



将基于对象的存储从**ONTAP S3** 迁移到**StorageGRID**

How to enable StorageGRID in your environment

NetApp
October 09, 2024

目录

将基于对象的存储从ONTAP S3迁移到StorageGRID	1
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3	1
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3	1
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3	13
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3	25
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3	34

将基于对象的存储从**ONTAP S3**迁移到**StorageGRID**

通过将基于对象的存储从**ONTAP S3**无缝迁移到**StorageGRID**来实现企业级**S3**

通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

迁移演示

本演示将用户和分段从ONTAP S3迁移到StorageGRID。

通过将基于对象的存储从**ONTAP S3**无缝迁移到**StorageGRID**来实现企业级**S3**

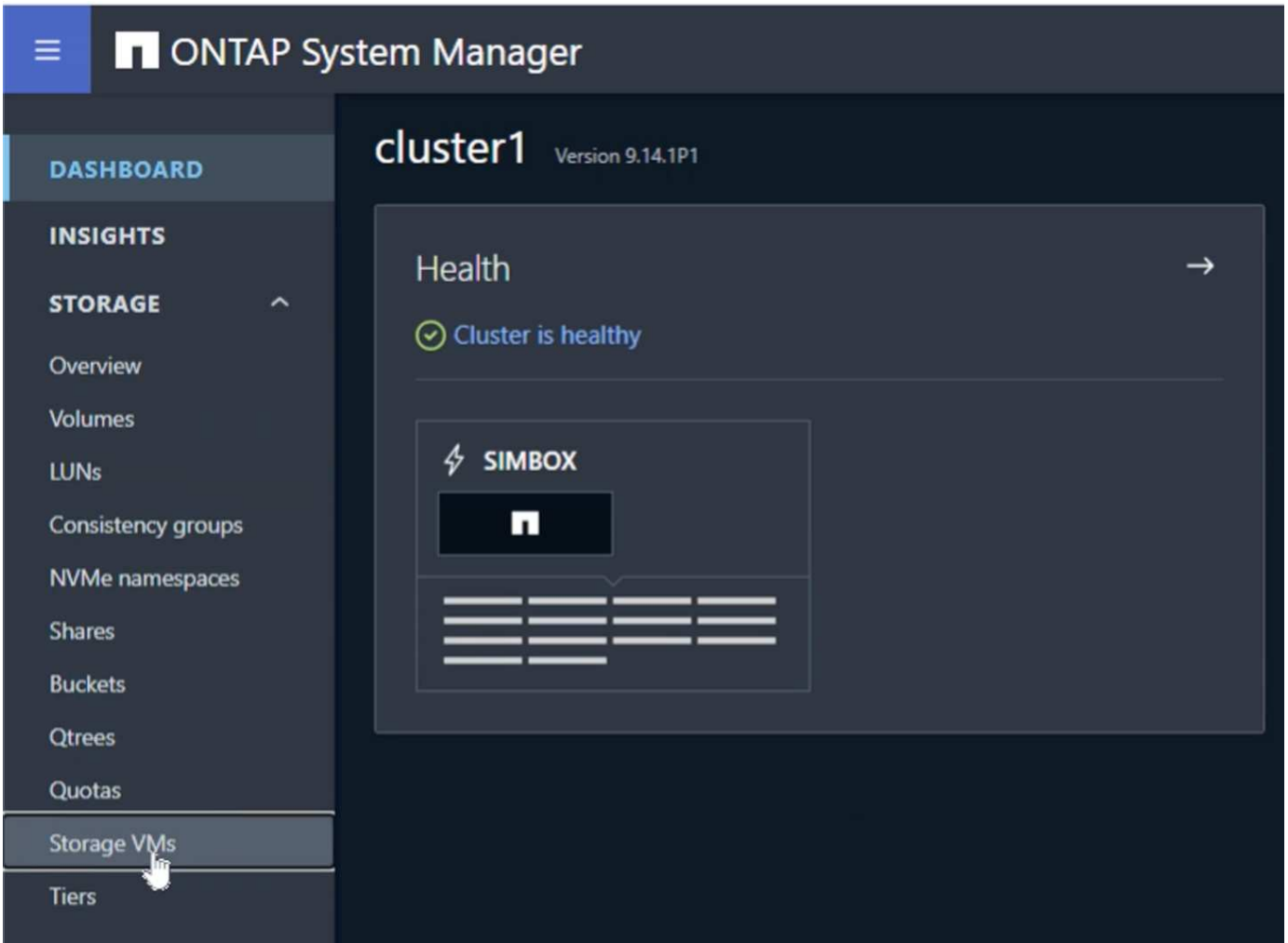
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

正在准备**ONTAP**

为了便于演示、我们将创建SVM对象存储服务器、用户、组、组策略和分段。

创建**Storage Virtual Machine**

在ONTAP系统管理器中、导航到Storage VM并添加新的Storage VM。



选中"启用S3"和"启用TLS"复选框并配置HTTP (S)端口。如果您的环境未使用默认值或不需、请定义IP、子网掩码并定义网关和广播域。

Add storage VM



STORAGE VM NAME

svm_demo

Access protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Enable S3

S3 SERVER NAME

s3portal.demo.netapp.com

Enable TLS

PORT

443

CERTIFICATE

Use system-generated certificate

Use external-CA signed certificate

Use HTTP (non-secure)

PORT

8080

DEFAULT LANGUAGE

c.utf_8

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

onPrem-01

IP ADDRESS

192.168.0.200

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

Default

Storage VM administration

Enable maximum capacity limit

The maximum capacity that all volumes in this storage VM can allocate. [Learn More](#)

Manage administrator account

Save

Cancel

在创建SVM过程中、将创建用户。下载此用户的S3密钥并关闭窗口。


Added storage VM ✕

STORAGE VM
svm_demo


S3 SERVER NAME
s3portal.demo.netapp.com

User details

USER NAME
sm_s3_user

 The secret key won't be displayed again. Save this key for future use.

ACCESS KEY

34EH21411SMW1YOV3NQY

SECRET KEY
[Show secret key](#)

Download Close


创建SVM后、编辑SVM并添加DNS设置。

Services

NIS

Not configured

Name service switch

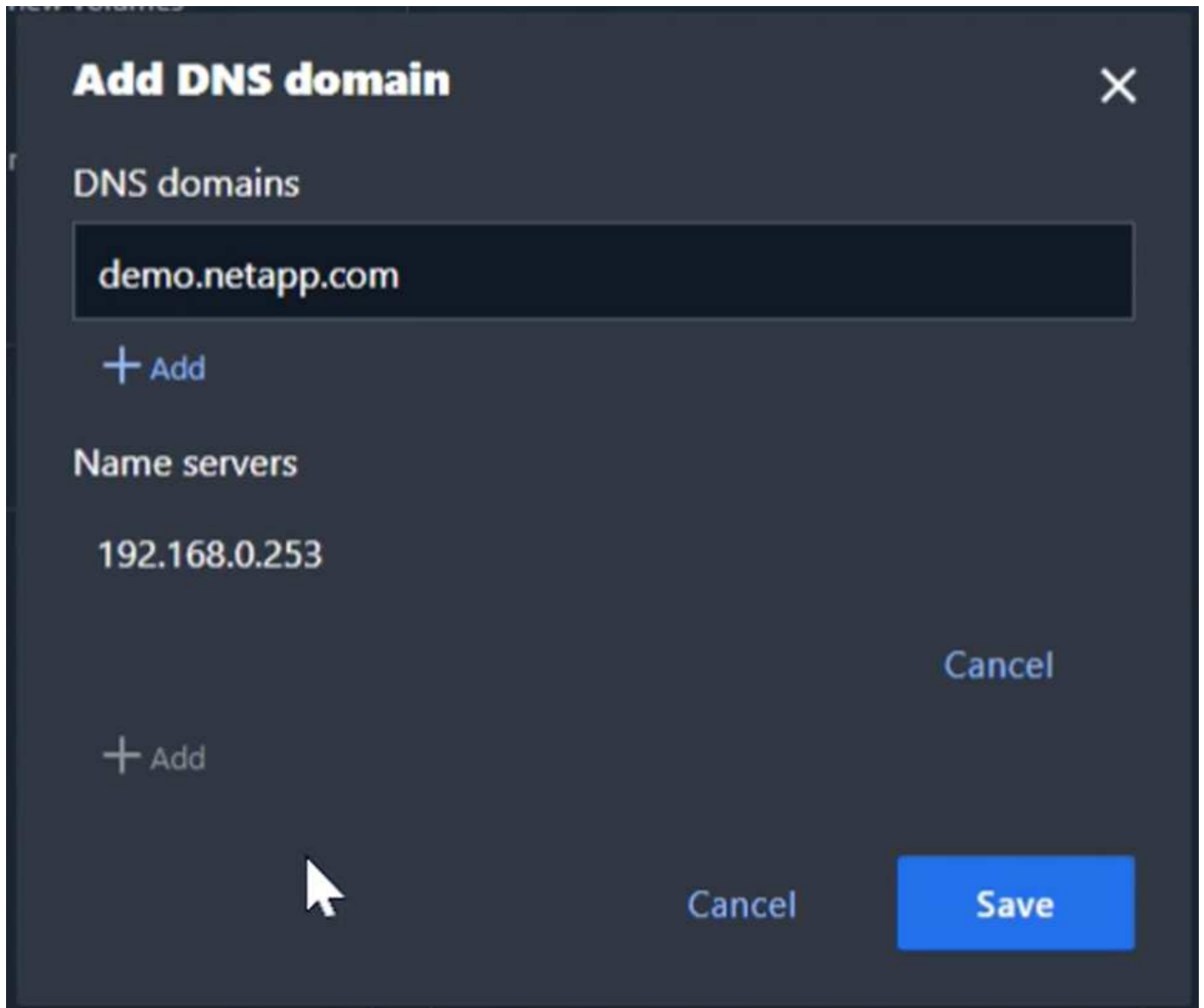
Services lookup order 

- HOSTS
Files, then DNS
- GROUP
Files
- NAME MAP
Files
- NETGROUP
Files

DNS

Not configured

定义DNS名称和IP。



创建SVM S3用户

现在、我们可以配置S3用户和组。编辑S3设置。

Protocols

NFS



Not configured

SMB/CIFS



Not configured

NVMe



Not configured

S3

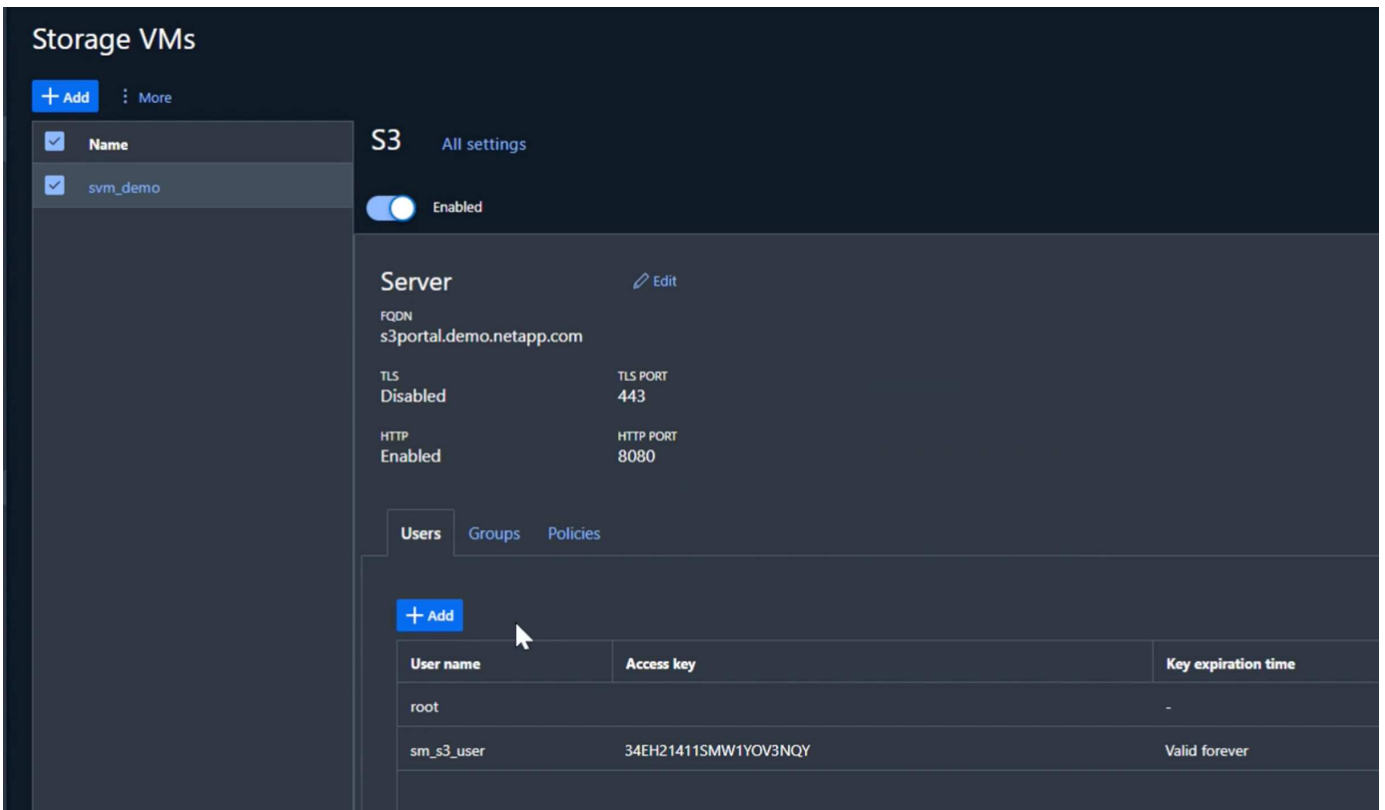


STATUS
✓ Enabled

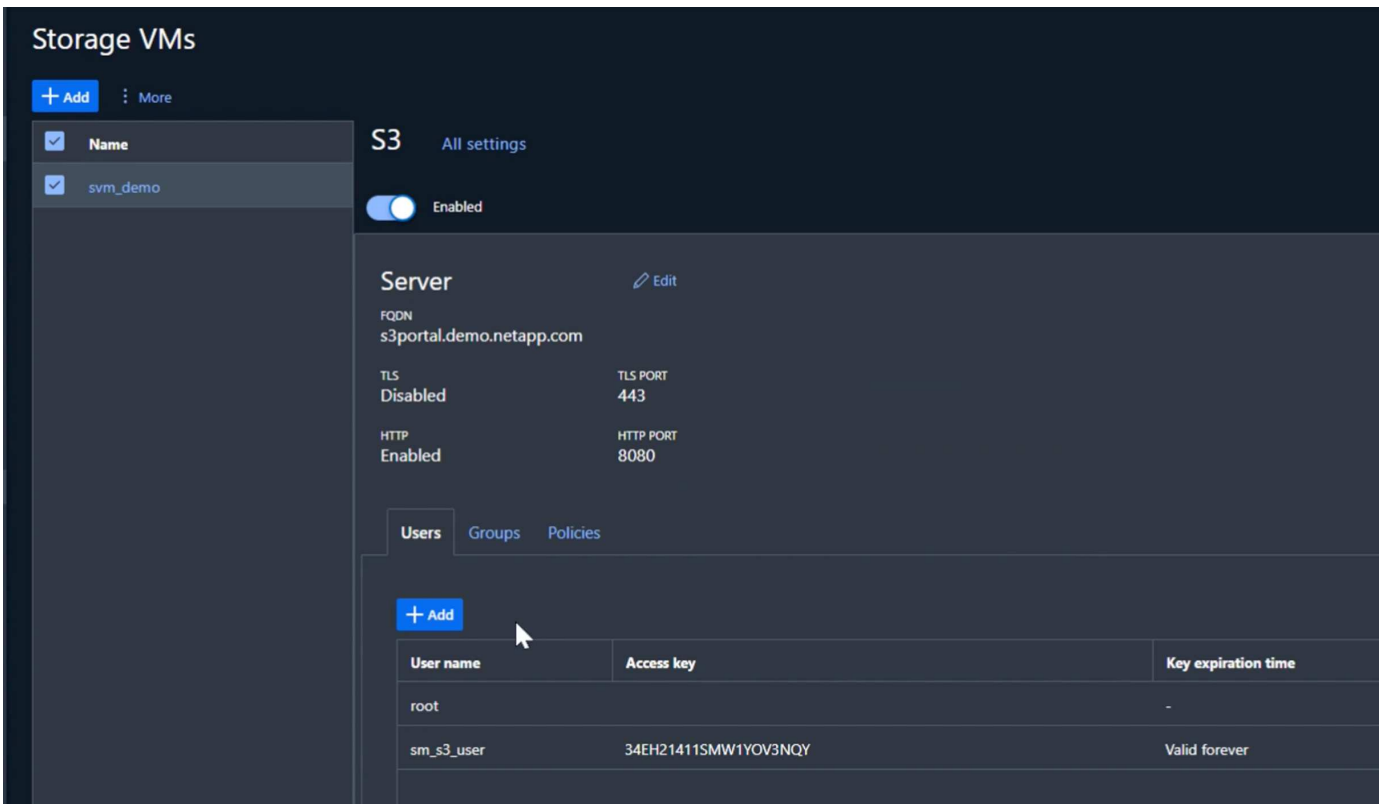
TLS
Disabled

HTTP
Enabled

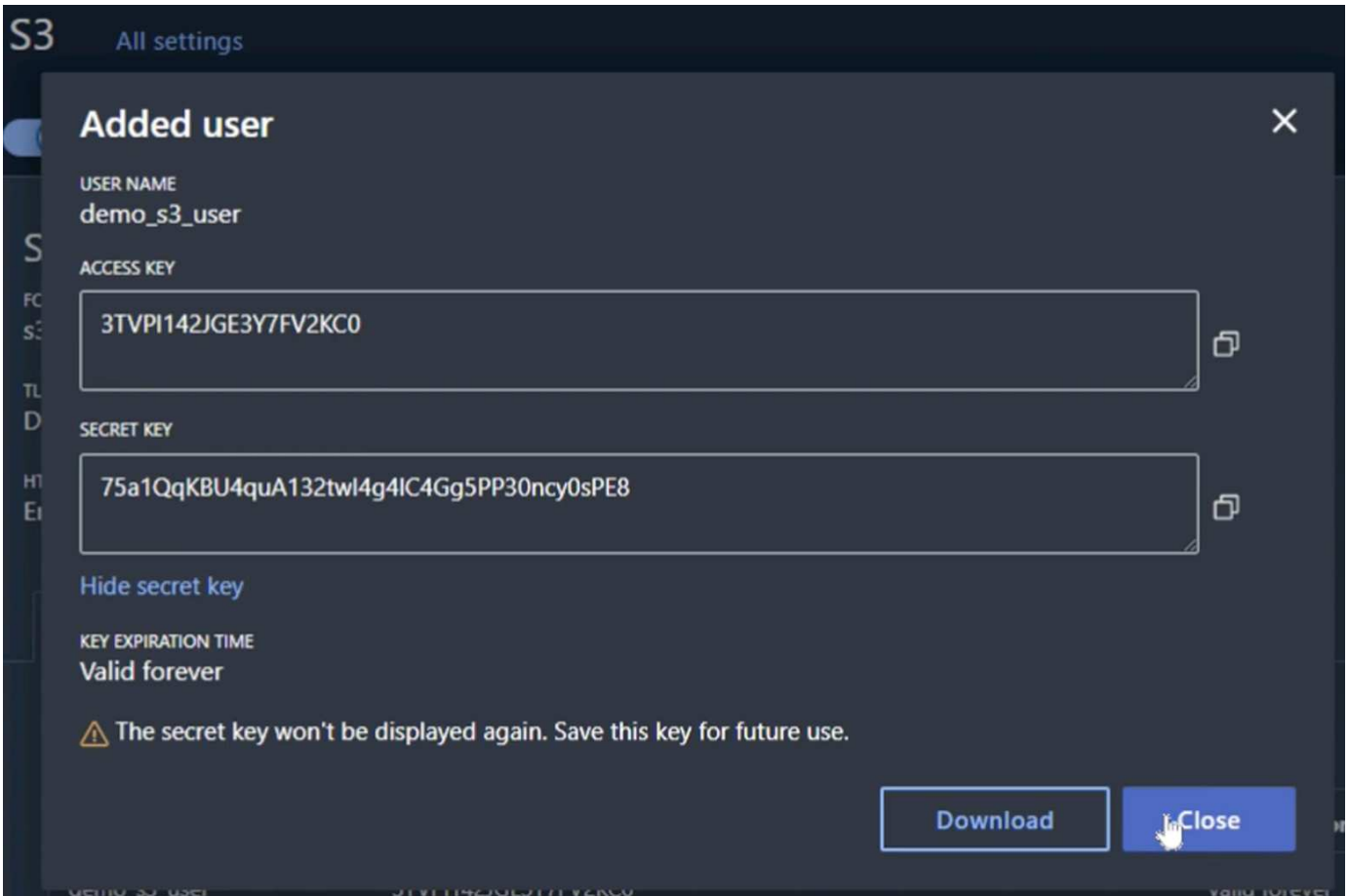
添加新用户。



输入用户名和密钥到期日期。

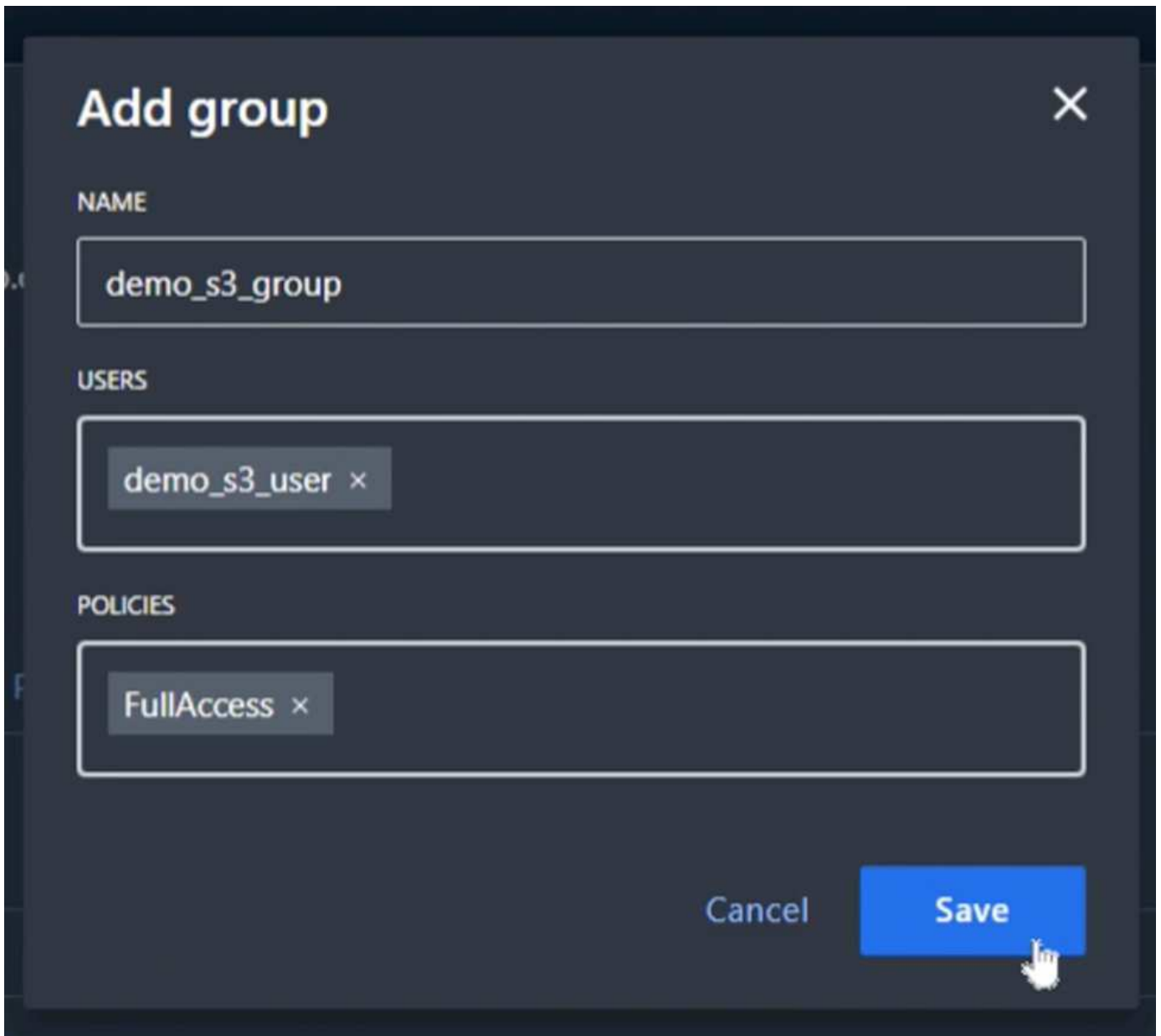


为新用户下载S3密钥。



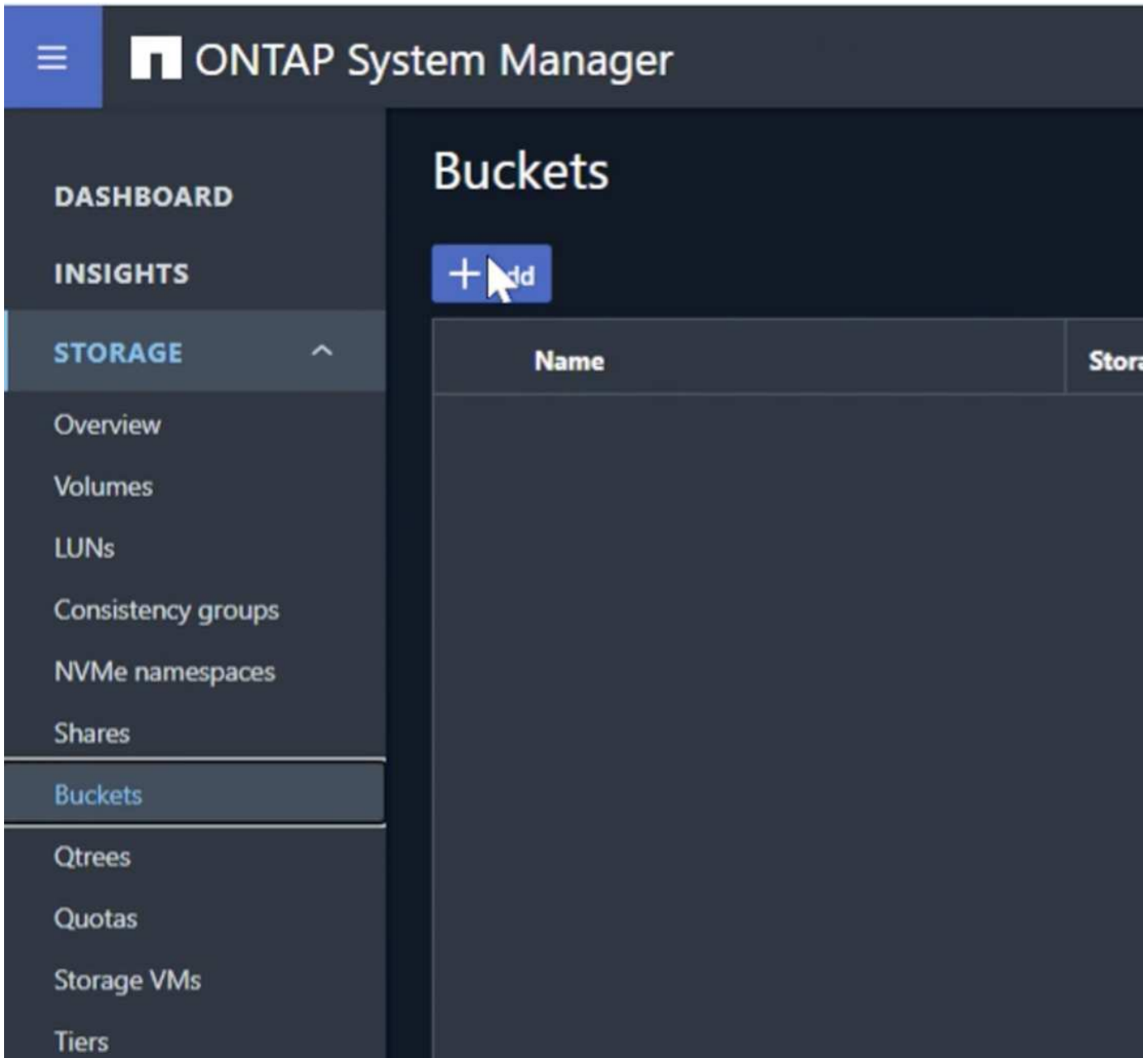
创建SVM S3组

在SVM S3设置的组选项卡上、添加一个具有上述创建用户和FullAccess权限的新组。



创建SVM S3存储分段

导航到"存储分段"部分、然后单击"+Add"按钮。



输入名称、容量并取消选中"Enable ListBucket"复选框、然后单击"更多选项"按钮。

Add bucket ×

NAME

CAPACITY

100 GiB

Enable ListBucket access for all users on the storage VM "svm_demo".
Enabling this will allow users to access the bucket.

在"更多选项"部分中、选中"启用版本控制"复选框、然后单击"保存"按钮。

Add bucket ×

NAME

FOLDER (OPTIONAL)

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

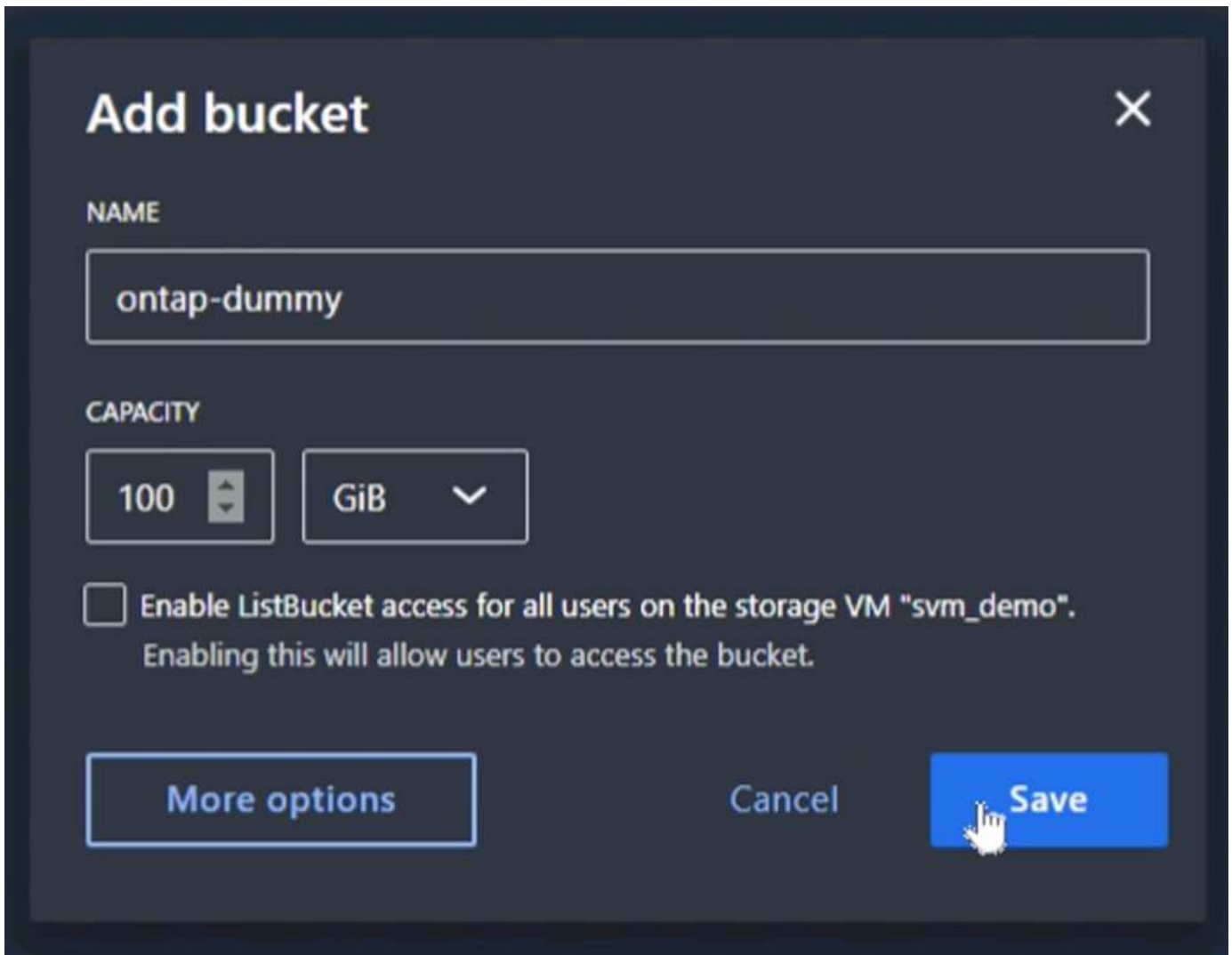
Use for tiering
If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.

Enable versioning
Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Not sure? [Get help selecting type](#)

重复此过程、并在未启用版本控制的情况下创建第二个存储分段。输入一个名称、与存储分段1的容量相同、并取消选中"Enable ListBucket"复选框、然后单击"Save (保存)"按钮。



作者：拉斐尔·吉德斯和阿伦·克莱因

通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

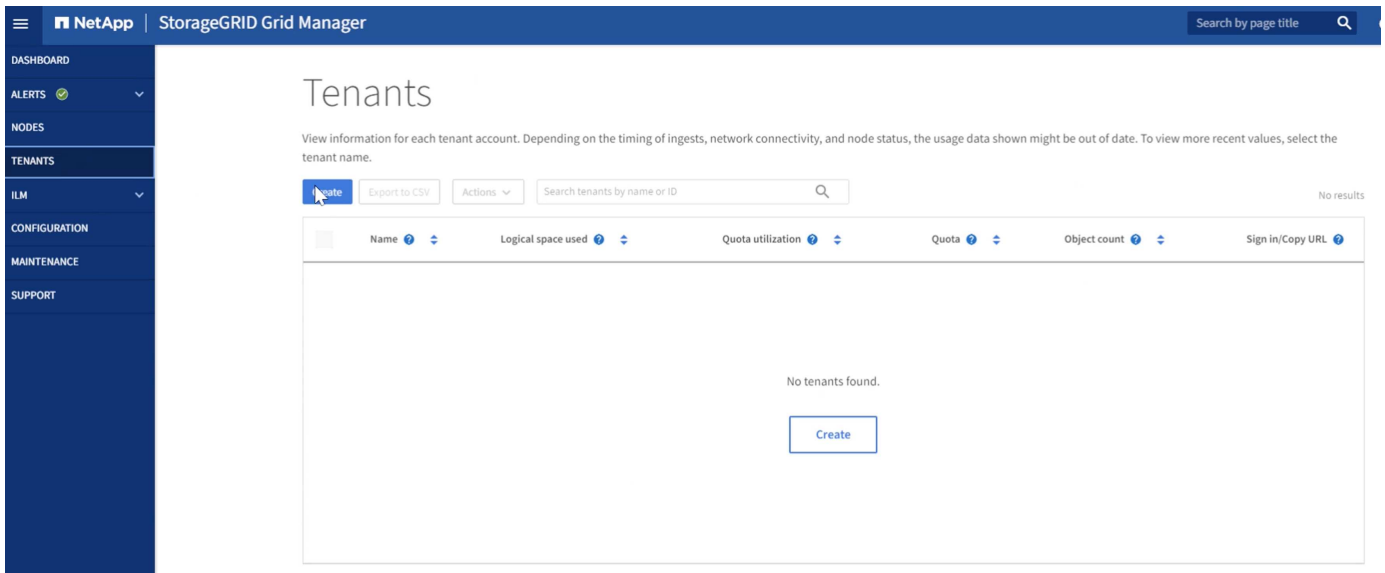
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

正在准备 StorageGRID

继续配置此演示、我们将创建租户、用户、安全组、组策略和存储分段。

创建租户

导航到"租户"选项卡、然后单击"创建"按钮

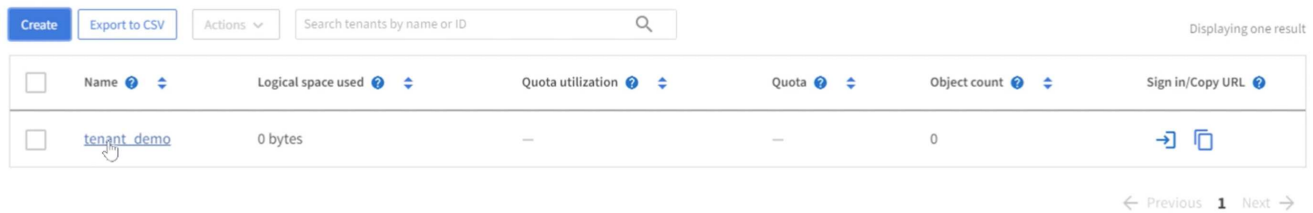


填写提供租户名称的租户的详细信息、选择S3作为客户端类型、不需要配额。无需选择平台服务或允许S3选择。如果选择、您可以选择使用自己的身份源。设置root密码、然后单击完成按钮。

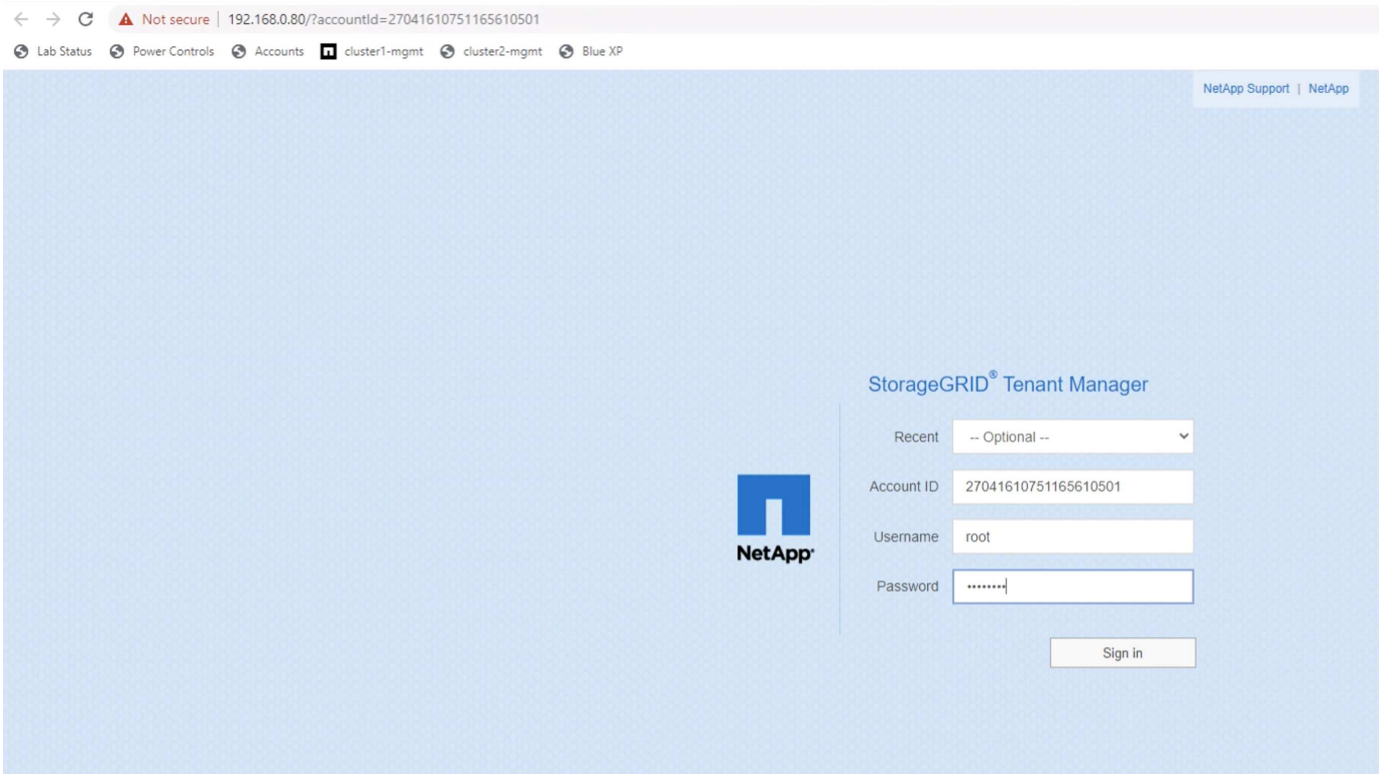
单击租户名称可查看租户详细信息。稍后您将需要租户ID、因此请将其复制。单击登录按钮。此操作将转到租户门户登录页面。保存此URL以供将来使用。

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

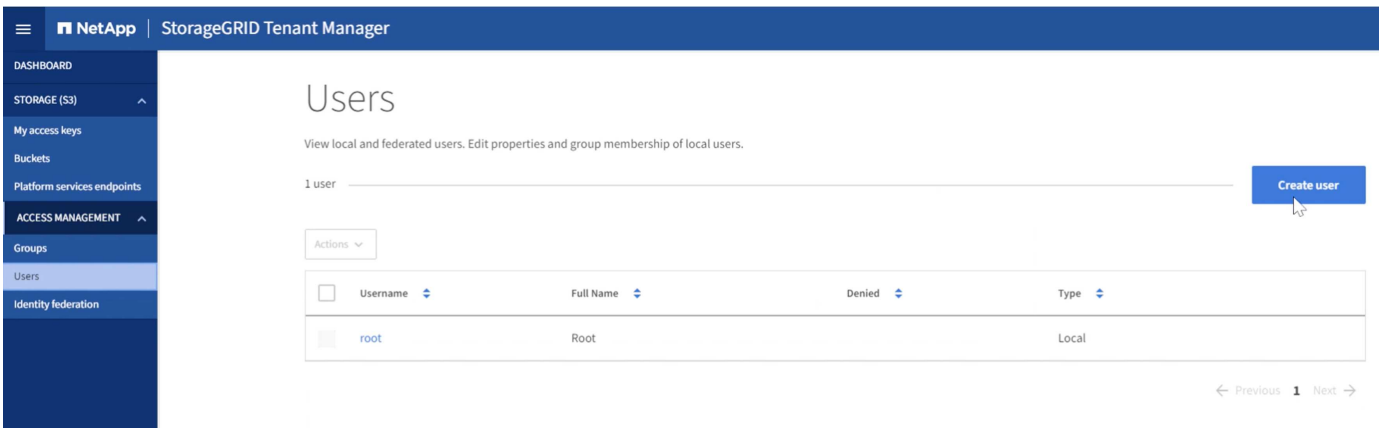


此操作将转到租户门户登录页面。保存此URL以供将来使用、然后输入root用户凭据。



创建用户

导航到用户选项卡并创建新用户。



Enter user credentials

Create a new local user and configure user access.

Full name 

Must contain at least 1 and no more than 128 characters

Username 

Password



Must contain at least 8 and no more than 32 characters

Confirm password



Deny access

Do you want to prevent this user from signing in regardless of assigned group permissions?



Yes



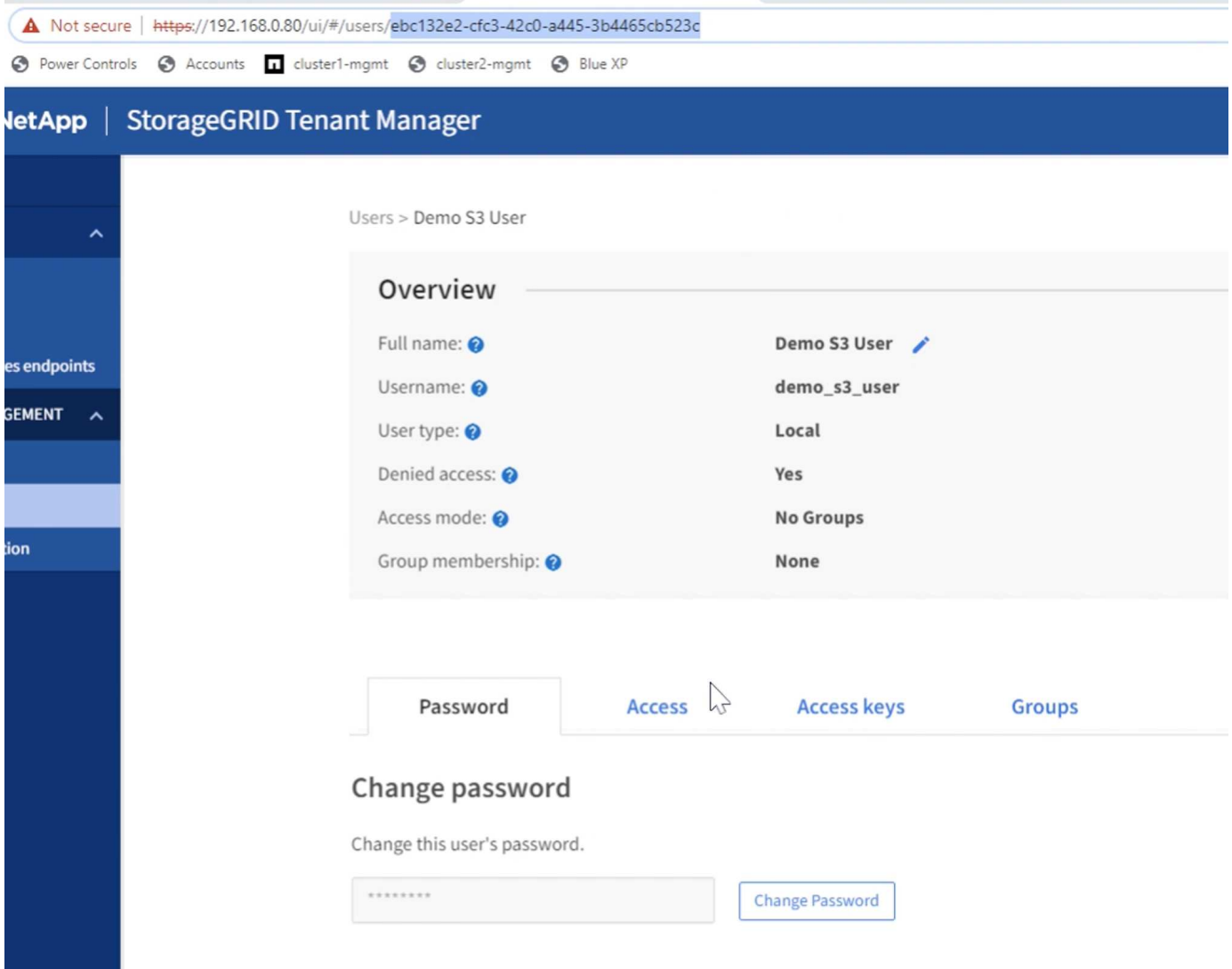
No

[Cancel](#)

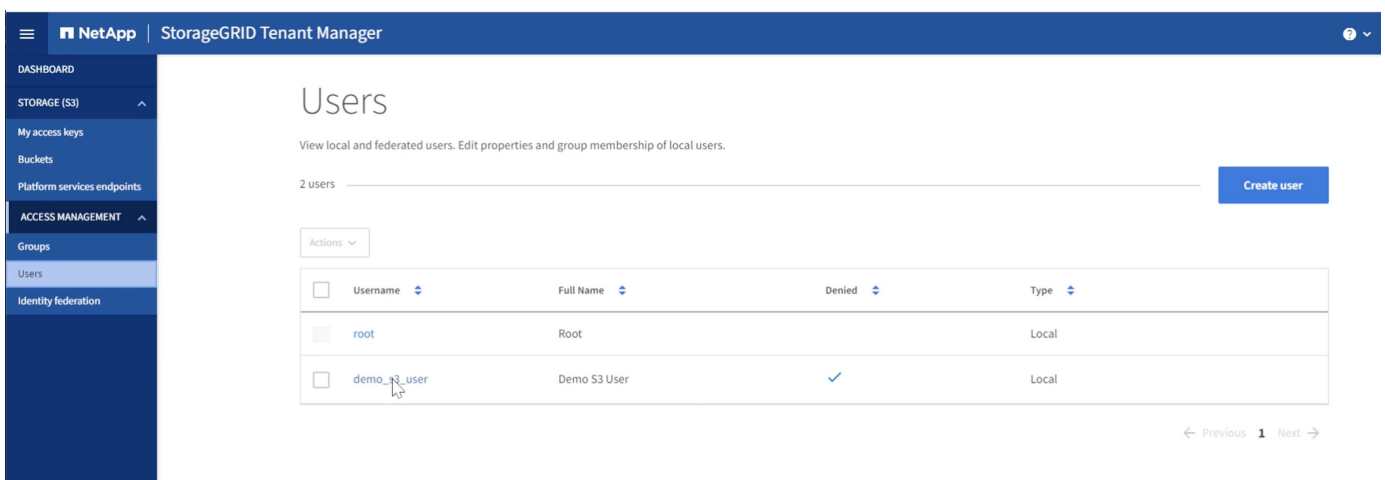
[Continue](#)

创建新用户后、单击用户名以打开该用户的详细信息。

复制URL中的用户ID、以供日后使用。



要创建S3密钥、请单击用户名。



选择"Access keys"(访问密钥)选项卡、然后单击"Create Key"(创建密钥)按钮。无需设置到期时间。下载S3密钥、因为关闭窗口后将无法再次检索这些密钥。

Create access key



1 Choose expiration time ————— 2 Download access key

Download access key

To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.

 You will not be able to view the Access key ID or Secret access key after you close this dialog.

Access key ID

7CT7L1X5MIO5091E86TR



Secret access key

RIJnC5N5FX9RSWgFdj6SQ7wMrFRZYu5bQLdNQT0c



 Download .csv

Finish

创建安全组

现在转到组页面并创建新组。

Create group ✕

- 1 Choose a group type
- 2 Manage permissions
- 3 Set S3 group policy
- 4 Add users
Optional

Choose a group type ?

Create a new local group or import a group from the external identity source.

Local group **Federated group**

Create local groups to assign permissions to any local users you defined in StorageGRID.

Display name

Must contain at least 1 and no more than 32 characters

Unique name ?

[Cancel](#) [Continue](#)

将组权限设置为只读。这是租户UI权限、而不是S3权限。

1 Choose a group type — 2 **Manage permissions** — 3 Set S3 group policy — 4 Add users
Optional

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode ?

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write Read-only

Group permissions ?

Select the permissions you want to assign to this group.

Root access
Allows users to access all administration features. Root access permission supersedes all other permissions.

Manage all buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.

Manage endpoints
Allows users to configure endpoints for platform services.

Manage your own S3 credentials
Allows users to create and delete their own S3 access keys.

[Previous](#) [Continue](#)

S3权限通过组策略(IAM策略)进行控制。将组策略设置为自定义、然后将json策略粘贴到框中。此策略将允许此组的用户列出租户的分段、并在名为"分段"的分段中执行任何S3操作、或者在名为"分段"的分段中执行子文件夹。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": ["arn:aws:s3:::bucket", "arn:aws:s3:::bucket/*"]
    }
  ]
}

```

×

Create group

✓ Choose a group type
✓ Manage permissions
3 Set S3 group policy
 4 Add users
Optional

Set S3 group policy ?

An S3 group policy controls user access permissions to specific specific S3 resources, including buckets. Non-root users have no access by default.

No S3 Access

Read Only Access

Full Access

Custom
(Must be a valid JSON formatted string.)

```

"Effect": "Allow",
"Action": "s3:ListAllMyBuckets",
"Resource": "arn:aws:s3::*"
},
{
  "Effect": "Allow",
  "Action": "s3:*",
  "Resource": ["arn:aws:s3:::bucket", "arn:aws:s3:::bucket/*"]
}
]
}

```

Previous
Continue

最后、将用户添加到组中并完成操作。

Create group

Choose a group type
 Manage permissions
 Set S3 group policy
 4 Add users Optional

Add users

(This step is optional. If required, you can save this group and add users later.)

Select local users to add to the group **Demo S3 Group**.

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	demo_s3_user	Demo S3 User	<input checked="" type="checkbox"/>

[Previous](#)
 [Create group](#)

创建两个存储分段

导航到存储分段选项卡、然后单击创建存储分段按钮。

NetApp | StorageGRID Tenant Manager

Buckets

Create buckets and manage bucket settings.

0 buckets [Create bucket](#)

Experimental S3 Console

Name	Region	Object Count	Space Used	Date Created
No buckets found				

[Create bucket](#)

定义分段名称和区域。

Create bucket ✕

1 Enter details 2 Manage object settings
Optional

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

Region ?

[Cancel](#) [Continue](#)

在第一个存储分段上启用版本控制。

Create bucket ✕

✓ Enter details 2 Manage object settings
Optional

Manage object settings Optional

Object versioning

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed.

Enable object versioning

[Previous](#) [Create bucket](#)

现在、在未启用版本控制的情况下创建第二个存储分段。

Create bucket ×

1 Enter details 2 Manage object settings
Optional

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

Region ?

Cancel

Continue

请勿在此第二个存储分段上启用版本控制。

Create bucket ×

✓ Enter details 2 Manage object settings
Optional

Manage object settings Optional

Object versioning

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed.

Enable object versioning

Previous

Create bucket

作者：拉斐尔·吉德斯和阿伦·克莱因

通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3


通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

填充源存储分段

让我们将一些对象放在源ONTAP分段中。我们将使用S3Browser进行此演示、但您可以使用您熟悉的任何工具。

使用上面创建的ONTAP用户S3密钥、将S3Browser配置为连接到ONTAP系统。

Add New Account online help

 **Add New Account**
Enter new account details and click Add new account

Display name:

Assign any name to your account.

Account type:

Choose the storage you want to work with. Default is Amazon S3 Storage.

REST Endpoint:

Specify S3-compatible API endpoint. It can be found in storage documentation. Example: rest.server.com:8080

Access Key ID:

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

Secret Access Key:

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

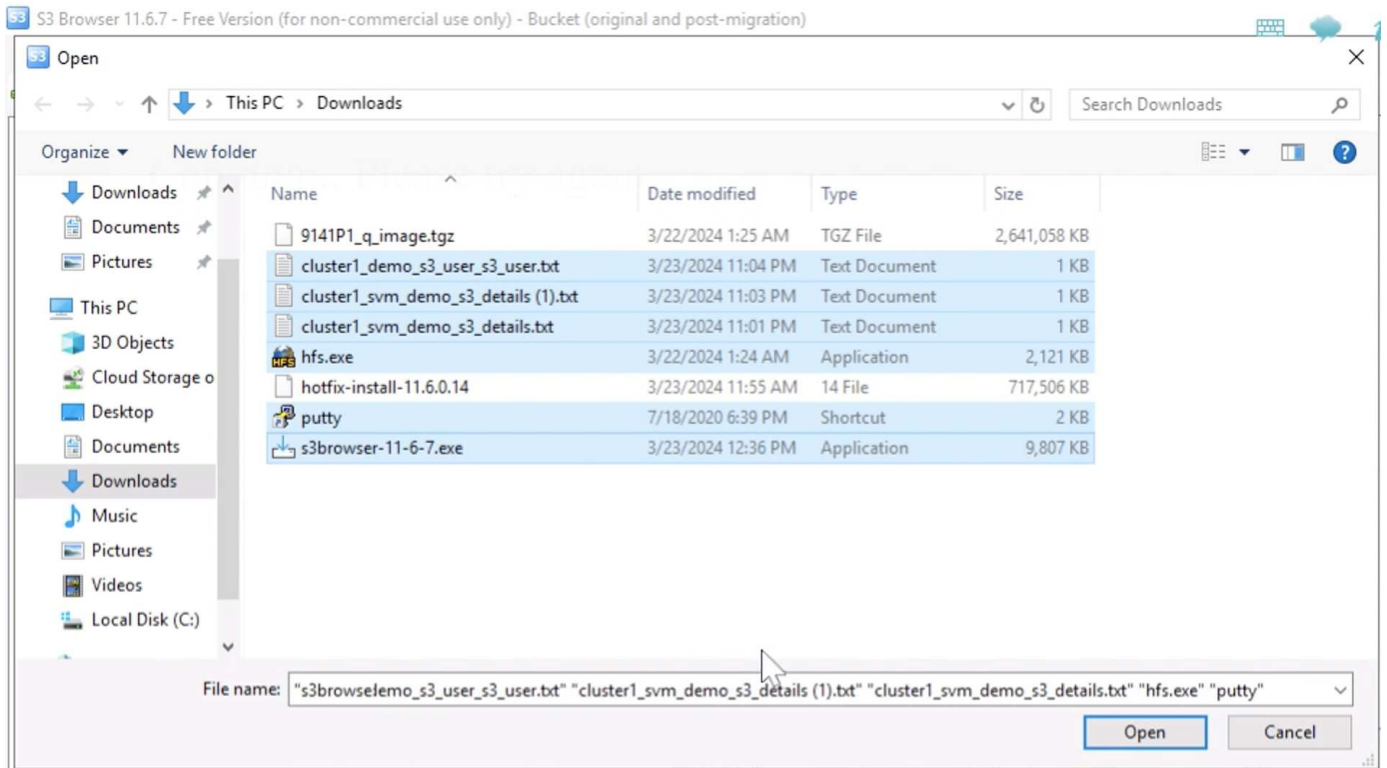
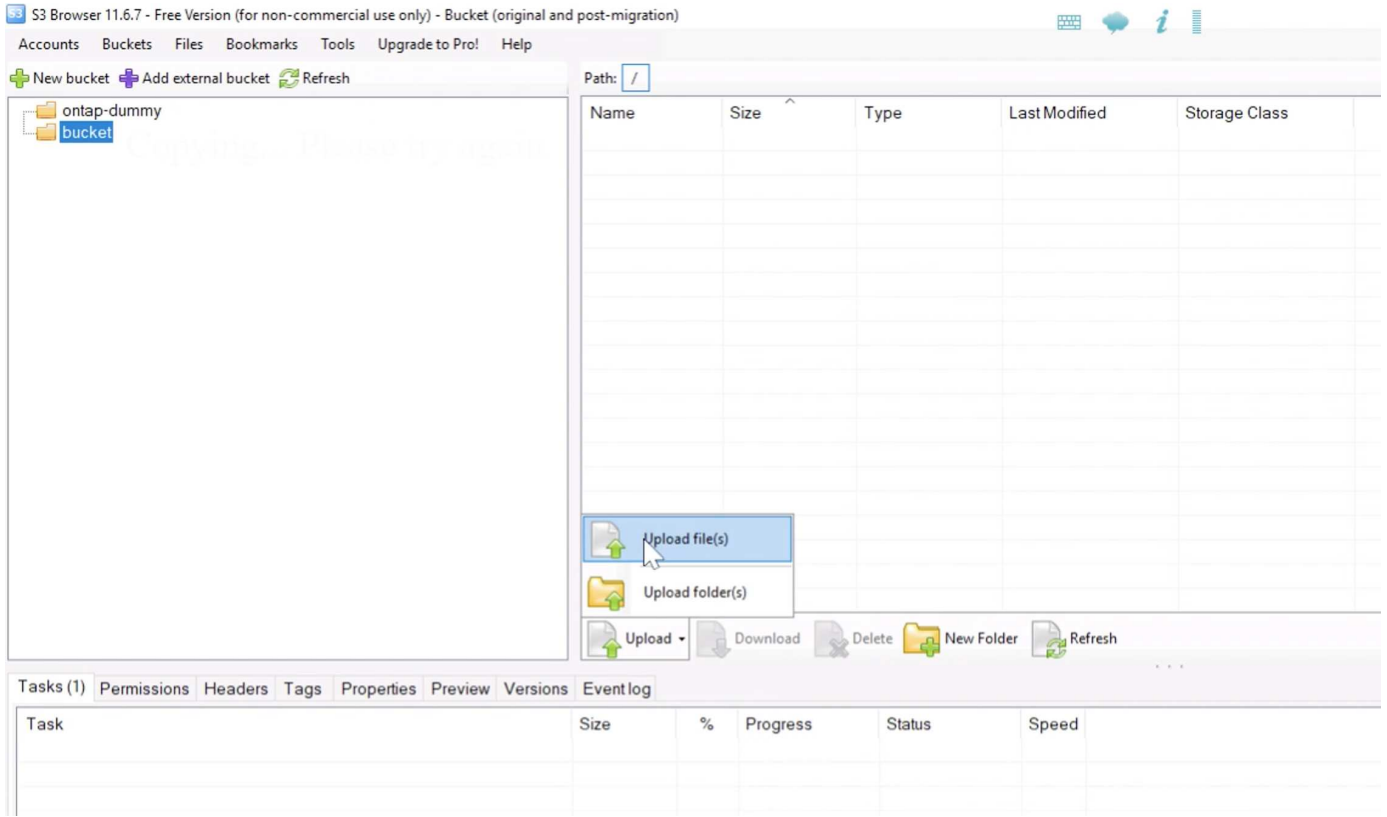
Encrypt Access Keys with a password:

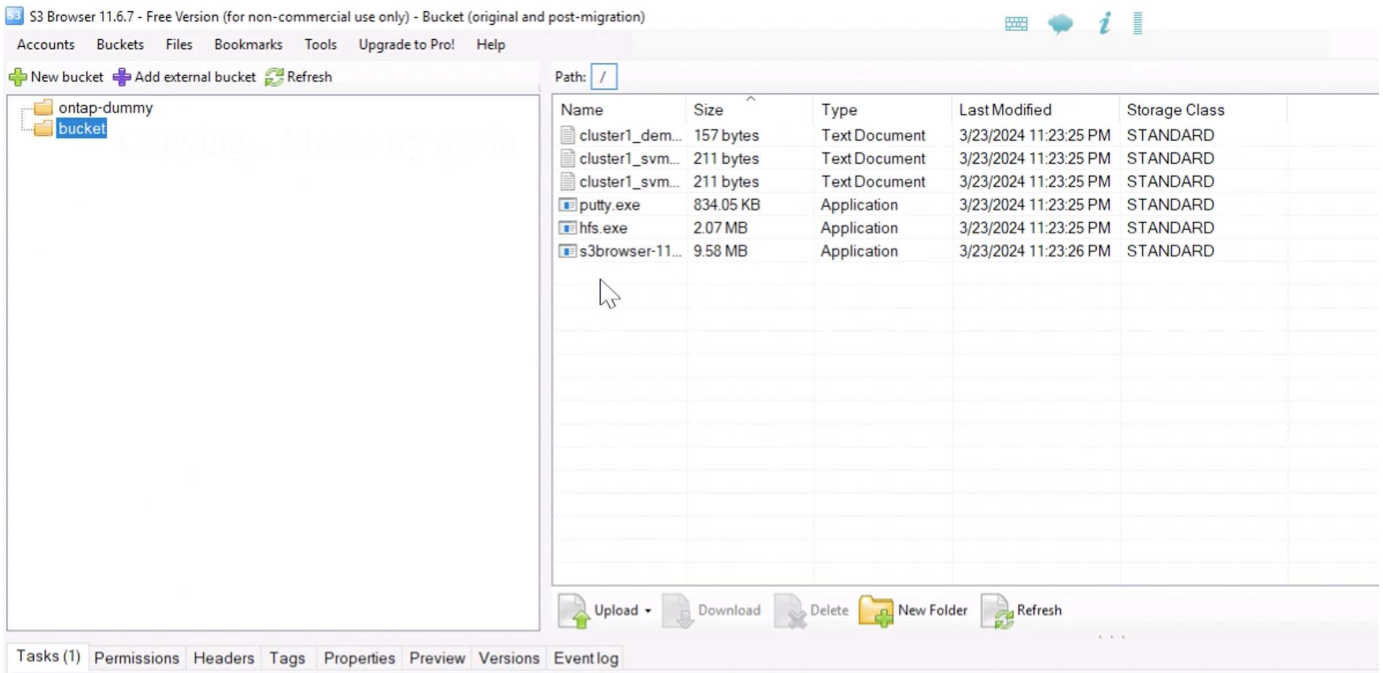
Turn this option on if you want to protect your Access Keys with a master password.

Use secure transfer (SSL/TLS)
If checked, all communications with the storage will go through encrypted SSL/TLS channel

[advanced settings..](#)

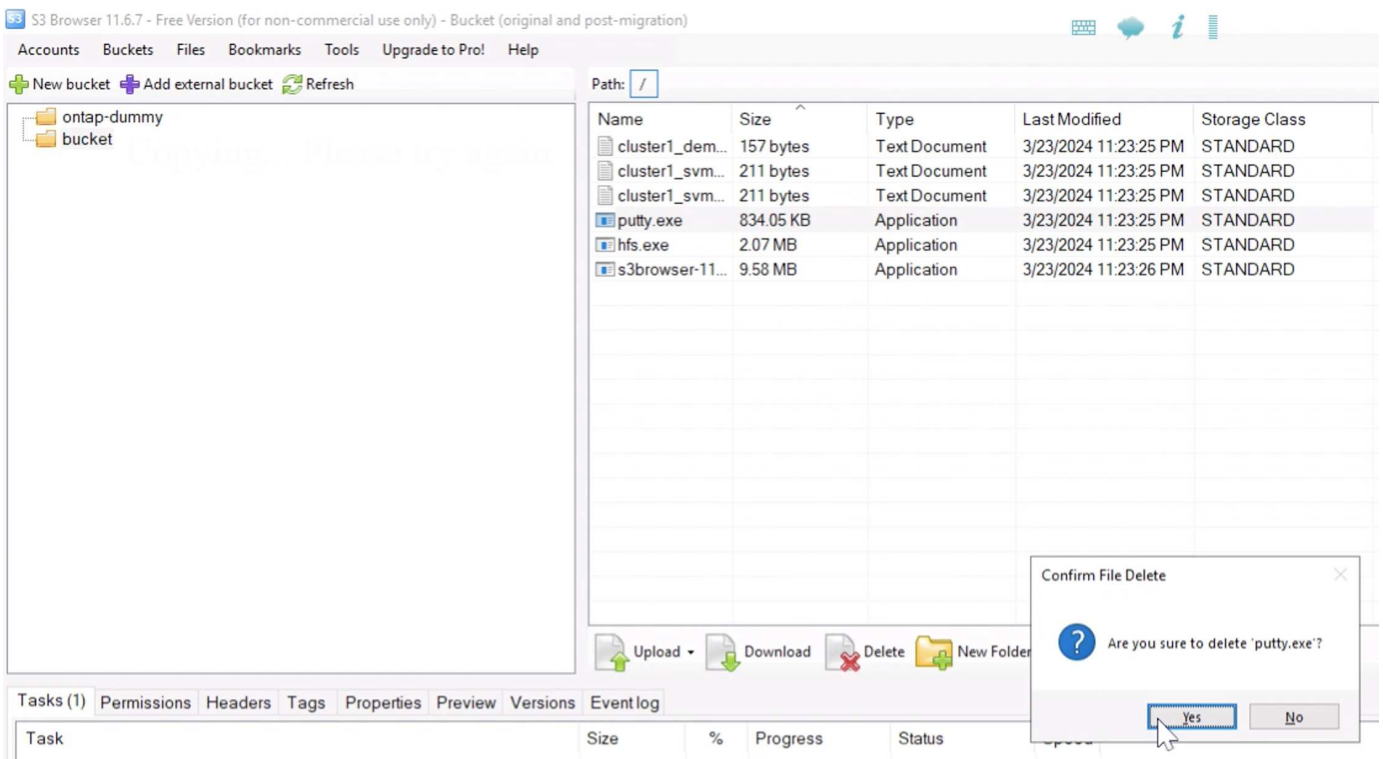
现在、我们将一些文件上传到启用了版本控制的存储分段。



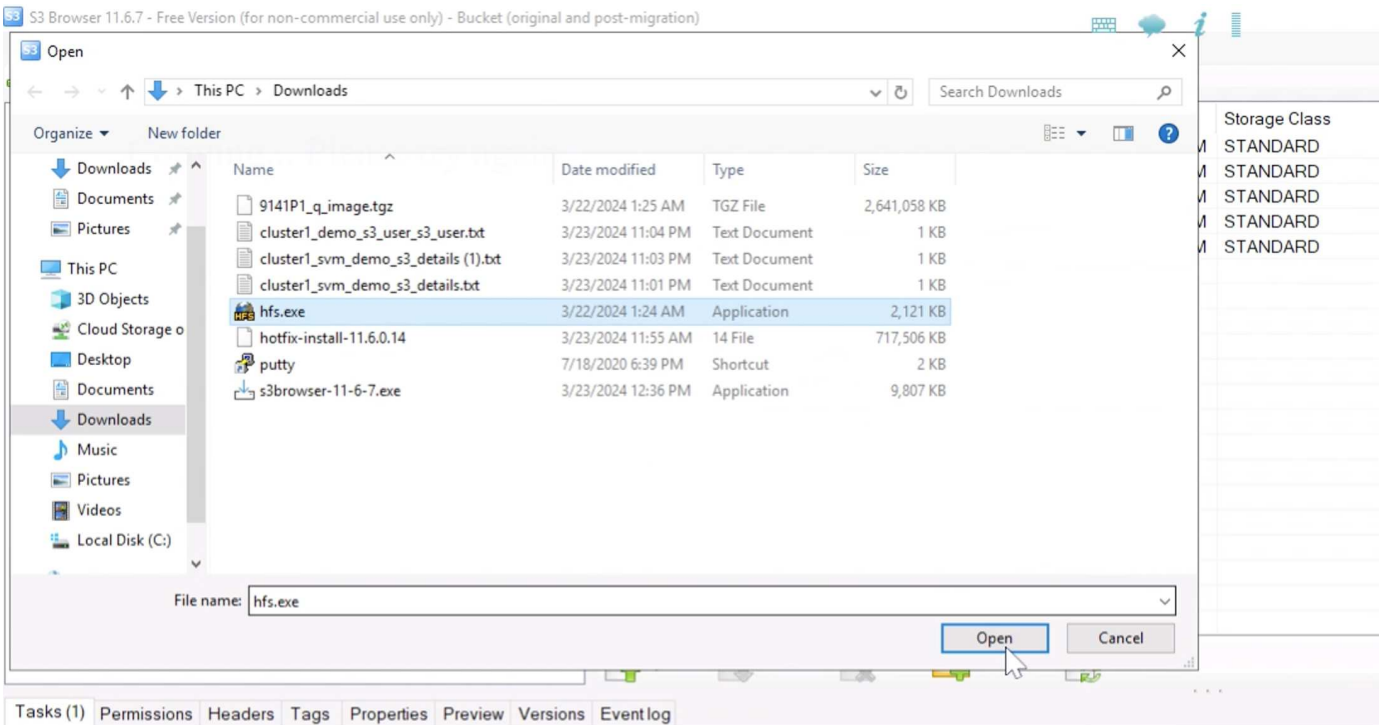


现在、让我们在分段中创建一些对象版本。

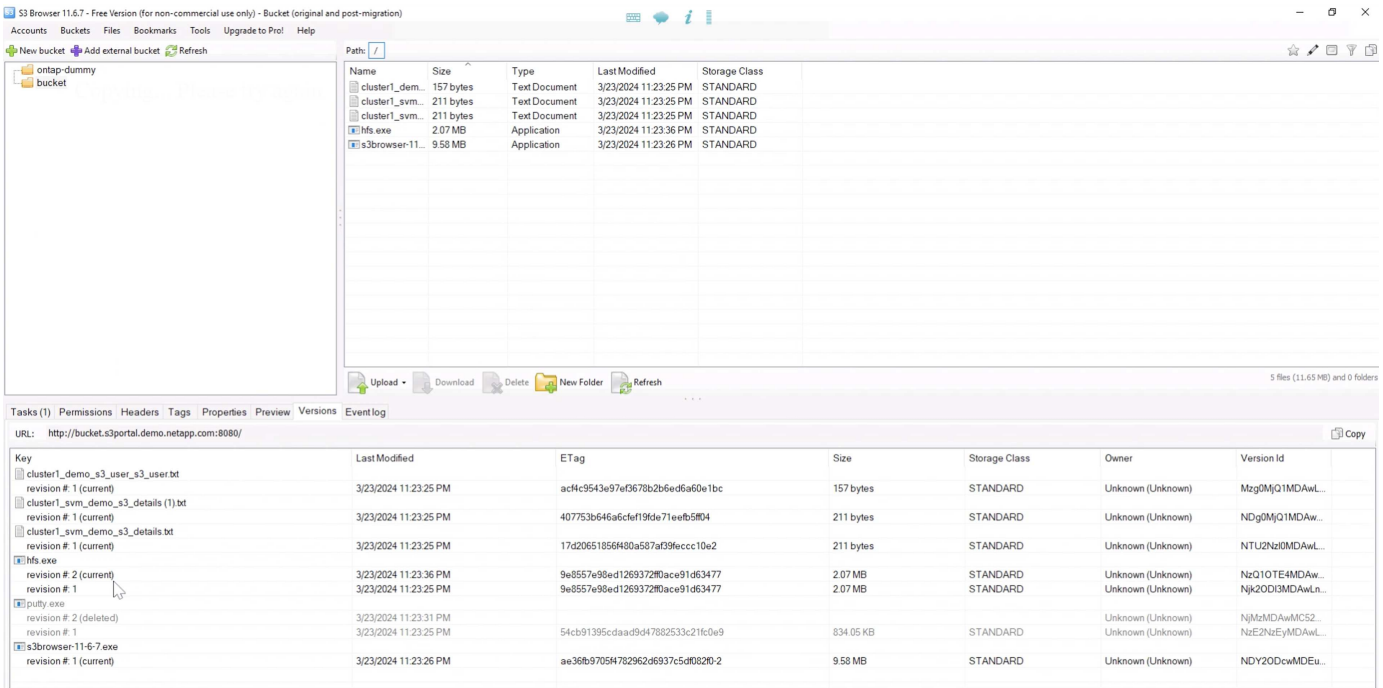
删除文件。



上传存储分段中已存在的文件以复制该文件并创建其新版本。



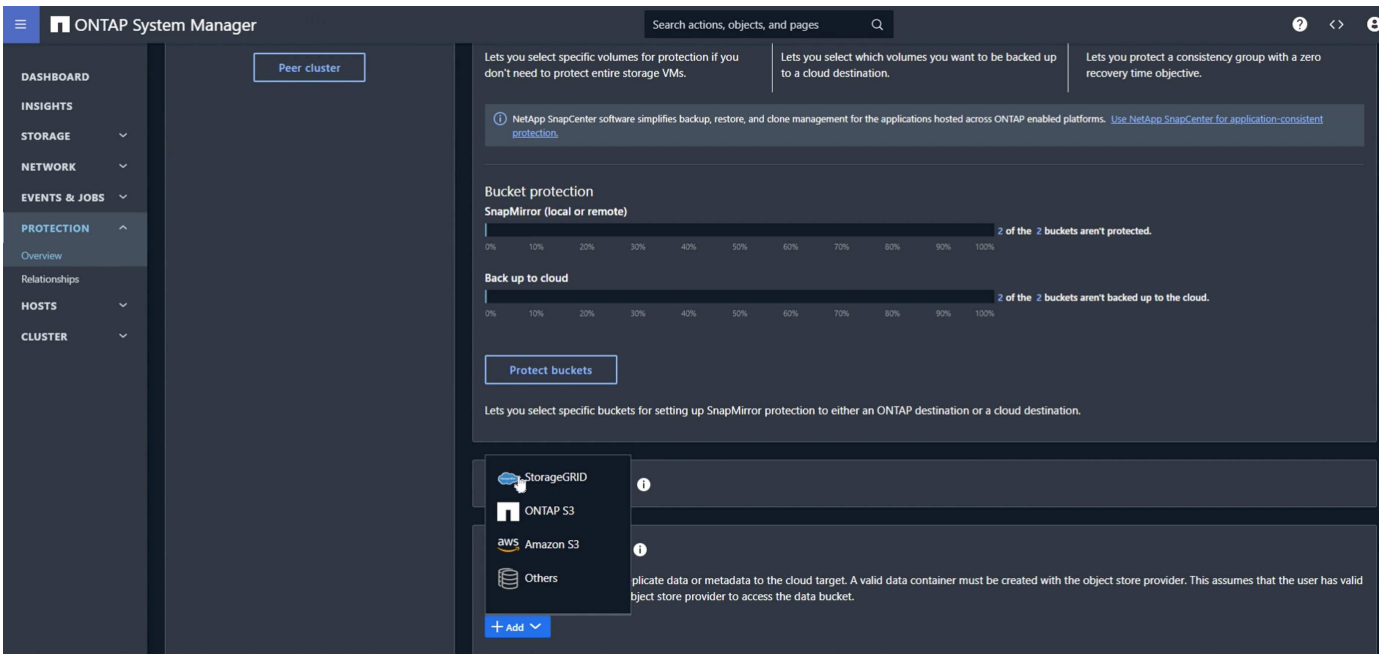
在S3Browser中、我们可以查看刚刚创建的对象版本。



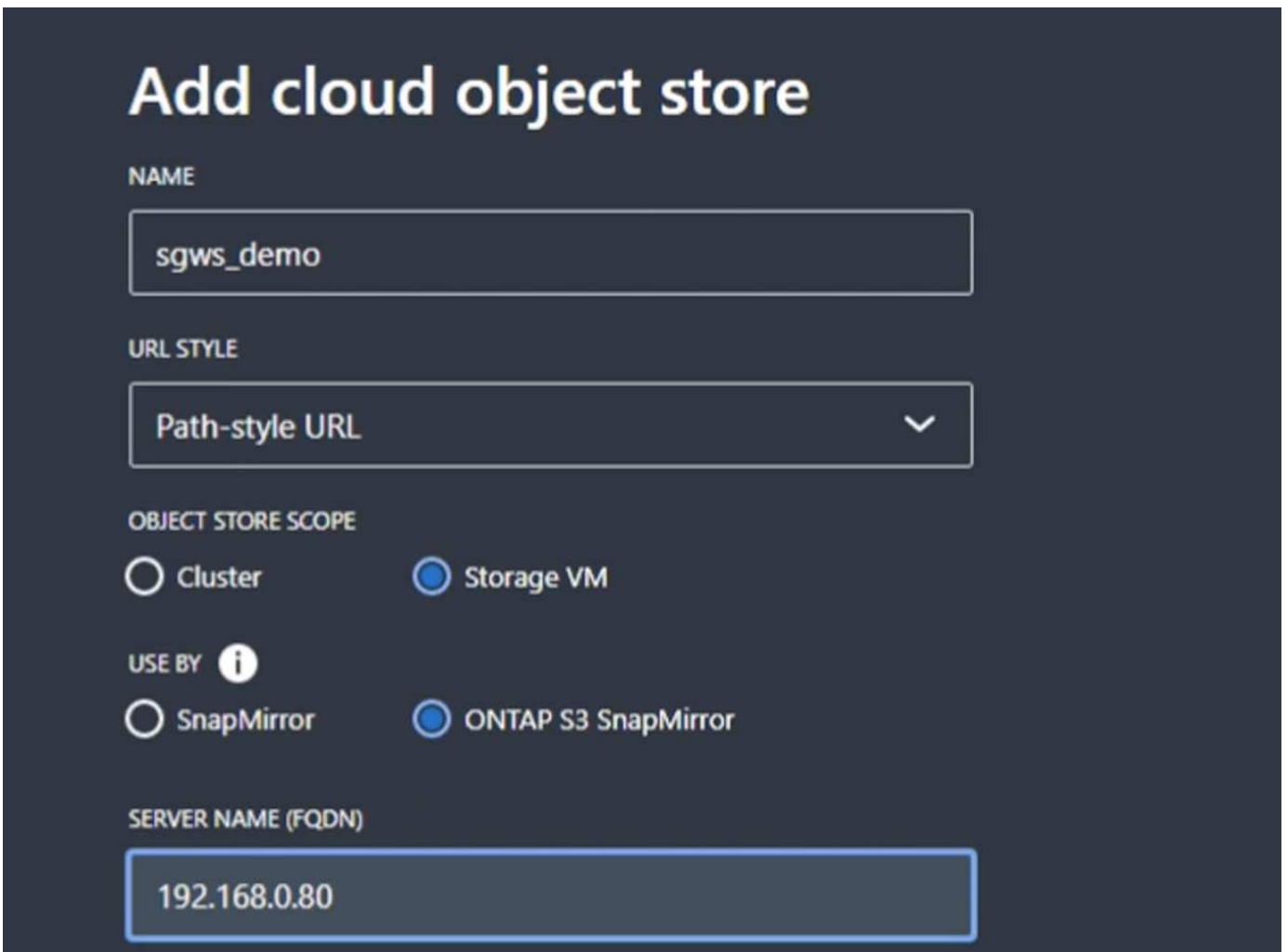
建立复制关系

让我们开始将数据从ONTAP发送到StorageGRID。

在ONTAP系统管理器中、导航到"保护/概述"。向下滚动到"Cloud object stores"(云对象存储)、然后单击"Add"(添加)按钮并选择StorageGRID (添加)。



通过提供名称和URL样式来输入StorageGRID信息(在此演示中、我们将使用Path-styleURL)。将对象存储范围设置为"Storage VM"。



如果您使用的是SSL、请设置负载均衡器端口并在此处复制StorageGRID端口证书。否则、请取消选

中"SSP"框并在此处输入HTTP端点端口。

为目标输入上述StorageGRID配置中的StorageGRID用户S3密钥和存储分段名称。

NODE	IP ADDRESS	SUBNET MASK	BROADCAST DOMAIN	GATEWAY
onPrem-01	192.168.0.113	24	Default	192.168.0.1

Use HTTP proxy

Save Cancel

现在、我们已配置目标、可以为此目标配置策略设置。展开"本地策略设置"、然后选择"持续"。

ONTAP System Manager

Back up to cloud

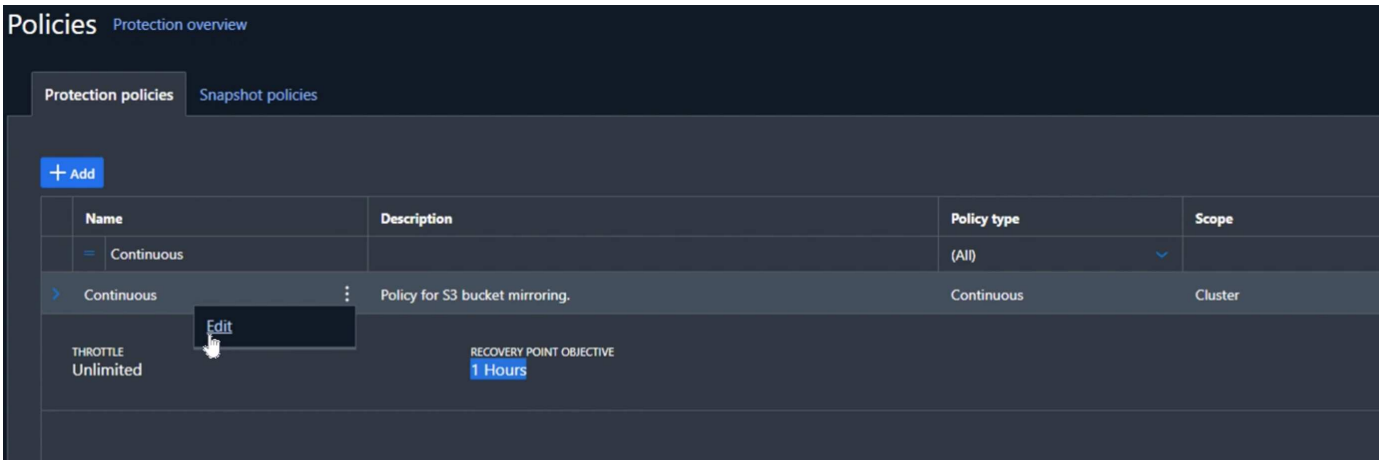
2 of the 2 buckets aren't backed up to the cloud.

Protect buckets

Local policy settings

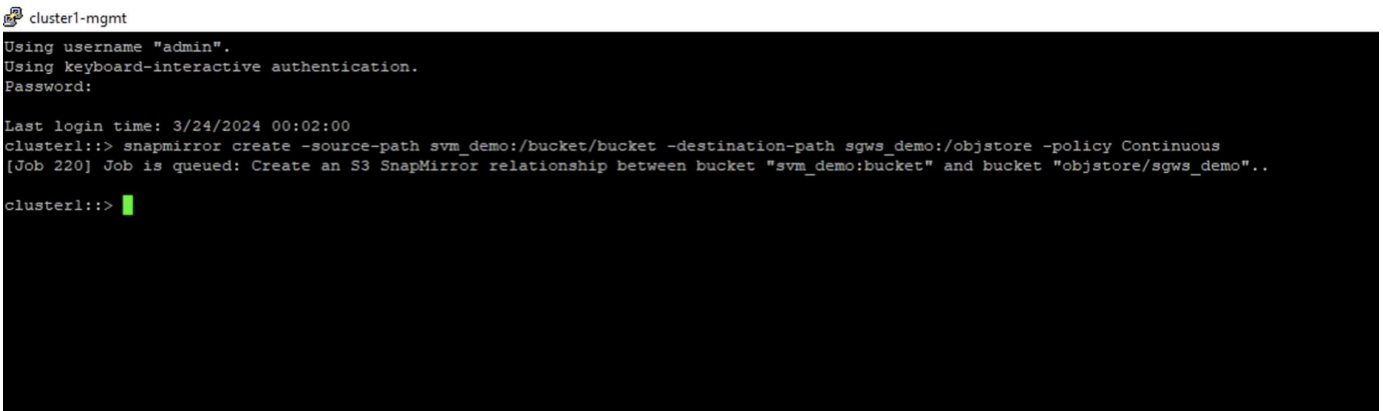
- Protection policies
- Snapshot policies
- Schedules

编辑持续策略并将"恢复点目标"从"1小时"更改为"3秒"。

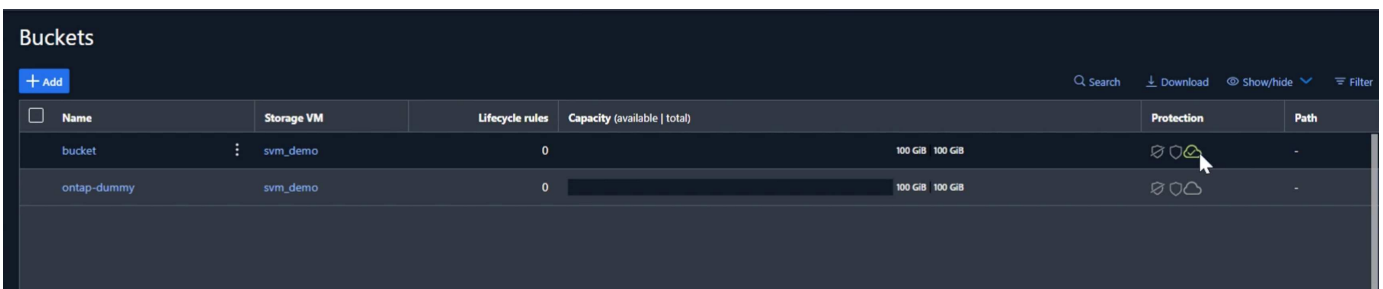


现在、我们可以将SnapMirror配置为复制存储分段。

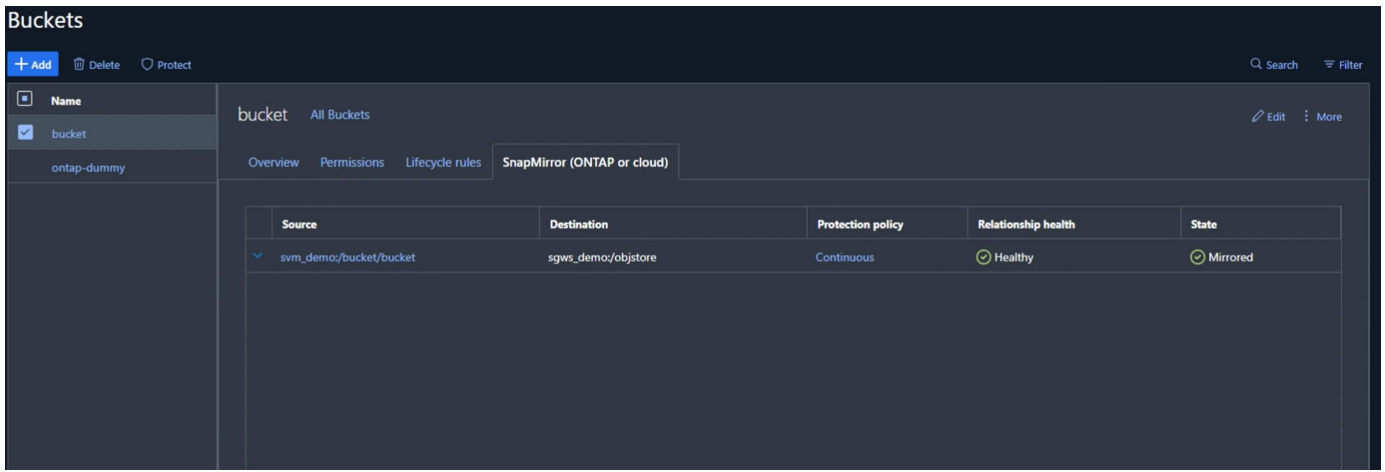
```
SnapMirror create -ssource-path sv_demo: /bket/bket-target-path sgws_demo: /objstore -policy continuous
```



此时、存储分段将在受保护的存储分段列表中显示一个云符号。

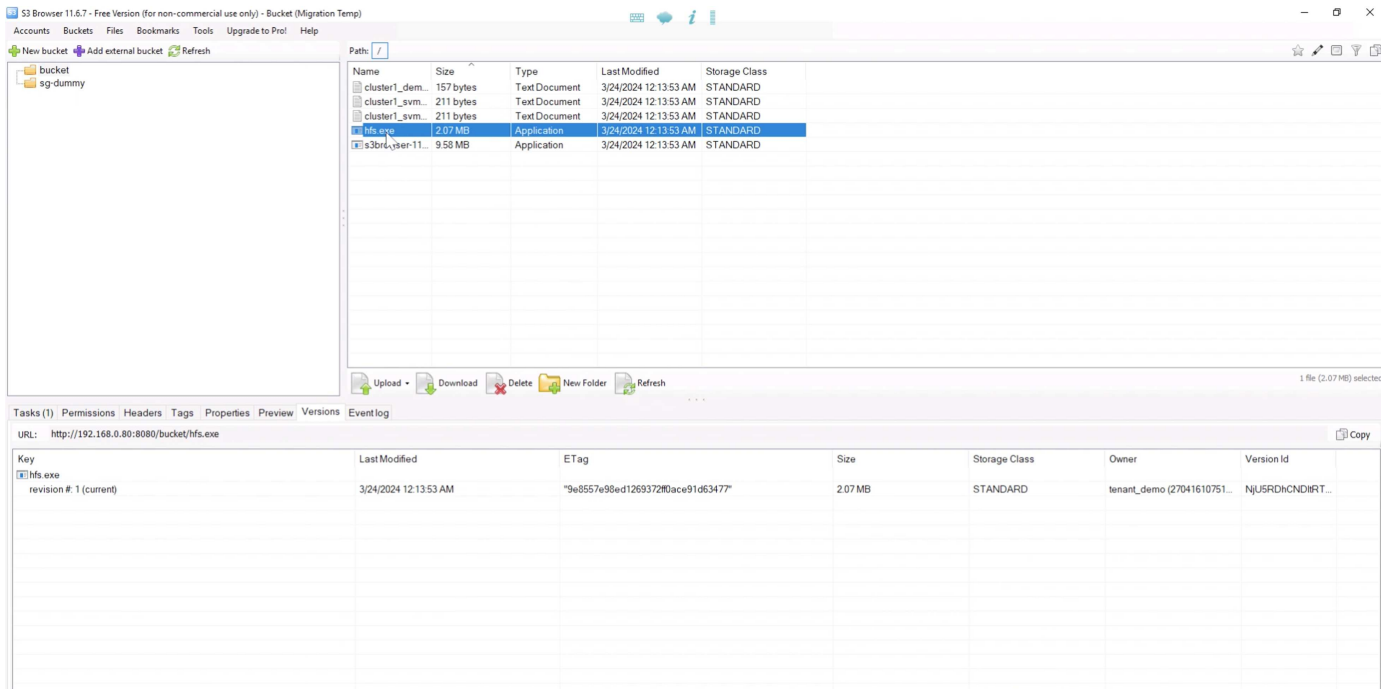


如果我们选择存储分段并转到SnapMirror (ONTAP或云)选项卡、我们将看到SnapMirror relationship状态。

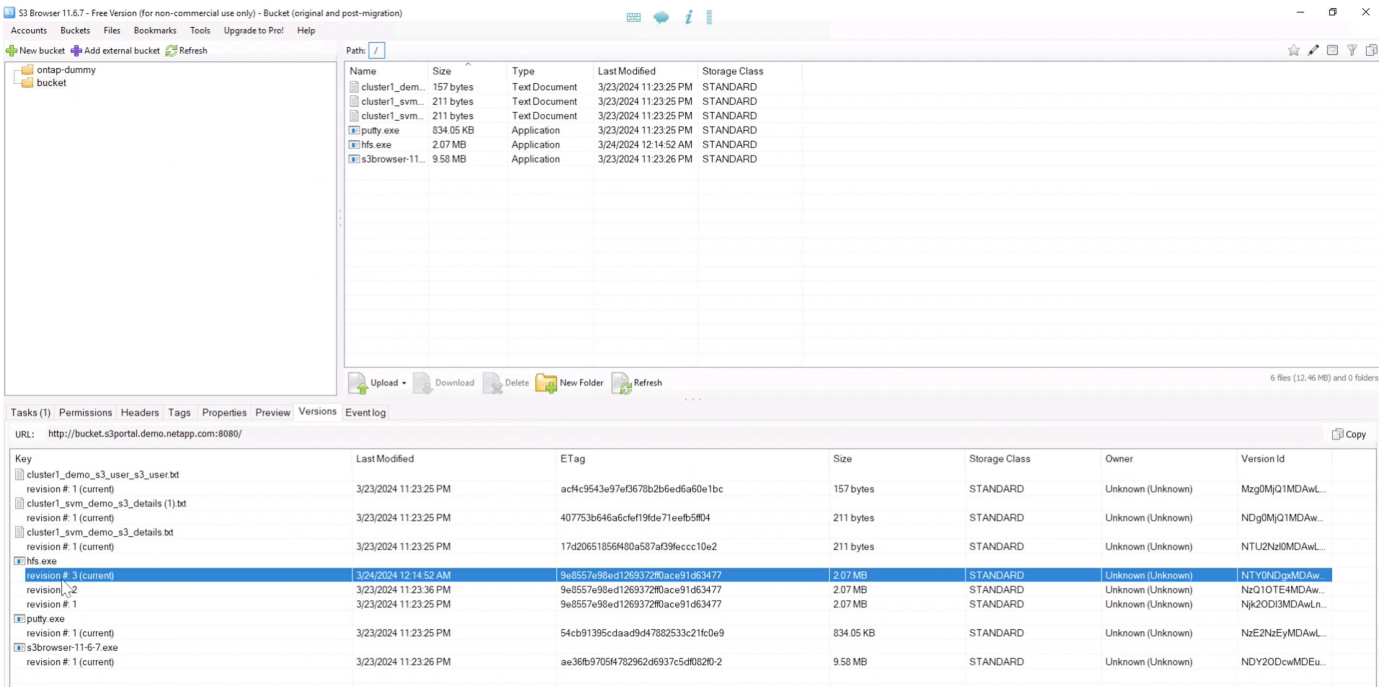


复制详细信息

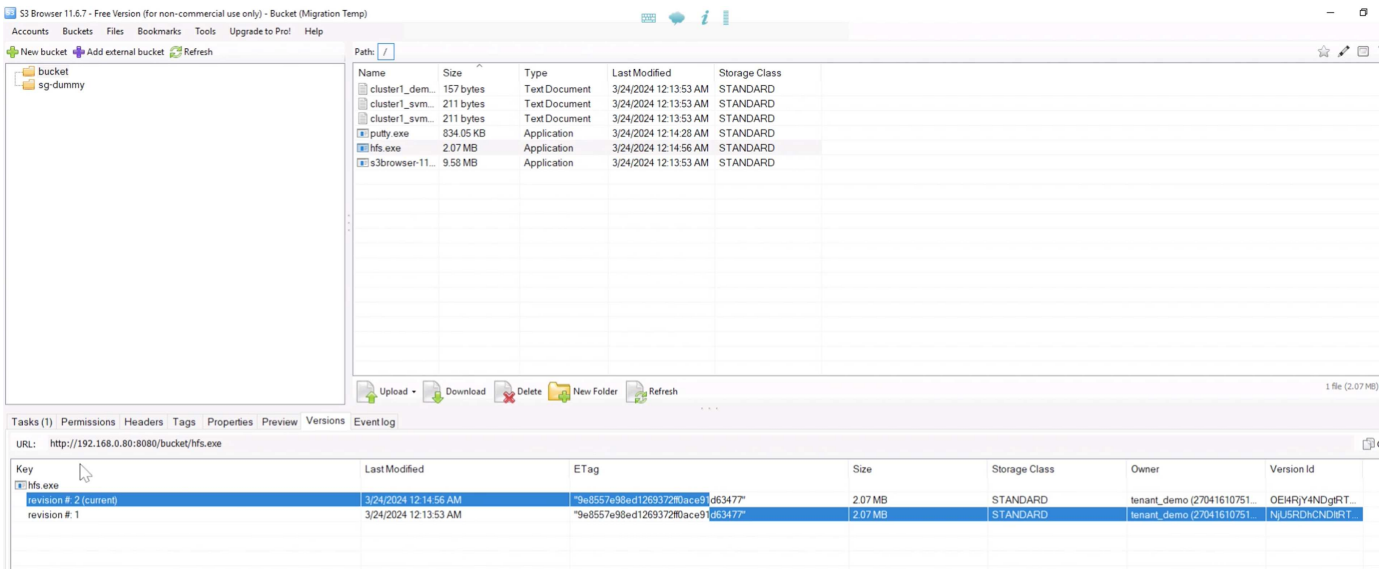
现在、我们已成功将存储分段从ONTAP复制到StorageGRID。但实际上复制的是什么？我们的源和目标都是分版本分段。先前版本是否也会复制到目标？如果我们使用S3Browser查看StorageGRID存储分段、我们会发现现有版本未复制、删除的对象不存在、该对象的删除标记也不存在。我们的复制对象在StorageGRID存储分段中只有1个版本。



在ONTAP分段中、让我们向先前使用的同一对象添加一个新版本、并了解其复制方式。



从StorageGRID的角度来看、我们会发现此存储分段中也创建了一个新版本、但缺少SnapMirror关系之前的初始版本。



这是因为ONTAP SnapMirror S3进程仅复制对象的当前版本。这就是我们在StorageGRID端创建分版本存储分段作为目标的原因。这样、StorageGRID就可以维护对象的版本历史记录。

作者：拉斐尔·吉德斯和阿伦·克莱因

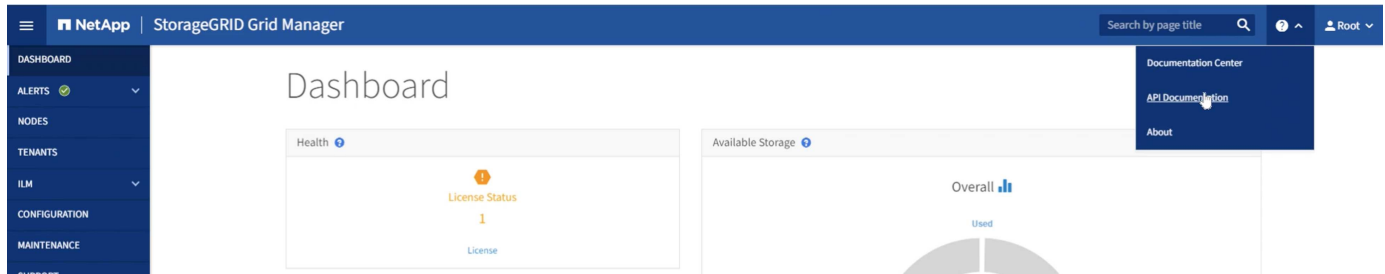
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

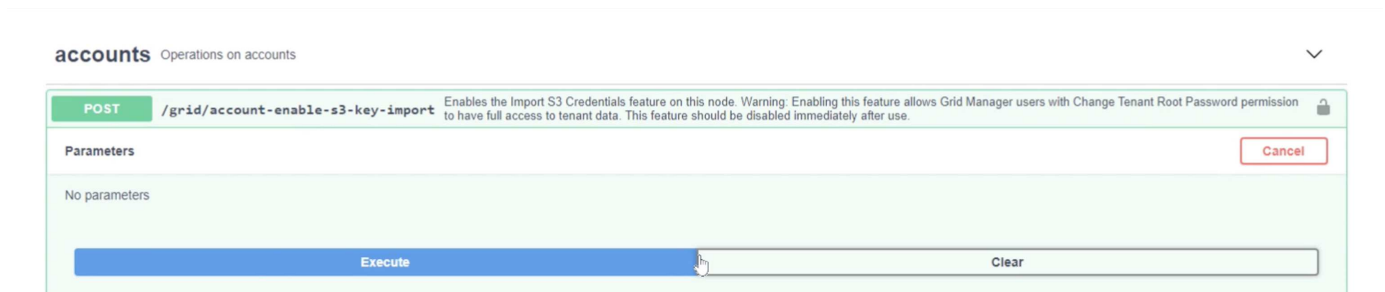
迁移S3密钥

对于迁移、大多数情况下您都需要迁移用户的凭据、而不是在目标端生成新的凭据。StorageGRID提供API以允许将S3密钥导入到用户。

登录到StorageGRID管理UI (而不是租户管理器UI)、打开API文档Swagger页面。



展开"accounts"(帐户)部分、选择"POST /grid /account-enable-s3-key-import "、单击"试用"按钮、然后单击"execute"(执行)按钮。



现在仍在"accounts"下向下滚动到"POST /grid /accounts/ {id} /user/ {user_id} /s3-access-keys"

下面是我们要输入先前收集的租户ID和用户帐户ID的位置。在json框中填写来自我们的ONTAP用户的字段和密钥。您可以设置密钥的到期时间、也可以删除、"Expires": 3456789 "、然后单击"执行"。

POST /grid/accounts/{id}/users/{user_id}/s3-access-keys Imports S3 credentials for a given user in a tenant account

Parameters

Name	Description
id * required string (path)	ID of Storage Tenant Account <input type="text" value="27041610751165610501"/>
user_id * required string (path)	ID of user in tenant account. <input type="text" value="ebc132e2-cfc3-42c0-a445-3b4465cb523c"/>
body * required (body)	Edit Value Model <pre>{ "accessKey": "3IVPI142JGE3Y7FV2KC0", "secretAccessKey": "75a1QqKBU4quA132twI4g41C4Gg5PP30ncy0sPE8" }</pre>

完成所有用户密钥导入后、您应在"accounts""POST /grid /account-disable" s3-key-import"中禁用密钥导入功能

POST /grid/account-disable-s3-key-import Disables the Import S3 Credentials feature on this node.

Parameters Cancel

No parameters

Execute

Responses Response content type: application/json

如果我们在租户管理器UI中查看用户帐户、可以看到新密钥已添加。

Overview

Full name: ?	Demo S3 User
Username: ?	demo_s3_user
User type: ?	Local
Denied access: ?	Yes
Access mode: ?	Read-only
Group membership: ?	Demo S3 Group

Password Access **Access keys** Groups

Manage access keys

Add or delete access keys for this user.

[Create key](#) Actions ▾

<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****86TR	None
<input type="checkbox"/>	*****2KC0	None

最终转换

如果打算永久将存储分段从ONTAP复制到StorageGRID、您可以到此结束。如果是从ONTAP S3迁移到StorageGRID、则需要结束迁移并进行转换。

在ONTAP系统管理器中、编辑S3组并将其设置为"ReadOnlyAccess"。这将防止用户再向ONTAP S3存储分段写入数据。

Edit group ✕

NAME

USERS

POLICIES

Cancel Save

只需将DNS配置为从ONTAP集群指向StorageGRID端点即可。请确保端点证书正确无误、如果需要虚拟托管模式请求、请在StorageGRID中添加端点域名

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1 +

您的客户端需要等待TTL过期、或者刷新DNS以解析到新系统、以便您可以测试一切正常。剩下的只是清理用于测试StorageGRID数据访问的初始临时S3密钥(而不是导入的密钥)、删除SnapMirror关系、然后删除ONTAP数据。

作者：拉斐尔·吉德斯和阿伦·克莱因

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。