



创建云存储池

StorageGRID 11.5

NetApp
April 11, 2024

目录

创建云存储池	1
S3：指定云存储池的身份验证详细信息	2
C2S S3：指定云存储池的身份验证详细信息	5
Azure：指定云存储池的身份验证详细信息	8

创建云存储池

创建云存储池时，您需要指定 StorageGRID 用于存储对象的外部存储分段或容器的名称和位置，云提供程序类型（Amazon S3 或 Azure Blob Storage）以及 StorageGRID 访问外部存储分段或容器所需的信息。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 您必须已查看配置云存储池的准则。
- 云存储池引用的外部存储分段或容器必须存在。
- 您必须拥有访问存储分段或容器所需的所有身份验证信息。

关于此任务

云存储池指定一个外部 S3 存储分段或 Azure Blob 存储容器。StorageGRID 会在您保存云存储池后立即对其进行验证，因此您必须确保云存储池中指定的存储分段或容器存在且可访问。

步骤

1. 选择* ILM >*存储池。

此时将显示存储池页面。此页面包含两个部分：存储池和云存储池。

The screenshot shows the 'Storage Pools' section of the StorageGRID management console. It includes a table with columns for Name, Used Space, Free Space, Total Capacity, and ILM Usage. Below the table is a section for 'Cloud Storage Pools' which is currently empty, with a 'No Cloud Storage Pools found.' message.

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

No Cloud Storage Pools found.

2. 在页面的Cloud Storage Pools部分中、单击*创建*。

此时将显示创建云存储池对话框。

Create Cloud Storage Pool

Display Name

Provider Type

▼

Bucket or Container

Cancel
Save

3. 输入以下信息：

字段	Description
显示名称	一个名称，用于简要说明云存储池及其用途。在配置 ILM 规则时，请使用易于识别的名称。
提供程序类型	您将在此云存储池中使用哪个云提供商： <ul style="list-style-type: none"> • Amazon S3 (为S3或C2S S3云存储池选择此选项) • Azure Blob存储 <ul style="list-style-type: none"> ◦ 注： * 选择提供程序类型时，页面底部将显示服务端点，身份验证和服务器验证部分。
存储分段或容器	为云存储池创建的外部 S3 存储分段或 Azure 容器的名称。此处指定的名称必须与存储分段或容器的名称完全匹配，否则创建云存储池将失败。保存云存储池后，您无法更改此值。

4. 根据选定提供程序类型，完成页面的服务端点，身份验证和服务器验证部分。

- ["S3：指定云存储池的身份验证详细信息"](#)
- ["C2S S3：指定云存储池的身份验证详细信息"](#)
- ["Azure：指定云存储池的身份验证详细信息"](#)

S3：指定云存储池的身份验证详细信息

在为 S3 创建云存储池时，必须选择云存储池端点所需的身份验证类型。您可以指定匿名或输入访问密钥 ID 和机密访问密钥。

您需要的内容

- 您必须已输入云存储池的基本信息并指定* Amazon S3*作为提供程序类型。

Create Cloud Storage Pool

Display Name ⓘ S3 Cloud Storage Pool

Provider Type ⓘ Amazon S3 ▼

Bucket or Container ⓘ my-s3-bucket

Service Endpoint

Protocol ⓘ HTTP HTTPS

Hostname ⓘ example.com or 0.0.0.0

Port (optional) ⓘ 443

Authentication

Authentication Type ⓘ ▼

Server Verification

Certificate Validation ⓘ Use operating system CA certificate ▼

Cancel

Save

- 如果您使用的是访问密钥身份验证、则必须知道外部S3存储分段的访问密钥ID和机密访问密钥。

步骤

1. 在 * 服务端点 * 部分中，提供以下信息：
 - a. 选择要在连接到云存储池时使用的协议。
默认协议为 HTTPS。
 - b. 输入云存储池的服务器主机名或 IP 地址。

例如：



请勿在此字段中包含存储分段名称。您可以在 * 分段或容器 * 字段中包含分段名称。

- a. (可选) 指定在连接到云存储池时应使用的端口。

将此字段留空可使用默认端口：端口 443 用于 HTTPS，端口 80 用于 HTTP。

2. 在 * 身份验证 * 部分中，选择云存储池端点所需的身份验证类型。

选项	Description
访问密钥	要访问云存储池存储分段，需要访问密钥 ID 和机密访问密钥。
匿名	每个人都有权访问云存储池存储分段。不需要访问密钥 ID 和机密访问密钥。
CAP (C2S 访问门户)	仅用于 C2S S3。转至 "C2S S3：指定云存储池的身份验证详细信息" 。

3. 如果选择了访问密钥，请输入以下信息：

选项	Description
访问密钥 ID	拥有外部存储分段的帐户的访问密钥 ID。
机密访问密钥	关联的机密访问密钥。

4. 在服务器验证部分中，选择应使用哪种方法验证与云存储池的 TLS 连接的证书：

选项	Description
使用操作系统 CA 证书	使用操作系统上安装的默认 CA 证书来保护连接。
使用自定义 CA 证书	使用自定义 CA 证书。单击 * 选择新 *、然后上传 PEM 编码的 CA 证书。
请勿验证证书	未验证用于 TLS 连接的证书。

5. 单击 * 保存 *。

保存云存储池时，StorageGRID 将执行以下操作：

- 验证存储分段和服务端点是否存在，以及是否可以使用您指定的凭据访问它们。
- 将标记文件写入存储分段，以将存储分段标识为云存储池。切勿删除名为的此文件 `x-ntap-sgws-cloud-pool-uuid`。

如果云存储池验证失败，您将收到一条错误消息，说明验证失败的原因。例如，如果存在证书错误或您指定的存

储分段不存在，则可能会报告错误。

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket: The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

请参见有关对云存储池进行故障排除的说明、解决问题描述 问题、然后重新尝试保存云存储池。

相关信息

["对云存储池进行故障排除"](#)

C2S S3：指定云存储池的身份验证详细信息

要将商用云服务（C2S）S3 服务用作云存储池，您必须将 C2S 访问门户（CAP）配置为身份验证类型，以便 StorageGRID 可以请求临时凭据来访问 C2S 帐户中的 S3 存储分段。

您需要的内容

- 您必须已输入Amazon S3云存储池的基本信息、包括服务端点。
- 您必须知道StorageGRID 将用于从CAP服务器获取临时凭据的完整URL、包括分配给C2S帐户的所有必需和可选API参数。
- 您必须拥有由适当的政府证书颁发机构(CA)颁发的服务器CA证书。StorageGRID 使用此证书来验证 CAP 服务器的身份。服务器 CA 证书必须使用 PEM 编码。
- 您必须拥有由适当的政府证书颁发机构(CA)颁发的客户端证书。StorageGRID 使用此证书向 CAP 服务器标识自身。客户端证书必须使用 PEM 编码，并且必须已授予对 C2S 帐户的访问权限。
- 您必须为客户端证书使用PEM编码的专用密钥。
- 如果客户端证书的私钥已加密、则必须具有用于对其进行解密的密码短语。

步骤

1. 在 * 身份验证 * 部分中，从 * 身份验证类型 * 下拉列表中选择 * CAP （ C2S Access Portal ） *。

此时将显示 CAP C2S 身份验证字段。

Create Cloud Storage Pool

Display Name ⓘ S3 Cloud Storage Pool

Provider Type ⓘ Amazon S3 ▼

Bucket or Container ⓘ my-s3-bucket

Service Endpoint

Protocol ⓘ HTTP HTTPS

Hostname ⓘ s3-aws-region.amazonaws.com

Port (optional) ⓘ 443

Authentication

Authentication Type ⓘ CAP (C2S Access Portal) ▼

Temporary Credentials URL ⓘ https://example.com/CAP/api/v1/credentials?agency=my

Server CA Certificate ⓘ

Client Certificate ⓘ

Client Private Key ⓘ

Client Private Key Passphrase (optional) ⓘ

Server Verification

Certificate Validation ⓘ Use operating system CA certificate ▼

Cancel

Save

2. 请提供以下信息：

- a. 对于 * 临时凭据 URL *，输入 StorageGRID 从 CAP 服务器获取临时凭据所使用的完整 URL，包括分配给 C2S 帐户的所有必需和可选 API 参数。
- b. 对于*服务器CA证书*、单击*选择新*、然后上传PEM编码的CA证书、StorageGRID 将使用该证书来验证CAP服务器。
- c. 对于*客户端证书*、单击*选择新证书*、然后将StorageGRID 用于标识自身的PEM编码证书上传到CAP服务器。
- d. 对于*客户端专用密钥*、单击*选择新*、然后上传PEM编码的客户端证书专用密钥。

如果私钥已加密，则必须使用传统格式。（不支持 PKCS 8 加密格式。）

- e. 如果客户端专用密钥已加密，请输入用于对客户端专用密钥进行解密的密码短语。否则，请将 * 客户端专用密钥密码短语 * 字段留空。

3. 在服务器验证部分中，提供以下信息：

- a. 对于 * 证书验证 *，选择 * 使用自定义 CA 证书 *。
- b. 单击*选择新*、然后上传PEM编码的CA证书。

4. 单击 * 保存 *。

保存云存储池时， StorageGRID 将执行以下操作：

- 验证存储分段和服务端点是否存在，以及是否可以使用您指定的凭据访问它们。
- 将标记文件写入存储分段，以将存储分段标识为云存储池。切勿删除名为的此文件 `x-ntap-sgws-cloud-pool-uuid`。

如果云存储池验证失败，您将收到一条错误消息，说明验证失败的原因。例如，如果存在证书错误或您指定的存储分段不存在，则可能会报告错误。

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket: The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

请参见有关对云存储池进行故障排除的说明、解决问题描述 问题、然后重新尝试保存云存储池。

相关信息

["对云存储池进行故障排除"](#)


Azure：指定云存储池的身份验证详细信息


为 Azure Blob 存储创建云存储池时，必须为 StorageGRID 用于存储对象的外部容器指定帐户名称和帐户密钥。


您需要的内容

- 您必须已输入云存储池的基本信息并指定* Azure Blob Storage*作为提供程序类型。* 共享密钥 * 显示在 * 身份验证类型 * 字段中。


Create Cloud Storage Pool

Display Name  Azure Cloud Storage Pool


Provider Type  Azure Blob Storage ▼


Bucket or Container  my-azure-container


Service Endpoint

URI  https://myaccount.blob.core.windows.net


Authentication

Authentication Type  Shared Key

Account Name 

Account Key 

Server Verification

Certificate Validation  Use operating system CA certificate ▼

- 您必须知道用于访问用于云存储池的Blob存储容器的统一资源标识符(Uniform Resource Identifier、URI)。
- 您必须知道存储帐户的名称和机密密钥。您可以使用 Azure 门户查找这些值。

步骤

1. 在 * 服务端点 * 部分中，输入用于访问用于云存储池的 Blob 存储容器的统一资源标识符（Uniform Resource Identifier，URI）。

使用以下格式之一指定 URI：

- `https://host:port`
- `http://host:port`

如果未指定端口，则默认情况下，端口 443 用于 HTTPS URI，端口 80 用于 HTTP URI。+* Azure Blob 存储容器的示例URI *：`https://myaccount.blob.core.windows.net`

2. 在 * 身份验证 * 部分中，提供以下信息：
 - a. 对于 * 帐户名称 *，输入拥有外部服务容器的 Blob 存储帐户的名称。
 - b. 对于 * 帐户密钥 *，输入 Blob 存储帐户的机密密钥。



对于 Azure 端点，您必须使用共享密钥身份验证。

3. 在 * 服务器验证 * 部分中，选择应使用哪种方法验证与云存储池的 TLS 连接的证书：

选项	Description
使用操作系统 CA 证书	使用操作系统上安装的默认CA证书来保护连接。
使用自定义 CA 证书	使用自定义 CA 证书。单击*选择新*、然后上传PEM编码的证书。
请勿验证证书	未验证用于 TLS 连接的证书。

4. 单击 * 保存 *。

保存云存储池时，StorageGRID 将执行以下操作：

- 验证容器和 URI 是否存在，以及是否可以使用您指定的凭据访问它们。
- 将标记文件写入容器，以将其标识为云存储池。切勿删除名为的此文件 `x-ntap-sgws-cloud-pool-uuid`。

如果云存储池验证失败，您将收到一条错误消息，说明验证失败的原因。例如，如果存在证书错误或您指定的容器不存在，则可能会报告错误。

请参见有关对云存储池进行故障排除的说明、解决问题描述 问题、然后重新尝试保存云存储池。

相关信息

["对云存储池进行故障排除"](#)

版权信息

版权所有 © 2024 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。