Controllare gli eventi S3

ONTAP 9

NetApp
April 24, 2024

Sommario

Controllare gli eventi S3

Controllare gli eventi S3

A partire da ONTAP 9.10.1, è possibile controllare i dati e gli eventi di gestione negli ambienti ONTAP S3. La funzionalità di audit S3 è simile alle funzionalità di auditing NAS esistenti e l'auditing S3 e NAS può coesistere in un cluster.

Quando si crea e si attiva una configurazione di controllo S3 su una SVM, gli eventi S3 vengono registrati in un file di registro. È possibile specificare i seguenti eventi da registrare:

- Eventi di accesso a oggetti (dati)

  GetObject, PutObject e DeleteObject

- Eventi di gestione

  Putbucket e Deletebucket

Il formato del log è JavaScript Object Notation (JSON).

Il limite combinato per le configurazioni di controllo S3 e NFS è di 50 SVM per cluster.

È richiesto il seguente bundle di licenza:

- Bundle core, per protocollo e storage ONTAP S3

Per ulteriori informazioni, vedere "Come funziona il processo di audit di ONTAP".

Auditing garantito

Per impostazione predefinita, è garantito il controllo S3 e NAS. ONTAP garantisce la registrazione di tutti gli eventi di accesso al bucket verificabili, anche se un nodo non è disponibile. Un'operazione bucket richiesta non può essere completata fino a quando il record di audit per tale operazione non viene salvato nel volume di staging sullo storage persistente. Se non è possibile eseguire il commit dei record di audit nei file di staging, a causa di spazio insufficiente o a causa di altri problemi, le operazioni del client vengono negate.

Requisiti di spazio per il controllo

Nel sistema di audit ONTAP, i record di audit vengono inizialmente memorizzati in file di staging binari su singoli nodi. Periodicamente, vengono consolidati e convertiti in registri eventi leggibili dall'utente, memorizzati nella directory del registro eventi di controllo per SVM.

I file di staging vengono memorizzati in un volume di staging dedicato, creato da ONTAP al momento della creazione della configurazione di audit. Esiste un volume di staging per aggregato.

È necessario pianificare uno spazio disponibile sufficiente nella configurazione di controllo:

- Per i volumi di staging in aggregati che contengono bucket controllati.
- Per il volume contenente la directory in cui sono memorizzati i registri degli eventi convertiti.

È possibile controllare il numero di registri eventi e quindi lo spazio disponibile nel volume utilizzando uno dei

due metodi per creare la configurazione di controllo S3:

- Un limite numerico; il `-rotate-limit` parametro controlla il numero minimo di file di audit che devono essere conservati.
- Un limite di tempo; il `-retention-duration` parametro controlla il periodo massimo di conservazione dei file.

In entrambi i parametri, una volta superato il valore configurato, è possibile eliminare i file di audit più vecchi per fare spazio a quelli più recenti. Per entrambi i parametri, il valore è 0, a indicare che tutti i file devono essere mantenuti. Per garantire uno spazio sufficiente, è quindi consigliabile impostare uno dei parametri su un valore diverso da zero.

A causa del controllo garantito, se lo spazio disponibile per i dati di audit si esaurisce prima del limite di rotazione, non è possibile creare dati di audit più recenti, con conseguente impossibilità per i client di accedere ai dati. Pertanto, la scelta di questo valore e dello spazio allocato per l'audit deve essere scelta con attenzione, ed è necessario rispondere agli avvisi sullo spazio disponibile dal sistema di audit.

Per ulteriori informazioni, vedere "Concetti di controllo di base".

Pianificare una configurazione di controllo S3

È necessario specificare una serie di parametri per la configurazione di controllo S3 o accettare le impostazioni predefinite. In particolare, è necessario considerare quali parametri di rotazione del log contribuiranno a garantire un adeguato spazio libero.

Vedere **`vserver object-store-server audit create`** pagina man per i dettagli della sintassi.

Parametri generali

Sono necessari due parametri da specificare quando si crea la configurazione di controllo. È possibile specificare anche tre parametri opzionali.

Tipo di informazione	Opzione	Obbligatorio
Nome SVM Nome della SVM su cui creare la configurazione di controllo. La SVM deve già esistere ed essere abilitata per S3.	`-verserver` *`svm_name`*	Sì
Percorso di destinazione del registro Specifica dove sono memorizzati i log di audit convertiti. Il percorso deve già esistere sulla SVM. Il percorso può contenere fino a 864 caratteri e deve disporre di permessi di lettura/scrittura. Se il percorso non è valido, il comando di configurazione del controllo non riesce.	`-destination` *`text`*	Sì

Categorie di eventi da controllare È possibile verificare le seguenti categorie di eventi: • Eventi Data GetObject, PutObject e DeleteObject • Gestione degli eventi Putbucket e Deletebucket L'impostazione predefinita prevede solo l'audit degli eventi dati.	`-events {data|management}, …`	No

È possibile inserire uno dei seguenti parametri per controllare il numero di file di log di audit. Se non viene immesso alcun valore, tutti i file di registro vengono conservati.

Tipo di informazione	Opzione	Obbligatorio
Limite di rotazione dei file di log Determina il numero di file di log di audit da conservare prima di estrarre il file di log più vecchio. Ad esempio, se si immette il valore 5, vengono conservati gli ultimi cinque file di registro. Il valore 0 indica che tutti i file di log vengono conservati. Il valore predefinito è 0.	`-rotate-limit` *`integer`*	No
Limite di durata dei file di log Determina per quanto tempo un file di log può essere conservato prima di essere cancellato. Ad esempio, se si immette un valore di 5d0h0m, i registri più vecchi di 5 giorni vengono cancellati. Il valore 0 indica che tutti i file di log vengono conservati. Il valore predefinito è 0.	`-retention duration` *`integer_time`*	No

Parametri per la rotazione del registro di controllo

È possibile ruotare i registri di audit in base alle dimensioni o alla pianificazione. L'impostazione predefinita prevede la rotazione dei registri di controllo in base alle dimensioni.

Ruotare i registri in base alle dimensioni del registro

Se si desidera utilizzare il metodo di rotazione del log predefinito e la dimensione del log predefinita, non è necessario configurare alcun parametro specifico per la rotazione del log. La dimensione predefinita del registro è 100 MB.

Se non si desidera utilizzare la dimensione predefinita del registro, è possibile configurare `-rotate-size` parametro per specificare una dimensione di log personalizzata.

Se si desidera ripristinare la rotazione solo in base alle dimensioni del log, utilizzare il comando seguente per annullare l'impostazione di `-rotate-schedule-minute` parametro:

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

Ruotare i registri in base a una pianificazione

Se si sceglie di ruotare i registri di controllo in base a una pianificazione, è possibile pianificare la rotazione dei registri utilizzando i parametri di rotazione basati sul tempo in qualsiasi combinazione.

- Se si utilizza la rotazione basata sul tempo, il `-rotate-schedule-minute` il parametro è obbligatorio.
- Tutti gli altri parametri di rotazione basati sul tempo sono opzionali.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- Il programma di rotazione viene calcolato utilizzando tutti i valori relativi al tempo. Ad esempio, se si specifica solo il `-rotate-schedule-minute` i file di log di audit vengono ruotati in base ai minuti specificati in tutti i giorni della settimana, durante tutte le ore in tutti i mesi dell'anno.
- Se si specificano solo uno o due parametri di rotazione basati sul tempo (ad esempio, `-rotate -schedule-month` e. `-rotate-schedule-minutes`), i file di log vengono ruotati in base ai valori dei minuti specificati in tutti i giorni della settimana, durante tutte le ore, ma solo durante i mesi specificati.

  Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato durante i mesi di gennaio, marzo e agosto tutti i lunedì, mercoledì e sabato alle 10:30

- Se si specificano i valori per entrambi `-rotate-schedule-dayofweek` e. `-rotate-schedule-day`, sono considerati indipendenti.

  Ad esempio, se si specifica `-rotate-schedule-dayofweek` Come venerdì e. `-rotate-schedule -day` Come 13, i registri di audit verrebbero ruotati ogni venerdì e il 13° giorno del mese specificato, non solo ogni venerdì 13.

- Se si desidera ripristinare la rotazione solo in base a una pianificazione, utilizzare il comando seguente per annullare l'impostazione di `-rotate-size parameter`:

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

Rotazione dei registri in base alle dimensioni e alla pianificazione dei registri

È possibile scegliere di ruotare i file di log in base alle dimensioni del log e a una pianificazione impostando sia il parametro -rotate-size che i parametri di rotazione basati sul tempo in qualsiasi combinazione. Ad esempio: Se `-rotate-size` È impostato su 10 MB e. `-rotate-schedule-minute` È impostato su 15, i file di log ruotano quando le dimensioni del file di log raggiungono i 10 MB o al 15° minuto di ogni ora (a seconda dell'evento che si verifica per primo).

Creare e abilitare una configurazione di controllo S3

Per implementare il controllo S3, creare prima una configurazione di controllo dell'archivio di oggetti persistente su una SVM abilitata per S3, quindi attivare la configurazione.

Di cosa hai bisogno

- Una SVM abilitata per S3.
- Spazio sufficiente per lo staging dei volumi nell'aggregato.

A proposito di questa attività

Per ogni SVM contenente i bucket S3 che si desidera controllare è necessaria una configurazione di controllo. È possibile attivare il controllo S3 su server S3 nuovi o esistenti. Le configurazioni di controllo persistono in un ambiente S3 fino a quando non vengono rimosse dal comando **vserver object-store-server audit delete**.

La configurazione di controllo S3 si applica a tutti i bucket della SVM selezionati per il controllo. Una SVM abilitata all'audit può contenere bucket controllati e non verificati.

Si consiglia di configurare il controllo S3 per la rotazione automatica del log, determinata dalle dimensioni del log o da una pianificazione. Se non si configura la rotazione automatica del log, tutti i file di log vengono conservati per impostazione predefinita. È inoltre possibile ruotare manualmente i file di log S3 utilizzando il comando **vserver object-store-server audit rotate-log**.

Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione non può trovarsi sul volume root.

Procedura

1. Creare la configurazione di controllo per ruotare i registri di controllo in base alle dimensioni del registro o a una pianificazione.

Se si desidera ruotare i registri di audit di…	Inserisci…
Dimensione del log	`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]}]`
Un calendario	`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`* Il `-rotate-schedule-minute` il parametro è obbligatorio se si configura la rotazione del log di audit basata sul tempo.

2. Abilita controllo S3:

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

Esempi

Nell'esempio seguente viene creata una configurazione di controllo che controlla tutti gli eventi S3

(impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. I registri vengono memorizzati nella directory /audit_log. Il limite delle dimensioni del file di log è di 200 MB. I log vengono ruotati quando raggiungono le dimensioni di 200 MB.

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

Nell'esempio seguente viene creata una configurazione di controllo che controlla tutti gli eventi S3 (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il limite delle dimensioni del file di registro è di 100 MB (impostazione predefinita) e i registri vengono conservati per 5 giorni prima di essere cancellati.

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

Nell'esempio seguente viene creata una configurazione di controllo che controlla gli eventi di gestione S3 e gli eventi di staging dei criteri di accesso centrale utilizzando la rotazione basata sul tempo. I registri di audit vengono ruotati mensilmente alle 12:30 tutti i giorni della settimana. Il limite di rotazione del log è 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
```

Selezionare i bucket per il controllo S3

È necessario specificare quali bucket eseguire il controllo in una SVM abilitata per l'audit.

Di cosa hai bisogno

- SVM abilitato per il controllo S3.

A proposito di questa attività

Le configurazioni di controllo S3 sono abilitate per SVM, ma è necessario selezionare i bucket nelle SVM che sono abilitati per l'audit. Se si aggiungono bucket alla SVM e si desidera che i nuovi bucket vengano controllati, è necessario selezionarli con questa procedura. È inoltre possibile avere bucket non controllati in una SVM abilitata per il controllo S3.

Le configurazioni di controllo persistono per i bucket fino a quando non vengono rimosse da `vserver object-store-server audit object-select delete` comando.

Procedura

Seleziona un bucket per 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` - specifica il tipo di accesso all'evento da sottoporre a verifica: `read-only`, `write-only` oppure `all` (il valore predefinito è `all`).
- `-permission` - specifica il tipo di autorizzazione all'evento da sottoporre a verifica: `allow-only`, `deny-only` oppure `all` (il valore predefinito è `all`).

Esempio

Nell'esempio seguente viene creata una configurazione di controllo del bucket che registra solo gli eventi consentiti con accesso in sola lettura:

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

Modificare una configurazione di controllo S3

È possibile modificare i parametri di controllo dei singoli bucket o la configurazione di controllo di tutti i bucket selezionati per l'audit nella SVM.

Se si desidera modificare la configurazione dell'audit per…	Inserisci…
Bucket individuali	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
Tutti i bucket di SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

Esempi

Nell'esempio seguente viene modificata una singola configurazione di controllo del bucket per controllare solo gli eventi di accesso di sola scrittura:

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

Nell'esempio riportato di seguito viene modificata la configurazione di controllo di tutti i bucket di SVM per modificare il limite delle dimensioni dei log a 10 MB e conservare 3 file di log prima della rotazione.

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

Mostrare le configurazioni di controllo S3

Una volta completata la configurazione di controllo, è possibile verificare che il controllo sia configurato correttamente e sia attivato. È inoltre possibile visualizzare informazioni su tutte le configurazioni di controllo dell'archivio di oggetti nel cluster.

A proposito di questa attività

È possibile visualizzare informazioni sulle configurazioni di controllo bucket e SVM.

- Bucket – utilizzare `vserver object-store-server audit event-selector show` comando

  Senza alcun parametro, il comando visualizza le seguenti informazioni sui bucket in tutte le SVM del cluster con configurazioni di controllo degli archivi di oggetti:

- Nome SVM
- Nome bucket
- Valori di accesso e autorizzazione

- SVM: Utilizzare `vserver object-store-server audit show` comando

  Senza alcun parametro, il comando visualizza le seguenti informazioni su tutte le SVM nel cluster con configurazioni di controllo degli archivi di oggetti:

  - Nome SVM
  - Stato di audit
  - Directory di destinazione

È possibile specificare `-fields` parametro per specificare le informazioni di configurazione di controllo da visualizzare.

Procedura

Mostra informazioni sulle configurazioni di controllo S3:

Se si desidera modificare la configurazione per…	Inserisci…
Bucket	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVM	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a un singolo bucket:

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

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i bucket di una SVM:

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

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

Nell'esempio riportato di seguito vengono visualizzati il nome, lo stato di controllo, i tipi di evento, il formato del registro e la directory di destinazione di tutte le SVM.

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

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

Nell'esempio seguente vengono visualizzati i nomi e i dettagli SVM relativi al registro di controllo per tutte le SVM.

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

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

Nell'esempio riportato di seguito vengono visualizzate tutte le informazioni di configurazione dell'audit relative a tutte le 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
```