



# **S3 对象存储管理**

## **ONTAP 9**

NetApp  
April 24, 2024

# 目录

- S3 对象存储管理 ..... 1
  - 了解ONTAP 9中的S3支持 ..... 1
  - 规划 ..... 4
  - 配置 ..... 8
  - 使用 S3 SnapMirror 保护存储分段 ..... 53
  - 审核 S3 事件 ..... 87

# S3 对象存储管理

## 了解ONTAP 9中的S3支持

### S3配置概述

从 ONTAP 9.8 开始，您可以在 ONTAP 集群中启用 ONTAP 简单存储服务（S3）对象存储服务器。

ONTAP 支持在为S3对象存储提供服务时采用两种内部使用情形：

- FabricPool 层到本地集群（分层到本地分段）或远程集群（云层）上的分段。
- S3 客户端应用程序访问本地集群或远程集群上的存储分段。

从ONTAP 9.14.1开始、您可以在MetroCluster IP和FC配置中的镜像或未镜像聚合中的SVM上启用S3对象存储服务器。

从ONTAP 9.12.1开始、您可以在MetroCluster IP配置中未镜像聚合中的SVM上启用S3对象存储服务器。有关MetroCluster IP配置中未镜像聚合的限制的详细信息、请参见 ["未镜像聚合的注意事项"](#)。

如果要按以下方式配置 S3 对象存储，应使用以下过程：

- 您希望从运行 ONTAP 的现有集群提供 S3 对象存储。

如果您需要在现有集群上使用 S3 功能，而无需额外的硬件和管理，则 ONTAP S3 是合适的。但是、NetApp StorageGRID软件仍然是NetApp对象存储的旗舰解决方案。有关详细信息，请参见 ["StorageGRID 文档"](#)。

- 您拥有集群管理员权限，而不是 SVM 管理员权限。

### 使用System Manager和ONTAP 命令行界面进行S3配置

您可以使用System Manager和ONTAP 命令行界面配置和管理ONTAP S3。启用S3并使用System Manager创建存储分段时、ONTAP 会选择最佳实践默认值以简化配置。如果需要指定配置参数、则可能需要使用ONTAP 命令行界面。如果您从CLI配置S3服务器和存储分段、则仍可根据需要使用System Manager对其进行管理、反之亦然。

使用 System Manager 创建 S3 存储分段时，ONTAP 会配置系统上可用性最高的默认性能服务级别。例如，在 AFF 系统上，默认设置为 \* 至尊 \*。性能服务级别是预定义的自适应服务质量（QoS）策略组。您可以指定自定义 QoS 策略组，也可以不指定策略组，而不指定默认服务级别之一。

预定义的自适应 QoS 策略组包括：

- \* 至尊 \*：用于预期延迟最低且性能最高的应用程序。
- \* 性能 \*：用于性能需求和延迟适中的应用程序。
- \* 值 \*：用于吞吐量和容量比延迟更重要的应用程序。
- \* 自定义 \*：指定自定义 QoS 策略或不指定 QoS 策略。

如果选择 \* 用于分层 \*，则不会选择任何性能服务级别，系统会尝试为分层数据选择具有最佳性能的低成本介质。

另请参见：["使用自适应 QoS 策略组"](#)。

ONTAP 会尝试在磁盘最合适的本地层上配置此存储分段，以满足所选的服务级别。但是，如果需要指定要包含在存储分段中的磁盘，请考虑通过指定本地层（聚合）从 CLI 配置 S3 对象存储。如果您通过 CLI 配置 S3 服务器，则仍可根据需要使用 System Manager 对其进行管理。

如果您希望能够指定用于存储分段的聚合，则只能使用命令行界面来执行此操作。

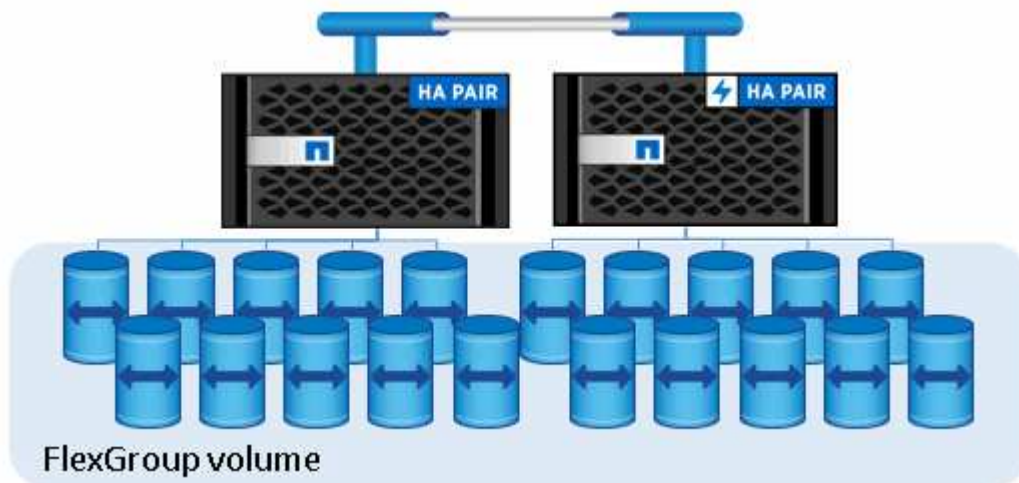
### 在 Cloud Volumes ONTAP 上配置 S3 存储分段

如果要从 Cloud Volumes ONTAP 提供存储分段、强烈建议您手动选择底层聚合、以确保它们仅使用一个节点。使用这两个节点的聚合可能会影响性能、因为这些节点将位于不同地理位置的可用性区域中、因此容易受到延迟问题的影响。因此、在 Cloud Volumes ONTAP 环境中、您应该执行此操作 [从 CLI 配置 S3 存储分段](#)。

否则、Cloud Volumes ONTAP 上的 S3 服务器在 Cloud Volumes ONTAP 中的配置和维护与在内部环境中相同。

### 架构

在 ONTAP 中，存储分段的底层架构是 FlexGroup 卷——一个命名空间，由多个成分卷组成，但作为一个卷进行管理。



存储分段仅受底层硬件的物理上限限制，架构上限可能更高。存储分段可以利用 FlexGroup 弹性大小调整功能，在 FlexGroup 卷的成分卷空间即将用尽时自动增加该成分卷的大小。每个 FlexGroup 卷的存储分段数不得超过 1000 个，或者限制为 FlexGroup 卷容量的 1/3（以考虑存储分段中的数据增长）。



不允许对包含 S3 分段的 FlexGroup 卷进行 NAS 或 SAN 协议访问。

您可以通过授权用户和客户端应用程序访问存储分段。



## 用例

客户端访问 ONTAP S3 服务的主要用例有三种：

- 对于使用 ONTAP S3 作为远程 FabricPool 容量（云）层的 ONTAP 系统  
包含容量层（对于 *c*冷\_数据）的 S3 服务器和存储分段与性能层（对于 *\_hot* 数据）位于不同的集群上。
- 对于使用 ONTAP S3 作为本地 FabricPool 层的 ONTAP 系统  
包含容量层的 S3 服务器和存储分段与性能层位于同一集群上，但位于不同的 HA 对上。
- 外部 S3 客户端应用程序

ONTAP S3 为在非 NetApp 系统上运行的 S3 客户端应用程序提供支持。

最好使用 HTTPS 访问 ONTAP S3 存储分段。启用 HTTPS 后，要与 SSL/TLS 正确集成，需要安全证书。然后，需要客户端用户`的访问权限和机密密钥才能使用 ONTAP S3 对用户进行身份验证，并为用户`授予在 ONTAP S3 中执行操作的访问权限。客户端应用程序还应有权访问根 CA 证书（ONTAP S3 服务器的签名证书），以便能够对服务器进行身份验证并在客户端和服务器之间创建安全连接。

用户在启用了 S3 的 SVM 中创建，其访问权限可以在存储分段或 SVM 级别进行控制，也就是说，可以为其授予对 SVM 中一个或多个存储分段的访问权限。

默认情况下，ONTAP S3 服务器上启用 HTTPS。可以为客户端访问禁用 HTTPS 并启用 HTTP，在这种情况下，不需要使用 CA 证书进行身份验证。但是，如果启用了 HTTP 且禁用了 HTTPS，则与 ONTAP S3 服务器的所有通信都将通过网络以明文形式发送。

对于追加信息，请参见 ["技术报告： ONTAP 最佳实践中的 S3"](#)

相关信息

## 规划

### S3 对象存储的 ONTAP 版本支持

从ONTAP 9.8开始、ONTAP 支持在内部环境中使用S3对象存储。从ONTAP 9.1.1开始、Cloud Volumes ONTAP 支持在云环境中使用S3对象存储。

#### Cloud Volumes ONTAP 支持S3

ONTAP S3在Cloud Volumes ONTAP 中的配置和功能与在内部环境中相同、但有一个例外：

- 底层聚合只能来自一个节点。了解更多信息 ["在CVO环境中创建存储分段"](#)。

云提供商	ONTAP 版本
Azure 酒店	ONTAP 9.9.1及更高版本
AWS	ONTAP 9.11.0及更高版本
Google Cloud	ONTAP 9.12.1及更高版本

#### ONTAP 9.7中的S3公有 预览

在 ONTAP 9.7 中， S3 对象存储是作为公有预览版引入的。该版本不适用于生产环境，从 ONTAP 9.8 开始将不再更新。只有 ONTAP 9.8 及更高版本支持在生产环境中使用 S3 对象存储。

使用 9.7 公有预览版创建的 S3 存储分段可在 ONTAP 9.8 及更高版本中使用，但无法利用功能增强功能。如果您使用 9.7 公有预览版创建了分段，则应将这些分段的内容迁移到 9.8 分段，以增强功能支持，安全性和性能。

### ONTAP S3 支持的操作

标准S3 REST API支持ONTAP S3操作、但如下所示除外。有关详细信息，请参见 ["Amazon S3 API参考"](#)。

#### 存储分段操作

ONTAP支持使用AWS S3 API执行以下操作：

存储分段操作	ONTAP 支持、从开始
CreateBucket	ONTAP 9.11.1
DeleteBucket	ONTAP 9.11.1
DeleteBucketPolicy	ONTAP 9.12.1
GetBucketAcl	ONTAP 9.8
GetBucketLifecycleConfiguration	ONTAP 9.13.1及更高版本 *仅支持过期操作

存储分段操作	<b>ONTAP</b> 支持、从开始
GetBucketLocation	ONTAP 9.10.1
GetBucketPolicy	ONTAP 9.12.1
HeadBucket	ONTAP 9.8
List桶	ONTAP 9.8
ListBucketVersioning	ONTAP 9.11.1
ListObjectVersies	ONTAP 9.11.1
PutBucket	<ul style="list-style-type: none"> <li>• ONTAP 9.11.1</li> <li>• ONTAP 9.8-仅支持ONTAP REST API</li> </ul>
PutBucketLifecycleConfiguration	ONTAP 9.13.1及更高版本 *仅支持过期操作
PutBucketPolicy	ONTAP 9.12.1

## 对象操作

从 ONTAP 9.1.1 开始，ONTAP S3 支持对象元数据和标记。

- PutObject和CreateMultipartUpload使用包括键值对 `x-amz-meta-<key>`。

例如： `x-amz-meta-project: ontap_s3`。

- GetObject 。和HeadObject返回用户定义的元数据。
- 与元数据不同，可以使用以下命令独立于对象读取标记：
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

从ONTAP 9.11.1开始、ONTAP S3支持使用以下ONTAP API进行对象版本控制和关联操作：

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

对象操作	<b>ONTAP</b> 支持、从开始
AbortMultipartUpload	ONTAP 9.8
CompleteMultipartUpload	ONTAP 9.8
CopyObject	ONTAP 9.12.1
CreateMultipartUpload	ONTAP 9.8
DeleteObject	ONTAP 9.8
DeleteObjects	ONTAP 9.11.1

对象操作	<b>ONTAP</b> 支持、从开始
DeleteObjectTagging	ONTAP 9.9.1
GetBucketVersioning	ONTAP 9.11.1
GetObject	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObject保留	ONTAP 9.14.1
GetObjectTagging	ONTAP 9.9.1
HeadObject	ONTAP 9.8
ListMultipartUpload	ONTAP 9.8
ListObjects	ONTAP 9.8
List对象V2	ONTAP 9.8
ListBucketVersions	ONTAP 9.11.1
ListParts	ONTAP 9.8
PutBucketVersioning	ONTAP 9.11.1
PutObject	ONTAP 9.8
PutObjectLockConfiguration	ONTAP 9.14.1
PutObject保留	ONTAP 9.14.1
PutObjectTagging	ONTAP 9.9.1
上传部件	ONTAP 9.8
上传PartCopy	ONTAP 9.12.1

## 组策略

这些操作并不特定于 S3，通常与身份和管理（IAM）流程相关。ONTAP 支持这些命令，但不使用 IAM REST API。

- 创建策略
- AttachGroup 策略

## 用户管理

这些操作并不特定于 S3，通常与 IAM 流程相关。

- CreateUser
- deleteuser
- CreateGroup
- DeleteGroup



## ONTAP S3 互操作性

ONTAP S3 服务器与其他 ONTAP 功能正常交互，但下表中所述除外。

功能区域	supported	不支持
Cloud Volumes ONTAP	<ul style="list-style-type: none"><li>• ONTAP 9.9.1 及更高版本中的 Azure 客户端</li><li>• ONTAP 9.11.0及更高版本中的AWS客户端</li><li>• ONTAP 9.12.1及更高版本中的Google Cloud Client</li></ul>	<ul style="list-style-type: none"><li>• 适用于 ONTAP 9.8 及更早版本中任何客户端的 Cloud Volumes ONTAP</li></ul>
数据保护	<ul style="list-style-type: none"><li>• Cloud Sync</li><li>• "对象版本控制" (从ONTAP 9.11.1开始)</li><li>• "S3 SnapMirror" (从ONTAP 9.10.1开始)</li><li>• MetroCluster IP配置(从ONTAP 9.12.1开始)</li><li>• SnapLock (从ONTAP 9.14.1开始)</li><li>• WORM (从ONTAP 9.14.1开始)</li></ul>	<ul style="list-style-type: none"><li>• 纠删编码</li><li>• 信息生命周期管理</li><li>• NDMP</li><li>• SMTape</li><li>• SnapMirror 云</li><li>• SVM 灾难恢复</li><li>• SyncMirror</li><li>• 用户创建的 Snapshot 副本</li></ul>
加密	<ul style="list-style-type: none"><li>• NetApp 聚合加密 ( NAE )</li><li>• NetApp 卷加密 ( NVE )</li><li>• NetApp 存储加密 ( NSE )</li><li>• TLS/SSL</li></ul>	<ul style="list-style-type: none"><li>• SLAG</li></ul>
存储效率	<ul style="list-style-type: none"><li>• 重复数据删除</li><li>• 压缩</li><li>• 数据缩减</li></ul>	<ul style="list-style-type: none"><li>• 聚合级别的效率</li><li>• 包含 ONTAP S3 分段的 FlexGroup 卷的卷克隆</li></ul>
存储虚拟化	-	NetApp FlexArray 虚拟化
服务质量 ( QoS )	<ul style="list-style-type: none"><li>• QoS 最大值 (上限)</li><li>• QoS 最小值 (下限)</li></ul>	-

功能区域	supported	不支持
其他功能	<ul style="list-style-type: none"> <li>• "审核 S3 事件" (从ONTAP 9.10.1开始)</li> </ul>	<ul style="list-style-type: none"> <li>• FlexCache 卷</li> <li>• fpolicy</li> <li>• qtree</li> <li>• 配额</li> </ul>

## ONTAP S3经验证的第三方解决方案

NetApp已验证以下第三方解决方案可用于ONTAP S3。  
如果您要查找的解决方案未列出、请联系您的NetApp客户代表。

已在**ONTAP S3**上验证第三方解决方案

NetApp已与相应的合作伙伴合作测试了这些解决方案。

- Amazon SageMaker
- Apache Hadoop S3A客户端
- Apache Kafka
- Commvault(V11)
- Confluent Kafka
- Red Hat码头
- Rubeck
- 白雪片
- Trino
- Veeam (V12)

## 配置

### 关于 **S3** 配置过程

#### **S3** 配置 workflow

配置 S3 包括评估物理存储和网络要求，然后选择特定于您的目标的工作流—配置对新的或现有 SVM 的 S3 访问，或者向已完全配置 S3 访问的现有 SVM 添加存储分段和用户。

在使用System Manager配置对新Storage VM的S3访问时、系统会提示您输入证书和网络信息、并在一次操作中创建Storage VM和S3对象存储服务器。



- "FlexGroup 卷管理"
- "NetApp 技术报告 4571-A：《NetApp ONTAP FlexGroup 卷最佳实践》"

如果您要从 Cloud Volumes ONTAP 提供存储分段、强烈建议您手动选择底层聚合、以确保它们仅使用一个节点。使用这两个节点的聚合可能会影响性能、因为这些节点将位于不同地理位置的可用性区域中、因此容易受到延迟问题的影响。了解相关信息 ["为 Cloud Volumes ONTAP 创建存储分段"](#)。

您可以使用 ONTAP S3 服务器创建本地 FabricPool 容量层，即与性能层位于同一集群中。例如，如果您将 SSD 磁盘连接到一个 HA 对，而您希望将 \_c冷\_ 数据分层到另一个 HA 对中的 HDD 磁盘，则此功能可能很有用。因此，在本使用情形中，S3 服务器和包含本地容量层的存储分段应与性能层位于不同的 HA 对中。单节点和双节点集群不支持本地分层。

## 步骤

1. 显示现有聚合中的可用空间：

```
storage aggregate show
```

如果聚合具有足够的空间或所需的节点位置、请记录其名称以用于 S3 配置。

```
cluster-1::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB    11.13GB   95% online    1 node1  raid_dp, normal
aggr_1         239.0GB    11.13GB   95% online    1 node1  raid_dp, normal
aggr_2         239.0GB    11.13GB   95% online    1 node2  raid_dp, normal
aggr_3         239.0GB    11.13GB   95% online    1 node2  raid_dp, normal
aggr_4         239.0GB   238.9GB   95% online    5 node3  raid_dp, normal
aggr_5         239.0GB   239.0GB   95% online    4 node4  raid_dp, normal
6 entries were displayed.
```

2. 如果没有具有足够空间的聚合或所需节点位置、请使用向现有聚合添加磁盘 `storage aggregate add-disks` 命令、或者使用创建新聚合 `storage aggregate create` 命令：

## 评估网络连接要求

在向客户端提供 S3 存储之前，您必须验证网络配置是否正确，以满足 S3 配置要求。

## 开始之前

必须配置以下集群网络对象：

- 物理和逻辑端口

- 广播域
- 子网（如果需要）
- IP 空间（除默认 IP 空间外，根据需要）
- 故障转移组（根据需要，除每个广播域的默认故障转移组外）
- 外部防火墙

#### 关于此任务

对于远程 FabricPool 容量（云）层和远程 S3 客户端，您必须使用数据 SVM 并配置数据 LIF。对于 FabricPool 云层，您还必须配置集群间 LIF；不需要集群对等。

对于本地 FabricPool 容量层，您必须使用系统 SVM（称为“集群”），但 LIF 配置有两个选项：

- 您可以使用集群 LIF。

在此选项中，无需进一步配置 LIF，但集群 LIF 上的流量将会增加。此外，其他集群将无法访问此本地层。

- 您可以使用数据和集群间 LIF。

此选项需要进行其他配置，包括为 S3 协议启用 LIF，但本地层也可作为远程 FabricPool 云层供其他集群访问。

#### 步骤

1. 显示可用的物理和虚拟端口：

```
network port show
```

- 如果可能，您应使用数据网络速度最快的端口。
- 数据网络中的所有组件都必须具有相同的 MTU 设置，才能获得最佳性能。

2. 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，请验证子网是否存在且具有足够的可用地址：

```
network subnet show
```

子网包含属于同一第 3 层子网的 IP 地址池。可使用创建子网 `network subnet create` 命令：

3. 显示可用 IP 空间：

```
network ipspace show
```

您可以使用默认 IP 空间或自定义 IP 空间。

4. 如果要使用 IPv6 地址，请验证是否已在集群上启用 IPv6：

```
network options ipv6 show
```

如果需要、您可以使用启用 IPv6 `network options ipv6 modify` 命令：

## 确定在何处配置新的 **S3** 存储容量

在创建新的 S3 存储分段之前，您必须确定是将其放置在新的还是现有的 SVM 中。此决定将决定您的工作流。

### 选项

- 如果要在新 SVM 或未启用 S3 的 SVM 中配置存储分段，请完成以下主题中的步骤。

["为 S3 创建 SVM"](#)

["为S3创建存储分段"](#)

虽然 S3 可以与 NFS 和 SMB 共存于 SVM 中，但如果满足以下条件之一，您可以选择创建新的 SVM：

- 首次在集群上启用 S3。
  - 集群中的现有 SVM 不希望启用 S3 支持。
  - 一个集群中有一个或多个启用了 S3 的 SVM，您希望使用另一个具有不同性能特征的 S3 服务器。  
在 SVM 上启用 S3 后，继续配置存储分段。
- 如果要在已启用 S3 的现有 SVM 上配置初始存储分段或其他存储分段，请完成以下主题中的步骤。

["为S3创建存储分段"](#)

## 配置对 **SVM** 的 **S3** 访问

### 为 **S3** 创建 **SVM**

虽然S3可以与SVM中的其他协议共存、但您可能需要创建一个新的SVM来隔离命名空间和工作负载。

#### 关于此任务

如果您仅从SVM提供S3对象存储、则S3服务器不需要任何DNS配置。但是，如果使用其他协议，则可能需要在 SVM 上配置 DNS。

在使用System Manager配置对新Storage VM的S3访问时、系统会提示您输入证书和网络信息、并在一次操作中创建Storage VM和S3对象存储服务器。

## 示例 1. 步骤

### System Manager

您应准备好将S3服务器名称输入为完全限定域名(FQDN)、客户端将使用该域名进行S3访问。S3服务器FQDN不能以分段名称开头。


您应准备为接口角色数据输入IP地址。

如果您使用的是外部 CA 签名证书，则在此操作步骤期间，系统将提示您输入此证书；您也可以选择使用系统生成的证书。

#### 1. 在 Storage VM 上启用 S3 。

- a. 添加新的Storage VM：单击\*存储> Storage VM\*、然后单击\*添加\*。

如果这是一个没有现有Storage VM的新系统：单击\*信息板>配置协议\*。

如果要将S3服务器添加到现有Storage VM：单击\*存储> Storage VM\*、选择一个Storage VM、单击\*设置\*、然后单击  在 \* S3 下。

- a. 单击 \* 启用 S3\* ，然后输入 S3 服务器名称。
- b. 选择证书类型。

无论选择系统生成的证书还是您自己的证书之一，客户端访问都需要此证书。

- c. 输入网络接口。

#### 2. 如果选择了系统生成的证书，则在确认创建新 Storage VM 后，您将看到证书信息。单击 \* 下载 \* 并保存以供客户端访问。

- 不会再显示此机密密钥。
- 如果您再次需要证书信息：单击\*存储>存储VM\*、选择Storage VM、然后单击\*设置\*。

### 命令行界面

#### 1. 验证 S3 是否已在集群上获得许可：

```
system license show -package s3
```

如果不是，请联系您的销售代表。

#### 2. 创建 SVM ：

```
vserver create -vserver <svm_name> -subtype default -rootvolume  
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security  
-style unix -language C.UTF-8 -data-services <data-s3-server>  
-ipSPACE <ipSPACE_name>
```

- 对使用UNIX设置 -rootvolume-security-style 选项

- 使用默认C.UTF-8 -language 选项

- ipspace 设置是可选的。

### 3. 验证新创建的 SVM 的配置和状态：

```
vserver show -vserver <svm_name>
```

◦ Vserver Operational State 字段必须显示 running 状态。如果显示 initializing 状态、表示某些中间操作(如创建根卷)失败、您必须删除SVM并重新创建它。

#### 示例

以下命令将在 IP 空间 ipspaceA 中创建用于数据访问的 SVM：

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

以下命令显示已创建根卷为1 GB的SVM、并且此SVM已自动启动并位于中 running 状态。根卷具有一个默认导出策略，该策略不包含任何规则，因此根卷在创建时不会导出。默认情况下、vsadmin用户帐户会创建在中 locked 状态。vsadmin 角色将分配给默认 vsadmin 用户帐户。



```

cluster-1::> vserver show -vserver svm1.example.com
                                Vserver: svm1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: unix
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
                                Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA

```

在 **SVM** 上创建并安装 **CA** 证书

要启用从 S3 客户端到启用了 S3 的 SVM 的 HTTPS 流量，需要证书颁发机构（CA）证书。

关于此任务

虽然可以将 S3 服务器配置为仅使用 HTTP，并且可以在不要求 CA 证书的情况下配置客户端，但最佳做法是使用 CA 证书保护发送到 ONTAP S3 服务器的 HTTPS 流量。

在本地分层使用情形中，IP 流量仅通过集群 LIF 时，不需要 CA 证书。

此操作步骤中的说明将创建并安装 ONTAP 自签名证书。此外，还支持来自第三方供应商的 CA 证书；有关详细信息，请参见管理员身份验证文档。

["管理员身份验证和 RBAC"](#)

请参见 `security certificate` 其他配置选项的手册页。

步骤

## 1. 创建自签名数字证书：

```
security certificate create -vserver svm_name -type root-ca -common-name ca_cert_name
```

。 -type root-ca 选项用于创建并安装自签名数字证书、以便通过充当证书颁发机构(CA)对其他证书进行签名。

。 -common-name 选项将创建SVM的证书颁发机构(Certificate Authority、CA)名称、并在生成证书的完整名称时使用。

默认证书大小为 2048 位。

示例

```
cluster-1::> security certificate create -vserver svm1.example.com -type root-ca -common-name svm1_ca
```

```
The certificate's generated name for reference:  
svm1_ca_159D1587CE21E9D4_svm1_ca
```

显示证书的生成名称时，请务必保存此证书，以供此操作步骤中稍后的步骤使用。

## 2. 生成证书签名请求：

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

。 -common-name 签名请求的参数必须是S3服务器名称(FQDN)。

如果需要，您可以提供 SVM 的位置和其他详细信息。

系统会提示您保留证书请求和私钥的副本，以供日后参考。

## 3. 使用 SVM\_CA 对 CSR 签名以生成 S3 服务器的证书：

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial ca_cert_serial_number [additional_options]
```

输入您在先前步骤中使用的命令选项：

。 -ca --您在步骤1中输入的CA的公用名。

。 -ca-serial --步骤1中的CA序列号。例如，如果 CA 证书名称为 svm1\_ca\_159D1587CE21E9D4\_svm1\_ca ，则序列号为 159D1587CE21E9d4 。

默认情况下，签名证书将在 365 天后过期。您可以选择其他值并指定其他签名详细信息。

出现提示时，复制并输入您在步骤 2 中保存的证书请求字符串。

此时将显示一个签名证书；请保存此证书以供日后使用。

#### 4. 在启用了 S3 的 SVM 上安装签名证书:

```
security certificate install -type server -vserver svm_name
```

出现提示时, 输入证书和专用密钥。

如果需要证书链, 您可以选择输入中间证书。

显示私钥和 CA 签名的数字证书时, 请保存它们以供将来参考。

#### 5. 获取公有密钥证书:

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

保存公有密钥证书以供稍后的客户端配置使用。

示例

```
cluster-1::> security certificate show -vserver svm1.example.com -common  
-name svm1_ca -type root-ca -instance  
  
Name of Vserver: svm1.example.com  
FQDN or Custom Common Name: svm1_ca  
Serial Number of Certificate: 159D1587CE21E9D4  
Certificate Authority: svm1_ca  
Type of Certificate: root-ca  
(DEPRECATED)-Certificate Subtype: -  
Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca  
Size of Requested Certificate in Bits: 2048  
Certificate Start Date: Thu May 09 10:58:39 2020  
Certificate Expiration Date: Fri May 08 10:58:39 2021  
Public Key Certificate: -----BEGIN CERTIFICATE-----  
MIIDZ ...==  
-----END CERTIFICATE-----  
  
Country Name: US  
State or Province Name:  
Locality Name:  
Organization Name:  
Organization Unit:  
Contact Administrator's Email Address:  
Protocol: SSL  
Hashing Function: SHA256  
Self-Signed Certificate: true  
Is System Internal Certificate: false
```

## 创建 S3 服务数据策略

您可以为 S3 数据和管理服务创建服务策略。要在 LIF 上启用 S3 数据流量，需要使用 S3 服务数据策略。

### 关于此任务

如果使用的是数据 LIF 和集群间 LIF，则需要使用 S3 服务数据策略。如果在本地分层使用情形中使用集群 LIF，则不需要此功能。

为 LIF 指定服务策略时，将使用该策略为 LIF 构建默认角色，故障转移策略和数据协议列表。

虽然可以为 SVM 和 LIF 配置多个协议，但最好将 S3 作为提供对象数据的唯一协议。

### 步骤

1. 将权限设置更改为高级：

```
set -privilege advanced
```

2. 创建服务数据策略：

```
network interface service-policy create -vserver svm_name -policy policy_name  
-services data-core,data-s3-server
```

。data-core 和 data-s3-server 服务是启用 ONTAP S3 所需的唯一服务、但也可以根据需要包括其他服务。

### 创建数据 LIF：

如果创建了新的 SVM，则为 S3 访问创建的专用 LIF 应为数据 LIF。

### 开始之前

- 底层物理或逻辑网络端口必须已配置为管理端口 up 状态。
- 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，则此子网必须已存在。

子网包含属于同一第 3 层子网的 IP 地址池。它们是使用创建的 `network subnet create` 命令：

- LIF 服务策略必须已存在。

### 关于此任务

- 您可以在同一网络端口上创建 IPv4 和 IPv6 LIF。
- 如果集群中有大量 LIF、则可以使用验证集群上支持的 LIF 容量 `network interface capacity show` 命令以及每个节点上支持的 LIF 容量 `network interface capacity details show` 命令(在高级权限级别)。
- 如果要启用远程 FabricPool 容量（云）分层，则还必须配置集群间 LIF。

### 步骤

1. 创建 LIF：


```
network interface create -vserver svm_name -lif lif_name -service-policy
service_policy_names -home-node node_name -home-port port_name {-address
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
data -auto-revert {true|false}
```

◦ -home-node 是LIF返回到的节点 network interface revert 命令将在LIF上运行。

您还可以使用指定LIF是否应自动还原到主节点和主端口 -auto-revert 选项

- -home-port 是LIF返回到的物理或逻辑端口 network interface revert 命令将在LIF上运行。
- 您可以使用指定IP地址 -address 和 -netmask 选项、或者使用启用从子网分配 -subnet\_name 选项
- 使用子网提供 IP 地址和网络掩码时，如果使用网关定义了子网，则在使用该子网创建 LIF 时，系统会自动向 SVM 添加指向该网关的默认路由。
- 如果您手动分配 IP 地址（而不使用子网），则在其他 IP 子网上存在客户端或域控制器时，可能需要配置指向网关的默认路由。。 network route create 手册页包含有关在SVM中创建静态路由的信息。
- -firewall-policy 选项中、使用相同的默认值 data 作为LIF角色。

如果需要，您可以稍后创建和添加自定义防火墙策略。



从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 ["为 LIF 配置防火墙策略"](#)。

- -auto-revert 用于指定在启动、更改管理数据库状态或建立网络连接等情况下、数据LIF是否自动还原到其主节点。默认设置为 false，但您可以将其设置为 true 具体取决于您环境中的网络管理策略。
- -service-policy 选项用于指定您创建的数据和管理服务策略以及所需的任何其他策略。

2. 如果要在中分配IPv6地址 -address 选项：

a. 使用 network ndp prefix show 命令以查看在各种接口上获取的RA前缀列表。

- network ndp prefix show 命令可在高级权限级别下使用。

b. 使用格式 prefix:id 手动构建IPv6地址。

prefix 是在各种接口上获取的前缀。

用于派生 `id` 下，选择一个随机的64位十六进制数。

3. 使用验证是否已成功创建LIF network interface show 命令：

4. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	network ping
IPv6地址	network ping6

示例

以下命令显示如何创建分配给S3数据LIF my-S3-policy 服务策略：

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

以下命令显示 cluster-1 中的所有 LIF 。数据 LIF datalif1 和 datalif3 配置了 IPv4 地址，而 datalif4 配置了 IPv6 地址：

```
cluster-1::> network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
cluster-1	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
true	clus1	up/up	192.0.2.12/24	node-1	e0a
true	clus2	up/up	192.0.2.13/24	node-1	e0b
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a
true	clus1	up/up	192.0.2.14/24	node-2	e0a
true	clus2	up/up	192.0.2.15/24	node-2	e0b
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com	datalif3	up/up	192.0.2.146/30	node-2	e0c
true	datalif4	up/up	2001::2/64	node-2	e0c

5 entries were displayed.

为远程 **FabricPool** 分层创建集群间 LIF

如果要使用 ONTAP S3 启用远程 FabricPool 容量（云）分层，则必须配置集群间 LIF。您可以在与数据网络共享的端口上配置集群间 LIF。这样可以减少集群间网络连接所需的端口数量。

开始之前

- 底层物理或逻辑网络端口必须已配置为管理端口 up 状态。
- LIF 服务策略必须已存在。

关于此任务

本地 Fabric Pool 分层或提供外部 S3 应用程序不需要集群间 LIF。

步骤

1. 列出集群中的端口：

```
network port show
```

以下示例显示了中的网络端口 cluster01：

```
cluster01::> network port show
```

(Mbps)						Speed	
Node	Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
-----							
cluster01-01							
	e0a	Cluster	Cluster		up	1500	auto/1000
	e0b	Cluster	Cluster		up	1500	auto/1000
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000
cluster01-02							
	e0a	Cluster	Cluster		up	1500	auto/1000
	e0b	Cluster	Cluster		up	1500	auto/1000
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000

2. 在系统 SVM 上创建集群间 LIF：

```
network interface create -vserver Cluster -lif LIF_name -service-policy
default-intercluster -home-node node -home-port port -address port_IP -netmask
netmask
```

以下示例将创建集群间生命周期 cluster01\_icl01 和 cluster01\_icl02：

```

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

### 3. 验证是否已创建集群间 LIF :

```
network interface show -service-policy default-intercluster
```

```

cluster01::> network interface show -service-policy default-intercluster

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0c
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0c
true				

### 4. 验证集群间 LIF 是否冗余:

```
network interface show -service-policy default-intercluster -failover
```

以下示例显示了集群间的生命周期 cluster01\_icl01 和 cluster01\_icl02 在上 e0c 端口将故障转移到 e0d 端口。



```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01	cluster01_icl01	cluster01-01:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-01:e0c, cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
192.168.1.201/24			Failover Targets: cluster01-02:e0c, cluster01-02:e0d	

### 创建 S3 对象存储服务器

ONTAP 对象存储服务器将数据作为 S3 对象进行管理，而不是由 ONTAP NAS 和 SAN 服务器提供的文件或块存储。

#### 开始之前

您应准备好将 S3 服务器名称输入为完全限定域名 (FQDN)、客户端将使用该域名进行 S3 访问。FQDN 不能以分段名称开头。

您应具有自签名 CA 证书（在先前步骤中创建）或由外部 CA 供应商签名的证书。在本地分层使用情形中，IP 流量仅通过集群 LIF 时，不需要 CA 证书。

#### 关于此任务

创建对象存储服务器时，将创建 UID 为 0 的 root 用户。不会为此 root 用户生成访问密钥或机密密钥。ONTAP 管理员必须运行 `object-store-server users regenerate-keys` 命令以设置此用户的访问密钥和机密密钥。



作为 NetApp 最佳实践，请勿使用此 root 用户。使用 root 用户的访问密钥或机密密钥的任何客户端应用程序都可以完全访问对象存储中的所有分段和对象。


请参见 `vserver object-store-server` 有关其他配置和显示选项的手册页。

## System Manager

如果要将S3服务器添加到现有Storage VM、请使用此操作步骤。要将S3服务器添加到新的Storage VM、请参见 ["为S3创建存储SVM"](#)。

您应准备为接口角色数据输入IP地址。

### 1. 在现有Storage VM上启用S3。

- 选择Storage VM：单击\*存储> Storage VM\*、选择一个Storage VM、单击\*设置\*、然后单击  在 \* S3 下。
- 单击 \* 启用 S3\* ，然后输入 S3 服务器名称。
- 选择证书类型。

无论选择系统生成的证书还是您自己的证书之一，客户端访问都需要此证书。

### d. 输入网络接口。

### 2. 如果选择了系统生成的证书，则在确认创建新 Storage VM 后，您将看到证书信息。单击 \* 下载 \* 并保存以供客户端访问。

- 不会再显示此机密密钥。
- 如果您再次需要证书信息：单击 \* 存储 > 存储 VM\* ，选择 Storage VM ，然后单击 \* 设置 \* 。

## 命令行界面

### 1. 创建 S3 服务器：

```
vserver object-store-server create -vserver svm_name -object-store-server  
s3_server_fqdn -certificate-name server_certificate_name -comment text  
[additional_options]
```

您可以在创建 S3 服务器时或以后任何时间指定其他选项。

- 如果要配置本地分层、则SVM名称可以是数据SVM或系统SVM (集群)名称。
- 证书名称应是服务器证书的名称(最终用户证书或叶证书)、而不是服务器CA证书(中间CA证书或根CA证书)。
- 默认情况下，HTTPS 在端口 443 上处于启用状态。您可以使用更改端口号 `-secure-listener -port` 选项

启用HTTPS后、要与SSL/TLS正确集成、需要CA证书。

- 默认情况下、HTTP处于禁用状态。启用后、服务器将侦听端口80。您可以使用启用它 `-is-http -enabled` 选项、或者使用更改端口号 `-listener-port` 选项

启用HTTP后、请求和响应将以明文形式通过网络发送。

### 2. 验证是否已配置S3：

```
vserver object-store-server show
```

## 示例

此命令将验证所有对象存储服务器的配置值：

```
cluster1::> vsriver object-store-server show

Vserver: vs1

Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

## 向启用了 S3 的 SVM 添加存储容量

### 创建存储分段

S3对象保留在\_bep桶\_中。它们不会作为文件嵌套在其他目录的目录中。

### 开始之前

包含S3服务器的Storage VM必须已存在。

### 关于此任务

- 从ONTAP 9.14.1开始、在S3 FlexGroup卷上创建存储分段时、已启用自动调整大小功能。这样可以避免在现有和新FlexGroup卷上创建存储分段期间分配过多的容量。根据以下准则、FlexGroup卷的大小将调整为所需的最小大小。所需的最小大小为FlexGroup卷中所有S3分段的总大小。
  - 从ONTAP 9.14.1开始、如果在创建新存储分段时创建了S3 FlexGroup卷、则会使用所需的最小大小创建FlexGroup卷。
  - 如果S3 FlexGroup卷是在ONTAP 9.14.1之前创建的、则在ONTAP 9.14.1之后创建或删除的第一个分段会将FlexGroup卷大小调整为所需的最小大小。
  - 如果S3 FlexGroup卷是在ONTAP 9.14.1之前创建的、并且已达到所需的最小大小、则在ONTAP 9.14.1之后创建或删除存储分段时、S3 FlexGroup卷的大小将保持不变。
- 存储服务级别是预定义的自适应服务质量（QoS）策略组，具有 *value*，*performage* 和 *\_Extreme* 默认级别。您还可以定义自定义 QoS 策略组并将其应用于存储分段，而不是默认存储服务级别之一。有关存储服务定义的详细信息、请参见 ["存储服务定义"](#)。有关性能管理的详细信息、请参见 ["性能管理"](#)。  
从 ONTAP 9.8 开始，在配置存储时，默认情况下会启用 QoS。您可以在配置过程中或稍后时间禁用 QoS 或选择自定义 QoS 策略。
- 如果要配置本地容量分层、则需要在数据Storage VM中创建存储分段和用户、而不是在S3服务器所在的系统Storage VM中创建存储分段和用户。
- 要进行远程客户端访问，您必须在启用了 S3 的 Storage VM 中配置存储分段。如果在未启用 S3 的 Storage VM 中创建存储分段，则此分段仅可用于本地分层。

- 从ONTAP 9.14.1开始、您可以执行此操作 ["在MetroCluster配置中的镜像或未镜像聚合上创建分段"](#)。
- 对于CLI、在创建存储分段时、您有两个配置选项：
  - Let ONTAP Select the underlying aggregates and FlexGroup components （默认）
    - ONTAP 会通过自动选择聚合来为第一个存储分段创建和配置 FlexGroup 卷。它将自动选择可用于您的平台的最高服务级别，或者您也可以指定存储服务级别。稍后在Storage VM中添加的任何其他分段都将具有相同的底层FlexGroup卷。
    - 或者，您也可以指定存储分层是否会使用存储分段，在这种情况下， ONTAP 会尝试选择低成本介质，以便为分层数据提供最佳性能。
  - 您可以选择底层聚合和FlexGroup组件(需要高级权限命令选项)：您可以选择手动选择必须创建存储分段和所属FlexGroup卷的聚合、然后指定每个聚合上的成分卷数。添加其他分段时：
    - 如果为新存储分段指定聚合和成分卷，则会为新存储分段创建新的 FlexGroup 。
    - 如果不为新存储分段指定聚合和成分卷，则新存储分段将添加到现有 FlexGroup 中。  
请参见 [FlexGroup 卷管理](#) 有关详细信息 ...

在创建存储分段时指定聚合和成分卷时，不会应用任何 QoS 策略组，默认或自定义。您可以稍后使用执行此操作 `vserver object-store-server bucket modify` 命令：

请参见 ["vserver object-store-server bucket modify"](#) 有关详细信息 ...

\*注意：\*如果您正在从Cloud Volumes ONTAP 提供存储分段、则应使用命令行界面操作步骤。强烈建议您手动选择底层聚合、以确保它们仅使用一个节点。使用这两个节点的聚合可能会影响性能、因为这些节点将位于不同地理位置的可用性区域中、因此容易受到延迟问题的影响。

#### 使用ONTAP命令行界面创建S3存储分段

1. 如果您计划自己选择聚合和FlexGroup组件、请将权限级别设置为高级(否则、管理权限级别就足够了)：  
`set -privilege advanced`

2. 创建存储分段：

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

Storage VM名称可以是数据Storage VM或 Cluster (系统Storage VM名称)。

如果未指定任何选项、ONTAP将创建一个800 GB的分段、并将服务级别设置为系统可用的最高级别。

如果您希望 ONTAP 根据性能或使用情况创建存储分段，请使用以下选项之一：

- 服务级别

包括 `-storage-service-level` 具有以下值之一的选项： `value`， `performance` 或 `extreme`。

- 分层

包括 `-used-as-capacity-tier true` 选项

如果要指定用于创建底层 FlexGroup 卷的聚合，请使用以下选项：

- °。 -aggr-list 参数用于指定要用于 FlexGroup 卷成分卷的聚合列表。

列表中的每个条目都会在指定聚合上创建一个成分卷。您可以多次指定一个聚合，以便在该聚合上创建多个成分卷。

为了在整个 FlexGroup 卷中保持性能一致，所有聚合都必须使用相同的磁盘类型和 RAID 组配置。

- °。 -aggr-list-multiplier 参数用于指定迭代随一起列出的聚合的次数 -aggr-list 参数 FlexGroup。

的默认值 -aggr-list-multiplier 参数为4。

### 3. 根据需要添加 QoS 策略组：

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy  
-group qos_policy_group
```

### 4. 验证存储分段创建：

```
vserver object-store-server bucket show [-instance]
```

## 示例

以下示例将为 Storage VM 创建存储分段 vs1 大小 1TB 并指定聚合：

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svml.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

## 使用 System Manager 创建 S3 存储分段

### 1. 在启用了 S3 的 Storage VM 上添加新存储分段。

- 单击 \* 存储 > 分段 \*，然后单击 \* 添加 \*。
- 输入名称，选择 Storage VM 并输入大小。
  - 如果此时单击 \* 保存 \*，则会使用以下默认设置创建一个存储分段：
    - 除非任何组策略已生效，否则不会向任何用户授予对存储分段的访问权限。



您不应使用 S3 root 用户管理 ONTAP 对象存储并共享其权限，因为它对对象存储具有无限制的访问权限。而是使用您分配的管理权限创建一个用户或组。

- 系统可用性最高的服务质量（性能）级别。
- 单击 \*Save\* 以使用这些默认值创建分段。

## 配置其他权限和限制

您可以在配置存储分段时单击 \*More Options (更多选项)\* 来配置对象锁定、用户权限和性能级别设置，也可以稍后修改这些设置。

如果要使用 S3 对象存储进行 FabricPool 分层，请考虑选择 \* 用于分层 \*（使用低成本介质，为分层数据提供最佳性能），而不是性能服务级别。

如果要为对象启用版本控制以便稍后恢复，请选择\*Enable Versioning\*。如果要在存储分段上启用对象锁定、则默认情况下会启用版本控制。有关对象版本控制的信息、请参见 ["在适用于Amazon的S3存储分段中使用版本控制"](#)。

从9.14.1开始、S3存储分段支持对象锁定。S3对象锁定需要标准SnapLock许可证。此许可证包含在中 ["ONTAP One"](#)。

在ONTAP One之前、SnapLock许可证包含在"安全性和合规性"包中。安全与合规性包不再提供、但仍然有效。虽然目前不需要、但现有客户可以选择这样做 ["升级到ONTAP One"](#)。

如果要在存储分段上启用对象锁定、则应执行此操作 ["验证是否已安装SnapLock许可证"](#)。如果未安装SnapLock许可证、则必须执行此操作 ["安装"](#) 启用对象锁定之前。

确认已安装SnapLock许可证后，要防止存储分段中的对象被删除或覆盖，请选择\*Enable object locking\*。锁定可以在所有或特定版本的对象上启用、并且只能在为集群节点初始化SnapLock Compliance时钟时才启用。请按照以下步骤操作：

1. 如果未在集群的任何节点上初始化SnapLock Compliance时钟，则会显示\*初始化SnapLock Compliance Clock\*按钮。单击\*初始化SnapLock Compliance Clock\*以初始化集群节点上的SnapLock Compliance时钟。
2. 选择\*监管\*模式可激活基于时间的锁定，该锁定允许对对象具有\_Write Once, Read Many(WORM)\_权限。即使在\_监管\_模式下、具有特定权限的管理员用户也可以删除这些对象。
3. 如果要对对象指定更严格的删除和更新规则，请选择\*Compliance模式。在此对象锁定模式下、对象只能在指定保留期限结束后过期。除非指定保留期限、否则对象将无限期保持锁定状态。
4. 如果希望锁定在特定时间段内有效、请指定锁定的保留期限(以天或年为单位)。



锁定适用于分版本和非分版本S3分段。对象锁定不适用于NAS对象。

您可以为存储分段配置保护和权限设置以及性能服务级别。



在配置权限之前、您必须已创建用户和组。

有关信息，请参见 ["为新存储分段创建镜像"](#)。

## 验证对存储分段的访问

在S3客户端应用程序(无论是ONTAP S3还是外部第三方应用程序)上、您可以输入以下命令来验证您对新创建存储分段的访问权限：

- S3 服务器 CA 证书。
- 用户的访问密钥和机密密钥。
- S3 服务器 FQDN 名称和存储分段名称。

在**MetroCluster**配置中的镜像或未镜像聚合上创建分段

从ONTAP 9.14.1开始、您可以在MetroCluster FC和IP配置中的镜像或未镜像聚合上配置分段。

## 关于此任务

- 默认情况下、存储分段配置在镜像聚合上。
- 与中所述的配置准则相同 ["创建存储分段"](#) 适用于在MetroCluster环境中创建存储分段。
- MetroCluster环境\*不\*支持以下S3对象存储功能：
  - S3 SnapMirror
  - S3存储分段生命周期管理
  - \*兼容\*模式下的S3对象锁定



支持\*监管\*模式下的S3对象锁定。

- 本地FabricPool层

## 开始之前

包含 S3 服务器的 SVM 必须已存在。

## 创建存储分段的过程

## 命令行界面

1. 如果您计划自己选择聚合和FlexGroup组件、请将权限级别设置为高级(否则、管理权限级别就足够了)  
: set -privilege advanced

2. 创建存储分段:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket  
<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates  
true/false]
```

设置 `-use-mirrored-aggregates` 选项 `true` 或 `false` 具体取决于您要使用镜像聚合还是未镜像聚合。



默认情况下、`-use-mirrored-aggregates` 选项设置为 `true`。

- SVM名称必须是数据SVM。
- 如果未指定任何选项、ONTAP将创建一个800 GB的分段、并将服务级别设置为系统可用的最高级别。
- 如果您希望 ONTAP 根据性能或使用情况创建存储分段, 请使用以下选项之一:

- 服务级别

包括 `-storage-service-level` 具有以下值之一的选项: `value`, `performance`` 或 ``extreme`。

- 分层

包括 `-used-as-capacity-tier true` 选项

- 如果要指定用于创建底层 FlexGroup 卷的聚合, 请使用以下选项:

- ◦ `-aggr-list` 参数用于指定要用于FlexGroup卷成分卷的聚合列表。

列表中的每个条目都会在指定聚合上创建一个成分卷。您可以多次指定一个聚合, 以便在该聚合上创建多个成分卷。

为了在整个 FlexGroup 卷中保持性能一致, 所有聚合都必须使用相同的磁盘类型和 RAID 组配置。

- ◦ `-aggr-list-multiplier` 参数用于指定迭代随一起列出的聚合的次数 `-aggr-list` 参数FlexGroup。

的默认值 `-aggr-list-multiplier` 参数为4。

3. 根据需要添加 QoS 策略组:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy  
-group qos_policy_group
```

4. 验证存储分段创建:

```
vserver object-store-server bucket show [-instance]
```



## 示例

以下示例将在镜像聚合上为SVM VS1创建大小为1 TB的分段：

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -size 1TB -use-mirrored-aggregates  
true
```

## System Manager

1. 在启用了 S3 的 Storage VM 上添加新存储分段。

- a. 单击 \* 存储 > 分段 \*，然后单击 \* 添加 \*。
- b. 输入名称，选择 Storage VM 并输入大小。

默认情况下、存储分段配置在镜像聚合上。如果要在未镜像聚合上创建存储分段，请选择\*更多选项\*，然后取消选中\*保护\*下的\*使用SyncMirror层\*复选框，如下图所示：

Add bucket

NAME

To use this bucket from a remote cluster, configure S3 service on storage VM "vs1".

FOLDER (OPTIONAL)

Browse

Specify the folder to map to this bucket.
[Know more](#)

CAPACITY

Size

GB

☐ Use tiering

If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.

☐ Enable versioning

Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Value

Not sure?
[Get help selecting type](#)

Permissions

☐ Copy access permissions from an existing bucket

Principal	Effect	Actions	Resources	Conditions
All users of this stor...	allow	ListBucket	*	

+ Add

Object locking

☐ Enable object locking

Object locking utilizes the "Write Once, Read Many" (WORM) model in which objects or their versions are protected from being deleted or overwritten during the specified retention period.

Protection

☒ Use the SynchS3 protection

Save

Cancel

- 如果此时单击 \* 保存 \*，则会使用以下默认设置创建一个存储分段：
  - 除非任何组策略已生效，否则不会向任何用户授予对存储分段的访问权限。



您不应使用 S3 root 用户管理 ONTAP 对象存储并共享其权限，因为它对对象存储具有无限制的访问权限。而是使用您分配的管理权限创建一个用户或组。

- 系统可用性最高的服务质量（性能）级别。
- 您可以在配置存储分段时单击 \* 更多选项 \* 来配置用户权限和性能级别，也可以稍后修改这些设置。
  - 在使用 \* 更多选项 \* 配置用户和组权限之前，您必须已创建用户和组。
  - 如果要使用 S3 对象存储进行 FabricPool 分层，请考虑选择 \* 用于分层 \*（使用低成本介

质，为分层数据提供最佳性能），而不是性能服务级别。

2. 在 S3 客户端应用程序（另一个 ONTAP 系统或外部第三方应用程序）上，输入以下命令验证对新存储分段的访问：
  - S3 服务器 CA 证书。
  - 用户的访问密钥和机密密钥。
  - S3 服务器 FQDN 名称和存储分段名称。

## 创建存储分段生命周期管理规则

从ONTAP 9.13.1开始、您可以创建生命周期管理规则来管理S3存储分段中的对象生命周期。您可以为存储分段中的特定对象定义删除规则、并通过这些规则使这些存储分段对象失效。这样、您就可以满足保留要求并高效管理整体S3对象存储。



如果为存储分段对象启用了对象锁定、则不会对锁定的对象应用对象到期的生命周期管理规则。有关对象锁定的信息、请参见 ["创建存储分段"](#)。

### 开始之前

包含 S3 服务器和存储分段且已启用 S3 的 SVM 必须已存在。请参见 ["为 S3 创建 SVM"](#) 有关详细信息 ...

### 关于此任务

创建生命周期管理规则时、可以将以下删除操作应用于存储分段对象：

- 删除当前版本-此操作将使规则标识的对象过期。如果在此存储分段上启用了版本控制、则S3会使所有过期对象不可用。如果未启用版本控制、则此规则将永久删除对象。CLI操作为 `Expiration`。
- 删除非当前版本-此操作指定S3何时可以永久删除非当前对象。CLI操作为 `NoncurrentVersionExpiration`。
- 删除已过期的删除标记-此操作将删除已过期的对象删除标记。  
在启用了版本控制的分段中、带有删除标记的对象将成为这些对象的当前版本。不会删除这些对象、也无法对其执行任何操作。如果没有与这些对象关联的当前版本、则这些对象将过期。CLI操作为 `Expiration`。
- 删除未完成的多部分上传-此操作设置允许许多部分上传保持进行中的最长时间(天)。之后、它们将被删除。CLI操作为 `AbortIncompleteMultipartUpload`。

您遵循的操作步骤取决于您使用的接口。对于ONTAP 9.13、1、您需要使用命令行界面。从ONTAP 9.14.1开始、您还可以使用System Manager。

### 使用命令行界面管理生命周期管理规则

从ONTAP 9.13.1开始、您可以使用ONTAP命令行界面创建生命周期管理规则、使S3存储分段中的对象过期。

### 开始之前

对于命令行界面、您需要在创建存储分段生命周期管理规则时为每种到期操作类型定义所需的字段。这些字段可在初始创建后进行修改。下表显示了每种操作类型的唯一字段。

操作类型	唯一字段
------	------

非当前版本到期	<ul style="list-style-type: none"> <li>• <code>-non-curr-days</code> -删除非当前版本之前的天数</li> <li>• <code>-new-non-curr-versions</code> -要保留的最新非最新版本的数量</li> </ul>
到期日期	<ul style="list-style-type: none"> <li>• <code>-obj-age-days</code> -自创建以来的天数，超过此天数后可以删除当前版本的对象</li> <li>• <code>-obj-exp-date</code> -对象应过期的特定日期</li> <li>• <code>-expired-obj-del-markers</code> -清理对象删除标记</li> </ul>
AbortIncompleteMultipartUpload	<ul style="list-style-type: none"> <li>• <code>-after-initiation-days</code> -启动的天数，超过此天数后可以中止上传</li> </ul>

为了使存储分段生命周期管理规则仅应用于特定的对象子集、管理员必须在创建规则时设置每个筛选器。如果在创建规则时未设置这些筛选器、则该规则将应用于存储分段中的所有对象。

在首次创建后、可以修改以下项的所有筛选器、但\_除外\_： +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

#### 步骤

1. 使用 `vserver object-store-server bucket lifecycle-management-rule create` 命令、其中包含您的到期操作类型所需的字段、用于创建存储分段生命周期管理规则。

#### 示例

以下命令将创建NonCurrentVersion Expiration分段生命周期管理规则：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

#### 示例

以下命令将创建到期分段生命周期管理规则：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

## 示例


以下命令将创建AbortIncompleteMultipartUpload分段生命周期管理规则：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

## 使用System Manager管理生命周期管理规则

从ONTAP 9.14.1开始、您可以使用System Manager使S3对象过期。您可以为S3对象添加、编辑和删除生命周期管理规则。此外、您还可以导入为一个存储分段创建的生命周期规则、并将其用于另一个存储分段中的对象。您可以禁用活动规则、并在稍后启用它。

## 添加生命周期管理规则

1. 单击\*存储>存储分段\*。
2. 选择要指定到期规则的存储分段。
3. 单击  图标并选择\*管理生命周期规则\*。
4. 单击\*添加>生命周期规则\*。
5. 在添加生命周期规则页面上、添加规则的名称。
6. 定义规则的范围，是要将其应用于存储分段中的所有对象还是特定对象。如果要指定对象、请至少添加以下筛选条件之一：
  - a. 前缀：指定规则应应用到的对象密钥名称的前缀。通常、它是对象的路径或文件夹。您可以为每个规则输入一个前缀。除非提供有效的前缀、否则规则适用场景存储分段中的所有对象。
  - b. 标记：为规则应应用到的对象最多指定三个键和值对(标记)。只能使用有效的密钥进行筛选。该值是可选的。但是、如果要添加值、请确保仅为相应的密钥添加有效值。
  - c. 大小：可以限制对象大小的最小值和最大值之间的范围。您可以输入其中一个值、也可以同时输入这两个值。默认单位为Mib。
7. 指定操作：
  - a. 使对象的当前版本过期：设置一条规则，使所有当前对象在自创建之日起的特定天数后或特定日期永久不可用。如果选择了\*删除过期对象删除标记\*选项，则此选项不可用。


- b. 永久删除非当前版本：指定版本在多少天后变为非当前版本、之后可以删除的天数以及要保留的版本数。
- c. 删除过期对象删除标记：选择此操作可删除具有过期删除标记的对象，即删除没有关联当前对象的标记。



如果选择了\*使当前对象版本过期\*选项，则此选项将不可用，此选项会在保留期限过后自动删除所有对象。当使用对象标记进行筛选时、此选项也将不可用。

- d. 删除不完整的多部分上传：设置删除不完整的多部分上传之前的天数。如果正在进行的多部分上传在指定保留期限内失败、您可以删除未完成的多部分上传。使用对象标记进行筛选时、此选项将不可用。
- e. 单击 \* 保存 \*。


## 导入生命周期规则

1. 单击\*存储>存储分段\*。
2. 选择要导入到期规则的存储分段。
3. 单击  图标并选择\*管理生命周期规则\*。
4. 单击\*添加>导入规则\*。
5. 选择要从中导入规则的存储分段。此时将显示为选定存储分段定义的生命周期管理规则。
6. 选择要导入的规则。您可以选择一次选择一个规则、第一个规则为默认选择。
7. 单击 \* 导入 \*。

## 编辑、删除或禁用规则

您只能编辑与规则关联的生命周期管理操作。如果使用对象标记筛选规则，则\*删除过期对象删除标记\*和\*删除未完成的多部分上传\*选项不可用。

删除规则后、该规则将不再应用于先前关联的对象。

1. 单击\*存储>存储分段\*。
2. 选择要编辑、删除或禁用生命周期管理规则的存储分段。
3. 单击  图标并选择\*管理生命周期规则\*。
4. 选择所需规则。您可以一次编辑和禁用一个规则。您可以一次删除多个规则。
5. 选择\*编辑\*、删除\*或\*禁用，然后完成操作步骤。

## 创建 S3 用户

所有ONTAP对象存储都需要用户授权、以限制与授权客户端的连接。

开始之前。

已启用S3的Storage VM必须已存在。

### 关于此任务

可以为S3用户授予对Storage VM中任何存储分段的访问权限。创建S3用户时、还会为此用户生成访问密钥和机密密钥。应与用户共享它们以及对象存储的FQDN和分段名称。可以使用查看S3用户密钥 `vserver object-`

store-server user show 命令:

您可以在存储分段策略或对象服务器策略中为 S3 用户授予特定访问权限。



创建新的对象存储服务器时、ONTAP会创建一个root用户(UID 0)、该用户是有权访问所有分段的特权用户。NetApp建议创建具有特定权限的管理员用户角色、而不是将ONTAP S3作为root用户进行管理。

#### 命令行界面

##### 1. 创建 S3 用户:

```
vserver object-store-server user create -vserver svm_name -user user_name  
-comment [-comment text] -key-time-to-live time
```


- 添加注释是可选的。
- 从ONTAP 9.14.1开始、您可以在中定义密钥的有效期 -key-time-to-live 参数。您可以按此格式添加保留期限、以指示访问密钥到期前的期限:  
P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W  
例如、如果要输入一天、两小时、三分钟和四秒的保留期限、请将值输入为 P1DT2H3M4S。除非指定、否则密钥的有效期不定。

以下示例将创建一个名为的用户 sm\_user1 在Storage VM上 vs0, 密钥保留期限为一周。

```
vserver object-store-server user create -vserver vs0 -user sm_user1  
-key-time-to-live P1W
```

2. 请务必保存访问密钥和机密密钥。从S3客户端访问时需要使用它们。

#### System Manager

1. 单击 \* 存储 > 存储 VM\*。选择需要添加用户的Storage VM、选择\*设置\*、然后单击  在 S3 下。
2. 要添加用户, 请单击\*用户>添加\*。
3. 输入用户的名称。
4. 从ONTAP 9.14.1开始、您可以指定为用户创建的访问密钥的保留期限。您可以指定密钥自动过期的保留期限(以天、小时、分钟或秒为单位)。默认情况下、该值设置为 0 这表示密钥无限期有效。
5. 单击 \* 保存 \*。此时将创建用户、并为该用户生成访问密钥和机密密钥。
6. 下载或保存访问密钥和机密密钥。从S3客户端访问时需要使用它们。

#### 后续步骤

- [创建或修改 S3 组](#)

#### 创建或修改 S3 组

您可以通过创建具有适当访问授权的用户组来简化存储分段访问。

#### 开始之前

启用了 S3 的 SVM 中的 S3 用户必须已存在。

#### 关于此任务

可以为 S3 组中的用户授予对 SVM 中任何存储分段的访问权限，但不能在多个 SVM 中进行访问。可以通过两种方式配置组访问权限：


- 在存储分段级别

创建一组 S3 用户后，您可以在存储分段策略语句中指定组权限，这些权限仅适用于该存储分段。

- 在 SVM 级别

创建一组 S3 用户后，您可以在组定义中指定对象服务器策略名称。这些策略决定了组成员的分段和访问权限。

#### System Manager

1. 编辑 Storage VM：单击 \* 存储 > Storage VM\*，单击此 Storage VM，单击 \* 设置\*，然后单击  在 S3 下。
2. 添加组：选择\*组\*、然后选择\*添加\*。
3. 输入组名称，然后从用户列表中进行选择。
4. 您可以选择现有组策略或立即添加一个策略，也可以稍后添加一个策略。

#### 命令行界面

1. 创建 S3 组：  

```
vserver object-store-server group create -vserver svm_name -name group_name  
-users user_name\(s\) [-policies policy_names] [-comment text\]
```

  - 。 -policies 在对象存储中只有一个存储分段的配置中、可以省略选项；组名称可以添加到存储分段策略中。
  - 。 -policies 选项可稍后使用添加 `vserver object-store-server group modify` 命令。

#### 重新生成密钥并修改其保留期限

在用户创建期间、系统会自动生成访问密钥和机密密钥、以便启用S3客户端访问。如果某个密钥已过期或泄露、您可以为用户重新生成密钥。

有关生成访问密钥的信息、请参见 ["创建 S3 用户"](#)。





## 命令行界面

1. 通过运行为用户重新生成访问和机密密钥 `vserver object-store-server user regenerate-keys` 命令：
2. 默认情况下、生成的密钥无限期有效。从9.14.1开始、您可以修改其保留期限、超过此期限、密钥将自动过期。您可以按以下格式添加保留期限：  
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`  
例如、如果要输入一天、两小时、三分钟和四秒的保留期限、请将值输入为 `P1DT2H3M4S`。

```
vserver object-store-server user regenerate-keys -vserver svm_name  
-user user -key-time-to-live 0
```

3. 保存访问密钥和机密密钥。从S3客户端访问时需要使用它们。

## System Manager

1. 单击 \* 存储 > 存储 VM\*，然后选择此 Storage VM。
2. 在 \* 设置 \* 选项卡中，单击  在 \* S3 \* 区块中。
3. 在\*USERS\*选项卡中，确认没有访问密钥，或者该密钥已过期。
4. 如果需要重新生成密钥、请单击  单击用户旁边的\*重新生成密钥\*。
5. 默认情况下、生成的密钥的有效期不定。从9.14.1开始、您可以修改其保留期限、超过此期限、密钥将自动过期。输入保留期限、以天、小时、分钟或秒为单位。
6. 单击 \* 保存 \*。此时将重新生成密钥。对密钥保留期限所做的任何更改都将立即生效。
7. 下载或保存访问密钥和机密密钥。从S3客户端访问时需要使用它们。

## 创建或修改访问策略语句

### 关于存储分段和对象存储服务器策略

用户和组对 S3 资源的访问由存储分段和对象存储服务器策略控制。如果用户或组数量较少，则在存储分段级别控制访问可能就已足够，但如果用户和组数量众多，则在对象存储服务器级别控制访问更容易。

### 修改存储分段策略

您可以向默认存储分段策略添加访问规则。其访问控制的范围是包含的存储分段，因此，只有一个存储分段时，它才是最合适的。

### 开始之前

必须已存在已启用S3且包含S3服务器和存储分段的Storage VM。

在授予权限之前，您必须已创建用户或组。

### 关于此任务

您可以为新用户和组添加新语句，也可以修改现有语句的属性。有关更多选项、请参见 `vserver object-store-server bucket policy` 手册页。

可以在创建存储分段时或稍后根据需要授予用户和组权限。您还可以修改存储分段容量和 QoS 策略组分配。

从ONTAP 9.9.1开始、如果您计划在ONTAP S3服务器上支持AWS客户端对象标记功能、请执行以下操作 `GetObjectTagging`，`PutObjectTagging`，和 `DeleteObjectTagging` 需要允许使用存储分段或组策略。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

## System Manager

### 步骤

1. 编辑存储分段：单击 \* 存储 > 存储分段 \*，单击所需分段，然后单击 \* 编辑 \*。  
添加或修改权限时，您可以指定以下参数：

- 主体：被授予访问权限的用户或组。
- 影响：允许或拒绝对用户或组的访问。
- 操作：给定用户或组在存储分段中允许执行的操作。
- 资源：允许或拒绝访问的存储分段中对象的路径和名称。

默认值 \*； bucketname\_\* 和 \*； bucketname/\*； 用于授予对存储分段中所有对象的访问权限。  
您还可以授予对单个对象的访问权限，例如 \*； bucketname/\_\*； readme.txt\*。

- 条件(可选)：尝试访问时评估的表达式。例如，您可以指定允许或拒绝访问的 IP 地址列表。



从ONTAP 9.14.1开始，您可以在\*Res型\*字段中为存储分段策略指定变量。这些变量是占位符、在评估策略时、这些占位符将替换为上下文值。例如、If \${aws:username} 指定为策略的变量、然后此变量将替换为请求上下文用户名、并且可以按照为该用户配置的方式执行策略操作。

### 命令行界面

#### 步骤

1. 向存储分段策略添加语句：

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

以下参数用于定义访问权限：

-effect	该语句可能允许或拒绝访问
-action	您可以指定 * 表示所有操作、或者包含以下一项或多项的列表： GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, 和 ListMultipartUploadParts。
-principal	一个或多个 S3 用户或组的列表。 <ul style="list-style-type: none"><li>• 最多可以指定 10 个用户或组。</li><li>• 如果指定了S3组、则必须采用的格式 group/group_name。</li><li>• * 可以指定为表示公共访问、即不使用访问密钥和机密密钥的访问。</li><li>• 如果未指定主体、则会为Storage VM中的所有S3用户授予访问权限。</li></ul>

-resource

分段及其包含的任何对象。通配符 \* 和 ? 可用于形成用于指定资源的正则表达式。对于资源、您可以在策略中指定变量。这些策略变量是在评估策略时用上下文值替换的占位符。

您可以选择使用指定文本字符串作为注释 -sid 选项

#### 示例

以下示例将为Storage VM svm1.example.com和bucket1创建对象存储服务器分段策略语句、指定允许对象存储服务器用户user1访问自述文件文件夹。

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

以下示例将为Storage VM svm1.example.com和bucket1创建对象存储服务器分段策略语句、该语句指定允许访问对象存储服务器组group1的所有对象。

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

从ONTAP 9.14.1开始、您可以为分段策略指定变量。以下示例将为Storage VM创建服务器分段策略语句 svm1 和 bucket1 和指定 `\${aws:username}` 作为策略资源的变量。评估策略时、策略变量将替换为请求上下文用户名、并且可以按照为该用户配置的方式执行策略操作。例如、在评估以下策略语句时、`\${aws:username}` 替换为执行S3操作的用户。如果是用户 user1 执行此操作时、该用户将被授予访问权限 bucket1 作为 bucket1/user1/\*。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

#### 创建或修改对象存储服务器策略

您可以创建可应用于对象存储中的一个或多个分段的策略。可以将对象存储服务器策略附加到用户组，从而简化跨多个存储分段的资源访问管理。

#### 开始之前

包含 S3 服务器和存储分段且已启用 S3 的 SVM 必须已存在。

#### 关于此任务

您可以通过在对象存储服务器组中指定默认或自定义策略来在 SVM 级别启用访问策略。只有在组定义中指定策略后，这些策略才会生效。



使用对象存储服务器策略时，您可以在组定义中指定主体（即用户和组），而不是在策略本身中指定主体。

访问 ONTAP S3 资源有三种只读默认策略：

- 完全访问
- NoS3 访问
- 只读访问

您也可以创建新的自定义策略，然后为新用户和组添加新语句，或者修改现有语句的属性。有关更多选项、请参见 `vserver object-store-server policy` ["命令参考"](#)。


从ONTAP 9.9.1开始、如果您计划在ONTAP S3服务器上支持AWS客户端对象标记功能、请执行以下操作  
`GetObjectTagging`，`PutObjectTagging`，和 `DeleteObjectTagging` 需要允许使用存储分段或组策略。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用System Manager创建或修改对象存储服务器策略

步骤

- 1. 编辑 Storage VM：单击 \* 存储 > Storage VM\*，单击此 Storage VM，单击 \* 设置 \*，然后单击  在 S3 下。
- 2. 添加用户：单击 \* 策略 \*，然后单击 \* 添加 \*。
  - a. 输入策略名称并从组列表中进行选择。
  - b. 选择现有默认策略或添加新策略。

添加或修改组策略时，您可以指定以下参数：

- group：授予访问权限的组。
- 影响：允许或拒绝对一个或多个组的访问。
- 操作：给定组的一个或多个分段中允许的操作。
- 资源：授予或拒绝访问权限的一个或多个分段中的对象的路径和名称。  
例如：
  - \* 授予对 Storage VM 中所有分段的访问权限。
  - \* bucketname\* 和 \* bucketname/\* 授予对特定存储分段中所有对象的访问权限。
  - \*bucketname/readme.txt 授予对特定存储分段中某个对象的访问权限。
- c. 如果需要，可将语句添加到现有策略中。

命令行界面

使用命令行界面创建或修改对象存储服务器策略

步骤

- 1. 创建对象存储服务器策略：

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

- 2. 为策略创建语句：

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

以下参数用于定义访问权限：

-effect	该语句可能允许或拒绝访问
---------	--------------

<code>-action</code>	您可以指定 * 表示所有操作、或者包含以下一项或多项的列表: <code>GetObject</code> , <code>PutObject</code> , <code>DeleteObject</code> , <code>ListBucket</code> , <code>GetBucketAcl</code> , <code>GetObjectAcl</code> , <code>ListAllMyBuckets</code> , <code>ListBucketMultipartUploads</code> , 和 <code>ListMultipartUploadParts</code> 。
<code>-resource</code>	分段及其包含的任何对象。通配符 * 和 ? 可用于形成用于指定资源的正则表达式。

您可以选择使用指定文本字符串作为注释 `-sid` 选项

默认情况下, 新的语句将添加到语句列表的末尾, 并按顺序进行处理。以后添加或修改语句时、您可以选择修改该语句的 `-index` 设置以更改处理顺序。

## 配置外部目录服务的S3访问

从ONTAP 9.14.1开始、外部目录服务已与ONTAP S3对象存储集成。这种集成通过外部目录服务简化了用户和访问管理。

您可以为属于外部目录服务的用户组提供对ONTAP对象存储环境的访问权限。轻型目录访问协议(LDAP)是一个用于与目录服务(如Active Directory)通信的接口、这些服务为身份和访问管理(IAM)提供数据库和服务。要提供访问权限、您需要在ONTAP S3环境中配置LDAP组。配置访问权限后、组成员将有权访问ONTAP S3存储分段。有关LDAP的信息、请参见 ["LDAP 使用概述"](#)。

您还可以将Active Directory用户组配置为快速绑定模式、以便验证用户凭据、并通过LDAP连接对第三方和开源S3应用程序进行身份验证。

### 开始之前

在配置LDAP组并为组访问启用快速绑定模式之前、请确保满足以下要求:

1. 已创建一个包含S3服务器且已启用S3的Storage VM。请参见 ["为 S3 创建 SVM"](#)。
2. 已在此Storage VM中创建存储分段。请参见 ["创建存储分段"](#)。
3. 已在Storage VM上配置DNS。请参见 ["配置 DNS 服务"](#)。
4. 此Storage VM上安装了LDAP服务器的自签名根证书颁发机构(CA)证书。请参见 ["在 SVM 上安装自签名根 CA 证书"](#)。
5. LDAP客户端在SVM上配置为启用TLS。请参见 ["创建 LDAP 客户端配置"](#) 和 ["请将LDAP客户端配置与SVM关联以了解相关信息"](#)。

## 配置外部目录服务的S3访问

1. 指定LDAP作为组的SVM的 `_name service database _`、并将密码指定给LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

有关此命令的详细信息、请参见 ["vserver services name-service ns-switch modify"](#) 命令：

2. 使用创建对象存储分段策略语句 `principal` 设置为要授予访问权限的LDAP组：

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

示例：以下示例将为创建存储分段策略语句 `buck1`。此策略允许对LDAP组进行访问 `group1` 资源(存储分段及其对象) `buck1`。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. 验证LDAP组中的用户 `group1` 能够从S3客户端执行S3操作。

使用LDAP快速绑定模式进行身份验证

1. 指定LDAP作为组的SVM的 `_name service database _`、并将密码指定给LDAP：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

有关此命令的详细信息、请参见 ["vserver services name-service ns-switch modify"](#) 命令：

2. 确保访问S3存储分段的LDAP用户具有存储分段策略中定义的权限。有关详细信息，请参见 ["修改存储分段策略"](#)。
3. 验证LDAP组中的用户是否可以执行以下操作：
  - a. 在S3客户端上按以下格式配置访问密钥：  
"NTAPFASTBIND" + base64-encode (user-name:password)  
示例 "NTAPFASTBIND" + base64-encode (LDAPUser: password)、这将导致出现此问题





S3客户端可能会提示输入机密密钥。如果没有机密密钥、则可以输入任何至少包含16个字符的密码。

- b. 从用户拥有权限的S3客户端执行基本S3操作。

允许LDAP或域用户生成自己的S3访问密钥

从ONTAP 9.14.1开始、作为ONTAP管理员、您可以创建自定义角色并将其授予本地或域组或轻型目录访问协议(Lightweight-Directory Access Protocol、LDAP)组、以便属于这些组的用户可以生成自己的访问权限和机密密钥来进行S3客户端访问。

您必须在Storage VM上执行一些配置步骤、才能创建自定义角色并将其分配给调用API以生成访问密钥的用户。

开始之前

确保满足以下要求：

1. 已创建一个包含S3服务器且已启用S3的Storage VM。请参见 ["为 S3 创建 SVM"](#)。
2. 已在此Storage VM中创建存储分段。请参见 ["创建存储分段"](#)。
3. 已在Storage VM上配置DNS。请参见 ["配置 DNS 服务"](#)。
4. 此Storage VM上安装了LDAP服务器的自签名根证书颁发机构(CA)证书。请参见 ["在 SVM 上安装自签名根 CA 证书"](#)。
5. LDAP客户端已在Storage VM上配置为启用TLS。请参见 ["创建 LDAP 客户端配置"](#) 和。
6. 将客户端配置与Vserver相关联。请参见 ["将 LDAP 客户端配置与 SVM 关联"](#) 和 ["vserver services name-service ldap create"](#)。
7. 如果您使用的是数据Storage VM、请在此VM上创建管理网络接口(LIF)和、并为此LIF创建一个服务策略。请参见 ["创建网络接口"](#) 和 ["network interface service-policy create"](#) 命令

配置用户以生成访问密钥

1. 指定LDAP作为组的Storage VM的\_name service database \_、并为LDAP设置密码：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

有关此命令的详细信息、请参见 ["vserver services name-service ns-switch modify"](#) 命令：

2. 创建可访问S3用户REST API端点的自定义角色：

```
security login rest-role create -vserver <vserver-name> -role <custom-role-
name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

在此示例中、将显示 s3-role 此角色是为Storage VM上的用户生成的 svm-1，授予所有访问权限，包括读取、创建和更新权限。

```
security login rest-role create -vserver svm-1 -role s3role -api  
"/api/protocols/s3/services/*/users" -access all
```

有关此命令的详细信息、请参见 ["security login rest-role create" 命令](#)：

3. 使用security login命令创建一个LDAP用户组、然后添加用于访问S3用户REST API端点的新自定义角色。有关此命令的详细信息、请参见 ["创建安全登录" 命令](#)：

```
security login create -user-or-group-name <ldap-group-name> -application  
http -authentication-method nsswitch -role <custom-role-name> -is-ns  
-switch-group yes
```

在此示例中、为LDAP组 ldap-group-1 在中创建 svm-1 和自定义角色 s3role 添加到其中、用于访问API端点、并在快速绑定模式下启用LDAP访问。

```
security login create -user-or-group-name ldap-group-1 -application http  
-authentication-method nsswitch -role s3role -is-ns-switch-group yes  
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

有关详细信息、请参见 ["使用LDAP快速绑定进行nsswitch身份验证"](#)。

将自定义角色添加到域或LDAP组后、该组中的用户可以对ONTAP进行有限的访问 /api/protocols/s3/services/{svm.uuid}/users 端点。通过调用API、域或LDAP组用户可以生成自己的访问权限和机密密钥来访问S3客户端。他们只能为自己生成密钥、而不能为其他用户生成密钥。

作为**S3**或**LDAP**用户、生成您自己的访问密钥

从ONTAP 9.14.1开始、如果管理员已授予您生成自己密钥的角色、您可以生成自己的访问权限和机密密钥来访问S3客户端。您只能使用以下ONTAP REST API端点为自己生成密钥。

#### HTTP方法和端点

此REST API调用使用以下方法和端点。有关此端点的其他方法的信息、请参见参考 ["API文档"](#)。

HTTP 方法	路径
发布	/api/protocols、s3/services / {svm.unid} /用户

## curl 示例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name": "_name_"}'
```

## JSON 输出示例

```
{
  "records": [
    {
      "access_key":
      "Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
      U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
      "A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
      rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

## 启用客户端对 S3 对象存储的访问

为远程 **FabricPool** 分层启用 **ONTAP S3** 访问

要将 ONTAP S3 用作远程 FabricPool 容量（云）层，ONTAP S3 管理员必须向远程 ONTAP 集群管理员提供有关 S3 服务器配置的信息。

关于此任务

要配置 FabricPool 云层，需要以下 S3 服务器信息：

- 服务器名称（FQDN）
- Bucket Name
- CA 证书
- 访问密钥
- 密码（机密访问密钥）

此外，还需要以下网络配置：

- 在为管理 SVM 配置的 DNS 服务器中，必须为远程 ONTAP S3 服务器的主机名提供一个条目，包括 S3 服务器的 FQDN 名称及其 LIF 上的 IP 地址。
- 必须在本地集群上配置集群间LIF、但不需要建立集群对等关系。

请参见有关将 ONTAP S3 配置为云层的 FabricPool 文档。

### "使用 FabricPool 管理存储层"

为本地 **FabricPool** 分层启用 **ONTAP S3** 访问

要将 ONTAP S3 用作本地 FabricPool 容量层，您必须根据创建的存储分段定义对象存储，然后将对象存储附加到性能层聚合以创建 FabricPool。

开始之前

您必须具有ONTAP S3服务器名称和存储分段名称、并且S3服务器必须已使用集群LUN (使用 `-vserver Cluster` 参数)。

关于此任务

对象存储配置包含有关本地容量层的信息，包括 S3 服务器和存储分段名称以及身份验证要求。

创建对象存储配置后，不能与其他对象存储或存储分段重新关联。您可以为本地层创建多个存储分段，但不能在一个存储分段中创建多个对象存储。

本地容量层不需要 FabricPool 许可证。

步骤

1. 为本地容量层创建对象存储：

```
storage aggregate object-store config create -object-store-name store_name
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- 。 `-container-name` 是您创建的S3存储分段。
- 。 `-access-key` 参数用于授权向ONTAP S3服务器发出的请求。
- 。 `-secret-password` 参数(机密访问密钥)用于对向ONTAP S3服务器发出的请求进行身份验证。
- 您可以设置 `-is-certificate-validation-enabled` 参数设置为 `false` 禁用ONTAP S3的证书检查。

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipspace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. 显示并验证对象存储配置信息：

```
storage aggregate object-store config show
```

3. 可选：要查看卷中处于非活动状态的数据量，请按照中的步骤进行操作 ["使用非活动数据报告确定卷中处于非活动状态的数据量"](#)。

查看卷中处于非活动状态的数据量有助于确定要用于 FabricPool 本地分层的聚合。

4. 将对象存储附加到聚合：

```
storage aggregate object-store attach -aggregate aggr_name -object-store-name
store_name
```

您可以使用 `allow-flexgroup true` 用于附加包含FlexGroup卷成分卷的聚合的选项。

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. 显示对象存储信息并验证连接的对象存储是否可用：

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
aggr1	MyLocalObjStore	available

## 从 S3 应用程序启用客户端访问

要使 S3 客户端应用程序能够访问 ONTAP S3 服务器，ONTAP S3 管理员必须向 S3 用户提供配置信息。

### 开始之前

S3客户端应用程序必须能够使用以下AWS签名版本与ONTAP S3服务器进行身份验证：

- 签名版本4、ONTAP 9.8及更高版本
- 签名版本2、ONTAP 9.11.1及更高版本

ONTAP S3不支持其他签名版本。

ONTAP S3 管理员必须已在存储分段策略或对象服务器策略中创建 S3 用户并为其授予以个人用户或组成员身份进行访问的权限。

S3 客户端应用程序必须能够解析 ONTAP S3 服务器名称，这要求 ONTAP S3 管理员为 S3 服务器的 LIF 提供 S3 服务器名称（FQDN）和 IP 地址。

关于此任务

要访问 ONTAP S3 存储分段，S3 客户端应用程序上的用户将输入 ONTAP S3 管理员提供的信息。


从 ONTAP 9.1.1 开始，ONTAP S3 服务器支持以下 AWS 客户端功能：

- 用户定义的对象元数据

使用 PUT（或 POST）创建对象时，可以将一组键值对作为元数据分配给对象。对对象执行 GET 或 HEAD 操作时，将返回用户定义的元数据以及系统元数据。

- 对象标记

可以为对象分配一组单独的键值对作为标记。与元数据不同，标记是使用 REST API 独立于对象创建和读取的，它们是在创建对象时或之后的任何时间实施的。



要使客户端能够获取和放置标记信息、请执行以下操作 `GetObjectTagging`，`PutObjectTagging`，和 `DeleteObjectTagging` 需要允许使用存储分段或组策略。

有关详细信息，请参见 AWS S3 文档。

步骤

1. 通过输入 S3 服务器名称和 CA 证书，使用 ONTAP S3 服务器对 S3 客户端应用程序进行身份验证。
2. 输入以下信息，在 S3 客户端应用程序上对用户进行身份验证：
  - S3 服务器名称（FQDN）和存储分段名称
  - 用户的访问密钥和机密密钥

## 存储服务定义

ONTAP 包括映射到相应最低性能因素的预定义存储服务。

集群或 SVM 中可用的实际存储服务集取决于构成 SVM 中聚合的存储类型。

下表显示了最低性能因素如何映射到预定义的存储服务：

存储服务	预期 IOPS （SLA）	峰值 IOPS （SLO）	最小卷 IOPS	估计延迟	是否强制实施预期 IOPS？
value	每TB 128个	每TB 512个	75	17毫秒	在 AFF 上：是 否则：否

存储服务	预期 IOPS （SLA）	峰值 IOPS （SLO）	最小卷 IOPS	估计延迟	是否强制实施预期 IOPS？
性能	2048 每 TB	每 TB 4096 个	500	2毫秒	是的。
极高	每TB 6144个	12288/ TB	1000	1毫秒	是的。

下表定义了每种类型的介质或节点的可用存储服务级别：

介质或节点	可用存储服务级别
Disk	value
虚拟机磁盘	value
FlexArray LUN	value
混合	value
容量优化的闪存	value
固态驱动器（SSD）—非 AFF	value
性能优化的闪存— SSD （AFF）	极高，性能，价值

## 使用 S3 SnapMirror 保护存储分段

### S3 SnapMirror 概述

从ONTAP 9.10.1开始、您可以使用SnapMirror镜像和备份功能保护ONTAP S3对象存储中的分段。与标准SnapMirror不同、S3 SnapMirror支持镜像和备份到非NetApp目标、如AWS S3。

S3 SnapMirror 支持从 ONTAP S3 存储分段到以下目标的活动镜像和备份层：

target	是否支持活动镜像和接管？	是否支持备份和还原？
ONTAP S3 <ul style="list-style-type: none"> <li>• 同一 SVM 中的存储分段</li> <li>• 同一集群上不同 SVM 中的存储分段</li> <li>• 不同集群上 SVM 中的存储分段</li> </ul>	✓	✓
StorageGRID		✓

target	是否支持活动镜像和接管？	是否支持备份和还原？
AWS S3		✓
适用于 Azure 的 Cloud Volumes ONTAP	✓	✓
适用于 AWS 的 Cloud Volumes ONTAP	✓	✓
适用于 Google Cloud 的 Cloud Volumes ONTAP	✓	✓

您可以保护 ONTAP S3 服务器上的现有存储分段，也可以在立即启用数据保护的情况下创建新存储分段。

## S3 SnapMirror 要求

- ONTAP 版本  
源集群和目标集群上必须运行ONTAP 9.10.1或更高版本。
- 许可  
ONTAP源系统和目标系统需要以下许可证包：
  - 核心软件包  
适用于ONTAP S3协议和存储。
  - 数据保护捆绑包  
S3 SnapMirror以其他NetApp对象存储目标(ONTAP S3、StorageGRID和Cloud Volumes ONTAP)为目标。
  - 数据保护包和混合云包  
S3 SnapMirror到第三方对象存储(包括AWS S3)。
- ONTAP S3
  - ONTAP S3 服务器必须运行源和目标 SVM 。
  - 建议但不要求在托管 S3 服务器的系统上安装用于 TLS 访问的 CA 证书。
    - 用于签署 S3 服务器证书的 CA 证书必须安装在托管 S3 服务器的集群的管理 Storage VM 上。
    - 您可以使用自签名 CA 证书或由外部 CA 供应商签名的证书。
    - 如果源或目标 Storage VM 未侦听 HTTPS ，则无需安装 CA 证书。
- 对等（对于 ONTAP S3 目标）
  - 必须配置集群间 LIF （对于远程 ONTAP 目标）。
  - 源集群和目标集群已建立对等关系（对于远程 ONTAP 目标）。
  - 源和目标 Storage VM 已建立对等关系（对于所有 ONTAP 目标）。
- SnapMirror 策略
  - 所有 S3 SnapMirror 关系都需要使用 S3 专用的 SnapMirror 策略，但您可以对多个关系使用同一策略。
  - 您可以创建自己的策略或接受默认的 \* 持续 \* 策略，其中包含以下值：
    - 限制（吞吐量 / 带宽的上限）—无限制。
    - 恢复点目标的时间： 1 小时（ 3600 秒）。
- root用户密钥  
S3 SnapMirror关系需要Storage VM root用户访问密钥；默认情况下、ONTAP不会分配这些密钥。首次创建 S3 SnapMirror 关系时，您必须验证源和目标 Storage VM 上是否存在这些密钥，如果不存在，则重新生成



这些密钥。如果需要重新生成这些密钥，则必须确保使用访问密钥和机密密钥对的所有客户端和所有 SnapMirror 对象存储配置都使用新密钥进行更新。

有关 S3 服务器配置的信息，请参见以下主题：

- ["在 Storage VM 上启用 S3 服务器"](#)
- ["关于 S3 配置过程"](#)

有关集群和 Storage VM 对等的信息，请参见以下主题：

- ["准备镜像和存储（ System Manager ， 步骤 1-6 ） "](#)
- ["集群和 SVM 对等（ CLI ） "](#)

## 支持的SnapMirror关系

S3 SnapMirror 支持扇出和级联关系。有关概述，请参见 ["扇出和级联数据保护部署"](#)。

S3 SnapMirror不支持扇入部署(多个源分段与单个目标分段之间的数据保护关系)。S3 SnapMirror 支持从多个集群到一个二级集群的多个存储分段镜像，但每个源存储分段在二级集群上必须有自己的目标存储分段。

## 控制对S3存储分段的访问

创建新存储分段时，您可以通过创建用户和组来控制访问。有关详细信息，请参见以下主题：

- ["添加 S3 用户和组（ System Manager ） "](#)
- ["创建 S3 用户（命令行界面） "](#)
- ["创建或修改 S3 组（命令行界面） "](#)

## 远程集群上的镜像和备份保护

为新存储分段（远程集群）创建镜像关系

创建新的 S3 存储分段时，您可以立即将其保护到远程集群上的 S3 SnapMirror 目标。



### 关于此任务

您需要在源系统和目标系统上执行任务。

### 开始之前


- 已完成 ONTAP 版本，许可和 S3 服务器配置的要求。
- 源集群和目标集群之间存在对等关系，源 Storage VM 和目标 Storage VM 之间存在对等关系。
- 源和目标 VM 需要 CA 证书。您可以使用自签名 CA 证书或由外部 CA 供应商签名的证书。

## System Manager

1. 如果这是此 Storage VM 的第一个 S3 SnapMirror 关系，请验证源和目标 Storage VM 是否都存在根用户密钥，如果没有，请重新生成这些密钥：
  - a. 单击 \* 存储 > 存储 VM\*，然后选择此 Storage VM。
  - b. 在 \* 设置 \* 选项卡中，单击  在 \* S3 \* 区块中。
  - c. 在 \* 用户 \* 选项卡中，验证是否存在 root 用户的访问密钥。
  - d. 如果没有，请单击  在 \* 根 \* 旁边，单击 \* 重新生成密钥 \*。  
如果已存在密钥，请勿重新生成该密钥。
2. 编辑 Storage VM 以在源和目标 Storage VM 中添加用户并将用户添加到组：

单击 \* 存储 > Storage VM\*，单击此 Storage VM，单击 \* 设置 \*，然后单击  在 S3 下。

请参见 ["添加 S3 用户和组"](#) 有关详细信息 ...

3. 在源集群上，如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：
  - a. 单击 \* 保护 > 概述 \*，然后单击 \* 本地策略设置 \*。
  - b. 单击  在 \* 保护策略 \* 旁边，单击 \* 添加 \*。
    - 输入策略名称和问题描述。
    - 选择策略范围，集群或 SVM
    - 为 S3 SnapMirror 关系选择 \* 持续 \*。
    - 输入 \* 限制 \* 和 \* 恢复点目标 \* 值。
4. 创建具有 SnapMirror 保护的存储分段：
  - a. 单击 \* 存储 > 分段 \*，然后单击 \* 添加 \*。验证权限是可选的，但建议这样做。
  - b. 输入名称，选择 Storage VM，输入大小，然后单击 \* 更多选项 \*。
  - c. 在 \* 权限 \* 下，单击 \* 添加 \*。
    - \* 主体 \* 和 \* 影响 \* —选择与您的用户组设置对应的值或接受默认值。
    - **Actions**-确保显示以下值：

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- **Results**-使用默认值 (*bucketname*, *bucketname/\**) 或您需要的其他值。

请参见 ["管理用户对存储分段的访问权限"](#) 有关这些字段的详细信息，请参见。

- d. 在 \* 保护 \* 下，选中 \* 启用 SnapMirror (ONTAP 或云) \*。然后输入以下值：
  - 目标
    - \* 目标: ONTAP System\*
    - \* 集群 \* : 选择远程集群。

- \* Storage VM\*：选择远程集群上的 Storage VM。
- \* S3 服务器 CA 证书\*：复制并粘贴 *source* 证书的内容。
- 源
  - \* S3 服务器 CA 证书：\* 复制并粘贴 *\_destination\_certificate* 的内容。

5. 选中 \* 如果您使用的是由外部 CA 供应商签名的证书，请在目标 \* 上使用相同的证书。
6. 如果单击 \* 目标设置 \*，您还可以输入自己的值来替代存储分段名称，容量和性能服务级别的默认值。
7. 单击 \* 保存 \*。此时将在源Storage VM中创建一个新分段、并将其镜像到目标Storage VM中创建的新分段。

## 备份锁定的铲斗

从ONTAP 9.14.1开始、您可以备份锁定的S3存储分段并根据需要进行还原。

在为新存储分段或现有存储分段定义保护设置时、您可以在目标存储分段上启用对象锁定、但前提是源集群和目标集群运行ONTAP 9.14.1或更高版本、并且源存储分段上启用了对象锁定。源分段的对象锁定模式和锁定保留期限将适用于目标分段上复制的对象。您也可以在\*目标设置\*部分中为目标存储分段定义不同的锁定保留期限。此保留期限也适用于从源存储分段和S3接口复制的任何非锁定对象。

有关如何在存储分段上启用对象锁定的信息、请参见 ["创建存储分段"](#)。

## 命令行界面

1. 如果这是此 SVM 的第一个 S3 SnapMirror 关系，请验证源和目标 SVM 是否都存在根用户密钥，如果没有，请重新生成这些密钥：

```
vserver object-store-server user show
```

验证是否存在 root 用户的访问密钥。如果没有，请输入：

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

如果已存在密钥，请勿重新生成该密钥。

2. 在源和目标 SVM 中创建分段：

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. 将访问规则添加到源和目标 SVM 的默认存储分段策略中：

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

#### 示例

```
src_cluster::> vservers object-store-server bucket policy add-  
statement -bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc  
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. 如果您没有现有的S3 SnapMirror策略、并且不想使用默认策略、请在源SVM上创建此策略：  
snapmirror policy create -vservers svm\_name -policy policy\_name -type  
continuous [-rpo integer] [-throttle throttle\_type] [-comment text]  
[additional\_options]

#### Parameters

- type continuous - S3 SnapMirror关系的唯一策略类型(必需)。
- -rpo -指定恢复点目标的时间(以秒为单位)(可选)。
- -throttle -指定吞吐量/带宽的上限(以千字节/秒为单位)(可选)。

#### 示例

```
src_cluster::> snapmirror policy create -vservers vs0 -type  
continuous -rpo 0 -policy test-policy
```

5. 在源集群和目标集群的管理 SVM 上安装 CA 服务器证书：

- a. 在源集群上、安装对\_deign\_ S3服务器证书签名的CA证书：

```
security certificate install -type server-ca -vservers src_admin_svm  
-cert-name dest_server_certificate
```

- b. 在目标集群上、安装对\_ssourc\_ S3服务器证书签名的CA证书：

```
security certificate install -type server-ca -vservers dest_admin_svm  
-cert-name src_server_certificate
```

如果您使用的证书由外部 CA 供应商签名，请在源和目标管理 SVM 上安装相同的证书。

请参见 security certificate install 有关详细信息、请参见手册页。

6. 在源 SVM 上，创建 S3 SnapMirror 关系：

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

您可以使用创建的策略或接受默认值。

#### 示例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy test-policy
```

#### 7. 验证镜像是否处于活动状态：

```
snapmirror show -policy-type continuous -fields status
```

为现有存储分段（远程集群）创建镜像关系

您可以随时开始保护现有的 S3 存储分段；例如，如果从 ONTAP 9.10.1 之前的版本升级了 S3 配置。

关于此任务

您需要在源集群和目标集群上执行任务。

开始之前

- 已完成 ONTAP 版本，许可和 S3 服务器配置的要求。
- 源集群和目标集群之间存在对等关系，源 Storage VM 和目标 Storage VM 之间存在对等关系。
- 源和目标 VM 需要 CA 证书。您可以使用自签名 CA 证书或由外部 CA 供应商签名的证书。



步骤

您可以使用 System Manager 或 ONTAP 命令行界面创建镜像关系。

## System Manager

1. 如果这是此 Storage VM 的第一个 S3 SnapMirror 关系，请验证源和目标 Storage VM 是否都存在根用户密钥，如果没有，请重新生成这些密钥：
  - a. 选择\*存储> Storage VM\*、然后选择Storage VM。
  - b. 在 \* 设置 \* 选项卡中，单击  在 \* S3 \* 区块中。
  - c. 在 \* 用户 \* 选项卡中，验证是否存在 root 用户的访问密钥。
  - d. 如果没有，请单击  在\*root\*旁边，单击\*Regerate Key.\*  
如果已存在密钥，请勿重新生成该密钥。
2. 验证源和目标 Storage VM 中的用户和组访问是否正确：  
选择\*存储> Storage VM\*、然后选择Storage VM、最后选择\*设置\*。最后、选择  在 \* S3 下。

请参见 "添加 S3 用户和组" 有关详细信息 ...

3. 在源集群上，如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：
  - a. 选择\*保护>概述\*，然后单击\*本地策略设置\*。
  - b. 选择 ...  在 \* 保护策略 \* 旁边，单击 \* 添加 \*。
  - c. 输入策略名称和问题描述。
  - d. 选择策略范围，集群或 SVM
  - e. 为 S3 SnapMirror 关系选择 \* 持续 \*。
  - f. 输入 \* 限制 \* 和 \* 恢复点目标 \* 值。
4. 验证现有存储分段的存储分段访问策略是否仍满足您的需求：
  - a. 单击 \* 存储 > 分段 \*，然后选择要保护的分段。
  - b. 在 \* 权限 \* 选项卡中，单击  编辑，然后单击\*权限\*下的\*添加\*。
    - \* 主体和影响 \*：选择与您的用户组设置对应的值，或者接受默认值。
    - 操作：确保显示以下值：

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- **Results:** 使用默认值 (*bucketname*, *bucketname/\**) 或您需要的其他值。

请参见 "管理用户对存储分段的访问权限" 有关这些字段的详细信息，请参见。

5. 使用 S3 SnapMirror 保护保护现有存储分段：
  - a. 单击 \* 存储 \* > \* 分段 \*，然后选择要保护的分段。
  - b. 单击 \* 保护 \* 并输入以下值：
    - 目标
      - \* 目标 \*： ONTAP 系统

- \* 集群 \*：选择远程集群。
- \* Storage VM\*：选择远程集群上的 Storage VM。
- \* S3 服务器 CA 证书 \*：复制并粘贴 *source* 证书的内容。
- 源
  - \* S3 服务器 CA 证书 \*：复制并粘贴 *\_destination\_certificate* 的内容。

6. 选中 \* 如果您使用的是由外部 CA 供应商签名的证书，请在目标 \* 上使用相同的证书。

7. 如果单击 \* 目标设置 \*，您还可以输入自己的值来替代存储分段名称，容量和性能服务级别的默认值。

8. 单击 \* 保存 \*。现有存储分段将镜像到目标Storage VM中的新存储分段。

## 备份锁定的铲斗

从ONTAP 9.14.1开始、您可以备份锁定的S3存储分段并根据需要进行还原。

在为新存储分段或现有存储分段定义保护设置时、您可以在目标存储分段上启用对象锁定、但前提是源集群和目标集群运行ONTAP 9.14.1或更高版本、并且源存储分段上启用了对象锁定。源分段的对象锁定模式和锁定保留期限将适用于目标分段上复制的对象。您也可以在\*目标设置\*部分中为目标存储分段定义不同的锁定保留期限。此保留期限也适用于从源存储分段和S3接口复制的任何非锁定对象。

有关如何在存储分段上启用对象锁定的信息、请参见 ["创建存储分段"](#)。

## 命令行界面

1. 如果这是此 SVM 的第一个 S3 SnapMirror 关系，请验证源和目标 SVM 是否都存在根用户密钥，如果没有，请重新生成这些密钥：

```
vserver object-store-server user show
```

验证是否存在 root 用户的访问密钥。如果没有，请输入：

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

如果已存在密钥，请勿重新生成该密钥。

2. 在目标 SVM 上创建一个存储分段作为镜像目标：

```
vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. 验证源和目标SVM中默认分段策略的访问规则是否正确：

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

#### 示例

```
src_cluster::> vsserver object-store-server bucket policy add-  
statement -bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc  
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. 在源 SVM 上，如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：

```
snapmirror policy create -vsserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

#### Parameters

- continuous –S3 SnapMirror关系的唯一策略类型(必需)。
- -rpo 指定恢复点目标的时间(以秒为单位)(可选)。
- -throttle 指定吞吐量/带宽的上限(以千字节/秒为单位)(可选)。

#### 示例

```
src_cluster::> snapmirror policy create -vsserver vs0 -type  
continuous -rpo 0 -policy test-policy
```

5. 在源集群和目标集群的管理 SVM 上安装 CA 证书：

- a. 在源集群上、安装对\_deign\_ S3服务器证书签名的CA证书：

```
security certificate install -type server-ca -vsserver src_admin_svm  
-cert-name dest_server_certificate
```

- b. 在目标集群上、安装对\_ssourc\_ S3服务器证书签名的CA证书：

```
security certificate install -type server-ca -vsserver dest_admin_svm  
-cert-name src_server_certificate
```

如果您使用的证书由外部 CA 供应商签名，请在源和目标管理 SVM 上安装相同的证书。

请参见 security certificate install 有关详细信息、请参见手册页。

6. 在源 SVM 上，创建 S3 SnapMirror 关系：

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

您可以使用创建的策略或接受默认值。



#### 示例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-bucket -destination-path vs1:/bucket/test-bucket-mirror -policy test-policy
```

#### 7. 验证镜像是否处于活动状态：

```
snapmirror show -policy-type continuous -fields status
```

从目标存储分段（远程集群）接管和提供数据

如果源存储分段中的数据不可用，您可以中断 SnapMirror 关系，使目标存储分段可写并开始提供数据。

关于此任务


执行接管操作时，源存储分段将转换为只读存储，而原始目标存储分段将转换为读写存储，从而反转 S3 SnapMirror 关系。

当禁用的源存储分段重新可用时，S3 SnapMirror 会自动重新同步这两个存储分段的内容。不必像卷 SnapMirror 部署所需的那样显式重新同步此关系。

接管操作必须从远程集群启动。

### System Manager

从不可用的存储分段进行故障转移并开始提供数据：

1. 单击 \* 保护 > 关系 \*，然后选择 \* S3 SnapMirror\*。
2. 单击 ，选择 \* 故障转移 \*，然后单击 \* 故障转移 \*。

命令行界面

1. 为目标存储分段启动故障转移操作：

```
snapmirror failover start -destination-path svm_name:/bucket/bucket_name
```

2. 验证故障转移操作的状态：

```
snapmirror show -fields status
```

#### 示例

```
dest_cluster::> snapmirror failover start -destination-path dest_svm1:/bucket/test-bucket-mirror
```

从目标 **Storage VM**（远程集群）还原存储分段

如果源存储分段中的数据丢失或损坏，您可以通过从目标存储分段还原对象来重新填充数据。

## 关于此任务


您可以将目标存储分段还原到现有存储分段或新存储分段。还原操作的目标分段必须大于目标分段的逻辑已用空间。

如果您使用现有存储分段，则在启动还原操作时，此存储分段必须为空。还原不会 "回滚" 某个存储分段，而是会使用先前的内容填充一个空存储分段。

必须从远程集群启动还原操作。

## System Manager

还原已备份的数据：

1. 单击 \* 保护 > 关系 \* ，然后选择 \* S3 SnapMirror\* 。
2. 单击  然后选择 \* 还原 \* 。
3. 在 \* 源 \* 下，选择 \* 现有分段 \* （默认值）或 \* 新分段 \* 。
  - 要还原到 \* 现有 Bucket\* （默认值），请完成以下操作：
    - 选择集群和 Storage VM 以搜索现有存储分段。
    - 选择现有存储分段。
    - 复制并粘贴 `_destination_S3` 服务器 CA 证书的内容。
  - 要还原到 \* 新存储分段 \* ，请输入以下值：
    - 用于托管新存储分段的集群和 Storage VM 。
    - 新存储分段的名称、容量和性能服务级别。  
请参见 ["存储服务级别"](#) 有关详细信息 ...
    - `_destination_S3` 服务器 CA 证书的内容。
4. 在 \* 目标 \* 下，复制并粘贴 *source* S3 服务器 CA 证书的内容。
5. 单击 \* 保护 > 关系 \* 以监控还原进度。

### 恢复锁定的存储分段

从ONTAP 9.14.1开始、您可以备份锁定的存储分段并根据需要进行还原。

您可以将对象锁定分段还原到新的或现有分段。在以下情况下、您可以选择对象锁定分段作为目标：

- 还原到新存储分段：启用对象锁定后、可以通过创建同时启用对象锁定的存储分段来还原存储分段。还原锁定的存储分段时、系统会复制原始存储分段的对象锁定模式和保留期限。您还可以为新存储分段定义不同的锁定保留期限。此保留期限适用于来自其他源的未锁定对象。
- 还原到现有存储分段：只要在现有存储分段上启用了版本控制和类似的对象锁定模式、便可将对象锁定存储分段还原到现有存储分段。保留原始存储分段的保留期限。
- 还原未锁定的存储分段：即使存储分段未启用对象锁定、您也可以将其还原到源集群上已启用对象锁定的存储分段。还原存储分段时、所有未锁定的对象都将被锁定、并且目标存储分段的保留模式和使用期限将适用于这些对象。

### 命令行界面

1. 创建新的目标存储分段以进行还原。有关详细信息，请参见 ["为新存储分段（云目标）创建备份关系"](#)。
2. 为目标存储分段启动还原操作：

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

### 示例

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-  
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

## 本地集群上的镜像和备份保护




为新存储分段创建镜像关系（本地集群）

创建新的 S3 存储分段时，您可以立即将其保护到同一集群上的 S3 SnapMirror 目标。您可以将数据镜像到与源不同的 Storage VM 或同一个 Storage VM 中的存储分段。


开始之前

- 已完成 ONTAP 版本，许可和 S3 服务器配置的要求。
- 源和目标 Storage VM 之间存在对等关系。
- 源和目标 VM 需要 CA 证书。您可以使用自签名 CA 证书或由外部 CA 供应商签名的证书。

## System Manager

1. 如果这是此 Storage VM 的第一个 S3 SnapMirror 关系，请验证源和目标 Storage VM 是否都存在根用户密钥，如果没有，请重新生成这些密钥：
  - a. 单击 \* 存储 > 存储 VM\*，然后选择此 Storage VM。
  - b. 在 \* 设置 \* 选项卡中，单击  在 S3 磁贴中。
  - c. 在 \* 用户 \* 选项卡中，验证是否存在 root 用户的访问密钥
  - d. 如果没有，请单击  在 \* 根 \* 旁边，单击 \* 重新生成密钥 \*。  
如果已存在密钥，请勿重新生成该密钥。
2. 编辑 Storage VM 以在源和目标 Storage VM 中添加用户并将用户添加到组：  
单击 \* 存储 > Storage VM\*，单击此 Storage VM，单击 \* 设置 \*，然后单击  在 S3 下。

请参见 ["添加 S3 用户和组"](#) 有关详细信息 ...

3. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：
  - a. 单击 \*Protection > Overview\*，然后单击 \*Local Policy Settings\*。
  - b. 单击  在 \* 保护策略 \* 旁边，单击 \* 添加 \*。
    - 输入策略名称和问题描述。
    - 选择策略范围，集群或 SVM
    - 为 S3 SnapMirror 关系选择 \* 持续 \*。
    - 输入 \* 限制 \* 和 \* 恢复点目标 \* 值。
4. 创建具有 SnapMirror 保护的存储分段：
  - a. 单击 \* 存储 > 分段 \*，然后单击 \* 添加 \*。
  - b. 输入名称，选择 Storage VM，输入大小，然后单击 \* 更多选项 \*。
  - c. 在 \* 权限 \* 下，单击 \* 添加 \*。验证权限是可选的，但建议这样做。
    - \* 主体 \* 和 \* 影响 \* —选择与您的用户组设置对应的值，或者接受默认值。
    - **Actions**-确保显示以下值：

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- **Results**-使用默认值 (bucketname, bucketname/\*) 或您需要的其他值

请参见 ["管理用户对存储分段的访问权限"](#) 有关这些字段的详细信息，请参见。

- d. 在 \* 保护 \* 下，选中 \* 启用 SnapMirror (ONTAP 或云) \*。然后输入以下值：
  - 目标
    - \* 目标 \*：ONTAP 系统
    - \* 集群 \*：选择本地集群。

- **Storage VM:** 选择本地集群上的Storage VM。
  - \* S3 服务器 CA 证书 \* : 复制并粘贴源证书的内容。
  - 源
    - \* S3 服务器 CA 证书 \* : 复制并粘贴目标证书的内容。
5. 选中 \* 如果您使用的是由外部 CA 供应商签名的证书, 请在目标 \* 上使用相同的证书。
  6. 如果单击 \* 目标设置 \* , 您还可以输入自己的值来替代存储分段名称, 容量和性能服务级别的默认值。
  7. 单击 \* 保存 \* 。此时将在源Storage VM中创建一个新分段、并将其镜像到目标Storage VM中创建的新分段。

#### 备份锁定的铲斗

从ONTAP 9.14.1开始、您可以备份锁定的S3存储分段并根据需要进行还原。

在为新存储分段或现有存储分段定义保护设置时、您可以在目标存储分段上启用对象锁定、但前提是源集群和目标集群运行ONTAP 9.14.1或更高版本、并且源存储分段上启用了对象锁定。源分段的对象锁定模式和锁定保留期限将适用于目标分段上复制的对象。您也可以在\*目标设置\*部分中为目标存储分段定义不同的锁定保留期限。此保留期限也适用于从源存储分段和S3接口复制的任何非锁定对象。

有关如何在存储分段上启用对象锁定的信息、请参见 ["创建存储分段"](#)。

#### 命令行界面

1. 如果这是此 SVM 的第一个 S3 SnapMirror 关系, 请验证源和目标 SVM 是否都存在根用户密钥, 如果没有, 请重新生成这些密钥:

```
vserver object-store-server user show
```

验证是否存在 root 用户的访问密钥。如果没有, 请输入:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

如果已存在密钥, 请勿重新生成该密钥。

2. 在源和目标 SVM 中创建分段:

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. 将访问规则添加到源和目标 SVM 的默认存储分段策略中:

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

#### Parameters

- continuous –S3 SnapMirror关系的唯一策略类型(必需)。
- -rpo 指定恢复点目标的时间(以秒为单位)(可选)。
- -throttle 指定吞吐量/带宽的上限(以千字节/秒为单位)(可选)。

#### 示例

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. 在管理 SVM 上安装 CA 服务器证书：

a. 在管理SVM上安装用于对\_sSource\_ S3服务器的证书进行签名的CA证书：

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```

b. 在管理SVM上安装用于对\_deign\_ S3服务器的证书进行签名的CA证书：

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate
```

如果您使用的是由外部CA供应商签名的证书、则只需在管理SVM上安装此证书即可。

请参见 security certificate install 有关详细信息、请参见手册页。

6. 创建S3 SnapMirror关系：

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy
policy_name]`
```

您可以使用创建的策略或接受默认值。

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
-policy test-policy
```

## 7. 验证镜像是否处于活动状态：

```
snapmirror show -policy-type continuous -fields status
```

为现有存储分段（本地集群）创建镜像关系




您可以随时开始保护同一集群上的现有 S3 存储分段；例如，如果您从 ONTAP 9.10.1 之前的版本升级了 S3 配置。您可以将数据镜像到与源不同的 Storage VM 或同一个 Storage VM 中的存储分段。

开始之前



- 已完成 ONTAP 版本，许可和 S3 服务器配置的要求。
- 源和目标 Storage VM 之间存在对等关系。
- 源和目标 VM 需要 CA 证书。您可以使用自签名 CA 证书或由外部 CA 供应商签名的证书。



## System Manager

1. 如果这是此 Storage VM 的第一个 S3 SnapMirror 关系，请验证源和目标 Storage VM 是否都存在根用户密钥，如果没有，请重新生成这些密钥：
  - a. 单击 \* 存储 > 存储 VM\*，然后选择此 Storage VM。
  - b. 在 \* 设置 \* 选项卡中，单击  在 \* S3 \* 区块中。
  - c. 在 \* 用户 \* 选项卡中，验证是否存在 root 用户的访问密钥。
  - d. 如果没有，请单击  在 \* 根 \* 旁边，单击 \* 重新生成密钥 \*。  
如果已存在密钥，请勿重新生成该密钥
2. 验证源和目标 Storage VM 中的用户和组访问是否正确：
  - 单击 \* 存储 > Storage VM\*，单击此 Storage VM，单击 \* 设置 \*，然后单击  在 S3 下。

请参见 ["添加 S3 用户和组"](#) 有关详细信息 ...

3. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：
  - a. 单击 \* 保护 > 概述 \*，然后单击 \* 本地策略设置 \*。
  - b. 单击  在 \* 保护策略 \* 旁边，单击 \* 添加 \*。
    - 输入策略名称和问题描述。
    - 选择策略范围，集群或 SVM
    - 为 S3 SnapMirror 关系选择 \* 持续 \*。
    - 输入 \* 限制 \* 和 \* 恢复点目标 \* 值。
4. 验证现有存储分段的存储分段访问策略是否继续满足您的需求：
  - a. 单击 \* 存储 > 分段 \*，然后选择要保护的分段。
  - b. 在 \* 权限 \* 选项卡中，单击  \* 编辑 \*，然后单击 \* 权限 \* 下的 \* 添加 \*。
    - \* 主体 \* 和 \* 影响 \* —选择与您的用户组设置对应的值，或者接受默认值。
    - **Actions**-确保显示以下值：

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- **Results**-使用默认值 (*bucketname*, *bucketname/\**) 或您需要的其他值。

请参见 ["管理用户对存储分段的访问权限"](#) 有关这些字段的详细信息，请参见。

5. 使用 S3 SnapMirror 保护现有存储分段：
  - a. 单击 \* 存储 \* > \* 分段 \*，然后选择要保护的分段。
  - b. 单击 \* 保护 \* 并输入以下值：
    - 目标
      - \* 目标 \*： ONTAP 系统

- \* 集群 \* : 选择本地集群。
- \* Storage VM\* : 选择相同或不同的 Storage VM 。
- \* S3 服务器 CA 证书 \* : 复制并粘贴 *source* 证书的内容。
- 源
  - \* S3 服务器 CA 证书 \* : 复制并粘贴 *\_destination\_certificate* 的内容。

6. 选中 \* 如果您使用的是由外部 CA 供应商签名的证书, 请在目标 \* 上使用相同的证书。

7. 如果单击 \* 目标设置 \*, 您还可以输入自己的值来替代存储分段名称, 容量和性能服务级别的默认值。

8. 单击 \* 保存 \*。现有存储分段将镜像到目标Storage VM中的新存储分段。

### 备份锁定的铲斗

从ONTAP 9.14.1开始、您可以备份锁定的S3存储分段并根据需要进行还原。

在为新存储分段或现有存储分段定义保护设置时、您可以在目标存储分段上启用对象锁定、但前提是源集群和目标集群运行ONTAP 9.14.1或更高版本、并且源存储分段上启用了对象锁定。源分段的对象锁定模式和锁定保留期限将适用于目标分段上复制的对象。您也可以在\*目标设置\*部分中为目标存储分段定义不同的锁定保留期限。此保留期限也适用于从源存储分段和S3接口复制的任何非锁定对象。

有关如何在存储分段上启用对象锁定的信息、请参见 ["创建存储分段"](#)。

### 命令行界面

1. 如果这是此 SVM 的第一个 S3 SnapMirror 关系, 请验证源和目标 SVM 是否都存在根用户密钥, 如果没有, 请重新生成这些密钥:

```
vserver object-store-server user show
```

验证是否存在 root 用户的访问密钥。如果没有, 请输入:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

如果已存在密钥, 请勿重新生成该密钥。

2. 在目标 SVM 上创建一个存储分段作为镜像目标:

```
vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. 验证源和目标 SVM 中默认分段策略的访问规则是否正确:

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`
```

#### 示例

```
clusterA::> vsserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

#### 4. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：

```
snapmirror policy create -vsserver svm_name -policy policy_name -type
continuous [-rpo _integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

##### Parameters

- continuous –S3 SnapMirror关系的唯一策略类型(必需)。
- -rpo 指定恢复点目标的时间(以秒为单位)(可选)。
- -throttle 指定吞吐量/带宽的上限(以千字节/秒为单位)(可选)。

#### 示例

```
clusterA::> snapmirror policy create -vsserver vs0 -type
continuous -rpo 0 -policy test-policy
```

#### 5. 在管理 SVM 上安装 CA 服务器证书：

##### a. 在管理SVM上安装用于对\_sSource\_ S3服务器的证书进行签名的CA证书：

```
security certificate install -type server-ca -vsserver admin_svm -cert
-name src_server_certificate
```

##### b. 在管理SVM上安装用于对\_deign\_ S3服务器的证书进行签名的CA证书：

```
security certificate install -type server-ca -vsserver admin_svm -cert
-name dest_server_certificate
```

如果您使用的是由外部CA供应商签名的证书，则只需在管理SVM上安装此证书即可。

请参见 security certificate install 有关详细信息，请参见手册页。

#### 6. 创建S3 SnapMirror关系：

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy
policy_name]
```

您可以使用创建的策略或接受默认值。

#### 示例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy test-policy
```

#### 7. 验证镜像是否处于活动状态：

```
snapmirror show -policy-type continuous -fields status
```

从目标存储分段（本地集群）接管和提供数据

如果源存储分段中的数据不可用，您可以中断 SnapMirror 关系，使目标存储分段可写并开始提供数据。

关于此任务


执行接管操作时，源存储分段将转换为只读存储，而原始目标存储分段将转换为读写存储，从而反转 S3 SnapMirror 关系。

当禁用的源存储分段重新可用时，S3 SnapMirror 会自动重新同步这两个存储分段的内容。您无需按照标准卷 SnapMirror 部署的要求明确重新同步此关系。

如果目标分段位于远程集群上，则必须从远程集群启动接管操作。

### System Manager

从不可用的存储分段进行故障转移并开始提供数据：

1. 单击 \* 保护 > 关系 \*，然后选择 \* S3 SnapMirror\*。
2. 单击 ，选择 \* 故障转移 \*，然后单击 \* 故障转移 \*。

命令行界面

1. 为目标存储分段启动故障转移操作：  

```
snapmirror failover start -destination-path svm_name:/bucket/bucket_name
```
2. 验证故障转移操作的状态：  

```
snapmirror show -fields status
```

#### 示例

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-bucket-mirror
```

从目标**Storage VM** (本地集群)还原存储分段

当源存储分段中的数据丢失或损坏时，您可以通过从目标存储分段还原对象来重新填充数据。

关于此任务


您可以将目标存储分段还原到现有存储分段或新存储分段。还原操作的目标分段必须大于目标分段的逻辑已用空间。

如果您使用现有存储分段，则在启动还原操作时，此存储分段必须为空。还原不会 " 回滚 " 某个存储分段，而是会使用先前的内容填充一个空存储分段。

还原操作必须从本地集群启动。

## System Manager

还原备份数据：

1. 单击 \* 保护 > 关系 \* ，然后选择存储分段。
2. 单击  然后选择 \* 还原 \* 。
3. 在 \* 源 \* 下，选择 \* 现有分段 \* （默认值）或 \* 新分段 \* 。
  - 要还原到 \* 现有 Bucket\* （默认值），请完成以下操作：
    - 选择集群和 Storage VM 以搜索现有存储分段。
    - 选择现有存储分段。
4. 复制并粘贴目标 S3 服务器 CA 证书的内容。
  - 要还原到 \* 新存储分段 \* ，请输入以下值：
    - 用于托管新存储分段的集群和 Storage VM 。
    - 新存储分段的名称、容量和性能服务级别。  
请参见 ["存储服务级别"](#) 有关详细信息 ...
    - 目标 S3 服务器 CA 证书的内容。
5. 在 \* 目标 \* 下，复制并粘贴源 S3 服务器 CA 证书的内容。
6. 单击 \* 保护 \* > 关系以监控还原进度。

恢复锁定的存储分段

从ONTAP 9.14.1开始、您可以备份锁定的存储分段并根据需要进行还原。

您可以将对象锁定分段还原到新的或现有分段。在以下情况下、您可以选择对象锁定分段作为目标：

- 还原到新存储分段：启用对象锁定后、可以通过创建同时启用对象锁定的存储分段来还原存储分段。还原锁定的存储分段时、系统会复制原始存储分段的对象锁定模式和保留期限。您还可以为新存储分段定义不同的锁定保留期限。此保留期限适用于来自其他源的未锁定对象。
- 还原到现有存储分段：只要在现有存储分段上启用了版本控制和类似的对象锁定模式、便可将对象锁定存储分段还原到现有存储分段。保留原始存储分段的保留期限。
- 还原未锁定的存储分段：即使存储分段未启用对象锁定、您也可以将其还原到源集群上已启用对象锁定的存储分段。还原存储分段时、所有未锁定的对象都将被锁定、并且目标存储分段的保留模式和使用期限将适用于这些对象。

命令行界面

1. 如果要将对象还原到新存储分段、请创建新存储分段。有关详细信息，请参见 ["为新存储分段（云目标）创建备份关系"](#)。
2. 为目标存储分段启动还原操作：

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

#### 示例

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

## 利用云目标实现备份保护

### 云目标关系的要求

确保源环境和目标环境满足从 S3 SnapMirror 备份保护到云目标的要求。

要访问数据分段，您必须具有对象存储提供程序的有效帐户凭据。

在集群连接到云对象存储之前，应在集群上配置集群间网络接口和 IP 空间。您应在每个节点上创建输入集群网络接口，以便将数据从本地存储无缝传输到云对象存储。

对于 StorageGRID 目标，您需要了解以下信息：

- 服务器名称，以完全限定域名（FQDN）或 IP 地址表示
- 存储分段名称；存储分段必须已存在
- 访问密钥
- 机密密钥

此外、需要使用在ONTAP S3集群的管理Storage VM上安装用于签署StorageGRID服务器证书的CA证书 security certificate install command。有关详细信息，请参见 ["安装 CA 证书"](#) 如果使用 StorageGRID。

对于 AWS S3 目标，您需要了解以下信息：

- 服务器名称，以完全限定域名（FQDN）或 IP 地址表示
- 存储分段名称；存储分段必须已存在
- 访问密钥
- 机密密钥

ONTAP 集群的管理 Storage VM 的 DNS 服务器必须能够将 FQDN（如果使用）解析为 IP 地址。

### 为新存储分段（云目标）创建备份关系

创建新的S3存储分段时、您可以立即将其备份到对象存储提供程序(可以是StorageGRID系统或Amazon S3部署)上的S3 SnapMirror目标分段。


### 开始之前

- 您拥有对象存储提供程序的有效帐户凭据和配置信息。
- 已在源系统上配置集群间网络接口和 IP 空间。


- 源Storage VM的DNS配置必须能够解析目标的FQDN。



## System Manager

1. 编辑 Storage VM 以添加用户，并将用户添加到组。
  - a. 单击 \* 存储 > Storage VM\*，单击此 Storage VM，单击 \* 设置\*，然后单击  在 \* S3 下。

请参见 "添加 S3 用户和组" 有关详细信息 ...

2. 在源系统上添加云对象存储：
  - a. 单击 \* 保护 > 概述\*，然后选择 \* 云对象存储\*。
  - b. 单击 \* 添加\*，然后选择 \* Amazon S3\* 或 \* StorageGRID\*。
  - c. 输入以下值：
    - 云对象存储名称
    - URL 模式（路径或虚拟托管）
    - Storage VM（为 S3 启用）
    - 对象存储服务器名称（FQDN）
    - 对象存储证书
    - 访问密钥
    - 机密密钥
    - 容器（分段）名称
3. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：
  - a. 单击 \* 保护 > 概述\*，然后单击 \* 本地策略设置\*。
  - b. 单击  在 \* 保护策略\* 旁边，单击 \* 添加\*。
    - 输入策略名称和问题描述。
    - 选择策略范围，集群或 SVM
    - 为 S3 SnapMirror 关系选择 \* 持续\*。
    - 输入 \* 限制\* 和 \* 恢复点目标\* 值。
4. 创建具有 SnapMirror 保护的存储分段：
  - a. 单击 \* 存储 > 分段\*，然后单击 \* 添加\*。
  - b. 输入名称，选择 Storage VM，输入大小，然后单击 \* 更多选项\*。
  - c. 在 \* 权限\* 下，单击 \* 添加\*。验证权限是可选的，但建议这样做。
    - \* 主体\* 和 \* 影响\* —选择与您的用户组设置对应的值或接受默认值。
    - **Actions**-确保显示以下值：

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

- **Results**-使用默认值 `_(bucketname, bucketname/*)` 或您需要的其他值。

请参见 ["管理用户对存储分段的访问权限"](#) 有关这些字段的详细信息，请参见。

- d. 在 \* 保护 \* 下，选中 \* 启用 SnapMirror (ONTAP 或云) \*，选择 \* 云存储 \*，然后选择 \* 云对象存储 \*。

单击 \* 保存 \* 时，将在源 Storage VM 中创建一个新存储分段，并将其备份到云对象存储。

#### 命令行界面

1. 如果这是此 SVM 的第一个 S3 SnapMirror 关系，请验证源和目标 SVM 是否都存在根用户密钥，如果没有，请重新生成这些密钥：

```
vserver object-store-server user show
```

确认是否存在root用户的访问密钥。如果没有，请输入：

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

如果已存在密钥，请勿重新生成该密钥。

2. 在源SVM中创建存储分段：

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. 将访问规则添加到默认分段策略：

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

#### 示例

```
clusterA::> vserver object-store-server bucket policy add-statement -bucket test-bucket -effect allow -action GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal -resource test-bucket, test-bucket /*
```

4. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：

```
snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]
```

#### Parameters

- \* type continuous –S3 SnapMirror关系的唯一策略类型(必需)。
- \* -rpo 指定恢复点目标的时间(以秒为单位)(可选)。
- \* -throttle –指定吞吐量/带宽的上限(以千字节/秒为单位)(可选)。

#### 示例

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

#### 5. 如果目标是StorageGRID系统、请在源集群的管理SVM上安装StorageGRID CA服务器证书:

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

请参见 `security certificate install` 有关详细信息、请参见手册页。

#### 6. 定义S3 SnapMirror目标对象存储:

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server  
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port  
port_number -access-key target_access_key -secret-password  
target_secret_key
```

##### Parameters

- \* `-object-store-name` 本地ONTAP系统上的对象存储目标的名称。
- \* `-usage` 使用 `data`。
- \* `-provider-type` `AWS_S3` 和 `SGWS` (StorageGRID)目标受支持。
- \* `-server` 目标服务器的FQDN或IP地址。
- \* `-is-ssl-enabled` 启用SSL是可选的，但建议使用。

请参见 `snapmirror object-store config create` 有关详细信息、请参见手册页。

#### 示例

```
src_cluster::> snapmirror object-store config create -vserver vs0  
-object-store-name sgws-store -usage data -provider-type SGWS  
-server sgws.example.com -container-name target-test-bucket -is-ssl  
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

#### 7. 创建S3 SnapMirror关系:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination  
-path object_store_name:/objstore -policy policy_name
```

##### Parameters

- \* `-destination-path` 您在上一步中创建的对象存储名称和固定值 `objstore`。

您可以使用创建的策略或接受默认值。

#### 示例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path sgws-store:/objstore -policy test-policy
```

#### 8. 验证镜像是否处于活动状态：

```
snapmirror show -policy-type continuous -fields status
```

为现有存储分段（云目标）创建备份关系

您可以随时开始备份现有的 S3 存储分段；例如，如果从 ONTAP 9.10.1 之前的版本升级了 S3 配置。

开始之前

- 您拥有对象存储提供程序的有效帐户凭据和配置信息。
- 已在源系统上配置集群间网络接口和 IP 空间。
- 源 Storage VM 的 DNS 配置必须能够解析目标的 FQDN 。

## System Manager


### 1. 验证是否已正确定义用户和组：

单击 \* 存储 > Storage VM\* ，单击此 Storage VM ，单击 \* 设置 \* ，然后单击  在 S3 下。

请参见 ["添加 S3 用户和组"](#) 有关详细信息 ...

### 2. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：

a. 单击 \* 保护 > 概述 \* ，然后单击 \* 本地策略设置 \* 。

b. 单击  在 \* 保护策略 \* 旁边，单击 \* 添加 \* 。

c. 输入策略名称和问题描述。

d. 选择策略范围，集群或 SVM

e. 为 S3 SnapMirror 关系选择 \* 持续 \* 。

f. 输入 \* 限制 \* 和 \* 恢复点目标值 \* 。

### 3. 在源系统上添加云对象存储：

a. 单击 \* 保护 > 概述 \* ，然后选择 \* 云对象存储 \* 。


b. 单击 \* 添加 \* ，然后为 StorageGRID Webscale 选择 \* Amazon S3\* 或 \* 其他 \* 。

c. 输入以下值：

- 云对象存储名称
- URL 模式（路径或虚拟托管）
- Storage VM （为 S3 启用）
- 对象存储服务器名称（FQDN）
- 对象存储证书
- 访问密钥
- 机密密钥
- 容器（分段）名称

### 4. 验证现有存储分段的存储分段访问策略是否仍满足您的需求：

a. 单击 \* 存储 \* > \* 分段 \* ，然后选择要保护的分段。

b. 在 \* 权限 \* 选项卡中，单击  \* 编辑 \* ，然后单击 \* 权限 \* 下的 \* 添加 \* 。

▪ \* 主体 \* 和 \* 影响 \* —选择与您的用户组设置对应的值或接受默认值。

▪ **Actions**-确保显示以下值：

GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl,  
ListBucketMultipartUploads, ListMultipartUploadParts

▪ **Results**-使用默认值 (*bucketname*, *bucketname/\**) 或您需要的其他值。

请参见 ["管理用户对存储分段的访问权限"](#) 有关这些字段的详细信息，请参见。

### 5. 使用 S3 SnapMirror 备份存储分段：

a. 单击 \* 存储 \* > \* 分段 \* ，然后选择要备份的分段。

b. 单击 \* 保护 \*，选择 \* 目标 \* 下的 \* 云存储 \*，然后选择 \* 云对象存储 \*。

单击 \* 保存 \* 时，现有存储分段将备份到云对象存储。

#### 命令行界面

1. 验证默认存储分段策略中的访问规则是否正确：

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

#### 示例

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

2. 如果您没有 S3 SnapMirror 策略，并且不想使用默认策略，请创建该策略：

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

#### Parameters

- \* type continuous –S3 SnapMirror关系的唯一策略类型(必需)。
- \* -rpo 指定恢复点目标的时间(以秒为单位)(可选)。
- \* -throttle 指定吞吐量/带宽的上限(以千字节/秒为单位)(可选)。

#### 示例

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

3. 如果目标是StorageGRID系统、请在源集群的管理SVM上安装StorageGRID CA证书：

```
security certificate install -type server-ca -vserver src_admin_svm -cert
-name storage_grid_server_certificate
```

请参见 security certificate install 有关详细信息、请参见手册页。

4. 定义S3 SnapMirror目标对象存储：

```
snapmirror object-store config create -vserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port
port_number -access-key target_access_key -secret-password
target_secret_key
```

#### Parameters

- \* -object-store-name 本地ONTAP系统上的对象存储目标的名称。

- \* `-usage` 使用 `data`。
- \* `-provider-type` `AWS_S3` 和 `SGWS (StorageGRID)` 目标受支持。
- \* `-server` 目标服务器的FQDN或IP地址。
- \* `-is-ssl-enabled` 启用SSL是可选的，但建议使用。

请参见 `snapmirror object-store config create` 有关详细信息、请参见手册页。

示例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

#### 5. 创建S3 SnapMirror关系：

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

##### Parameters

- \* `-destination-path` 您在上一步中创建的对象存储名称和固定值 `objstore`。

您可以使用创建的策略或接受默认值。

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

#### 6. 验证镜像是否处于活动状态：

```
snapmirror show -policy-type continuous -fields status
```

### 从云目标还原存储分段

当源存储分段中的数据丢失或损坏时、您可以通过从目标存储分段还原来重新填充数据。


#### 关于此任务

您可以将目标存储分段还原到现有存储分段或新存储分段。还原操作的目标存储分段必须大于目标存储分段的逻辑已用空间。

如果您使用现有存储分段，则在启动还原操作时，此存储分段必须为空。还原不会 "回滚" 某个存储分段，而是会使用先前的内容填充一个空存储分段。

## System Manager

还原备份数据：

1. 单击 \* 保护 > 关系 \* ，然后选择 \* S3 SnapMirror\* 。
2. 单击  然后选择 \* 还原 \* 。
3. 在 \* 源 \* 下，选择 \* 现有分段 \* （默认值）或 \* 新分段 \* 。
  - 要还原到 \* 现有 Bucket\* （默认值），请完成以下操作：
    - 选择集群和 Storage VM 以搜索现有存储分段。
    - 选择现有存储分段。
    - 复制并粘贴 `_destination_S3` 服务器 CA 证书的内容。
  - 要还原到 \* 新存储分段 \* ，请输入以下值：
    - 用于托管新存储分段的集群和 Storage VM 。
    - 新存储分段的名称，容量和性能服务级别。  
请参见 ["存储服务级别"](#) 有关详细信息 ...
    - 目标 S3 服务器 CA 证书的内容。
4. 在 \* 目标 \* 下，复制并粘贴 *source* S3 服务器 CA 证书的内容。
5. 单击 \* 保护 > 关系 \* 以监控还原进度。

命令行界面操作步骤

1. 创建新的目标存储分段以进行还原。有关详细信息，请参见 ["为存储分段（云目标）创建备份关系"](#)。
2. 为目标存储分段启动还原操作：

```
snapmirror restore -source-path object_store_name:/objstore -destination-path svm_name:/bucket/bucket_name
```

示例

以下示例将目标存储分段还原到现有存储分段。

```
clusterA::> snapmirror restore -source-path sgws.store:/objstore  
-destination-path vs0:/bucket/test-bucket
```


## 修改镜像策略

您可能需要修改 S3 镜像策略；例如，如果要调整 RPO 和限制值。



## System Manager

如果要调整这些值，可以编辑现有保护策略。

1. 单击\*保护>关系\*，然后为要修改的关系选择保护策略。
2. 单击  在策略名称旁边，单击 \* 编辑 \*。

命令行界面

修改S3 SnapMirror策略：

```
snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer]
[-throttle throttle_type] [-comment text]
```

### Parameters

- -rpo 指定恢复点目标的时间(以秒为单位)。
- -throttle 指定吞吐量/带宽的上限(以千字节/秒为单位)。

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

## 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
------	----	----------

<p><u>_SVM 名称 _</u></p> <p>要创建审核配置的 SVM 的名称。</p> <p>SVM 必须已存在并已为 S3 启用。</p>	<p><code>-verserver svm_name</code></p>	<p>是的。</p>
<p><u>日志目标路径 _</u></p> <p>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。</p> <p>路径长度最多可包含 864 个字符，并且必须具有读写权限。</p> <p>如果路径无效，审核配置命令将失败。</p>	<p><code>-destination text</code></p>	<p>是的。</p>
<p><u>要审核的事件的类别 _</u></p> <p>可以审核以下事件类别：</p> <ul style="list-style-type: none"> <li>• 数据 GetObject、PutObject和DeleteObject事件</li> <li>• 管理 PutBucket"和DeleteBucket"事件</li> </ul> <p>默认情况下、仅审核数据事件。</p>	<p><code>-events {data management}, ...</code></p>	<p>否</p>

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
<p><u>日志文件轮换限制 _</u></p> <p>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。</p> <p>值为 0 表示所有日志文件均已保留。默认值为0。</p>	<p><code>-rotate-limit integer</code></p>	<p>否</p>
<p><u>日志文件持续时间限制_</u></p> <p>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。</p> <p>值为 0 表示所有日志文件均已保留。默认值为0。</p>	<p><code>-retention duration integer_time</code></p>	<p>否</p>

#### 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	<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>
计划	<pre>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。</pre>

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	<code>vserver object-store-server audit event-selector modify -vserver <i>svm_name</i> [-bucket <i>bucket_name</i>] [<i>parameters to modify</i>]</code>
SVM 中的所有分段	<code>vserver object-store-server audit modify -vserver <i>svm_name</i> [<i>parameters to modify</i>]</code>

### 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	<code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>
svms	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

#### 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
```

Vserver	Rotation File Size	Rotation Schedule	Rotation 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
```

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。