配置
ONTAP 9

NetApp
April 29, 2024

目录

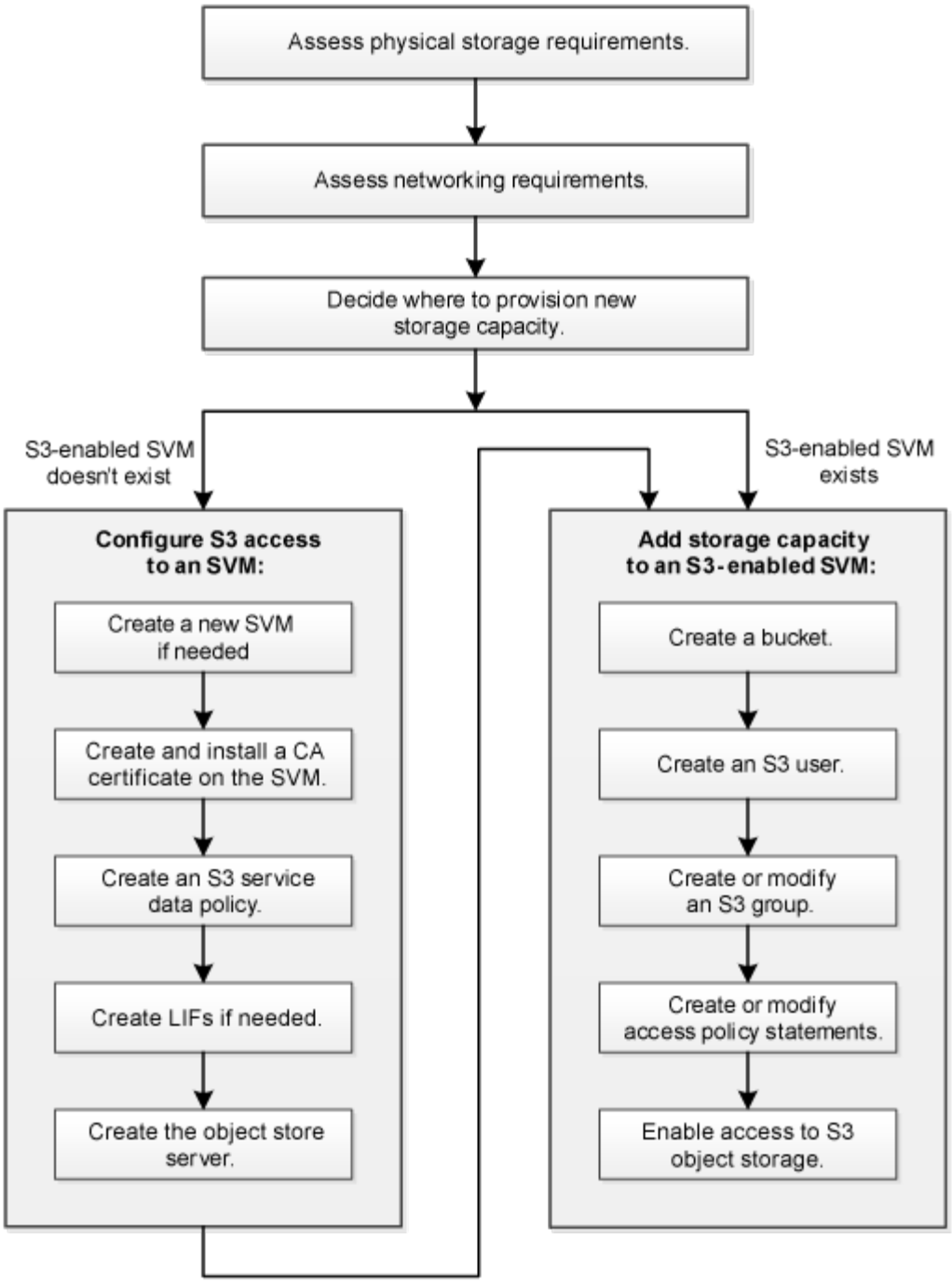
配置

关于 S3 配置过程

S3 配置工作流

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。



评估物理存储要求

在为客户端配置 S3 存储之前，您必须确保现有聚合中有足够的空间用于新对象存储。如果没有、您可以向现有聚合添加磁盘、或者创建所需类型和位置的新聚合。

关于此任务

在启用了 S3 的 SVM 中创建 S3 存储分段时，系统会自动创建一个 FlexGroup 卷来支持存储分段。您可以让 ONTAP Select 自动对底层聚合和 FlexGroup 组件执行 FlexGroup （默认设置），也可以自行选择底层聚合和组件。

如果您决定指定聚合和 FlexGroup 组件，例如，如果您对底层磁盘有特定的性能要求，则应确保聚合配置符合

配置 FlexGroup 卷的最佳实践准则。了解更多信息。

- "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 `false` 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的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

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            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
node-2
            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
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
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
                                                                     Speed
   (Mbps)
   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
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
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
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          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。

示例 **2.** 步骤

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。
   a. 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。
   b. 单击 * 启用 S3* ，然后输入 S3 服务器名称。
   c. 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::> vserver 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: svm1_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
svm1.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 M众多(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

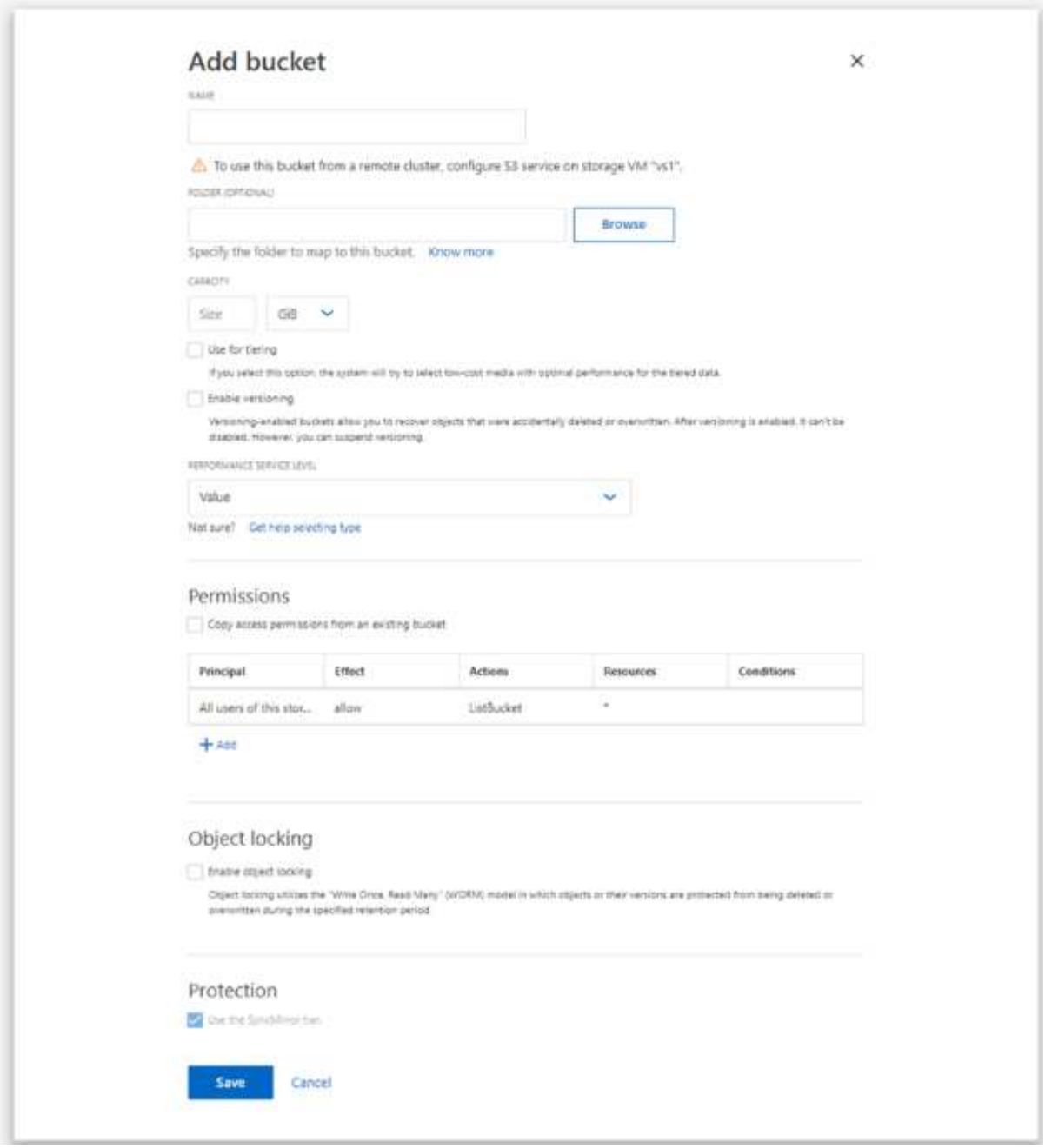
以下示例将在镜像聚合上为SVM VS1创建大小为1 TB的分段：

```
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：



- 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	• `-non-curr-days` -删除非当前版本之前的天数 • `-new-non-curr-versions` -要保留的最新非最新版本的数量
到期日期	• `-obj-age-days` -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 • `-obj-exp-date` -对象应过期的特定日期 • `-expired-obj-del-markers` -清理对象删除标记
AbortIncompleteMultipartUpload	• `-after-initiation-days` -启动的天数，超过此天数后可以中止上传

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鞑*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。 • 最多可以指定 10 个用户或组。 • 如果指定了S3组、则必须采用的格式 `group/group_name`. • `*` 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。 • 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。

-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::> vserver 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::> vserver 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

-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, ListAllMyBuckets, ListBucketMultipartUploads, 和 ListMultipartUploadParts。
-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。

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
NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=

> 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
   -ipspace 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
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