



稽核S3事件

ONTAP 9

NetApp
February 12, 2026

目錄

稽核S3事件	1
瞭解如何稽核 ONTAP S3 事件	1
物件存取（資料）事件（依版本）	1
依版本管理事件	1
保證稽核	3
稽核所需的空間	3
規劃 ONTAP S3 稽核組態	3
一般參數	3
稽核記錄輪調的參數	4
建立並啟用 ONTAP S3 稽核組態	5
選擇 ONTAP S3 稽核的儲存區	7
修改 ONTAP S3 稽核組態	8
顯示 ONTAP S3 稽核組態	8

稽核S3事件

瞭解如何稽核 ONTAP S3 事件

從功能完善的S59.10.1開始ONTAP，您可以在ONTAP 支援功能完善的支援環境中稽核資料與管理事件。S3稽核功能類似於現有的NAS稽核功能，S3和NAS稽核可共存於叢集內。

當您SVM上建立及啟用S3稽核組態時，S3事件會記錄在記錄檔中。您可以指定要記錄的下列事件：

物件存取（資料）事件（依版本）

9.11.1：

- listBucketVerions
- ListBucket（9.10.1的ListObjects已重新命名為此項目）
- ListAllMyb鏟斗（已將9.10.1的清單鏟斗重新命名為此）

9.10.1：

- 標題物件
- GetObject
- PuttObject
- 刪除物件
- 列表桶
- 清單物件
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- 刪除ObjectTagging
- PuttObjectTagging
- ListUploads
- 清單零件

依版本管理事件

9.15.1：

- GetBucketCORS
- PuttBucketCORS

- DeleteBucketCORS

9.14.1 :

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1 :

- PutBucketLifecycle
- 刪除 BucketLifecycle
- GetBucketLifecycle

9.12.1 :

- GetBucketPolicy
- CopyObject
- 上傳PartCopy
- PuttBucketPolicy
- 刪除BucketPolicy

9.11.1 :

- GetBucketVersion
- PuttBucketVersion

9.10.1 :

- 標題庫
- GetBucketAcl
- GetObjectAcl
- 推桿
- 刪除Bucket
- ModifyObjectTagging
- GetBucketLocation

記錄格式為JavaScript物件標記法（Json）。

S3和NFS稽核組態的總限制為每個叢集400個SVM。

需要下列授權：

- ONTAP One（原為核心產品組合的一部分）, 適用於ONTAP S3 傳輸協定和儲存設備

如需詳細資訊、請參閱 "[如何執行不稽核程序ONTAP](#)"。

保證稽核

根據預設、S3和NAS稽核是保證的。即使節點無法使用、也能保證記錄所有可稽核的儲存貯體存取事件。ONTAP在將該作業的稽核記錄儲存至持續儲存設備上的接移磁碟區之前、無法完成要求的儲存區作業。如果因為空間不足或其他問題而無法在暫存檔案中提交稽核記錄、則會拒絕用戶端作業。

稽核所需的空間

在不稽核系統中ONTAP、稽核記錄一開始會儲存在個別節點的二進位暫存檔案中。這些記錄會定期整合並轉換成使用者可讀取的事件記錄、這些記錄會儲存在SVM的稽核事件記錄目錄中。

暫存檔案儲存在專屬的暫存磁碟區中、ONTAP此磁碟區是由建立稽核組態時由支援所建立。每個Aggregate有一個接移磁碟區。

您必須在稽核組態中規劃足夠的可用空間：

- 適用於集合體中包含稽核桶的暫存磁碟區。
- 用於儲存已轉換事件記錄之目錄的磁碟區。

建立S3稽核組態時、您可以使用下列兩種方法之一來控制事件記錄的數量、以及磁碟區中的可用空間：

- 數值限制 `-rotate-limit` 參數控制必須保留的稽核檔案數量下限。
- 時間限制 `-retention-duration` 參數控制檔案可保留的最長期間。

在這兩個參數中、一旦超過設定、就能刪除較舊的稽核檔案、為較新的稽核檔案留出空間。這兩個參數的值都是0、表示必須維護所有檔案。因此、為了確保有足夠空間、最佳做法是將其中一個參數設定為非零值。

由於稽核保證、如果稽核資料的可用空間在旋轉限制之前用盡、就無法建立較新的稽核資料、導致用戶端無法存取資料。因此、您必須謹慎選擇此值及分配給稽核的空間、而且必須回應稽核系統中有關可用空間的警告。

如需詳細資訊、請參閱 "[基本稽核概念](#)"。

規劃 ONTAP S3 稽核組態

您必須為S3稽核組態指定多個參數、或接受預設值。特別是、您應該考慮哪些記錄旋轉參數有助於確保有足夠的可用空間。

如"[指令參考資料ONTAP](#)"需詳細`vserver object-store-server audit create`資訊，請參閱。

一般參數

建立稽核組態時、必須指定兩個必要參數。您也可以指定三個選用參數。

資訊類型	選項	必要
------	----	----

SVM名稱 要在其中建立稽核組態的SVM名稱。 SVM必須已經存在、且已啟用S3。	-vserver <i>svm_name</i>	是的
記錄目的地路徑 指定轉換後的稽核記錄儲存位置。路徑必須已存在於SVM上。 路徑長度最多可達864個字元、且必須具有讀寫權限。 如果路徑無效、稽核組態命令就會失敗。	-destination <i>text</i>	是的
要稽核的事件類別_ 您可以稽核下列事件類別： • 資料 GetObject 、 PutObject 和 DeleteObject 事件 • 管理 PutBucket 和 DeleteBucket 活動 預設為僅稽核資料事件。	-events {data management}, ...	否

您可以輸入下列其中一個參數、以控制稽核記錄檔的數量。如果未輸入任何值、則會保留所有記錄檔。

資訊類型	選項	必要
記錄檔案旋轉限制 決定要保留多少稽核記錄檔、然後再將最舊的記錄檔轉出。例如、如果您輸入值5、則會保留最後五個記錄檔。 值0表示保留所有記錄檔。預設值為 0 。	-rotate-limit <i>integer</i>	否
記錄檔案持續時間限制 決定在刪除記錄檔之前可以保留多久。例如、如果您輸入5d0h0m的值、超過5天的記錄就會刪除。 值0表示保留所有記錄檔。預設值為 0 。	-retention duration <i>integer_time</i>	否

稽核記錄輪調的參數

您可以根據大小或排程來旋轉稽核記錄。預設值是根據大小來旋轉稽核記錄。

根據記錄大小來旋轉記錄

如果您要使用預設的記錄檔旋轉方法和預設的記錄檔大小、則不需要設定任何特定的記錄檔旋轉參數。預設記錄

大小為100 MB。

如果您不想使用預設記錄大小、可以設定 `-rotate-size` 指定自訂記錄大小的參數。

如果您想要僅根據記錄大小重設旋轉、請使用下列命令取消設定 `-rotate-schedule-minute` 參數：

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

根據排程來旋轉記錄

如果您選擇根據排程來旋轉稽核記錄、您可以使用任何組合的時間型旋轉參數來排程記錄輪調。

- 如果您使用時間型旋轉、則會使用 `-rotate-schedule-minute` 參數為必填。
- 所有其他的時間型旋轉參數都是選用的。
 - `-rotate-schedule-month`
 - `-rotate-schedule-dayofweek`
 - `-rotate-schedule-day`
 - `-rotate-schedule-hour`
- 旋轉排程是使用所有與時間相關的值來計算。例如、如果您只指定 `-rotate-schedule-minute` 參數時、稽核記錄檔會根據一週中所有天所指定的分鐘數、在一年中所有月份的所有小時內進行旋轉。
- 如果只指定一或兩個時間型旋轉參數（例如、`-rotate-schedule-month` 和 `-rotate-schedule-minutes`）、「記錄檔會根據您在一週的所有天、所有時間、但僅在指定的月份內所指定的分鐘值來旋轉。

例如、您可以指定稽核日誌在一月、三月和八月的所有週一、週三和週六上午10：30進行輪調

- 如果您同時指定兩者的值 `-rotate-schedule-dayofweek` 和 `-rotate-schedule-day` 的問題。

例如、如果您指定 `-rotate-schedule-dayofweek` 星期五和 `-rotate-schedule-day` 截至 13 日、稽核記錄將會在每週五和指定月份的第 13 天、而不只是在每週五的第 13 天輪調。

- 如果您想要僅根據排程重設旋轉、請使用下列命令取消設定 `-rotate-size` parameter：

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

根據記錄大小和排程來旋轉記錄

您可以選擇根據記錄大小和排程來旋轉記錄檔、方法是在任何組合中設定 `-rotate-size` 參數和時間型旋轉參數。例如：IF `-rotate-size` 設為 10 MB、且 `-rotate-schedule-minute` 設為 15、當記錄檔大小達到 10 MB 或每小時 15 分鐘（以先發生的事件為準）時、記錄檔會旋轉。

如需有關本程序中所述命令["指令參考資料ONTAP"](#)的詳細資訊，請參閱。

建立並啟用 ONTAP S3 稽核組態

若要實作S3稽核、您必須先在啟用S3的SVM上建立持續性物件存放區稽核組態、然後啟用該組態。

開始之前

- 您有啟用 S3 的 SVM 。
- 確認您有足夠的空間在本端層中暫存磁碟區 。

關於這項工作

每個包含您要稽核之 S3 儲存區的 SVM 都需要稽核組態。您可以在新的或現有的 S3 伺服器上啟用 S3 稽核。稽核組態會保留在 S3 環境中、直到* vserver object-store-server 稽核 DELETE * 命令移除為止。

S3 稽核組態會套用至您選取進行稽核的 SVM 中的所有儲存區。啟用稽核的 SVM 可包含稽核和未稽核的儲存區。

建議您設定 S3 稽核以自動進行記錄輪調、視記錄大小或排程而定。如果您未設定自動記錄旋轉，則預設會保留所有記錄檔。您也可以使用* vserver object-store-server 稽核 rotate-log* 命令手動旋轉 S3 記錄檔。

如果 SVM 是 SVM 災難恢復來源、則目的地路徑無法位於根磁碟區上。

步驟

1. 建立稽核組態、根據記錄大小或排程來旋轉稽核記錄。

如果您想要以下列方式來旋轉稽核記錄...	輸入...
記錄檔大小	<pre>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]}]</pre>
排程	<pre>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-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [- rotate-schedule-day chron_dayofmonth] [-rotate- schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre> <p>◦ -rotate-schedule-minute 如果您正在設定時間型稽核記錄輪調、則需要參數。</p>

2. 啟用 S3 稽核：

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

範例

下列範例會建立稽核組態、使用大小型旋轉功能來稽核所有 S3 事件（預設值）。記錄儲存在/Audit 記錄目錄中。記錄檔大小上限為 200 MB。當記錄大小達到 200 MB 時、就會進行旋轉。

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

```
-size 200MB
```

下列範例會建立稽核組態、使用大小型旋轉功能來稽核所有S3事件（預設值）。記錄檔大小上限為100 MB（預設值）、而且記錄會保留5天、之後才會刪除。

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

下列範例會建立稽核組態、以稽核S3管理事件、以及使用時間型輪調的集中存取原則暫存事件。稽核記錄會每月於下午12：30循環一次一週中的所有天。記錄旋轉限制為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
```

選擇 ONTAP S3 稽核的儲存區

您必須在啟用稽核的SVM中指定要稽核的儲存區。

開始之前

- 您已啟用 SVM 進行 S3 稽核。

關於這項工作

S3 稽核組態是以每個 SVM 為基礎啟用、但您必須在 SVMS 中選取已啟用稽核的儲存區。如果您將儲存區新增至SVM、而且想要稽核新的儲存區、則必須使用此程序來選取這些儲存區。您也可以在SVM中啟用未稽核的儲存區以進行S3稽核。

在命令移除之前，貯體的稽核組態會持續保留 vserver object-store-server audit event-selector delete。

步驟

1. 選取S3稽核的儲存庫：

```
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**：指定要稽核的事件存取類型：read-only、write-only 或 all（預設為 all）。
- **-permission**：指定要稽核的事件權限類型：allow-only、deny-only 或 all（預設為 all）。

範例

下列範例會建立只記錄允許唯讀存取的事件的庫區稽核組態：

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

修改 ONTAP S3 稽核組態

您可以修改個別儲存區的稽核參數、或是在SVM中選取要稽核的所有儲存區的稽核組態。

如果您想要修改稽核組態...	輸入...
個別庫存箱	vserver object-store-server audit event-selector modify -vserver <i>svm_name</i> [-bucket <i>bucket_name</i>] [parameters to modify]
SVM中的所有儲存區	vserver object-store-server audit modify -vserver <i>svm_name</i> [parameters to modify]

範例

下列範例會修改個別的儲存區稽核組態、以僅稽核純寫入的存取事件：

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

以下範例修改 SVM 中所有貯體的稽核組態、將記錄大小限制變更為 10MB 、並在旋轉前保留 3 個記錄檔。

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

顯示 ONTAP S3 稽核組態

完成稽核組態之後、您可以確認稽核設定正確且已啟用。您也可以顯示叢集中所有物件存放區稽核組態的相關資訊。

關於這項工作

您可以顯示關於儲存區和SVM稽核組態的資訊。

- 貯體：使用 `vserver object-store-server audit event-selector show` 命令

如果沒有任何參數、命令會在叢集中的所有SVM中、以物件存放區稽核組態顯示下列關於貯體的資訊：

- SVM名稱
- 儲存區名稱
- 存取和權限值

- SVM：使用 `vserver object-store-server audit show` 命令

如果沒有任何參數、命令會顯示叢集中所有具有物件存放區稽核組態之SVM的下列資訊：

- SVM名稱

- 稽核狀態

- 目標目錄

您可以指定 `-fields` 用於指定要顯示哪些稽核組態資訊的參數。

步驟

顯示S3稽核組態的相關資訊：

如果您要修改下列項目的組態...	輸入...
桶	<code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>
SVM	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

範例

下列範例顯示單一儲存區的資訊：

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

下列範例顯示SVM上所有儲存區的資訊：

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

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

下列範例顯示所有SVM的名稱、稽核狀態、事件類型、記錄格式及目標目錄。

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

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

下列範例顯示所有SVM稽核記錄的SVM名稱和詳細資料。

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

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

下列範例會以清單形式顯示所有SVM的所有稽核組態資訊。

```
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
```

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP 「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。