审核 S3 事件

ONTAP 9

NetApp
April 24, 2024

目录

审核 S3 事件

审核 S3 事件

从 ONTAP 9.10.1 开始，您可以审核 ONTAP S3 环境中的数据和管理事件。S3 审核功能与现有 NAS 审核功能类似， S3 和 NAS 审核可以同时位于集群中。

在 SVM 上创建和启用 S3 审核配置时， S3 事件会记录在日志文件中。您可以指定要记录的以下事件：

- 对象访问（数据）事件

  GetObject ， PutObject 和 DeleteObject

- 管理事件

  PutBucket 和 DeleteBucket

日志格式为 JavaScript 对象表示法（ JSON ）。

S3 和 NFS 审核配置的组合限制为每个集群 50 个 SVM 。

需要以下许可证包：

- 核心捆绑包、适用于ONTAP S3协议和存储

有关详细信息，请参见 "ONTAP 审核过程的工作原理"。

有保障的审核

默认情况下， S3 和 NAS 审核是有保证的。ONTAP 保证记录所有可审核的存储分段访问事件，即使节点不可用也是如此。在将请求的存储分段操作的审核记录保存到永久性存储上的暂存卷之前，无法完成该操作。如果由于空间不足或其他问题而无法在暂存文件中提交审核记录，则会拒绝客户端操作。

审核的空间要求

在 ONTAP 审核系统中，审核记录最初存储在各个节点上的二进制暂存文件中。它们会定期进行整合并转换为用户可读的事件日志，这些日志存储在 SVM 的审核事件日志目录中。

暂存文件存储在专用暂存卷中，此暂存卷由 ONTAP 在创建审核配置时创建。每个聚合有一个暂存卷。

您必须在审核配置中规划足够的可用空间：

- 用于包含已审核分段的聚合中的暂存卷。
- 对于包含已转换事件日志存储目录的卷。

在创建 S3 审核配置时，您可以使用以下两种方法之一来控制事件日志的数量，从而控制卷中的可用空间：

- 一个数字限制； `-rotate-limit` 参数用于控制必须保留的最小审核文件数。

- 时间限制； `-retention-duration` 参数用于控制可保留文件的最长期限。

在这两个参数中，一旦超过配置的值，就可以删除较旧的审核文件，以便为较新的审核文件腾出空间。对于这两个参数，此值均为 0 ，表示必须保留所有文件。因此，为了确保空间充足，最佳做法是将其中一个参数设置为非零值。

由于审核有保障，如果可用于审核数据的空间在轮换限制之前用尽，则无法创建较新的审核数据，从而导致客户端无法访问数据。因此，必须仔细选择此值以及分配给审核的空间，并且您必须对审核系统中有关可用空间的警告做出响应。

有关详细信息，请参见 "基本审核概念"。

规划 S3 审核配置

您必须为 S3 审核配置指定多个参数或接受默认值。具体而言，您应考虑哪些日志轮换参数有助于确保有足够的可用空间。

请参见 *`vserver object-store-server audit create`*有关语法详细信息的手册页。

常规参数

创建审核配置时，必须指定两个必需参数。此外，您还可以指定三个可选参数。

信息类型	选项	Required
_SVM 名称 _ 要创建审核配置的 SVM 的名称。 SVM 必须已存在并已为 S3 启用。	`-verserver` *`svm_name`*	是的。
日志目标路径 _ 指定转换后的审核日志的存储位置。此路径必须已存在于 SVM 上。 路径长度最多可包含 864 个字符，并且必须具有读写权限。 如果路径无效，审核配置命令将失败。	`-destination` *`text`*	是的。
要审核的事件的类别 _ 可以审核以下事件类别： • 数据 GetObject、PutObject和DeleteObject事件 • 管理 PutBucket"和DeleteBucket"事件 默认情况下、仅审核数据事件。	`-events {data|management}, …`	否

您可以输入以下参数之一来控制审核日志文件的数量。如果未输入任何值，则会保留所有日志文件。

信息类型	选项	Required
日志文件轮换限制 _ 确定在将最旧的日志文件转出之前要保留的审核日志文件数。例如，如果输入值 5 ，则会保留最后五个日志文件。 值为 0 表示所有日志文件均已保留。默认值为0。	`-rotate-limit` *`integer`*	否
日志文件持续时间限制_ 确定日志文件在被删除之前可以保留多长时间。例如，如果输入值 5d0h0m ，超过 5 天的日志将被删除。 值为 0 表示所有日志文件均已保留。默认值为0。	`-retention duration` *`integer_time`*	否

用于审核日志轮换的参数

您可以根据大小或计划轮换审核日志。默认情况下，会根据大小轮换审核日志。

根据日志大小轮换日志

如果要使用默认日志轮换方法和默认日志大小，则无需为日志轮换配置任何特定参数。默认日志大小为 100 MB 。

如果不想使用默认日志大小、则可以配置 `-rotate-size` 用于指定自定义日志大小的参数。

如果要仅根据日志大小重置轮换、请使用以下命令取消设置 `-rotate-schedule-minute` 参数：

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

根据计划轮换日志

如果您选择根据计划轮换审核日志，则可以通过使用基于时间的轮换参数的任意组合来计划日志轮换。

- 如果使用基于时间的旋转、则 `-rotate-schedule-minute` 参数为必填项。
- 所有其他基于时间的轮换参数均为可选参数。
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- 轮换计划使用所有与时间相关的值进行计算。 例如、如果仅指定 `-rotate-schedule-minute` 参数、审核日志文件将根据一周中所有日期指定的分钟数在一年中所有月份的所有时间内进行轮换。
- 如果您仅指定一个或两个基于时间的旋转参数(例如、 `-rotate-schedule-month` 和 `-rotate -schedule-minutes`)、日志文件将根据您在一周中的所有日期指定的分钟值进行轮换、在所有时间内、

但仅在指定月份内。

例如，您可以指定在 1 月， 3 月和 8 月期间，在所有星期一，星期三和星期六的上午 10： 30 轮换审核日志

- 指定这两者的值 `-rotate-schedule-dayofweek` 和 `-rotate-schedule-day`、它们会独立考虑。

  例如、如果指定 `-rotate-schedule-dayofweek` 作为星期五和 `-rotate-schedule-day` 如果为13、则审核日志将在每个星期五和指定月份的第13天轮换、而不仅仅是在每个星期五的第13天轮换。

- 如果要仅根据计划重置轮换、请使用以下命令取消设置 `-rotate-size parameter`：

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

根据日志大小和计划轮换日志

您可以选择通过任意组合设置 -rotate-size 参数和基于时间的轮换参数来根据日志大小和计划轮换日志文件。例如：if `-rotate-size` 设置为10 MB、然后 `-rotate-schedule-minute` 设置为15时、日志文件将在日志文件大小达到10 MB时或每小时的15分钟(以先发生的事件为准)轮换。

创建并启用 S3 审核配置

要实施 S3 审核，首先要在启用了 S3 的 SVM 上创建永久性对象存储审核配置，然后启用此配置。

您需要的内容

- 启用了 S3 的 SVM 。
- 为聚合中的暂存卷提供足够的空间。

关于此任务

对于包含要审核的 S3 分段的每个 SVM ，需要进行审核配置。您可以在新的或现有的 S3 服务器上启用 S3 审核。审核配置会保留在 S3 环境中，直到被 * vserver object-store-server audit delete* 命令删除为止。

S3 审核配置适用场景您选择进行审核的 SVM 中的所有存储分段。启用了审核的 SVM 可以包含已审核和未审核的分段。

建议您根据日志大小或计划为自动日志轮换配置 S3 审核。如果不配置自动日志轮换，则默认情况下会保留所有日志文件。您还可以使用 * vserver object-store-server audit rotate-log* 命令手动轮换 S3 日志文件。

如果 SVM 是 SVM 灾难恢复源，则目标路径不能位于根卷上。

操作步骤

1. 创建审核配置以根据日志大小或计划轮换审核日志。

审核日志轮换方式	输入 ...
日志大小	`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]}]`
计划	`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`* 。`-rotate-schedule-minute` 如果要配置基于时间的审核日志轮换、则需要参数。

2. 启用 S3 审核：

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

示例

以下示例将创建一个审核配置，该配置使用基于大小的轮换来审核所有 S3 事件（默认值）。日志存储在 /audit_log 目录中。日志文件大小限制为 200 MB 。日志大小达到 200 MB 时会进行轮换。

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

以下示例将创建一个审核配置，该配置使用基于大小的轮换来审核所有 S3 事件（默认值）。日志文件大小限制为 100 MB （默认值），日志会保留 5 天，然后才会被删除。

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

以下示例将创建一个审核配置，用于审核 S3 管理事件以及使用基于时间的轮换的中央访问策略暂存事件。审核日志每月在中午 12： 30 轮换一次在一周的所有日期。日志轮换限制为 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
```

选择用于 S3 审核的存储分段

您必须指定要在启用了审核的 SVM 中审核的分段。

您需要的内容

- 为 S3 审核启用了 SVM 。

关于此任务

S3审核配置会按SVM启用、但您必须在SVM中选择已启用审核的分段。如果要将存储分段添加到 SVM 中并对新存储分段进行审核，则必须使用此操作步骤选择这些存储分段。您还可以在 SVM 中启用非审核分段以进行 S3 审核。

审核配置会一直保留到分段为止、直到被删除为止 `vserver object-store-server audit object-select delete` 命令：

操作步骤

选择用于 S3 审核的存储分段：

```
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` -指定要审核的事件访问类型： `read-only`， `write-only` 或 `all` (默认为 `all`）。
- `-permission` -指定要审核的事件权限的类型： `allow-only`， `deny-only` 或 `all` (默认为 `all`）。

示例

以下示例将创建一个存储分段审核配置，该配置仅记录允许的具有只读访问权限的事件：

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

修改 S3 审核配置

您可以修改单个存储分段的审核参数或在 SVM 中选择用于审核的所有存储分段的审核配置。

要修改的审核配置	输入 ...
单个存储分段	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
SVM 中的所有分段	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

示例

以下示例将修改单个存储分段审核配置，以便仅审核只写访问事件：

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

以下示例将修改SVM中所有分段的审核配置、将日志大小限制更改为10 MB、并在轮换前保留3个日志文件。

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

显示 S3 审核配置

完成审核配置后，您可以验证是否已正确配置并启用审核。您还可以显示有关集群中所有对象存储审核配置的信息。

关于此任务

您可以显示有关存储分段和 SVM 审核配置的信息。

- 存储分段—使用 `vserver object-store-server audit event-selector show` 命令

  如果没有任何参数，此命令将显示集群中所有 SVM 中具有对象存储审核配置的分段的以下信息：

  - SVM name
  - Bucket Name
  - 访问和权限值
- SVM—使用 `vserver object-store-server audit show` 命令

  如果没有任何参数，此命令将显示集群中具有对象存储审核配置的所有 SVM 的以下信息：

  - SVM name
  - 审核状态
  - 目标目录

您可以指定 `-fields` 用于指定要显示的审核配置信息的参数。

操作步骤

显示有关 S3 审核配置的信息：

要修改的配置	输入 ...
存储分段	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
svms	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

示例

以下示例显示了单个存储分段的信息：

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

以下示例显示了 SVM 上所有分段的信息：

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

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

以下示例显示了所有 SVM 的名称，审核状态，事件类型，日志格式和目标目录。

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

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

以下示例显示了 SVM 名称以及有关所有 SVM 的审核日志的详细信息。

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

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

以下示例以列表形式显示有关所有 SVM 的所有审核配置信息。

```
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
```