启用客户端对 S3 对象存储的访问

ONTAP 9

NetApp
April 24, 2024

目录

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