Fonctionnement de l'audit

ONTAP 9

NetApp
March 24, 2023

Table des matières

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. Auparavant, les utilisateurs pouvaient supprimer le travail de consolidation d'audit à l'aide des commandes du gestionnaire de tâches telles que `job delete`. Les utilisateurs ne sont plus autorisés à supprimer le travail de consolidation d'audit.

Informations sur le copyright

Informations sur les marques commerciales