Lenovo

使用 DM 系列硬件创建本地云基础结构

ONTAP® 9

第一版 (2022 年 1 月)

目录

第 1 章　决定是否要使用本指南

本指南介绍如何使用 Lenovo 存储管理软件来配置 S3 客户端对 SVM 中存储桶包含的对象的访问权限。其中包括示例和高级配置选项。

如果要按照下面的方法配置 S3 对象存储，应使用本指南：

- 希望从其他 DM 系列系统使用 ONTAP S3 提供 S3 对象存储。

  如果您希望在现有集群上使用 S3 功能而无需其他硬件和管理，则适合部署 ONTAP。
- 希望使用 ThinkSystem DM 系列存储管理软件，而不想使用 ONTAP 命令行界面或自动脚本工具。

  注：如果您希望能够指定将哪些聚合用于存储桶，则只能使用 CLI 来实现此目的。
- 希望使用最佳实践，而不是探索每种可用选项。

  CLI 帮助和 ONTAP 手册页提供有关命令语法的详细信息。
- 不希望阅读大量概念性背景知识。

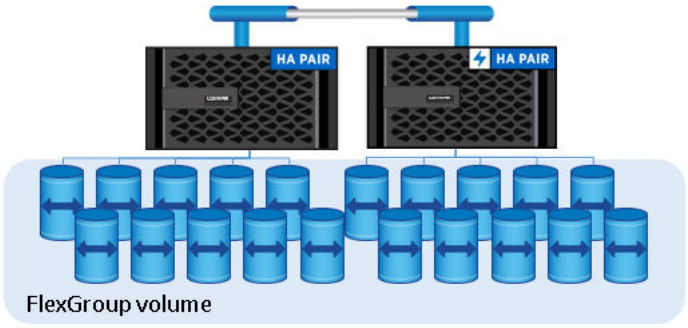
  Lenovo ThinkSystem 存储信息中心提供了有关 ONTAP 技术和与外部服务交互相关的其他信息。
- 拥有集群管理员权限，而不是 SVM 管理员权限。

如果本指南不适合您的情况，应改为参阅以下文档：

- ONTAP 命令行界面

第 2 章　关于 ONTAP 9 中的 S3 支持

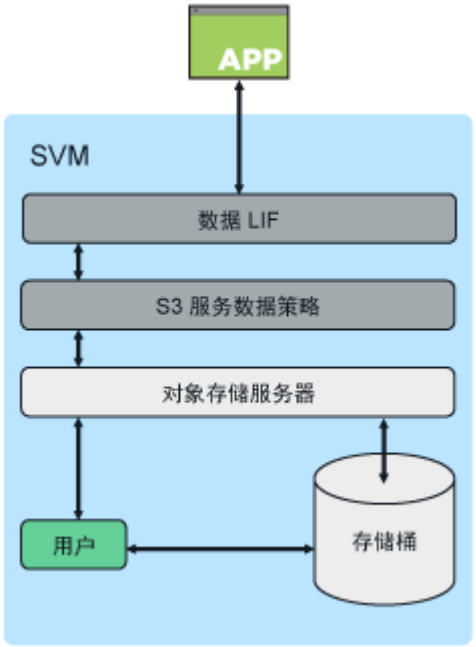
在 **ONTAP** 中，存储桶的底层架构是 **FlexGroup** 卷：这是由多个成分卷组成但作为单个卷进行管理的单个名称空间。



存储桶仅受限于底层硬件的物理最大值，架构最大值可能更高。如果存储空间不足，存储桶可以利用 **FlexGroup** 弹性大小调整功能来自动增大 **FlexGroup** 卷的成分卷。限制为每个 **FlexGroup** 卷为 **1000** 个存储桶，或 **FlexGroup** 卷容量的 **1/3**（旨在适应存储桶中的数据增长）。

注：不允许通过 **NAS** 或 **SAN** 协议访问包含托管在辅助 **DM** 系列系统上的 **S3** 存储桶的 **FlexGroup** 卷。

通过授权的用户和客户端应用程序可以访问存储桶。



客户端访问 **ONTAP S3** 服务有三种主要用例：

- 用于使用 **ONTAP S3** 作为远程 **FabricPool** 容量（云）层的 **ONTAP** 系统
  包含容量层（用于*冷*数据）的 **S3** 服务器和存储桶与性能层（用于*热*数据）位于不同集群。

- 用于使用 **ONTAP S3** 作为本地 **FabricPool** 层的 **ONTAP** 系统

  包含容量层的 **S3** 服务器和存储桶与性能层位于同一集群，但位于不同的 **HA** 对中。
- 用于外部 **S3** 客户端应用程序

  ONTAP S3 服务于在非 **Lenovo** 系统上运行的 **S3** 客户端应用程序。

我们将重点介绍对于我们的主系统用作远程 **FabricPool**（云）层的 **ONTAP S3**。

最好是使用 **HTTPS** 提供对 **ONTAP S3** 存储桶的访问。启用 **HTTPS** 后，需要安全证书才能与 **SSL/TLS** 正确集成。然后，还需要客户端用户的访问权限和机密密钥，以便向 **ONTAP S3** 进行用户认证，并授予用户的访问权限以进行 **ONTAP S3** 中的操作。客户端应用程序还应该有权访问根 **CA** 证书（**ONTAP S3** 服务器的签名证书），以便能够认证服务器并在客户端和服务器之间建立安全连接。

在辅助系统上已启用 **S3** 的 **SVM** 中创建用户，并可在存储桶或 **SVM** 级别控制这些用户的访问权限，也就是可允许用户访问 **SVM** 中的一个或多个存储桶。

默认情况下会在 **ONTAP S3** 服务器上启用 **HTTPS**。可以禁用 **HTTPS** 并为客户端访问启用 **HTTP**，在这种情况下，不需要使用 **CA** 证书进行认证。但是，当启用 **HTTP** 而禁用 **HTTPS** 时，与 **ONTAP S3** 服务器的所有通信均通过网络以明文形式发送。

本文档中将不会介绍此方法。

S3 对象存储的 ONTAP 版本支持

我们将在本指南中重点介绍 **ONTAP 9.10.1**，因为它具有用于管理辅助系统存储桶的扩展选项。

ONTAP S3 限制

托管 **S3** 对象存储的 **SVM** 不支持某些标准的 **ONTAP** 功能，包括：

不支持的 **ONTAP** 功能：

- **Cloud Volumes ONTAP**
- **FlexCache** 卷
- **MetroCluster**
- **NDMP**
- **SnapMirror Cloud**
- **SMTape**
- 包含 **ONTAP S3** 存储桶的 **Flexgroup** 的卷克隆

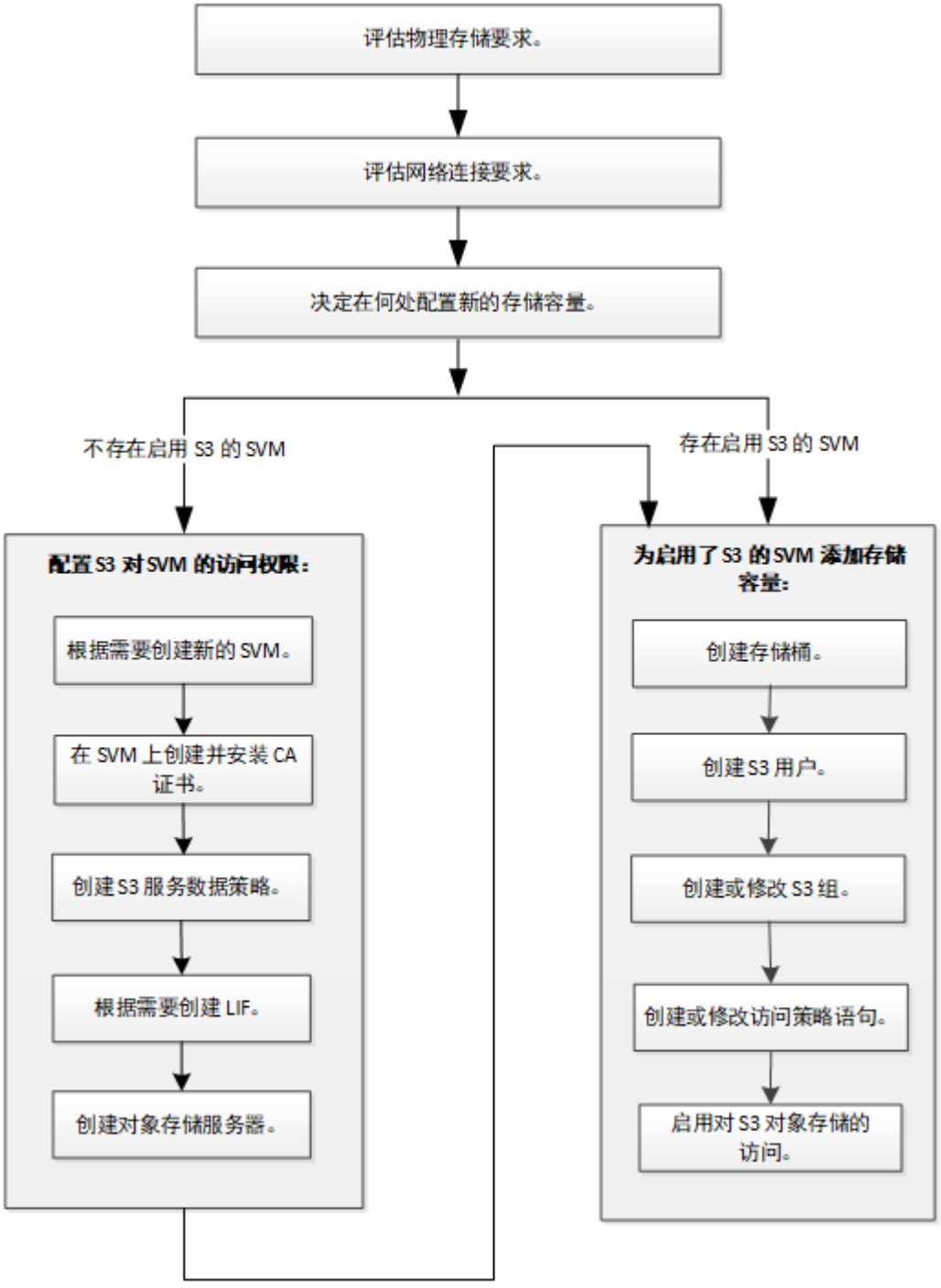
  注： 在 **ONTAP 9.10.1** 中，可使用 **SnapMirror** 为 **S3** 存储桶进行灾难恢复，但我们在本指南中不讨论此主题。

不支持的对象存储功能：

- 对象版本控制
- 擦除编码

第 3 章　S3 配置工作流程

要配置 **S3**，需要评估物理存储和网络连接要求，然后根据您的具体目标为新的 **SVM** 或现有 **SVM** 配置 **S3** 访问权限，或在已完全配置 **S3** 访问权限的现有 **SVM** 上添加存储桶和用户。



评估物理存储要求

在为客户端配置 S3 存储之前，必须确保现有聚合中为新对象存储提供了足够的空间。如果空间不足，可在现有聚合中添加磁盘，或创建所需类型的新聚合。

关于本任务

在已启用 S3 的 SVM 中创建 S3 存储桶时，将自动创建 FlexGroup 卷以支持该存储桶。您可以让 ONTAP 自动选择底层聚合和 FlexGroup 组件（默认设置），您也可以自己选择底层聚合和 FlexGroup 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关于配置 FlexGroup 卷的最佳实践准则。

FlexGroup 卷管理

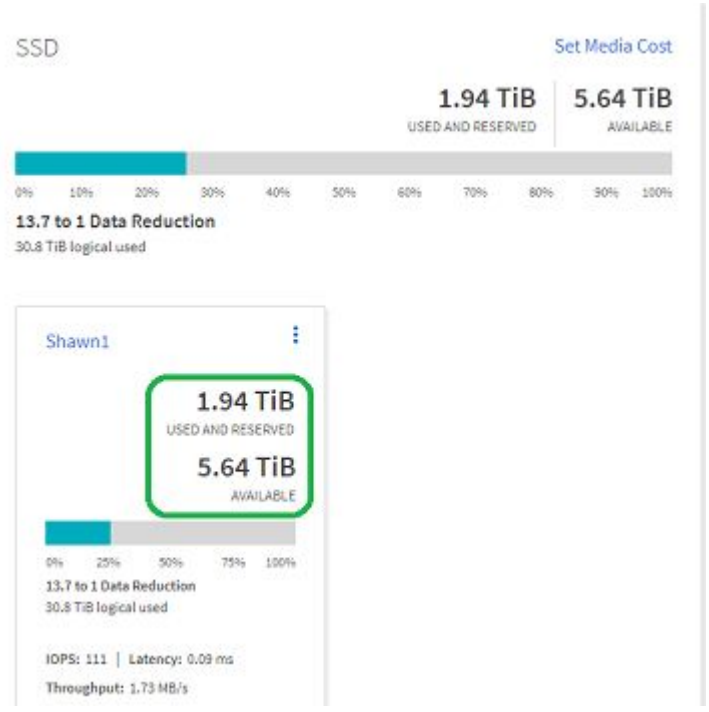
您可以使用 ONTAP S3 服务器创建本地 FabricPool 容量层；也就是说，该层与性能层位于同一集群中。例如，当您在一个 HA 对上连接了固态硬盘，同时希望将*冷*数据分层到另一个 HA 对中的硬盘时，就可以采用这种方法。因此，在此用例中，S3 服务器和包含本地容量层的存储桶应位于与性能层不同的 HA 对中。双节点集群不支持本地分层。在本指南中不会介绍这种启用 ONTAP S3 的模式。

过程

步骤 1. 打开 DM 系列 System Manager，并转到 Storage（存储） → Tiers（层）。

如果某一聚合具有足够空间，请为您的 S3 配置记录该聚合的名称。

示例



步骤 2. 如果任何聚合都没有足够的空间，请添加新聚合，其中要将驱动器添加到系统，然后选择 Storage（存储） → Tiers（层） → +Add Local tier（+添加本地层）。

评估网络连接要求

向客户端提供 S3 存储之前，必须验证已正确配置网络连接，可以满足 S3 配置要求。

开始之前

必须配置以下集群网络连接对象：

- 物理和逻辑端口
- 广播域
- 子网（如有必要）
- IPspace（除默认 IPspace 之外，根据需要进行配置）
- 故障转移组（除了每个广播域的默认故障转移组之外，根据需要进行配置）
- 外部防火墙

关于本任务

我们将使用本地 FabricPool（云）层。为此，还必须配置集群间 LIF；但不需要配置集群对等。

对于本地 FabricPool 容量层，您必须使用系统 SVM（称为“集群”），而我们将使用数据和集群间 LIF。此选项要求进行其他配置（包括为 S3 协议启用 LIF），但是本地层也将可作为远程 FabricPool 云层供其他集群访问。

过程

步骤 1. 使用 DM 系列 System Manager 显示可用的物理和虚拟端口：Network（网络） → Ethernet Ports（以太网端口）

- 数据网络应尽可能使用具有最高速度的端口。
- 数据网络中的所有组件必须具有相同的 MTU 设置，以达到最佳性能。

步骤 2. 确定每个网络端口可使用的广播域：转到 DM 系列存储管理软件，然后选择 Network（网络） → Overview（概述） → Broadcast Domains（广播域）。

随后将根据每个网络端口所在的广播域列出该端口。

步骤 3. 显示可用的 IPspace：转到 DM 系列存储管理软件，然后选择 Network（网络） → Overview（概述） → IPspaces。

可使用默认 IPspace 或自定义 IPspace。

决定在何处配置新的 S3 存储容量

在创建新的 S3 存储桶之前，必须决定将其放置在新的还是现有的 SVM 中。此决策将决定工作流程。

如果想在新的 SVM 或未启用 S3 的 SVM 中配置存储桶，请完成以下主题中的步骤。

第 9 页第 4 章 “为 SVM 配置 S3 访问权限”

第 15 页第 5 章 “为已启用 S3 的 SVM 添加存储容量”

尽管 S3 能够在 SVM 中与 NFS 和 SMB/CIFS 共存，但如果满足以下条件之一，您可以选择创建一个新的 SVM：

– 首次在集群上启用 S3。
– 您希望不为集群中的现有 SVM 启用 S3 支持。

– 在集群中有一个或多个已启用 S3 的 SVM，并且您需要另一个具有不同性能特征的 S3 服务器。

在 SVM 上启用 S3 后，请继续配置存储桶。
如果要在已启用 S3 的现有 SVM 上配置初始存储桶或额外的存储桶，请完成以下主题中的步骤。

第 15 页第 5 章 “为已启用 S3 的 SVM 添加存储容量”

第 4 章　为 SVM 配置 S3 访问权限

配置 **S3** 涉及创建新 **SVM** 或在现有 **SVM** 上启用 **S3**，然后创建 **S3** 服务策略、专用的数据 **LIF** 和 **S3** 服务器。

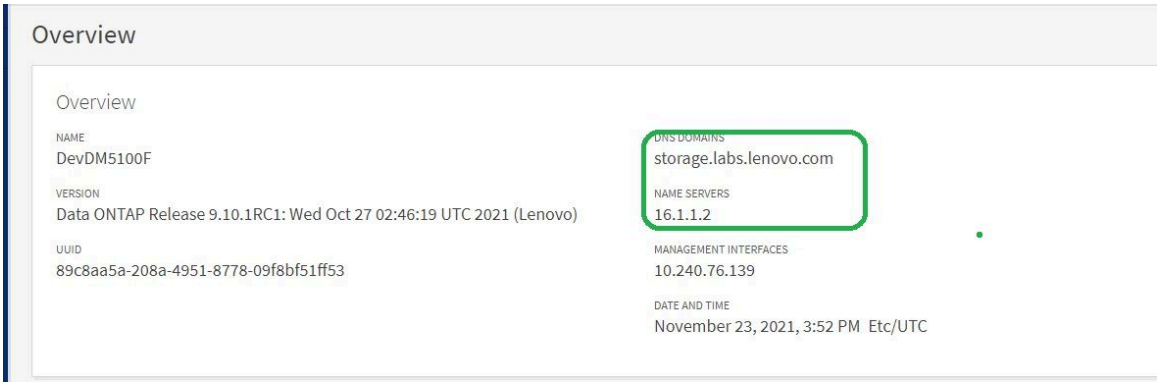
创建 S3 SVM 和服务器

尽管 **S3** 可在 **SVM** 中与其他 **NAS** 协议共存，但您可以创建一个新的 **SVM** 来隔离名称空间和工作负载。

关于本任务

我们的示例将使用专用的 **S3 SVM**。

应首先确保已经为本地和远程 **DM** 系列系统配置了 **DNS**。转到 **DM** 系列存储管理软件，然后选择 **Cluster（集群）** ➙ **Overview（概述）**。

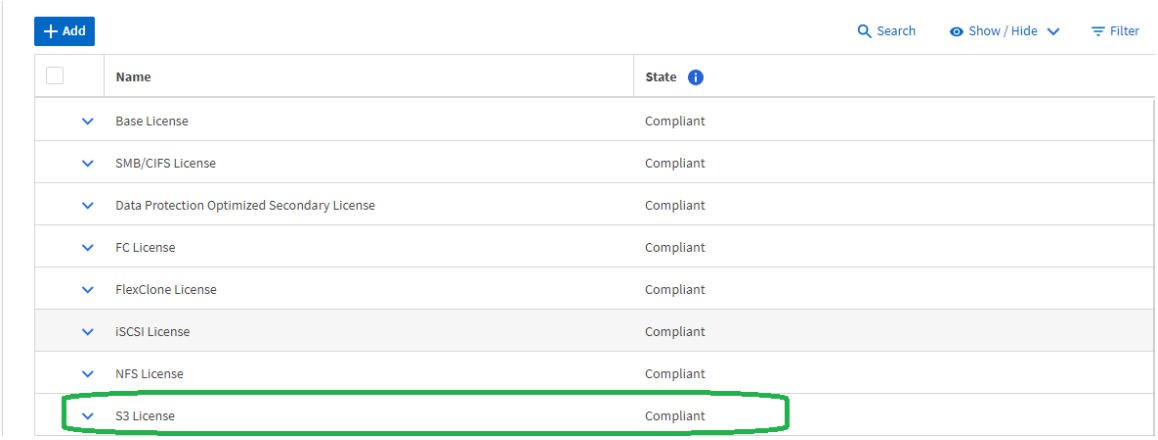


要添加 **DNS** 域，请在 **DNS DOMAINS（DNS 域）**下单击 **More（更多）**，然后选择 **Edit（编辑）** ➙ **+Add（+添加）**。

要添加名称服务器，请在 **NAME SERVERS（名称服务器）**下单击 **More（更多）**，然后选择 **Edit（编辑）** ➙ **+Add（+添加）**。

过程

步骤 **1.** 确认已在集群上许可了 **S3**：转到 **DM** 系列存储管理软件，然后选择 **Cluster（集群）** ➙ **Settings（设置）** ➙ **License（许可）**



步骤 2. 创建启用了 S3 的 SVM。

a. 转到 DM 系列存储管理软件，然后选择 Storage（存储） → Storage VMs（存储虚拟机）。

b. 选择 +Add（+添加）以创建新 SVM。

c. 为该新 SVM 选择一个名称。

d. 在数据协议部分选择 Enable S3（启用 S3），然后提供 S3 服务器名称。

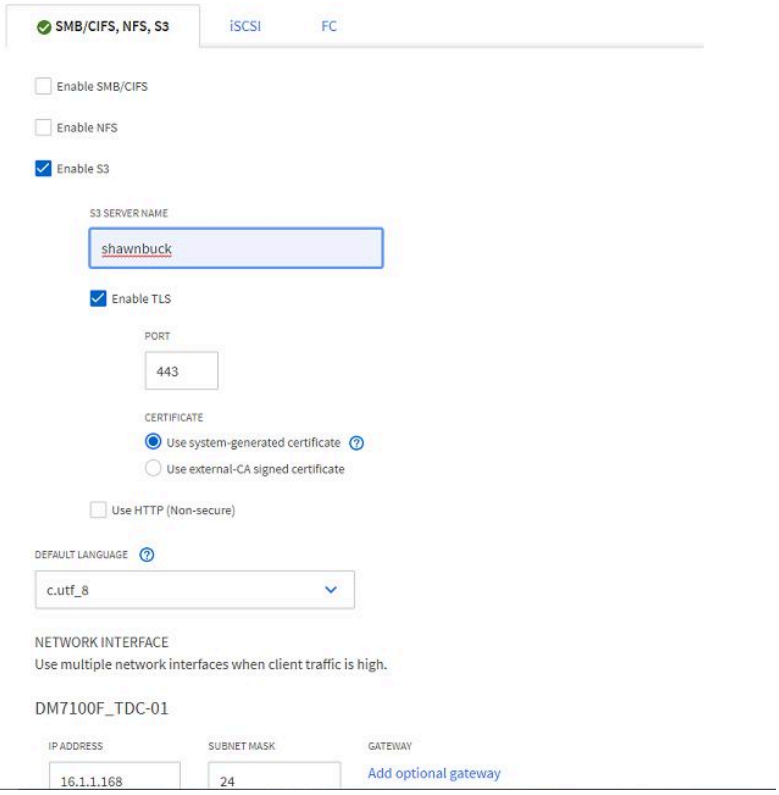
注：这是您以后将用于连接到存储桶的名称。

e. 确认选中了 Enable TLS（启用 TLS）并列出了所使用的端口。

f. 选择要使用外部证书还是由系统/ONTAP 生成的证书。

g. 提供要用于此 S3 SVM 的新数据 LIF 的 IP 地址。

h. 单击 Save（保存）。

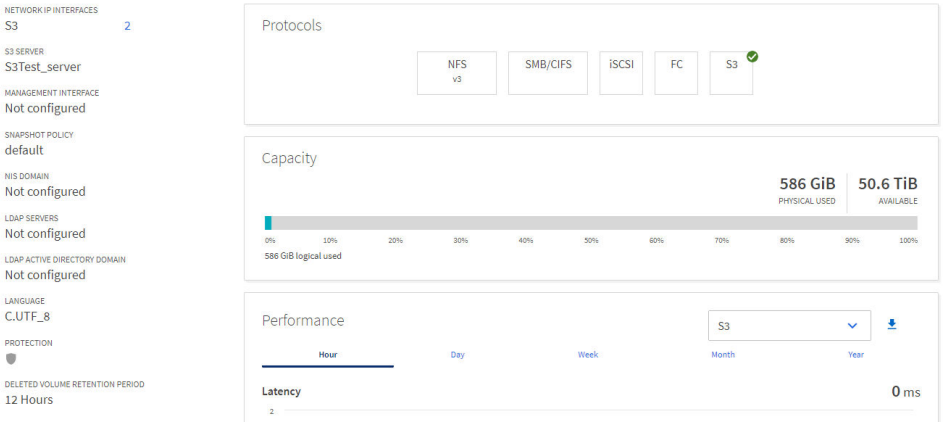


步骤 3. 验证新创建的 SVM 的配置和状态：

a. 转到 DM 系列存储管理软件，然后选择 Storage（存储） → Storage VMs（存储虚拟机）。

b. 通过单击已创建的 SVM 的名称将其选中。

c. 确认启用了相关协议并创建了所需接口。



验证证书颁发机构

ONTAP 9.10.1 中新增的最重要的功能之一就是支持使用 **DM** 系列 **System Manager** 来创建托管存储桶的新 **S3 SVM**。其中包括创建证书颁发机构。

过程

步骤 1. 确认创建了所选的证书：

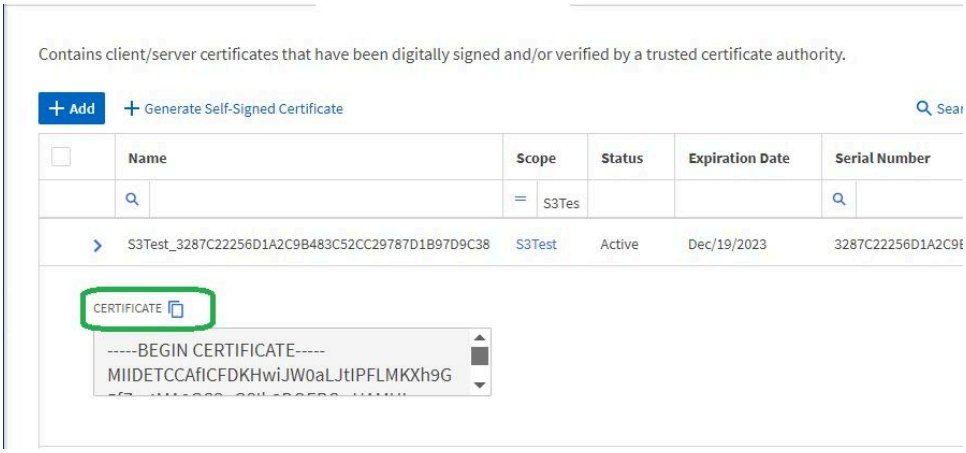
a. 转到 DM 系列存储管理软件，然后选择 Storage（存储） → Storage VMs（存储虚拟机）。

b. 单击所创建的 S3 存储虚拟机。

c. 选择 Settings（设置）。

d. 选择 Security（安全） → Certificates（证书）。

e. 选择“Client/Server Certificates（客户端/服务器证书）”选项卡。
随后将显示分配给您的 S3 SVM 的证书。



创建 S3 服务数据策略

可为 **S3** 数据和管理服务创建服务策略。必须通过 **S3** 服务数据策略才能在 **LIF** 上启用 **S3** 数据流量。

关于本任务

如果使用数据 **LIF** 和集群间 **LIF**，则需要 **S3** 服务数据策略。如果将集群 **LIF** 用于本地分层用例，则不需要此策略。

如果为 **LIF** 指定了服务策略，将使用该策略为这个 **LIF** 构造默认角色、故障转移策略和数据协议列表。

尽管可以为 **SVM** 和 **LIF** 配置多种协议，但最好是仅使用 **S3** 作为提供对象数据时的唯一协议。

过程

步骤 **1.** 将权限设置更改为高级：
```
set -privilege advanced
```
步骤 **2.** 创建一个服务数据策略：
```
network interface service-policy create -vserver svm_name -policy policy_name -services
data-s3-server
```
data-s3-server 服务策略是启用 **S3** 服务时所需的唯一策略，但可以根据需要包含其他服务策略。

验证数据 LIF

如果创建了新的 **SVM**，则为 **S3** 访问创建的专用 **LIF** 应该是数据 **LIF**。

开始之前

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

  子网中包含属于同一第 **3** 层子网的一组 **IP** 地址。它们是使用 `network subnet create` 命令创建的。
- **LIF** 服务策略必须已存在。

关于本任务

- 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**，可使用 `network interface capacity show` 命令验证集群支持的 **LIF** 容量，并使用 `network interface capacity details show` 命令（高级权限级别）验证每个节点支持的 **LIF** 容量。
- 我们将创建一个远程（云）层 **S3** 对象存储，因此我们将提供在辅助系统上配置的数据 **LIF**。在主系统上，我们将采用集群间 **LIF**。

过程

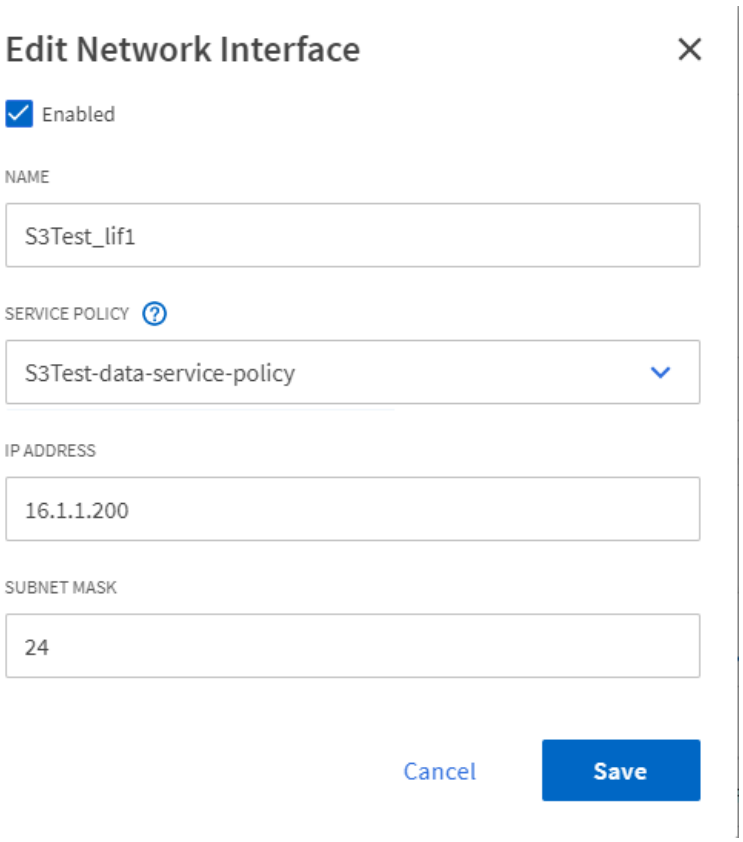
步骤 **1.** 验证之前创建的数据 **LIF**：

a. 选择 **Network（网络）** → **Overview（概述）**。

b. 找到分配给该存储虚拟机的 **LIF**。

c. 选择 **Edit（编辑）**。

d. 确认正确配置了数据服务策略。



注：如果使用了在创建 SVM 期间分配的默认服务策略，并且未按上述说明创建唯一的服务策略，则该 SVM 还可能显示为“S3, NAS”。

在主系统上创建集群间 LIF 用于远程 FabricPool 分层

在本节中，我们将在主系统上创建集群间 LIF，用于连接到我们在辅助系统上的 S3 SVM。

开始之前

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

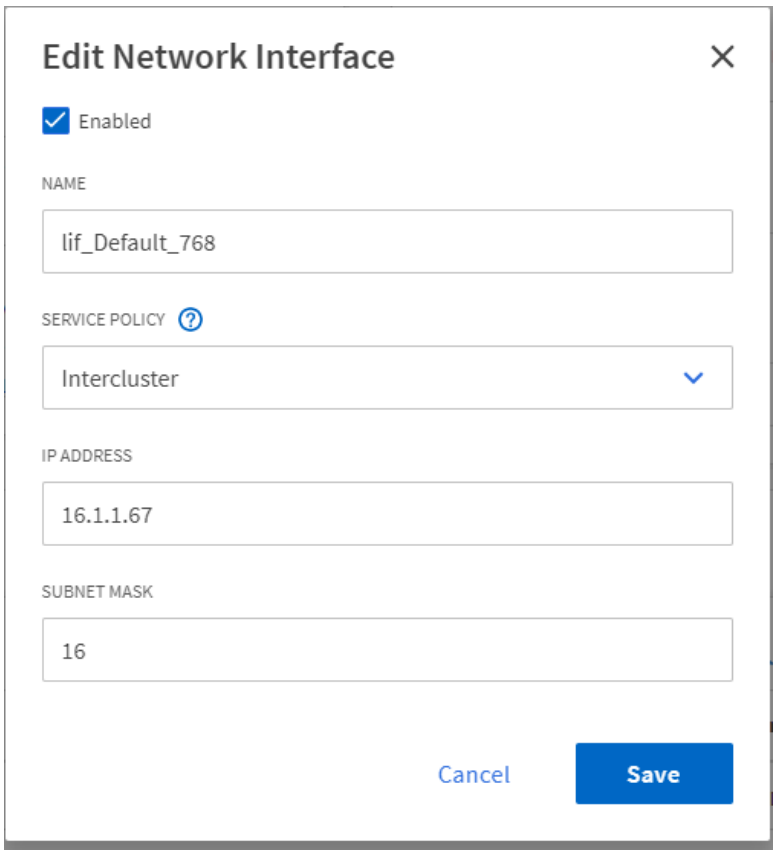
过程

步骤 1. 转到 DM 系列存储管理软件，然后执行如下操作：

a. 选择 Network（网络） → Overview（概述）。
b. 在“Network Interfaces（网络接口）”选项卡下单击 +Add（+添加）。
c. 选择 Intercluster（集群间）作为角色。
d. 为新 LIF 指定名称和主节点。
e. 为新 LIF 指定 IP 地址和网络掩码。
f. 单击 Save（保存）。

步骤 2. 验证是否已创建集群间 LIF：

a. 选择 Network（网络） → Overview（概述）。
b. 找到已创建的端口并从中选择一个。
c. 单击 Edit（编辑）。
d. 确认已启用该端口，并且角色为集群间。


Edit Network Interface
Enabled
NAME
lif_Default_768
SERVICE POLICY
Intercluster
IP ADDRESS
16.1.1.67
SUBNET MASK
16
Cancel
Save

第 5 章　为已启用 S3 的 SVM 添加存储容量

要向已启用 **S3** 的 **SVM** 添加存储容量，必须创建存储桶以提供存储容器。

创建存储桶

S3 对象保留在*存储桶* 中，不会像文件一样逐级嵌套在目录中。

开始之前

必须具备包含 **S3** 服务器的 **SVM**。

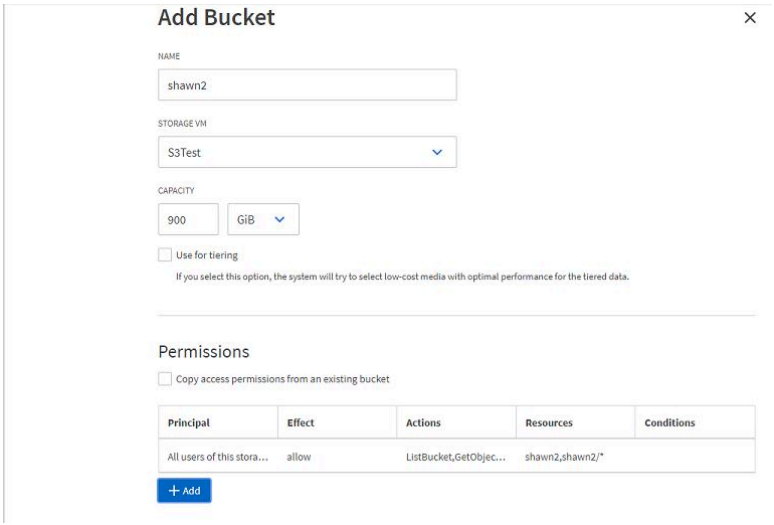
关于本任务

从 **DM** 系列存储管理软件创建存储桶时，请勿选择配置选项：

- **ONTAP** 将选择底层聚合和 **FlexGroup** 组件
  - **ONTAP** 可以自动选择聚合，从而为第一个存储桶创建并配置 **FlexGroup** 卷。它将自动选择适用于您平台的最高服务级别，或者您也可以指定存储服务级别。您稍后在 **SVM** 中添加的所有其他存储桶将具有相同的底层 **FlexGroup** 卷。
  - 在此过程中，可指定是否将该存储桶用于分层，在这种情况下，**ONTAP** 会尝试为分层的数据选择高性能低成本的介质。

过程

步骤 **1.** 转到 **DM** 系列存储管理软件。
步骤 **2.** 选择 **Storage（存储）** → **Buckets（存储桶）**。
步骤 **3.** 单击 **+Add（+ 添加）**。
步骤 **4.** 为该存储桶提供名称，并选择之前创建的 **S3 SVM**。
步骤 **5.** 选择容量并单击更多选项。
步骤 **6.** 单击 **Use for tiering（用于分层）**，以确保存储桶使用低成本硬盘而非固态硬盘。
步骤 **7.** 选择是从以前的存储桶复制权限还是单击“**+Add**（+添加）”以添加新权限。
步骤 **8.** 单击 **Save（保存）**。



注：还可使用此选项在存储桶之间启用 **SnapMirror**，但我们在本次讨论中不涉及此主题。

创建 S3 用户

为了限制与授权客户端的连接，所有 **ONTAP** 对象存储上都需要用户授权。

开始之前

必须具备已启用 **S3** 的 **SVM**。

关于本任务

可以授权 **S3** 用户访问 **SVM** 中的任何存储桶，但不能访问多个 **SVM** 中的存储桶。

创建 **S3** 用户时，将生成访问密钥和机密密钥。必须将这些密钥连同对象存储的 **FQDN** 和存储桶名称一起共享给用户。可以使用 `vserver object-store-server user show` 命令显示 **S3** 用户的密钥。

您可以在存储桶策略或对象服务器策略中向 **S3** 用户授予特定的访问权限。

注：创建对象存储服务器时，将创建一个根用户（**UID 0**），这是一个有权访问所有存储桶的特权用户。最好不要以根用户身份管理 **ONTAP S3**，而是创建具有特定权限的管理员用户角色。

过程

步骤 **1.** 创建 **S3** 用户：

```
vserver object-store-server user create -vserver svm_name -user user_name [-comment text]
```

创建或修改 S3 组

可通过创建具有适当访问权限的用户组来简化存储桶访问。

开始之前

已启用 **S3** 的 **SVM** 中必须事先存在 **S3** 用户。

关于本任务

可以授权 **S3** 组中的用户访问 **SVM** 中的任何存储桶，但不能访问多个 **SVM** 中的存储桶。可以通过两种方式配置组访问权限：

- 在存储桶级别

  在创建 **S3** 用户组后，可以在存储桶策略语句中指定组权限，并且这些权限仅应用于该存储桶。

- 在 **SVM** 级别

  在创建 **S3** 用户组后，可以在组定义中指定对象服务器策略名称。这些策略决定了存储桶和组成员的访问权限。

过程

步骤 **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]
```

在对象存储中只有一个存储桶的配置中，可以省略 **-policies** 选项；可以将组名称添加到存储桶策略中。

稍后在创建对象存储服务器策略后，可以使用 `vserver object-store-server group modify` 命令添加 **-policies** 选项。

创建或修改访问策略语句

用户和组对 **S3** 资源的访问由存储桶和对象存储服务器策略进行控制。如果用户或组的数量很少，可能只需在存储桶级别控制访问权限；如果用户和组的数量较多，则最好在对象存储服务器级别控制访问权限。

修改存储桶策略

可在创建存储桶的同时创建存储桶策略。

关于本任务

如果在第 **15** 页 “创建存储桶”的第 **3** 步中单击 **+Add（+添加）**，将会显示以下选项，并需要您配置这些选项。

过程

步骤 **1.** 选择用户类型。此存储虚拟机的所有用户、所有公共和匿名用户或由用户定义的帐户。

步骤 **2.** 将 **EFFECT（效果）**设置为 **Allow（允许）**或 **Deny（拒绝）**。

步骤 **3.** 设置各个权限。

步骤 **4.** 单击 **Save（保存）**。

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一个或多个存储桶的策略。通过将对象存储服务器策略附加到用户组，可以简化跨多个存储桶的资源访问权限管理。

开始之前

必须具备包含 **S3** 服务器和存储桶且已启用 **S3** 的 **SVM**。

关于本任务

可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** 级别上启用访问策略。只有在组定义中指定策略后，策略才会生效。

注：使用对象存储服务器策略时，请在组定义（而非策略本身）中指定主体（即用户和组）。

存在三种用于访问 **ONTAP S3** 资源的只读默认策略：

- **FullAccess**
- **NoS3Access**
- **ReadOnlyAccess**

还可以创建新的自定义策略，然后为新用户和组添加新的语句；也可以修改现有语句的属性。有关更多选项，请参阅 `vserver object-store-server policy` 手册页。

过程

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`*`]`

步骤 **2.** 创建策略语句：
`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`*`]`

以下参数将定义访问权限：

-effect	语句可以是允许或拒绝访问
-action	可以指定 * 来表示所有操作，也可以指定包含以下一项或多项的列表：GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, 和 ListMultipartUploadParts。
-resource	存储桶及其包含的任何对象。可使用通配符 *和 ？ 来构建一个用于指定资源的正则表达式。

（可选）可以使用 **-sid** 选项来指定一个文本字符串作为注释。

默认情况下，新语句将添加到语句列表的末尾，而该列表会按顺序进行处理。稍后添加或修改语句时，可以选择通过修改语句的 **-index** 设置来更改处理顺序。

验证客户端对 S3 对象存储的访问权限

配置 **S3** 服务器和存储桶之后，**S3** 管理员可以为客户端系统（包括具有远程 **FabricPool** 容量（云）层的 **ONTAP** 系统和 **S3** 客户端应用程序）或本地 **FabricPool** 容量层提供对于对象存储的访问权限。

启用 ONTAP S3 访问权限以进行远程 FabricPool 分层

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。

关于本任务

为了配置 **FabricPool** 云层，必须提供以下 **S3** 服务器信息：

- 服务器名称（**FQDN**）
- 存储桶名称
- **CA** 证书
- 访问密钥
- 密码（机密访问密钥）

此外，需要以下网络配置：

- 在为管理 **SVM** 配置的 **DNS** 服务器中，必须存在对应于远程 **ONTAP S3** 服务器主机名的条目，包括 **S3** 服务器的 **FQDN** 名称及其 **LIF** 上的 **IP** 地址。
- 虽然不需要集群对等，但必须在本地和远程集群上都配置集群间 **LIF**。

连接 ONTAP S3 对象存储作为云层

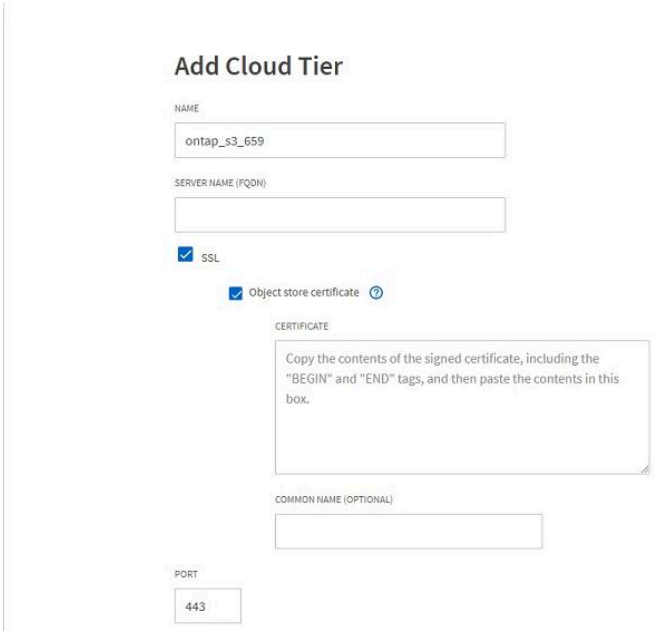
获得上述所有信息后，即可连接远程 **DM** 系列设备，将其作为主 **DM** 系列系统的云层。以下步骤将引导您完成该过程。

开始之前

开始之前，需要在主系统上定义一个本地层。

过程

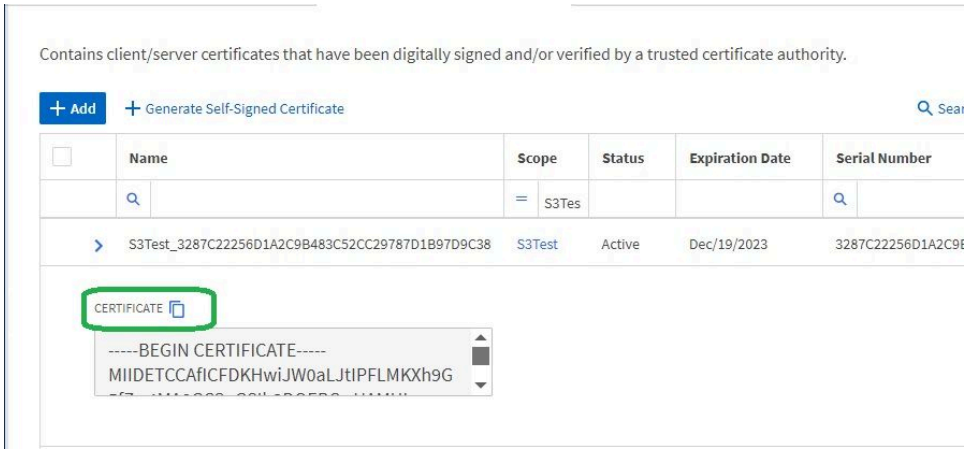
步骤 1. 选择使用辅助系统上的 ONTAP S3 存储桶添加云层。
步骤 2. 选择 Storage（存储） → Tiers（层）。
步骤 3. 选择 +Add Cloud Tier（+添加云层） → ONTAP S3。



步骤 4. 指定先前记下的 FQDN。确认已启用“SSL”框，并提供 S3 SVM 的证书。我们将在以下步骤中逐一介绍。

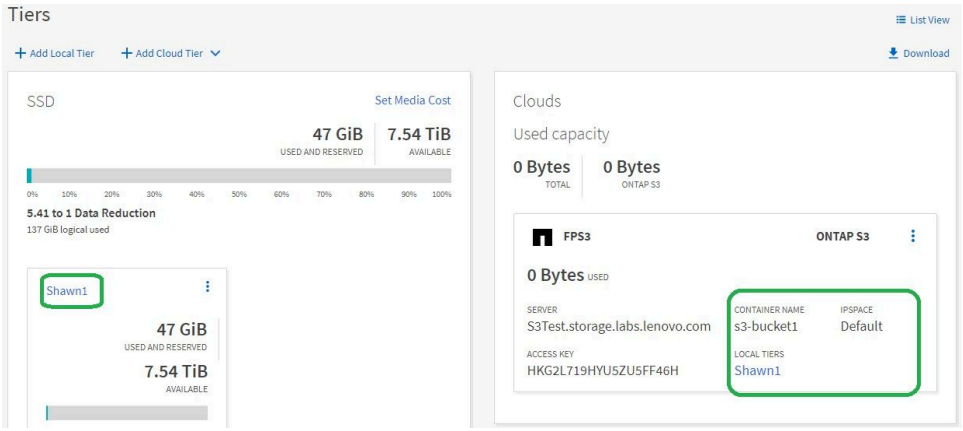
a. 要检索 FQDN，请在辅助系统上选择 Storage（存储） → Storage VMs（存储虚拟机），并单击 SVM 名称。然后转到 Settings（设置），并单击铅笔图标 以编辑该名称。

b. 指定该 SVM 的证书。要检索证书，请选择 Storage（存储） → Storage VMs（存储虚拟机）。单击该存储虚拟机以选中它。选择 Settings（设置） → Certificates（证书），并单击箭头。找到证书，并单击证书旁的箭头图标 。随后将显示一个选项，用于将证书复制到剪贴板。



c. 提供与分配给该存储桶的 **S3** 用户关联的访问密钥和机密密钥。其中将不显示机密密钥，如果丢失了该密钥，则必须重新创建，但如果需要，您可以复制访问密钥。

d. 单击 **Save（保存）**以完成连接云层的操作。



定义卷的分层策略

连接辅助系统作为云层后，需要按卷指定分层策略以确定数据位置。

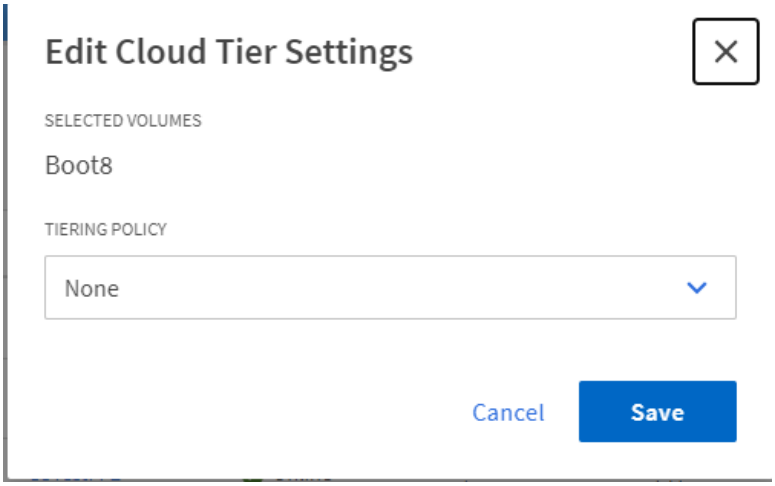
关于本任务

此分层策略决定何时将数据从本地层移动到云层。有四个分层选项。应选择与数据访问模式相符的策略。

- **Auto（自动）**：这是卷的默认设置。将根据固件默认值完成操作。
- **Snapshot Only（仅快照）**：将快照数据移动到云层，但从不将根卷数据发送到云层。
- **None（无）**：阻止将任何卷数据移动到云。
- **All（全部）**：将包括快照数据在内的所有数据都移动到云。

还有额外的一点需要考虑，那就是根据所指定的策略移出数据之前所需的最小冷却天数。默认情况下，最小冷却天数设置为 **31**。该值最低可以设置为 **2**，但要注意，这意味着数据将从较慢的云层提供，直到通过访问将其移回本地层，因此要进行大量的数据移动操作。您需要使用 **CLI** 来设置最小冷却天数，例如 `DevDM5100F::*> volume modify -vserver S3TestFP2 -volume Dat3 -tiering-minimum-cooling-days 2 Volume modify successful on volume Dat3 of Vserver S3TestFP2`。

可使用 DM 系列存储管理软件更改分层策略：选择 **Storage（存储）** → **Volumes（卷）**。选择要修改的卷，然后选择 ... 并单击 **Edit Cloud Tier Settings（编辑云层设置）**。

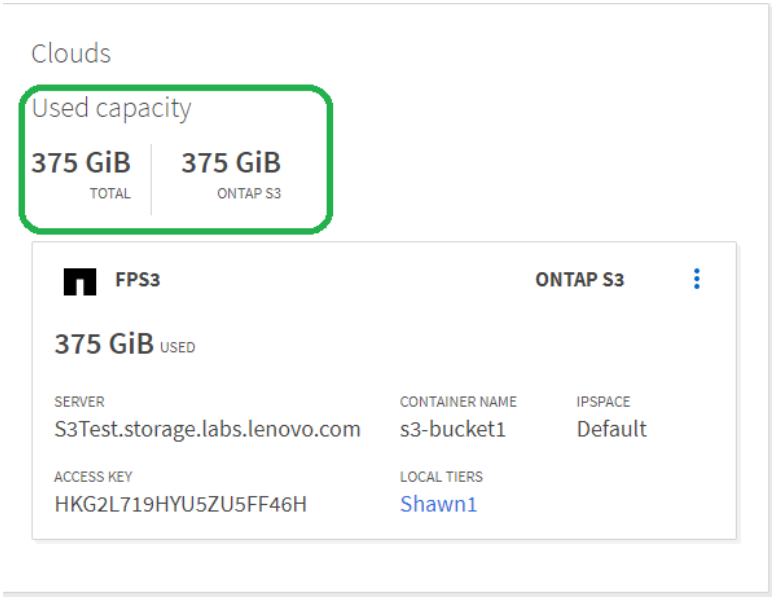


验证云层

一切配置完毕并满足冷却期后，系统就会将数据移动到云层。

关于本任务

可转到 **Storage（存储）** → **Tiers（层）**来验证云层。当您查看云层时，系统会显示已根据您指定的设置转移的数据量。



启用 ONTAP S3 访问权限以进行 FabricPool 分层

要将 **ONTAP S3** 用作本地 **FabricPool** 容量层，必须基于所创建的存储桶定义对象存储，然后将该对象存储连接到性能层聚合以创建 **FabricPool**。

开始之前

您必须具有 **ONTAP S3** 服务器名称和存储桶名称。

关于本任务

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

对象存储配置一经创建，就不得再与其他对象存储或存储桶重新关联。您可以为本地层创建多个存储桶，但不能在单个存储桶中创建多个对象存储。

本地容量层不需要 **FabricPool** 许可证。

过程

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`* `-ispace Cluster -provider-type ONTAP_S3 -server` *`S3_server_name`* `-container-name` *`bucket_name`* `-access-key` *`access_key`* `-secret-password` *`password`*

- **-container-name** 即您所创建的 **S3** 存储桶。
- **-access-key** 参数授权对 **ONTAP S3** 服务器的请求。
- **-secret-password**参数（秘密访问密钥）对 **ONTAP S3** 服务器的请求进行身份验证。
- 您可以将 **-is-certificate-validation-enabled** 参数设置为 **false**，以禁用 **ONTAP S3** 的证书检查。

示例

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

步骤 **2.** 显示并验证对象存储配置信息：
`storage aggregate object-store config show`

步骤 **3.** 可选：要查看卷中的非活动数据量，请按照使用 **FabricPool** 管理存储层中的步骤操作。
查看卷中的非活动数据量有助于确定要用于 **FabricPool** 本地分层的聚合。

步骤 **4.** 将对象存储连接到聚合：
`storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

可使用 **allow-flexgroup** true 选项来连接包含 **FlexGroup** 卷成分卷的聚合。

示例

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

步骤 **5.** 显示对象存储信息，确认已连接的对象存储为可用状态：
`storage aggregate object-store show`

示例

```
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权限

为了使 **S3** 客户端应用程序访问 **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 **AWS Signature Version 4** 向 **ONTAP S3** 服务器进行认证。**ONTAP S3** 不支持更早的签名版本。

ONTAP S3 管理员必须已创建 S3 用户，并在存储桶策略或对象存储服务器策略中以单个用户或组成员的身份授予他们访问权限。

S3 客户端应用程序必须能够解析 ONTAP S3 服务器名称，因此要求 ONTAP S3 管理员提供 S3 服务器名称（FQDN）以及 S3 服务器 LIF 的 IP 地址。

关于本任务

要访问 ONTAP S3 存储桶，S3 客户端应用程序上的用户需要输入 ONTAP S3 管理员提供的信息。

从 ONTAP 9.9.1 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。在对对象执行 GET/HEAD 操作时，用户定义的元数据会随系统元数据一起返回。

  注：要使客户端能够获取和放置标记信息，需要使用存储桶或组策略启用操作 `GetObjectTagging`、`PutObjectTagging` 和 `DeleteObjectTagging`。
- 对象标记：可以指定单独的一组键值对作为对象分类标记。与元数据不同，标记通过 REST API 独立于对象创建和读取，并在对象创建时或创建后的任意时间实施。标记还可用在存储桶和用户策略的条件策略语句中。

有关更多信息，请参阅 AWS S3 文档。

过程

步骤 1. 通过输入 S3 服务器名称和 CA 证书，向 ONTAP S3 服务器认证 S3 客户端应用程序。

步骤 2. 通过输入以下信息，在 S3 客户端应用程序上对用户进行认证：

- S3 服务器名称（FQDN）和存储桶名称
- 用户的访问密钥和机密密钥

第 6 章　存储服务定义

ONTAP 包括映射到相应最小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由 **SVM** 中构成聚合的存储类型决定。

下表显示了最小性能因素如何映射到预定义存储服务：

存储服务	预期 IOPS（SLA）	峰值 IOPS（SLO）	最小卷 IOPS	估计的延迟	是否执行了预期 IOPS?
价值	**128/TB**	**512/TB**	**75**	**17** 毫秒	在全闪存阵列上：是 否则：否
性能	**2048/TB**	**4096/TB**	**500**	**2** 毫秒	是
极端	**6144/TB**	**12288/TB**	**1000**	**1** 毫秒	是

下表定义了每种介质或节点的可用存储服务级别：

介质或节点	可用的存储服务级别
磁盘	价值
虚拟机磁盘	价值
混合	价值
容量优化闪存	价值
固态硬盘（SSD）- 非全闪存阵列	价值
性能优化闪存 - 固态硬盘（全闪存阵列）	极端、性能、价值

附录 A　联系支持机构

可联系支持以获取问题帮助。

可通过 **Lenovo** 授权服务提供商获取硬件服务。要查找 **Lenovo** 授权提供保修服务的服务提供商，请访问 **http://support.lenovo.com.cn/lenovo/wsi/station/servicestation/default.aspx**，然后使用筛选功能搜索不同国家/地区的支持信息。关于 **Lenovo** 支持电话号码，请参阅 **https://datacentersupport.lenovo.com/supportphonelist** 了解所在区域的详细支持信息。

附录 B　声明

Lenovo 可能不会在全部国家/地区都提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 **Lenovo** 代表咨询。

任何对 **Lenovo** 产品、程序或服务的引用并非意在明示或暗示只能使用该 **Lenovo** 产品、程序或服务。只要不侵犯 **Lenovo** 的知识产权，任何同等功能的产品、程序或服务，都可以代替 **Lenovo** 产品、程序或服务。但是，用户需自行负责评估和验证任何其他产品、程序或服务的运行。

Lenovo 公司可能已拥有或正在申请与本文档中所描述内容有关的各项专利。提供本文档并非要约，因此本文档不提供任何专利或专利申请下的许可证。您可以用书面方式将查询寄往以下地址：

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

Lenovo“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些管辖区域在某些交易中不允许免除明示或暗含的保修，因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。**Lenovo** 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本文档中描述的产品不应该用于移植或其他生命支持应用（其中的故障可能导致人身伤害或死亡）。本文档中包含的信息不影响或更改 **Lenovo** 产品规格或保修。根据 **Lenovo** 或第三方的知识产权，本文档中的任何内容都不能充当明示或暗含的许可或保障。本文档中所含的全部信息均在特定环境中获得，并且作为演示提供。在其他操作环境中获得的结果可能不同。

Lenovo 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

在本出版物中对非 **Lenovo** 网站的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些网站的保修。那些网站中的资料不是此 **Lenovo** 产品资料的一部分，使用那些网站带来的风险将由您自行承担。

此处包含的任何性能数据都是在受控环境下测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量可能是通过推算估计出的。实际结果可能会有差异。本文档的用户应验证其特定环境的适用数据。

商标

LENOVO、**LENOVO** 徽标和 **THINKSYSTEM** 是 **Lenovo** 的商标。所有其他商标均是其各自所有者的财产。**© 2022 Lenovo.**