Auditoria S3 eventos

ONTAP 9

NetApp
January 17, 2025

Índice

Auditoria S3 eventos

Auditoria S3 eventos

A partir do ONTAP 9.10,1, você pode auditar dados e eventos de gerenciamento em ambientes ONTAP S3. A funcionalidade de auditoria do S3 é semelhante aos recursos de auditoria nas existentes, e a auditoria do S3 e nas pode coexistir em um cluster.

Quando você cria e ativa uma configuração de auditoria do S3 em um SVM, os eventos do S3 são registrados em um arquivo de log. Você pode especificar os seguintes eventos a serem registrados:

Eventos de acesso a objetos (dados) por lançamento

9.11.1:

- ListBucketVersions
- ListBucket (ListObjects of 9.10.1 foi renomeado para este)
- ListAllMyBuckets (ListBuckets de 9.10.1 foi renomeado para este)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPCompletar
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- Marcação de objetos
- ListUploads
- ListParts

Eventos de gerenciamento por liberação

9.15.1:

- GetBucketCORS
- PutBucketCORS

- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- Retenção PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- Política de GetBucketPolicy
- CopyObject
- UploadPartCopy
- Política de PutBucketPolicy
- DeleteBucketPolicy

9.11.1:

- GetBucketControle de versão
- PutBucketControle de versão

9.10.1:

- Balde para a cabeça
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketlocalização

O formato de log é JavaScript Object Notation (JSON).

O limite combinado para configurações de auditoria S3 e NFS é de 400 SVMs por cluster.

É necessária a seguinte licença:

- ONTAP One, anteriormente parte do pacote principal, para protocolo e storage ONTAP S3

Para obter mais informações, "Como funciona o processo de auditoria do ONTAP"consulte .

Auditoria garantida

Por padrão, a auditoria S3 e nas é garantida. O ONTAP garante que todos os eventos de acesso de bucket auditáveis sejam registrados, mesmo que um nó não esteja disponível. Uma operação de bucket solicitada não pode ser concluída até que o Registro de auditoria dessa operação seja salvo no volume de estadiamento no armazenamento persistente. Se os Registros de auditoria não puderem ser confirmados nos arquivos de teste, seja por espaço insuficiente ou por causa de outros problemas, as operações do cliente serão negadas.

Requisitos de espaço para auditoria

No sistema de auditoria do ONTAP, os Registros de auditoria são armazenados inicialmente em arquivos de teste binário em nós individuais. Periodicamente, eles são consolidados e convertidos em logs de eventos legíveis pelo usuário, que são armazenados no diretório de log de eventos de auditoria do SVM.

Os arquivos de estadiamento são armazenados em um volume de estadiamento dedicado, que é criado pelo ONTAP quando a configuração de auditoria é criada. Há um volume de estadiamento por agregado.

Você precisa Planejar espaço disponível suficiente na configuração de auditoria:

- Para os volumes de estadiamento em agregados que contêm buckets auditados.
- Para o volume que contém o diretório onde os logs de eventos convertidos são armazenados.

Você pode controlar o número de logs de eventos e, portanto, o espaço disponível no volume, usando um de dois métodos ao criar a configuração de auditoria S3:

- Um limite numérico; o `-rotate-limit` parâmetro controla o número mínimo de arquivos de auditoria que devem ser preservados.
- Um limite de tempo; o `-retention-duration` parâmetro controla o período máximo que os arquivos podem ser preservados.

Em ambos os parâmetros, uma vez que o configurado é excedido, os arquivos de auditoria mais antigos podem ser excluídos para abrir espaço para os mais novos. Para ambos os parâmetros, o valor é 0, indicando que todos os arquivos devem ser mantidos. Para garantir espaço suficiente, é, portanto, uma prática recomendada definir um dos parâmetros para um valor não zero.

Devido à auditoria garantida, se o espaço disponível para os dados de auditoria acabar antes do limite de rotação, os dados de auditoria mais recentes não podem ser criados, resultando em falha no acesso dos clientes aos dados. Portanto, a escolha desse valor e do espaço alocado à auditoria deve ser escolhida cuidadosamente, e você deve responder a avisos sobre o espaço disponível do sistema de auditoria.

Para obter mais informações, "Conceitos básicos de auditoria"consulte .

Planejar uma configuração de auditoria S3

Você deve especificar vários parâmetros para a configuração de auditoria S3 ou aceitar os padrões. Em particular, você deve considerar quais parâmetros de rotação de log ajudarão a garantir espaço livre adequado.

Consulte a *`vserver object-store-server audit create`página man * para obter detalhes de sintaxe.

Parâmetros gerais

Há dois parâmetros necessários que você deve especificar ao criar a configuração de auditoria. Há também três parâmetros opcionais que você pode especificar.

Tipo de informação	Opção	Obrigatório
Nome da SVM Nome do SVM no qual você pode criar a configuração de auditoria. O SVM já deve existir e estar habilitado para S3.	`-vserver` *`svm_name`*	Sim
Log Destination path Especifica onde os logs de auditoria convertidos são armazenados. O caminho já deve existir no SVM. O caminho pode ter até 864 carateres de comprimento e deve ter permissões de leitura e gravação. Se o caminho não for válido, o comando de configuração de auditoria falhará.	`-destination` *`text`*	Sim
Categorias de eventos a auditar As seguintes categorias de eventos podem ser auditadas: • Eventos GetObject, PutObject e DeleteObject de dados • Eventos PutBucket de Gestão e DeleteBucket O padrão é auditar somente eventos de dados.	`-events {data|management}, …`	Não

Pode introduzir um dos seguintes parâmetros para controlar o número de ficheiros de registo de auditoria. Se nenhum valor for inserido, todos os arquivos de log serão retidos.

Tipo de informação	Opção	Obrigatório
Limite de rotação de arquivos de log Determina quantos arquivos de log de auditoria devem ser mantidos antes de girar o arquivo de log mais antigo. Por exemplo, se você inserir um valor de 5, os últimos cinco arquivos de log serão retidos. Um valor de 0 indica que todos os arquivos de log são mantidos. O valor padrão é 0.	`-rotate-limit` *`integer`*	Não

Limite de duração dos ficheiros de registo Determina por quanto tempo um arquivo de log pode ser retido antes de ser excluído. Por exemplo, se você inserir um valor de 5d0h0m, os logs com mais de 5 dias serão excluídos. Um valor de 0 indica que todos os arquivos de log são mantidos. O valor padrão é 0.	`-retention duration` *`integer_time`*	Não

Parâmetros para rotação do log de auditoria

Você pode girar os logs de auditoria com base no tamanho ou na programação. O padrão é girar os logs de auditoria com base no tamanho.

Rode registos com base no tamanho do registo

Se você quiser usar o método de rotação de log padrão e o tamanho padrão do log, não será necessário configurar nenhum parâmetro específico para a rotação de log. O tamanho padrão do log é de 100 MB.

Se você não quiser usar o tamanho padrão do log, você pode configurar o `-rotate-size` parâmetro para especificar um tamanho de log personalizado.

Se você quiser redefinir a rotação com base em um tamanho de log sozinho, use o seguinte comando para desdefinir o `-rotate-schedule-minute` parâmetro:

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

Gire os logs com base em um agendamento

Se você optar por girar os logs de auditoria com base em um agendamento, poderá agendar a rotação de logs usando os parâmetros de rotação baseados em tempo em qualquer combinação.

- Se utilizar rotação baseada no tempo, o `-rotate-schedule-minute` parâmetro é obrigatório.
- Todos os outros parâmetros de rotação baseados no tempo são opcionais.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- O programa de rotação é calculado utilizando todos os valores relacionados com o tempo. Por exemplo, se você especificar apenas o `-rotate-schedule-minute` parâmetro, os arquivos de log de auditoria serão girados com base nos minutos especificados em todos os dias da semana, durante todas as horas em todos os meses do ano.
- Se você especificar apenas um ou dois parâmetros de rotação baseados no tempo (por exemplo, `-rotate-schedule-month` e `-rotate-schedule-minutes`), os arquivos de log serão girados com base nos valores de minuto especificados em todos os dias da semana, durante todas as horas, mas somente durante os meses especificados.

  Por exemplo, você pode especificar que o log de auditoria deve ser girado durante os meses de janeiro,

março e agosto em todas as segundas, quartas e sábados às 10:30 da manhã

- Se você especificar valores para ambos `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, eles serão considerados independentemente.

  Por exemplo, se você especificar `-rotate-schedule-dayofweek` como sexta-feira e `-rotate -schedule-day` como 13, os logs de auditoria serão girados em todas as sextas-feiras e no dia 13th do mês especificado, não apenas em todas as sextas-feiras, dia 13th.

- Se quiser redefinir a rotação com base em um agendamento sozinho, use o seguinte comando para desmarcar o `-rotate-size parameter`:

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

Rode registos com base no tamanho e na programação do registo

Você pode optar por girar os arquivos de log com base no tamanho do log e em uma programação, definindo o parâmetro -Rotate-size e os parâmetros de rotação baseados no tempo em qualquer combinação. Por exemplo: Se `-rotate-size` estiver definido para 10 MB e `-rotate-schedule-minute` estiver definido para 15, os arquivos de log rodam quando o tamanho do arquivo de log atinge 10 MB ou nos 15th minutos de cada hora (o que ocorrer primeiro).

Crie e habilite uma configuração de auditoria S3

Para implementar a auditoria do S3, primeiro você cria uma configuração de auditoria de armazenamento de objetos persistente em um SVM habilitado para S3 e, em seguida, ativa a configuração.

O que você vai precisar

- SVM habilitado para S3.
- Espaço suficiente para estadiamento de volumes no agregado.

Sobre esta tarefa

É necessária uma configuração de auditoria para cada SVM que contenha buckets do S3 que você deseja auditar. Você pode habilitar a auditoria S3 em servidores S3 novos ou existentes. As configurações de auditoria persistem em um ambiente S3 até serem removidas pelo comando **vserver object-store-server audit delete**.

A configuração de auditoria do S3 se aplica a todos os buckets do SVM que você selecionar para auditoria. Um SVM habilitado para auditoria pode conter buckets auditados e não auditados.

É recomendável configurar a auditoria S3 para rotação automática de logs, determinada pelo tamanho do log ou por um agendamento. Se você não configurar a rotação automática de log, todos os arquivos de log serão retidos por padrão. Você também pode girar arquivos de log S3 manualmente usando o comando **vserver object-store-server audit rotate-log**.

Se o SVM for uma fonte de recuperação de desastres do SVM, o caminho de destino não poderá estar no volume raiz.

Procedimento

1. Crie a configuração de auditoria para girar logs de auditoria com base no tamanho do log ou em uma programação.

Se você quiser girar logs de auditoria…	Digite…
Tamanho do registo	`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]}]`
Uma programação	`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`* O `-rotate-schedule-minute` parâmetro é necessário se você estiver configurando a rotação de log de auditoria baseada em tempo.

2. Ativar auditoria S3:

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

Exemplos

O exemplo a seguir cria uma configuração de auditoria que audita todos os eventos S3 (o padrão) usando rotação baseada em tamanho. Os logs são armazenados no diretório /audit_log. O limite de tamanho do arquivo de log é de 200 MB. Os logs são girados quando atingem 200 MB de tamanho.

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

O exemplo a seguir cria uma configuração de auditoria que audita todos os eventos S3 (o padrão) usando rotação baseada em tamanho. O limite de tamanho do arquivo de log é de 100 MB (o padrão) e os logs são mantidos por 5 dias antes de serem excluídos.

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

O exemplo a seguir cria uma configuração de auditoria que audita eventos de gerenciamento S3 e eventos de preparação de políticas de acesso central usando rotação baseada em tempo. Os logs de auditoria são girados mensalmente, às 12:30 horas em todos os dias da semana. O limite de rotação do registo é 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
```

Selecione buckets para auditoria S3

Você precisa especificar quais buckets auditar em um SVM habilitado para auditoria.

O que você vai precisar

- Um SVM foi habilitado para auditoria S3.

Sobre esta tarefa

As configurações de auditoria do S3 são habilitadas por SVM, mas você precisa selecionar os buckets no SVMS que estão habilitados para auditoria. Se você adicionar buckets ao SVM e quiser que os novos buckets sejam auditados, selecione-os com este procedimento. Também é possível ter buckets não auditados em uma SVM habilitada para auditoria S3.

As configurações de auditoria persistem para buckets até serem removidas pelo `vserver object-store-server audit event-selector delete` comando.

Procedimento

Selecione um bucket para a auditoria 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` - especifica o tipo de acesso a eventos a ser auditado: `read-only`, `write-only` ou `all` (o padrão é `all`).
- `-permission` - especifica o tipo de permissão de evento a ser auditado: `allow-only`, `deny-only` ou `all` (o padrão é `all`).

Exemplo

O exemplo a seguir cria uma configuração de auditoria de bucket que somente Registra eventos permitidos com acesso somente leitura:

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

Modificar uma configuração de auditoria S3

É possível modificar os parâmetros de auditoria de buckets individuais ou a configuração de auditoria de todos os buckets selecionados para auditoria no SVM.

Se você quiser modificar a configuração de auditoria para…	Digite…
Baldes individuais	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`

Se você quiser modificar a configuração de auditoria para…	Digite…
Todos os buckets no SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* [*`parameters to modify`*]

Exemplos

O exemplo a seguir modifica uma configuração de auditoria de bucket individual para auditar somente eventos de acesso somente gravação:

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

O exemplo a seguir modifica a configuração de auditoria de todos os buckets no SVM para alterar o limite de tamanho do log para 10MB e reter arquivos de log 3 antes de girar.

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

Mostrar configurações de auditoria do S3

Depois de concluir a configuração de auditoria, você pode verificar se a auditoria está configurada corretamente e está habilitada. Você também pode exibir informações sobre todas as configurações de auditoria de armazenamento de objetos no cluster.

Sobre esta tarefa

É possível exibir informações sobre configurações de auditoria de bucket e SVM.

- Buckets – use o `vserver object-store-server audit event-selector show` comando

  Sem parâmetros, o comando exibe as seguintes informações sobre buckets em todos os SVMs no cluster com configurações de auditoria de armazenamento de objetos:

  - Nome do SVM
  - Nome do intervalo
  - Valores de acesso e permissão
- SVMs – use o `vserver object-store-server audit show` comando

  Sem parâmetros, o comando exibe as seguintes informações sobre todos os SVMs no cluster com configurações de auditoria de armazenamento de objetos:

  - Nome do SVM
  - Estado de auditoria
  - Diretório de destino

Você pode especificar o `-fields` parâmetro para especificar quais informações de configuração de auditoria serão exibidas.

Procedimento

Mostrar informações sobre configurações de auditoria do S3:

Se pretender modificar a configuração para…	Digite…
Baldes	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVMs	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Exemplos

O exemplo a seguir exibe informações para um único 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
```

O exemplo a seguir exibe informações de todos os buckets em um SVM:

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

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

O exemplo a seguir exibe o nome, o estado de auditoria, os tipos de eventos, o formato de log e o diretório de destino para todos os SVMs.

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

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

O exemplo a seguir exibe os nomes e detalhes da SVM sobre o log de auditoria de todos os SVMs.

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

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

O exemplo a seguir exibe em forma de lista todas as informações de configuração de auditoria sobre todos os SVMs.

```
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
```

Informações sobre direitos autorais

Informações sobre marcas comerciais