file-Operations*.

> L'analyse antivirus n'est pas effectuée sur un partage SMB disposant du `continuously-available` paramètre défini sur `Yes`.

Étape

1. Modifier la valeur du profil Vscan file-Operations pour un partage SMB :

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante remplace le profil des opérations de fichier Vscan pour un partage SMB par `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

Commandes permettant de gérer les règles d'accès

Vous pouvez modifier, désactiver ou supprimer une stratégie On-Access. Vous pouvez

afficher un résumé et les détails de la règle.

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Création d'une règle on-Access	`vserver vscan on-access-policy create`
Modifier une stratégie d'accès	`vserver vscan on-access-policy modify`
Activez une stratégie on-Access	`vserver vscan on-access-policy enable`
Désactivez une stratégie on-Access	`vserver vscan on-access-policy disable`
Supprimez une on-Access policy	`vserver vscan on-access-policy delete`
Afficher un récapitulatif et des détails d'une stratégie d'accès	`vserver vscan on-access-policy show`
Ajouter à la liste des chemins à exclure	`vserver vscan on-access-policy paths-to-exclude add`
Supprimer de la liste des chemins à exclure	`vserver vscan on-access-policy paths-to-exclude remove`
Afficher la liste des chemins à exclure	`vserver vscan on-access-policy paths-to-exclude show`
Ajouter à la liste des extensions de fichier à exclure	`vserver vscan on-access-policy file-ext-to-exclude add`
Supprimer de la liste des extensions de fichier à exclure	`vserver vscan on-access-policy file-ext-to-exclude remove`
Afficher la liste des extensions de fichier à exclure	`vserver vscan on-access-policy file-ext-to-exclude show`
Ajouter à la liste des extensions de fichier à inclure	`vserver vscan on-access-policy file-ext-to-include add`
Supprimer de la liste des extensions de fichier à inclure	`vserver vscan on-access-policy file-ext-to-include remove`
Afficher la liste des extensions de fichier à inclure	`vserver vscan on-access-policy file-ext-to-include show`

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

Configurer l'acquisition à la demande

Configuration de la numérisation à la demande

Vous pouvez utiliser l'analyse à la demande pour rechercher immédiatement ou planifier la présence de virus dans les fichiers.

Vous pouvez exécuter des analyses uniquement pendant les heures creuses, par exemple. Vous pouvez également rechercher des fichiers très volumineux exclus de cette analyse lors d'une analyse à l'accès. Vous pouvez utiliser une planification cron pour spécifier quand la tâche s'exécute.

À propos de cette rubrique

- Vous pouvez affecter un planning lorsque vous créez une tâche.
- Une seule tâche peut être planifiée à la fois sur un SVM.
- La numérisation à la demande ne prend pas en charge la lecture de liens symboliques ou de fichiers de flux.

> La numérisation à la demande ne prend pas en charge la lecture de liens symboliques ou de fichiers de flux.

> Pour créer une tâche à la demande, au moins une stratégie d'accès doit être activée. Il peut s'agir de la stratégie par défaut ou d'une stratégie d'accès créée par l'utilisateur.

Créer une tâche à la demande

Une tâche à la demande définit la portée de l'analyse antivirus à la demande. Vous pouvez spécifier la taille maximale des fichiers à scanner, les extensions et les chemins des fichiers à inclure dans le scan, ainsi que les extensions et chemins des fichiers à exclure du scan. Les fichiers des sous-répertoires sont analysés par défaut.

Description de la tâche

- Dix (10) tâches à la demande au maximum peuvent être effectuées pour chaque SVM, mais une seule peut être active.
- Une tâche à la demande crée un rapport, qui contient des informations sur les statistiques relatives aux analyses. Ce rapport est accessible à l'aide d'une commande ou en téléchargeant le fichier de rapport créé par la tâche à l'emplacement défini.

Avant de commencer

- Vous devez avoir création d'une stratégie d'accès. La stratégie peut être créée par défaut ou par l'utilisateur. Sans la stratégie On-Access, vous ne pouvez pas activer la numérisation.

Étapes

1. Créer une tâche à la demande :

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
```

`-no-ext true|false -directory-recursion true|false`

- Le `-file-ext-to-exclude` le réglage remplace le `-file-ext-to-include` réglage.
- Réglez `-scan-files-with-no-ext` à vrai pour numériser des fichiers sans extensions.

  Pour obtenir la liste complète des options, reportez-vous au "référence de commande".

  La commande suivante crée une tâche à la demande nommée `Task1` Sur la `vs1'Svm:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> Vous pouvez utiliser le `job show` commande permettant d'afficher l'état du travail. Vous pouvez utiliser le `job pause` et `job resume` commandes permettant d'interrompre et de redémarrer le travail, ou le `job stop` commande pour mettre fin au travail.

2. Vérifiez que la tâche à la demande a été créée :

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails de `Task1` tâche :

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                           Vserver: vs1
                         Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

Une fois que vous avez terminé

Vous devez activer l'analyse sur la SVM avant que la tâche ne soit planifiée.

Planifiez une tâche à la demande

Vous pouvez créer une tâche sans affecter de planification et utiliser le `vserver vscan on-demand-task schedule` pour attribuer un planning ou pour ajouter un planning lors de la création de la tâche.

Description de la tâche

Planification affectée avec `vserver vscan on-demand-task schedule` la commande remplace un planning déjà affecté par le `vserver vscan on-demand-task create` commande.

Étapes

1. Planifier une tâche à la demande :

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   La commande suivante planifie une tâche à accès nommée `Task2` sur le `vs2` SVM :

   ```
   cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
   -name Task2 -schedule daily
   [Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
   command to view the status.
   ```

Pour afficher l'état du travail, utilisez le `job show` commande. Le `job pause` et `job resume` les commandes, respectivement, permettent de suspendre et de redémarrer le travail ; le `job stop` la commande met fin au travail.

2. Vérifiez que la tâche à la demande a été planifiée :

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les détails de `Task 2` tâche :

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                           Vserver: vs2
                         Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
```

Une fois que vous avez terminé

Vous devez activer l'analyse sur la SVM avant que la tâche ne soit planifiée.

Exécutez immédiatement une tâche à la demande

Vous pouvez exécuter une tâche à la demande immédiatement, que vous ayez affecté ou non un planning.

Avant de commencer

On doit avoir activé l'analyse sur le SVM.

Étape

1. Exécuter une tâche à la demande immédiatement :

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   La commande suivante exécute une tâche à accès nommée `Task1` sur le `vs1` SVM :

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

Vous pouvez utiliser le `job show` commande permettant d'afficher l'état du travail. Vous pouvez utiliser le `job pause` et `job resume` commandes permettant d'interrompre et de redémarrer le travail, ou le `job stop` commande pour mettre fin au travail.

Commandes permettant de gérer des tâches à la demande

Vous pouvez modifier, supprimer ou annuler la planification d'une tâche à la demande. Vous pouvez afficher un résumé et des détails de la tâche et gérer les rapports de la tâche.

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Créer une tâche à la demande	`vserver vscan on-demand-task create`
Modifier une tâche à la demande	`vserver vscan on-demand-task modify`
Supprimer une tâche à la demande	`vserver vscan on-demand-task delete`
Exécutez une tâche à la demande	`vserver vscan on-demand-task run`
Planifiez une tâche à la demande	`vserver vscan on-demand-task schedule`
Annulez la planification d'une tâche à la demande	`vserver vscan on-demand-task unschedule`
Consultez le récapitulatif des tâches à la demande et les détails correspondant	`vserver vscan on-demand-task show`
Consultez les rapports à la demande	`vserver vscan on-demand-task report show`
Supprimer des rapports à la demande	`vserver vscan on-demand-task report delete`

Pour plus d'informations sur ces commandes, consultez les pages de manuels.

Bonnes pratiques de configuration de la fonctionnalité antivirus externe dans ONTAP

Envisagez les recommandations suivantes pour la configuration de la fonctionnalité

externe dans ONTAP.

- Limiter les utilisateurs privilégiés aux opérations d'analyse antivirus. Les utilisateurs normaux doivent être déconseillés d'utiliser des informations d'identification d'utilisateur privilégiées. Cette restriction peut être obtenue en désactivant les droits de connexion pour les utilisateurs privilégiés sur Active Directory.
- Les utilisateurs privilégiés ne sont pas tenus de faire partie d'un groupe d'utilisateurs disposant d'un grand nombre de droits dans le domaine, tels que le groupe d'administrateurs ou le groupe d'opérateurs de sauvegarde. Les utilisateurs privilégiés doivent être validés uniquement par le système de stockage de sorte qu'ils soient autorisés à créer des connexions au serveur Vscan et à accéder aux fichiers pour l'analyse antivirus.
- Utiliser les ordinateurs exécutant des serveurs Vscan uniquement à des fins d'analyse antivirus. Pour décourager l'utilisation générale, désactivez les services de terminal Windows et les autres dispositions d'accès à distance sur ces ordinateurs et accordez le droit d'installer de nouveaux logiciels sur ces ordinateurs uniquement aux administrateurs.
- Dédiez les serveurs Vscan à l'analyse antivirus et ne les utilisez pas pour d'autres opérations, telles que les sauvegardes. Vous pouvez décider d'exécuter le serveur Vscan en tant que machine virtuelle (VM). Si vous exécutez le serveur Vscan en tant que VM, assurez-vous que les ressources allouées à la VM ne sont pas partagées et suffisantes pour effectuer une analyse antivirus.
- Fournir le CPU, la mémoire et la capacité disque appropriés au serveur Vscan pour éviter toute sur-allocation des ressources La plupart des serveurs Vscan sont conçus pour utiliser plusieurs serveurs CPU core et pour répartir la charge entre les CPU.
- NetApp recommande d'utiliser un réseau dédié avec un VLAN privé pour la connexion de la SVM au serveur Vscan de sorte que le trafic de scan n'est pas affecté par d'autres trafic réseau client. Créer une carte d'interface réseau (NIC) distincte dédiée au VLAN antivirus sur le serveur Vscan et à la LIF de données sur la SVM Cette étape simplifie l'administration et le dépannage en cas de problèmes réseau. Le trafic antivirus doit être isolé à l'aide d'un réseau privé. Le serveur antivirus doit être configuré pour communiquer avec le contrôleur de domaine (DC) et ONTAP de l'une des manières suivantes :
  - Le DC doit communiquer avec les serveurs antivirus via le réseau privé utilisé pour isoler le trafic.
  - Le serveur DC et antivirus doivent communiquer via un autre réseau (pas le réseau privé mentionné précédemment), qui n'est pas le même que le réseau client CIFS.
  - Pour activer l'authentification Kerberos pour la communication antivirus, créez une entrée DNS pour les LIFs privées et un nom principal de service sur le DC correspondant à l'entrée DNS créée pour la LIF privée. Utiliser ce nom lors de l'ajout d'une LIF au antivirus Connector. Le DNS doit pouvoir renvoyer un nom unique pour chaque LIF privée connectée au connecteur antivirus.

> Si la LIF du trafic Vscan est configurée sur un port différent de la LIF pour le trafic client, la LIF Vscan peut basculer vers un autre nœud en cas de défaillance de port. La modification rend le serveur Vscan inaccessible depuis le nouveau nœud et les notifications de scan pour les opérations de fichier sur le nœud échouent. Vérifier que le serveur Vscan est accessible via au moins une LIF sur un nœud de sorte qu'il puisse traiter les demandes de scan pour les opérations de fichier effectuées sur ce nœud.

- Connecter le système de stockage NetApp et le serveur Vscan en utilisant au moins un réseau 1GbE.
- Pour un environnement avec plusieurs serveurs Vscan, connectez tous les serveurs qui ont des connexions réseau hautes performances similaires. La connexion des serveurs Vscan améliore les performances en permettant le partage de charge.
- Pour les sites distants et les succursales, NetApp recommande d'utiliser un serveur Vscan local plutôt qu'un serveur Vscan distant, car le premier est le candidat idéal à une latence élevée. Si le coût est un facteur, utilisez un ordinateur portable ou un PC pour une protection antivirus modérée. Vous pouvez

planifier des analyses complètes périodiques du système de fichiers en partageant les volumes ou les qtrees et en les analysant à partir de n'importe quel système du site distant.

- Utiliser plusieurs serveurs Vscan pour scanner les données sur la SVM à des fins d'équilibrage de charge et de redondance La quantité de charge de travail CIFS et le trafic antivirus résultant varient selon les SVM. Surveillez la latence CIFS et l'analyse antivirus sur le contrôleur de stockage. Surveiller la tendance des résultats au fil du temps. Si la latence CIFS et la latence de l'analyse antivirus augmentent en raison des files d'attente des processeurs ou des applications sur les serveurs Vscan, les clients CIFS peuvent rencontrer de longs délais d'attente. Ajouter des serveurs Vscan supplémentaires pour distribuer la charge.
- Installez la dernière version de ONTAP antivirus Connector.
- Maintenez les moteurs antivirus et les définitions à jour. Consultez vos partenaires pour obtenir des recommandations sur la fréquence de mise à jour.
- Dans un environnement multi-tanancy, un pool de scanner (pool de serveurs Vscan) peut être partagé avec plusieurs SVM à condition que les serveurs Vscan et les SVM fassent partie du même domaine ou du même domaine de confiance.
- La stratégie de logiciel antivirus pour les fichiers infectés doit être définie sur « delete » ou « quarantine », qui est la valeur par défaut définie par la plupart des fournisseurs d'antivirus. Si le « vscan-fileop-profile » est défini sur « write_only » et si un fichier infecté est trouvé, le fichier reste dans le partage et peut être ouvert car l'ouverture d'un fichier ne déclenche pas de scan. Le scan antivirus est déclenché uniquement après la fermeture du fichier.
- Le `scan-engine timeout` la valeur doit être inférieure à `scanner-pool request-timeout` valeur. Si la valeur est supérieure, l'accès aux fichiers peut être retardé et peut éventuellement prendre du temps. Pour éviter cela, configurez le `scan-engine timeout` à 5 secondes de moins que le `scanner-pool request-timeout` valeur. Reportez-vous à la documentation du fournisseur du moteur de numérisation pour obtenir des instructions sur la façon de modifier le `scan-engine timeout` paramètres. Le `scanner-pool timeout` peut être modifié à l'aide de la commande suivante en mode avancé et en fournissant la valeur appropriée pour `request-timeout` paramètre : `vserver vscan scanner-pool modify`.
- Pour un environnement dimensionné pour les charges de travail d'analyse à l'accès et nécessitant l'analyse à la demande, NetApp recommande de planifier la tâche d'analyse à la demande en dehors des heures de pointe afin d'éviter toute charge supplémentaire sur l'infrastructure antivirus existante.

Pour en savoir plus sur les meilleures pratiques propres à nos partenaires, rendez-vous sur "Solutions partenaires Vscan".

Activer l'analyse antivirus sur un SVM

Vous devez activer l'analyse antivirus sur un SVM avant de pouvoir exécuter une analyse à la demande ou à l'accès.

Étapes

1. Activer l'analyse antivirus sur un SVM :

   ```
   vserver vscan enable -vserver data_SVM
   ```

   > Vous pouvez utiliser le `vserver vscan disable` pour désactiver l'analyse antivirus, si nécessaire.

   La commande suivante active l'analyse antivirus sur le `vs1` SVM :

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

2. Vérifier que l'analyse antivirus est activée sur le SVM :

   `vserver vscan show -vserver data_SVM`

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche le statut Vscan du `vs1` SVM :

```
cluster1::> vserver vscan show -vserver vs1

                          Vserver: vs1
                      Vscan Status: on
```

Réinitialisez l'état des fichiers numérisés

Il peut arriver que vous souhaitiez réinitialiser l'état d'analyse des fichiers numérisés correctement sur un SVM en utilisant le `vserver vscan reset` commande pour ignorer les informations mises en cache pour les fichiers. Vous pouvez utiliser cette commande pour redémarrer le traitement de l'analyse antivirus en cas de mauvaise configuration d'une analyse, par exemple.

Description de la tâche

Après avoir exécuté le `vserver vscan reset` commande, tous les fichiers admissibles seront numérisés la prochaine fois qu'ils seront consultés.

> Cette commande peut avoir un impact négatif sur les performances, en fonction du nombre et de la taille des fichiers à réanalyser.

Ce dont vous aurez besoin

Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   `set -privilege advanced`

2. Réinitialiser l'état des fichiers numérisés :

   `vserver vscan reset -vserver data_SVM`

   La commande suivante réinitialise l'état des fichiers numérisés sur le `vs1` SVM :

```
cluster1::> vserver vscan reset -vserver vs1
```

Afficher les informations du journal des événements Vscan

Vous pouvez utiliser le `vserver vscan show-events` Commande pour afficher les informations du journal des événements concernant les fichiers infectés, les mises à jour vers les serveurs Vscan, et le même type. Vous pouvez afficher les informations d'événements pour le cluster ou pour des nœuds, SVM ou serveurs Vscan spécifiques.

Avant de commencer

Des privilèges avancés sont requis pour afficher le journal des événements Vscan.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Afficher les informations du journal des événements Vscan :

   ```
   vserver vscan show-events
   ```

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante affiche les informations du journal des événements du cluster `cluster1`:

   ```
   cluster1::*> vserver vscan show-events

   Vserver     Node            Server          Event Type        Event Time
   ----------- --------------- --------------- -----------------
   -----------------
   vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
   11:37:38
   vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
   11:37:08
   vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
   11:34:55
   3 entries were displayed.
   ```

Surveillez et résolvez les problèmes de connectivité

Problèmes de connectivité potentiels impliquant l'option Scan-obligatoire

Vous pouvez utiliser le `vserver vscan connection-status show` Commandes pour afficher des informations sur les connexions du serveur Vscan qui vous seront peut-être utiles dans le dépannage des problèmes de connectivité.

Par défaut, le `scan-mandatory` L'option d'analyse On-Access refuse l'accès aux fichiers lorsqu'une connexion au serveur Vscan n'est pas disponible pour l'analyse. Bien que cette option offre des fonctions de sécurité importantes, elle peut entraîner des problèmes dans quelques situations.

- Avant d'activer l'accès client, il faut s'assurer qu'au moins un serveur Vscan est connecté à un SVM sur chaque nœud qui dispose d'une LIF. Si vous devez connecter les serveurs aux SVM après avoir autorisé l'accès client, vous devez désactiver le `scan-mandatory` Option sur le SVM pour s'assurer que l'accès aux fichiers n'est pas refusé car une connexion au serveur Vscan n'est pas disponible. Vous pouvez réactiver l'option après la connexion du serveur.
- Si une LIF cible héberge toutes les connexions de serveur Vscan pour un SVM, la connexion entre le serveur et la SVM sera perdue si la LIF est migrée. Pour vous assurer que l'accès aux fichiers n'est pas refusé car une connexion au serveur Vscan n'est pas disponible, vous devez désactiver le système `scan-mandatory` Option avant de migrer la LIF. Vous pouvez réactiver l'option après la migration de la LIF.

Chaque SVM doit disposer d'au moins deux serveurs Vscan qui lui sont affectés. Il s'agit d'une meilleure pratique de connexion des serveurs Vscan au système de stockage sur un réseau différent de celui utilisé pour l'accès client.

Commandes pour afficher l'état de connexion du serveur Vscan

Vous pouvez utiliser le `vserver vscan connection-status show` Commandes pour afficher les informations récapitulatives et détaillées sur l'état de la connexion au serveur Vscan.

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Afficher un récapitulatif des connexions du serveur Vscan	`vserver vscan connection-status show`
Afficher les détails des connexions du serveur Vscan	`vserver vscan connection-status show-all`
Afficher les détails des serveurs Vscan connectés	`vserver vscan connection-status show-connected`
Afficher les détails des serveurs Vscan disponibles qui ne sont pas connectés	`vserver vscan connection-status show-not-connected`

Pour plus d'informations sur ces commandes, reportez-vous au "Pages de manuel ONTAP".

Résolution des problèmes liés à l'analyse antivirus

Pour les problèmes courants d'analyse antivirus, il existe des causes possibles et des moyens de les résoudre. L'analyse antivirus est également appelée Vscan.

Problème	Comment le résoudre

Les serveurs Vscan ne peuvent pas se connecter à Système de stockage clustered ONTAP.	Vérifier si la configuration scanner pool spécifie l'adresse IP du serveur Vscan. Vérifiez également si les utilisateurs privilégiés autorisés dans la liste scanner pool sont actifs. Pour vérifier le scanner pool, exécutez le `vserver vscan scanner-pool show` dans l'invite de commande du système de stockage. Si les serveurs Vscan ne peuvent toujours pas se connecter, il peut y avoir un problème au niveau du réseau.
Les clients observent une latence élevée.	Il est probablement temps d'ajouter d'autres serveurs Vscan au pool de scanner.
Trop d'acquisitions sont déclenchées.	Modifier la valeur du `vscan-fileop-profile` paramètre permettant de limiter le nombre d'opérations de fichiers surveillées pour l'analyse antivirus.
Certains fichiers ne sont pas numérisés.	Vérifiez la stratégie d'accès. Il est possible que le chemin de ces fichiers ait été ajouté à la liste d'exclusion de chemin ou que leur taille dépasse la valeur configurée pour les exclusions. Pour vérifier la stratégie On-Access, exécutez `vserver vscan on-access-policy show` dans l'invite de commande du système de stockage.
Accès au fichier refusé.	Vérifiez si le paramètre *scan-obligatoire* est spécifié dans la configuration de la stratégie. Ce paramètre refuse l'accès aux données si aucun serveur Vscan n'est connecté. Modifiez le paramètre si nécessaire.

Surveiller l'état et les activités de performance

Vous pouvez surveiller les aspects critiques du module Vscan, tels que le statut de connexion du serveur Vscan,
La santé des serveurs Vscan et le nombre de fichiers analysés. Ces informations sont utiles
Vous diagnostiquez les problèmes liés au serveur Vscan.

Afficher les informations de connexion au serveur Vscan

Vous pouvez afficher le statut de connexion des serveurs Vscan pour gérer les connexions qui sont déjà utilisées
et les connexions disponibles. Diverses commandes affichent des informations
À propos du statut de connexion des serveurs Vscan.

Commande…	Informations affichées…
`vserver vscan connection-status show`	Résumé de l'état de la connexion

`vserver vscan connection-status show-all`	Informations détaillées sur l'état de la connexion
`vserver vscan connection-status show-not-connected`	État des connexions disponibles mais non connectées
`vserver vscan connection-status show-connected`	Informations sur le serveur Vscan connecté

Pour plus d'informations sur ces commandes, reportez-vous au "pages de manuel".

Afficher les statistiques du serveur Vscan

Vous pouvez afficher les statistiques spécifiques au serveur Vscan pour surveiller les performances et diagnostiquer les problèmes liés à
analyse antivirus Vous devez collecter un échantillon de données avant de pouvoir utiliser le `statistics show` commande à
Afficher les statistiques du serveur Vscan.
Pour compléter un échantillon de données, procédez comme suit :

Étape

1. Exécutez le `statistics start` commande et le `optional statistics` commande d'arrêt.

Afficher les statistiques des requêtes et des latences du serveur Vscan

Vous pouvez utiliser ONTAP `offbox_vscan` Compteurs par SVM pour surveiller le taux de Vscan Requêtes de serveur envoyées et reçues par seconde et latences de serveur dans tous les Vscan serveurs. Pour afficher ces statistiques, procédez comme suit :

Étape

1. Exécutez les statistiques show `object offbox_vscan -instance SVM` commande avec compteurs suivants :

Compteur…	Informations affichées…
`scan_request_dispatched_rate`	Nombre de requêtes antivirus envoyées par ONTAP aux serveurs Vscan par seconde
`scan_noti_received_rate`	Nombre de requêtes antivirus reçues par ONTAP des serveurs Vscan par seconde
`dispatch_latency`	Latence dans ONTAP pour identifier un serveur Vscan disponible et envoyer la demande à ce serveur Vscan
`scan_latency`	Latence aller-retour de ONTAP au serveur Vscan, y compris le temps que le scan doit s'exécuter

Exemple de statistiques générées à partir d'un compteur ONTAP externe vscan

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
--------------------------------------------------------------------
```

Afficher les statistiques des requêtes et des latences individuelles du serveur Vscan

Vous pouvez utiliser ONTAP `offbox_vscan_server` Compteurs sur un serveur Vscan par SVM, par serveur Vscan externe,
Et par nœud pour surveiller le taux des requêtes du serveur Vscan expédiées et la latence du serveur sur Chaque serveur Vscan individuellement. Pour collecter ces informations, procédez comme suit :

Étape

1. Exécutez le `statistics show -object offbox_vscan -instance SVM:servername:nodename` avec les compteurs suivants :

Compteur…	Informations affichées…
`scan_request_dispatched_rate`	Nombre de demandes d'analyse antivirus envoyées par ONTAP
`scan_latency`	Latence aller-retour de ONTAP au serveur Vscan, y compris le temps que le scan doit s'exécuter Vers les serveurs Vscan par seconde

Exemple de statistiques générées à partir d'un compteur ONTAP offbox_vscan_Server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-----------------------------------------------------------------
```

Afficher les statistiques d'utilisation du serveur Vscan

Vous pouvez également utiliser ONTAP `offbox_vscan_server` Compteurs pour la collecte de l'utilisation Vscan côté serveur
statistiques. Ces statistiques sont suivies par SVM, par serveur Vscan externe et par nœud. Ils
Inclure l'utilisation des CPU sur le serveur Vscan, la profondeur de file d'attente pour les opérations de scan sur le serveur Vscan
(actuel et maximal), mémoire utilisée et réseau utilisé.
Ces statistiques sont transmises par l'antivirus Connector aux compteurs statistiques de ONTAP. Ils
sont basées sur des données interrogées toutes les 20 secondes et doivent être collectées plusieurs fois pour plus de précision ;
sinon, les valeurs affichées dans les statistiques reflètent uniquement la dernière interrogation. L'utilisation du processeur et les files d'attente sont
il est particulièrement important de surveiller et d'analyser. Une valeur élevée pour une file d'attente moyenne peut indiquer que l'
Le serveur Vscan présente un goulet d'étranglement.
Pour collecter les statistiques d'utilisation du serveur Vscan sur un SVM, un serveur Vscan par—serveur externe, et par—nœud
basis, effectuez l'étape suivante :

Étape

1. Collectez les statistiques d'utilisation du serveur Vscan

   Exécutez le `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` avec les commandes suivantes `offbox_vscan_server` compteurs :

Compteur…	Informations affichées…
`scanner_stats_pct_cpu_used`	Utilisation du CPU sur le serveur Vscan
`scanner_stats_pct_input_queue_avg`	File d'attente moyenne des requêtes de scan sur le serveur Vscan
`scanner_stats_pct_input_queue_hiwatermark`	File d'attente de pointe des requêtes de scan sur le serveur Vscan

`scanner_stats_pct_mem_used`	Mémoire utilisée sur le serveur Vscan
`scanner_stats_pct_network_used`	Réseau utilisé sur le serveur Vscan

Exemple de statistiques d'utilisation pour le serveur Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

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 `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 EVTX 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">00000000000000;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">00000000000401;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
   ```

   ```
                                   Junction                      Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   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.text
   ```

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 EVTX 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` marquez, 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)
  F

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
Nom du SVM Nom du SVM sur lequel créer la configuration d'audit. Le SVM doit déjà exister.	`-vserver vserver_name`	Oui.	Oui.	

Chemin de destination du journal 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).	`-destination text`	Oui.	Oui.	

Catégories d'événements à auditer Spécifie les catégories d'événements à auditer. Les catégories d'événements suivantes peuvent être auditées : • Événements d'accès aux fichiers (SMB et NFSv4) • Événements de connexion et de déconnexion SMB • Événements d'activation de stratégie d'accès central Les événements de transfert de stratégie d'accès central sont disponibles à partir des domaines Active Directory de Windows 2012. • 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 La valeur par défaut consiste à auditer l'accès aux fichiers et les événements de connexion et de déconnexion SMB. **Remarque :** avant de pouvoir spécifier `cap-staging` 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.	`-events` {`file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`

audit-policy-change	user-account	security-group	authorization-policy-change}	Non
		Format de sortie du fichier journal Détermine 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.	-format {xml	evtx}

Non			*Limite de rotation des fichiers journaux* Détermine 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. Valeur de `0` indique que tous les fichiers journaux sont conservés. La valeur par défaut est 0.	`-rotate-limit integer`

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
Limite de taille du fichier journal Détermine la limite de taille du fichier journal d'audit.	`-rotate-size` {`integer`[KO	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
Horaire de rotation du journal : mois 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.	`-rotate-schedule-month chron_month`	Non		
Horaire de rotation du journal : jour de la semaine 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.	`-rotate-schedule -dayofweek chron_dayofweek`	Non		
Horaire de rotation du journal : jour 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.	`-rotate-schedule-day chron_dayofmonth`	Non		

Horaire de rotation du journal : heure Détermine le planning horaire pour la rotation du journal d'audit. Les valeurs valides vont de `0` de minuit à `23` (11 h 00). Spécification `all` 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).	`-rotate-schedule-hour chron_hour`	Non		
Horaire de rotation du journal : minute Détermine la planification des minutes pour la rotation du journal d'audit. 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.	`-rotate-schedule-minute chron_minute`	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::> vserver audit create -vserver 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::> vserver audit create -vserver 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::> vserver audit create -vserver 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
```

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).

Ce dont vous avez besoin

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.

Étape

1. Activer l'audit sur le SVM :

   ```
   vserver audit enable -vserver vserver_name
   ```

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

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: evtx
                  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
   ```

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.

Ce dont vous avez besoin

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 DALC.

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	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	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	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 auditables, 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 CLS 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 (SALC) 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	`vserver security file-directory show -vserver vserver_name -path path`
En tant que liste détaillée	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemples

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin `/corp` Au SVM vs1. Le chemin dispose d'une sécurité NTFS efficace. Le descripteur de sécurité NTFS contient à la fois une entrée RACL RÉUSSIE/ÉCHEC.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin `/datavol1` Au SVM vs1. Le chemin contient à la fois des fichiers standard et des SACL de dossier et des SALC de Storage-Level Access Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

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::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

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

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

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::*> vserver 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 `vserver cifs users-and-groups <local-group>` et `vserver 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	`vserver audit enable -vserver vserver_name`
Désactivé	`vserver audit disable -vserver vserver_name`

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: 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
```

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	`vserver audit modify` avec le `-destination` paramètre

Modifier la catégorie d'événements à auditer	`vserver audit modify` avec le `-events` paramètre 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).
Modifiez le format du journal	`vserver audit modify` avec le `-format` paramètre
Activation des sauvegardes automatiques en fonction de la taille du fichier journal interne	`vserver audit modify` avec le `-rotate-size` paramètre
Activation des sauvegardes automatiques en fonction d'un intervalle de temps	`vserver audit modify` avec le `-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, et `-rotate-schedule-minute` paramètres
Spécification du nombre maximal de fichiers journaux enregistrés	`vserver audit modify` avec le `-rotate-limit` 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.

- Les administrateurs des SVM et du cluster peuvent déterminer l'espace de volume insuffisant en affichant des informations sur l'utilisation et la configuration des volumes et des agrégats.
- 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 :
>
> - Si le répertoire de destination est supprimé.
> - Si la limite du fichier sur 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          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
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 disposent d'un espace disponible inférieur à 2 Go, 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.

Utilisez FPolicy pour le contrôle et la gestion des fichiers sur SVM

Analysez FPolicy

De quoi sont les deux parties de la solution FPolicy

FPolicy est un système de notification d'accès aux fichiers qui permet de surveiller et de gérer les événements d'accès aux fichiers sur les machines virtuelles de stockage (SVM) à l'aide de solutions partenaires. Les solutions de partenaires vous aident à prendre en charge divers cas d'utilisation tels que la gouvernance et la conformité des données, la protection contre les ransomwares et la mobilité des données.

Les solutions partenaires incluent à la fois les solutions tierces prises en charge par NetApp et les produits NetApp sécurité des workloads et Cloud Data Sense.

Une solution FPolicy possède deux parties. La structure ONTAP FPolicy gère les activités sur le cluster et envoie des notifications à l'application partenaire (ou serveurs externes FPolicy). Les serveurs externes FPolicy traitent les notifications envoyées par ONTAP FPolicy pour répondre aux cas d'utilisation des clients.

Le framework ONTAP crée et gère la configuration FPolicy, surveille les événements de fichier et envoie des notifications aux serveurs FPolicy externes. ONTAP FPolicy fournit l'infrastructure qui permet la communication entre les serveurs FPolicy externes et les nœuds de machine virtuelle de stockage (SVM).

La structure FPolicy se connecte aux serveurs FPolicy externes et envoie des notifications pour certains événements du système de fichiers aux serveurs FPolicy lorsque ces événements se produisent suite à l'accès client. Les serveurs FPolicy externes traitent les notifications et réenvoient les réponses au nœud. Ce qui se produit à la suite du traitement des notifications dépend de l'application et si la communication entre le nœud et les serveurs externes est asynchrone ou synchrone.

Quelles sont les notifications synchrones et asynchrones

FPolicy envoie des notifications aux serveurs FPolicy externes par le biais de l'interface FPolicy. Les notifications sont envoyées en mode synchrone ou asynchrone. Le mode de notification détermine le rôle de ONTAP après l'envoi de notifications aux serveurs FPolicy.

- **Notifications asynchrones**

  Grâce aux notifications asynchrones, le nœud n'attend pas de réponse du serveur FPolicy, ce qui améliore le débit global du système. Ce type de notification est adapté aux applications où le serveur FPolicy n'exige aucune action résultant de l'évaluation des notifications. Par exemple, les notifications asynchrones sont utilisées lorsque l'administrateur de la machine virtuelle de stockage (SVM) souhaite surveiller et auditer l'activité d'accès aux fichiers.

  Lorsqu'un serveur FPolicy fonctionnant en mode asynchrone est en panne du réseau, les notifications FPolicy générées lors de la panne sont stockées sur le nœud de stockage. Lorsque le serveur FPolicy est de nouveau en ligne, il est averti des notifications stockées et peut les récupérer du nœud de stockage. La durée pendant laquelle les notifications peuvent être stockées en cas de panne peut être configurée pendant 10 minutes.

  À partir de ONTAP 9.14.1, FPolicy permet de configurer un magasin persistant pour capturer les

événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

- **Notifications synchrones**

  Lorsqu'il est configuré pour s'exécuter en mode synchrone, le serveur FPolicy doit accuser réception de chaque notification avant que l'opération client ne puisse continuer. Ce type de notification est utilisé lorsqu'une action est requise en fonction des résultats de l'évaluation des notifications. Par exemple, les notifications synchrones sont utilisées lorsque l'administrateur du SVM souhaite autoriser ou refuser des requêtes en fonction de critères spécifiés sur le serveur FPolicy externe.

Applications synchrones et asynchrones

Il existe de nombreuses utilisations possibles pour les applications FPolicy, asynchrone et synchrone.

Les applications asynchrones sont celles où le serveur FPolicy externe n'affecte pas l'accès aux fichiers ou aux répertoires ou ne modifie pas les données du SVM. Par exemple :

- Journalisation des audits et des accès aux fichiers
- Gestion des ressources de stockage

Les applications synchrones sont celles dont l'accès aux données est modifié ou quand le serveur FPolicy externe. Par exemple :

- La gestion des quotas
- Blocage de l'accès aux fichiers
- Archivage des fichiers et gestion du stockage hiérarchisé
- Services de cryptage et de décryptage
- Services de compression et de décompression

Les magasins persistants FPolicy

À partir de ONTAP 9.14.1, FPolicy permet de configurer un magasin persistant pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

Cette fonctionnalité est uniquement disponible en mode externe FPolicy. L'application partenaire que vous utilisez doit prendre en charge cette fonctionnalité. Vous devez collaborer avec votre partenaire pour vous assurer que cette configuration FPolicy est prise en charge.

Et des meilleures pratiques

Les administrateurs du cluster doivent configurer un volume pour le magasin persistant sur chaque SVM sur lequel FPolicy est activé. Lorsqu'il est configuré, un magasin persistant capture tous les événements FPolicy correspondants, qui sont ensuite traités dans le pipeline FPolicy et envoyés au serveur externe.

Le stockage persistant reste tel qu'il était au moment de la réception du dernier événement en cas de redémarrage inattendu ou lorsque FPolicy est désactivé et réactivé. Après une opération de basculement, les nouveaux événements sont stockés et traités par le nœud partenaire. Après une opération de rétablissement, le magasin persistant reprend le traitement de tout événement non traité qui pourrait rester en provenance de lorsque le basculement du nœud s'est produit. Les événements en direct seraient prioritaires sur les événements non traités.

Si le volume du magasin persistant passe d'un nœud à un autre dans la même SVM, les notifications qui ne sont pas encore traitées seront également déplacées vers le nouveau nœud. Vous devez exécuter à nouveau le `fpolicy persistent-store create` sur l'un des nœuds après le déplacement du volume, afin de garantir que la notification en attente est transmise au serveur externe.

Le volume de stockage persistant est configuré par SVM. Pour chaque SVM activé FPolicy, vous devez créer un volume de stockage persistant.

Créez le volume de stockage persistant sur le nœud avec les LIF qui prévoient que le trafic maximal sera surveillé par Fpolicy.

Si les notifications accumulées dans le magasin persistant dépassent la taille du volume provisionné, FPolicy commence à supprimer la notification entrante avec les messages EMS appropriés.

Le nom du volume de stockage persistant et le chemin de jonction spécifiés au moment de la création du volume doivent correspondre.

Définissez la règle de snapshot sur `none` pour ce volume au lieu de `default`. Cela permet de s'assurer qu'il n'y a pas de restauration accidentelle de l'instantané, ce qui entraîne la perte des événements actuels et d'empêcher le traitement des événements en double.

Rendre le volume de stockage persistant inaccessible pour l'accès au protocole utilisateur externe (CIFS/NFS) afin d'éviter toute corruption accidentelle ou suppression des enregistrements d'événements persistants. Pour ce faire, une fois FPolicy activé, démontez le volume dans ONTAP pour supprimer le chemin de jonction, ce qui le rend inaccessible pour l'accès au protocole utilisateur.

Pour plus d'informations, voir "Créez des magasins persistants".

Types de configuration FPolicy

Il existe deux types de configuration de base pour les serveurs FPolicy. Une seule configuration utilise des serveurs FPolicy externes pour traiter les notifications et agir. L'autre configuration n'utilise pas de serveurs FPolicy externes. Il utilise à la place le serveur FPolicy interne et natif ONTAP pour bloquer simplement les fichiers en fonction des extensions.

- **Configuration de serveur FPolicy externe**

  La notification est envoyée au serveur FPolicy qui présente la requête et applique des règles pour déterminer si le nœud doit autoriser l'opération de fichier demandée. Pour les règles synchrones, le serveur FPolicy envoie ensuite une réponse au nœud pour autoriser ou bloquer l'opération de fichier demandée.

- **Configuration de serveur FPolicy native**

  La notification est tramée en interne. La requête est autorisée ou refusée en fonction des paramètres d'extension de fichier configurés dans le cadre FPolicy.

Remarque : les demandes d'extension de fichier refusées ne sont pas consignées.

Quand créer une configuration FPolicy native

Les configurations FPolicy natives utilisent le moteur FPolicy interne de ONTAP pour surveiller et bloquer les opérations basées sur l'extension du fichier. Cette solution ne nécessite pas de serveurs FPolicy externes (serveurs FPolicy). L'utilisation d'une configuration native de blocage de fichiers est appropriée lorsque cette solution simple est tout ce qui est nécessaire.

Le blocage de fichiers natif vous permet de surveiller toutes les opérations de fichiers qui correspondent aux événements de filtrage et d'opération configurés, puis de refuser l'accès aux fichiers avec des extensions particulières. Il s'agit de la configuration par défaut.

Cette configuration permet de bloquer l'accès aux fichiers en fonction de l'extension du fichier uniquement. Par exemple, pour bloquer les fichiers contenant `mp3` extensions, vous configurez une stratégie pour fournir des notifications pour certaines opérations avec des extensions de fichier cible de `mp3`. La règle est configurée pour refuser `mp3` demandes de fichiers pour les opérations qui génèrent des notifications.

Les configurations FPolicy natives sont les suivantes :

- Le blocage de fichiers natif est également pris en charge par le filtrage de fichiers basé sur serveur FPolicy.
- Les applications natives de blocage de fichiers et de filtrage de fichiers sur serveur FPolicy peuvent être configurées simultanément.

  Pour ce faire, vous pouvez configurer deux règles FPolicy distinctes pour la machine virtuelle de stockage (SVM), une configurée pour le blocage natif des fichiers et une configurée pour le filtrage des fichiers basé sur serveur FPolicy.

- La fonctionnalité native de blocage de fichiers ne permet d'afficher que les fichiers basés sur les extensions et non sur le contenu du fichier.
- Dans le cas de liens symboliques, le blocage de fichiers natif utilise l'extension de fichier du fichier racine.

En savoir plus sur "FPolicy : blocage de fichiers natif".

Quand créer une configuration utilisant des serveurs FPolicy externes

Les configurations FPolicy qui utilisent des serveurs FPolicy externes pour traiter et gérer les notifications proposent des solutions fiables pour les cas d'utilisation où il est nécessaire de bloquer simplement des fichiers en fonction de l'extension des fichiers.

Pour ce faire, vous devez créer une configuration qui utilise des serveurs FPolicy externes lorsque vous souhaitez effectuer des tâches telles que la surveillance et l'enregistrement des événements d'accès aux fichiers, fournir des services de quotas, exécuter des blocages de fichiers selon des critères autres que les extensions de fichiers simples, fournir des services de migration des données à l'aide d'applications de gestion du stockage hiérarchisé, Vous pouvez également proposer un ensemble de règles à très grande granularité qui contrôlent uniquement un sous-ensemble de données du serveur virtuel de stockage (SVM).

Rôles liés aux composants du cluster avec l'implémentation FPolicy

Le cluster, les SVM contenant les machines virtuelles de stockage et les LIF de données jouent tous un rôle dans l'implémentation d'une FPolicy.

- **cluster**

  Le cluster contient le framework de gestion FPolicy. Il gère et gère les informations relatives à toutes les configurations FPolicy du cluster.

- **SVM**

  Une configuration FPolicy est définie au niveau de la SVM. L'étendue de la configuration est le SVM, et ne fonctionne que sur les ressources SVM. Une configuration SVM ne peut pas surveiller et envoyer de notifications pour les demandes d'accès aux fichiers effectuées pour les données résidant sur une autre SVM.

  Les configurations FPolicy peuvent être définies sur le SVM d'administration. Une fois les configurations définies sur le SVM d'administration, elles peuvent être consultées et utilisées dans tous les SVM.

- **LIF de données**

  Les connexions aux serveurs FPolicy sont effectuées via les LIF de données appartenant au SVM avec la configuration FPolicy. Les LIF de données utilisées pour ces connexions peuvent basculer de la même manière que les LIF de données utilisées pour un accès client normal.

Fonctionnement de FPolicy avec des serveurs FPolicy externes

Une fois FPolicy configuré et activé sur le SVM, FPolicy s'exécute sur chaque nœud auquel le SVM participe. FPolicy est chargé de l'établissement et de la maintenance des connexions avec des serveurs FPolicy externes (serveurs FPolicy), pour le traitement des notifications, ainsi que pour la gestion des messages de notification vers et depuis des serveurs FPolicy.

Dans le cadre de la gestion des connexions, FPolicy possède également les responsabilités suivantes :

- Garantit que la notification des fichiers circule via le LIF correct vers le serveur FPolicy.
- Garantit que lorsque plusieurs serveurs FPolicy sont associés à une règle, l'équilibrage de la charge est réalisé lors de l'envoi de notifications aux serveurs FPolicy.
- Tentatives de rétablissement de la connexion en cas de panne de la connexion à un serveur FPolicy.
- Envoie les notifications aux serveurs FPolicy par le biais d'une session authentifiée.
- Gère la connexion de données de type passthrough établie par le serveur FPolicy pour le traitement des requêtes client lorsque la lecture-passe est activée.

Mode d'utilisation des canaux de contrôle pour les communications FPolicy

FPolicy initie une connexion du canal de contrôle à un serveur FPolicy externe à partir des LIFs de données de chaque nœud participant sur un SVM (Storage Virtual machine). FPolicy utilise des canaux de contrôle pour la transmission des notifications de fichiers. Par conséquent, un serveur FPolicy peut voir plusieurs connexions de canaux de contrôle basées sur la topologie SVM.

Utilisation des canaux privilégiés d'accès aux données pour la communication synchrone

Dans le cas d'une utilisation synchrone, le serveur FPolicy accède aux données résidant sur la machine virtuelle de stockage (SVM) via un chemin d'accès privilégié aux données. L'accès via le chemin privilégié expose l'ensemble du système de fichiers au serveur FPolicy. Elle peut accéder aux fichiers de données afin de collecter des informations, de scanner des fichiers, de lire des fichiers ou d'écrire dans des fichiers.

Étant donné que le serveur FPolicy externe peut accéder à l'intégralité du système de fichiers à partir de la racine de la SVM via le canal de données privilégié, la connexion de canal de données privilégié doit être sécurisée.

Comment les identifiants de connexion FPolicy sont utilisés avec les canaux d'accès aux données privilégiés

Le serveur FPolicy établit des connexions privilégiées aux données avec les nœuds du cluster grâce à des informations d'identification Windows spécifiques enregistrées avec la configuration FPolicy. SMB est le seul protocole pris en charge pour établir une connexion de canal avec accès aux données privilégié.

Si le serveur FPolicy nécessite un accès privilégié aux données, les conditions suivantes doivent être remplies :

- Une licence SMB doit être activée sur le cluster.
- Le serveur FPolicy doit fonctionner avec les identifiants configurés dans la configuration FPolicy.

Lors de la connexion à un canal de données, FPolicy utilise les informations d'identification du nom d'utilisateur Windows spécifié. Les données sont accessibles via le partage ONTAP_ADMIN$ par l'administrateur.

L'attribution d'informations d'identification de super utilisateur pour l'accès privilégié aux données signifie

ONTAP utilise la combinaison de l'adresse IP et des identifiants de l'utilisateur configurés dans la configuration FPolicy pour attribuer les identifiants des super utilisateurs au serveur FPolicy.

Lorsque le serveur FPolicy accède aux données, l'état du super utilisateur accorde les privilèges suivants :

- Évitez les contrôles d'autorisation

  L'utilisateur évite les vérifications de l'accès aux fichiers et aux répertoires.

- Privilèges de verrouillage spéciaux

  ONTAP permet l'accès en lecture, en écriture ou en modification à n'importe quel fichier, indépendamment des verrous existants. Si le serveur FPolicy possède des verrous de plage d'octets sur le fichier, il entraîne la suppression immédiate des verrouillages existants sur ce dernier.

- Évitez les vérifications FPolicy

  L'accès ne génère aucune notification FPolicy.

Gestion du traitement des règles par FPolicy

Il peut y avoir plusieurs règles FPolicy attribuées à votre SVM (Storage Virtual machine) ; chacune avec une priorité différente. Pour créer une configuration FPolicy appropriée sur le SVM, il est important de comprendre la façon dont FPolicy gère le traitement des règles.

Chaque requête d'accès aux fichiers est initialement évaluée afin de déterminer les règles qui surveillent cet événement. S'il s'agit d'un événement surveillé, les informations relatives à l'événement surveillé et les politiques intéressées sont transmises à FPolicy où il est évalué. Chaque stratégie est évaluée par ordre de priorité attribuée.

Lors de la configuration des règles, vous devez tenir compte des recommandations suivantes :

- Lorsque vous voulez qu'une règle soit toujours évaluée avant d'autres règles, configurez-la avec une priorité plus élevée.
- Si le succès de l'opération d'accès aux fichiers demandée sur un événement contrôlé est une condition préalable à une demande de fichier évaluée par rapport à une autre stratégie, donnez à la stratégie qui contrôle le succès ou l'échec de l'opération de premier fichier une priorité plus élevée.

  Par exemple, si l'une des règles gère la fonctionnalité d'archivage et de restauration des fichiers FPolicy, et une seconde gère les opérations d'accès aux fichiers sur le fichier en ligne, la règle de gestion de la restauration des fichiers doit avoir une priorité plus élevée afin que le fichier soit restauré avant que l'opération gérée par la seconde stratégie puisse être autorisée.

- Si vous souhaitez évaluer toutes les règles pouvant s'appliquer à une opération d'accès aux fichiers, donnez une priorité inférieure aux règles synchrones.

Vous pouvez réorganiser les priorités de stratégie pour les stratégies existantes en modifiant le numéro de séquence de stratégie. Toutefois, pour que FPolicy évalue les règles en fonction de l'ordre de priorité modifié, vous devez désactiver et réactiver cette règle avec le numéro de séquence modifié.

Ce que est le processus de communication nœud à serveur FPolicy

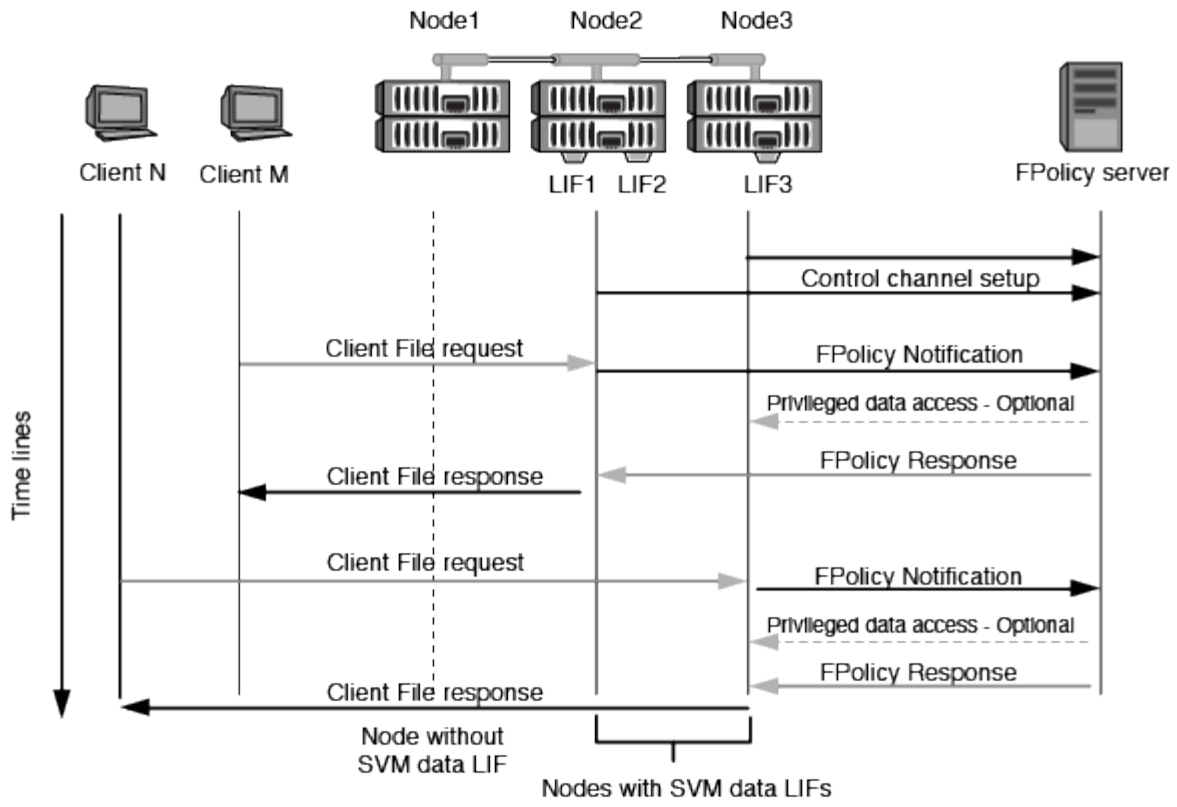
Pour planifier correctement la configuration de FPolicy, vous devez comprendre le processus de communication nœud à serveur FPolicy externe.

Chaque nœud qui participe sur chaque machine virtuelle de stockage (SVM) établit une connexion avec un serveur FPolicy externe (serveur FPolicy) à l'aide du protocole TCP/IP. Les connexions aux serveurs FPolicy sont configurées à l'aide des LIF de données du nœud. Par conséquent, un nœud participant ne peut établir une connexion que si le nœud possède une LIF de données opérationnelles pour le SVM.

Chaque processus FPolicy sur les nœuds participants tente d'établir une connexion avec le serveur FPolicy lorsque cette règle est activée. Il utilise l'adresse IP et le port du moteur externe FPolicy spécifiés dans la configuration des règles.

Cette connexion établit un canal de contrôle depuis chaque nœud participant sur chaque SVM vers le serveur FPolicy via la LIF de données. En outre, si des adresses LIF de données IPv4 et IPv6 sont présentes sur le même nœud participant, FPolicy tente d'établir des connexions pour IPv4 et IPv6. Par conséquent, dans un scénario où le SVM s'étend sur plusieurs nœuds ou si des adresses IPv4 et IPv6 sont présentes, le serveur FPolicy doit être prêt à traiter plusieurs requêtes de configuration de canal de contrôle provenant du cluster après l'activation de la politique FPolicy sur le SVM.

Par exemple, si un cluster possède trois nœuds—Node1, Node2 et nœud3- ainsi que les LIF de données du SVM se répartissent uniquement sur Node2 et nœud3, les canaux de contrôle sont lancés uniquement sur le nœud2 et celui du nœud3, indépendamment de la répartition des volumes de données. Supposons que Node2 possède deux LIF de données—LIF1 et LIF2—qui appartiennent à la SVM et que la connexion initiale est de LIF1. En cas d'échec de LIF1, FPolicy tente d'établir un canal de contrôle à partir de LIF2.



Comment FPolicy gère la communication externe lors de la migration ou du basculement de LIF

Les LIFs de données peuvent être migrées sur des ports data qui se trouvent sur le même nœud ou vers des ports data sur un nœud distant.

Lorsqu'une LIF de données subit une panne ou est migrée, une nouvelle connexion de canal de contrôle est établie vers le serveur FPolicy. FPolicy peut ensuite réessayer les requêtes des clients SMB et NFS ayant dépassé le délai d'attente. En conséquence, de nouvelles notifications sont envoyées aux serveurs FPolicy externes. Le nœud rejette les réponses du serveur FPolicy aux requêtes SMB et NFS d'origine avec temporisation.

Comment FPolicy gère la communication externe lors du basculement de nœud

Si le nœud de cluster qui héberge les ports de données utilisés pour la communication FPolicy tombe en panne, ONTAP interrompt la connexion entre le serveur FPolicy et le nœud.

Vous pouvez atténuer l'impact du basculement de cluster sur le serveur FPolicy en configurant la règle de basculement pour migrer le port de données utilisé dans la communication FPolicy vers un autre nœud actif. Une fois la migration terminée, une nouvelle connexion est établie à l'aide du nouveau port de données.

Si la règle de basculement n'est pas configurée pour migrer le port de données, le serveur FPolicy doit attendre l'apparition du nœud défaillant. Une fois le nœud activé, une nouvelle connexion est lancée à partir de ce nœud avec un nouvel ID de session.

> Le serveur FPolicy détecte les connexions interrompues avec le message du protocole de maintien de la disponibilité. Le délai d'expiration pour la purge de l'ID de session est déterminé lors de la configuration de FPolicy. Le délai de mise en veille par défaut est de deux minutes.

Fonctionnement des services FPolicy sur les espaces de noms des SVM

ONTAP offre un espace de noms de machine virtuelle de stockage unifié. Les volumes du cluster sont regroupés par des jonctions pour fournir un système de fichiers unique et logique. Le serveur FPolicy connaît la topologie de l'espace de noms et fournit des services FPolicy à l'échelle de l'espace de noms.

Le namespace est spécifique et contenu au sein du SVM ; par conséquent, vous pouvez voir le namespace uniquement depuis le contexte SVM. Les espaces de noms présentent les caractéristiques suivantes :

- Un nom d'espace unique existe dans chaque SVM, la racine de l'espace de noms étant le volume root, représenté dans le namespace par la barre oblique (/).
- Tous les autres volumes ont des points de jonction sous la racine (/).
- Les jonctions des volumes sont transparentes pour les clients.
- Une exportation NFS unique peut donner accès à l'espace de noms complet, sinon les export policy peuvent exporter des volumes spécifiques.
- Les partages SMB peuvent être créés sur le volume, dans des qtrees au sein du volume, ou sur n'importe quel répertoire dans le namespace.
- L'architecture d'espace de noms est flexible.

  Voici quelques exemples d'architectures d'espaces de noms classiques :

  - Un espace de noms avec une seule branche à la racine
  - Un espace de noms avec plusieurs branches à la racine
  - Un namespace avec plusieurs volumes non ramifiés en dehors de la racine

La fonctionnalité de gestion du stockage hiérarchique de FPolicy permet d'améliorer la facilité d'utilisation de la gestion hiérarchique du stockage

La fonctionnalité Passthrough Read permet au serveur FPolicy (fonctionnant comme serveur HSM (gestion hiérarchique du stockage)) de fournir un accès en lecture aux fichiers hors ligne sans avoir à rappeler le fichier du système de stockage secondaire au système de stockage primaire.

Lorsqu'un serveur FPolicy est configuré pour fournir HSM les fichiers stockés sur un serveur SMB, la migration de fichiers basée sur des règles se produit lorsque les fichiers sont stockés hors ligne sur le stockage secondaire et qu'un seul fichier stub reste sur le stockage primaire. Même si un fichier stub apparaît comme un fichier normal pour les clients, il s'agit en fait d'un fichier parse de la même taille que le fichier d'origine. Le fichier sparse a le jeu de bits hors ligne SMB et pointe vers le fichier réel qui a été migré vers le stockage secondaire.

En général, lorsqu'une demande de lecture pour un fichier hors ligne est reçue, le contenu demandé doit être rappelé dans le stockage principal, puis accessible par le biais du stockage principal. Le besoin de rappeler des données dans le stockage primaire a plusieurs effets indésirables. L'augmentation de la latence aux demandes des clients, due à la nécessité de rappeler le contenu avant de répondre à la demande et l'augmentation de la consommation d'espace nécessaire pour les fichiers rappelés sur l'infrastructure de stockage primaire, soit un effet indésirable.

La fonctionnalité de passerelle FPolicy permet au serveur HSM (serveur FPolicy) de fournir un accès en lecture aux fichiers migrés hors ligne sans avoir à rappeler le fichier du système de stockage secondaire au

système de stockage primaire. Au lieu de rappeler les fichiers dans le stockage primaire, les demandes de lecture peuvent être traitées directement depuis le système de stockage secondaire.

> La fonction de déchargement des copies (ODX) n'est pas prise en charge par l'opération de lecture intermédiaire FPolicy.

La fonctionnalité Passthrough Read améliore la convivialité en offrant les avantages suivants :

- Les demandes de lecture peuvent être traitées même si l'espace de stockage primaire n'est pas suffisant pour récupérer les données demandées dans le stockage primaire.
- Meilleure gestion de la capacité et des performances lorsqu'une poussée de récupération des données peut se produire, par exemple si un script ou une solution de sauvegarde doit accéder à de nombreux fichiers hors ligne.
- Les demandes de lecture de fichiers hors ligne des copies Snapshot peuvent être traitées.

  Étant donné que les copies Snapshot sont en lecture seule, le serveur FPolicy ne peut pas restaurer le fichier d'origine si le fichier stub est situé dans une copie Snapshot. L'utilisation de la lecture passthrough élimine ce problème.

- Des règles peuvent être définies pour définir ce contrôle lorsque les demandes de lecture sont traitées par l'accès au fichier sur le système de stockage secondaire et lorsqu'un fichier hors ligne doit être rappelé sur le système de stockage principal.

  Par exemple, il est possible de créer une règle sur le serveur HSM qui spécifie le nombre d'accès au fichier hors ligne pendant une période donnée avant que le fichier ne soit remigré vers le stockage principal. Ce type de stratégie évite de rappeler les fichiers rarement utilisés.

Mode de gestion des requêtes de lecture lors de l'activation du mode de gestion FPolicy

Vous devez comprendre comment les requêtes de lecture sont gérées lorsque le mode de lecture intermédiaire FPolicy est activé afin de pouvoir configurer de manière optimale la connectivité entre le SVM et les serveurs FPolicy.

Lorsque la fonction de lecture intermédiaire FPolicy est activée et que le SVM reçoit une demande de fichier hors ligne, FPolicy envoie une notification au serveur FPolicy (serveur HSM) par l'intermédiaire du canal de connexion standard.

Après avoir reçu la notification, le serveur FPolicy lit les données du chemin de fichier envoyé dans la notification et envoie les données demandées à la SVM via la connexion de données privilégiée par lecture-intermédiaire établie entre le SVM et le serveur FPolicy.

Une fois les données envoyées, le serveur FPolicy répond à la demande de lecture comme ALLOW ou DENY. En fonction de l'autorisation ou du refus de la demande de lecture, ONTAP envoie les informations demandées ou envoie un message d'erreur au client.

Planification de la configuration FPolicy

D'exigences, de considérations et de meilleures pratiques pour la configuration de FPolicy

Avant de créer et de configurer des configurations FPolicy sur vos SVM, vous devez connaître certaines exigences, considérations et meilleures pratiques relatives à la configuration de FPolicy.

Les fonctionnalités FPolicy sont configurées soit via l'interface de ligne de commandes soit via l'API REST.

Conditions requises pour la configuration de FPolicy

Avant de configurer et d'activer FPolicy sur votre machine virtuelle de stockage (SVM), vous devez connaître certaines exigences.

- Tous les nœuds du cluster doivent exécuter une version de ONTAP qui prend en charge FPolicy.
- Si vous n'utilisez pas le moteur FPolicy natif ONTAP, vous devez installer des serveurs FPolicy externes (serveurs FPolicy).
- Les serveurs FPolicy doivent être installés sur un serveur accessible depuis les LIFs de données du SVM sur lequel les règles FPolicy sont activées.

> Depuis ONTAP 9.8, ONTAP fournit un service LIF client pour les connexions FPolicy sortantes avec l'ajout du `data-fpolicy-client` services. "En savoir plus sur les LIF et les règles de service".

- L'adresse IP du serveur FPolicy doit être configurée en tant que serveur principal ou secondaire dans la configuration du moteur externe de la politique FPolicy.
- Si les serveurs FPolicy accèdent aux données sur un canal de données privilégié, les exigences supplémentaires suivantes doivent être respectées :
  - SMB doit être sous licence sur le cluster.

    Un accès privilégié aux données se fait à l'aide de connexions SMB.
  - Les informations d'identification utilisateur doivent être configurées pour accéder aux fichiers via le canal de données privilégié.
  - Le serveur FPolicy doit fonctionner avec les identifiants configurés dans la configuration FPolicy.
  - Toutes les LIFs de données utilisées pour communiquer avec les serveurs FPolicy doivent être configurées de sorte à avoir `cifs` comme l'un des protocoles autorisés.

    Cela inclut les LIFs utilisées pour les connexions passthrough-read.
- À partir de ONTAP 9.14.1, FPolicy permet de configurer un magasin persistant pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

Meilleures pratiques et recommandations lors de la configuration de FPolicy

Lors de la configuration de FPolicy sur des machines virtuelles de stockage (SVM), familiarisez-vous avec les bonnes pratiques et recommandations générales de configuration pour garantir que votre configuration FPolicy offre des performances de contrôle fiables et des résultats qui répondent à vos besoins.

Pour obtenir des instructions spécifiques relatives aux performances, au dimensionnement et à la configuration, utilisez votre application partenaire FPolicy.

Configuration des règles

La configuration du moteur externe FPolicy, les événements et l'étendue des SVM peuvent améliorer votre expérience et votre sécurité globale.

- Configuration du moteur externe FPolicy pour les SVM :
  - Le renforcement de la sécurité implique des coûts de performance. L'activation de la communication SSL (Secure Sockets Layer) a un effet sur les performances lors de l'accès aux partages.
  - Le moteur externe FPolicy doit être configuré avec plusieurs serveurs FPolicy de manière à fournir la résilience et la haute disponibilité du traitement des notifications du serveur FPolicy.
- Configuration des événements FPolicy pour les SVM :

  La surveillance des opérations de fichiers influence votre expérience globale. Par exemple, le filtrage des opérations de fichiers indésirables côté stockage améliore votre expérience. NetApp recommande de configurer les éléments suivants :

  - Surveillance des types minimaux d'opérations de fichiers et activation du nombre maximal de filtres sans rompre le cas d'utilisation.
  - Utilisation de filtres pour les opérations getattr, lecture, écriture, ouverture et fermeture. La part des environnements de home Directory SMB et NFS est élevée.
- Configuration du périmètre FPolicy pour les SVM :

  Limitez l'étendue des règles aux objets de stockage concernés, tels que les partages, les volumes et les exportations, au lieu de les activer sur l'ensemble du SVM. NetApp recommande de vérifier les extensions de répertoire. Si le `is-file-extension-check-on-directories-enabled` le paramètre est défini sur `true`, les objets de répertoire sont soumis aux mêmes vérifications d'extension que les fichiers ordinaires.

Configuration du réseau

La connectivité réseau entre le serveur FPolicy et le contrôleur doit présenter une faible latence. NetApp recommande de séparer le trafic FPolicy du trafic client en utilisant un réseau privé.

De plus, vous devez placer des serveurs externes FPolicy (serveurs FPolicy) à proximité immédiate du cluster avec une connectivité à large bande passante afin d'obtenir une latence minimale et une connectivité à large bande passante.

> Si la LIF du trafic FPolicy est configurée sur un port différent de la LIF pour le trafic client, la LIF FPolicy peut basculer vers l'autre nœud en raison d'une défaillance de port. Par conséquent, le serveur FPolicy devient inaccessible depuis le nœud ce qui provoque l'échec des notifications FPolicy pour les opérations de fichier sur le nœud. Pour éviter ce problème, vérifiez que le serveur FPolicy peut être accessible via au moins une LIF du nœud afin de traiter les requêtes FPolicy pour les opérations de fichiers effectuées sur ce nœud.

Configuration matérielle

Vous pouvez avoir le serveur FPolicy sur un serveur physique ou virtuel. Si le serveur FPolicy se trouve dans un environnement virtuel, vous devez allouer des ressources dédiées (CPU, réseau et mémoire) au serveur virtuel.

Le taux nœud/serveur FPolicy du cluster doit être optimisé pour s'assurer que les serveurs FPolicy ne sont pas surchargés et peuvent introduire des latences lorsque le SVM répond aux demandes du client. Le ratio optimal dépend de l'application partenaire pour laquelle le serveur FPolicy est utilisé. NetApp recommande de faire équipe avec ses partenaires pour déterminer la valeur appropriée.

Configuration à règles multiples

La règle FPolicy pour le blocage natif a la priorité la plus élevée, quel que soit le numéro de séquence, et les règles qui modifient la décision ont une priorité plus élevée que les autres. La priorité de la règle dépend de l'utilisation. NetApp recommande de faire équipe avec ses partenaires pour déterminer la priorité appropriée.

Considérations de taille

FPolicy effectue un contrôle en ligne des opérations SMB et NFS, envoie des notifications au serveur externe et attend une réponse, selon le mode de communication externe du moteur (synchrone ou asynchrone). Ce processus affecte les performances des accès SMB et NFS ainsi que des ressources CPU.

Pour résoudre tout problème, NetApp recommande de travailler avec ses partenaires pour évaluer et dimensionner l'environnement avant d'activer FPolicy. Les performances sont affectées par plusieurs facteurs, notamment le nombre d'utilisateurs, les caractéristiques de la charge de travail, tels que les opérations par utilisateur et la taille des données, la latence du réseau et les défaillances ou la lenteur du serveur.

Contrôle des performances

FPolicy est un système basé sur les notifications. Les notifications sont envoyées à un serveur externe pour traitement et pour générer une réponse à ONTAP. Ce processus aller-retour augmente la latence pour l'accès client.

La surveillance des compteurs de performances sur le serveur FPolicy et dans ONTAP vous permet d'identifier les goulets d'étranglement dans la solution et de configurer les paramètres nécessaires pour une solution optimale. Par exemple, une augmentation de la latence FPolicy a un effet en cascade sur la latence d'accès SMB et NFS. Par conséquent, vous devez contrôler à la fois la charge de travail (SMB et NFS) et la latence FPolicy. En outre, vous pouvez utiliser des règles de qualité de service dans ONTAP pour configurer une charge de travail pour chaque volume ou SVM activé pour FPolicy.

NetApp recommande d'exécuter `statistics show –object workload` commande permettant d'afficher les statistiques des charges de travail. De plus, vous devez surveiller les paramètres suivants :

- Latences moyennes, en lecture et en écriture
- Nombre total d'opérations
- Compteurs de lecture et d'écriture

Vous pouvez contrôler les performances des sous-systèmes FPolicy à l'aide des compteurs FPolicy suivants.

> Vous devez être en mode diagnostic pour collecter les statistiques relatives à FPolicy.

Étapes

1. Collectez les compteurs FPolicy :
   a. `statistics start -object fpolicy -instance` *`instance_name`* `-sample-id` *`ID`*
   b. `statistics start -object fpolicy_policy -instance` *`instance_name`* `-sample-id` *`ID`*
2. Afficher les compteurs FPolicy :
   a. `statistics show -object fpolicy –instance` *`instance_name`* `-sample-id` *`ID`*
   b. `statistics show -object fpolicy_server –instance` *`instance_name`* `-sample-id` *`ID`*

Le `fpolicy` et `fpolicy_server` les compteurs fournissent des informations sur plusieurs paramètres de performances décrits dans le tableau suivant.

Compteurs	Description
• compteurs « fpolicy »*	demandes_abandonnées
Nombre de demandes d'écran pour lesquelles le traitement est abandonné sur le SVM	nombre_événements
Liste des événements entraînant une notification	latence_demande_max
Latence maximale des demandes d'écran	demandes_en_attente
Nombre total de demandes d'écran en cours de traitement	requêtes_traitées
Nombre total de requêtes d'écran effectuées via le traitement fpolicy sur la SVM	liste_latence_de_la_demande
Histogramme de latence pour les demandes d'écran	taux_envoyé_demandes
Nombre de demandes d'écran envoyées par seconde	taux_de_réception_demandes
Nombre de demandes d'écran reçues par seconde	• compteurs « fpolicy_server »*
latence_demande_max	Latence maximale pour une demande d'écran
demandes_en_attente	Nombre total de demandes d'écran en attente de réponse
latence_de_la_demande	Latence moyenne pour une demande d'écran
liste_latence_de_la_demande	Histogramme de latence pour les demandes d'écran
taux_envoyé_demande	Nombre de requêtes d'écran envoyées au serveur FPolicy par seconde
taux_de_réception_réponse	Nombre de réponses d'écran reçues du serveur FPolicy par seconde

Gérer le flux de travail FPolicy et la dépendance vis-à-vis d'autres technologies

NetApp recommande de désactiver une règle FPolicy avant d'apporter toute modification de la configuration. Par exemple, si vous souhaitez ajouter ou modifier une adresse IP dans le moteur externe configuré pour la

stratégie activé, désactivez d'abord la stratégie.

Si vous configurez FPolicy pour surveiller les volumes NetApp FlexCache, NetApp vous recommande de ne pas configurer FPolicy pour surveiller les opérations de lecture et de fichier getattr. La surveillance de ces opérations dans ONTAP nécessite la récupération des données I2P (inode-to-path). Les données I2P ne pouvant pas être récupérées à partir de volumes FlexCache, elles doivent être récupérées à partir du volume d'origine. Le contrôle de ces opérations élimine donc les avantages de performance que FlexCache peut offrir.

Lorsque FPolicy et une solution antivirus externe sont déployés, la solution antivirus reçoit d'abord les notifications. Le traitement FPolicy démarre uniquement une fois l'analyse antivirus terminée. Il est important de dimensionner correctement les solutions antivirus, car une analyse antivirus lente peut affecter les performances globales.

Considérations relatives à la mise à niveau en lecture directe et au rétablissement

Vous devez connaître certaines considérations relatives à la mise à niveau et à la restauration avant de procéder à une mise à niveau vers une version de ONTAP qui prend en charge la lecture d'un mot de passe-passe ou avant de restaurer une version qui ne prend pas en charge la lecture d'un fichier passthrough.

Mise à niveau

Une fois que tous les nœuds sont mis à niveau vers une version de ONTAP qui prend en charge le mode de lecture intermédiaire FPolicy, le cluster est capable d'utiliser la fonctionnalité de lecture intermédiaire. Cependant, la lecture du mot de passe est désactivée par défaut sur les configurations FPolicy existantes. Pour utiliser la lecture passerelle sur les configurations FPolicy existantes, vous devez désactiver la règle FPolicy et modifier la configuration, puis réactiver la configuration.

Rétablissement

Avant de revenir à une version de ONTAP qui ne prend pas en charge la lecture passthrough FPolicy, vous devez remplir les conditions suivantes :

- Désactivez toutes les stratégies à l'aide de passthrough-read, puis modifiez les configurations affectées pour qu'elles n'utilisent pas passthrough-read.
- Désactivez la fonctionnalité FPolicy sur le cluster en désactivant chaque politique FPolicy sur le cluster.

Avant de revenir à une version de ONTAP qui ne prend pas en charge les magasins persistants, assurez-vous qu'aucune des stratégies Fpolicy ne dispose d'un magasin persistant configuré. Si un magasin persistant est configuré, la restauration échouera.

Quelles sont les étapes de configuration d'une configuration FPolicy

Avant de pouvoir surveiller l'accès aux fichiers, FPolicy doit être créé et activé sur la machine virtuelle de stockage (SVM) pour laquelle les services FPolicy sont requis.

Les étapes de configuration et d'activation d'une configuration FPolicy sur le SVM sont les suivantes :

1. Créer un moteur externe FPolicy.

   Le moteur externe FPolicy identifie les serveurs FPolicy externes associés à une configuration FPolicy spécifique. Si le moteur interne FPolicy « natif » est utilisé pour créer une configuration native de blocage de fichiers, il n'est pas nécessaire de créer un moteur externe FPolicy.

2. Créez un événement FPolicy.

Un événement FPolicy décrit ce que la règle FPolicy doit surveiller. Les événements consistent en des protocoles et des opérations de fichiers à surveiller et peuvent contenir une liste de filtres. Les événements utilisent des filtres pour restreindre la liste des événements surveillés pour lesquels le moteur externe FPolicy doit envoyer des notifications. Les événements spécifient également si la règle surveille les opérations de volume.

3. Créez une règle FPolicy.

   Il incombe à la politique FPolicy d'associer, au périmètre approprié, l'ensemble des événements à surveiller et pour lesquels des notifications d'événements surveillés doivent être envoyées au serveur FPolicy désigné (ou au moteur natif si aucun serveur FPolicy n'est configuré). Cette politique définit également si le serveur FPolicy possède des droits d'accès privilégiés aux données pour lesquelles il reçoit des notifications. Un serveur FPolicy a besoin d'un accès privilégié si le serveur doit accéder aux données. Les cas d'utilisation classiques où un accès privilégié est nécessaire comprennent le blocage de fichiers, la gestion des quotas et la gestion hiérarchique du stockage. C'est l'endroit où vous spécifiez si la configuration de cette règle utilise un serveur FPolicy ou le serveur FPolicy interne « natif ».

   Une stratégie spécifie si le filtrage est obligatoire. Si le filtrage est obligatoire et que tous les serveurs FPolicy sont en panne ou qu'aucune réponse n'est reçue des serveurs FPolicy dans une période de temporisation définie, l'accès aux fichiers est refusé.

   Les limites d'une politique sont le SVM. Une politique ne peut s'appliquer à plusieurs SVM. Cependant, un SVM spécifique peut avoir plusieurs règles FPolicy, avec chacune des combinaisons de périmètre, d'événements et de configurations de serveur externes mêmes ou différentes.

4. Configuration de la portée de la règle

   Le périmètre FPolicy détermine quels volumes, partages ou règles d'exportation agissent ou excluent par la surveillance. L'étendue détermine également quelles extensions de fichier doivent être incluses ou exclues de la surveillance FPolicy.

   > Les listes d'exclusion ont priorité sur les listes d'inclusion.

5. Activez la règle FPolicy.

   Lorsque la stratégie est activée, les canaux de contrôle et, éventuellement, les canaux de données privilégiés sont connectés. Le processus FPolicy dédié aux nœuds sur lesquels le SVM participe à la surveillance de l'accès aux fichiers et aux dossiers. Pour les événements correspondant aux critères configurés, il envoie des notifications aux serveurs FPolicy (ou au moteur natif si aucun serveur FPolicy n'est configuré).

> Si la stratégie utilise un blocage de fichiers natif, un moteur externe n'est pas configuré ou associé à la stratégie.

Planification de la configuration du moteur externe FPolicy

Planification de la configuration du moteur externe FPolicy

Avant de configurer le moteur externe FPolicy (moteur externe), vous devez comprendre les conséquences de cette opération pour créer un moteur externe et les paramètres de configuration disponibles. Ces informations vous aident à déterminer les valeurs à définir pour chaque paramètre.

Informations définies lors de la création du moteur externe FPolicy

La configuration du moteur externe définit les informations dont FPolicy a besoin pour établir et gérer les connexions avec les serveurs FPolicy externes (serveurs FPolicy), notamment les informations suivantes :

- Nom du SVM
- Nom du moteur
- Les adresses IP des serveurs FPolicy principaux et secondaires et le numéro de port TCP à utiliser lors de la connexion aux serveurs FPolicy
- Indique si le type de moteur est asynchrone ou synchrone
- Authentification de la connexion entre le nœud et le serveur FPolicy

  Si vous choisissez de configurer l'authentification SSL mutuelle, vous devez également configurer les paramètres qui fournissent les informations de certificat SSL.

- Comment gérer la connexion à l'aide de divers paramètres de privilèges avancés

  Cela inclut des paramètres qui définissent des éléments tels que les valeurs de temporisation, les valeurs de relance, les valeurs de maintien de la vie, les valeurs maximales de demande, les valeurs de taille de tampon de réception et d'envoi, ainsi que les valeurs de temporisation de la session.

Le `vserver fpolicy policy external-engine create` Permet de créer un moteur externe FPolicy.

Quels sont les paramètres externes de base du moteur

Pour planifier la configuration, vous pouvez utiliser le tableau suivant des paramètres de configuration de base de FPolicy :

Type d'information	Option
SVM Spécifie le nom du SVM que vous souhaitez associer à ce moteur externe. Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.	`-vserver vserver_name`

Nom du moteur Spécifie le nom à attribuer à la configuration du moteur externe. Vous devez spécifier le nom du moteur externe ultérieurement lors de la création de la règle FPolicy. Ceci associe le moteur externe à la politique. Le nom peut comporter jusqu'à 256 caractères. Le nom doit comporter jusqu'à 200 caractères si vous configurez le nom du moteur externe dans une configuration de reprise après incident de MetroCluster ou de SVM. Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants : • `a` à `z` • `A` à `Z` • `0` à `9` • «»_», «»-", and ".»	`-engine-name engine_name`
Serveurs FPolicy primaires Spécifie les serveurs FPolicy principaux vers lesquels le nœud envoie des notifications pour une règle FPolicy donnée. La valeur est indiquée comme une liste d'adresses IP délimitée par des virgules. Si plusieurs adresses IP de serveur principal sont spécifiées, chaque nœud sur lequel le SVM participe crée une connexion de contrôle à chaque serveur FPolicy principal spécifié au moment de l'activation de la règle. Si vous configurez plusieurs serveurs FPolicy principaux, des notifications sont envoyées selon une séquence périodique aux serveurs FPolicy. Si le moteur externe est utilisé dans une configuration de reprise sur incident de MetroCluster ou de SVM, indiquez les adresses IP des serveurs FPolicy du site source en tant que serveurs principaux. Les adresses IP des serveurs FPolicy du site de destination doivent être spécifiées en tant que serveurs secondaires.	`-primary-servers IP_address,...`
Numéro de port Spécifie le numéro de port du service FPolicy.	`-port integer`

Serveurs FPolicy secondaires Spécifie les serveurs FPolicy secondaires vers lesquels envoyer les événements d'accès aux fichiers pour une politique FPolicy donnée. La valeur est indiquée comme une liste d'adresses IP délimitée par des virgules. Les serveurs secondaires sont utilisés uniquement lorsqu'aucun des serveurs primaires n'est accessible. Les connexions aux serveurs secondaires sont établies lorsque la stratégie est activée, mais les notifications sont envoyées aux serveurs secondaires uniquement si aucun des serveurs primaires n'est accessible. Si vous configurez plusieurs serveurs secondaires, des notifications sont envoyées aux serveurs FPolicy de manière périodique.	`-secondary-servers IP_address,...`
Type de moteur externe Indique si le moteur externe fonctionne en mode synchrone ou asynchrone. Par défaut, FPolicy fonctionne en mode synchrone. Lorsqu'il est réglé sur `synchronous`, Le traitement des requêtes de fichier envoie une notification au serveur FPolicy, mais ne se poursuit qu'après avoir reçu une réponse du serveur FPolicy. À ce stade, le flux de demande continue ou le traitement génère un déni, selon que la réponse du serveur FPolicy permet l'action demandée. Lorsqu'il est réglé sur `asynchronous`, Le traitement des requêtes de fichier envoie une notification au serveur FPolicy, puis continue.	`-extern-engine-type external_engine_type` La valeur de ce paramètre peut être l'une des suivantes : • `synchronous` • `asynchronous`
Option *SSL pour la communication avec le serveur FPolicy* Spécifie l'option SSL pour la communication avec le serveur FPolicy. Ce paramètre est obligatoire. Vous pouvez choisir l'une des options en fonction des informations suivantes : • Lorsqu'il est réglé sur `no-auth`, aucune authentification n'a lieu. La liaison de communication est établie sur TCP. • Lorsqu'il est réglé sur `server-auth`, Le SVM authentifie le serveur FPolicy à l'aide de l'authentification du serveur SSL. • Lorsqu'il est réglé sur `mutual-auth`, L'authentification mutuelle a lieu entre le SVM et le serveur FPolicy ; le SVM authentifie le serveur FPolicy et le serveur FPolicy authentifie le SVM. Si vous choisissez de configurer l'authentification SSL mutuelle, vous devez également configurer l' `-certificate-common-name`, `-certificate-serial`, et `-certifcate-ca` paramètres.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}

FQDN du certificat ou nom commun personnalisé Spécifie le nom du certificat utilisé si l'authentification SSL entre le SVM et le serveur FPolicy est configurée. Vous pouvez spécifier le nom du certificat en tant que FQDN ou en tant que nom commun personnalisé. Si vous spécifiez `mutual-auth` pour le `-ssl-option` paramètre, vous devez spécifier une valeur pour le `-certificate-common-name` paramètre.	`-certificate-common-name` `text`
Numéro de série du certificat Spécifie le numéro de série du certificat utilisé pour l'authentification si l'authentification SSL entre le SVM et le serveur FPolicy est configurée. Si vous spécifiez `mutual-auth` pour le `-ssl-option` paramètre, vous devez spécifier une valeur pour le `-certificate-serial` paramètre.	`-certificate-serial` `text`
Autorité de certification Spécifie le nom de l'autorité de certification du certificat utilisé pour l'authentification si l'authentification SSL entre le SVM et le serveur FPolicy est configurée. Si vous spécifiez `mutual-auth` pour le `-ssl-option` paramètre, vous devez spécifier une valeur pour le `-certificate-ca` paramètre.	`-certificate-ca` `text`

Quelles sont les options avancées du moteur externe

Vous pouvez utiliser le tableau suivant des paramètres de configuration avancée FPolicy pour personnaliser ou non votre configuration avec des paramètres avancés. Ces paramètres permettent de modifier le comportement de communication entre les nœuds du cluster et les serveurs FPolicy :

Type d'information	Option

Délai d'annulation d'une demande Spécifie l'intervalle de temps en heures (`h`), minutes (`m`), ou secondes (`s`) Que le nœud attend une réponse du serveur FPolicy. Si l'intervalle de temporisation passe, le nœud envoie une requête d'annulation au serveur FPolicy. Le nœud envoie ensuite la notification à un autre serveur FPolicy. Ce délai aide à gérer un serveur FPolicy qui ne répond pas, ce qui peut améliorer la réponse des clients SMB/NFS. Par ailleurs, l'annulation des demandes après une période de temporisation peut faciliter la libération des ressources système, car la demande de notification est déplacée d'un serveur FPolicy défaillant/défectueux vers un autre serveur FPolicy. La plage de cette valeur est de `0` à `100`. Si la valeur est définie sur `0`, L'option est désactivée et les messages de requête d'annulation ne sont pas envoyés au serveur FPolicy. La valeur par défaut est `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Délai d'attente pour l'abandon d'une demande Spécifie le délai d'expiration en heures (`h`), minutes (`m`), ou secondes (`s`) pour l'abandon d'une demande. La plage de cette valeur est de `0` à `200`.	`-reqs-abort-timeout` ` `integer`[h
m	s]
Intervalle pour l'envoi de demandes d'état Spécifie l'intervalle en heures (`h`), minutes (`m`), ou secondes (`s`) Après quoi une requête d'état est envoyée au serveur FPolicy. La plage de cette valeur est de `0` à `50`. Si la valeur est définie sur `0`, L'option est désactivée et les messages de requête d'état ne sont pas envoyés au serveur FPolicy. La valeur par défaut est `10s`.	`-status-req-interval integer`[h
m	s]
Nombre maximal de requêtes en attente sur le serveur FPolicy Spécifie le nombre maximal de requêtes en attente pouvant être mises en file d'attente sur le serveur FPolicy. La plage de cette valeur est de `1` à `10000`. La valeur par défaut est `500`.	`-max-server-reqs integer`

Timeout pour la déconnexion d'un serveur FPolicy non réactif Spécifie l'intervalle de temps en heures (`h`), minutes (`m`), ou secondes (`s`) Après quoi la connexion au serveur FPolicy est interrompue. La connexion est interrompue après le délai d'expiration uniquement si la file d'attente du serveur FPolicy contient le nombre maximal de requêtes autorisées et qu'aucune réponse n'est reçue dans le délai d'expiration. Le nombre maximal de demandes est de `50` (valeur par défaut) ou le numéro spécifié par le `max-server-reqs-` paramètre. La plage de cette valeur est de `1` à `100`. La valeur par défaut est `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervalle d'envoi de messages de maintien de la disponibilité au serveur FPolicy Spécifie l'intervalle de temps en heures (`h`), minutes (`m`), ou secondes (`s`) À laquelle les messages de maintien de la disponibilité sont envoyés au serveur FPolicy. Les messages de maintien de la vie détectent les connexions à demi-ouverture. La plage de cette valeur est de `10` à `600`. Si la valeur est définie sur `0`, L'option est désactivée et les messages de maintien en service ne peuvent pas être envoyés aux serveurs FPolicy. La valeur par défaut est `120s`.	`-keep-alive-interval-integer`[h
m	s]
Tentatives de reconnexion maximales Spécifie le nombre maximal de fois que le SVM tente de se reconnecter au serveur FPolicy une fois la connexion interrompue. La plage de cette valeur est de `0` à `20`. La valeur par défaut est `5`.	`-max-connection-retries integer`
Taille du tampon de réception Spécifie la taille du tampon de réception du socket connecté pour le serveur FPolicy. La valeur par défaut est 256 kilo-octets (Ko). Lorsque la valeur est définie sur 0, la taille du tampon de réception est définie sur une valeur définie par le système. Par exemple, si la taille par défaut de la mémoire tampon de réception du socket est de 65536 octets, en définissant la valeur ajustable sur 0, la taille de la mémoire tampon de socket est définie sur 65536 octets. Vous pouvez utiliser n'importe quelle valeur autre que celle par défaut pour définir la taille (en octets) du tampon de réception.	`-recv-buffer-size integer`

Envoyer la taille du tampon Spécifie la taille du tampon d'envoi du socket connecté pour le serveur FPolicy. La valeur par défaut est 256 kilo-octets (Ko). Lorsque la valeur est définie sur 0, la taille du tampon d'envoi est définie sur une valeur définie par le système. Par exemple, si la taille par défaut du tampon d'envoi du socket est définie sur 65536 octets, en définissant la valeur ajustable sur 0, la taille de la mémoire tampon du socket est définie sur 65536 octets. Vous pouvez utiliser n'importe quelle valeur autre que celle par défaut pour définir la taille (en octets) du tampon d'envoi.	`-send-buffer-size integer`
Délai de purge d'un ID de session pendant la reconnexion Spécifie l'intervalle en heures (`h`), minutes (`m`), ou secondes (`s`) Après quoi un nouvel ID de session est envoyé au serveur FPolicy pendant les tentatives de reconnexion. Si la connexion entre le contrôleur de stockage et le serveur FPolicy est interrompue et la reconnexion est effectuée au sein du `-session -timeout` Intervalle, l'ancien ID de session est envoyé au serveur FPolicy pour qu'il puisse envoyer les réponses aux anciennes notifications. La valeur par défaut est définie sur 10 secondes.	`-session-timeout` [`integer`h][`integer`m][`integer`s]

Informations supplémentaires sur la configuration des moteurs externes FPolicy pour utiliser les connexions authentifiées SSL

Vous devez connaître des informations supplémentaires pour configurer le moteur externe FPolicy de façon à utiliser le protocole SSL lors de la connexion aux serveurs FPolicy.

Authentification de serveur SSL

Si vous choisissez de configurer le moteur externe FPolicy pour l'authentification du serveur SSL, vous devez installer le certificat public de l'autorité de certification (CA) qui a signé le certificat du serveur FPolicy avant de créer le moteur externe.

Authentification mutuelle

Si vous configurez les moteurs externes FPolicy pour utiliser l'authentification mutuelle SSL lors du raccordement des LIF de données des machines virtuelles de stockage aux serveurs FPolicy externes, avant de créer le moteur externe, Vous devez installer le certificat public de l'autorité de certification qui a signé le certificat du serveur FPolicy avec le certificat public et le fichier de clé pour l'authentification de la SVM. Vous ne devez pas supprimer ce certificat lorsque des règles FPolicy utilisent le certificat installé.

Si le certificat est supprimé pendant que FPolicy l'utilise pour l'authentification mutuelle lors de la connexion à un serveur FPolicy externe, vous ne pouvez pas réactiver une règle FPolicy désactivée qui utilise ce certificat. La politique FPolicy ne peut pas être réactivée dans ce cas, même si un nouveau certificat avec les mêmes paramètres est créé et installé sur le SVM.

Si le certificat a été supprimé, vous devez installer un nouveau certificat, créer de nouveaux moteurs externes FPolicy utilisant le nouveau certificat et associer les nouveaux moteurs externes à la politique FPolicy que vous souhaitez réactiver en modifiant la règle FPolicy.

Installer les certificats pour SSL

Le certificat public de l'autorité de certification utilisé pour signer le certificat du serveur FPolicy est installé à l'aide du `security certificate install` commande avec `-type` paramètre défini sur `client-ca`. La clé privée et le certificat public requis pour l'authentification de la SVM sont installés à l'aide de `security certificate install` commande avec `-type` paramètre défini sur `server`.

Les certificats ne sont pas répliqués dans les relations de SVM de reprise après incident avec une configuration sans ID-preserve

Les certificats de sécurité utilisés pour l'authentification SSL lors des connexions aux serveurs FPolicy ne répliquent pas les données vers des destinations de reprise après incident des SVM avec des configurations sans ID-preserve. Bien que la configuration du moteur externe FPolicy sur le SVM soit répliquée, les certificats de sécurité ne sont pas répliqués. Vous devez installer manuellement les certificats de sécurité sur la destination.

Lorsque vous configurez la relation de SVM Disaster Recovery, la valeur que vous sélectionnez pour le `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), tous les détails de la configuration FPolicy sont répliqués, y compris les informations du certificat de sécurité. Vous devez installer les certificats de sécurité sur la destination uniquement si vous définissez l'option sur `false` (Non-ID-preserve).

Restrictions liées aux moteurs externes FPolicy avec configurations de reprise après incident MetroCluster et SVM

Vous pouvez créer un moteur externe FPolicy à étendue du cluster en attribuant la machine virtuelle de stockage du cluster (SVM) au moteur externe. Cependant, lors de la création d'un moteur externe « cluster-scoped » dans une configuration de reprise après incident de MetroCluster ou de SVM, il existe certaines restrictions lors du choix de la méthode d'authentification utilisée par le SVM pour la communication externe avec le serveur FPolicy.

Il existe trois options d'authentification que vous pouvez choisir lors de la création de serveurs FPolicy externes : aucune authentification, authentification de serveur SSL et authentification mutuelle SSL. Bien qu'il n'y ait aucune restriction lors du choix de l'option d'authentification si le serveur FPolicy externe est affecté à un SVM de données, il existe des restrictions lors de la création d'un moteur externe FPolicy d'étendue au cluster :

Configuration	Autorisé ?
Reprise après incident de MetroCluster ou SVM et moteur externe FPolicy à étendue du cluster sans authentification (le protocole SSL n'est pas configuré)	Oui.
Reprise après incident de MetroCluster ou SVM et moteur externe FPolicy à étendue du cluster avec serveur SSL ou authentification mutuelle SSL	Non

- En cas d’existence d’un moteur externe FPolicy avec authentification SSL et que vous souhaitez créer une configuration de reprise après incident MetroCluster ou SVM, vous devez modifier ce moteur externe afin qu’il n’utilise aucune authentification ou supprimer le moteur externe avant de créer la configuration de reprise après incident MetroCluster ou SVM.
- Si la configuration de reprise après incident de MetroCluster ou SVM existe déjà, ONTAP vous empêche de créer un moteur externe FPolicy à étendue du cluster avec l’authentification SSL.

Remplir la fiche de configuration du moteur externe FPolicy

Vous pouvez utiliser cette fiche technique pour enregistrer les valeurs nécessaires lors du processus de configuration du moteur externe FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer le moteur externe.

Informations concernant la configuration de base d’un moteur externe

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration du moteur externe, puis enregistrer la valeur des paramètres que vous souhaitez inclure.

Type d’information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom du moteur	Oui.	Oui.	
Serveurs FPolicy principaux	Oui.	Oui.	
Numéro de port	Oui.	Oui.	
Serveurs FPolicy secondaires	Non		
Type de moteur externe	Non		
Option SSL pour la communication avec le serveur FPolicy externe	Oui.	Oui.	
Nom de domaine complet du certificat ou nom commun personnalisé	Non		
Numéro de série du certificat	Non		
Autorité de certification	Non		

Informations relatives aux paramètres avancés du moteur externe

Pour configurer un moteur externe avec des paramètres avancés, vous devez saisir la commande de configuration en mode Advanced Privilege.

Type d'information	Obligatoire	Inclure	Vos valeurs
Délai d'annulation d'une demande	Non		
Délai d'abandon d'une demande	Non		
Intervalle d'envoi des demandes d'état	Non		
Nombre maximal de requêtes en attente sur le serveur FPolicy	Non		
Délai de déconnexion d'un serveur FPolicy non réactif	Non		
Intervalle d'envoi de messages de sauvegarde au serveur FPolicy	Non		
Nombre maximal de tentatives de reconnexion	Non		
Taille de la mémoire tampon de réception	Non		
Taille de la mémoire tampon d'envoi	Non		
Délai de purge d'un ID de session pendant la reconnexion	Non		

Planification de la configuration des événements FPolicy

Planifier l'présentation de la configuration des événements FPolicy

Avant de configurer des événements FPolicy, vous devez comprendre ce qu'il signifie pour créer un événement FPolicy. Vous devez déterminer les protocoles à surveiller, les événements à surveiller et les filtres d'événements à utiliser. Ces informations vous aident à planifier les valeurs que vous souhaitez définir.

Ce qu'il signifie pour créer un événement FPolicy

La création de l'événement FPolicy consiste à définir les informations nécessaires au processus FPolicy pour déterminer les opérations d'accès aux fichiers à surveiller et pour lesquelles des notifications d'événements surveillés doivent être envoyées au serveur FPolicy externe. La configuration des événements FPolicy définit les informations de configuration suivantes :

- Nom de la machine virtuelle de stockage (SVM)
- Nom de l'événement
- Les protocoles à surveiller

  FPolicy peut surveiller les opérations d'accès aux fichiers SMB, NFSv3 et NFSv4.

- Quelles opérations de fichier surveiller

  Toutes les opérations de fichier ne sont pas valides pour chaque protocole.

- Les filtres de fichier à configurer

  Seules certaines combinaisons d'opérations de fichier et de filtres sont valides. Chaque protocole dispose de son propre ensemble de combinaisons prises en charge.

- Contrôler le montage et le démontage de volumes

> Il y a une dépendance avec trois des paramètres (`-protocol`, `-file-operations`, `-filters`). Les combinaisons suivantes sont valides pour les trois paramètres :
>
> - Vous pouvez spécifier le `-protocol` et `-file-operations` paramètres.
> - Vous pouvez spécifier les trois paramètres.
> - Vous ne pouvez spécifier aucun des paramètres.

Contenu de la configuration des événements FPolicy

Pour vous aider à planifier votre configuration, vous pouvez utiliser la liste suivante de paramètres de configuration des événements FPolicy disponibles :

Type d'information	Option
SVM Spécifie le nom du SVM que vous souhaitez associer à cet événement FPolicy. Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.	`-vserver vserver_name`

Nom de l'événement Spécifie le nom à attribuer à l'événement FPolicy. Lorsque vous créez la politique FPolicy, vous associez l'événement FPolicy à la règle à l'aide du nom de l'événement. Le nom peut comporter jusqu'à 256 caractères. Le nom doit comporter jusqu'à 200 caractères si vous configurez l'évènement dans une configuration de reprise d'activité de MetroCluster ou de SVM. Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants : • `a` à `z` • `A` à `Z` • `0` à `9` • « `_`, `"-", and "`.»	`-event-name event_name`
Protocole Spécifie le protocole à configurer pour l'événement FPolicy. La liste pour `-protocol` peut inclure l'une des valeurs suivantes : • `cifs` • `nfsv3` • `nfsv4` Si vous spécifiez `-protocol`, vous devez alors spécifier une valeur valide dans l' `-file-operations` paramètre. Au fur et à mesure que la version du protocole change, les valeurs valides peuvent changer.	`-protocol protocol`

Opérations_fichier Spécifie la liste des opérations sur les fichiers pour l'événement FPolicy. L'événement vérifie les opérations spécifiées dans cette liste à partir de toutes les demandes client utilisant le protocole spécifié dans `-protocol` paramètre. Vous pouvez lister une ou plusieurs opérations de fichier à l'aide d'une liste délimitée par des virgules. La liste pour `-file-operations` peut inclure une ou plusieurs des valeurs suivantes : • `close` pour les opérations de fermeture de fichier • `create` pour les opérations de création de fichier • `create-dir` pour les opérations de création de répertoire • `delete` pour les opérations de suppression de fichier • `delete_dir` pour les opérations de suppression de répertoire • `getattr` pour obtenir les opérations d'attribut • `link` pour les opérations de liaison • `lookup` pour les opérations de recherche • `open` pour les opérations d'ouverture de fichier • `read` pour les opérations de lecture de fichiers • `write` pour les opérations d'écriture de fichiers • `rename` pour les opérations de renommage de fichiers • `rename_dir` pour les opérations de renommage de répertoire • `setattr` pour les opérations de définition d'attribut • `symlink` pour les opérations de lien symbolique ⓘ Si vous spécifiez `-file-operations`, vous devez alors spécifier un protocole valide dans l' `-protocol` paramètre.	`-file-operations file_operations,...`

Filtres Spécifie la liste des filtres pour une opération de fichier donnée pour le protocole spécifié. Les valeurs dans le `-filters` paramètre utilisé pour filtrer les demandes client. La liste peut comprendre un ou plusieurs des éléments suivants : Si vous spécifiez le `-filters` paramètre, vous devez ensuite spécifier également des valeurs valides pour le `-file-operations` et `-protocol` paramètres. • `monitor-ads` option permettant de filtrer la demande client pour un autre flux de données. • `close-with-modification` option permettant de filtrer la demande client pour fermer avec modification. • `close-without-modification` option permettant de filtrer la demande client pour la fermeture sans modification. • `first-read` option permettant de filtrer la demande client pour la première lecture. • `first-write` option permettant de filtrer la demande client pour la première écriture. • `offline-bit` option permettant de filtrer la demande client pour le jeu de bits hors ligne. La configuration de ce filtre permet au serveur FPolicy de recevoir une notification uniquement lorsque des fichiers hors ligne sont utilisés. • `open-with-delete-intent` option permettant de filtrer la demande client pour ouvrir avec l'intention de suppression. La configuration de ce filtre entraîne la réception d'une notification sur le serveur FPolicy uniquement lorsqu'une tentative est effectuée pour ouvrir un fichier avec l'intention de le supprimer. Ceci est utilisé par les systèmes de fichiers lorsque `FILE_DELETE_ON_CLOSE` l'indicateur est spécifié. • `open-with-write-intent` option permettant de filtrer la demande client pour ouvrir avec une intention d'écriture. La configuration de ce filtre entraîne la réception d'une notification sur le serveur FPolicy uniquement lorsqu'une tentative est effectuée pour ouvrir un fichier avec l'intention d'y écrire un objet. • `write-with-size-change` option permettant de filtrer la demande d'écriture client avec changement de taille.	`-filters filter, ...`

Filtres suite • `setattr-with-owner-change` option permettant de filtrer les demandes setattr du client pour changer le propriétaire d'un fichier ou d'un répertoire. • `setattr-with-group-change` option permettant de filtrer les demandes setattr du client pour changer le groupe d'un fichier ou d'un répertoire. • `setattr-with-sacl-change` Option permettant de filtrer les demandes setattr du client pour changer la SACL sur un fichier ou un répertoire. Ce filtre est disponible uniquement pour les protocoles SMB et NFSv4. • `setattr-with-dacl-change` Option permettant de filtrer les demandes setattr du client pour changer le DACL sur un fichier ou un répertoire. Ce filtre est disponible uniquement pour les protocoles SMB et NFSv4. • `setattr-with-modify-time-change` option permettant de filtrer les demandes setattr du client pour modifier l'heure de modification d'un fichier ou d'un répertoire. • `setattr-with-access-time-change` option permettant de filtrer les demandes setattr du client pour modifier l'heure d'accès d'un fichier ou d'un répertoire. • `setattr-with-creation-time-change` option permettant de filtrer les demandes setattr du client pour modifier l'heure de création d'un fichier ou d'un répertoire. Cette option n'est disponible que pour le protocole SMB. • `setattr-with-mode-change` option permettant de filtrer les demandes setattr du client pour changer les bits de mode d'un fichier ou d'un répertoire. • `setattr-with-size-change` option permettant de filtrer les demandes setattr du client pour modifier la taille d'un fichier. • `setattr-with-allocation-size-change` option permettant de filtrer les demandes setattr du client pour modifier la taille d'allocation d'un fichier. Cette option n'est disponible que pour le protocole SMB. • `exclude-directory` option permettant de filtrer les demandes client pour les opérations d'annuaire. Lorsque ce filtre est spécifié, les opérations du répertoire ne sont pas surveillées.	`-filters filter, ...`

Est une opération de volume requise Spécifie si une surveillance est requise pour les opérations de montage et de démontage de volumes. La valeur par défaut est `false`.	`-volume-operation` {`true`
`false`} `-filters filter`, ...	*Notifications de refus d'accès FPolicy* À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Ces notifications sont précieuses pour la sécurité, la protection contre les ransomware et la gouvernance. Des notifications seront générées pour l'opération de fichier ayant échoué en raison d'un manque d'autorisation, notamment : • Défaillances dues aux autorisations NTFS. • Échecs dus aux bits de mode Unix. • Défaillances dues à des ACL NFSv4.
`-monitor-fileop-failure` {`true`	`false`}

Opérations de fichiers et combinaisons de filtres prises en charge que FPolicy peut surveiller pour SMB

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations et de filtres sont prises en charge pour la surveillance des opérations d'accès aux fichiers SMB.

Le tableau suivant fournit la liste des combinaisons d'opérations de fichiers et de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers SMB :

Opérations de fichiers prises en charge	Filtres pris en charge
fermer	surveillance-ads, hors ligne-bit, fermeture-avec-modification, fermeture-sans-modification, gros-avec-lecture, exclure-répertoire
création	surveillance-ads, hors ligne-bit

dir_de_création	Aucun filtre n’est actuellement pris en charge pour cette opération de fichier.
supprimer	surveillance-ads, hors ligne-bit
dir_de_suppression	Aucun filtre n’est actuellement pris en charge pour cette opération de fichier.
getattr	offline-bit, exclude-dir
la transparence	monitor-ads, offline-bit, open-with-delete-intentionnel, open-with-write-intentions, exclude-dir
lecture	surveillance-ads, hors-ligne-bit, première lecture
écriture	surveillance-ads, hors-ligne-bit, première-écriture, écriture-avec-changement de taille
renommer	surveillance-ads, hors ligne-bit
rename_dir	Aucun filtre n’est actuellement pris en charge pour cette opération de fichier.
définir	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d’échec des opérations sur les fichiers en raison d’un manque d’autorisations. Le tableau suivant répertorie les combinaisons de filtres et d’opérations de fichiers refusés d’accès pris en charge pour la surveillance FPolicy des événements d’accès aux fichiers SMB :

Opération de fichier d’accès refusé prise en charge	Filtres pris en charge
la transparence	NA

Opérations de fichiers et combinaisons de filtres prises en charge pouvant être moniteurs par FPolicy pour NFSv3

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d’opérations sur les fichiers et de filtres sont prises en charge pour surveiller les opérations d’accès aux fichiers NFSv3.

Le tableau suivant répertorie les opérations de fichiers et les combinaisons de filtres prises en charge pour la surveillance FPolicy des événements d’accès aux fichiers NFSv3 :

Opérations de fichiers prises en charge	Filtres pris en charge
création	bit hors ligne
dir_de_création	Aucun filtre n’est actuellement pris en charge pour cette opération de fichier.
supprimer	bit hors ligne
dir_de_suppression	Aucun filtre n’est actuellement pris en charge pour cette opération de fichier.
lien	bit hors ligne
recherche	offline-bit, exclude-dir
lecture	bit hors ligne, première lecture
écriture	bit hors ligne, première écriture, écriture avec changement de taille
renommer	bit hors ligne
rename_dir	Aucun filtre n’est actuellement pris en charge pour cette opération de fichier.
définir	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modif_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	bit hors ligne

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d’échec des opérations sur les fichiers en raison d’un manque d’autorisations. Le tableau suivant répertorie les combinaisons de filtres et d’opérations de fichiers refusés d’accès prises en charge pour la surveillance FPolicy des événements d’accès aux fichiers NFSv3 :

Opération de fichier d’accès refusé prise en charge	Filtres pris en charge
l’accès	NA
création	NA
dir_de_création	NA
supprimer	NA
dir_de_suppression	NA

lien	NA
lecture	NA
renommer	NA
rename_dir	NA
définir	NA
écriture	NA

Opérations de fichiers et combinaisons de filtres prises en charge que FPolicy peut surveiller pour NFSv4

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations et de filtres sont prises en charge pour surveiller les opérations d'accès aux fichiers NFSv4.

Le tableau suivant fournit la liste des combinaisons d'opérations de fichiers et de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv4 :

Opérations de fichiers prises en charge	Filtres pris en charge
fermer	bit hors ligne, répertoire d'exclusion
création	bit hors ligne
dir_de_création	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
supprimer	bit hors ligne
dir_de_suppression	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
getattr	bit hors ligne, répertoire d'exclusion
lien	bit hors ligne
recherche	bit hors ligne, répertoire d'exclusion
la transparence	bit hors ligne, répertoire d'exclusion
lecture	bit hors ligne, première lecture
écriture	bit hors ligne, première écriture, écriture avec changement de taille

renommer	bit hors ligne
rename_dir	Aucun filtre n’est actuellement pris en charge pour cette opération de fichier.
définir	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	bit hors ligne

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d’échec des opérations sur les fichiers en raison d’un manque d’autorisations. La liste des opérations d’accès refusé aux fichiers et des combinaisons de filtres prises en charge pour la surveillance FPolicy des événements d’accès aux fichiers NFSv4 est fournie dans le tableau suivant :

Opération de fichier d’accès refusé prise en charge	Filtres pris en charge
l’accès	NA
création	NA
dir_de_création	NA
supprimer	NA
dir_de_suppression	NA
lien	NA
la transparence	NA
lecture	NA
renommer	NA
rename_dir	NA
définir	NA
écriture	NA

Remplissez la fiche de configuration des événements FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration des événements FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer l'événement FPolicy.

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration des événements FPolicy, puis noter la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom de l'événement	Oui.	Oui.	
Protocole	Non		
Opérations sur les fichiers	Non		
Filtres	Non		
Opération de volume	Non		
Événements d'accès refusé (Support à partir de ONTAP 9.13)	Non		

Planifiez la configuration de la règle FPolicy

Planifier l'présentation de la configuration de la règle FPolicy

Avant de configurer la règle FPolicy, vous devez comprendre les paramètres requis lors de la création de la règle ainsi que les raisons pour lesquelles vous pouvez vouloir configurer certains paramètres facultatifs. Ces informations vous aident à déterminer les valeurs à définir pour chaque paramètre.

Lors de la création d'une politique FPolicy, vous associez cette règle à ce qui suit :

- Le serveur virtuel de stockage (SVM)
- Un ou plusieurs événements FPolicy
- Moteur externe FPolicy

Vous pouvez également configurer plusieurs paramètres de stratégie facultatifs.

Contenu de la configuration des règles FPolicy

Vous pouvez utiliser la liste suivante de règles FPolicy disponibles et de paramètres facultatifs pour vous aider à planifier votre configuration :

Type d'information	Option	Obligatoire	Valeur par défaut
Nom du SVM Spécifie le nom du SVM sur lequel vous souhaitez créer une politique FPolicy.	`-vserver vserver_name`	Oui.	Aucune
Nom de la politique Spécifie le nom de la politique FPolicy. Le nom peut comporter jusqu'à 256 caractères. Le nom doit comporter jusqu'à 200 caractères si la stratégie est configurée dans une configuration de reprise après incident de MetroCluster ou de SVM. Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants : • `a` à `z` • `A` à `Z` • `0` à `9` • «»_», «»-", and ".»	`-policy-name policy_name`	Oui.	Aucune
Noms d'événements Spécifie une liste d'événements séparés par des virgules à associer à la politique FPolicy. • Vous pouvez associer plusieurs événements à une stratégie. • Un événement est spécifique à un protocole. • Vous pouvez utiliser une seule stratégie pour surveiller les événements d'accès aux fichiers pour plusieurs protocoles en créant un événement pour chaque protocole que la stratégie doit surveiller, puis en associant les événements à la stratégie. • Les événements doivent déjà exister.	`-events event_name, ...`	Oui.	Aucune

Nom du moteur externe Spécifie le nom du moteur externe à associer à la politique FPolicy. • Un moteur externe contient les informations requises par le nœud pour envoyer des notifications à un serveur FPolicy. • Vous pouvez configurer FPolicy de façon à utiliser le moteur externe natif ONTAP pour simplifier le blocage des fichiers ou à utiliser un moteur externe configuré pour utiliser des serveurs FPolicy externes (serveurs FPolicy) pour obtenir des fonctions plus sophistiquées de blocage et de gestion des fichiers. • Si vous souhaitez utiliser le moteur externe natif, vous ne pouvez pas spécifier de valeur pour ce paramètre ou vous pouvez le spécifier `native` comme valeur. • Si vous souhaitez utiliser des serveurs FPolicy, la configuration du moteur externe doit déjà exister.	`-engine engine_name`	Oui (à moins que la politique n'utilise le moteur natif ONTAP interne)	`native`
Est un screening obligatoire Indique si un filtrage d'accès aux fichiers obligatoire est requis. • Le paramètre de filtrage obligatoire détermine quelle action est prise en cas d'incident d'accès aux fichiers lorsque tous les serveurs principaux et secondaires sont en panne ou qu'aucune réponse n'est reçue des serveurs FPolicy au cours d'une période de temporisation donnée. • Lorsqu'il est réglé sur `true`, les événements d'accès aux fichiers sont refusés. • Lorsqu'il est réglé sur `false`, les événements d'accès aux fichiers sont autorisés.	`-is-mandatory` {`true`	`false`}	Non

`true`	*Autoriser l'accès privilégié* Indique si vous souhaitez que le serveur FPolicy possède un accès privilégié aux fichiers et dossiers surveillés à l'aide d'une connexion de données privilégiée. S'ils sont configurés, les serveurs FPolicy peuvent accéder aux fichiers à partir de la racine de l'SVM contenant les données surveillées à l'aide de la connexion de données privilégiée. Pour l'accès privilégié aux données, SMB doit être sous licence sur le cluster et toutes les LIFs de données utilisées pour se connecter aux serveurs FPolicy doivent être configurées de ce fait `cifs` comme l'un des protocoles autorisés. Si vous souhaitez configurer la policy pour autoriser les accès privilégiés, vous devez également spécifier le nom d'utilisateur du compte que vous souhaitez que le serveur FPolicy utilise pour cet accès privilégié.	`-allow -privileged -access` {`yes`	`no`}

Non (sauf si la lecture passthrough est activée)	`no`	*Nom d'utilisateur privilégié* Spécifie le nom d'utilisateur du compte que les serveurs FPolicy utilisent pour l'accès aux données privilégié. • La valeur de ce paramètre doit utiliser le format "daomain\user name". • Si `-allow -privileged -access` est défini sur `no`, toute valeur définie pour ce paramètre est ignorée.	`-privileged -user-name user_name`

Non (sauf si l'accès privilégié est activé)	Aucune	*Autoriser la lecture_passthrough* Spécifie si les serveurs FPolicy peuvent fournir des services de passe-lecture pour les fichiers qui ont été archivés sur le stockage secondaire (fichiers hors ligne) par les serveurs FPolicy : • Passthrough-read est un moyen de lire les données pour les fichiers hors ligne sans restaurer les données dans le stockage primaire. La lecture Passthrough réduit les latences de réponse. Les fichiers ne sont donc pas rappelés dans le stockage primaire, ce qui évite de l'avoir à remonter pour répondre à la demande de lecture. De plus, la lecture intermédiaire optimise l'efficacité du stockage puisque vous n'avez plus besoin d'utiliser l'espace de stockage principal avec des fichiers rappelés uniquement pour satisfaire les demandes de lecture.	`-is-passthrough-read-enabled` {`true`

Condition pour les configurations de l'étendue FPolicy si la politique FPolicy utilise le moteur natif

Si vous configurez la règle FPolicy pour utiliser le moteur natif, il existe une condition spécifique à la définition du périmètre FPolicy configuré pour la règle.

Le périmètre FPolicy définit les limites de la règle FPolicy s'applique, par exemple, si la FPolicy s'applique à des volumes ou des partages spécifiés. Un certain nombre de paramètres limitent davantage l'étendue à laquelle la politique FPolicy s'applique. L'un de ces paramètres, `-is-file-extension-check-on-directories-enabled`indique s'il faut vérifier les extensions de fichier sur les répertoires. La valeur par défaut est `false, ce qui signifie que les extensions de fichiers des répertoires ne sont pas vérifiées.

Lorsqu'une politique de FPolicy utilisant le moteur natif est activée sur un partage ou un volume et sur `-is-file-extension-check-on-directories-enabled` le paramètre est défini sur `false` pour le périmètre de la politique, l'accès au répertoire est refusé. Avec cette configuration, car les extensions de fichier ne sont pas vérifiées pour les répertoires, toute opération de répertoire est refusée si elle relève de la portée de la stratégie.

Pour vous assurer que l'accès au répertoire a réussi lors de l'utilisation du moteur natif, vous devez définir le `-is-file-extension-check-on-directories-enabled parameter` à `true` lors de la création de la portée.

Avec ce paramètre défini sur `true`, Les contrôles d'extension se produisent pour les opérations d'annuaire et la décision d'autoriser ou de refuser l'accès est prise en fonction des extensions incluses ou exclues dans la configuration du périmètre FPolicy.

- Lorsqu'ils sont activés, les serveurs FPolicy fournissent les données du fichier sur un canal de données privilégié distinct ouvert spécifiquement pour les lectures passantes.
- Si vous souhaitez configurer passthrough-read, la stratégie doit également être configurée pour autoriser l'accès privilégié.

Remplissez la fiche de règles FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration de la politique FPolicy. Il est important d'enregistrer si vous souhaitez inclure chaque paramètre dans la configuration de la règle FPolicy, puis d'enregistrer la valeur des paramètres à inclure.

Type d'information	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	
Nom de la règle	Oui.	
Noms des événements	Oui.	
Nom du moteur externe		
Un screening obligatoire est-il requis ?		
Autoriser l'accès privilégié		
Nom d'utilisateur privilégié		
La lecture passthrough est-elle activée ?		

Planification de la configuration du cadre FPolicy

Planifier l'présentation de la configuration du cadre FPolicy

Avant de configurer le cadre FPolicy, vous devez comprendre ce qu'il signifie. Vous devez comprendre le contenu de la configuration du périmètre. Vous devez également comprendre les règles de priorité de la portée. Ces informations peuvent vous aider à planifier les valeurs que vous souhaitez définir.

Ce qu'il signifie pour créer une étendue FPolicy

La création du périmètre FPolicy consiste à définir les limites de la règle FPolicy. Le serveur virtuel de stockage (SVM) est la limite de base. Lorsque vous créez un cadre pour une politique FPolicy, vous devez définir la politique FPolicy à laquelle elle s'applique, et vous devez désigner la SVM à laquelle vous souhaitez appliquer le périmètre.

Un certain nombre de paramètres limitent davantage la portée au sein de la SVM spécifiée. Vous pouvez restreindre la portée en spécifiant ce qui doit être inclus dans la portée ou en spécifiant ce qui à exclure de la portée. Après avoir appliqué une portée à une stratégie activée, les vérifications d'événements de stratégie sont appliquées à la portée définie par cette commande.

Des notifications sont générées pour les événements d'accès aux fichiers où des correspondances sont trouvées dans les options « inclure ». Les notifications ne sont pas générées pour les événements d'accès aux fichiers où des correspondances sont trouvées dans les options « exclure ».

La configuration du périmètre FPolicy définit les informations de configuration suivantes :

- Nom du SVM
- Nom de la règle
- Les partages à inclure ou à exclure de ce qui est surveillé
- Les règles d'exportation à inclure ou à exclure de ce qui est surveillé
- Les volumes à inclure ou à exclure de ce qui est surveillé
- Les extensions de fichier à inclure ou exclure de ce qui est surveillé
- Vérification de l'extension de fichier sur les objets de répertoire

> Il existe des considérations spéciales à prendre en compte pour ce qui est des règles FPolicy de cluster. La politique de FPolicy de cluster est une règle que l'administrateur du cluster crée pour le SVM d'admin. Si l'administrateur du cluster crée également le périmètre de cette politique FPolicy de cluster, l'administrateur du SVM ne peut pas créer de étendue pour cette même politique. Toutefois, si l'administrateur du cluster ne crée pas de périmètre pour la politique de FPolicy de cluster, tout administrateur du SVM peut créer le périmètre de cette politique. Si l'administrateur SVM crée un périmètre pour cette politique FPolicy de cluster, l'administrateur du cluster ne peut pas créer par la suite une étendue de cluster pour cette même policy de cluster. En effet, l'administrateur du cluster ne peut pas remplacer la portée de la même politique de cluster.

Les règles de priorité de la portée

Les règles de priorité suivantes s'appliquent aux configurations du périmètre :

- Lorsqu'un partage est inclus dans le `-shares-to-include` le paramètre et le volume parent du partage sont inclus dans le `-volumes-to-exclude` paramètre, `-volumes-to-exclude` a priorité sur `-shares-to-include`.
- Lorsqu'une export-policy est incluse dans le `-export-policies-to-include` et le volume parent de la export policy est inclus dans le `-volumes-to-exclude` paramètre, `-volumes-to-exclude` a priorité sur `-export-policies-to-include`.
- Un administrateur peut spécifier les deux `-file-extensions-to-include` et `-file-extensions-to-exclude` listes.

  Le `-file-extensions-to-exclude` le paramètre est vérifié avant le `-file-extensions-to-include` le paramètre est vérifié.

Contenu de la configuration de l'étendue FPolicy

Pour planifier votre configuration, vous pouvez utiliser la liste suivante des paramètres de configuration du périmètre FPolicy disponibles :

> Lors de la configuration des partages, des règles d'exportation, des volumes et des extensions de fichiers à inclure ou à exclure du périmètre, les paramètres d'inclusion et d'exclusion peuvent inclure des métacaractères tels que «»?`" and "`*». L'utilisation d'expressions régulières n'est pas prise en charge.

Type d'information	Option
SVM Spécifie le nom du SVM sur lequel vous souhaitez créer une étendue FPolicy. Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.	`-vserver vserver_name`
Nom de la politique Spécifie le nom de la politique FPolicy à laquelle vous souhaitez associer le périmètre. La politique FPolicy doit déjà exister.	`-policy-name policy_name`
Actions à inclure Spécifie une liste de partages délimitée par des virgules pour contrôler la politique FPolicy à laquelle le périmètre est appliqué.	`-shares-to-include share_name, ...`
Actions à exclure Spécifie une liste de partages délimitée par des virgules, à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.	`-shares-to-exclude share_name, ...`

Volumes à inclure Spécifie une liste de volumes séparés par des virgules à surveiller pour la politique FPolicy à laquelle le périmètre est appliqué.	`-volumes-to-include volume_name`, ...
Volumes à exclure Spécifie une liste de volumes séparés par des virgules à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.	`-volumes-to-exclude volume_name`, ...
Exporter les stratégies à inclure Spécifie une liste des règles d'exportation séparées par des virgules pour surveiller la politique FPolicy à laquelle le périmètre est appliqué.	`-export-policies-to -include export_policy_name`, ...
Exporter des stratégies à exclure Spécifie une liste de règles d'exportation séparées par des virgules afin d'exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.	`-export-policies-to -exclude export_policy_name`, ...
Extensions de fichier à inclure Spécifie une liste d'extensions de fichiers délimitée par des virgules pour surveiller la politique FPolicy à laquelle le périmètre est appliqué.	`-file-extensions-to -include file_extensions`, ...
Extension de fichier à exclure Spécifie une liste d'extensions de fichiers délimitée par des virgules à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.	`-file-extensions-to -exclude file_extensions`, ...
La vérification de l'extension de fichier sur le répertoire est-elle activée ? Indique si les vérifications d'extension de nom de fichier s'appliquent également aux objets de répertoire. Si ce paramètre est défini sur `true`, les objets de répertoire sont soumis aux mêmes contrôles d'extension que les fichiers normaux. Si ce paramètre est défini sur `false`, les noms de répertoire ne correspondent pas pour les postes et les notifications sont envoyées pour les répertoires même si leurs extensions de nom ne correspondent pas. Si la politique FPolicy à laquelle l'étendue est affectée est configurée pour utiliser le moteur natif, ce paramètre doit être défini sur `true`.	`-is-file-extension -check-on-directories -enabled` {`true`
`false`	}

Remplissez la fiche de l'étendue FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration du périmètre FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer

l'étendue FPolicy.

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration de l'étendue FPolicy, puis noter la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom de la règle	Oui.	Oui.	
Partages à inclure	Non		
Partages à exclure	Non		
Volumes à inclure	Non		
Volumes à exclure	Non		
Export-policy à inclure	Non		
Exporter les règles à exclure	Non		
Extensions de fichier à inclure	Non		
Extension de fichier à exclure	Non		
La vérification de l'extension de fichier sur le répertoire est-elle activée ?	Non		

Créer la configuration FPolicy

Créez le moteur externe FPolicy

Vous devez créer un moteur externe pour commencer à créer une configuration FPolicy. Le moteur externe définit la façon dont FPolicy établit et gère les connexions aux serveurs FPolicy externes. Si votre configuration utilise le moteur ONTAP interne (moteur externe natif) pour le blocage simple des fichiers, vous n'avez pas besoin de configurer un moteur externe FPolicy distinct et n'avez pas besoin de réaliser cette étape.

Ce dont vous avez besoin

Le "moteur externe" la fiche doit être remplie.

Description de la tâche

Si le moteur externe est utilisé dans une configuration MetroCluster, indiquez les adresses IP des serveurs FPolicy du site source en tant que serveurs primaires. Les adresses IP des serveurs FPolicy du site de destination doivent être spécifiées en tant que serveurs secondaires.

Étapes

1. Créez le moteur externe FPolicy à l'aide de `vserver fpolicy policy external-engine create` commande.

   La commande suivante crée un moteur externe sur une machine virtuelle de stockage (SVM) vs1.example.com. Aucune authentification n'est requise pour les communications externes avec le serveur FPolicy.

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. Vérifiez la configuration du moteur externe FPolicy à l'aide du `vserver fpolicy policy external-engine show` commande.

   Les informations d'affichage de la commande suivante concernant tous les moteurs externes configurés sur le SVM vs1.example.com :

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                   Primary        Secondary
   External
   Vserver            Engine       Servers        Servers       Port Engine
   Type
   ---------------    -----------  -------------- ----------- ------
   -----------
   vs1.example.com    engine1      10.1.1.2,      -             6789
   synchronous
                                   10.1.1.3
   ```

   La commande suivante affiche des informations détaillées sur le moteur externe nommé « moteur1 » sur le SVM vs1.example.com :

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

   ```
                                Vserver: vs1.example.com
                                 Engine: engine1
                Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
        Port Number of FPolicy Service: 6789
             Secondary FPolicy Servers: -
                  External Engine Type: synchronous
   SSL Option for External Communication: no-auth
            FQDN or Custom Common Name: -
          Serial Number of Certificate: -
                 Certificate Authority: -
   ```

Créez l'événement FPolicy

Dans le cadre de la configuration de règles FPolicy, vous devez créer un événement FPolicy. Lors de sa création, vous associez l'événement à la politique FPolicy. Un événement définit le protocole à surveiller et les événements d'accès aux fichiers à surveiller et à filtrer.

Avant de commencer

Vous devez terminer l'événement FPolicy "feuille de calcul".

Créez l'événement FPolicy

1. Créez l'événement FPolicy à l'aide de `vserver fpolicy policy event create` commande.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Vérifiez la configuration d'événement FPolicy à l'aide de `vserver fpolicy policy event show` commande.

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                      Event                 File                       Is Volume
   Vserver            Name      Protocols Operations    Filters   Operation
   ---------------    --------- --------- ------------- ---------
   ------------
   vs1.example.com    event1    cifs      open, close,  -         false
                                          read, write
   ```

Créez les événements de refus d'accès FPolicy

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Ces notifications sont précieuses pour la sécurité, la protection contre les ransomware et la gouvernance.

1. Créez l'événement FPolicy à l'aide de `vserver fpolicy policy event create` commande.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -monitor-fileop-failure true -file-operations open
   ```

Créez des magasins persistants

À partir de ONTAP 9.14.1, FPolicy vous permet de configurer un "Magasins persistants" Pour capturer les événements d'accès aux fichiers pour les politiques asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

Et des meilleures pratiques

- Avant d'utiliser la fonction de stockage persistant, assurez-vous que vos applications partenaires prennent en charge cette configuration.
- Le volume de stockage persistant est configuré par SVM. Pour chaque SVM activé FPolicy, vous avez besoin d'un volume de stockage persistant.
- Le nom du volume de stockage persistant et le chemin de jonction spécifiés au moment de la création du volume doivent correspondre.
- Créez le volume de stockage persistant sur le nœud avec les LIF qui prévoient que le trafic maximal sera surveillé par Fpolicy.
- Définissez la règle de snapshot sur `none` pour ce volume au lieu de `default`. Cela permet de s'assurer qu'il n'y a pas de restauration accidentelle de l'instantané, ce qui entraîne la perte des événements actuels et d'empêcher le traitement des événements en double.
- Rendre le volume de stockage persistant inaccessible pour l'accès au protocole utilisateur externe (CIFS/NFS) afin d'éviter toute corruption accidentelle ou suppression des enregistrements d'événements persistants. Pour ce faire, une fois FPolicy activé, démontez le volume dans ONTAP pour supprimer le chemin de jonction, ce qui le rend inaccessible pour l'accès au protocole utilisateur.

Étapes

1. Créer sur le SVM un volume vide pouvant être provisionné pour le magasin persistant :

   ```
   volume create -vserver <SVM Name> -volume <volume> -state <online> -junction
   -path <path> -policy <default> -unix-permissions <777> -size <value>
   -aggregate <aggregate name> -snapshot-policy <none>
   ```

   - La taille du volume de stockage persistant dépend de la durée pendant laquelle vous souhaitez conserver les événements qui ne sont pas livrés au serveur externe (application partenaire).

     Par exemple, si vous souhaitez que 30 minutes d'événements se poursuivent dans un cluster avec une capacité de 30 000 notifications par seconde :

     Taille du volume requis = 30000 x 30 x 60 x 0,6 Ko (taille moyenne des enregistrements de notification) = 32400000 Ko = ~32 Go

   Pour connaître le taux de notification approximatif, vous pouvez accéder à votre application partenaire FPolicy ou utiliser le compteur FPolicy `requests_dispatched_rate`.

   - Un utilisateur administrateur disposant de privilèges RBAC suffisants (pour créer un volume) créera un volume (à l'aide de la commande cli du volume ou de l'API REST) de la taille souhaitée et fournira le nom de ce volume en tant que `-volume` Dans le magasin persistant, créez la commande CLI ou l'API REST.
2. Créez le magasin persistant :

   ```
   vserver fpolicy persistent store create -vserver <SVM> -persistent-store
   <PS_name> -volume <volume>
   ```

   - Stockage persistant : nom du magasin persistant
   - Volume : volume du magasin persistant
3. Une fois le magasin persistant créé, vous pouvez créer la règle FPolicy et ajouter le nom du magasin persistant à cette règle.
   Pour plus d'informations, voir "Créez la règle FPolicy".

Créez la règle FPolicy

Lorsque vous créez la politique FPolicy, vous associez un moteur externe et un ou plusieurs événements à la règle. La politique spécifie également si un filtrage obligatoire est nécessaire, si les serveurs FPolicy ont un accès privilégié aux données sur la machine virtuelle de stockage (SVM) et si la lecture passe-automatique pour les fichiers hors ligne est activée.

Ce dont vous avez besoin

- La fiche de politique FPolicy doit être remplie.
- Si vous prévoyez de configurer la règle pour utiliser les serveurs FPolicy, le moteur externe doit exister.
- Il faut au moins un événement FPolicy que vous prévoyez d'associer à la règle FPolicy.
- Si vous souhaitez configurer l'accès aux données privilégié, un serveur SMB doit exister sur la SVM.
- Pour configurer un magasin persistant pour une stratégie, le type de moteur doit être **async** et la stratégie doit être **non obligatoire**.

  Pour plus d'informations, voir "Créez des magasins persistants".

Étapes

1. Créez la règle FPolicy :

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name, [-persistent-store
   PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
   privileged-user-name domain\user_name] [-is-passthrough-read-enabled
   {true|false}]
   ```

   - Vous pouvez ajouter un ou plusieurs événements à la règle FPolicy.
   - Par défaut, le tramage obligatoire est activé.
   - Si vous souhaitez autoriser l'accès privilégié en définissant l' `-allow-privileged-access` paramètre à `yes`, vous devez également configurer un nom d'utilisateur privilégié pour l'accès privilégié.
   - Si vous souhaitez configurer Passthrough-read en définissant le paramètre `-is-passthrough-read -enabled` paramètre à `true`, vous devez également configurer l'accès privilégié aux données.

     La commande suivante crée une politique nommée « politique 1 » qui est associée à l'événement « event1 » et au moteur externe « moteur1 ». Cette règle utilise des valeurs par défaut dans la configuration de la stratégie :
     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
     -events event1 -engine engine1
     ```

     La commande suivante crée une politique nommée « politique 2 » qui est associée à l'événement « event2 » et au moteur externe « moteur2 ». Cette stratégie est configurée pour utiliser l'accès privilégié à l'aide du nom d'utilisateur spécifié. La lecture passe-système est activée :

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
     -events event2 -engine engine2 -allow-privileged-access yes -privileged-
     user-name example\archive_acct -is-passthrough-read-enabled true
     ```

La commande suivante crée une politique nommée ""native1""" qui est associée à l'événement ""event3"". Cette règle utilise le moteur natif et les valeurs par défaut dans la configuration de la règle :

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. Vérifiez la configuration de la politique FPolicy à l'aide de `vserver fpolicy policy show` commande.

   La commande suivante affiche des informations sur les trois politiques FPolicy configurées, y compris les informations suivantes :

   - SVM associé à la politique
   - Moteur externe associé à la politique
   - Événements associés à la politique
   - Indique si un screening obligatoire est requis
   - Si un accès privilégié est requis
     `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                         Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

Créez le périmètre FPolicy

Après avoir créé la règle FPolicy, vous devez créer une étendue FPolicy. Lors de la création du périmètre, vous associez ce dernier à une règle FPolicy. Le périmètre définit les limites applicables à la politique FPolicy. Les portées peuvent inclure ou exclure des fichiers basés sur des partages, des règles d'exportation, des volumes et des extensions de fichier.

Ce dont vous avez besoin

La fiche de l'étendue de FPolicy doit être remplie. La politique FPolicy doit exister avec un moteur externe associé (si cette règle est configurée pour utiliser des serveurs FPolicy externes) et doit avoir au moins un événement FPolicy associé.

Étapes

1. Créez le cadre FPolicy à l'aide de `vserver fpolicy policy scope create` commande.

   ```
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. Vérifiez la configuration du cadre FPolicy à l'aide du `vserver fpolicy policy scope show` commande.

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
 Export Policies to Include: -
 Export Policies to Exclude: -
 File Extensions to Include: -
 File Extensions to Exclude: -
```

Activez la règle FPolicy

Une fois que vous avez configuré une configuration de règles FPolicy, vous activez cette règle. L'activation de la stratégie définit sa priorité et lance la surveillance de l'accès aux fichiers pour la stratégie.

Ce dont vous avez besoin

La politique FPolicy doit exister avec un moteur externe associé (si cette règle est configurée pour utiliser des serveurs FPolicy externes) et doit avoir au moins un événement FPolicy associé. Le cadre de la politique FPolicy doit exister et doit être attribué à la politique FPolicy.

Description de la tâche

La priorité est utilisée lorsque plusieurs règles sont activées sur la machine virtuelle de stockage (SVM) et qu'une seule règle a souscrit au même événement d'accès aux fichiers. Les règles qui utilisent la configuration du moteur natif ont une priorité plus élevée que les règles pour tout autre moteur, quel que soit le numéro de séquence qui leur est attribué lors de l'activation de la stratégie.

> Une policy ne peut pas être activée sur le SVM admin

Étapes

1. Activez la politique FPolicy à l'aide de `vserver fpolicy enable` commande.

   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
   -sequence-number 1
   ```

2. Vérifiez que la politique FPolicy est activée à l'aide du `vserver fpolicy show` commande.

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                       Sequence
   Vserver          Policy Name         Number  Status   Engine
   ---------------  ----------------- --------  -------- ---------
   vs1.example.com  policy1                   1  on       engine1
   ```

Gérer les configurations FPolicy

Modifier les configurations FPolicy

Commandes permettant de modifier les configurations FPolicy

Vous pouvez modifier les configurations FPolicy en modifiant les éléments de la configuration. Vous pouvez modifier les moteurs externes, les événements FPolicy, les étendues FPolicy et les règles FPolicy. Vous pouvez également activer ou désactiver les règles FPolicy. Lorsque vous désactivez la règle FPolicy, la surveillance des fichiers est interrompue.

Il est recommandé de désactiver la règle FPolicy avant de modifier la configuration.

Si vous voulez modifier…	Utilisez cette commande…
Moteurs externes	`vserver fpolicy policy external-engine modify`
Événements	`vserver fpolicy policy event modify`
Étendues	`vserver fpolicy policy scope modify`
Stratégies	`vserver fpolicy policy modify`

Consultez les pages de manuels pour les commandes pour plus d'informations.

Activez ou désactivez les règles FPolicy

Vous pouvez activer les règles FPolicy une fois la configuration terminée. L'activation de la stratégie définit sa priorité et lance la surveillance de l'accès aux fichiers pour la stratégie. Vous pouvez désactiver les règles FPolicy pour arrêter la surveillance des accès aux fichiers correspondant à cette règle.

Ce dont vous avez besoin

La configuration FPolicy doit être réalisée avant l'activation des règles FPolicy.

Description de la tâche

- La priorité est utilisée lorsque plusieurs règles sont activées sur la machine virtuelle de stockage (SVM) et qu'une seule règle a souscrit au même événement d'accès aux fichiers.
- Les règles qui utilisent la configuration du moteur natif ont une priorité plus élevée que les règles pour tout autre moteur, quel que soit le numéro de séquence qui leur est attribué lors de l'activation de la stratégie.
- Pour modifier la priorité d'une règle FPolicy, vous devez la désactiver puis la réactiver à l'aide du nouveau numéro de séquence.

Étape

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activez une règle FPolicy	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
Désactiver une règle FPolicy	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

Affiche des informations sur les configurations FPolicy

Fonctionnement des commandes show

Il est utile lors de l'affichage d'informations sur la configuration FPolicy pour comprendre la `show` les commandes fonctionnent.

A `show` la commande sans paramètre supplémentaire affiche les informations sous forme récapitulative. De plus, chaque `show` la commande dispose des deux mêmes paramètres facultatifs mutuellement exclusifs. `-instance` et `-fields`.

Lorsque vous utilisez le `-instance` paramètre avec un `show` commande, la sortie de la commande affiche des informations détaillées au format de liste. Dans certains cas, le résultat détaillé peut être long et inclure plus d'informations que vous n'en avez besoin. Vous pouvez utiliser le `-fields fieldname[,fieldname…]` paramètre permettant de personnaliser la sortie afin qu'elle affiche les informations uniquement pour les champs que vous spécifiez. Vous pouvez définir les champs que vous pouvez spécifier en saisissant `?` après le `-fields` paramètre.

> La sortie d'un `show` commande avec `-fields` paramètre peut afficher d'autres champs pertinents et nécessaires associés aux champs demandés.

Toutes les `show` la commande comporte un ou plusieurs paramètres facultatifs qui filtrent la sortie et vous permettent de réduire la portée des informations affichées dans la sortie de la commande. Vous pouvez définir l'identité des paramètres facultatifs disponibles pour une commande en saisissant `?` après le `show` commande.

Le `show` La commande prend en charge les motifs de style UNIX et les caractères génériques pour vous permettre de faire correspondre plusieurs valeurs dans les arguments de paramètres-commande. Par exemple, vous pouvez utiliser l'opérateur générique (*), L'opérateur NOT (!), l'opérateur OR (|), l'opérateur Range (integer…integer), l'opérateur moins-que (<), l'opérateur plus grand-que (>), l'opérateur MOINS-égal ou égal à (<=) et l'opérateur supérieur ou égal à (>=) lors de la spécification de valeurs.

Pour plus d'informations sur l'utilisation de modèles de style UNIX et de caractères génériques, reportez-vous au Utilisation de l'interface de ligne de commandes ONTAP.

Commandes permettant d'afficher des informations sur les configurations FPolicy

Vous utilisez le `fpolicy show` Commandes permettant d'afficher des informations sur la configuration FPolicy, y compris les informations sur les moteurs, événements, étendues et règles FPolicy externes.

Pour afficher des informations sur FPolicy…	Utilisez cette commande…
Moteurs externes	`vserver fpolicy policy external-engine show`
Événements	`vserver fpolicy policy event show`
Étendues	`vserver fpolicy policy scope show`
Stratégies	`vserver fpolicy policy show`

Consultez les pages de manuels pour les commandes pour plus d'informations.

Affiche des informations sur l'état des règles FPolicy

Vous pouvez afficher des informations sur le statut des règles FPolicy pour déterminer si une règle est activée, le moteur externe qu'elle est configuré à utiliser, le numéro de séquence correspondant à la règle et à quel serveur virtuel de stockage (SVM) la politique FPolicy est associée.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle
- Numéro de séquence de police
- Statut de la stratégie

Outre l'affichage des informations sur l'état des règles de FPolicy configurées sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande, ou `-fields ?` pour déterminer les champs que vous pouvez utiliser.

Étape

1. Afficher des informations filtrées sur l'état des règles FPolicy à l'aide de la commande appropriée :

Pour afficher des informations d'état sur les stratégies…	Entrez la commande…
Sur le cluster	`vserver fpolicy show`
Dont le statut est spécifié	`vserver fpolicy show -status {on
off}`	Sur un SVM spécifié

`vserver fpolicy show -vserver vserver_name`	Avec le nom de la règle spécifiée
`vserver fpolicy show -policy-name policy_name`	Qui utilisent le moteur externe spécifié

Exemple

Les exemples suivants affichent les informations sur les règles FPolicy sur le cluster :

```
cluster1::> vserver fpolicy show
                                          Sequence
Vserver             Policy Name             Number  Status      Engine
------------------- ------------------- --------  ---------   ---------
FPolicy             cserver_policy      -         off         eng1
vs1.example.com     v1p1                -         off         eng2
vs1.example.com     v1p2                -         off         native
vs1.example.com     v1p3                -         off         native
vs1.example.com     cserver_policy      -         off         eng1
vs2.example.com     v1p1                3         on          native
vs2.example.com     v1p2                1         on          eng3
vs2.example.com     cserver_policy      2         on          eng1
```

Affiche des informations sur les règles FPolicy activées

Vous pouvez afficher des informations sur les règles FPolicy activées pour déterminer le moteur externe FPolicy à utiliser, la priorité de la règle et le SVM associé à la règle FPolicy.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle
- Priorité de la stratégie

Vous pouvez utiliser les paramètres de la commande pour filtrer la sortie de la commande par critères spécifiés.

Étape

1. Afficher des informations sur les règles FPolicy activées à l'aide de la commande appropriée :

Si vous souhaitez afficher des informations sur les stratégies activées…	Entrez la commande…

Sur le cluster	`vserver fpolicy show-enabled`
Sur un SVM spécifié	`vserver fpolicy show-enabled -vserver vserver_name`
Avec le nom de la règle spécifiée	`vserver fpolicy show-enabled -policy-name policy_name`
Avec le numéro de séquence spécifié	`vserver fpolicy show-enabled -priority integer`

Exemple

Les exemples suivants affichent les informations sur les règles FPolicy activées sur le cluster :

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

Gérez les connexions du serveur FPolicy

Connectez-vous à des serveurs FPolicy externes

Pour activer le traitement de fichiers, vous devrez peut-être vous connecter manuellement à un serveur FPolicy externe si la connexion a déjà été interrompue. Une connexion est interrompue une fois le délai d'expiration du serveur atteint ou en raison d'une erreur. L'administrateur peut également mettre fin manuellement à une connexion.

Description de la tâche

En cas d'erreur fatale, la connexion au serveur FPolicy peut être interrompue. Après avoir résolu le problème à l'origine de l'erreur fatale, vous devez vous reconnecter manuellement au serveur FPolicy.

Étapes

1. Connectez-vous au serveur FPolicy externe à l'aide de `vserver fpolicy engine-connect` commande.

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

2. Vérifiez que le serveur FPolicy externe est connecté à l'aide du `vserver fpolicy show-engine` commande.

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

Effectue la déconnexion des serveurs FPolicy externes

Vous devrez peut-être vous déconnecter manuellement d'un serveur FPolicy externe. Cette opération peut être utile si le serveur FPolicy présente des problèmes avec le traitement des demandes de notification ou si vous devez effectuer une maintenance sur le serveur FPolicy.

Étapes

1. Déconnectez-vous du serveur FPolicy externe à l'aide de `vserver fpolicy engine-disconnect` commande.

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

2. Vérifiez que le serveur FPolicy externe est déconnecté à l'aide de `vserver fpolicy show-engine` commande.

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

Affiche des informations sur les connexions aux serveurs FPolicy externes

Vous pouvez afficher les informations d'état des connexions aux serveurs FPolicy externes pour le cluster ou pour une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent vous aider à déterminer quels serveurs FPolicy sont connectés.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom du nœud
- Nom de la règle FPolicy
- Adresse IP du serveur FPolicy
- État du serveur FPolicy
- Type de serveur FPolicy

En plus d'afficher les informations relatives aux connexions FPolicy sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande. Vous pouvez entrer `?` après le `-fields` paramètre pour déterminer les champs que vous pouvez utiliser.

Étape

1. Afficher des informations filtrées sur l'état de connexion entre le nœud et le serveur FPolicy à l'aide de la commande appropriée :

Pour afficher les informations sur l'état des connexions à propos des serveurs FPolicy…	Entrer…

Que vous spécifiez	`vserver fpolicy show-engine -server IP_address`
Pour un SVM spécifié	`vserver fpolicy show-engine -vserver vserver_name`
Associés à une politique spécifiée	`vserver fpolicy show-engine -policy-name policy_name`
Avec l'état du serveur que vous spécifiez	`vserver fpolicy show-engine -server-status status` La liste ci-dessous répertorie les différents États du serveur : • `connected` • `disconnected` • `connecting` • `disconnecting`
Avec le type spécifié	`vserver fpolicy show-engine -server-type type` Le type de serveur FPolicy peut être l'un des suivants : • `primary` • `secondary`
Qui ont été déconnectés avec la raison spécifiée	`vserver fpolicy show-engine -disconnect-reason text` La déconnexion peut être due à plusieurs raisons. Les raisons courantes de la déconnexion sont les suivantes : • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

Exemple

Cet exemple affiche des informations sur les connexions des moteurs externes aux serveurs FPolicy du SVM vs1.example.com :

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                                Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

Cet exemple affiche des informations uniquement sur les serveurs FPolicy connectés :

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

Affiche des informations sur l'état de la connexion de passerelle FPolicy

Vous pouvez afficher des informations sur l'état de la connexion de passage en lecture FPolicy à des serveurs FPolicy externes pour le cluster ou à un SVM spécifié. Ces informations peuvent vous aider à identifier les serveurs FPolicy dotés de connexions de données de type « passthrough read » et pour lesquels les serveurs FPolicy sont déconnectés.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle FPolicy
- Nom du nœud
- Adresse IP du serveur FPolicy
- État de la connexion de lecture intermédiaire FPolicy

En plus d'afficher les informations relatives aux connexions FPolicy sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande. Vous pouvez entrer `?` après le `-fields` paramètre pour déterminer les champs que vous pouvez utiliser.

Étape

1. Afficher des informations filtrées sur l'état de connexion entre le nœud et le serveur FPolicy à l'aide de la commande appropriée :

Pour afficher les informations sur l'état de la connexion…	Entrez la commande…
État de la connexion de lecture « pashrough FPolicy » pour le cluster	`vserver fpolicy show-passthrough-read-connection`
État de connexion de passerelle FPolicy pour un SVM spécifié	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
État de la connexion de lecture intermédiaire FPolicy pour une règle spécifiée	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
État détaillé de la connexion de lecture intermédiaire FPolicy pour une règle spécifiée	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`
État de la connexion de lecture intermédiaire FPolicy pour l'état que vous spécifiez	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` La liste ci-dessous répertorie les différents États du serveur : • `connected` • `disconnected`

Exemple

La commande suivante affiche des informations relatives aux connexions de lecture passerelle de tous les serveurs FPolicy du cluster :

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                            FPolicy           Server
Vserver          Policy Name   Node         Server            Status
---------------  ------------- ------------ -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

La commande suivante affiche des informations détaillées sur les connexions en lecture pasde serveurs FPolicy configurées dans la politique « Pol_cifs_1 » :

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                          Node: FPolicy-01
                                       Vserver: vs1.example.com
                                        Policy: pol_cifs_1
                                        Server: 1.1.1.1
                Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                  Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

Vérifiez l’accès à l’aide du suivi de sécurité

Fonctionnement des traces de sécurité

Vous pouvez ajouter des filtres de suivi des autorisations pour demander à ONTAP de consigner des informations sur la raison pour laquelle les serveurs SMB et NFS d’une machine virtuelle de stockage (SVM) autorise ou refuse la demande d’un client ou d’un utilisateur d’effectuer une opération. Cela peut être utile lorsque vous voulez vérifier que votre schéma de sécurité d’accès aux fichiers est approprié ou lorsque vous souhaitez résoudre les problèmes d’accès aux fichiers.

Les traces de sécurité vous permettent de configurer un filtre qui détecte les opérations client sur SMB et NFS sur le SVM et trace tous les contrôles d’accès correspondant à ce filtre. Vous pouvez alors afficher les résultats de la trace, ce qui fournit un résumé pratique de la raison pour laquelle l’accès a été autorisé ou refusé.

Lorsque vous voulez vérifier les paramètres de sécurité de l’accès SMB ou NFS sur des fichiers et dossiers de votre SVM ou si vous êtes confronté à un problème d’accès, vous pouvez rapidement ajouter un filtre pour activer le suivi des autorisations.

La liste suivante présente des faits importants sur le fonctionnement des traces de sécurité :

- ONTAP applique des traces de sécurité au niveau du SVM.
- Chaque requête entrante est criblée pour voir si elle correspond aux critères de filtrage des traces de sécurité activées.
- Des traces sont effectuées pour les demandes d’accès aux fichiers et aux dossiers.
- Les traces peuvent être filtrées en fonction des critères suivants :
  - Adresse IP du client
  - Chemin SMB ou NFS
  - Nom Windows
  - Nom UNIX

- Les demandes sont examinées pour les résultats des réponses *autorisé* et *refusé*.
- Chaque demande correspondant aux critères de filtrage des tracés activés est enregistrée dans le journal des résultats de suivi.
- L'administrateur du stockage peut configurer une temporisation sur un filtre pour la désactiver automatiquement.
- Si une demande correspond à plusieurs filtres, les résultats du filtre dont le numéro d'index est le plus élevé sont enregistrés.
- L'administrateur du stockage peut imprimer les résultats à partir du journal des résultats de suivi pour déterminer pourquoi une demande d'accès a été autorisée ou refusée.

Types de contrôles d'accès surveillance des traces de sécurité

Les vérifications d'accès d'un fichier ou d'un dossier sont effectuées en fonction de plusieurs critères. Les traces de sécurité contrôlent les opérations sur tous ces critères.

Les types de vérifications d'accès que contrôle des traces de sécurité comprennent les éléments suivants :

- Méthode de sécurité volume et qtree
- Sécurité efficace du système de fichiers contenant les fichiers et les dossiers sur lesquels des opérations sont demandées
- Mappage d'utilisateurs
- Les autorisations de niveau partage
- Les autorisations de niveau exportation
- Les autorisations de niveau fichier
- Sécurité de la protection d'accès au niveau du stockage

Considérations relatives à la création de traces de sécurité

Lorsque vous créez des traces de sécurité sur des machines virtuelles de stockage (SVM), tenez compte de plusieurs points à prendre en compte. Par exemple, vous devez savoir quels protocoles vous pouvez créer une trace, quels styles de sécurité sont pris en charge et quel est le nombre maximum de traces actives.

- Vous ne pouvez créer que des traces de sécurité sur des SVM.
- Chaque entrée de filtre de trace de sécurité est spécifique au SVM.

  On doit spécifier le SVM sur lequel vous souhaitez exécuter le tracé.

- Vous pouvez ajouter des filtres de suivi des permissions pour les requêtes SMB et NFS.
- On doit configurer le serveur SMB ou NFS sur le SVM sur lequel vous souhaitez créer des filtres de trace.
- Vous pouvez créer des traces de sécurité pour les fichiers et les dossiers résidant sur NTFS, UNIX, ainsi que sur des volumes et des qtrees de type sécurité mixtes.
- Vous pouvez ajouter un maximum de 10 filtres de suivi des permissions par SVM.
- Vous devez spécifier un numéro d'index de filtre lors de la création ou de la modification d'un filtre.

  Les filtres sont pris en compte dans l'ordre du numéro d'index. Les critères d'un filtre avec un numéro

d'index plus élevé sont pris en compte avant les critères avec un nombre d'index plus faible. Si la demande suivie correspond aux critères de plusieurs filtres activés, seul le filtre dont le numéro d'index est le plus élevé est déclenché.

- Une fois que vous avez créé et activé un filtre de trace de sécurité, vous devez exécuter des demandes de fichier ou de dossier sur un système client pour générer l'activité que le filtre de trace peut capturer et ouvrir une session dans le journal des résultats de trace.
- Vous devez ajouter des filtres de suivi des autorisations pour la vérification de l'accès aux fichiers ou le dépannage uniquement.

  L'ajout de filtres de suivi des autorisations a un effet mineur sur les performances du contrôleur.

  Lorsque vous avez terminé l'activité de vérification ou de dépannage, vous devez désactiver ou supprimer tous les filtres de suivi des autorisations. En outre, les critères de filtrage que vous sélectionnez doivent être aussi spécifiques que possible pour que ONTAP n'envoie pas un grand nombre de résultats de trace au journal.

Exécuter des traces de sécurité

Présenter les traces de sécurité

Une trace de sécurité implique la création d'un filtre de trace de sécurité, la vérification des critères de filtre, la génération de demandes d'accès sur un client SMB ou NFS qui correspondent aux critères de filtre, ainsi que l'affichage des résultats.

Une fois que vous avez terminé d'utiliser un filtre de sécurité pour capturer des informations de trace, vous pouvez modifier le filtre et le réutiliser ou le désactiver si vous n'en avez plus besoin. Après avoir affiché et analysé les résultats de trace du filtre, vous pouvez les supprimer s'ils ne sont plus nécessaires.

Créer des filtres de trace de sécurité

Vous pouvez créer des filtres de trace de sécurité qui détectent les opérations des clients SMB et NFS sur les SVM (Storage Virtual machines) et vérifient tous les contrôles d'accès correspondant au filtre. Vous pouvez utiliser les résultats des tracés de sécurité pour valider votre configuration ou résoudre des problèmes d'accès.

Description de la tâche

Il existe deux paramètres requis pour la commande vserver Security trace filter create :

Paramètres requis	Description
`-vserver vserver_name`	*Nom du SVM* Nom du SVM qui contient les fichiers ou les dossiers sur lesquels vous souhaitez appliquer le filtre de trace de sécurité.

`-index index_number`	*Filtrer l'index numéro* Le numéro d'index que vous souhaitez appliquer au filtre. Vous êtes limité à un maximum de 10 filtres de trace par SVM. Les valeurs autorisées pour ce paramètre sont de 1 à 10.

Un certain nombre de paramètres de filtre facultatifs vous permettent de personnaliser le filtre de trace de sécurité afin de réduire les résultats générés par le tracé de sécurité :

Paramètre de filtre	Description
`-client-ip IP_Address`	Ce filtre spécifie l'adresse IP à partir de laquelle l'utilisateur accède au SVM.
`-path path`	Ce filtre indique le chemin d'accès sur lequel appliquer le filtre de suivi des autorisations. La valeur pour `-path` peut utiliser l'un des formats suivants : • Le chemin complet, en commençant par la racine du partage ou de l'exportation • Chemin partiel, relatif à la racine du partage Vous devez utiliser les séparateurs de répertoire de style UNIX du répertoire de style NFS dans la valeur de chemin d'accès.
`-windows-name win_user_name` ou `-unix -name``unix_user_name`	Vous pouvez spécifier le nom d'utilisateur Windows ou le nom d'utilisateur UNIX dont vous souhaitez effectuer le suivi des demandes d'accès. La variable de nom d'utilisateur n'est pas sensible à la casse. Vous ne pouvez pas spécifier à la fois un nom d'utilisateur Windows et un nom d'utilisateur UNIX dans le même filtre. Même si vous pouvez suivre les événements d'accès SMB et NFS, il est possible d'utiliser l'utilisateur UNIX mappé et les groupes d'utilisateurs UNIX mappés lors des vérifications d'accès sur des données de style de sécurité UNIX ou mixtes.
`-trace-allow {yes`	`no}`
Le suivi des événements de refus est toujours activé pour un filtre de trace de sécurité. Vous pouvez éventuellement suivre les événements. Pour suivre les événements d'autorisation, définissez ce paramètre sur `yes`.	`-enabled {enabled`
`disabled}`	Vous pouvez activer ou désactiver le filtre de trace de sécurité. Par défaut, le filtre de trace de sécurité est activé.

`-time-enabled integer`	Vous pouvez spécifier un délai d'attente pour le filtre, après lequel il est désactivé.

Étapes

1. Créer un filtre de trace de sécurité :

   `vserver security trace filter create -vserver vserver_name -index index_numberfilter_parameters`

   `filter_parameters` est une liste des paramètres de filtre facultatifs.

   Pour plus d'informations, consultez les pages de manuels relatives à la commande.

2. Vérifiez l'entrée du filtre de trace de sécurité :

   `vserver security trace filter show -vserver vserver_name -index index_number`

Exemples

La commande suivante crée un filtre de trace de sécurité pour tout utilisateur accédant à un fichier avec un chemin de partage `\\server\share1\dir1\dir2\file.txt` À partir de l'adresse IP 10.10.10.7. Le filtre utilise un chemin complet pour le `-path` option. L'adresse IP du client utilisée pour accéder aux données est 10.10.10.7. Le filtre est sorti après 30 minutes :

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

La commande suivante crée un filtre de trace de sécurité utilisant un chemin relatif pour l' `-path` option. Le filtre trace l'accès pour un utilisateur Windows nommé « joe ». Joe accède à un fichier avec un chemin de partage `\\server\share1\dir1\dir2\file.txt`. Les traces de filtre autorisent et refusent les événements :

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                Vserver: vs1
                           Filter Index: 2
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: mydomain\joe
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Affiche des informations sur les filtres de trace de sécurité

Vous pouvez afficher des informations sur les filtres de trace de sécurité configurés sur votre SVM (Storage Virtual machine). Cela vous permet de voir quels types d'événements d'accès chaque filtre trace.

Étape

1. Affiche des informations sur les entrées du filtre de trace de sécurité à l'aide de `vserver security trace filter show` commande.

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

Exemples

La commande suivante affiche des informations sur tous les filtres de trace de sécurité sur le SVM vs1 :

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Affiche les résultats du suivi de sécurité

Vous pouvez afficher les résultats de suivi de sécurité générés pour les opérations de fichiers qui correspondent aux filtres de trace de sécurité. Les résultats permettent de valider votre configuration de sécurité d'accès aux fichiers ou de résoudre les problèmes d'accès aux fichiers SMB et NFS.

Ce dont vous avez besoin

Un filtre de trace de sécurité activé doit exister et des opérations doivent avoir été effectuées à partir d'un client SMB ou NFS correspondant au filtre de trace de sécurité pour générer les résultats de trace de sécurité.

Description de la tâche

Vous pouvez afficher un récapitulatif de tous les résultats de la trace de sécurité ou personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque les résultats du suivi de sécurité contiennent un grand nombre d'enregistrements.

Si vous ne spécifiez aucun des paramètres facultatifs, les éléments suivants s'affichent :

- Nom de la machine virtuelle de stockage (SVM)
- Nom du nœud
- Numéro d'index de trace de sécurité
- Style de sécurité
- Chemin
- Raison
- Nom d'utilisateur

  Le nom d'utilisateur s'affiche en fonction de la configuration du filtre de trace :

Si le filtre est configuré…	Alors…
Avec un nom d'utilisateur UNIX	Le résultat du suivi de sécurité affiche le nom d'utilisateur UNIX.
Avec un nom d'utilisateur Windows	Le résultat du suivi de sécurité affiche le nom d'utilisateur Windows.
Sans nom d'utilisateur	Le résultat du suivi de sécurité affiche le nom d'utilisateur Windows.

Vous pouvez personnaliser la sortie à l'aide de paramètres facultatifs. Voici certains des paramètres facultatifs que vous pouvez utiliser pour affiner les résultats renvoyés dans le résultat de la commande :

Paramètre facultatif	Description
`-fields field_name, ...`	Affiche la sortie sur les champs que vous choisissez. Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.
`-instance`	Affiche des informations détaillées sur les événements de trace de sécurité. Utilisez ce paramètre avec d'autres paramètres facultatifs pour afficher des informations détaillées sur des résultats de filtre spécifiques.
`-node node_name`	Affiche des informations uniquement sur les événements du nœud spécifié.

`-vserver vserver_name`	Affiche des informations uniquement sur les événements du SVM spécifié.
`-index integer`	Affiche des informations sur les événements survenus à la suite du filtre correspondant au numéro d'index spécifié.
`-client-ip IP_address`	Affiche des informations sur les événements survenus à la suite de l'accès au fichier à partir de l'adresse IP du client spécifiée.
`-path path`	Affiche des informations sur les événements qui se sont produits suite à l'accès au fichier au chemin spécifié.
`-user-name user_name`	Affiche des informations sur les événements qui se sont produits à la suite de l'accès au fichier par l'utilisateur Windows ou UNIX spécifié.
`-security-style security_style`	Affiche des informations sur les événements survenus sur les systèmes de fichiers avec le style de sécurité spécifié.

Pour plus d'informations sur les autres paramètres facultatifs que vous pouvez utiliser avec la commande, reportez-vous à la page man.

Étape

1. Affiche les résultats du filtre de trace de sécurité à l'aide de l' `vserver security trace trace-result show` commande.

   `vserver security trace trace-result show -user-name domain\user`

   ```
   Vserver: vs1

   Node     Index   Filter Details         Reason
   -------- ------- ---------------------  ----------------------------
   node1    3       User:domain\user       Access denied by explicit ACE
                    Security Style:mixed
                    Path:/dir1/dir2/

   node1    5       User:domain\user       Access denied by explicit ACE
                    Security Style:unix
                    Path:/dir1/
   ```

Modifier les filtres de trace de sécurité

Si vous souhaitez modifier les paramètres de filtre facultatifs utilisés pour déterminer les événements d'accès qui sont tracés, vous pouvez modifier les filtres de trace de sécurité existants.

Description de la tâche

Vous devez identifier le filtre de trace de sécurité à modifier en précisant le nom de la machine virtuelle de stockage (SVM) sur laquelle le filtre est appliqué et le numéro d'index du filtre. Vous pouvez modifier tous les paramètres de filtre facultatifs.

Étapes

1. Modifier un filtre de trace de sécurité :

   `vserver security trace filter modify -vserver vserver_name -index index_numberfilter_parameters`

   - `vserver_name` Est le nom du SVM sur lequel vous souhaitez appliquer un filtre de trace de sécurité.
   - `index_number` est le numéro d'index que vous souhaitez appliquer au filtre. Les valeurs autorisées pour ce paramètre sont de 1 à 10.
   - `filter_parameters` est une liste des paramètres de filtre facultatifs.

2. Vérifiez l'entrée du filtre de trace de sécurité :

   `vserver security trace filter show -vserver vserver_name -index index_number`

Exemple

La commande suivante modifie le filtre de trace de sécurité avec l'index numéro 1. Le filtre trace les événements pour tout utilisateur accédant à un fichier avec un chemin de partage `\\server\share1\dir1\dir2\file.txt` À partir de n'importe quelle adresse IP. Le filtre utilise un chemin complet pour le `-path` option. Les traces de filtre autorisent et refusent les événements :

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                      Windows User Name: -
                         UNIX User Name: -
                     Trace Allow Events: yes
                         Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Supprimer les filtres de trace de sécurité

Lorsque vous n'avez plus besoin d'une entrée de filtre de trace de sécurité, vous pouvez la supprimer. Étant donné que vous pouvez disposer d'un maximum de 10 filtres de suivi de sécurité par machine virtuelle de stockage (SVM), la suppression des filtres inutiles vous permet de créer de nouveaux filtres si vous avez atteint le maximum.

Description de la tâche

Pour identifier de manière unique le filtre de trace de sécurité que vous souhaitez supprimer, vous devez spécifier les éléments suivants :

- Nom du SVM auquel le filtre de trace est appliqué
- Numéro d'index du filtre de trace

Étapes

1. Identifiez le numéro d'index de filtre de l'entrée de filtre de trace de sécurité que vous souhaitez supprimer :

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. À l'aide des informations de numéro d'index de filtre de l'étape précédente, supprimez l'entrée de filtre :

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

   ```
   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. Vérifiez que l'entrée du filtre de trace de sécurité est supprimée :

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

Supprimer les enregistrements de trace de sécurité

Une fois que vous avez terminé d'utiliser un enregistrement de suivi de filtre pour vérifier la sécurité d'accès aux fichiers ou pour résoudre les problèmes d'accès client SMB ou NFS, vous pouvez supprimer l'enregistrement de trace de sécurité du journal de suivi de sécurité.

Description de la tâche

Avant de pouvoir supprimer un enregistrement de trace de sécurité, vous devez connaître le numéro de séquence de l'enregistrement.

> Chaque machine virtuelle de stockage (SVM) peut stocker un maximum de 128 traces. Si le maximum est atteint sur la SVM, les anciens enregistrements de trace sont automatiquement supprimés au fur et à mesure de l'ajout de nouveaux enregistrements. Si vous ne souhaitez pas supprimer manuellement les enregistrements de trace sur ce SVM, vous pouvez laisser ONTAP supprimer automatiquement les plus anciens résultats de trace une fois que le maximum est atteint pour laisser place à de nouveaux résultats.

Étapes

1. Identifiez le numéro de séquence de l'enregistrement à supprimer :

   ```
   vserver security trace trace-result show -vserver vserver_name -instance
   ```

2. Supprimer l'enregistrement de trace de sécurité :

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name -seqnum integer

   vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
   999
   ```

   - `-node node_name` est le nom du nœud de cluster sur lequel l'événement de suivi des autorisations que vous souhaitez supprimer s'est produit.

     Ce paramètre est obligatoire.

   - `-vserver vserver_name` Est le nom du SVM sur lequel l'événement de suivi des permissions que vous souhaitez supprimer s'est produit.

     Ce paramètre est obligatoire.

   - `-seqnum integer` est le numéro de séquence de l'événement de journal que vous souhaitez supprimer.

     Ce paramètre est obligatoire.

Supprimer tous les enregistrements de trace de sécurité

Si vous ne souhaitez pas conserver les enregistrements de trace de sécurité existants, vous pouvez supprimer tous les enregistrements d'un nœud à l'aide d'une seule commande.

Étape

1. Supprimer tous les enregistrements de trace de sécurité :

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name *
   ```

   - `-node node_name` est le nom du nœud de cluster sur lequel l'événement de suivi des autorisations

que vous souhaitez supprimer s'est produit.

- `-vserver vserver_name` Est le nom de la machine virtuelle de stockage (SVM) sur laquelle l'événement de suivi des permissions que vous souhaitez supprimer s'est produit.

Interpréter les résultats du suivi de sécurité

Les résultats du suivi de sécurité indiquent la raison pour laquelle une demande a été autorisée ou refusée. Sortie affiche le résultat sous la forme d'une combinaison de la raison d'autoriser ou de refuser l'accès et de l'emplacement dans le chemin de vérification d'accès où l'accès est autorisé ou refusé. Vous pouvez utiliser les résultats pour isoler et identifier les raisons pour lesquelles les actions sont ou ne sont pas autorisées.

Recherche d'informations sur les listes de types de résultats et les détails du filtre

Vous pouvez trouver les listes de types de résultats et les détails de filtre qui peuvent être inclus dans les résultats de trace de sécurité dans les pages de manuel de l' `vserver security trace trace-result show` commande.

Exemple de sortie du `Reason` champ dans un `Allow` type de résultat

Voici un exemple de sortie du `Reason` champ qui apparaît dans les résultats de trace se connecte à un `Allow` type de résultat :

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

Exemple de sortie du `Reason` champ dans un `Allow` type de résultat

Voici un exemple de sortie du `Reason` champ qui apparaît dans le journal des résultats de trace dans un `Deny` type de résultat :

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

Exemple de sortie du `Filter details` légale

Voici un exemple de sortie du `Filter details` dans le journal des résultats de trace, qui répertorie le style de sécurité efficace du système de fichiers contenant des fichiers et des dossiers qui correspondent aux critères de filtre :

```
Security Style: MIXED and ACL
```

Où trouver des informations complémentaires

Une fois que vous avez testé l'accès client SMB, vous pouvez effectuer une configuration SMB avancée ou ajouter un accès SAN. Après avoir testé l'accès client NFS avec succès, vous pouvez effectuer une configuration NFS avancée ou ajouter un accès SAN. Une fois les accès au protocole terminés, vous devez protéger le volume root du SVM.

Configuration SMB

Vous pouvez configurer davantage l'accès SMB à l'aide des éléments suivants :

- "Gestion SMB"

  Décrit la configuration et la gestion de l'accès aux fichiers à l'aide du protocole SMB.

- "Rapport technique NetApp 4191 : guide des meilleures pratiques pour les services de fichiers Windows dans clustered Data ONTAP 8.2"

  Fournit une brève présentation de l'implémentation SMB et d'autres fonctionnalités des services de fichiers Windows avec des recommandations et des informations de dépannage de base pour ONTAP.

- "Rapport technique NetApp 3740 : SMB 2 le protocole CIFS nouvelle génération dans Data ONTAP"

  Décrit les fonctionnalités, les détails de configuration et son implémentation de SMB 2 dans ONTAP.

Configuration NFS

Vous pouvez configurer davantage l'accès NFS à l'aide des éléments suivants :

- "Gestion NFS"

  Décrit comment configurer et gérer l'accès aux fichiers à l'aide du protocole NFS.

- "Rapport technique NetApp 4067 : Guide des meilleures pratiques et de mise en œuvre de NFS"

  Sert de guide opérationnel NFSv3 et NFSv4 et présente le système d'exploitation ONTAP avec un point sur NFSv4.

- "Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

  Fournit une liste complète des meilleures pratiques, limites, recommandations et considérations relatives à la configuration des fichiers LDAP, NIS, DNS et utilisateurs et groupes locaux à des fins d'authentification.

- "Rapport technique NetApp 4616 : NFS Kerberos dans ONTAP avec Microsoft Active Directory"
- "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"
- "Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"

  Décrit les meilleures pratiques à suivre lors de l'implémentation des composants NFSv4 sur des clients AIX, Linux ou Solaris reliés à des systèmes exécutant ONTAP.

Protection du volume racine

Après avoir configuré les protocoles sur le SVM, il faut s'assurer que son volume root est protégé :

- "Protection des données"

  Décrit la procédure de création d'un miroir de partage de charge pour protéger le volume racine du SVM, une pratique recommandée par NetApp pour les SVM compatibles avec NAS. Décrit également la procédure de restauration rapide en cas de défaillances ou de pertes de volumes en promouvant le volume racine du SVM à partir d'un miroir de partage de charge.

Gestion du chiffrement avec System Manager

Crypter les données stockées à l'aide du chiffrement logiciel

Utilisez le chiffrement de volume pour garantir que les données de volume ne peuvent pas être lues si le périphérique sous-jacent est requalifié, perdu ou volé. Le chiffrement de volume n'a pas besoin de disques spéciaux, il est compatible avec tous les disques durs et SSD.

Le chiffrement de volume requiert un gestionnaire de clés. Vous pouvez configurer le gestionnaire de clés intégré à l'aide de System Manager. Vous pouvez également utiliser un gestionnaire de clés externe, mais vous devez d'abord le configurer à l'aide de l'interface de ligne de commande de ONTAP.

Une fois le gestionnaire de clés configuré, les nouveaux volumes sont chiffrés par défaut.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Sous **Encryption**, cliquez sur ⚙ Pour configurer le gestionnaire de clés intégré pour la première fois.
3. Pour crypter les volumes existants, cliquez sur **Storage > volumes**.
4. Sur le volume souhaité, cliquez sur ⋮ Puis cliquez sur **Modifier**.
5. Sélectionnez **Activer le cryptage**.

Chiffrez les données stockées à l'aide de disques à autochiffrement

Le cryptage de disque garantit que toutes les données d'un niveau local ne peuvent pas être lues si l'équipement sous-jacent est requalifié, perdu ou volé. Le chiffrement de disque requiert des disques SSD ou des disques durs à autocryptage spéciaux.

Le chiffrement des disques requiert un gestionnaire de clés. Vous pouvez configurer le gestionnaire de clés intégré à l'aide de System Manager. Vous pouvez également utiliser un gestionnaire de clés externe, mais vous devez d'abord le configurer à l'aide de l'interface de ligne de commande de ONTAP.

Si ONTAP détecte des disques à autochiffrement, il vous invite à configurer le gestionnaire de clés intégré lorsque vous créez le niveau local.

Étapes

1. Sous **Encryption**, cliquez sur ⚙ pour configurer le gestionnaire de clés intégré.
2. Si vous voyez un message indiquant que les disques doivent faire l'objet d'un renouvellement de clés,

cliquez sur ⋮, Puis cliquez sur **Rekey Disks**.

Gestion du chiffrement via l'interface de ligne de commandes

Présentation du chiffrement NetApp

NetApp propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

- Le chiffrement logiciel associé à NetApp Volume Encryption (NVE) prend en charge le chiffrement des données sur un volume à la fois
- Le chiffrement matériel utilisant NetApp Storage Encryption (NSE) prend en charge le chiffrement de disque intégral (FDE) des données au moment de leur écriture.

Configurez NetApp Volume Encryption

Configurer la présentation de NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Une clé de chiffrement accessible uniquement au système de stockage garantit que les données du volume ne peuvent pas être lues si l'appareil sous-jacent est requalifié, perdu ou volé.

Présentation de NVE

Avec NVE, les métadonnées et les données (y compris les copies Snapshot) sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume. Un serveur de gestion externe des clés ou un gestionnaire de clés intégré (OKM) sert les clés pour les nœuds :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol). Il est recommandé de configurer des serveurs de gestion externe des clés sur un système de stockage différent de vos données.
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés aux nœuds du même système de stockage que vos données.

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe. La licence VE est incluse avec "ONTAP One". Lorsqu'un gestionnaire de clés externe ou intégré est configuré, la configuration du chiffrement des données au repos est modifiée pour les nouveaux agrégats et les nouveaux volumes. Par défaut, NetApp Aggregate Encryption (NAE) sera activé dans les nouveaux agrégats. Par défaut, les nouveaux volumes qui ne font pas partie d'un agrégat NAE ont sur lequel le chiffrement de volume NetApp (NVE) est activé. Lorsqu'un serveur SVM (Data Storage Virtual machine) est configuré avec son propre gestionnaire de clés à l'aide d'une gestion mutualisée des clés, alors le volume créé pour ce SVM est automatiquement configuré avec NVE.

Vous pouvez activer le chiffrement sur un volume nouveau ou existant. NVE prend en charge la gamme complète de fonctionnalités d'efficacité du stockage, notamment la déduplication et la compression. À partir de ONTAP 9.14.1, vous pouvez Activez NVE sur les volumes root du SVM existant.

> Si vous utilisez SnapLock, vous pouvez activer le chiffrement uniquement sur les nouveaux volumes SnapLock vides. Vous ne pouvez pas activer le chiffrement sur un volume SnapLock existant.

Vous pouvez utiliser NVE sur n'importe quel type d'agrégat (HDD, SSD, hybride, LUN de baie), avec n'importe quel type RAID et dans n'importe quelle implémentation ONTAP prise en charge, y compris ONTAP Select. Vous pouvez également utiliser NVE avec le chiffrement matériel pour « chiffrer » les données sur des disques à autochiffrement.

Lorsque NVE est activé, le « core dump » est également chiffré.

Chiffrement d'agrégat

En général, une clé unique est attribuée à chaque volume chiffré. Lorsque le volume est supprimé, la clé est supprimée.

Depuis ONTAP 9.6, il est possible d'utiliser *NetApp Aggregate Encryption (NAE)* pour attribuer des clés à l'agrégat contenant pour le chiffrement des volumes. Lors de la suppression d'un volume chiffré, les clés de l'agrégat sont préservées. Les clés sont supprimées si l'agrégat entier est supprimé.

Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. NVE ne prend cependant pas en charge la déduplication au niveau de l'agrégat.

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe.

Les volumes NVE et NAE peuvent coexister sur un même agrégat. Par défaut, les volumes NAE sont chiffrés avec un chiffrement au niveau des agrégats. Vous pouvez remplacer la valeur par défaut lorsque vous chiffrez le volume.

Vous pouvez utiliser le `volume move` Commande de conversion d'un volume NVE en volume NAE, et inversement. Vous pouvez répliquer un volume NAE sur un volume NVE.

Vous ne pouvez pas utiliser `secure purge` Commandes sur un volume NAE.

Quand utiliser des serveurs externes de gestion des clés

Bien qu'il soit moins coûteux et généralement plus pratique d'utiliser le gestionnaire de clés intégré, vous devez configurer des serveurs KMIP si les conditions suivantes sont vraies :

- Votre solution de gestion des clés de chiffrement doit être conforme à la norme FIPS 140-2 (Federal information Processing Standards) ou OASIS KMIP.
- Vous avez besoin d'une solution à plusieurs clusters et d'une gestion centralisée des clés de chiffrement.
- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

Champ d'application de la gestion externe des clés

Le périmètre de la gestion externe des clés détermine si les serveurs de gestion des clés sécurisent tous les SVM dans le cluster ou bien uniquement les SVM sélectionnés :

- Vous pouvez utiliser une *cluster scope* pour configurer la gestion des clés externe pour tous les SVM du cluster. L'administrateur du cluster a accès à chaque clé stockée sur les serveurs.

- Depuis ONTAP 9.6, vous pouvez utiliser une *SVM scope* pour configurer la gestion externe des clés pour une SVM nommée dans le cluster. C'est le mieux adapté aux environnements mutualisés dans lesquels chaque locataire utilise un autre SVM (ou ensemble de SVM) pour transmettre les données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire.
- Vous pouvez utiliser ONTAP 9.10.1 depuis Azure Key Vault et Google Cloud KMS Protection des clés NVE uniquement pour les SVM de données. Ce dernier est disponible pour le KMS d'AWS à partir de la version 9.12.0.

Vous pouvez utiliser les deux étendues du même cluster. Si les serveurs de gestion des clés ont été configurés pour un SVM, ONTAP utilise uniquement ces serveurs pour sécuriser les clés. Sinon, ONTAP sécurise les clés avec les serveurs de gestion des clés configurés pour le cluster.

Une liste de gestionnaires de clés externes validés est disponible dans le "Matrice d'interopérabilité NetApp (IMT)". Pour trouver cette liste, entrez le terme « gestionnaires de clés » dans la fonction de recherche de l'IMT.

Détails du support

Le tableau suivant présente les détails de la prise en charge de NVE :

Ressource ou fonctionnalité	Détails du support
Plateformes	Une fonctionnalité de déchargement AES-ni est requise. Consultez la page Hardware Universe (HWU) pour vérifier que NVE et NAE sont pris en charge pour votre plateforme.

Le cryptage	Depuis ONTAP 9.7, les volumes et les agrégats nouvellement créés sont chiffrés par défaut lorsque vous ajoutez une licence VE (Volume Encryption) et qu'un gestionnaire de clés intégré ou externe est configuré. Si vous devez créer un agrégat non chiffré, utilisez la commande suivante :
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Si vous avez besoin de créer un volume de texte brut, utilisez la commande suivante :
	
	`volume create -encrypt false`
	
	Le chiffrement n'est pas activé par défaut lorsque :
	
	• La licence VE n'est pas installée.
	• Le gestionnaire de clés n'est pas configuré.
	• La plateforme ou le logiciel ne prend pas en charge le chiffrement.
	• Le chiffrement matériel est activé.

ONTAP	Toutes les implémentations de ONTAP. La prise en charge de ONTAP Cloud est disponible dans ONTAP 9.5 et versions ultérieures.
Périphériques	HDD, SSD, hybride, LUN de baie.

RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Volumes de données et volumes root SVM existants. Il n'est pas possible de chiffrer des données sur des volumes de métadonnées MetroCluster. Dans les versions de ONTAP antérieures à 9.14.1, vous ne pouvez pas chiffrer les données sur le volume racine du SVM avec NVE. À partir de ONTAP 9.14.1, ONTAP prend en charge NVE sur les volumes root du SVM.
Chiffrement d'agrégat	Depuis la version ONTAP 9.6, NVE prend en charge le chiffrement au niveau des agrégats (NAE) : • Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. • Vous ne pouvez pas reKey un volume de chiffrement au niveau de l'agrégat. • La suppression sécurisée n'est pas prise en charge sur les volumes de chiffrement au niveau des agrégats. • Outre les volumes de données, NAE prend en charge le chiffrement des volumes root du SVM et du volume de métadonnées MetroCluster. NAE ne prend pas en charge le chiffrement du volume racine.
Étendue des SVM	Depuis ONTAP 9.6, NVE prend en charge le périmètre des SVM pour la gestion externe des clés uniquement, et non pour le gestionnaire de clés intégré. MetroCluster est pris en charge à partir de ONTAP 9.8.
Efficacité du stockage	Déduplication, compression, compaction, FlexClone. Les clones utilisent la même clé que le parent, même après le fractionnement du clone. Vous devez effectuer une `volume move` sur un clone divisé, après quoi le clone divisé aura une clé différente.
La réplication	• Pour la réplication de volume, les volumes source et de destination peuvent avoir des paramètres de chiffrement différents. Le chiffrement peut être configuré pour la source et non configuré pour la destination, et inversement. • Pour la réplication SVM, le volume de destination est automatiquement chiffré, sauf si le nœud de destination ne contient pas de nœud qui prend en charge le chiffrement de volume, dans ce cas la réplication réussit, mais le volume de destination n'est pas chiffré. • Dans le cas de configurations MetroCluster, chaque cluster extrait les clés de gestion externes des serveurs de clés configurés. Les clés OKM sont répliquées vers le site partenaire par le service de réplication de la configuration.
La conformité	Depuis ONTAP 9.2, SnapLock est pris en charge en mode conformité et entreprise pour les nouveaux volumes uniquement. Vous ne pouvez pas activer le chiffrement sur un volume SnapLock existant.

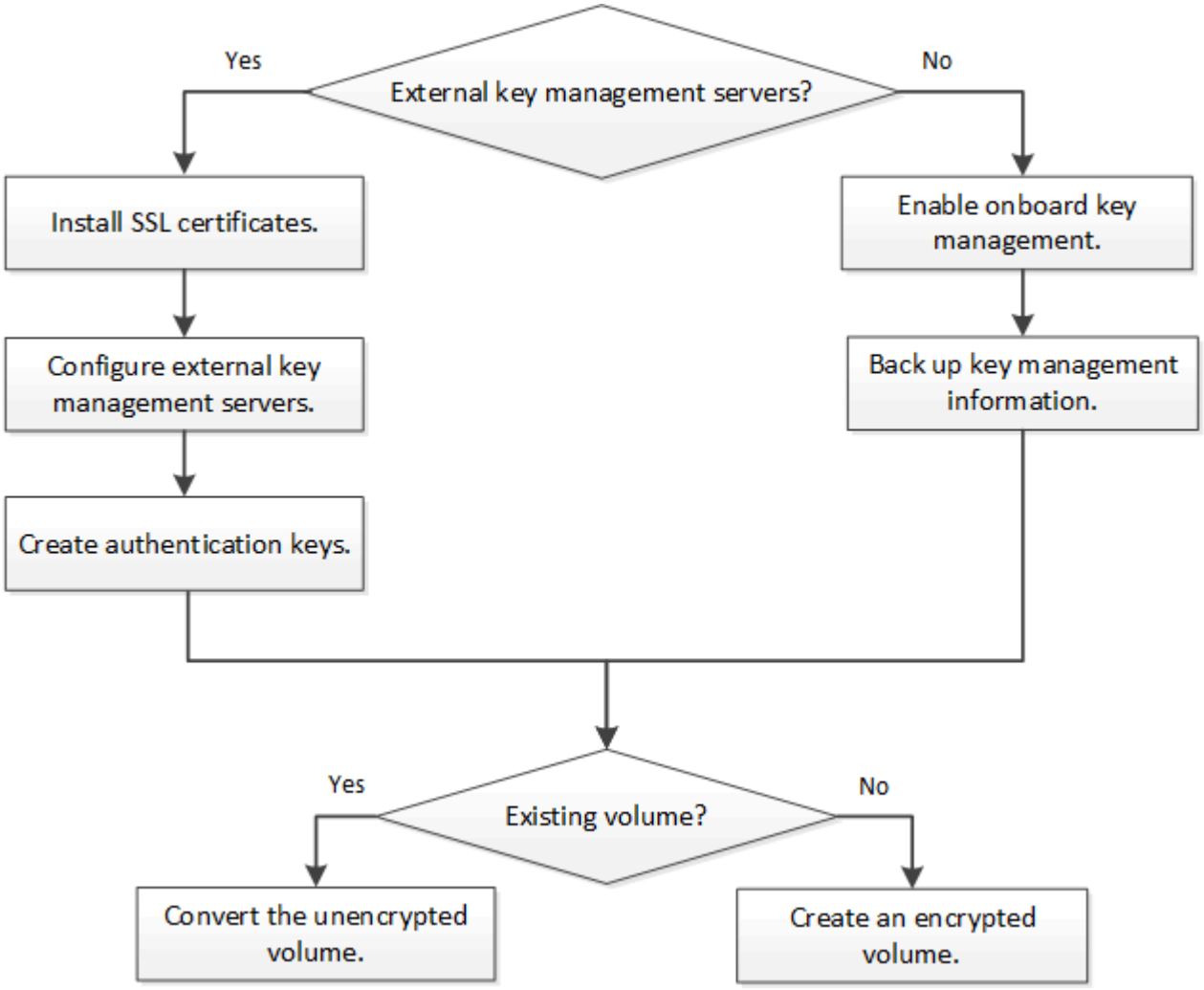
FlexGroups	FlexGroups est pris en charge à partir de ONTAP 9.2. Les agrégats de destination doivent être du même type que les agrégats source, au niveau des volumes ou de l'agrégat. ONTAP 9.5 prend en charge le renouvellement de clés des volumes FlexGroup sur place,
Transition depuis la version 7-mode	À partir de 7-mode transition Tool 3.3, vous pouvez utiliser l'interface de ligne de commandes de l'outil 7-mode transition Tool pour effectuer une transition basée sur les copies vers les volumes de destination NVE sur le système en cluster.

Informations associées

"FAQ : NetApp Volume Encryption et NetApp Aggregate Encryption"

Flux de travail NetApp Volume Encryption

Vous devez configurer les services de gestion des clés avant d'activer le chiffrement de volume. Vous pouvez activer le chiffrement sur un nouveau volume ou sur un volume existant.



"Vous devez installer la licence VE" Et configurez les services de gestion des clés avant de chiffrer les données avec NVE. Avant d'installer la licence, vous devriez "Déterminez si votre version de ONTAP prend en charge NVE".

Configurez NVE

Déterminez si votre version de cluster prend en charge NVE

Vous devez déterminer si votre version de cluster prend en charge NVE avant d'installer la licence. Vous pouvez utiliser le `version` pour déterminer la version du cluster.

Description de la tâche

La version en cluster est la version la plus basse d'ONTAP s'exécutant sur n'importe quel nœud du cluster.

Étape

1. Déterminez si votre version de cluster prend en charge NVE :

   ```
   version -v
   ```

   NVE n'est pas pris en charge si la sortie de la commande affiche le texte « 1Ono-DARE » (pour « pas de chiffrement des données au repos »), ou si vous utilisez une plateforme non répertoriée dans le "Détails du support".

   La commande suivante détermine si NVE est pris en charge sur `cluster1`.

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   La sortie de `1Ono-DARE` Indique que NVE n'est pas pris en charge sur la version du cluster.

Installez la licence

Une licence VE vous permet d'utiliser cette fonctionnalité sur tous les nœuds du cluster. Cette licence est requise avant de pouvoir chiffrer les données avec NVE. Il est inclus avec "ONTAP One".

Avant ONTAP One, la licence VE était incluse avec le pack de chiffrement. Le pack de chiffrement n'est plus proposé, mais reste valide. Bien qu'ils ne soient pas encore requis, les clients existants peuvent choisir de le faire "Passez à ONTAP One".

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez avoir reçu la clé de licence VE de votre représentant commercial ou avoir installé ONTAP One.

Étapes

1. "Vérifiez que la licence VE est installée".

   Le nom du package de licences VE est `VE`.

2. Si la licence n'est pas installée, "Utilisez System Manager ou l'interface de ligne de commandes ONTAP pour l'installer".

Configurer la gestion externe des clés en vue d'ensemble

Vous pouvez utiliser un ou plusieurs serveurs externes de gestion des clés pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Un serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).

> Pour ONTAP 9.1 et les versions antérieures, les LIFs de node-management doivent être attribuées à des ports configurés avec le rôle de node-management avant de pouvoir utiliser le gestionnaire de clés externe.

NetApp Volume Encryption (NVE) prend en charge le gestionnaire de clés intégré dans ONTAP 9.1 et les versions ultérieures. Depuis la version ONTAP 9.3, NVE prend en charge le protocole KMIP (externe Key Management) et le gestionnaire de clés intégré. À partir de ONTAP 9.10.1, vous pouvez l'utiliser Azure Key Vault ou Google Cloud Key Manager Service Pour protéger vos clés NVE. À partir de ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. Voir Configurez les serveurs de clés en cluster.

Gérez des gestionnaires de clés externes avec System Manager

À partir de la version ONTAP 9.7, vous pouvez stocker et gérer les clés d'authentification et de chiffrement à l'aide du gestionnaire de clés intégré. À partir de ONTAP 9.13.1, vous pouvez également utiliser des gestionnaires de clés externes pour stocker et gérer ces clés.

Le gestionnaire de clés intégré stocke et gère les clés dans une base de données sécurisée interne au cluster. L'étendue du cluster est celle-ci. Un gestionnaire de clés externe stocke et gère les clés à l'extérieur du cluster. Il peut s'agir du cluster ou de la VM de stockage. Un ou plusieurs gestionnaires de clés externes peuvent être utilisés. Les conditions suivantes s'appliquent :

- Si le gestionnaire de clés intégré est activé, un gestionnaire de clés externe ne peut pas être activé au niveau du cluster, mais il peut être activé au niveau de la VM de stockage.
- Si un gestionnaire de clés externe est activé au niveau du cluster, le gestionnaire de clés intégré ne peut pas être activé.

Lorsque vous utilisez des gestionnaires de clés externes, vous pouvez enregistrer jusqu'à quatre serveurs de clés principaux par machine virtuelle de stockage et par cluster. Chaque serveur de clés principal peut être mis en cluster avec jusqu'à trois serveurs de clés secondaires.

Configurez un gestionnaire de clés externe

Pour ajouter un gestionnaire de clés externe à une VM de stockage, il est conseillé d'ajouter une passerelle en option lors de la configuration de l'interface réseau de la VM de stockage. Si la machine virtuelle de stockage a été créée sans la route réseau, vous devrez créer la route explicitement pour le gestionnaire de clés externe. Voir "Créer une LIF (interface réseau)".

Étapes

Vous pouvez configurer un gestionnaire de clés externe à partir de différents emplacements dans System Manager.

1. Pour configurer un gestionnaire de clés externe, effectuez l'une des étapes de démarrage suivantes.

Flux de travail	Navigation	Étape de départ
Configurer le gestionnaire de clés	**Cluster** > **Paramètres**	Accédez à la section **sécurité**. Sous **cryptage**, sélectionnez ⚙. Sélectionnez **Gestionnaire de clés externe**.
Ajouter un niveau local	**Stockage** > **niveaux**	Sélectionnez **+ Ajouter un niveau local**. Cochez la case « configurer le gestionnaire de clés ». Sélectionnez **Gestionnaire de clés externe**.
Préparez le stockage	**Tableau de bord**	Dans la section **capacité**, sélectionnez **préparer le stockage**. Sélectionnez ensuite « configurer le gestionnaire de clés ». Sélectionnez **Gestionnaire de clés externe**.
Configuration du chiffrement (gestionnaire de clés dans le périmètre de la VM de stockage uniquement)	**Stockage** > **machines virtuelles de stockage**	Sélectionnez la VM de stockage. Sélectionnez l'onglet **Paramètres**. Dans la section **cryptage** sous **sécurité**, sélectionnez ⚙.

2. Pour ajouter un serveur de clés principal, sélectionnez + Add , Et renseignez les champs **adresse IP ou Nom d'hôte** et **Port**.
3. Les certificats installés existants sont répertoriés dans les champs **KMIP Server CA Certificates** et **KMIP client Certificate**. Vous pouvez effectuer l'une des actions suivantes :
   - Sélectionnez ⌄ pour sélectionner les certificats installés que vous souhaitez mapper au gestionnaire de clés. (Plusieurs certificats d'autorité de certification de service peuvent être sélectionnés, mais un seul certificat client peut être sélectionné.)
   - Sélectionnez **Ajouter un nouveau certificat** pour ajouter un certificat qui n'a pas encore été installé et le mapper au gestionnaire de clés externe.
   - Sélectionnez × en regard du nom du certificat pour supprimer les certificats installés que vous ne souhaitez pas mapper au gestionnaire de clés externe.
4. Pour ajouter un serveur de clés secondaire, sélectionnez **Ajouter** dans la colonne **Secondary Key Servers** et fournissez ses détails.
5. Sélectionnez **Enregistrer** pour terminer la configuration.

Modifier un gestionnaire de clés externe existant

Si vous avez déjà configuré un gestionnaire de clés externe, vous pouvez modifier ses paramètres.

Étapes

1. Pour modifier la configuration d'un gestionnaire de clés externe, effectuez l'une des étapes de démarrage suivantes.

Portée	Navigation	Étape de départ

Gestionnaire de clés externe de l'étendue du cluster	**Cluster** > **Paramètres**	Accédez à la section **sécurité**. Sous **cryptage**, sélectionnez ⋮, Puis sélectionnez **Modifier le gestionnaire de clés externe**.
Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe	**Stockage** > **machines virtuelles de stockage**	Sélectionnez la VM de stockage. Sélectionnez l'onglet **Paramètres**. Dans la section **cryptage** sous **sécurité**, sélectionnez ⋮, Puis sélectionnez **Modifier le gestionnaire de clés externe**.

2. Les serveurs de clés existants sont répertoriés dans le tableau **Key Servers**. Vous pouvez effectuer les opérations suivantes :
   - Ajoutez un nouveau serveur de clés en sélectionnant + Add .
   - Supprimez un serveur de clés en sélectionnant ⋮ à la fin de la cellule de la table qui contient le nom du serveur de clés. Les serveurs de clés secondaires associés à ce serveur de clés principal sont également supprimés de la configuration.

Supprimez un gestionnaire de clés externe

Un gestionnaire de clés externe peut être supprimé si les volumes sont non chiffrés.

Étapes

1. Pour supprimer un gestionnaire de clés externe, effectuez l'une des opérations suivantes.

Portée	Navigation	Étape de départ
Gestionnaire de clés externe de l'étendue du cluster	**Cluster** > **Paramètres**	Accédez à la section **sécurité**. Sous **cryptage**, sélectionnez SELECT ⋮, Puis sélectionnez **Supprimer le gestionnaire de clés externe**.
Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe	**Stockage** > **machines virtuelles de stockage**	Sélectionnez la VM de stockage. Sélectionnez l'onglet **Paramètres**. Dans la section **cryptage** sous **sécurité**, sélectionnez ⋮, Puis sélectionnez **Supprimer le gestionnaire de clés externe**.

Migration des clés entre les gestionnaires de clés

Lorsque plusieurs gestionnaires de clés sont activés sur un cluster, les clés doivent être migrées d'un gestionnaire de clés vers un autre. System Manager effectue automatiquement ce processus.

- Si le gestionnaire de clés intégré ou un gestionnaire de clés externe est activé au niveau du cluster et que certains volumes sont chiffrés, Ensuite, lorsque vous configurez un gestionnaire de clés externe au niveau de la VM de stockage, les clés doivent être migrées du gestionnaire de clés intégré ou du gestionnaire de clés externe au niveau du cluster vers le gestionnaire de clés externe au niveau de la VM de stockage. System Manager effectue automatiquement ce processus.
- Si les volumes ont été créés sans chiffrement sur une machine virtuelle de stockage, les clés n'ont pas besoin d'être migrées.

Installez les certificats SSL sur le cluster

Le cluster et le serveur KMIP utilisent des certificats SSL KMIP pour vérifier l'identité de l'autre et établir une connexion SSL. Avant de configurer la connexion SSL avec le serveur KMIP, vous devez installer les certificats SSL du client KMIP pour le cluster et le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.

Description de la tâche

Dans une paire haute disponibilité, les deux nœuds doivent utiliser les mêmes certificats SSL publics et privés KMIP. Si vous connectez plusieurs paires haute disponibilité au même serveur KMIP, tous les nœuds des paires haute disponibilité doivent utiliser les mêmes certificats SSL publics et privés.

Avant de commencer

- L'heure doit être synchronisée sur le serveur qui crée les certificats, le serveur KMIP et le cluster.
- Vous devez avoir obtenu le certificat public du client SSL KMIP pour le cluster.
- Vous devez avoir obtenu la clé privée associée au certificat client SSL KMIP pour le cluster.
- Le certificat client SSL KMIP ne doit pas être protégé par un mot de passe.
- Vous devez avoir obtenu le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.
- Dans un environnement MetroCluster, vous devez installer les mêmes certificats SSL KMIP sur les deux clusters.

> Vous pouvez installer les certificats client et serveur sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

Étapes

1. Installez les certificats client SSL KMIP pour le cluster :

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Vous êtes invité à entrer les certificats SSL KMIP publics et privés.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Installez le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP :

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Gestion externe des clés dans ONTAP 9.6 et versions ultérieures (NVE)

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Depuis ONTAP 9.6, il est possible de configurer un gestionnaire de clés externe distinct pour sécuriser les clés utilisées par un SVM de données pour accéder aux données chiffrées.

À partir de ONTAP 9.11.1, vous pouvez ajouter jusqu'à 3 serveurs de clés secondaires par serveur de clés principal pour créer un serveur de clés en cluster. Pour plus d'informations, voir Configurez les serveurs de clés externes en cluster.

Description de la tâche

Vous pouvez connecter jusqu'à quatre serveurs KMIP à un cluster ou un SVM. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

Le périmètre de la gestion externe des clés détermine si les serveurs de gestion des clés sécurisent tous les SVM dans le cluster ou bien uniquement les SVM sélectionnés :

- Vous pouvez utiliser une *cluster scope* pour configurer la gestion des clés externe pour tous les SVM du cluster. L'administrateur du cluster a accès à chaque clé stockée sur les serveurs.
- Depuis ONTAP 9.6, vous pouvez utiliser une *SVM scope* pour configurer la gestion externe des clés pour une SVM de données dans le cluster. C'est le mieux adapté aux environnements mutualisés dans lesquels chaque locataire utilise un autre SVM (ou ensemble de SVM) pour transmettre les données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire.
- Pour les environnements mutualisés, installez une licence pour *MT_EK_MGMT* à l'aide de la commande suivante :

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

Vous pouvez utiliser les deux étendues du même cluster. Si les serveurs de gestion des clés ont été configurés pour un SVM, ONTAP utilise uniquement ces serveurs pour sécuriser les clés. Sinon, ONTAP sécurise les clés avec les serveurs de gestion des clés configurés pour le cluster.

Vous pouvez configurer la gestion intégrée des clés au niveau du cluster et la gestion externe des clés au niveau de SVM. Vous pouvez utiliser le `security key-manager key migrate` Commande pour migrer les clés de la gestion intégrée des clés au périmètre du cluster vers des gestionnaires de clés externes au périmètre des SVM

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Si vous souhaitez activer la gestion externe des clés dans un environnement MetroCluster, MetroCluster doit être entièrement configuré avant d'activer la gestion externe des clés.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

Étapes

1. Configurer la connectivité du gestionnaire de clés pour le cluster :

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

- Le `security key-manager external enable` la commande remplace le `security key-manager setup` commande. Si vous exécutez la commande à l'invite de connexion du cluster, *`admin_SVM`* Par défaut au SVM admin du cluster actuel. Vous devez être l'administrateur du cluster pour configurer le périmètre du cluster. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés.
- Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour le SVM admin, vous devez répéter l'opération `security key-manager external enable` commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour `cluster1` avec trois serveurs de clés externes. Le premier serveur de clés est spécifié à l'aide de son nom d'hôte et de son port, le second est spécifié à l'aide d'une adresse IP et du port par défaut, et le troisième est spécifié à l'aide d'une adresse et d'un port IPv6 :

```
clusterl::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Configurer un SVM gestionnaire de clés :

```
security key-manager external enable -vserver SVM -key-servers
host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

- Si vous exécutez la commande à l'invite de connexion du SVM, `SVM` Par défaut au SVM actuel On doit être un administrateur de cluster ou de SVM pour configurer le cadre de la SVM. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés.
- Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour une SVM de données, vous n'avez pas besoin de répéter le `security key-manager external enable` commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour `svm1` avec un serveur à une seule clé qui écoute le port par défaut 5696 :

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Répétez la dernière étape pour tout SVM supplémentaire.

> Vous pouvez également utiliser le `security key-manager external add-servers` Commande permettant de configurer des SVM supplémentaires Le `security key-manager external add-servers` la commande remplace le `security key-manager add` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

4. Vérifiez que tous les serveurs KMIP configurés sont connectés :

   `security key-manager external show-status -node node_name`

   > Le `security key-manager external show-status` la commande remplace le `security key-manager show -status` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> security key-manager external show-status

   Node  Vserver  Key Server                                       Status
   ----  -------  ----------------------------------------
   -------------
   node1
         svm1
                  keyserver.svm1.com:5696                          available
         cluster1
                  10.0.0.10:5696                                   available
                  fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
                  ks1.local:15696                                  available
   node2
         svm1
                  keyserver.svm1.com:5696                          available
         cluster1
                  10.0.0.10:5696                                   available
                  fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
                  ks1.local:15696                                  available

   8 entries were displayed.
   ```

5. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

   `volume encryption conversion start`

   Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

Activez la gestion externe des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre

serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

Description de la tâche

ONTAP configure la connectivité du serveur KMIP pour tous les nœuds du cluster.

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

Étapes

1. Configurer la connectivité du gestionnaire de clés pour les nœuds du cluster :

   `security key-manager setup`

   La configuration du gestionnaire de clés démarre.

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

2. Entrez la réponse appropriée à chaque invite.
3. Ajoutez un serveur KMIP :

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

5. Vérifiez que tous les serveurs KMIP configurés sont connectés :

   `security key-manager show -status`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

   ```
   volume encryption conversion start
   ```

   Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

Gérer les clés avec un fournisseur cloud

À partir de ONTAP 9.10.1, vous pouvez l'utiliser "Azure Key Vault (AKV)" et "Service de gestion des clés (KMS cloud) de Google Cloud Platform" Pour protéger vos clés de chiffrement ONTAP dans une application hébergée dans le cloud. À partir de ONTAP 9.12.0, vous pouvez également protéger les clés NVE avec "KMS D'AWS".

Vous pouvez utiliser AWS KMS, AKV et Cloud KMS pour protéger les données "Clés NetApp Volume Encryption (NVE)" Uniquement pour les SVM de données.

Description de la tâche

La gestion des clés avec un fournisseur cloud peut être activée via l'interface de ligne de commandes ou l'API REST ONTAP.

Lorsque vous utilisez un fournisseur cloud pour protéger vos clés, sachez que par défaut, une LIF de SVM de données communique avec le terminal de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification du fournisseur cloud (login.microsoftonline.com pour Azure ; oauth2.googleapis.com pour le Cloud KMS). Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Lorsque vous utilisez un service de gestion des clés de fournisseur cloud, vous devez connaître les limites suivantes :

- La gestion des clés du fournisseur cloud n'est pas disponible pour le chiffrement du stockage NetApp (NSE) et le chiffrement d'agrégat NetApp (NAE). "KMIP externes" peut être utilisé à la place.
- La gestion des clés du fournisseur cloud n'est pas disponible pour les configurations MetroCluster.
- La gestion des clés du fournisseur cloud peut uniquement être configurée sur un SVM de données.

Avant de commencer

- Vous devez avoir configuré le KMS sur le fournisseur cloud approprié.
- Les nœuds du cluster ONTAP doivent prendre en charge NVE.
- "Vous devez avoir installé les licences Volume Encryption (VE) et MTEKM (Encryption Key Management)

multitenant". Ces licences sont incluses avec "ONTAP One".

- Vous devez être administrateur du cluster ou du SVM.
- La SVM de données ne doit pas inclure de volumes chiffrés ni utiliser un gestionnaire de clés. Si le SVM de données inclut des volumes chiffrés, vous devez les migrer avant de configurer le KMS.

Activez la gestion externe des clés

L'activation de la gestion externe des clés dépend du gestionnaire de clés que vous utilisez. Choisissez l'onglet du gestionnaire de clés et de l'environnement appropriés.

AWS

Avant de commencer

- Vous devez créer un octroi pour la clé KMS AWS qui sera utilisée par le rôle IAM gérant le chiffrement. Le rôle IAM doit inclure une politique permettant les opérations suivantes :
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

  Pour plus d'informations, consultez la documentation AWS pour "subventions".

Activez AWS KMV sur un SVM ONTAP

1. Avant de commencer, procurez-vous l'ID de clé d'accès et la clé secrète sur votre serveur KMS AWS.
2. Définissez le niveau de privilège sur avancé :
   `set -priv advanced`
3. Activer AWS KMS :
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Lorsque vous y êtes invité, entrez la clé secrète.
5. Vérifiez que le KMS AWS a été correctement configuré :
   `security key-manager external aws show -vserver` *`svm_name`*

Azure

Activez Azure Key Vault sur un SVM ONTAP

1. Avant de commencer, vous devez obtenir les informations d'authentification appropriées à partir de votre compte Azure, soit un secret client, soit un certificat.
   Vous devez également vous assurer que tous les nœuds du cluster fonctionnent correctement. Vous pouvez le vérifier à l'aide de la commande `cluster show`.
2. Définissez le niveau privilégié sur avancé
   `set -priv advanced`
3. Activation de AKV sur le SVM
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   Lorsque vous y êtes invité, entrez le certificat client ou le secret client de votre compte Azure.
4. Vérifiez que la fonction AKV est activée correctement :
   `security key-manager external azure show vserver` *`svm_name`*
   Si l'accessibilité du service n'est pas OK, établir la connectivité au service de gestion des clés AKV via la LIF du SVM de données.

Google Cloud

Activez le serveur KMS cloud sur une SVM ONTAP

1. Avant de commencer, procurez-vous la clé privée du fichier de clé de compte Google Cloud KMS au format JSON. Elles sont disponibles dans votre compte GCP.
   Vous devez également vous assurer que tous les nœuds du cluster fonctionnent correctement. Vous pouvez le vérifier à l'aide de la commande `cluster show`.

2. Définir le niveau privilégié sur avancé :
   `set -priv advanced`
3. Activation du KMS cloud sur le SVM
   `security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
   Lorsque vous y êtes invité, entrez le contenu du fichier JSON avec la clé privée du compte de service
4. Vérifiez que Cloud KMS est configuré avec les paramètres appropriés :
   `security key-manager external gcp show vserver` *`svm_name`*
   Le statut de `kms_wrapped_key_status` sera le cas "`UNKNOWN`" si aucun volume chiffré n'a été créé.
   Si la accessibilité du service n'est pas satisfaisante, établissez la connectivité au service de gestion des clés GCP via LIF du SVM de données.

Si un ou plusieurs volumes chiffrés sont déjà configurés pour un SVM de données et que les clés NVE correspondantes sont gérées par le gestionnaire de clés intégré des SVM d'administration, ces clés doivent être migrées vers le service externe de gestion des clés. Pour ce faire via l'interface de ligne de commandes, lancer la commande :
`security key-manager key migrate -from-Vserver` *`admin_SVM`* `-to-Vserver` *`data_SVM`*
Il n'est pas possible de créer de nouveaux volumes chiffrés pour le SVM de données du locataire tant que toutes les clés NVE du SVM de données ne sont pas migrées correctement.

Informations associées

- "Chiffrez les volumes avec les solutions de chiffrement NetApp pour Cloud Volumes ONTAP"

Intégrez la gestion des clés dans ONTAP 9.6 et versions ultérieures (NVE)

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque à chiffrement automatique.

Description de la tâche

Vous devez exécuter le `security key-manager onboard sync` commande à chaque ajout d'un nœud au cluster.

Si vous avez une configuration MetroCluster, vous devez exécuter `security key-manager onboard enable` d'abord sur le cluster local, puis exécutez le `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'entre eux. Lorsque vous exécutez le `security key-manager onboard enable` à partir du cluster local, puis effectuez une synchronisation sur le cluster distant. vous n'avez pas besoin d'exécuter le `enable` commandez à nouveau à partir du cluster distant.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. Vous pouvez utiliser le `cc-mode-enabled=yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `cc-mode-enabled=yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier

`-encrypt-destination true`.

Lors de la configuration du chiffrement des données ONTAP au repos, pour répondre aux exigences relatives aux solutions commerciales pour les données classées (CSfC), vous devez utiliser NSE avec NVE et vous assurer que le gestionnaire de clés intégré est activé en mode critères communs. Reportez-vous à la "Description de la solution CSFC" Pour en savoir plus sur CSfC.

Lorsque le gestionnaire de clés intégré est activé en mode critères communs (`cc-mode-enabled=yes`), le comportement du système est modifié de l'une des manières suivantes :

- Le système surveille les tentatives consécutives de mot de passe de cluster ayant échoué lorsqu'il fonctionne en mode critères communs.

  Si vous ne saisissez pas la phrase secrète appropriée au démarrage, les volumes chiffrés ne sont pas montés. Pour corriger cette situation, vous devez redémarrer le nœud et saisir la phrase secrète correcte du cluster. Une fois démarré, le système peut saisir jusqu'à 5 tentatives consécutives de saisie de la phrase secrète du cluster dans une période de 24 heures pour toute commande nécessitant une phrase secrète comme paramètre. Si la limite est atteinte (par exemple, vous n'avez pas saisi correctement la phrase de passe du cluster 5 fois de suite) alors vous devez attendre l'expiration du délai de 24 heures ou redémarrer le nœud pour réinitialiser la limite.

- Les mises à jour d'images système utilisent le certificat de signature de code NetApp RSA-3072 avec des digests signés SHA-384 pour vérifier l'intégrité de l'image au lieu du certificat de signature de code RSA-2048 NetApp habituel et des digests signés par code SHA-256.

  La commande de mise à niveau vérifie que le contenu de l'image n'a pas été modifié ou corrompu en vérifiant diverses signatures numériques. Le processus de mise à jour de l'image passe à l'étape suivante si la validation réussit ; sinon, la mise à jour de l'image échoue. Voir la `cluster image` pour plus d'informations sur les mises à jour système.

Le gestionnaire de clés intégré stocke les clés dans la mémoire volatile. Le contenu de la mémoire volatile est effacé lors du redémarrage ou de l'arrêt du système. Dans des conditions de fonctionnement normales, le contenu de la mémoire volatile est effacé dans les 30 secondes lorsqu'un système est arrêté.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer le gestionnaire de clés intégré.

Étapes

1. Lancez la configuration du gestionnaire de clés :

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

> Réglez `cc-mode-enabled=yes` pour demander aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `cc-mode-enabled=yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Le `- cc-mode-enabled` Cette option n'est pas prise en charge dans les configurations MetroCluster. Le `security key-manager onboard enable` la commande remplace le `security key-manager setup` commande.

L'exemple suivant démarre la commande Key Manager setup sur cluster1 sans exiger la saisie de la phrase de passe après chaque redémarrage :

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

> Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

3. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
4. Vérifiez que les clés d'authentification ont été créées :

```
security key-manager key query -key-type NSE-AK
```

> Le `security key-manager key query` la commande remplace le `security key-manager query key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                Key Type Encryption   Restored

-----------------------------------  -------- ------------ --------

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

   `volume encryption conversion start`

   Le gestionnaire de clés intégré doit être entièrement configuré avant de convertir les volumes. Dans un environnement MetroCluster, le gestionnaire de clés intégré doit être configuré sur les deux sites.

Une fois que vous avez terminé

Copiez la phrase secrète dans un emplacement sécurisé à l'extérieur du système de stockage pour une utilisation ultérieure.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir "Sauvegardez manuellement les informations intégrées de gestion des clés".

Gestion intégrée des clés dans ONTAP 9.5 et versions antérieures (NVE)

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.

Description de la tâche

Vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Si vous disposez d'une configuration MetroCluster, consultez les consignes suivantes :

- Dans ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local et `security key-manager setup -sync-metrocluster-config yes` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Avant ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local, attendez environ 20 secondes, puis exécutez `security key-manager setup` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier `-encrypt-destination true`.

> Après une tentative de phrase de passe, vous devez redémarrer le nœud.

Avant de commencer

- Si vous utilisez NSE ou NVE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données du gestionnaire de clés externe.

  "Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer le gestionnaire de clés intégré.

Étapes

1. Lancez la configuration du gestionnaire de clés :

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option permettant aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées.

   L'exemple suivant commence à configurer le gestionnaire de clés sur le cluster 1 sans que la phrase de passe ne soit saisie après chaque redémarrage :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Entrez `yes` à l'invite, configurez la gestion intégrée des clés.
3. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

> Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

4. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
5. Vérifier que les clés sont configurées pour tous les nœuds :

   `security key-manager key show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

   ```
   volume encryption conversion start
   ```

   Le gestionnaire de clés intégré doit être entièrement configuré avant de convertir les volumes. Dans un environnement MetroCluster, le gestionnaire de clés intégré doit être configuré sur les deux sites.

Une fois que vous avez terminé

Copiez la phrase secrète dans un emplacement sécurisé à l'extérieur du système de stockage pour une utilisation ultérieure.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir "Sauvegardez manuellement les informations intégrées de gestion des clés".

Activez la gestion intégrée des clés dans les nouveaux nœuds ajoutés

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.

> Pour ONTAP 9.5 et les versions antérieures, vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.
>
> Pour ONTAP 9.6 et versions ultérieures, vous devez exécuter le `security key-manager sync` commande à chaque ajout d'un nœud au cluster.
>
> Si vous ajoutez un nœud à un cluster dont la gestion intégrée des clés est configurée, vous exécutez cette commande pour actualiser les clés manquantes.

Si vous disposez d'une configuration MetroCluster, consultez les consignes suivantes :

- Avec ONTAP 9.6, vous devez exécuter `security key-manager onboard enable` sur le cluster local, puis s'exécute `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Dans ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local et `security key-manager setup -sync-metrocluster-config yes` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Avant ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local, attendez environ 20 secondes, puis exécutez `security key-manager setup` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier `-encrypt-destination true`.

Après une tentative de phrase de passe, vous devez redémarrer le nœud.

Chiffrement des données de volume avec NVE

Chiffrement des données de volume avec NVE

Depuis ONTAP 9.7, le chiffrement de l'agrégat et du volume est activé par défaut lorsque vous disposez de la licence VE et de la gestion intégrée ou externe des clés. Pour ONTAP 9.6 et version antérieure, vous pouvez activer le chiffrement sur un nouveau volume ou sur un volume existant. Vous devez avoir installé la licence VE et activé la gestion des clés avant de pouvoir activer le chiffrement de volume. NVE est conforme à la norme FIPS-140-2 de niveau 1.

Chiffrement au niveau de l'agrégat avec licence VE

Depuis la version ONTAP 9.7, les nouveaux agrégats et volumes créés sont chiffrés par défaut lorsque vous disposez de "Licence VE" et une gestion intégrée ou externe des clés. Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de chiffrer les volumes.

Description de la tâche

Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. NVE ne prend cependant pas en charge la déduplication au niveau de l'agrégat.

Un agrégat activé pour le chiffrement au niveau de l'agrégat est appelé agrégat *NAE* (pour le chiffrement d'agrégat NetApp). Tous les volumes d'un agrégat NAE doivent être chiffrés avec un chiffrement NAE ou NVE. Grâce au chiffrement au niveau des agrégats, les volumes que vous créez dans l'agrégat sont chiffrés avec un chiffrement NAE par défaut. Vous pouvez remplacer le par défaut pour utiliser le chiffrement NVE.

Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Activer ou désactiver le chiffrement au niveau des agrégats :

Pour…	Utilisez cette commande…
Créez un agrégat NAE avec ONTAP 9.7 ou version ultérieure	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Créez un agrégat NAE avec ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

Conversion d'un agrégat non-NAE en agrégat NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Conversion d'un agrégat NAE en agrégat non-NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante active le chiffrement au niveau de l'agrégat sur `aggr1`:

- ONTAP 9.7 ou version ultérieure :

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 ou version antérieure :

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Vérifier que l'agrégat est activé pour le chiffrement :

   `storage aggregate show -fields encrypt-with-aggr-key`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante vérifie que `aggr1` est activé pour le chiffrement :

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Une fois que vous avez terminé

Exécutez le `volume create` commande permettant de créer les volumes chiffrés.

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

Activer le chiffrement sur un nouveau volume

Vous pouvez utiliser le `volume create` commande permettant d'activer le chiffrement

sur un nouveau volume.

Description de la tâche

Vous pouvez chiffrer les volumes à l'aide de NetApp Volume Encryption (NVE) et, à partir de ONTAP 9.6, NetApp Aggregate Encryption (NAE). Pour en savoir plus sur NAE et NVE, consultez le présentation du chiffrement de volume.

La procédure d'activation du chiffrement sur un nouveau volume dans ONTAP varie en fonction de la version de ONTAP que vous utilisez et de votre configuration spécifique :

- À partir de ONTAP 9.4, si vous l'activez `cc-mode` Lorsque vous configurez le gestionnaire de clés intégré, les volumes que vous créez avec le `volume create` la commande est automatiquement chiffrée, que vous spécifiez ou non `-encrypt true`.
- Dans ONTAP 9.6 et les versions antérieures, vous devez utiliser `-encrypt true` avec `volume create` commandes permettant d'activer le chiffrement (à condition que vous n'ayez pas activé `cc-mode`).
- Si vous voulez créer un volume NAE dans ONTAP 9.6, vous devez activer NAE au niveau des agrégats. Reportez-vous à la section Activation du chiffrement au niveau de l'agrégat avec la licence VE pour plus de détails sur cette tâche.
- Depuis la version ONTAP 9.7, les nouveaux volumes créés sont chiffrés par défaut lorsque vous disposez de "Licence VE" et une gestion intégrée ou externe des clés. Par défaut, les nouveaux volumes créés dans un agrégat NAE seront de type NAE plutôt que NVE.
  - Dans ONTAP 9.7 et versions ultérieures, si vous ajoutez `-encrypt true` à la `volume create` Commande de création d'un volume dans un agrégat NAE, au lieu de NAE pour le volume le chiffrement NVE. Tous les volumes d'un agrégat NAE doivent être chiffrés avec NVE ou NAE.

> Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

Étapes

1. Créez un nouveau volume et spécifiez si le chiffrement est activé sur le volume. Si le nouveau volume se trouve dans un agrégat NAE, le volume en est par défaut un volume NAE :

Pour créer…	Utilisez cette commande…
Volume NAE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Un volume NVE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + Dans les versions ONTAP 9.6 et antérieures, où NAE n'est pas pris en charge, `-encrypt true` Spécifie que le volume doit être chiffré avec NVE. Dans ONTAP 9.7 et versions ultérieures, où les volumes sont créés dans des agrégats NAE, `-encrypt true` Remplace le type de chiffrement par défaut de NAE pour créer un volume NVE.
Volume de texte brut	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

Pour obtenir la syntaxe complète de la commande, reportez-vous à la page de référence de la commande LINK:https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html[`volume create`^].

2. Vérifiez que les volumes sont activés pour le chiffrement :

   ```
   volume show -is-encrypted true
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous au "référence de commande".

Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de chiffrement d'un nœud, ONTAP « transmet automatiquement » une clé de chiffrement au serveur lorsque vous chiffrez un volume.

=
:allow-uri-read:

Activez le chiffrement sur un volume existant

Vous pouvez utiliser le `volume move start` ou le `volume encryption conversion start` commande permettant d'activer le chiffrement sur un volume existant.

Description de la tâche

- Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption conversion start` commande permettant de chiffrer un volume existant « à la place », sans avoir à déplacer le volume vers un autre emplacement. Vous pouvez également utiliser le `volume move start` commande.
- Pour ONTAP 9.2 et les versions antérieures, vous pouvez utiliser uniquement le `volume move start` commande permettant d'activer le chiffrement en déplaçant un volume existant.

Activez le chiffrement sur un volume existant à l'aide de la commande Volume Encryption conversion start

Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption conversion start` commande permettant de chiffrer un volume existant « à la place », sans avoir à déplacer le volume vers un autre emplacement.

Une fois que vous avez lancé une opération de conversion, elle doit être terminée. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption conversion pause` commande pour mettre l'opération en pause, et le `volume encryption conversion resume` commande pour reprendre l'opération.

> Vous ne pouvez pas utiliser `volume encryption conversion start` Pour convertir un volume SnapLock.

Étapes

1. Activer le chiffrement sur un volume existant :

   ```
   volume encryption conversion start -vserver SVM_name -volume volume_name
   ```

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante active le chiffrement sur un volume existant `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

Le système crée une clé de chiffrement pour le volume. Les données du volume sont chiffrées.

2. Vérifiez l'état de l'opération de conversion :

   `volume encryption conversion show`

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche le statut de l'opération de conversion :

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ---------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Une fois l'opération de conversion terminée, vérifiez que le volume est activé pour le chiffrement :

   `volume show -is-encrypted true`

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

Activez le chiffrement sur un volume existant à l'aide de la commande volume Move start

Vous pouvez utiliser le `volume move start` commande permettant d'activer le chiffrement en déplaçant un volume existant. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Vous pouvez utiliser le même agrégat ou un autre agrégat.

Description de la tâche

- Vous pouvez utiliser ONTAP 9.8 depuis `volume move start` Pour activer le chiffrement sur un volume SnapLock ou FlexGroup.

- Depuis ONTAP 9.4, si vous activez « cc-mode » lors de la configuration du gestionnaire de clés intégré, les volumes que vous créez avec le système `volume move start` la commande est automatiquement chiffrée. Vous n'avez pas besoin de spécifier `-encrypt-destination true`.
- Depuis ONTAP 9.6, il est possible d'utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de déplacer les volumes. Un volume chiffré avec une clé unique est appelé *volume NVE* (ce qui signifie qu'il utilise le chiffrement de volume NetApp). Un volume chiffré avec une clé au niveau de l'agrégat est appelé un volume NAE_ (pour le chiffrement d'agrégat NetApp). Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.
- À partir de ONTAP 9.14.1, vous pouvez chiffrer un volume root SVM avec NVE. Pour plus d'informations, voir Configurer le chiffrement de volume NetApp sur un volume root SVM.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche, ou un administrateur de SVM à qui l'administrateur du cluster a délégué des pouvoirs.

"Délégation d'autorité pour exécuter la commande de déplacement de volume"

Étapes

1. Déplacez un volume existant et spécifiez si le chiffrement est activé sur le volume :

Pour convertir…	Utilisez cette commande…
Volume en texte brut vers un volume NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
Un volume NVE ou en texte clair vers un volume NAE (en supposant que le chiffrement au niveau de l'agrégat est activé sur la destination)	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
Un volume NAE vers un volume NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
Volume NAE en volume en texte brut	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
Un volume NVE vers un volume en texte brut	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante convertit un volume en texte brut nommé `vol1` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

En supposant que le chiffrement au niveau de l'agrégat soit activé sur la destination, la commande suivante convertit un volume NVE ou en texte brut nommé `vol1` Pour un volume NAE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

La commande suivante convertit un volume NAE nommé `vol2` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NAE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NVE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Afficher le type de chiffrement des volumes du cluster :

   `volume show -fields encryption-type none|volume|aggregate`

   Le `encryption-type` Ce champ est disponible dans ONTAP 9.6 et versions ultérieures.

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche le type de cryptage des volumes dans `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Vérifiez que les volumes sont activés pour le chiffrement :

   `volume show -is-encrypted true`

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche les volumes chiffrés sur `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de chiffrement d'un nœud, ONTAP transmet automatiquement une clé de chiffrement au serveur lorsque vous chiffrez un volume.

Configurer le chiffrement de volume NetApp sur un volume root SVM

À partir de la version ONTAP 9.14.1, vous pouvez activer NetApp Volume Encryption (NVE) sur un volume racine de machine virtuelle de stockage (SVM). Avec NVE, le volume racine est chiffré avec une clé unique, pour renforcer la sécurité au niveau du SVM.

Description de la tâche

NVE sur un volume root SVM ne peut être activé qu'une fois le SVM créé.

Avant de commencer

- Le volume racine du SVM ne doit pas se trouver sur un agrégat chiffré avec le chiffrement d'agrégat NetApp (NAE).
- Vous devez avoir activé le chiffrement avec Onboard Key Manager ou un gestionnaire de clés externe.
- Vous devez exécuter ONTAP 9.14.1 ou une version ultérieure.
- Pour migrer un SVM contenant un volume racine chiffré avec NVE, vous devez convertir le volume racine du SVM en volume texte brut une fois la migration terminée, puis re-chiffrer le volume racine du SVM.
  - Si l'agrégat de destination de la migration du SVM utilise NAE, le volume racine hérite de NAE par défaut.
- Si la SVM est dans une relation de SVM DR :
  - Les paramètres de chiffrement d'un SVM en miroir ne sont pas copiés vers la destination. Si vous activez NVE sur la source ou la destination, vous devez activer NVE séparément sur le volume racine du SVM en miroir.
  - Si tous les agrégats du cluster de destination utilisent NAE, le volume racine du SVM utilisera NAE.

Étapes

Vous pouvez activer NVE sur un volume root SVM via l'interface de ligne de commandes ONTAP ou System Manager.

CLI

Vous pouvez activer NVE sur le volume racine du SVM sans déplacement ou en déplaçant le volume entre les agrégats.

Chiffrez le volume racine sur place

1. Convertir le volume root en volume chiffré :

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Confirmez que le chiffrement a réussi. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

Chiffrer le volume root du SVM en le déplaçant

1. Lancer un déplacement de volume :

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   Pour plus d'informations sur `volume move`, voir Déplacer un volume.

2. Confirmez le `volume move` l'opération a réussi avec le `volume move show` commande. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

System Manager

1. Accédez à **stockage** > **volumes**.
2. En regard du nom du volume root du SVM à chiffrer, sélectionner ⋮ Puis **Modifier**.
3. Sous l'en-tête **stockage et optimisation**, sélectionnez **Activer le cryptage**.
4. Sélectionnez **Enregistrer**.

Activer le chiffrement de volume racine de nœud

Depuis ONTAP 9.8, vous pouvez utiliser NetApp Volume Encryption pour protéger le volume racine de votre nœud.

Description de la tâche

Cette procédure s'applique au volume racine du nœud. Elle ne s'applique pas aux volumes root du SVM. Les volumes root des SVM peuvent être protégés via le chiffrement au niveau des agrégats et À partir de ONTAP 9.14.1, NVE.

Une fois le chiffrement du volume racine démarré, il doit être terminé. Vous ne pouvez pas interrompre l'opération. Une fois le cryptage terminé, vous ne pouvez pas attribuer de nouvelle clé au volume racine et vous ne pouvez pas effectuer de suppression sécurisée.

Avant de commencer

- Votre système doit utiliser une configuration haute disponibilité.
- Le volume racine du nœud doit déjà être créé.
- Votre système doit disposer d'un gestionnaire de clés intégré ou d'un serveur de gestion des clés externe à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Étapes

1. Chiffrer le volume root :

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. Vérifiez l'état de l'opération de conversion :

   ```
   volume encryption conversion show
   ```

3. Une fois l'opération de conversion terminée, vérifiez que le volume est crypté :

   ```
   volume show -fields
   ```

   Voici un exemple de sortie pour un volume chiffré.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

Configuration du chiffrement matériel NetApp

Configuration de la présentation de NetApp Hardware-based Encryption

Le chiffrement matériel NetApp prend en charge le chiffrement de disque intégral (FDE) des données au fur et à mesure de leur écriture. Les données ne peuvent pas être lues si une clé de chiffrement est stockée sur le micrologiciel. La clé de chiffrement, à son tour, n'est accessible qu'à un nœud authentifié.

Présentation du cryptage matériel NetApp

Un nœud s'authentifie auprès d'un disque auto-chiffré à l'aide d'une clé d'authentification extraite d'un serveur de gestion externe des clés ou d'un gestionnaire de clés intégré :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol). Il est recommandé de configurer des serveurs de gestion externe des clés sur un système de stockage différent de vos données.
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données.

Vous pouvez utiliser NetApp Volume Encryption avec chiffrement matériel pour « paramétrer la fonctionnalité de chiffrement » des données sur des disques à autochiffrement.

Lorsque les disques à chiffrement automatique sont activés, le « core dump » est également chiffré.

> Si une paire haute disponibilité utilise des disques avec cryptage SAS ou NVMe (SED, NSE, FIPS), vous devez suivre les instructions de la rubrique Retour d'un lecteur FIPS ou SED en mode non protégé Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Types de disques à autocryptage pris en charge

Deux types de disques à autocryptage sont pris en charge :

- Tous les systèmes FAS et AFF prennent en charge les disques SAS ou NVMe certifiés FIPS avec le chiffrement automatique. Ces unités, appelées unités *FIPS,* sont conformes aux exigences de la publication 140-2 de la norme fédérale de traitement des informations, niveau 2. Les fonctionnalités certifiées permettent d'ajouter des protections au chiffrement, comme la prévention d'attaques par déni de service sur le disque. Les disques FIPS ne peuvent pas être combinés avec d'autres types de disques sur le même nœud ou la même paire HA.
- Depuis ONTAP 9.6, les disques NVMe à autocryptage n'ayant pas encore été testés FIPS sont pris en charge sur des systèmes AFF A800, A320 et versions ultérieures. Ces disques, appelés *SED*, offrent les mêmes fonctionnalités de cryptage que les disques FIPS, mais peuvent être combinés avec des disques sans cryptage sur un même nœud ou une paire haute disponibilité.
- Tous les disques validés FIPS utilisent un module cryptographique de firmware qui a été validé par FIPS. Le module cryptographique du lecteur FIPS n'utilise aucune clé générée en dehors du disque (la phrase de passe d'authentification entrée dans le lecteur est utilisée par le module cryptographique du firmware du disque pour obtenir une clé de chiffrement).

> Les disques sans chiffrement sont des disques qui ne sont pas des disques SED ou FIPS.

> Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

Quand utiliser la gestion externe des clés

Le gestionnaire de clés intégré est moins coûteux et généralement plus pratique, mais vous devez utiliser une gestion externe des clés si l'un des éléments suivants est vrai :

- La stratégie de votre entreprise nécessite une solution de gestion des clés qui utilise un module cryptographique FIPS 140-2 de niveau 2 (ou supérieur).
- Vous avez besoin d'une solution à plusieurs clusters et d'une gestion centralisée des clés de chiffrement.
- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

Détails du support

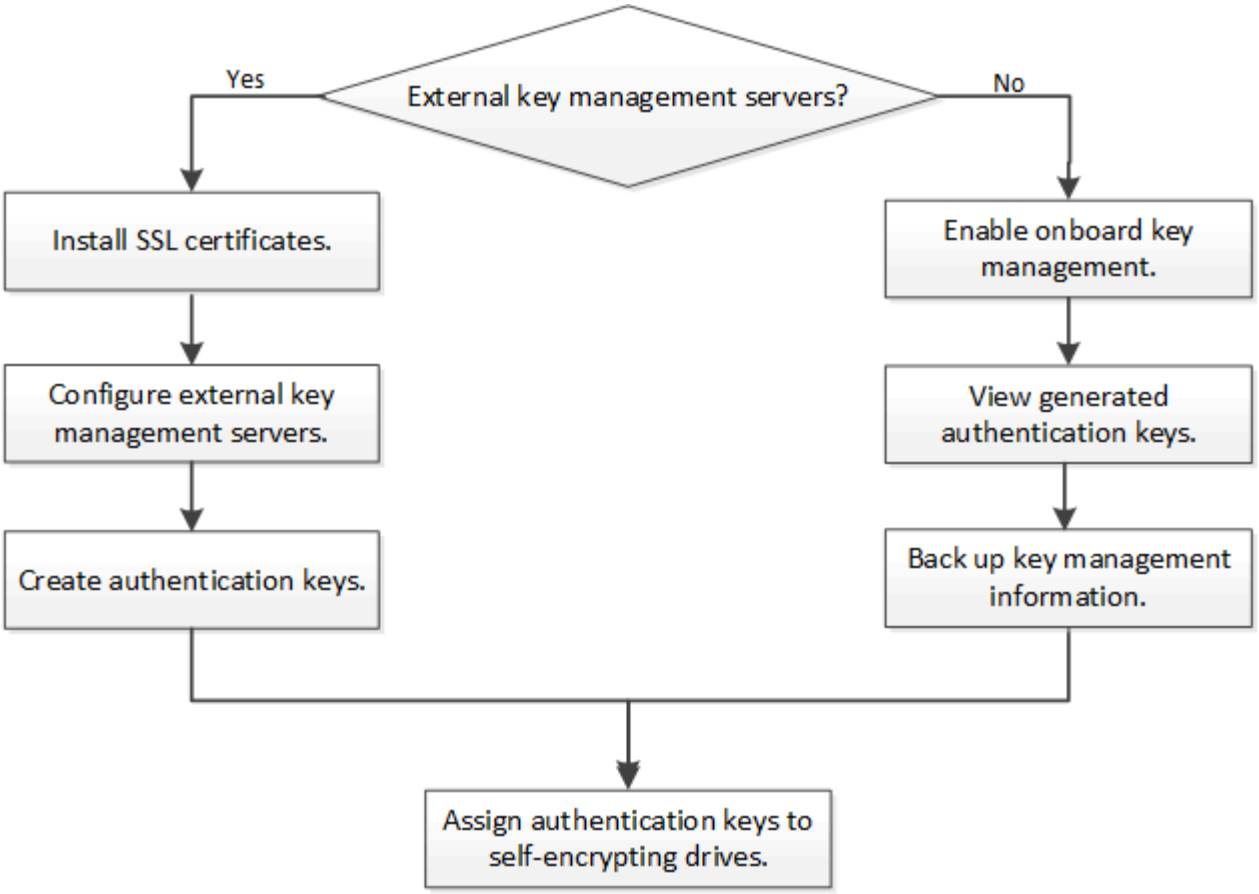
Le tableau suivant présente des détails importants sur la prise en charge du chiffrement matériel. Consultez la matrice d'interopérabilité pour obtenir les dernières informations sur les serveurs, les systèmes de stockage et les tiroirs disques KMIP pris en charge.

Ressource ou fonctionnalité	Détails du support

Jeux de disques non homogènes	• Les disques FIPS ne peuvent pas être combinés avec d'autres types de disques sur le même nœud ou la même paire HA. Les paires haute disponibilité conformes peuvent coexister avec des paires haute disponibilité non conformes dans le même cluster. • Les disques SED peuvent être combinés avec des disques sans cryptage sur un même nœud ou une même paire haute disponibilité.
Type de disque	• Les disques FIPS peuvent être des disques SAS ou NVMe. • Les disques SED doivent être des disques NVMe.
Interfaces réseau de 10 Go	Depuis ONTAP 9.3, les configurations de gestion des clés KMIP prennent en charge des interfaces réseau de 10 Gbit pour les communications avec des serveurs de gestion des clés externes.
Ports de communication avec le serveur de gestion des clés	Depuis ONTAP 9.3, vous pouvez utiliser n'importe quel port du contrôleur de stockage pour la communication avec le serveur de gestion des clés. Dans le cas contraire, vous devez utiliser le port e0M pour la communication avec les serveurs de gestion des clés. Selon le modèle du contrôleur de stockage, certaines interfaces réseau peuvent ne pas être disponibles durant le processus de démarrage pour la communication avec les serveurs de gestion des clés.
MetroCluster (MCC)	• Les disques NVMe prennent en charge MCC. • Les disques SAS ne prennent pas en charge MCC.

Flux de production de cryptage matériel

Vous devez configurer les services de gestion des clés pour que le cluster puisse s'authentifier sur le disque auto-chiffré. Vous pouvez utiliser un serveur de gestion externe des clés ou un gestionnaire de clés intégré.



Informations associées

- "NetApp Hardware Universe"
- "NetApp Volume Encryption et chiffrement d'agrégat NetApp"

Configurez la gestion externe des clés

Configurer la gestion externe des clés en vue d'ensemble

Vous pouvez utiliser un ou plusieurs serveurs externes de gestion des clés pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Un serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Pour ONTAP 9.1 et les versions antérieures, les LIFs de node-management doivent être attribuées à des ports configurés avec le rôle de node-management avant de pouvoir utiliser le gestionnaire de clés externe.

NetApp Volume Encryption (NVE) peut être implémenté avec le gestionnaire de clés intégré dans ONTAP 9.1 et les versions ultérieures. Dans ONTAP 9.3 et versions ultérieures, NVE peut être implémenté avec une gestion des clés externe (KMIP) et un gestionnaire de clés intégré. À partir de ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. Voir Configurez les serveurs de clés en cluster.

Collectez des informations réseau dans ONTAP 9.2 et versions antérieures

Si vous utilisez ONTAP 9.2 ou une version antérieure, vous devez remplir la fiche de configuration du réseau avant d'activer la gestion externe des clés.

> Depuis ONTAP 9.3, le système détecte automatiquement toutes les informations réseau nécessaires.

Élément	Remarques	Valeur
Nom de l'interface réseau de gestion des clés		
Adresse IP de l'interface réseau de gestion des clés	Adresse IP de la LIF de node management, au format IPv4 ou IPv6	
Longueur du préfixe réseau IPv6 de gestion des clés	Si vous utilisez IPv6, la longueur du préfixe réseau IPv6	
Masque de sous-réseau de l'interface réseau de gestion des clés		
Adresse IP de la passerelle d'interface réseau de gestion des clés		
Adresse IPv6 pour l'interface réseau du cluster	Requis uniquement si vous utilisez IPv6 pour l'interface réseau de gestion des clés	
Numéro de port pour chaque serveur KMIP	Facultatif. Le numéro de port doit être le même pour tous les serveurs KMIP. Si vous ne fournissez pas de numéro de port, il prend par défaut le port 5696, qui est le port attribué par Internet Numbers Authority (IANA) pour KMIP.	
Nom de la balise clé	Facultatif. Le nom de la balise clé est utilisé pour identifier toutes les clés appartenant à un nœud. Le nom de la balise par défaut est le nom du nœud.	

Informations associées

"Rapport technique NetApp 3954 : exigences et procédures de préinstallation pour IBM Tivoli Lifetime Key Manager pour NetApp Storage Encryption"

"Rapport technique NetApp 4074 : exigences et procédures de préinstallation pour NetApp Storage Encryption pour SafeNet KeySecure"

Installez les certificats SSL sur le cluster

Le cluster et le serveur KMIP utilisent des certificats SSL KMIP pour vérifier l'identité de l'autre et établir une connexion SSL. Avant de configurer la connexion SSL avec le serveur KMIP, vous devez installer les certificats SSL du client KMIP pour le cluster et le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.

Description de la tâche

Dans une paire haute disponibilité, les deux nœuds doivent utiliser les mêmes certificats SSL publics et privés KMIP. Si vous connectez plusieurs paires haute disponibilité au même serveur KMIP, tous les nœuds des paires haute disponibilité doivent utiliser les mêmes certificats SSL publics et privés.

Avant de commencer

- L'heure doit être synchronisée sur le serveur qui crée les certificats, le serveur KMIP et le cluster.
- Vous devez avoir obtenu le certificat public du client SSL KMIP pour le cluster.
- Vous devez avoir obtenu la clé privée associée au certificat client SSL KMIP pour le cluster.
- Le certificat client SSL KMIP ne doit pas être protégé par un mot de passe.
- Vous devez avoir obtenu le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.
- Dans un environnement MetroCluster, vous devez installer les mêmes certificats SSL KMIP sur les deux clusters.

> Vous pouvez installer les certificats client et serveur sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

Étapes

1. Installez les certificats client SSL KMIP pour le cluster :

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Vous êtes invité à entrer les certificats SSL KMIP publics et privés.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Installez le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP :

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Activation de la gestion externe des clés dans ONTAP 9.6 et versions ultérieures (basée sur le matériel)

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

À partir de ONTAP 9.11.1, vous pouvez ajouter jusqu'à 3 serveurs de clés secondaires par serveur de clés principal pour créer un serveur de clés en cluster. Pour plus d'informations, voir Configurez les serveurs de clés externes en cluster.

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

Étapes

1. Configurer la connectivité du gestionnaire de clés pour le cluster :

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > - Le `security key-manager external enable` la commande remplace le `security key-manager setup` commande. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.
   > - Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour le SVM admin, vous devez répéter l'opération `security key-manager external enable` commande sur le cluster partenaire.

   La commande suivante active la gestion externe des clés pour `cluster1` avec trois serveurs de clés externes. Le premier serveur de clés est spécifié à l'aide de son nom d'hôte et de son port, le second est spécifié à l'aide d'une adresse IP et du port par défaut, et le troisième est spécifié à l'aide d'une adresse et d'un port IPv6 :

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Vérifiez que tous les serveurs KMIP configurés sont connectés :

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

   > Le `security key-manager external show-status` la commande remplace le `security key-manager show -status` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Activez la gestion externe des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

Description de la tâche

ONTAP configure la connectivité du serveur KMIP pour tous les nœuds du cluster.

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

Étapes

1. Configurer la connectivité du gestionnaire de clés pour les nœuds du cluster :

   ```
   security key-manager setup
   ```

   La configuration du gestionnaire de clés démarre.

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

2. Entrez la réponse appropriée à chaque invite.

3. Ajoutez un serveur KMIP :

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

5. Vérifiez que tous les serveurs KMIP configurés sont connectés :

   `security key-manager show -status`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      -----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

   `volume encryption conversion start`

   Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

Configurez les serveurs de clés externes en cluster

À partir de ONTAP 9.11.1, il est possible de configurer la connectivité aux serveurs de gestion externe des clés en cluster sur un SVM. Avec des serveurs de clés en cluster, vous pouvez désigner des serveurs de clés principaux et secondaires sur une SVM. Lors

de l'enregistrement des clés, ONTAP essaie d'abord d'accéder à un serveur de clés principal avant de tenter d'accéder aux serveurs secondaires de manière séquentielle jusqu'à ce que l'opération s'effectue correctement, ce qui évite la duplication des clés.

Les serveurs de clés externes peuvent être utilisés pour les clés NSE, NVE, NAE et SED. Un SVM peut prendre en charge jusqu'à quatre principaux serveurs KMIP externes. Chaque serveur principal peut prendre en charge jusqu'à trois serveurs de clés secondaires.

Avant de commencer

- "La gestion des clés KMIP doit être activée pour le SVM".
- Ce processus prend uniquement en charge les serveurs de clés qui utilisent KMIP. Pour obtenir la liste des serveurs de clés pris en charge, reportez-vous à la "Matrice d'interopérabilité NetApp".
- Tous les nœuds du cluster doivent exécuter ONTAP 9.11.1 ou une version ultérieure.
- L'ordre des serveurs répertorie les arguments dans `-secondary-key-servers` Paramètre correspond à l'ordre d'accès des serveurs de gestion externe des clés (KMIP).

Créer un serveur de clés mis en cluster

La procédure de configuration varie selon que vous avez configuré ou non un serveur de clés principal.

Ajout de serveurs de clés primaires et secondaires à un SVM

1. Vérifier qu'aucune gestion des clés n'a été activée pour le cluster :
   `security key-manager external show -vserver` *`svm_name`*
   Si le SVM possède déjà le maximum de quatre serveurs de clés principaux activés, vous devez supprimer l'un des serveurs de clés principaux existants avant d'en ajouter un nouveau.
2. Activez le gestionnaire de clés principal :
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Ajoutez des serveurs de clés secondaires à un serveur de clés principal existant

1. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Pour plus d'informations sur les serveurs de clés secondaires, reportez-vous à la section [mod-secondary].

Modifier les serveurs de clés en cluster

Vous pouvez modifier les clusters de serveurs de clés externes en modifiant l'état (principal ou secondaire) de

serveurs de clés spécifiques, en ajoutant et en supprimant des serveurs de clés secondaires ou en modifiant l'ordre d'accès des serveurs de clés secondaires.

Conversion des serveurs de clés principaux et secondaires

Pour convertir un serveur de clés principal en serveur de clés secondaire, vous devez d'abord le supprimer de la SVM avec le `security key-manager external remove-servers` commande.

Pour convertir un serveur de clés secondaire en serveur de clés principal, vous devez d'abord supprimer le serveur de clés secondaire de son serveur de clés principal existant. Voir [mod-secondary]. Si vous convertissez un serveur de clés secondaire en serveur principal lors de la suppression d'une clé existante, toute tentative d'ajout d'un nouveau serveur avant la suppression et la conversion peut entraîner la duplication des clés.

Modifier les serveurs de clés secondaires

Les serveurs de clés secondaires sont gérés à l'aide du `-secondary-key-servers` paramètre du `security key-manager external modify-server` commande. Le `-secondary-key-servers` le paramètre accepte une liste séparée par des virgules. L'ordre spécifié des serveurs de clés secondaires dans la liste détermine la séquence d'accès des serveurs de clés secondaires. L'ordre d'accès peut être modifié en exécutant la commande `security key-manager external modify-server` les serveurs de clés secondaires étant entrés dans une séquence différente.

Pour supprimer un serveur de clés secondaire, le `-secondary-key-servers` les arguments doivent inclure les serveurs clés que vous voulez conserver lors de l'omission de celui à supprimer. Pour supprimer tous les serveurs de clés secondaires, utilisez l'argument `-`, indiquant aucun.

Pour plus d'informations, reportez-vous au `security key-manager external` dans le "Référence de commande ONTAP".

Créez des clés d'authentification dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser le `security key-manager key create` Commande permettant de créer les clés d'authentification d'un nœud et de les stocker sur les serveurs KMIP configurés.

Description de la tâche

Si votre configuration de sécurité exige que vous utilisiez des clés différentes pour l'authentification des données et l'authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d'elles. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que pour l'accès aux données.

ONTAP crée des clés d'authentification pour tous les nœuds du cluster.

- Cette commande n'est pas prise en charge lorsque le gestionnaire de clés intégré est activé. Toutefois, deux clés d'authentification sont créées automatiquement lorsque le gestionnaire de clés intégré est activé. Les clés peuvent être affichées à l'aide de la commande suivante :

  ```
  security key-manager key query -key-type NSE-AK
  ```

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.
- Vous pouvez utiliser le `security key-manager key delete` commande permettant de supprimer les

clés inutilisées. Le `security key-manager key delete` La commande échoue si la clé donnée est actuellement utilisée par ONTAP. (Vous devez avoir des privilèges supérieurs à « admin » pour utiliser cette commande.)

> Dans un environnement MetroCluster, avant de supprimer une clé, veillez à ce que cette clé ne soit pas utilisée sur le cluster partenaire. Vous pouvez utiliser les commandes suivantes sur le cluster partenaire pour vérifier que la clé n'est pas utilisée :
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

   > Réglage `prompt-for-key=true` provoque l'invite de l'administrateur de cluster à utiliser la phrase secrète lors de l'authentification de disques cryptés. Dans le cas contraire, le système génère automatiquement une phrase de passe de 32 octets. Le `security key-manager key create` la commande remplace le `security key-manager create-key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant crée les clés d'authentification pour `cluster1`, génération automatique d'une phrase de passe de 32 octets :

   ```
   cluster1::> security key-manager key create
   Key ID:
   000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

2. Vérifiez que les clés d'authentification ont été créées :

   ```
   security key-manager key query -node node
   ```

   > Le `security key-manager key query` la commande remplace le `security key-manager query key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

   L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Création de clés d’authentification dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser le `security key-manager create-key` Commande permettant de créer les clés d’authentification d’un nœud et de les stocker sur les serveurs KMIP configurés.

Description de la tâche

Si votre configuration de sécurité exige que vous utilisiez des clés différentes pour l’authentification des données et l’authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d’elles. Si ce n’est pas le cas, vous pouvez utiliser la même clé d’authentification pour la conformité FIPS que celle utilisée pour l’accès aux données.

ONTAP crée des clés d’authentification pour tous les nœuds du cluster.

- Cette commande n’est pas prise en charge lorsque la gestion intégrée des clés est activée.

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.

  Vous pouvez utiliser le logiciel du serveur de gestion des clés pour supprimer toutes les clés inutilisées, puis exécuter de nouveau la commande.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

   `security key-manager create-key`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

   L'exemple suivant crée les clés d'authentification pour `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Vérifiez que les clés d'authentification ont été créées :

   `security key-manager query`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)

Vous pouvez utiliser le `storage encryption disk modify` Commande permettant d'attribuer une clé d'authentification de données à un lecteur FIPS ou SED. Les nœuds de cluster utilisent cette clé pour verrouiller ou déverrouiller des données chiffrées sur le disque.

Description de la tâche

Un disque à chiffrement automatique est protégé contre tout accès non autorisé uniquement si son ID de clé d'authentification est défini sur une valeur autre que celle par défaut. L'ID sécurisé du fabricant (MSID), qui possède l'ID de clé 0x0, est la valeur par défaut standard des lecteurs SAS. Pour les disques NVMe, la valeur standard par défaut est une clé nulle, représentée sous forme d'ID de clé vierge. Lorsque vous attribuez l'ID de clé à un disque auto-crypté, le système remplace son ID de clé d'authentification par une valeur autre que celle par défaut.

Cette procédure n'est pas perturbatrice.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Attribuez une clé d'authentification de données à un lecteur FIPS ou SED :

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous pouvez utiliser le `security key-manager query -key-type NSE-AK` Commande permettant d'afficher les ID de clés.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Vérifiez que les clés d'authentification ont été attribuées :

   `storage encryption disk show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```

Configurez la gestion intégrée des clés

Activez la gestion intégrée des clés dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser le gestionnaire de clés intégré pour authentifier les nœuds de cluster sur un lecteur FIPS ou SED. Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données. Le gestionnaire de clés intégré est conforme à la norme FIPS-140-2 de niveau 1.

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.

Description de la tâche

Vous devez exécuter le `security key-manager onboard enable` commande à chaque ajout d'un nœud au cluster. Dans les configurations MetroCluster, vous devez exécuter `security key-manager onboard enable` sur le cluster local, puis s'exécute `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. Sauf dans MetroCluster, vous pouvez utiliser `cc-mode-enabled=yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Lorsque le gestionnaire de clés intégré est activé en mode critères communs (`cc-mode-enabled=yes`), le comportement du système est modifié de l'une des manières suivantes :

- Le système surveille les tentatives consécutives de mot de passe de cluster ayant échoué lorsqu'il fonctionne en mode critères communs.

  Si NetApp Storage Encryption (NSE) est activé et que vous ne saisissez pas la phrase secrète appropriée au démarrage, le système ne peut pas s'authentifier sur ses disques et redémarre automatiquement. Pour corriger ce problème, vous devez saisir la phrase secrète correcte du cluster à l'invite de démarrage. Une fois démarré, le système peut saisir jusqu'à 5 tentatives consécutives de saisie de la phrase secrète du cluster dans une période de 24 heures pour toute commande nécessitant une phrase secrète comme paramètre. Si la limite est atteinte (par exemple, vous n'avez pas saisi correctement la phrase de passe du cluster 5 fois de suite) alors vous devez attendre l'expiration du délai de 24 heures ou redémarrer le nœud pour réinitialiser la limite.

- Les mises à jour d'images système utilisent le certificat de signature de code NetApp RSA-3072 avec des digests signés SHA-384 pour vérifier l'intégrité de l'image au lieu du certificat de signature de code RSA-2048 NetApp habituel et des digests signés par code SHA-256.

  La commande de mise à niveau vérifie que le contenu de l'image n'a pas été modifié ou corrompu en vérifiant diverses signatures numériques. Le processus de mise à jour de l'image passe à l'étape suivante si la validation réussit ; sinon, la mise à jour de l'image échoue. Pour plus d'informations sur les mises à jour du système, reportez-vous à la page de manuel « image du cluster ».

Le gestionnaire de clés intégré stocke les clés dans la mémoire volatile. Le contenu de la mémoire volatile est effacé lors du redémarrage ou de l'arrêt du système. Dans des conditions de fonctionnement normales, le contenu de la mémoire volatile est effacé dans les 30 secondes lorsqu'un système est arrêté.

Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe.

  "Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant que le gestionnaire de clés intégré ne soit configuré.

Étapes

1. Lancez la commande de configuration du gestionnaire de clés :

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

> Réglez `cc-mode-enabled=yes` pour demander aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Le `- cc-mode-enabled` Cette option n'est pas prise en charge dans les configurations MetroCluster. Le `security key-manager onboard enable` la commande remplace le `security key-manager setup` commande.

L'exemple suivant démarre la commande Key Manager setup sur cluster1 sans exiger la saisie de la phrase de passe après chaque redémarrage :

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

> Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

3. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
4. Vérifiez que les clés d'authentification ont été créées :

```
security key-manager key query -node node
```

> Le `security key-manager key query` la commande remplace le `security key-manager query key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Une fois que vous avez terminé

Copiez la phrase secrète dans un emplacement sécurisé à l'extérieur du système de stockage pour une utilisation ultérieure.

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster. Vous devez également sauvegarder les informations manuellement pour les utiliser en cas d'incident.

Activez la gestion intégrée des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser le gestionnaire de clés intégré pour authentifier les nœuds de cluster sur un lecteur FIPS ou SED. Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données. Le gestionnaire de clés intégré est conforme à la norme FIPS-140-2 de niveau 1.

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un volume chiffré ou à un disque auto-chiffré.

Description de la tâche

Vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Si vous disposez d'une configuration MetroCluster, consultez les consignes suivantes :

- Dans ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local et `security key-manager setup -sync-metrocluster-config yes` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Avant ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local, attendez environ 20 secondes, puis exécutez `security key-manager setup` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier `-encrypt-destination true`.

> Après une tentative de phrase de passe, vous devez redémarrer le nœud.

Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe.

  "Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant que le gestionnaire de clés intégré ne soit configuré.

Étapes

1. Lancez la configuration du gestionnaire de clés :

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option permettant aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées.

   L'exemple suivant commence à configurer le gestionnaire de clés sur le cluster 1 sans que la phrase de passe ne soit saisie après chaque redémarrage :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Entrez `yes` à l'invite, configurez la gestion intégrée des clés.
3. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

> Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

4. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
5. Vérifier que les clés sont configurées pour tous les nœuds :

   `security key-manager key show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Une fois que vous avez terminé

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir "Sauvegardez manuellement les informations intégrées de gestion des clés".

Attribution d'une clé d'authentification des données à un lecteur FIPS ou SED (gestion des clés intégrée)

Vous pouvez utiliser le `storage encryption disk modify` Commande permettant d'attribuer une clé d'authentification de données à un lecteur FIPS ou SED. Les nœuds de cluster utilisent cette clé pour accéder aux données du disque.

Description de la tâche

Un disque à chiffrement automatique est protégé contre tout accès non autorisé uniquement si son ID de clé d'authentification est défini sur une valeur autre que celle par défaut. L'ID sécurisé du fabricant (MSID), qui possède l'ID de clé 0x0, est la valeur par défaut standard des lecteurs SAS. Pour les disques NVMe, la valeur standard par défaut est une clé nulle, représentée sous forme d'ID de clé vierge. Lorsque vous attribuez l'ID de clé à un disque auto-crypté, le système remplace son ID de clé d'authentification par une valeur autre que celle par défaut.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Attribuez une clé d'authentification de données à un lecteur FIPS ou SED :

   ```
   storage encryption disk modify -disk disk_ID -data-key-id key_ID
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous pouvez utiliser le `security key-manager key query -key-type NSE-AK` Commande permettant d'afficher les ID de clés.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Vérifiez que les clés d'authentification ont été attribuées :

   ```
   storage encryption disk show
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Attribuez une clé d'authentification FIPS 140-2 à un disque FIPS

Vous pouvez utiliser le `storage encryption disk modify` commande avec `-fips -key-id` Option permettant d'attribuer une clé d'authentification FIPS 140-2 à un disque FIPS. Les nœuds de cluster utilisent cette clé pour des opérations autres que l'accès aux données, comme empêcher les attaques de déni de service sur le disque.

Description de la tâche

Votre configuration de sécurité peut nécessiter l'utilisation de clés différentes pour l'authentification des données et l'authentification FIPS 140-2-2. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que celle utilisée pour l'accès aux données.

Cette procédure n'est pas perturbatrice.

Avant de commencer

Le firmware du disque doit prendre en charge la conformité à la norme FIPS 140-2-2. Le "Matrice d'interopérabilité NetApp" contient des informations sur les versions de micrologiciel de lecteur prises en charge.

Étapes

1. Vous devez d'abord vous assurer que vous avez attribué une clé d'authentification des données. Pour ce faire, utilisez un gestionnaire de clés externe ou un gestionnaire de clés intégré. Vérifiez que la clé est affectée à la commande `storage encryption disk show`.
2. Attribution d'une clé d'authentification FIPS 140-2 aux disques SED :

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

3. Vérifiez que la clé d'authentification a été attribuée :

   `storage encryption disk show -fips`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
--------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Activez le mode compatible FIPS au niveau du cluster pour les connexions de serveurs KMIP

Vous pouvez utiliser le `security config modify` commande avec `-is-fips-enabled` Option permettant d'activer le mode conforme à la norme FIPS au niveau du cluster pour les données en transit. Cela force le cluster à utiliser OpenSSL en mode FIPS lors de la connexion à des serveurs KMIP.

Description de la tâche

Lorsque vous activez le mode cluster compatible FIPS, le cluster n'utilise automatiquement que les suites de chiffrement conformes à la norme TLS1.2 et FIPS. Le mode conforme à la norme FIPS à l'échelle du cluster est désactivé par défaut.

Vous devez redémarrer manuellement les nœuds du cluster après avoir modifié la configuration de sécurité à l'échelle du cluster.

Avant de commencer

- Le contrôleur de stockage doit être configuré en mode conforme à la norme FIPS.
- Tous les serveurs KMIP doivent prendre en charge TLSv1.2. Le système nécessite TLSv1.2 pour terminer la connexion au serveur KMIP lorsque le mode conforme FIPS à l'échelle du cluster est activé.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifiez que TLSv1.2 est pris en charge :

```
security config show -supported-protocols
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Activer le mode compatible FIPS à l'échelle du cluster :

```
security config modify -is-fips-enabled true -interface SSL
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

4. Redémarrez les nœuds du cluster manuellement.
5. Vérifiez que le mode compatible FIPS à l'échelle du cluster est activé :

```
security config show
```

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

Gestion du cryptage NetApp

Déchiffrement des données de volume

Vous pouvez utiliser le `volume move start` commande pour déplacer et annuler le

chiffrement des données de volume.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir "Autorité déléguée pour exécuter la commande volume Move".

Étapes

1. Déplacer un volume chiffré existant sans chiffrer les données sur le volume :

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et déchiffre les données sur le volume :

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   Le système supprime la clé de cryptage du volume. Les données du volume sont non chiffrées.

2. Vérifiez que le volume est désactivé pour le chiffrement :

   `volume show -encryption`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante indique si les volumes sont présents `cluster1` sont chiffrées :

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Déplacement d'un volume chiffré

Vous pouvez utiliser le `volume move start` commande permettant de déplacer un volume chiffré. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

Description de la tâche

Le déplacement échoue si le nœud de destination ou le volume de destination ne prend pas en charge le chiffrement de volume.

Le `-encrypt-destination` option pour `volume move start` la valeur par défaut est true pour les

volumes chiffrés. La nécessité de spécifier que vous ne souhaitez pas que le volume de destination soit chiffré garantit que vous ne déchiffrez pas par inadvertance les données sur le volume.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir "autorité déléguée pour exécuter la commande de déplacement de volume".

Étapes

1. Déplacez un volume chiffré et laissez les données sur le volume chiffré :

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et conserve les données sur le volume chiffrées :

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. Vérifiez que le volume est activé pour le chiffrement :

   `volume show -is-encrypted true`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante affiche les volumes chiffrés sur `cluster1`:

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  --------- ----
   vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
   ```

Autorité déléguée pour exécuter la commande volume Move

Vous pouvez utiliser le `volume move` commande pour chiffrer un volume existant, déplacer un volume chiffré ou annuler le chiffrement d'un volume. Les administrateurs du cluster peuvent exécuter `volume move` Ils peuvent se passer eux-mêmes de la commande ou déléguer à l'autorité pour qu'elle exécute la commande aux administrateurs du SVM.

Description de la tâche

Par défaut, les administrateurs du SVM sont affectés au système `vsadmin` rôle, qui ne comprend pas l'autorité nécessaire pour déplacer les volumes. Vous devez affecter le `vsadmin-volume` Rôle aux administrateurs

SVM afin de leur permettre d'exécuter les `volume move` commande.

Étape

1. Déléguer l'autorité pour exécuter le `volume move` commande :

   `security login modify -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`vsadmin-volume`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante permet à l'administrateur du SVM d'exécuter le `volume move` commande.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   SVM-admin -application ssh -authmethod domain -role vsadmin-volume
   ```

Modifiez la clé de chiffrement d'un volume à l'aide de la commande Volume Encryption rekey start

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption rekey start` commande pour changer la clé de chiffrement.

Description de la tâche

Une fois que vous avez démarré une opération de recontact, elle doit être terminée. Il n'y a pas de retour à l'ancienne clé. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption rekey pause` commande pour mettre l'opération en pause, et le `volume encryption rekey resume` commande pour reprendre l'opération.

Jusqu'à la fin de l'opération de renouvellement de clé, le volume est composé de deux touches. Les nouvelles écritures et les lectures correspondantes utiliseront la nouvelle clé. Sinon, les lectures utilisent l'ancienne clé.

> Vous ne pouvez pas utiliser `volume encryption rekey start` Pour rétablir un volume SnapLock.

Étapes

1. Modifier une clé de chiffrement :

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   La commande suivante modifie la clé de chiffrement pour `vol1` Sur SVM`vs1`:

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. Vérifier l'état de l'opération de renouvellement de clé :

   `volume encryption rekey show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

La commande suivante affiche l'état de l'opération de renouvellement de clés :

```
cluster1::> volume encryption rekey show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ---------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Une fois l'opération de renouvellement de clés terminée, vérifiez que le volume est activé pour le chiffrement :

   `volume show -is-encrypted true`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Modifiez la clé de chiffrement d'un volume à l'aide de la commande volume Move start

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser le `volume move start` commande pour changer la clé de chiffrement. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

Description de la tâche

Vous ne pouvez pas utiliser `volume move start` Pour reKey un volume SnapLock ou FlexGroup.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir "autorité déléguée pour exécuter la commande de déplacement de volume".

Étapes

1. Déplacer un volume existant et modifier la clé de chiffrement :

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante déplace un volume existant nommé **`vol1`** vers l'agrégat de destination **`aggr2`** et

modifie la clé de chiffrement :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

Une nouvelle clé de chiffrement est créée pour le volume. Les données du volume restent chiffrées.

2. Vérifiez que le volume est activé pour le chiffrement :

   `volume show -is-encrypted true`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Rotation des clés d'authentification pour NetApp Storage Encryption

Vous pouvez faire tourner les clés d'authentification lorsque vous utilisez NetApp Storage Encryption (NSE).

Description de la tâche

La rotation des clés d'authentification dans un environnement NSE est prise en charge si vous utilisez External Key Manager (KMIP).

> La rotation des clés d'authentification dans un environnement NSE n'est pas prise en charge pour Onboard Key Manager (OKM).

Étapes

1. Utilisez le `security key-manager create-key` commande permettant de générer de nouvelles clés d'authentification.

   Vous devez générer de nouvelles clés d'authentification avant de pouvoir modifier les clés d'authentification.

2. Utilisez le `storage encryption disk modify -disk * -data-key-id` commande pour modifier les clés d'authentification.

Supprimez un volume chiffré

Vous pouvez utiliser le `volume delete` commande de suppression d'un volume chiffré.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir "autorité déléguée pour exécuter la commande de déplacement de volume".
- Le volume doit être hors ligne.

Étape

1. Supprimez un volume chiffré :

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante supprime un volume chiffré nommé `vol1`:

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   Entrez `yes` lorsque vous êtes invité à confirmer la suppression.

   Le système supprime la clé de cryptage du volume au bout de 24 heures.

   Utiliser `volume delete` avec le `-force true` option permettant de supprimer un volume et de détruire immédiatement la clé de chiffrement correspondante. Cette commande nécessite des privilèges avancés. Pour plus d'informations, consultez la page man.

Une fois que vous avez terminé

Vous pouvez utiliser le `volume recovery-queue` pour restaurer un volume supprimé pendant la période de rétention après l'émission du `volume delete` commande :

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"Comment utiliser la fonction de récupération de volume"

Supprimez les données de façon sécurisée sur un volume chiffré

Supprimez les données de façon sécurisée dans une vue d'ensemble du volume chiffré

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée pour nettoyer les données sans interruption sur les volumes NVE. La suppression des données sur un volume chiffré garantit qu'elles ne peuvent pas être récupérées depuis le support physique, par exemple en cas de « pillage », où les traces de données peuvent être laissées derrière lors de l'écrasement des blocs ou pour supprimer en toute sécurité les données d'un locataire vide.

La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE. Vous ne pouvez pas nettoyer un volume non chiffré. Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

Considérations relatives à l’utilisation de la suppression sécurisée

- Les volumes créés dans un agrégat pour NetApp Aggregate Encryption (NAE) ne prennent pas en charge la suppression sécurisée.
- La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE.
- Vous ne pouvez pas nettoyer un volume non chiffré.
- Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

Les fonctions de purge sécurisée varient en fonction de votre version de ONTAP.

ONTAP 9.8 et versions ultérieures

- La suppression sécurisée est prise en charge par MetroCluster et FlexGroup.
- Si le volume en cours de purge est à l'origine d'une relation SnapMirror, il n'est pas nécessaire de rompre la relation SnapMirror pour effectuer une purge sécurisée.
- La méthode de rechiffrement est différente pour les volumes qui utilisent la protection des données SnapMirror, contre les volumes qui n'utilisent pas la protection des données SnapMirror (DP) ou ceux qui utilisent la protection étendue des données SnapMirror.
  - Par défaut, les volumes utilisant le mode de protection des données SnapMirror (DP) recryptent les données à l'aide de la méthode de chiffrement du déplacement de volume.
  - Par défaut, les volumes qui n'utilisent pas la protection des données SnapMirror ou les volumes en utilisant le mode XDP (SnapMirror Extended Data protection) utilisent la méthode de rechiffrement sur place.
  - Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge re-encryption-method [volume-move|in-place-rekey]` commande.
- Par défaut toutes les copies Snapshot des volumes FlexVol sont automatiquement supprimées lors de l'opération de suppression sécurisée. Par défaut, les copies Snapshot des volumes FlexGroup et les volumes qui utilisent la protection des données SnapMirror ne sont pas automatiquement supprimées lors de l'opération de suppression sécurisée. Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge delete-all-snapshots [true|false]` commande.

ONTAP 9.7 et versions antérieures :

- La purge sécurisée ne prend pas en charge les éléments suivants :
  - FlexClone
  - SnapVault
  - FabricPool
- Si le volume en cours de purge est la source d'une relation SnapMirror, vous devez interrompre la relation SnapMirror avant de pouvoir purger le volume.

  Si des copies Snapshot sont occupées dans le volume, vous devez libérer les copies Snapshot avant de pouvoir purger le volume. Par exemple, vous devrez peut-être séparer un volume FlexClone de son volume parent.

- L'appel réussi de la fonction de suppression sécurisée déclenche un déplacement de volume qui recrypte les données restantes non supprimées avec une nouvelle clé.

  Le volume déplacé reste sur l'agrégat actuel. L'ancienne clé est automatiquement détruite, ce qui permet de s'assurer que les données supprimées ne peuvent pas être récupérées du support de stockage.

Supprimez en toute sécurité les données d'un volume chiffré sans une relation SnapMirror

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée vers les données « ``cribs'' sans interruption sur les volumes NVE.

Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données

contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
2. Sur le système de stockage, passez au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

3. Si les fichiers que vous souhaitez purger en toute sécurité sont dans les instantanés, supprimez-les :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Supprimez les fichiers supprimés de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   La commande suivante supprime de manière sécurisée les fichiers supprimés sur `vol1` Sur SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Vérifier l'état de l'opération de purge sécurisée :

   ```
   volume encryption secure-purge show
   ```

Supprimez en toute sécurité les données d'un volume chiffré avec une relation SnapMirror asynchrone

Depuis ONTAP 9.8, vous pouvez utiliser une suppression sécurisée des données « `réplication```ss" sans interruption sur les volumes NVE avec une relation SnapMirror asynchrone.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.

- Des privilèges avancés sont requis pour cette tâche.

Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Étapes

1. Sur le système de stockage, basculer sur le niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Répétez cette étape pour chaque volume de la relation SnapMirror asynchrone.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans les copies Snapshot de base, procédez comme suit :

   a. Créez une copie Snapshot sur le volume de destination dans la relation SnapMirror asynchrone :

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Mettre à jour SnapMirror pour transférer la copie Snapshot de base :

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   Répétez cette étape pour chaque volume de la relation SnapMirror asynchrone.

   a. Les étapes de répétition (a) et (b) sont égales au nombre de copies Snapshot de base plus une.

Par exemple, si vous avez deux copies Snapshot de base, vous devez répéter les étapes (a) et (b) trois fois.

b. Vérifier la présence de la copie Snapshot de base :

```
snapshot show -vserver SVM_name -volume volume_name
```

c. Supprimer la copie Snapshot de base :

```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

6. Supprimez les fichiers supprimés de manière sécurisée :

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Répétez cette étape pour chaque volume de la relation SnapMirror asynchrone.

La commande suivante purge de manière sécurisée les fichiers supprimés sur « 'vol1' » du SVM « vs1 » :

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Vérifier l'état de l'opération de purge sécurisée :

```
volume encryption secure-purge show
```

Frottez les données sur un volume chiffré avec une relation SnapMirror synchrone

À partir de ONTAP 9.8, vous pouvez utiliser une suppression sécurisée pour « nettoyer » les données de volumes NVE sans interruption avec une relation SnapMirror synchrone.

Description de la tâche

Une purge sécurisée peut prendre plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Sur le système de stockage, passez au niveau de privilège avancé :

```
set -privilege advanced
```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Répétez cette étape pour l'autre volume de votre relation SnapMirror synchrone.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. Si le fichier de suppression sécurisée se trouve dans les copies Snapshot de base ou communes, mettez à jour SnapMirror pour déplacer la copie Snapshot commune :

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   Il existe deux copies Snapshot communes. Cette commande doit donc être émise deux fois.

6. Si le fichier de suppression sécurisée se trouve dans la copie Snapshot cohérente au niveau des applications, supprimez la copie Snapshot sur les deux volumes de la relation SnapMirror synchrone :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   Effectuer cette étape sur les deux volumes.

7. Supprimez les fichiers supprimés de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Répétez cette étape pour chaque volume de la relation SnapMirror synchrone.

   La commande suivante supprime en toute sécurité les fichiers supprimés sur « vol1 » sur le SMV « vs1 ».

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Vérifier l'état de l'opération de purge sécurisée :

   ```
   volume encryption secure-purge show
   ```

Modifiez la phrase secrète intégrée pour la gestion des clés

Il est recommandé d'appliquer régulièrement une meilleure pratique de sécurité à la modification de la phrase secrète intégrée pour la gestion des clés. Copiez la nouvelle

phrase secrète intégrée pour la gestion des clés dans un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Modifiez la phrase secrète intégrée pour la gestion des clés :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager onboard update-passphrase`
ONTAP 9.5 et versions antérieures	`security key-manager update-passphrase`

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

   La commande suivante de ONTAP 9.6 vous permet de modifier la phrase secrète de gestion intégrée des clés pour `cluster1`:

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Entrez `y` à l'invite, vous pouvez modifier la phrase secrète intégrée pour la gestion des clés.
4. Saisissez la phrase de passe actuelle à l'invite de phrase de passe actuelle.
5. À l'invite de la nouvelle phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

   Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

6. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.

Une fois que vous avez terminé

Dans un environnement MetroCluster, vous devez mettre à jour la phrase secrète sur le cluster partenaire :

- Dans ONTAP 9.5 et les versions antérieures, vous devez exécuter `security key-manager update-passphrase` avec la même phrase secrète sur le cluster partenaire.
- Dans ONTAP 9.6 et versions ultérieures, vous êtes invité à exécuter `security key-manager onboard sync` avec la même phrase secrète sur le cluster partenaire.

Copiez le mot de passe de gestion des clés intégré vers un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Vous devez sauvegarder manuellement les informations de gestion des clés chaque fois que vous modifiez la phrase secrète de gestion intégrée des clés.

"Sauvegarde manuelle des informations de gestion intégrée des clés"

Sauvegardez manuellement les informations intégrées de gestion des clés

Vous devez copier les informations de gestion intégrée des clés dans un emplacement sécurisé en dehors du système de stockage dès que vous configurez la phrase secrète Onboard Key Manager.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Description de la tâche

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster. Vous devez également sauvegarder manuellement les informations de gestion des clés pour une utilisation en cas d'incident.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Afficher les informations de gestion des clés du cluster :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager onboard show-backup`
ONTAP 9.5 et versions antérieures	`security key-manager backup show`

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

+
La commande 9.6 suivante affiche les informations de sauvegarde de la gestion des clés pour `cluster1`:

+

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. Copiez les informations de sauvegarde dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident.

Restaurez les clés de chiffrement intégrées de gestion des clés

La procédure à suivre pour restaurer vos clés de chiffrement de gestion intégrée des clés varie en fonction de votre version d'ONTAP.

Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe. Pour plus d'informations, voir "passez à la gestion intégrée des clés grâce à la gestion externe des clés"
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

ONTAP 9.8 et versions ultérieures avec volume racine chiffré

Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine n'est pas crypté, suivez la procédure pour ONTAP 9.6 ou une version ultérieure.

Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine est chiffré, vous devez définir une phrase de passe de récupération de la gestion des clés intégrée à l'aide du menu de démarrage. Ce processus est également nécessaire si vous effectuez un remplacement de support de démarrage.

1. Démarrez le nœud sur le menu de démarrage et sélectionnez option `(10) Set onboard key management recovery secrets`.
2. Entrez `y` pour utiliser cette option.
3. Entrez à l'invite le phrase secrète de gestion intégrée des clés pour le cluster.
4. À l'invite, entrez les données de la clé de sauvegarde.

   Le nœud revient au menu de démarrage.

5. Dans le menu de démarrage, sélectionnez option `(1) Normal Boot`.

ONTAP 9.6 et versions ultérieures

1. Vérifiez que la clé doit être restaurée :
   `security key-manager key query -node node`
2. Restaurer la clé :
   `security key-manager onboard sync`

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

   La commande ONTAP 9.6 suivante synchronise les clés dans la hiérarchie de clés intégrée :

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

3. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

ONTAP 9.5 et versions antérieures

1. Vérifiez que la clé doit être restaurée :
   `security key-manager key show`
2. Si vous exécutez ONTAP 9.8 ou version ultérieure et que votre volume racine est chiffré, procédez comme suit :

   Si vous exécutez ONTAP 9.6 ou 9.7, ou si vous utilisez ONTAP 9.8 ou une version ultérieure et que votre

volume racine n'est pas chiffré, ignorez cette étape.

3. Restaurer la clé :
   `security key-manager setup -node node`

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

4. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

Restaurez les clés de chiffrement externes pour la gestion des clés

Vous pouvez restaurer manuellement des clés de chiffrement de gestion externe des clés et les transférer vers un autre nœud. Vous pouvez le faire si vous redémarrez un nœud qui était temporairement arrêté lorsque vous avez créé les clés du cluster.

Description de la tâche

Dans ONTAP 9.6 et versions ultérieures, vous pouvez utiliser le `security key-manager key query -node node_name` commande pour vérifier si votre clé doit être restaurée.

Dans ONTAP 9.5 et les versions antérieures, vous pouvez utiliser le `security key-manager key show` commande pour vérifier si votre clé doit être restaurée.

> Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Si vous exécutez ONTAP 9.8 ou version ultérieure et que le volume racine est chiffré, procédez comme suit :

   Si vous exécutez ONTAP 9.7 ou une version antérieure, ou si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine n'est pas chiffré, ignorez cette étape.

   a. Définissez les bootargs :

      ```
      setenv kmip.init.ipaddr <ip-address>

      setenv kmip.init.netmask <netmask>

      setenv kmip.init.gateway <gateway>

      setenv kmip.init.interface e0M

      boot_ontap
      ```

   b. Démarrez le nœud sur le menu de démarrage et sélectionnez option `(11) Configure node for external key management`.

   c. Suivez les invites pour saisir le certificat de gestion.

      Une fois toutes les informations relatives au certificat de gestion saisies, le système revient au menu

de démarrage.

d. Dans le menu de démarrage, sélectionnez option `(1) Normal Boot`.

2. Restaurer la clé :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 et versions antérieures

> `node` tous les nœuds par défaut. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée.

La commande ONTAP 9.6 suivante restaure les clés d'authentification externes de gestion des clés vers tous les nœuds de `cluster1`:

```
cluster1::> security key-manager external restore
```

Remplacer les certificats SSL

Tous les certificats SSL ont une date d'expiration. Vous devez mettre à jour vos certificats avant qu'ils n'expirent pour éviter toute perte d'accès aux clés d'authentification.

Avant de commencer

- Vous devez avoir obtenu le certificat public et la clé privée de remplacement pour le cluster (certificat client KMIP).
- Vous devez avoir obtenu le certificat public de remplacement pour le serveur KMIP (certificat KMIP Server-CA).
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Dans un environnement MetroCluster, vous devez remplacer le certificat SSL KMIP sur les deux clusters.

> Vous pouvez installer les certificats client et serveur de remplacement sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

Étapes

1. Installez le nouveau certificat KMIP Server-ca :

```
security certificate install -type server-ca -vserver <>
```

2. Installez le nouveau certificat client KMIP :

```
security certificate install -type client -vserver <>
```

3. Mettez à jour la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés :

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   Si vous exécutez ONTAP 9.6 ou version ultérieure dans un environnement MetroCluster et que vous souhaitez modifier la configuration du gestionnaire de clés sur le SVM admin, vous devez exécuter la commande sur les deux clusters de la configuration.

> La mise à jour de la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés renvoie une erreur si les clés publiques/privées du nouveau certificat client sont différentes des clés installées précédemment. Consultez l'article de la base de connaissances "Le nouveau certificat client les clés publiques ou privées sont différentes du certificat client existant" pour obtenir des instructions sur la manière de neutraliser cette erreur.

Remplacez un lecteur FIPS ou SED

Vous pouvez remplacer un lecteur FIPS ou SED de la même façon que vous remplacez un disque ordinaire. Veillez à attribuer de nouvelles clés d'authentification des données au disque de remplacement. Pour un lecteur FIPS, vous pouvez également attribuer une nouvelle clé d'authentification FIPS 140-2.

> Si une paire haute disponibilité est utilisée "Cryptage SAS ou disques NVMe (SED, NSE, FIPS)", vous devez suivre les instructions de la rubrique "Retour d'un lecteur FIPS ou SED en mode non protégé" Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Avant de commencer

- Vous devez connaître l'ID de clé pour la clé d'authentification utilisée par le lecteur.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Vérifiez que le disque a été marqué défectueux :

   ```
   storage disk show -broken
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Retirez le disque défectueux et remplacez-le par un nouveau lecteur FIPS ou SED, en suivant les instructions du guide matériel de votre modèle de tiroir disque.
3. Attribuez la propriété du disque récemment remplacé :

   `storage disk assign -disk disk_name -owner node`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Vérifiez que le nouveau disque a été affecté :

   `storage encryption disk show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Attribuez les clés d'authentification des données au lecteur FIPS ou SED.

   "Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)"

6. Si nécessaire, attribuez une clé d'authentification FIPS 140-2 au lecteur FIPS.

   "Attribution d'une clé d'authentification FIPS 140-2 à un lecteur FIPS"

Rendre les données d'un lecteur FIPS ou SED inaccessibles

Rendre les données sur un lecteur FIPS ou SED inaccessibles

Si vous souhaitez rendre les données stockées sur un lecteur FIPS ou SED définitivement inaccessibles, mais que l'espace inutilisé du lecteur reste disponible pour les nouvelles données, vous pouvez désinfecter le disque. Si vous souhaitez rendre les données définitivement inaccessibles et que vous n'avez pas besoin de réutiliser le lecteur, vous pouvez le détruire.

- Nettoyage de disque

  Lorsque vous procédez à la suppression d'un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l'état de verrouillage à la mise sous tension sur FALSE et définit l'ID de clé sur une valeur par défaut, soit l'ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

- Destruction du disque

  Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi définitivement inutilisable et les données qu'il y a définitivement inaccessibles.

Vous pouvez supprimer ou détruire des disques auto-cryptés ou tous les disques auto-cryptés d'un nœud.

Désinfectez un lecteur FIPS ou SED

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et utiliser le lecteur pour les nouvelles données, vous pouvez utiliser le `storage encryption disk sanitize` commande de nettoyage du disque.

Description de la tâche

Lorsque vous procédez à la suppression d'un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l'état de verrouillage à la mise sous tension sur FALSE et définit l'ID de clé sur une valeur par défaut, soit l'ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du lecteur FIPS ou SED pour les désinfecter :

   `storage aggregate delete -aggregate` *`aggregate_name`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identifiez l'ID du disque pour le lecteur FIPS ou SED à désinfecter :

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Si un lecteur FIPS est exécuté en mode FIPS-Compliance, définissez l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

`storage encryption disk modify -disk disk_id -fips-key-id 0x0`

Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Désinfectez le lecteur :

`storage encryption disk sanitize -disk disk_id`

Vous pouvez utiliser cette commande pour désinfecter uniquement les disques de rechange à chaud ou endommagés. Pour désinfecter tous les disques, quel que soit leur type, utilisez le `-force-all-state` option. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

> ONTAP vous invite à saisir une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

Détruire un lecteur FIPS ou SED

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et que vous n'avez pas besoin de réutiliser le lecteur, vous pouvez utiliser `storage encryption disk destroy` commande de destruction du disque.

Description de la tâche

Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi pratiquement inutilisable et les données qu'il y a définitivement inaccessibles. Cependant, vous pouvez réinitialiser le disque à ses paramètres configurés en usine à l'aide de l'ID de sécurité physique (PSID) imprimé sur l'étiquette du disque. Pour plus d'informations, voir "Remise en service d'un lecteur FIPS ou SED en cas de perte de clés d'authentification".

> Vous ne devez pas détruire un disque FIPS ou SED sauf si vous disposez du service NRD plus (non-Returnable Disk plus). La destruction d'un disque annule sa garantie.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du disque FIPS ou SED à détruire :

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identifiez l'ID de disque pour le lecteur FIPS ou SED à détruire :

   ```
   storage encryption disk show
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ----------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Détruire le disque :

   ```
   storage encryption disk destroy -disk disk_id
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous êtes invité à entrer une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Données d'urgence déchirées sur un lecteur FIPS ou SED

En cas d'urgence en matière de sécurité, vous pouvez instantanément empêcher l'accès à un disque FIPS ou SED, même si l'alimentation n'est pas disponible pour le système de stockage ou le serveur KMIP.

Avant de commencer

- Si vous utilisez un serveur KMIP qui n'est pas alimenté, vous devez configurer le serveur KMIP avec un élément d'authentification facilement détruit (par exemple, une carte à puce ou un lecteur USB).
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Exécutez la suppression d'urgence des données sur un lecteur FIPS ou SED :

Si…	Alors…

L'alimentation est disponible pour le système de stockage et vous avez le temps de mettre celui-ci hors ligne aisément	a. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
	b. Mettre tous les agrégats hors ligne et les supprimer
	c. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	d. Si le lecteur est en mode FIPS-compliance, définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID par défaut :
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. Arrêter le système de stockage.
	f. Démarre en mode de maintenance.
	g. Procédez à la suppression ou à la destruction des disques :
	◦ Pour rendre les données sur les disques inaccessibles et continuer à réutiliser les disques, procédez comme suit :
	`disk encrypt sanitize -all`
	◦ Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques :
	`disk encrypt destroy disk_id1 disk_id2 …`
		Le système de stockage est sous tension et vous devez immédiatement détruire les données

a. **Si vous souhaitez rendre les données sur les disques inaccessibles et que vous pourrez toujours les réutiliser, désinfectez les disques :**
b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
c. Définissez le niveau de privilège sur avancé :
`set -privilege advanced`
d. Si le lecteur est en mode FIPS-compliance, définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID par défaut :
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Procédez à la suppression du disque :
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques :**
	b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
	c. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	d. Détruire les disques :
	`storage encryption disk destroy -disk * -force-all-states true`
		Le système de stockage fonctionne de façon incohérente, laissant le système se trouve dans un état désactivé en permanence et toutes les données sont effacées. Pour réutiliser le système, vous devez le reconfigurer.

L'alimentation est disponible pour le serveur KMIP, mais pas pour le système de stockage	a. Connectez-vous au serveur KMIP. b. Détruire toutes les clés associées aux lecteurs FIPS ou les disques SED qui contiennent les données auxquelles vous souhaitez empêcher l'accès. Cela empêche l'accès aux clés de cryptage du disque par le système de stockage.	L'alimentation n'est pas disponible pour le serveur KMIP ou le système de stockage

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

Renvoyez un lecteur FIPS ou SED au service en cas de perte de clés d'authentification

Le système traite un lecteur FIPS ou SED comme étant rompu si vous perdez

définitivement les clés d'authentification pour lui et que vous ne pouvez pas les récupérer du serveur KMIP. Bien que vous ne puissiez pas accéder ou récupérer les données sur le disque, vous pouvez prendre des mesures pour rendre à nouveau disponible l'espace inutilisé de SED pour les données.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Description de la tâche

Vous ne devez utiliser ce processus que si vous êtes certain que les clés d'authentification du lecteur FIPS ou SED sont définitivement perdues et que vous ne pouvez pas les récupérer.

Si les disques sont partitionnés, ils doivent d'abord être départitionnés avant que vous ne puissiez démarrer ce processus.

> La commande permettant de départitionner un disque est uniquement disponible au niveau diagnostic et ne doit être effectuée qu'avec NetApp support supervision. **Il est fortement recommandé de contacter le support NetApp avant de continuer.** vous pouvez également consulter l'article de la base de connaissances "Comment départitionner un lecteur de réserve dans ONTAP".

Étapes

1. Renvoyez un lecteur FIPS ou SED au service :

Si le SEDS est…	Procédez comme suit…

Pas en mode de conformité FIPS, ni en mode de conformité FIPS et la clé FIPS est disponible	a. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	b. Réinitialisez la clé FIPS sur l'ID sécurisé de fabrication par défaut 0x0 :
	`storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`*
	c. Vérifiez que l'opération a réussi :
	`storage encryption disk show-status`
	Si l'opération a échoué, utilisez le processus PSID dans cette rubrique.
	d. Procédez au nettoyage du disque défaillant :
	`storage encryption disk sanitize -disk` *`disk_id`*
	Vérifiez que l'opération a réussi avec la commande `storage encryption disk show-status` avant de passer à l'étape suivante.
	e. Éliminez la panne du disque désinfecté :
	`storage disk unfail -spare true -disk` *`disk_id`*
	f. Vérifiez si le disque est propriétaire :
	`storage disk show -disk` *`disk_id`*
	
	Si le disque ne possède pas de propriétaire, attribuez-en un.
	`storage disk assign -owner node -disk` *`disk_id`*
	
	i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :
	
	`system node run -node` *`node_name`*
	
	Exécutez le `disk sanitize release` commande.
	g. Quittez le nodeshell. Éliminez à nouveau la panne du disque :
	`storage disk unfail -spare true -disk` *`disk_id`*
	h. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :
	`storage disk show -disk` *`disk_id`*

En mode FIPS-compliance, la clé FIPS n'est pas disponible et les disques SED ont un PSID imprimé sur l'étiquette	a. Procurez-vous le PSID du disque à partir de l'étiquette du disque. b. Définissez le niveau de privilège sur avancé : `set -privilege advanced` c. Réinitialise le disque en fonction des paramètres configurés en usine : `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Vérifiez que l'opération a réussi avec la commande `storage encryption disk show-status` avant de passer à l'étape suivante. d. Si vous utilisez ONTAP 9.8P5 ou une version antérieure, passez à l'étape suivante. Si vous exécutez ONTAP 9.8P6 ou une version ultérieure, éliminez la panne du disque désinfecté. `storage disk unfail -disk` *`disk_id`* e. Vérifiez si le disque est propriétaire : `storage disk show -disk` *`disk_id`* Si le disque ne possède pas de propriétaire, attribuez-en un. `storage disk assign -owner node -disk` *`disk_id`* i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter : `system node run -node` *`node_name`* Exécutez le `disk sanitize release` commande. f. Quittez le nodeshell. Éliminez à nouveau la panne du disque : `storage disk unfail -spare true -disk` *`disk_id`* g. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat : `storage disk show -disk` *`disk_id`*

Pour connaître la syntaxe complète de la commande, reportez-vous au "référence de commande".

Retournez un lecteur FIPS ou SED en mode non protégé

Un lecteur FIPS ou SED est protégé contre les accès non autorisés uniquement si l'ID de clé d'authentification du nœud est défini sur une valeur autre que la valeur par défaut. Vous pouvez rétablir un lecteur FIPS ou SED en mode non protégé à l'aide de la `storage encryption disk modify` Commande pour définir l'ID de clé sur la valeur par défaut.

Si une paire haute disponibilité utilise des disques avec cryptage SAS ou NVMe (SED, NSE, FIPS), vous devez suivre cette procédure pour tous les disques de la paire haute disponibilité avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Si un lecteur FIPS est exécuté en mode FIPS-Compliance, définissez l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Confirmer la réussite de l'opération à l'aide de la commande :

   ```
   storage encryption disk show-status
   ```

   Répétez la commande show-status jusqu'à ce que les chiffres de "disques commencés" et de "disques réalisés" soient identiques.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start                Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp            Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------   ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

   ```
   storage encryption disk modify -disk disk_id -data-key-id 0x0
   ```

   La valeur de `-data-key-id` Doit être défini sur 0x0 si vous retournez un disque SAS ou NVMe en mode non protégé.

   Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Confirmer la réussite de l'opération à l'aide de la commande :

```
storage encryption disk show-status
```

Répétez la commande show-status jusqu'à ce que les chiffres soient identiques. L'opération est terminée lorsque les numéros dans "disques commencés" et "disques terminés" sont les mêmes.

Mode Maintenance

Depuis ONTAP 9.7, vous pouvez ressaisir un disque FIPS à partir du mode de maintenance. Si vous ne pouvez pas utiliser les instructions de l'interface de ligne de commandes ONTAP décrites dans la section précédente, vous devez utiliser le mode de maintenance.

Étapes

1. Définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

   `disk encrypt rekey 0x0 *disklist*`

3. Vérifiez que la clé d'authentification FIPS a bien été reclés :

   `disk encrypt show_fips`

4. Confirmer que la clé d'authentification des données a bien été reclés avec :

   `disk encrypt show`

   Votre sortie affichera probablement soit l'ID de clé MSID 0x0 par défaut, soit la valeur de 64 caractères détenue par le serveur de clés. Le `Locked?` ce champ fait référence au verrouillage des données.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Supprimez une connexion externe au gestionnaire de clés

Si vous n'avez plus besoin du serveur, vous pouvez déconnecter un serveur KMIP d'un nœud. Par exemple, vous pouvez déconnecter un serveur KMIP lorsque vous passez au

chiffrement de volume.

Description de la tâche

Lorsque vous déconnectez un serveur KMIP d'un nœud d'une paire haute disponibilité, le système déconnecte automatiquement le serveur de tous les nœuds du cluster.

> Si vous prévoyez de continuer à utiliser la gestion externe des clés après la déconnexion d'un serveur KMIP, assurez-vous qu'un autre serveur KMIP est disponible pour assurer le service des clés d'authentification.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Déconnectez un serveur KMIP du nœud actuel :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 et versions antérieures

Dans un environnement MetroCluster, il faut répéter ces commandes sur les deux clusters pour le SVM admin.

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande ONTAP 9.6 suivante désactive les connexions à deux serveurs de gestion des clés externes pour `cluster1`, le premier nommé `ks1`, Écoute sur le port par défaut 5696, le second avec l'adresse IP 10.0.0.20, écoute sur le port 24482 :

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Modifiez les propriétés du serveur de gestion externe des clés

À partir de ONTAP 9.6, vous pouvez utiliser le `security key-manager external modify-server` Commande permettant de modifier le délai d'attente d'E/S et le nom d'utilisateur d'un serveur de gestion de clés externe.

Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.
- Dans un environnement MetroCluster, vous devez répéter ces étapes sur les deux clusters pour la SVM d'administration.

Étapes

1. Sur le système de stockage, passez au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Modifiez les propriétés externes du serveur du gestionnaire de clés pour le cluster :

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. Si vous exécutez la commande à l'invite de connexion du cluster, *`admin_SVM`* Par défaut au SVM admin du cluster actuel. Vous devez être l'administrateur de cluster pour modifier les propriétés du serveur du gestionnaire de clés externe.

   La commande suivante remplace la valeur de temporisation par 45 secondes pour le `cluster1` serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. Modifier les propriétés du serveur gestionnaire de clés externe pour un SVM (NVE uniquement) :

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. Si vous exécutez la commande à l'invite de connexion du SVM, *`SVM`* Par défaut au SVM actuel Vous devez être l'administrateur du cluster ou de SVM pour modifier les propriétés du serveur externe Key Manager.

   La commande suivante modifie le nom d'utilisateur et le mot de passe de `svm1` serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

   ```
   svml::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. Répétez la dernière étape pour tout SVM supplémentaire.

Transition vers la gestion externe des clés à partir de la gestion intégrée des clés

Pour basculer de la gestion externe des clés à partir de la gestion intégrée des clés, vous devez supprimer la configuration intégrée de la gestion des clés avant de pouvoir activer la gestion externe des clés.

Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

  "Retour d'un lecteur FIPS ou SED en mode non protégé"

- Pour le chiffrement logiciel, vous devez déchiffrer tous les volumes.

  "Sans chiffrement des données de volume"

- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Supprimez la configuration intégrée de gestion des clés d'un cluster :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 et versions antérieures	`security key-manager delete-key-database`

Pour connaître la syntaxe complète de la commande, reportez-vous au "Pages de manuel ONTAP".

Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés

Pour basculer vers la gestion intégrée des clés à partir d'une gestion externe des clés, vous devez supprimer la configuration de gestion externe des clés pour pouvoir activer la gestion intégrée des clés.

Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

  "Retour d'un lecteur FIPS ou SED en mode non protégé"

- Vous devez avoir supprimé toutes les connexions externes du gestionnaire de clés.

  "Suppression d'une connexion externe au gestionnaire de clés"

- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Procédure

La procédure de transition de la gestion des clés dépend de la version de ONTAP que vous utilisez.

ONTAP 9.6 et versions ultérieures

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Utiliser la commande :

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   > Dans un environnement MetroCluster, il faut répéter la commande sur les deux clusters pour la SVM admin.

ONTAP 9.5 et versions antérieures

Utiliser la commande :
`security key-manager delete-kmip-config`

Que se passe-t-il lorsque les serveurs de gestion des clés ne sont pas accessibles lors du processus de démarrage

ONTAP prend certaines précautions afin d'éviter tout comportement indésirable dans l'éventualité où un système de stockage configuré pour NSE ne puisse pas atteindre l'un des serveurs de gestion des clés spécifiés lors du processus de démarrage.

Si le système de stockage est configuré pour NSE, les disques SED sont de nouveau et verrouillés, et les disques SED sont sous tension, le système de stockage doit récupérer les clés d'authentification requises à partir des serveurs de gestion des clés pour s'authentifier auprès des disques SED avant qu'ils puissent accéder aux données.

Le système de stockage tente de contacter les serveurs de gestion des clés spécifiés pendant jusqu'à trois heures. Si le système de stockage ne peut pas atteindre l'un d'eux après ce délai, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Si le système de stockage contacte avec succès un serveur de gestion de clés spécifié, il tente alors d'établir une connexion SSL pendant 15 minutes. Si le système de stockage ne parvient pas à établir de connexion SSL avec un serveur de gestion de clés spécifié, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Pendant que le système de stockage tente de contacter et de se connecter aux serveurs de gestion des clés, il affiche des informations détaillées sur les tentatives de contact ayant échoué au niveau de l'interface de ligne de commande. Vous pouvez interrompre les tentatives de contact à tout moment en appuyant sur Ctrl-C.

Par mesure de sécurité, les disques SED ne permettent qu'un nombre limité de tentatives d'accès non autorisées, après quoi ils désactivent l'accès aux données existantes. Si le système de stockage ne peut pas contacter les serveurs de gestion des clés spécifiés pour obtenir les clés d'authentification appropriées, il peut uniquement tenter de s'authentifier auprès de la clé par défaut, ce qui entraîne une tentative d'échec et un incident. Si le système de stockage est configuré pour redémarrer automatiquement en cas de panique, il entre dans une boucle d'amorçage qui entraîne des tentatives d'authentification continues sur les disques SED ayant échoué.

Dans ces scénarios, l'arrêt du système de stockage a été conçu pour éviter que le système de stockage ne pénètre dans une boucle d'amorçage et qu'il puisse y avoir des pertes de données inattendues suite au

verrouillage permanent des disques SED, raison du dépassement de la limite de sécurité d'un certain nombre de tentatives d'authentification consécutives ayant échoué. La limite et le type de protection de verrouillage dépendent des spécifications de fabrication et du type de SED :

Type SED	Nombre de tentatives d'authentification consécutives ayant échoué entraînant un blocage	Type de protection de verrouillage lorsque la limite de sécurité est atteinte
DISQUES DURS	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
X440_PHM2800MCTO SSD NSE 800 Go avec révisions du firmware NA00 ou NA01	5	Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.
X577_PHM2800MNA00 SSD NSE 800 Go avec révisions de firmware ou NA01	5	Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.
X440_PHM2800MCTO SSD NSE 800 Go avec révisions de firmware plus élevées	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
X577_PHM2800MCTO SSD NSE 800 Go avec révisions de micrologiciel plus élevées	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
Tous les autres modèles de SSD	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.

Pour tous les types SED, une authentification réussie réinitialise le nombre d'essayer à zéro.

Si vous rencontrez ce scénario lorsque le système de stockage est arrêté en raison d'un échec d'accès aux serveurs de gestion de clés spécifiés, vous devez d'abord identifier et corriger la cause de l'échec de communication avant de poursuivre le démarrage du système de stockage.

Désactiver le chiffrement par défaut

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe. Si nécessaire, vous pouvez désactiver le chiffrement par défaut pour l'ensemble du cluster.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche, ou un administrateur de SVM à qui l'administrateur du cluster a délégué des pouvoirs.

Étape

1. Pour désactiver le chiffrement par défaut pour l'ensemble du cluster dans ONTAP 9.7 ou version ultérieure, exécutez la commande suivante :

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```