



# 向启用了 **S3** 的 **SVM** 添加存储容量

## ONTAP 9

NetApp  
February 12, 2026

# 目录

向启用了 S3 的 SVM 添加存储容量 .....	1
创建ONTAP S3存储分段 .....	1
使用ONTAP命令行界面创建S3存储分段 .....	2
使用System Manager创建S3存储分段 .....	3
增加或减少ONTAP S3存储分段大小 .....	4
在MetroCluster配置中的镜像或未镜像聚合上创建ONTAP S3存储分段 .....	5
创建存储分段的过程 .....	5
创建ONTAP S3存储分段生命周期管理规则 .....	9
使用命令行界面管理生命周期管理规则 .....	10
使用System Manager管理生命周期管理规则 .....	11
创建ONTAP S3用户 .....	13
创建或修改ONTAP S3用户组以控制对分段的访问 .....	14
重新生成ONTAP S3密钥并修改其保留期限 .....	15

# 向启用了 S3 的 SVM 添加存储容量

## 创建ONTAP S3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、则需要和数据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：

有关的详细信息 `vserver object-store-server bucket modify`，请参见"[ONTAP 命令参考](#)"。

\*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：

有关此过程中所述命令的更多信息，请参见["ONTAP 命令参考"](#)。

```
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。

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。

- 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。

如果对分段启用了版本控制、则可以使用S3客户端将对象锁定保留时间放置在特定版本的对象上。锁定对象的特定版本不会阻止删除对象的其他版本。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。创建分段时、必须启用S3对象锁定。无法对已有分段启用对象锁定。对象锁定只能在本机S3用例中使用。配置为使用S3协议的多协议NAS卷应使用SnapLock将数据提交到WORM存储。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。虽然目前并不需要，但现有客户可以选择["升级到ONTAP One"](#)。如果您在存储桶上启用对象锁定，您应该["验证是否已安装SnapLock许可证"](#)。如果未安装SnapLock许可证，则必须["安装"](#)启用对象锁定之前，请先执行此操作。

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。

## 增加或减少ONTAP S3存储分段大小

必要时、您可以增加或减小现有存储分段的大小。

### 步骤

您可以使用System Manager或ONTAP命令行界面管理存储分段大小。

## System Manager

1. 选择\*存储>存储分段\*并找到要修改的存储分段。
2. 单击  存储分段名称旁边的，然后选择\*Edit\*。
3. 在\*编辑存储分段\*窗口中，更改存储分段的容量。
4. 保存。

### 命令行界面

1. 更改铲斗容量：

```
vserver object-store-server bucket modify -vserver <SVM_name>  
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

## 在MetroCluster配置中的镜像或未镜像聚合上创建ONTAP S3存储分段

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：
  - SnapMirror S3
  - 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)

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

CAPACITY  
 Size

Use for 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

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 S3 protection.

- 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、输入以下内容以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ONTAP S3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 ...
- 在多协议NAS卷中使用S3或在MetroCluster配置中使用S3时、不支持存储分段生命周期管理规则。

### 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`。



非当前版本取决于当前版本的创建或修改时间。如果意外删除或覆盖对象、则延迟删除非当前对象会很有用。例如、您可以将到期规则配置为在非当前版本变为非当前版本五天后将其删除。例如、假设在2014年1月1日上午10:30 UTC、您创建了一个名为(version ID 111111)的对象 `photo.gif`。在2014年1月2日上午11:30 UTC、您意外删除了 `photo.gif`(版本ID 111111)、这将使用新的版本ID (如版本ID)创建一个删除标记 4857693。在删除操作永久化之前、您现在有五天时间恢复的原始版本 `photo.gif`(版本ID 111111)。2014年1月8日00:00 UTC、生命周期到期规则将在其成为非最新版本五天后运行并永久删除 `photo.gif`(版本ID 111111)。

- 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：指定删除非当前版本之前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ONTAP S3用户

创建具有特定权限的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。

为了增强安全性、从ONTAP 9.15.1开始、访问密钥和机密密钥仅在创建S3用户时显示、不能再次显示。如果密钥丢失，"[必须重新生成新密钥](#)"。

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S3下的。 
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ONTAP S3用户组以控制对分段的访问

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Storage VM、单击\*设置\*、然后单击  S3下的。
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ONTAP S3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](#)"。

## System Manager

1. 单击 \* 存储 > 存储 VM\* ，然后选择此 Storage VM 。
2. 在\*Settings\*选项卡中，单击  \*S3\*磁贴。
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  用户旁边的，然后单击\*Regenerate Key\*。
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。

### 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。

## 版权信息

版权所有 © 2026 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。