



# 使用**SnapMirror S3**保护存储分段 ONTAP 9

NetApp  
January 17, 2025

# 目录

使用SnapMirror S3保护存储分段 .....	1
SnapMirror S3概述 .....	1
远程集群上的镜像和备份保护 .....	3
本地集群上的镜像和备份保护 .....	13
利用云目标实现备份保护 .....	24
修改镜像策略 .....	32

# 使用SnapMirror S3保护存储分段

## SnapMirror S3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、SnapMirror S3支持镜像和备份到非NetApp目标、如AWS S3。

SnapMirror S3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>	是的。	是的。
StorageGRID	否	是的。
AWS S3	否	是的。
适用于 Azure 的 Cloud Volumes ONTAP	是的。	是的。
适用于 AWS 的 Cloud Volumes ONTAP	是的。	是的。
适用于 Google Cloud 的 Cloud Volumes ONTAP	是的。	是的。

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。

## SnapMirror S3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

中提供了以下许可证 **"ONTAP One"** ONTAP源系统和目标系统上需要使用软件套件才能访问：

- ONTAP S3协议和存储
- SnapMirror S3以其他NetApp对象存储目标(ONTAP S3、StorageGRID和Cloud Volumes ONTAP)为目标
- SnapMirror S3以目标第三方对象存储为目标，包括AWS S3 (可在中找到**"ONTAP One兼容包"**)

- 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(对于远程ONTAP目标)、并且源集群和目标集群的集群间LUN可以连接到源和目标S3服务器数据LUN。
  - 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SnapMirror S3关系都需要使用特定于S3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）。



请注意、如果SnapMirror关系中有两个S3存储分段、并且配置了生命周期策略、使对象的当前版本过期(即被删除)、则同一操作会复制到配对存储分段。即使配对存储分段为只读或被动存储、也是如此。

- root用户密钥SnapMirror S3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SnapMirror S3关系时、您必须验证这些密钥是否同时位于源Storage VM和目标Storage VM上、如果不存在、则重新生成它们。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ONTAP 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

SnapMirror S3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"](#)。

SnapMirror S3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)。SnapMirror S3可以支持将多个存储分段镜像从多个集群镜像到一个二级集群、但每个源存储分段必须在二级集群上具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SnapMirror S3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SnapMirror S3关系、请验证源Storage VM和目标Storage VM是否都存在root用户密钥、如果它们未执行以下操作、请重新生成它们：
  - a. 单击 \* 存储 > 存储 VM\* ，然后选择此 Storage VM 。
  - b. 在\*Settings\*选项卡中，单击  \*S3\*磁贴。
  - 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\*root\*旁边的，  然后单击\*Regerate Key\*。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Storage VM、单击\*设置\*、然后单击  S3下的。

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SnapMirror S3策略、并且不想使用默认策略、请创建此策略：

- a. 单击 \* 保护 > 概述 \* ，然后单击 \* 本地策略设置 \* 。
- b. 单击  **Protection Policies**\*旁边的，然后单击\*Add\*。

- 输入策略名称和问题描述。
- 选择策略范围，集群或 SVM
- 为SnapMirror S3关系选择\*连续\*。
- 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 *sourc* 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SnapMirror S3关系、请验证源和目标SVM是否都存在root用户密钥、如果不存在、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::> 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. 如果您没有SnapMirror S3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 -vsserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

### Parameters

- `type continuous`—SnapMirror S3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 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 -vsserver src_admin_svm  
-cert-name dest_server_certificate
```

- b. 在目标集群上、安装对`_ssource_` 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SnapMirror S3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SnapMirror S3关系、请验证源Storage VM和目标Storage VM是否都存在root用户密钥、如果它们未执行以下操作、请重新生成它们：
  - a. 选择\*存储> Storage VM\*、然后选择Storage VM。
  - b. 在\*Settings\*选项卡中，单击  \*S3\*磁贴。
  - 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\*root\*旁边的，  然后单击\*Regerate Key.\*如果已存在密钥，请勿重新生成该密钥。
2. 验证现有用户和组是否存在、以及是否具有源和目标Storage VM中的正确访问权限：选择\*存储> Storage VMs\*、\*然后选择Storage VM\*、再选择\*设置\*选项卡。最后，找到\*S3\*磁贴，选择  ，然后依次选择\*USERS\*选项卡和\*Groups\*选项卡以查看用户和组访问设置。

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SnapMirror S3策略、并且不想使用默认策略、请创建此策略：
  - a. 选择\*保护>概述\*，然后单击\*本地策略设置\*。
  - b. 选择  保护策略\*旁边的，然后单击\*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SnapMirror S3关系选择\*连续\*。
  - 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SnapMirror S3保护功能保护现有存储分段：
  - 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SnapMirror S3关系、请验证源和目标SVM是否存在root用户密钥、如果没有、  
`vserver object-store-server user show``请重新生成这些密钥: +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::> 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SnapMirror S3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 -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parameters

- continuous—SnapMirror S3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 -vserver 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 -vserver 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SnapMirror S3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分段、而原始目标存储分段将转换为读写存储分段、从而反转 SnapMirror S3 关系。

当禁用的源存储分段再次可用时、SnapMirror S3 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\* SnapMirror S3\*。
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\* SnapMirror S3\*。
2. 单击 ，然后选择\*Restore\*。
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SnapMirror S3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SnapMirror S3关系、请验证源Storage VM和目标Storage VM是否都存在root用户密钥、如果它们未执行以下操作、请重新生成它们：
  - a. 单击 \* 存储 > 存储 VM\* ，然后选择此 Storage VM 。
  - b. 在\*Settings\*选项卡中，单击  S3磁贴。
  - 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\*root\*旁边的，  然后单击\*Regerate Key\*。如果已存在密钥，请勿重新生成该密钥。
2. 编辑源和目标Storage VM中的Storage VM以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S3。 

请参见 ["添加 S3 用户和组"](#) 有关详细信息 ...

3. 如果您没有SnapMirror S3策略、并且不想使用默认策略、请创建此策略：
  - a. 单击\*Protection > Overview\*，然后单击\*Local Policy Settings\*。
  - b. 单击  **Protection Policies**\*旁边的，然后单击\*Add\*。
    - 输入策略名称和问题描述。
    - 选择策略范围，集群或 SVM
    - 为SnapMirror S3关系选择\*连续\*。
    - 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**\*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SnapMirror S3关系、请验证源和目标SVM是否都存在root用户密钥、如果不存在、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,GetObjectAcl,  
ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. 如果您没有SnapMirror S3策略、并且不想使用默认策略、请创建此策略：

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

#### Parameters

- continuous—SnapMirror S3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SnapMirror S3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SnapMirror S3关系、请验证源Storage VM和目标Storage VM是否都存在root用户密钥、如果它们未执行以下操作、请重新生成它们：
  - a. 单击 \* 存储 > 存储 VM\* ，然后选择此 Storage VM 。
  - b. 在\*Settings\*选项卡中，单击  \*S3\*磁贴。
  - 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\*root\*旁边的，  然后单击\*Regerate Key\*。如果已存在密钥，请勿重新生成该密钥
2. 验证现有用户和组是否存在、以及是否具有源和目标Storage VM中的正确访问权限：选择\*存储> Storage VMs、\*然后选择Storage VM、最后选择\*设置\*选项卡。最后，找到\*S3\*磁贴，选择  ，然后依次选择\*USERS\*选项卡和\*Groups\*选项卡以查看用户和组访问设置。

请参见 ["添加 S3 用户和组"](#) 有关详细信息 ...

3. 如果您没有SnapMirror S3策略、并且不想使用默认策略、请创建此策略：
  - a. 单击 \* 保护 > 概述 \* ，然后单击 \* 本地策略设置 \* 。
  - b. 单击  **Protection Policies**\*旁边的，然后单击\*Add。
    - 输入策略名称和问题描述。
    - 选择策略范围，集群或 SVM
    - 为SnapMirror S3关系选择\*连续\*。
    - 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SnapMirror S3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SnapMirror S3关系、请验证源和目标SVM是否都存在root用户密钥、如果不存在、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::> 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SnapMirror S3策略、并且不想使用默认策略、请创建此策略：

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

#### Parameters

- continuous—SnapMirror S3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. 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SnapMirror S3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分段、而原始目标存储分段将转换为读写存储分段、从而反转 SnapMirror S3 关系。

当禁用的源存储分段再次可用时、SnapMirror S3 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\* SnapMirror S3\*。
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\*Restore\*。
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对云目标进行SnapMirror S3备份保护的要求。

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。

在集群可以连接到云对象存储之前，应在集群上配置集群间的CIFS和IP空间。您应在每个节点上创建集群间L，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 `security certificate install command` 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。有关详细信息，请参见["安装 CA 证书" If you use 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SnapMirror S3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Storage VM，单击\*设置\*，然后单击\*S3\*  下的。

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SnapMirror S3策略、并且不想使用默认策略、请创建此策略：
  - a. 单击 \* 保护 > 概述 \*，然后单击 \* 本地策略设置 \*。
  - b. 单击  **Protection Policies**\*旁边的，然后单击\*Add。
    - 输入策略名称和问题描述。
    - 选择策略范围，集群或 SVM
    - 为SnapMirror S3关系选择\*连续\*。
    - 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SnapMirror S3关系、请验证源和目标SVM是否都存在root用户密钥、如果不存在、

`vserver object-store-server user show``请重新生成这些密钥：+确认root用户是否有访问密钥。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SnapMirror S3策略、并且不想使用默认策略、请创建此策略：

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

参数：\* type continuous—SnapMirror S3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SnapMirror S3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SnapMirror S3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\*、单击存储VM、单击\*设置\*、然后单击S3下的。

请参见 ["添加 S3 用户和组"](#) 有关详细信息 ...


2. 如果您没有SnapMirror S3策略、并且不想使用默认策略、请创建此策略：

- a. 单击 \* 保护 > 概述 \* ，然后单击 \* 本地策略设置 \* 。
- b. 单击  **Protection Policies**\*旁边的，然后单击\*Add。
- 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SnapMirror S3关系选择\*连续\*。
- 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SnapMirror S3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SnapMirror S3策略、并且不想使用默认策略、请创建此策略：

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

参数：\* type continuous—SnapMirror S3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SnapMirror S3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SnapMirror S3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-ebp
-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\* SnapMirror S3\*。
2. 单击 ，然后选择\*Restore\*。
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  策略名称旁边的，然后单击\*Edit\*。

命令行界面

修改SnapMirror S3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
```

## 版权信息

版权所有 © 2025 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。