Prüfung von S3-Ereignissen

ONTAP 9

NetApp
February 12, 2026

Inhalt

Prüfung von S3-Ereignissen

Hier erhalten Sie Informationen über das Auditing von ONTAP S3 Ereignissen

Ab ONTAP 9.10.1 können Daten- und Managementereignisse in ONTAP S3 Umgebungen geprüft werden. Die S3-Audit-Funktion ähnelt den vorhandenen NAS-Audit-Funktionen. Zudem können S3- und NAS-Audits in einem Cluster nebeneinander bestehen.

Wenn Sie eine S3-Audit-Konfiguration auf einer SVM erstellen und aktivieren, werden S3-Ereignisse in einer Protokolldatei aufgezeichnet. Sie können die folgenden Ereignisse angeben, die protokolliert werden sollen:

Objektzugriffsereignisse (Daten) nach Freigabe

9.11.1:

- ListBucketVersions
- ListBucket (ListObjects von 9.10.1 wurde in dieses umbenannt)
- ListAllMyBuckets (ListBuckets von 9.10.1 wurde in diese umbenannt)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuchs
- ListObjekte
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- ListUploads
- ListenTeile

Management-Ereignisse nach Freigabe

9.15.1:

- GetBucketCORS

- PutBucketCORS
- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockKonfiguration
- GetBucketObjectLockKonfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- GetBucketPolicy
- CopyObject
- UploadPartCopy
- PutBucketPolicy
- DeleteBucketRichtlinien

9.11.1:

- GetBucketVersioning
- PutBucketVersioning

9.10.1:

- HeadBucket
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

Das Protokollformat ist JavaScript Object Notation (JSON).

Der kombinierte Grenzwert für S3- und NFS-Audit-Konfigurationen beträgt 400 SVMs pro Cluster.

Die folgende Lizenz ist erforderlich:

- ONTAP One – ehemals Teil des Kernpakets – für ONTAP S3 Protokoll und Storage

Weitere Informationen finden Sie unter "Funktionsweise des ONTAP-Prüfprozesses".

Garantierte Audits

S3- und NAS-Audits sind standardmäßig gewährleistet. ONTAP garantiert, dass alle prüffähigen Bucket-Zugriffsereignisse aufgezeichnet werden, selbst wenn ein Node nicht verfügbar ist. Ein angeforderter Bucket-Vorgang kann erst abgeschlossen werden, wenn der Prüfdatensatz für diesen Vorgang im Staging-Volume auf persistentem Storage gespeichert wird. Wenn Audit-Datensätze nicht in den Staging-Dateien übergeben werden können, entweder aufgrund von unzureichendem Speicherplatz oder wegen anderer Probleme, werden Client-Vorgänge verweigert.

Speicherplatzanforderungen für Auditing

Im ONTAP-Auditersystem werden die Audit-Datensätze zunächst in binären Staging-Dateien auf einzelnen Knoten gespeichert. Sie werden in regelmäßigen Abständen konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis der Auditereignisse für die SVM gespeichert sind.

Die Staging-Dateien werden in einem dedizierten Staging-Volume gespeichert, das von ONTAP beim Erstellen der Audit-Konfiguration erstellt wird. Es gibt ein Staging-Volume pro Aggregat.

In der Überwachungskonfiguration müssen ausreichend Platz vorhanden sein:

- Für die Staging-Volumes in Aggregaten, die geprüfte Buckets enthalten
- Für das Volume, das das Verzeichnis enthält, in dem konvertierte Ereignisprotokolle gespeichert werden.

Sie können die Anzahl der Ereignisprotokolle und damit den verfügbaren Speicherplatz im Volume mit einer von zwei Methoden zum Erstellen der S3-Überwachungskonfiguration steuern:

- Ein numerischer Grenzwert; der `-rotate-limit` Parameter steuert die Mindestanzahl an Audit-Dateien, die beibehalten werden müssen.
- Ein Zeitlimit; der `-retention-duration` Parameter steuert den maximalen Zeitraum, in dem Dateien aufbewahrt werden können.

In beiden Parametern können nach dem Überschreiten der Konfiguration ältere Audit-Dateien gelöscht werden, um Platz für neuere zu schaffen. Für beide Parameter ist der Wert 0, was bedeutet, dass alle Dateien gepflegt werden müssen. Um ausreichend Platz zu gewährleisten, empfiehlt es sich daher, einen der Parameter auf einen Wert ohne Null zu setzen.

Aus Gründen der garantierten Prüfung kann es nicht möglich sein, neue Audit-Daten zu erstellen, wenn der für Audit-Daten verfügbare Speicherplatz vor dem jeweiligen Rotationslimit überschritten wird, was zu einem Ausfall des Clients, der auf Daten zugreift, führt. Daher muss die Auswahl dieses Werts und des Platzes, der für die Prüfung zugewiesen wird, sorgfältig ausgewählt werden, und Sie müssen auf Warnungen über den verfügbaren Speicherplatz des Auditsystems reagieren.

Weitere Informationen finden Sie unter "Grundlegende Prüfungskonzepte".

Planen Sie eine ONTAP S3 Auditing-Konfiguration

Sie müssen eine Reihe von Parametern für die S3-Überwachungskonfiguration angeben oder die Standardeinstellungen akzeptieren. Insbesondere sollten Sie berücksichtigen, welche Protokollrotationsparameter dazu beitragen, ausreichend freien Speicherplatz zu gewährleisten.

Erfahren Sie mehr über `vserver object-store-server audit create` in der "ONTAP-

Befehlsreferenz".

Allgemeine Parameter

Es gibt zwei erforderliche Parameter, die Sie beim Erstellen der Überwachungskonfiguration angeben müssen. Es gibt außerdem drei optionale Parameter, die Sie angeben können.

Informationstyp	Option	Erforderlich
SVM Name Name der SVM, auf der die Audit-Konfiguration erstellt werden soll. Die SVM muss bereits vorhanden und für S3 aktiviert sein.	`-vserver svm_name`	Ja.
Zielpfad protokollieren Gibt an, wo die konvertierten Audit-Protokolle gespeichert werden. Der Pfad muss auf der SVM bereits vorhanden sein. Der Pfad kann bis zu 864 Zeichen lang sein und muss über Lese-/Schreibberechtigungen verfügen. Wenn der Pfad nicht gültig ist, schlägt der Befehl für die Prüfungskonfiguration fehl.	`-destination text`	Ja.
Kategorien von Ereignissen zur Prüfung Folgende Ereigniskategorien können geprüft werden: • Data GetObject, PutObject und DeleteObject Ereignisse • Management-Events „PutBucket“ und „DeleteBucket“ Standardmäßig werden nur Datenereignisse geprüft.	`-events {data|management}, …`	Nein

Sie können einen der folgenden Parameter eingeben, um die Anzahl der Audit-Log-Dateien zu steuern. Wenn kein Wert eingegeben wird, bleiben alle Protokolldateien erhalten.

Informationstyp	Option	Erforderlich
Log-Dateien Rotationsgrenze Legt fest, wie viele Audit-Log-Dateien gespeichert werden sollen, bevor die älteste Protokolldatei ausgedreht wird. Wenn Sie beispielsweise einen Wert von 5 eingeben, werden die letzten fünf Protokolldateien beibehalten. Der Wert 0 gibt an, dass alle Protokolldateien aufbewahrt werden. Der Standardwert ist 0.	`-rotate-limit integer`	Nein

Dauer der Protokolldateien Legt fest, wie lange eine Protokolldatei aufbewahrt werden kann, bevor sie gelöscht wird. Wenn Sie beispielsweise einen Wert von 5d0h0m eingeben, werden Protokolle gelöscht, die älter als 5 Tage sind. Der Wert 0 gibt an, dass alle Protokolldateien aufbewahrt werden. Der Standardwert ist 0.	`-retention duration` *`integer_time`*	Nein

Parameter für die Drehung des Prüfprotokolls

Sie können Prüfprotokolle basierend auf Größe oder Zeitplan drehen. Standardmäßig werden Auditprotokolle auf der Grundlage der Größe gedreht.

Drehen Sie Protokolle basierend auf der Protokollgröße

Wenn Sie die Standard-Protokollrotation-Methode und die Standard-Protokollgröße verwenden möchten, müssen Sie keine spezifischen Parameter für die Protokollrotation konfigurieren. Die Standard-Protokollgröße beträgt 100 MB.

Wenn Sie die Standard-Protokollgröße nicht verwenden möchten, können Sie den `-rotate-size` Parameter so konfigurieren, dass eine benutzerdefinierte Protokollgröße angegeben wird.

Wenn Sie die Rotation allein anhand einer Protokollgröße zurücksetzen möchten, verwenden Sie den folgenden Befehl, um die Einstellung des `-rotate-schedule-minute` Parameters aufzuheben:

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

Protokolle nach einem Zeitplan drehen

Wenn Sie die Prüfprotokolle nach einem Zeitplan drehen möchten, können Sie die Protokollrotation mithilfe der zeitbasierten Rotationsparameter in beliebiger Kombination planen.

- Wenn Sie `-rotate-schedule-minute` eine zeitbasierte Rotation verwenden, ist der Parameter obligatorisch.
- Alle anderen zeitbasierten Rotationsparameter sind optional.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- Der Rotationsplan wird unter Verwendung aller zeitbezogenen Werte berechnet. Wenn Sie beispielsweise nur den `-rotate-schedule-minute` Parameter angeben, werden die Audit-Log-Dateien basierend auf den an allen Wochentagen festgelegten Minuten gedreht, während aller Stunden an allen Monaten des Jahres.
- Wenn Sie nur einen oder zwei zeitbasierte Rotationsparameter angeben (z. B. `-rotate-schedule -month` und `-rotate-schedule-minutes`), werden die Protokolldateien basierend auf den Minutenwerten gedreht, die Sie an allen Wochentagen, zu allen Stunden, aber nur während der angegebenen Monate angegeben haben.

Sie können z. B. angeben, dass das Audit-Protokoll in den Monaten Januar, März und August alle Montag, Mittwoch und Samstag um 10:30 Uhr gedreht werden soll

- Wenn Sie Werte für `-rotate-schedule-dayofweek` und angeben `-rotate-schedule-day`, werden diese unabhängig voneinander betrachtet.

  Wenn Sie beispielsweise `-rotate-schedule-dayofweek` Freitag und `-rotate-schedule-day` 13 angeben, werden die Prüfprotokolle an jedem Freitag und am 13. Tag des angegebenen Monats gedreht, nicht nur an jedem Freitag, dem 13…

- Wenn Sie die Rotation auf Basis eines Zeitplans zurücksetzen möchten, verwenden Sie den folgenden Befehl, um die Einstellung aufzuheben `-rotate-size parameter`:

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

Drehen Sie Protokolle basierend auf der Protokollgröße und dem Zeitplan

Sie können wählen, ob Sie die Protokolldateien basierend auf der Protokollgröße und einem Zeitplan drehen möchten, indem Sie den Parameter -rotieren-size und die zeitbasierten Rotationsparameter in einer beliebigen Kombination einstellen. Beispiel: Wenn `-rotate-size` auf 10 MB gesetzt ist und `-rotate-schedule -minute` auf 15 eingestellt ist, drehen sich die Protokolldateien, wenn die Größe der Protokolldatei 10 MB oder auf die 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt) erreicht.

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Erstellen und Aktivieren einer ONTAP S3 Auditing-Konfiguration

Für die Implementierung der S3-Prüfung wird zuerst eine persistente Objektspeicherauditierung auf einer S3-fähigen SVM erstellt, dann die Konfiguration aktiviert.

Bevor Sie beginnen

- Sie haben eine S3-fähige SVM.
- Vergewissern Sie sich, dass ausreichend Speicherplatz für das Staging von Volumes in der lokalen Ebene vorhanden ist.

Über diese Aufgabe

Für jede SVM, die S3-Buckets enthält, die Sie prüfen möchten, ist eine Audit-Konfiguration erforderlich. Sie können S3-Prüfungen auf neuen oder vorhandenen S3-Servern aktivieren. Das Auditing von Konfigurationen bleibt in einer S3-Umgebung erhalten, bis sie mit dem Befehl **vserver Object-Store-Server Audit delete** entfernt werden.

Die S3-Audit-Konfiguration gilt für alle Buckets der SVM, die Sie für das Auditing auswählen. Eine SVM, die für Audits aktiviert ist, kann geprüfte und nicht geprüfte Buckets enthalten.

Es wird empfohlen, die S3-Prüfung für automatische Protokollrotation anhand von Protokollgröße oder Zeitplan zu konfigurieren. Wenn Sie die automatische Protokollrotation nicht konfigurieren, bleiben alle Protokolldateien standardmäßig erhalten. Sie können S3-Protokolldateien auch manuell mit dem Befehl **vserver object-Store-Server Audit rotieren-log** drehen.

Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Zielpfad nicht auf dem Root-Volume befinden.

Schritte

1. Erstellen Sie die Überwachungskonfiguration, um Prüfprotokolle basierend auf Protokollgröße oder einem Zeitplan zu drehen.

Wenn Sie die Prüfprotokolle drehen möchten, um…	Eingeben…
Protokollgröße	`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]}]`
Einen Zeitplan	`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`* Der `-rotate-schedule-minute` Parameter ist erforderlich, wenn Sie die zeitbasierte Rotation des Überwachungsprotokolls konfigurieren.

2. S3-Auditing aktivieren:

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

Beispiele

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die alle S3-Ereignisse (die Standardeinstellung) anhand von größenbasierter Rotation prüft. Die Protokolle werden im Verzeichnis /Audit_log gespeichert. Die maximale Größe der Protokolldatei beträgt 200 MB. Die Protokolle werden gedreht, wenn sie 200 MB groß.

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

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die alle S3-Ereignisse (die Standardeinstellung) anhand von größenbasierter Rotation prüft. Die maximale Protokolldateigröße beträgt 100 MB (Standard) und die Protokolle werden 5 Tage lang aufbewahrt, bevor sie gelöscht werden.

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

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die S3-Managementereignisse und zentrale Zugriffs- und Staging-Ereignisse mithilfe zeitbasierter Rotation prüft. Die Prüfprotokolle werden monatlich um

12:30 Uhr an allen Wochentagen gedreht. Die Protokollrotationsgrenze ist 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
```

Wählen Sie Buckets für ONTAP S3 Auditing aus

Sie müssen angeben, welche Buckets in einer SVM mit Audit-Aktivierung geprüft werden sollen.

Bevor Sie beginnen

- Sie haben eine SVM für die S3-Prüfung aktiviert.

Über diese Aufgabe

S3-Audit-Konfigurationen sind auf SVM-Basis aktiviert, jedoch müssen Sie die Buckets für SVMS auswählen, die für die Prüfung aktiviert sind. Wenn der SVM Buckets hinzugefügt werden sollen und die neuen Buckets geprüft werden sollen, müssen Sie diese bei diesem Verfahren auswählen. Es können auch nicht geprüfte Buckets in einer SVM für die S3-Prüfung aktiviert sein.

Die Überwachungskonfigurationen bleiben für Buckets bestehen, bis `vserver object-store-server audit event-selector delete` sie mit dem Befehl entfernt werden.

Schritte

1. Wählen Sie einen Bucket für die S3-Prüfung aus:

   ```
   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`: Gibt die Art des zu überwachenden Ereigniszugriffs an: `read-only`, `write-only` Oder `all` (Standard ist `all`).
   - `-permission`: Gibt die Art der zu prüfenden Ereignisberechtigung an: `allow-only`, `deny-only` Oder `all` (Standard ist `all`).

Beispiel

Im folgenden Beispiel wird eine Bucket-Audit-Konfiguration erstellt, die nur erlaubte Ereignisse mit schreibgeschütztem Zugriff protokolliert:

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

Ändern Sie eine ONTAP S3 Überwachungskonfiguration

Sie können die Audit-Parameter einzelner Buckets oder die Auditing-Konfiguration aller für das Audit in der SVM ausgewählten Buckets ändern.

Wenn Sie die Audit-Konfiguration ändern möchten für…	Eingeben…
Einzelne Buckets	`vserver object-store-server audit event-selector modify -vserver` *svm_name* `[-bucket` *bucket_name*`] [`*parameters to modify*`]`
Alle Buckets in der SVM	`vserver object-store-server audit modify -vserver` *svm_name* `[`*parameters to modify*`]`

Beispiele

Im folgenden Beispiel wird eine individuelle Bucket-Audit-Konfiguration geändert, um nur schreibgeschützten Zugriffsereignisse zu überwachen:

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

Im folgenden Beispiel wird die Audit-Konfiguration aller Buckets in der SVM geändert, um die Protokollgröße auf 10 MB zu ändern und 3 Protokolldateien vor der Drehung aufzubewahren.

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

Zeigen Sie die ONTAP S3 Audit-Konfigurationen an

Nach Abschluss der Überwachungskonfiguration können Sie überprüfen, ob die Prüfung ordnungsgemäß konfiguriert und aktiviert ist. Sie können auch Informationen zu allen Objektspeicherprüfungen im Cluster anzeigen.

Über diese Aufgabe

Sie können Informationen zu Bucket- und SVM-Audit-Konfigurationen anzeigen.

- Buckets: Verwenden Sie den `vserver object-store-server audit event-selector show` Befehl

  Ohne Parameter zeigt der Befehl die folgenden Informationen über Buckets in allen SVMs im Cluster mit Objektspeicherprüfungen-Konfigurationen an:

  - SVM-Name
  - Bucket-Name
  - Zugriffs- und Berechtigungswerte
- SVMs: Verwenden Sie den `vserver object-store-server audit show` Befehl

  Ohne Parameter zeigt der Befehl die folgenden Informationen über alle SVMs im Cluster mit Objektspeicherprüfungen-Konfigurationen an:

- SVM-Name
- Audit-Status
- Zielverzeichnis

Sie können den `-fields` Parameter angeben, um festzulegen, welche Audit-Konfigurationsinformationen angezeigt werden sollen.

Schritte

Informationen zu S3-Audit-Konfigurationen anzeigen:

Wenn Sie die Konfiguration ändern möchten für…	Eingeben…
Buckets	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVMs	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Beispiele

Im folgenden Beispiel werden Informationen für einen einzelnen Bucket angezeigt:

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

Im folgenden Beispiel werden Informationen für alle Buckets einer SVM angezeigt:

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

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

Im folgenden Beispiel werden Name, Audit-Status, Ereignistypen, Protokollformat und Zielverzeichnis für alle SVMs angezeigt.

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

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

Im folgenden Beispiel werden die Namen und Details zu den SVM-Protokollen für alle SVMs angezeigt.

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

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

Das folgende Beispiel zeigt alle Informationen zur Audit-Konfiguration über alle SVMs in Listenform.

```
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
```