提供对NAS数据的S3客户端访问

ONTAP 9

NetApp
September 12, 2024

目录

提供对NAS数据的S3客户端访问

S3多协议概述

从ONTAP 9.12.1开始、您可以使运行S3协议的客户端访问为使用NFS和SMB协议的客户端提供的相同数据、而无需重新格式化。通过此功能、可以继续为NAS客户端提供NAS数据、同时向运行S3应用程序(如数据挖掘和人工智能)的S3客户端提供对象数据。

S3多协议功能可解决两种使用情形：

1. 使用S3客户端访问现有NAS数据

   如果您的现有数据是使用传统NAS客户端(NFS或SMB)创建的、并且位于NAS卷(FlexVol 或FlexGroup 卷)上、则现在可以使用S3客户端上的分析工具访问此数据。

2. 为能够使用NAS和S3协议执行I/O的现代客户端提供后端存储

   现在、您可以为Spark和Kafka等应用程序提供集成访问、这些应用程序可以使用NAS和S3协议读写相同的数据。

S3多协议的工作原理

使用ONTAP 多协议、您可以将相同的数据集作为文件层次结构或存储分段中的对象来呈现。为此、ONTAP 会创建"S3 NAS分段"、以使S3客户端能够使用S3对象请求在NAS存储中创建、读取、删除和枚举文件。此映射符合NAS安全配置、可观察文件和目录访问权限、并根据需要写入安全审核记录。

此映射是通过将指定的NAS目录层次结构显示为S3分段来实现的。目录层次结构中的每个文件都表示为S3对象、该对象的名称与映射的目录相对、目录边界由斜杠字符("/")表示。

正常的ONTAP定义的S3用户可以访问此存储、该存储受为映射到NAS目录的存储分段定义的存储分段策略的约束。为此、必须在S3用户和SMB/NFS用户之间定义映射。SMB/NFS用户的凭据将用于NAS权限检查、并包含在这些访问所产生的任何审核记录中。

当文件由SMB或NFS客户端创建时、文件会立即放置在目录中、因此在写入任何数据之前、客户端可以看到该文件。S3客户端希望使用不同的语义、在写入新对象的所有数据之前、新对象不会显示在命名空间中。将S3映射到NAS存储会使用S3语义创建文件、从而使这些文件在外部不可见、直到S3创建命令完成为止。

S3 NAS存储分段的数据保护

S3 NAS的"分段"只是S3客户端的NAS数据映射、而不是标准S3分段。因此、无需使用NetApp SnapMirror S3功能保护S3 NAS分段。相反、您可以使用SnapMirror异步卷复制来保护包含S3 NAS分段的卷。不支持SnapMirror同步和SVM灾难恢复。

从ONTAP 9.14.1开始、MetroCluster IP和FC配置的镜像和未镜像聚合支持S3 NAS分段。

了解 "SnapMirror异步"。

审核S3 NAS存储分段

由于S3 NAS存储分段不是传统的S3存储分段、因此无法配置S3审核来审核其访问权限。了解更多信息 "S3审核"。

但是、可以使用传统的ONTAP 审核过程审核S3 NAS存储分段中映射的NAS文件和目录以查看访问事件。因此、S3操作可能会触发NAS审核事件、但以下情况除外：

- 如果S3策略配置(组或存储分段策略)拒绝S3客户端访问、则不会对此事件启动NAS审核。这是因为在执行SVM审核检查之前会检查S3权限。
- 如果S3 GET请求的目标文件大小为0、则会将0个内容返回到GET请求、并且不会记录读取访问权限。
- 如果S3 GET请求的目标文件位于用户无遍历权限的文件夹中、则访问尝试将失败、并且事件不会记录。

了解相关信息 "审核SVM上的NAS事件"。

S3和NAS互操作性

ONTAP S3 NAS分段支持标准NAS和S3功能、但此处列出的功能除外。

S3 NAS存储分段当前不支持NAS功能

FabricPool 容量层

S3 NAS存储分段不能配置为FabricPool 的容量层。

S3 NAS存储分段当前不支持S3功能

AWS用户元数据

- 在当前版本中、作为S3用户元数据一部分收到的键值对不会与对象数据一起存储在磁盘上。
- 前缀为"x-AMZ-meta"的请求标头将被忽略。

AWS标记

- 在PUT对象和Multipart启动请求上、会忽略前缀为"x-AMZ-Tagging"的标头。
- 更新现有文件上的标记的请求(即使用"标记查询字符串"的PUT、GET和Delete请求)将被拒绝、并显示错误。

版本控制

无法在存储分段映射配置中指定版本控制。

- 包含非空版本规范(versionId=xyz query-string)的请求会收到错误响应。
- 影响存储分段版本控制状态的请求将被拒绝、但出现错误。

多部分操作

不支持以下操作：

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload

- ListMultipartUpload

S3客户端访问的NAS数据要求

请务必了解、在映射NAS文件和目录以进行S3访问时、存在一些固有的不兼容性。在使用S3 NAS分段提供NAS文件层次结构之前、可能需要对其进行调整。

通过使用S3存储分段语法映射NAS目录、S3 NAS分段可提供对该目录的S3访问、并且目录树中的文件将被视为对象。对象名称是相对于S3存储分段配置中指定的目录的文件的斜杠分隔路径名。

如果使用S3 NAS分段提供文件和目录、则此映射会产生一些要求：

- S3名称限制为1024字节、因此使用S3无法访问路径名较长的文件。
- 文件和目录名称不得超过255个字符、因此对象名称的连续非斜杠(‘/’)字符不能超过255个
- 使用反斜杠(‘\’)字符分隔的SMB路径名将在S3中显示为包含正斜杠(‘/’)字符的对象名称。
- 某些合法S3对象名称对不能同时位于映射的NAS目录树中。例如、合法S3对象名称"part1/part2"和"part1/part2/part3"映射到NAS目录树中不能同时存在的文件、因为"part1/part2"是第一个名称中的文件、而另一个名称中的目录。
  - 如果"part1/part2"是现有文件、则在S3上创建"part1/part2/part3"将失败。
  - 如果"part1/part2/part3"是现有文件、则S3创建或删除"part1/part2"将失败。
  - 创建与现有对象名称匹配的S3对象将替换已存在的对象(位于未版本控制的分段中)；该对象保留在NAS中、但需要完全匹配。上述示例不会通过发生原因 删除现有对象、因为名称发生冲突时不匹配。

虽然对象存储可支持大量任意名称、但如果将大量名称放置在一个目录中、则NAS目录结构可能会遇到性能问题。特别是、其中没有斜杠(‘/’)字符的名称将全部放置在NAS映射的根目录中。如果应用程序大量使用不是"不适合NAS的"名称、则最好托管在实际对象存储分段上、而不是NAS映射上。

启用对NAS数据的S3协议访问

启用S3协议访问包括确保启用了NAS的SVM满足与启用了S3的服务器相同的要求、包括添加对象存储服务器以及验证网络连接和身份验证要求。

对于新的ONTAP 安装、建议在将SVM配置为向客户端提供NAS数据后启用对SVM的S3协议访问。要了解有关NAS协议配置的信息、请参见：

- "NFS配置"
- "SMB配置"

开始之前

在启用S3协议之前、必须配置以下内容：

- 已获得S3协议和所需NAS协议(NFS、SMB或两者)的许可。
- 已为所需的NAS协议配置SVM。
- NFS和/或SMB服务器已存在。
- 已配置DNS和任何其他所需服务。

- 正在将NAS数据导出或共享到客户端系统。

关于此任务

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。可以使用以下三种来源的CA证书：

- SVM上的新ONTAP 自签名证书。
- SVM上的现有ONTAP 自签名证书。
- 第三方证书。

您可以对S3/NAS存储分段使用与提供NAS数据相同的数据LIF。如果需要特定的IP地址、请参见 "创建数据 LIF："。要在LIF上启用S3数据流量、需要使用S3服务数据策略；您可以修改SVM的现有服务策略以包括S3。

创建S3对象服务器时、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。

System Manager

1. 在配置了NAS协议的Storage VM上启用S3。
   a. 单击*存储> Storage VM*、选择一个NAS就绪的Storage VM、单击设置、然后单击 ⚙ S3下的。
   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SVM：+是否允许使用S3协议 `vserver show -fields allowed-protocols`
2. 记录此SVM的公有 密钥证书。+ 如果需要新的ONTAP自签名证书、请参见 "在 SVM 上创建并安装 CA 证书"。
3. 更新服务数据策略
   a. 显示SVM +的服务数据策略 `network interface service-policy show -vserver *svm_name*`
   b. 添加 `data-core` 和 `data-s3-server services` (如果不存在)。+ `network interface service-policy add-service -vserver *svm_name* -policy *policy_name* -service data-core,data-s3-server`
4. 验证SVM上的数据LIF是否满足您的要求：+ `network interface show -vserver *svm_name*`
5. 创建S3服务器：+ `vserver object-store-server create -vserver *svm_name* -object-store-server *s3_server_fqdn* -certificate-name *ca_cert_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。

- 默认情况下， HTTPS 在端口 443 上处于启用状态。您可以使用-secure listener-port选项更改端口号。+ 启用 HTTPS 后，要与 SSL/TLS 正确集成，需要 CA 证书。从ONTAP 9.15.1开始、S3对象存储支持TLS 1.3。
- 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-is-http-enabled选项启用此端口、也可以使用-listener-port选项更改端口号。+ 启用 HTTP 后，所有请求和响应都将通过网络以明文形式发送。
  1. 验证是否已根据需要配置S3：+ `vserver object-store-server show`

示例+ 以下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
```

创建S3 NAS存储分段

S3 NAS存储分段是S3存储分段名称和NAS路径之间的映射。通过S3 NAS分段、您可以为SVM命名空间中具有现有卷和目录结构的任何部分提供S3访问权限。

开始之前

- 在包含NAS数据的SVM中配置了S3对象服务器。
- NAS数据符合 "S3客户端访问的要求"。

关于此任务

您可以配置S3 NAS存储分段以指定SVM根目录中的任何一组文件和目录。

您还可以设置分段策略、以便根据以下参数的任意组合允许或禁止访问NAS数据：

- 文件和目录
- 用户和组权限
- S3操作

例如、您可能希望使用单独的存储分段策略、为一组用户授予只读数据访问权限、并使用另一个存储分段策略、允许受限组对该数据的一部分执行操作。

由于S3 NAS的"分段"是映射而不是S3分段、因此标准S3分段的以下属性不适用于S3 NAS分段。

- **aggr-list \ aggr-list-multi**倍 频**\ storage-service-level \ volume \ size \ exex**懦**-aggr-list \ QoS-policy-group+** 配置S3 NAS分段时、不会创建任何卷或qtree。
- *角色\ is -protored \ is -proted-in-on-NAS \ is -proted-on-Cloud *+ S3 ONTAP存储分段不使用SnapMirror S3进行保护或镜像、而是使用在卷粒度级别提供的常规SnapMirror保护。
- 版本控制状态+ NAS卷通常采用Snapshot技术来保存不同的版本。但是、S3 NAS存储分段当前不支持版本控制。
- *逻辑使用\ object-count *+ 可通过volume命令为NAS卷提供等效统计信息。

System Manager

在启用了NAS的Storage VM上添加新的S3 NAS存储分段。

1. 单击 * 存储 > 分段 * ，然后单击 * 添加 * 。
2. 输入S3 NAS存储分段的名称并选择Storage VM、不要输入大小、然后单击*更多选项*。
3. 输入有效的路径名称或单击浏览以从有效路径名称列表中进行选择。+ 输入有效的路径名后、与S3 NAS配置无关的选项将被隐藏。
4. 如果已将S3用户映射到NAS用户并创建了组、则可以配置其权限、然后单击*保存*。+ 在此步骤中配置权限之前、您必须已将S3用户映射到NAS用户。

否则、请单击*保存*以完成S3 NAS存储分段配置。

命令行界面

在包含NAS文件系统的SVM中创建S3 NAS存储分段。+ `vserver object-store-server bucket create -vserver svm_name -bucket bucket_name -type nas -nas-path junction_path [-comment text]`

示例：+ `cluster1::> vserver object-store-server bucket create -bucket testbucket -type nas -path /vol1`

启用S3客户端用户

要使S3客户端用户能够访问NAS数据、您必须将S3用户名映射到相应的NAS用户、然后向其授予使用存储分段服务策略访问NAS数据的权限。

开始之前

客户端访问的用户名—Linux/UNIX、Windows和S3客户端用户—必须已存在。

关于此任务

通过将S3用户名映射到相应的Linux/UNIX或Windows用户、可以在S3客户端访问NAS文件时对这些文件进行授权检查。通过提供S3用户名_Pattern_来指定S3到NAS的映射、该用户名可以表示为单个名称或POSIX正则表达式、并提供Linux/UNIX或Windows用户名_Replacement。

如果不存在名称映射、则会使用默认名称映射、其中S3用户名本身将用作UNIX用户名和Windows用户名。您可以使用修改UNIX和Windows默认用户名映射 `vserver object-store-server modify` 命令：

仅支持本地名称映射配置；不支持LDAP。

将S3用户映射到NAS用户后、您可以为用户授予权限、以指定其有权访问的资源(目录和文件)以及允许或不允许在其中执行的操作。

System Manager

1. 为UNIX或Windows客户端(或两者)创建本地名称映射。
   a. 单击*存储>分段*、然后选择启用了S3/NAS的Storage VM。
   b. 选择*Settings*，然后单击 → **Name Mapping**(在*Host Users and Groups*下)。
   c. 在* S3到Windows 或 S3到UNIX*图块(或两者)中、单击*添加*、然后输入所需的*模式*(S3)和*替换*(NAS)用户名。
2. 创建存储分段策略以提供客户端访问。
   a. 单击*Storage > Buckets*，单击所需S3存储分段旁边的，然后单击 ⋮ **Edit**。
   b. 单击*添加*并提供所需的值。
      - 主体—提供S3用户名或使用默认值(所有用户)。
      - 影响-选择*允许*或*拒绝*。
      - 操作-输入这些用户和资源的操作。对象存储服务器当前为S3 NAS分段支持的一组资源操作包括：GetObject、PutObject、DeleteObject、ListBucketAcl、GetBucketAcl、 GetObjectAcl 、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、GetBucketVersioning、PutBucketVersioning和ListBucketVersions。此参数可使用通配符。
      - 资源-输入允许或拒绝操作的文件夹或文件路径、或者使用默认值(存储分段的根目录)。

命令行界面

1. 为UNIX或Windows客户端(或两者)创建本地名称映射。+ `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` —映射评估的优先级编号；输入1或2。
   - `-pattern` —S3用户名或正则表达式
   - `-replacement` —Windows或UNIX用户名

示例+ `vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1 -replacement win_user_1 vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1 -replacement unix_user_1`

1. 创建存储分段策略以提供客户端访问。+ `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` -指定在用户请求操作时是允许还是拒绝访问。
   - `-action <Action>, …` -指定允许或拒绝的资源操作。对象存储服务器当前为S3 NAS分段支持的一组资源操作包括：GetObject、PutObject、DeleteObject、ListBucketAcl、GetBucketAcl、GetObjectAcl、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、 GetBucketVersioning、PutBucketVersioning和ListBucketVersions。此参数可使用通配符。
   - `-principal <Objectstore Principal>, …` -根据在此参数中指定的对象存储服务器用户或组验证请求访问的用户。
     - 通过向组名称添加前缀group/来指定对象存储服务器组。

        - `-principal` -(连字符)授予所有用户访问权限。

    - `-resource <text>, …` -指定为其设置了允许/拒绝权限的分段、文件夹或对象。此参数可使用通配符。

    - `[-sid <SID>]` -指定对象存储服务器存储分段策略语句的可选文本注释。

示例+
```
cluster1::> vserver object-store-server bucket policy add-statement
-bucket testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```