Audit des événements S3

ONTAP 9

NetApp
April 24, 2024

Sommaire

Audit des événements S3 1
Audit des événements S3 1
Planification d’une configuration d’audit S3 2
Créez et activez une configuration d’audit S3 5
Sélectionnez des compartiments pour l’audit S3 6
Modifiez une configuration d’audit S3 7
Affiche les configurations d’audit S3 8

Audit des événements S3

Audit des événements S3

Depuis ONTAP 9.10.1, vous pouvez auditer les événements de gestion et de données dans des environnements ONTAP S3. La fonctionnalité d'audit S3 est similaire aux fonctionnalités d'audit NAS existantes, et l'audit S3 et NAS peut coexister dans un cluster.

Lorsque vous créez et activez une configuration d'audit S3 sur un SVM, les événements S3 sont enregistrés dans un fichier journal. Vous pouvez spécifier les événements suivants à enregistrer :

- Événements d'accès aux objets (données)

  GetObject, PutObject et DeleteObject

- Les événements de gestion

  PutBucket et DeleteBucket

Le format du journal est JavaScript Object notation (JSON).

La limite combinée des configurations d'audit S3 et NFS est de 50 SVM par cluster.

Le pack de licences suivant est requis :

- Bundle de base pour le protocole et le stockage ONTAP S3

Pour plus d'informations, voir "Fonctionnement du processus d'audit ONTAP".

Audit garanti

Par défaut, l'audit S3 et NAS est garanti. ONTAP garantit l'enregistrement de tous les événements d'accès au compartiment vérifiables, même si un nœud est indisponible. Une opération de compartiment demandée ne peut être effectuée qu'une fois l'enregistrement d'audit pour cette opération enregistré dans le volume intermédiaire du stockage persistant. Si les enregistrements d'audit ne peuvent pas être archivés dans les fichiers de transfert, soit en raison d'un espace insuffisant, soit en raison d'autres problèmes, les opérations du client sont refusées.

Besoins en espace pour l'audit

Dans le système d'audit ONTAP, les enregistrements d'audit sont initialement stockés dans des fichiers intermédiaires binaires sur des nœuds individuels. 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.

Les fichiers de sauvegarde sont stockés dans un volume de sauvegarde dédié, qui est créé par ONTAP lors de la création de la configuration d'audit. Il existe un volume intermédiaire par agrégat.

Vous devez prévoir suffisamment d'espace disponible dans la configuration d'audit :

- Pour les volumes intermédiaires dans des agrégats contenant des compartiments audités.

- Pour le volume contenant le répertoire dans lequel les journaux d'événements convertis sont stockés.

Vous pouvez contrôler le nombre de journaux d'événements et donc l'espace disponible dans le volume à l'aide de l'une des deux méthodes suivantes lors de la création de la configuration d'audit S3 :

- Une limite numérique ; le `-rotate-limit` paramètre contrôle le nombre minimal de fichiers d'audit qui doivent être conservés.
- Une limite de temps ; le `-retention-duration` paramètre contrôle la période maximale pendant laquelle les fichiers peuvent être conservés.

Dans les deux paramètres, une fois que la configuration est dépassée, les fichiers d'audit plus anciens peuvent être supprimés afin de faire place à des fichiers plus récents. Pour les deux paramètres, la valeur est 0, ce qui indique que tous les fichiers doivent être conservés. Afin de garantir un espace suffisant, il est donc recommandé de définir un des paramètres sur une valeur non nulle.

En raison de l'audit garanti, si l'espace disponible pour les données d'audit s'exécute avant la limite de rotation, des données d'audit plus récentes ne peuvent pas être créées, ce qui entraîne une incapacité des clients à accéder aux données. Par conséquent, le choix de cette valeur et de l'espace alloué à l'audit doit être soigneusement choisi, et vous devez répondre aux avertissements concernant l'espace disponible du système d'audit.

Pour plus d'informations, voir "Concepts d'audit de base".

Planification d'une configuration d'audit S3

Vous devez spécifier un certain nombre de paramètres pour la configuration d'audit S3 ou accepter les valeurs par défaut. En particulier, vous devez tenir compte des paramètres de rotation du journal qui vous aideront à garantir un espace libre adéquat.

Voir la **`vserver object-store-server audit create`** page man pour les détails de syntaxe.

Paramètres généraux

Vous devez spécifier deux paramètres requis lors de la création de la configuration d'audit. Vous pouvez également spécifier trois paramètres facultatifs.

Type d'information	Option	Obligatoire
Nom du SVM Nom du SVM sur lequel créer la configuration d'audit. Le SVM doit déjà exister et être activé pour S3.	`-verserver` *`svm_name`*	Oui.

Chemin de destination du journal Spécifie l'emplacement de stockage des journaux d'audit convertis. Le chemin doit déjà exister sur le 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.	`-destination` *`text`*	Oui.
Catégories d'événements à auditer Les catégories d'événements suivantes peuvent être auditées : • les données Événements GetObject, PutObject et DeleteObject • gestion Événements PutBucket et DeleteBucket La valeur par défaut est d'auditer uniquement les événements de données.	`-events {data|management}, …`	Non

Vous pouvez entrer l'un des paramètres suivants pour contrôler le nombre de fichiers journaux d'audit. Si aucune valeur n'est saisie, tous les fichiers journaux sont conservés.

Type d'information	Option	Obligatoire
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. Une valeur de 0 indique que tous les fichiers journaux sont conservés. La valeur par défaut est 0.	`-rotate-limit` *`integer`*	Non
Limite de durée des fichiers journaux Détermine la durée pendant laquelle un fichier journal peut être conservé avant d'être supprimé. Par exemple, si vous entrez une valeur de 5 portes 0h0m, les journaux de plus de 5 jours sont supprimés. Une valeur de 0 indique que tous les fichiers journaux sont conservés. La valeur par défaut est 0.	`-retention duration` *`integer_time`*	Non

Paramètres de rotation du journal d'audit

Vous pouvez faire pivoter les journaux d'audit en fonction de la taille ou de la planification. La valeur par défaut

consiste à faire pivoter les journaux d'audit en fonction de la taille.

Rotation des journaux en fonction de la taille du journal

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. La taille du journal par défaut est de 100 Mo.

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.

Si vous souhaitez réinitialiser la rotation en fonction d'une taille de journal seule, utilisez la commande suivante pour annuler la sélection `-rotate-schedule-minute` paramètre :

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Rotation des journaux en fonction d'un planning

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.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- 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 réinitialiser la rotation en fonction d'une planification seule, utilisez la commande suivante pour annuler la définition du `-rotate-size parameter`:

```
vserver audit modify -vserver svm_name -destination / -rotate-size -
```

Rotation des journaux en fonction de la taille du journal et de la planification

Vous pouvez choisir de faire pivoter les fichiers journaux en fonction de la taille du journal et d'une planification en définissant à la fois le paramètre -rotation-taille et les 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).

Créez et activez une configuration d'audit S3

Pour implémenter l'audit S3, vous devez d'abord créer une configuration d'audit de magasin d'objets persistant sur un SVM compatible avec S3, puis activer la configuration.

Ce dont vous avez besoin

- SVM compatible S3.
- Espace suffisant pour les volumes intermédiaires dans l'agrégat.

Description de la tâche

Une configuration d'audit est requise pour chaque SVM contenant des compartiments S3 que vous souhaitez auditer. Vous pouvez activer l'audit S3 sur des serveurs S3 nouveaux ou existants. Les configurations d'audit restent conservées dans un environnement S3 jusqu'à ce qu'elles soient supprimées par la commande **vserver Object-store-Server audit delete**.

La configuration d'audit de S3 s'applique à toutes les compartiments du SVM que vous sélectionnez pour l'audit. Un SVM activé pour un audit peut contenir des compartiments audités et non audités.

Il est recommandé de configurer l'audit S3 pour une rotation automatique des journaux, déterminée par la taille du journal ou par une planification. Si vous ne configurez pas la rotation automatique des journaux, tous les fichiers journaux sont conservés par défaut. Vous pouvez également faire pivoter les fichiers journaux S3 manuellement à l'aide de la commande **vserver Object-store-Server audit rotate-log**.

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.

Procédure

1. 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 object-store-server audit create -vserver svm_name -destination path [[-events] {data|management}, …] {[-rotate-limit integer] | [-retention-duration [integer_d][_integer_h][_integer_m][_integers]]} [-rotate-size {integer[KB|MB|GB|TB|PB]}]`

Si vous souhaitez faire pivoter les journaux d'audit en…	Entrer…
Un planning	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integerd`*`][`*`integerh`*`] [`*`integerm`*`][`*`integers`*`]] } [-rotate-schedule-month` *`chron_month`*`] [-rotate-schedule-dayofweek` *`chron_dayofweek`*`] [-rotate-schedule-day` *`chron_dayofmonth`*`] [-rotate-schedule-hour` *`chron_hour`*`] -rotate-schedule-minute` *`chron_minute`* Le `-rotate-schedule-minute` le paramètre est requis si vous configurez la rotation du journal d'audit basée sur le temps.

2. Activation de l'audit S3 :

   `vserver object-store-server audit enable -vserver` *`svm_name`*

Exemples

L'exemple suivant illustre une configuration d'audit qui audite tous les événements S3 (par défaut) à l'aide d'une rotation basée sur la taille. Les journaux sont stockés dans le répertoire /audit_log. La taille maximale du fichier journal est de 200 Mo. 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 illustre une configuration d'audit qui audite tous les événements S3 (par défaut) à l'aide d'une rotation basée sur la taille. La taille maximale du fichier journal est de 100 Mo (valeur par défaut) et les journaux sont conservés pendant 5 jours avant leur suppression.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

L'exemple suivant crée une configuration d'audit qui audite les événements de gestion S3 et les événements d'activation de règles d'accès centrales à l'aide d'une rotation basée sur le temps. 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
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Sélectionnez des compartiments pour l'audit S3

Vous devez spécifier les compartiments à auditer dans une SVM activée par l'audit.

Ce dont vous avez besoin

- SVM activé pour l'audit S3.

Description de la tâche

Les configurations d'audit S3 sont activées par SVM, mais vous devez sélectionner les compartiments des SVM activés pour l'audit. Si vous ajoutez des compartiments au SVM et que vous souhaitez auditer les nouveaux compartiments, vous devez les sélectionner avec cette procédure. Vous pouvez également disposer de compartiments non audités dans une SVM activée pour l'audit de S3.

Les configurations d'audit restent conservées pour les compartiments jusqu'à ce qu'elles soient supprimées par le `vserver object-store-server audit object-select delete` commande.

Procédure

Sélectionner un compartiment pour l'audit S3 :

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket
bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-
only|deny-only|all}]
```

- `-access` - spécifie le type d'accès aux événements à auditer : `read-only`, `write-only` ou `all` (la valeur par défaut est `all`).
- `-permission` - spécifie le type d'autorisation d'événement à auditer : `allow-only`, `deny-only` ou `all` (la valeur par défaut est `all`).

Exemple

L'exemple suivant crée une configuration d'audit de compartiment qui connecte uniquement les événements autorisés avec un accès en lecture seule :

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Modifiez une configuration d'audit S3

Vous pouvez modifier les paramètres d'audit de compartiments individuels ou la configuration d'audit de toutes les compartiments sélectionnés pour l'audit dans la SVM.

Si vous souhaitez modifier la configuration d'audit pour…	Entrer…
Seaux individuels	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
Tous les compartiments du SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

Exemples

L'exemple suivant modifie la configuration d'audit de compartiment individuel pour auditer uniquement les événements d'accès en écriture :

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

L'exemple suivant modifie la configuration d'audit de tous les buckets du SVM de manière à définir la taille limite des logs à 10 Mo et à conserver 3 fichiers journaux avant de faire pivoter.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Affiche les configurations d'audit S3

Une fois la configuration d'audit terminée, vous pouvez vérifier que l'audit est correctement configuré et activé. Vous pouvez également afficher des informations sur toutes les configurations d'audit du magasin d'objets du cluster.

Description de la tâche

Vous pouvez afficher des informations sur les configurations d'audit de compartiment et SVM.

- Godets : utilisez le `vserver object-store-server audit event-selector show` commande

  Sans aucun paramètre, la commande affiche les informations suivantes sur les compartiments de tous les SVM du cluster avec des configurations d'audit de magasin d'objets :

  - Nom du SVM
  - Nom du compartiment
  - Valeurs d'accès et d'autorisation
- SVM : utilisez le `vserver object-store-server audit show` commande

  Sans aucun paramètre, la commande affiche les informations suivantes sur tous les SVM du cluster avec des configurations d'audit du magasin d'objets :

  - Nom du SVM
  - État d'audit
  - Répertoire cible

Vous pouvez spécifier le `-fields` paramètre pour spécifier les informations de configuration d'audit à afficher.

Procédure

Afficher des informations sur les configurations d'audit S3 :

Si vous souhaitez modifier la configuration pour…	Entrer…
Seaux	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVM	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Exemples

L'exemple suivant affiche les informations pour un seul compartiment :

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

L'exemple suivant affiche les informations pour toutes les compartiments d'un SVM :

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

L'exemple suivant affiche le nom, l'état d'audit, les types d'événements, le format du journal et le répertoire cible de tous les SVM.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

L'exemple suivant affiche les noms des SVM et des détails sur le journal d'audit de tous les SVM.

```
cluster1::> vserver object-store-server audit show -log-save-details

                  Rotation                           Rotation
      Vserver     File Size Rotation Schedule        Limit
      ----------- --------- ------------------------ --------
      vs1         100MB     -                        0
```

L'exemple suivant s'affiche sous forme de liste toutes les informations de configuration d'audit relatives à tous les SVM.

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                           Log Format: json
                  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
                  Log Retention Time: 0s
```