Consignation des audits

ONTAP 9

NetApp
April 24, 2024

Sommaire

Consignation des audits

Mise en œuvre de la journalisation des audits par ONTAP

Les activités de gestion enregistrées dans le journal d'audit sont incluses dans les rapports AutoSupport standard et certaines activités de consignation sont incluses dans les messages EMS. Vous pouvez également transférer le journal d'audit aux destinations que vous spécifiez et afficher les fichiers journaux d'audit à l'aide de l'interface de ligne de commande ou d'un navigateur Web.

Depuis ONTAP 9.11.1, vous pouvez afficher le contenu des journaux d'audit à l'aide de System Manager.

Depuis ONTAP 9.12.1, ONTAP fournit des alertes de falsification pour les journaux d'audit. ONTAP exécute une tâche d'arrière-plan quotidienne pour vérifier l'altération des fichiers audit.log et envoie une alerte EMS s'il trouve des fichiers journaux qui ont été modifiés ou falsifiés.

ONTAP consigne les activités de gestion qui sont effectuées sur le cluster, par exemple la requête émise, l'utilisateur qui a déclenché la demande, la méthode d'accès de l'utilisateur et l'heure de la demande.

Les activités de gestion peuvent être de l'un des types suivants :

- DÉFINIR les demandes, qui s'appliquent généralement aux commandes ou opérations non affichées
  - Ces demandes sont émises lorsque vous exécutez un `create`, `modify`, ou `delete` commande, par exemple.
  - Les demandes de série sont consignées par défaut.
- OBTENIR les demandes, qui récupèrent les informations et les affichent dans l'interface de gestion
  - Ces demandes sont émises lorsque vous exécutez un `show` commande, par exemple.
  - Les demandes GET ne sont pas consignées par défaut, mais vous pouvez contrôler si LES demandes GET sont envoyées depuis l'interface de ligne de commande ONTAP (`-cliget`), à partir de l'API ONTAP (`-ontapiget`), ou à partir de l'API REST (`-httpget`) sont consignés dans le fichier.

ONTAP enregistre les activités de gestion dans `/mroot/etc/log/mlog/audit.log` fichier d'un nœud. Les commandes des trois shells pour les commandes CLI—le clustershell, le nodeshell et le systemshell non-interactif (les commandes du systemshell interactives ne sont pas consignées)--ainsi que les commandes d'API sont consignées ici. Les journaux d'audit incluent des horodatages pour indiquer si tous les nœuds d'un cluster sont synchronisés.

Le `audit.log` Le fichier est envoyé par l'outil AutoSupport aux destinataires spécifiés. Vous pouvez également transférer le contenu en toute sécurité vers des destinations externes que vous spécifiez (par exemple, un serveur Splunk ou syslog).

Le `audit.log` le fichier fait l'objet d'une rotation quotidienne. La rotation se produit également lorsqu'elle atteint 100 Mo et que les 48 copies précédentes sont conservées (avec un total maximum de 49 fichiers). Lorsque le fichier d'audit effectue sa rotation quotidienne, aucun message EMS n'est généré. Si le fichier d'audit tourne parce que sa taille limite de fichier est dépassée, un message EMS est généré.

Modifications de la journalisation des audits dans ONTAP 9

À partir de ONTAP 9, le `command-history.log` le fichier est remplacé par `audit.log`, et le `mgwd.log` le fichier ne contient plus d'informations d'audit. Si vous effectuez une mise à niveau vers ONTAP 9, il est recommandé de consulter les scripts ou les outils qui font référence aux fichiers hérités et à leur contenu.

Après la mise à niveau vers ONTAP 9, existant `command-history.log` les fichiers sont conservés. Ils sont tournés vers l'extérieur (supprimés) comme nouveaux `audit.log` les fichiers sont pivotés dans (créés).

Outils et scripts qui vérifient le `command-history.log` le fichier peut continuer à fonctionner, car un lien logiciel de `command-history.log` à `audit.log` est créée lors de la mise à niveau. Cependant, les outils et les scripts qui vérifient le `mgwd.log` le fichier échoue, car ce fichier ne contient plus d'informations d'audit.

Les journaux d'audit dans ONTAP 9 et les versions ultérieures n'incluent plus les entrées suivantes, car elles ne sont pas considérées comme utiles et n'entraînent pas d'activité de journalisation inutile :

- Commandes internes exécutées par ONTAP (c'est-à-dire où username=root)
- Alias de commande (séparément de la commande à laquelle ils pointent)

Depuis ONTAP 9, vous pouvez transmettre les journaux d'audit de manière sécurisée vers des destinations externes à l'aide des protocoles TCP et TLS.

Afficher le contenu du journal d'audit

Vous pouvez afficher le contenu du cluster `/mroot/etc/log/mlog/audit.log` Fichiers via l'interface de ligne de commandes de ONTAP, System Manager ou un navigateur Web.

Les entrées du fichier journal du cluster sont les suivantes :

Temps

Horodatage de l'entrée du journal.

Client supplémentaire

Application utilisée pour se connecter au cluster. Voici des exemples de valeurs possibles `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, et `service-processor`.

Utilisateur

Nom d'utilisateur de l'utilisateur distant.

État

État actuel de la demande d'audit, qui pourrait être `success`, `pending`, ou `error`.

Messagerie

Champ facultatif qui peut contenir une erreur ou des informations supplémentaires sur l'état d'une commande.

ID de session

ID de session sur lequel la demande est reçue. Un ID de session est attribué à chaque session SSH *session*, tandis que chaque HTTP, ONTAPI ou SNMP *request* se voit attribuer un ID de session unique.

VM de stockage

SVM via lequel l'utilisateur a connecté.

Portée

S'affiche `svm` Lorsque la demande se trouve sur une machine virtuelle de stockage de données ; dans le cas contraire, s'affiche `cluster`.

ID de commande

ID de chaque commande reçue lors d'une session CLI. Cela vous permet de mettre en corrélation une demande et une réponse. Les requêtes ZAPI, HTTP et SNMP ne possèdent pas d'ID de commande.

Vous pouvez afficher les entrées des journaux du cluster depuis l'interface de ligne de commandes de ONTAP, depuis un navigateur Web et depuis ONTAP 9.11.1, depuis System Manager.

System Manager

- Pour afficher l'inventaire, sélectionnez **Evénements et travaux > journaux d'audit**.
  Chaque colonne dispose de commandes pour filtrer, trier, rechercher, afficher et inventorier les catégories. Les détails de l'inventaire peuvent être téléchargés sous forme de classeur Excel.
- Pour définir des filtres, cliquez sur le bouton **Filter** en haut à droite, puis sélectionnez les champs souhaités.
  Vous pouvez également afficher toutes les commandes exécutées dans la session au cours de laquelle un échec s'est produit en cliquant sur le lien ID de session.

CLI

Pour afficher les entrées d'audit fusionnées à partir de plusieurs nœuds du cluster, entrez :
`security audit log show` *`[parameters]`*

Vous pouvez utiliser le `security audit log show` commande permettant d'afficher les entrées d'audit de nœuds individuels ou fusionnées à partir de plusieurs nœuds du cluster. Vous pouvez également afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web. Voir la page man pour plus de détails.

Navigateur Web

Vous pouvez afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web. "Découvrez comment accéder aux fichiers log, core dump et MIB d'un nœud à l'aide d'un navigateur Web".

Gérer les paramètres de demande GET d'audit

Lorsque LES demandes DÉFINIES sont consignées par défaut, les demandes GET ne le sont pas. Cependant, vous pouvez contrôler si LES requêtes GET sont envoyées depuis ONTAP HTML (`-httpget`), l'interface de ligne de commande ONTAP (`-cliget`), ou à partir des API ONTAP (`-ontapiget`) sont consignés dans le fichier.

Vous pouvez modifier les paramètres de la journalisation des audits depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

System Manager

1. Sélectionnez **événements et travaux > journaux d'audit**.
2. Cliquez sur ⚙ dans le coin supérieur droit, choisissez les demandes à ajouter ou à supprimer.

CLI

- Pour spécifier que les demandes GET depuis l'interface de ligne de commande ou les API ONTAP doivent être enregistrées dans le journal d'audit (fichier audit.log), en plus des demandes SET par défaut, entrez :
  ```
  security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]
  ```
- Pour afficher les paramètres actuels, entrez :
  ```
  security audit show
  ```

Consultez les pages de manuel pour plus de détails.

Gérer les destinations du journal d'audit

Vous pouvez transférer le journal d'audit vers un maximum de 10 destinations. Par exemple, vous pouvez transférer le journal vers un serveur Splunk ou syslog à des fins de surveillance, d'analyse ou de sauvegarde.

Description de la tâche

Pour configurer le transfert, vous devez fournir l'adresse IP de l'hôte syslog ou Splunk, son numéro de port, un protocole de transmission et la fonction syslog à utiliser pour les journaux transférés. "En savoir plus sur les installations de syslog".

Vous pouvez sélectionner l'une des valeurs de transmission suivantes :

UDP non crypté

Protocole de datagramme utilisateur sans sécurité (par défaut)

TCP non chiffré

Protocole de contrôle de transmission sans sécurité

TCP chiffré

Protocole de contrôle de transmission avec TLS (transport Layer Security)
Une option **Verify Server** est disponible lorsque le protocole TCP chiffré est sélectionné.

Vous pouvez transférer les journaux d'audit depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

System Manager

- Pour afficher les destinations du journal d'audit, sélectionnez **Cluster > Paramètres**.
  Le nombre de destinations du journal s'affiche dans la mosaïque **gestion des notifications**. Cliquez sur ⋮ pour afficher les détails.
- Pour ajouter, modifier ou supprimer des destinations du journal d'audit, sélectionnez **Evénements et travaux > journaux d'audit**, puis cliquez sur **gérer destinations d'audit** dans le coin supérieur droit de l'écran.
  Cliquez sur + Add ou cliquez sur ⋮ Dans la colonne **adresse hôte** pour modifier ou supprimer des entrées.

CLI

1. Pour chaque destination vers laquelle vous souhaitez transférer le journal d'audit, spécifiez l'adresse IP ou le nom d'hôte de destination et les options de sécurité.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - Si le `cluster log-forwarding create` la commande ne peut pas envoyer de requête ping à l'hôte de destination pour vérifier la connectivité, la commande échoue avec une erreur. Bien qu'il ne soit pas recommandé, utiliser le `-force` le paramètre utilisé avec la commande ignore la vérification de connectivité.
   - Lorsque vous définissez le `-verify-server` paramètre à `true`, l'identité de la destination de transfert de journal est vérifiée en validant son certificat. Vous pouvez définir la valeur sur `true` uniquement lorsque vous sélectionnez `tcp-encrypted` valeur dans le `-protocol` légale.

2. Vérifiez que les enregistrements de destination sont corrects à l'aide du `cluster log-forwarding show` commande.

```
cluster1::> cluster log-forwarding show

                                                  Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

Consultez les pages de manuel pour plus de détails.