



# **Migrating object-based storage from ONTAP S3 to StorageGRID**

StorageGRID solutions and resources

NetApp  
December 12, 2025

# Table of Contents

- Migrating object-based storage from ONTAP S3 to StorageGRID. . . . . 1
  - Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID . . . . . 1
    - Migration Demo . . . . . 1
  - Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID . . . . . 1
    - Preparing ONTAP . . . . . 1
  - Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID . . . . . 13
    - Preparing StorageGRID . . . . . 13
  - Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID . . . . . 25
    - Populate the Source Bucket. . . . . 25
  - Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID . . . . . 34
    - Migrate S3 Keys. . . . . 35

# Migrating object-based storage from ONTAP S3 to StorageGRID

## Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

### Migration Demo

This is a demonstration on migrating users and buckets from ONTAP S3 to StorageGRID.

## Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

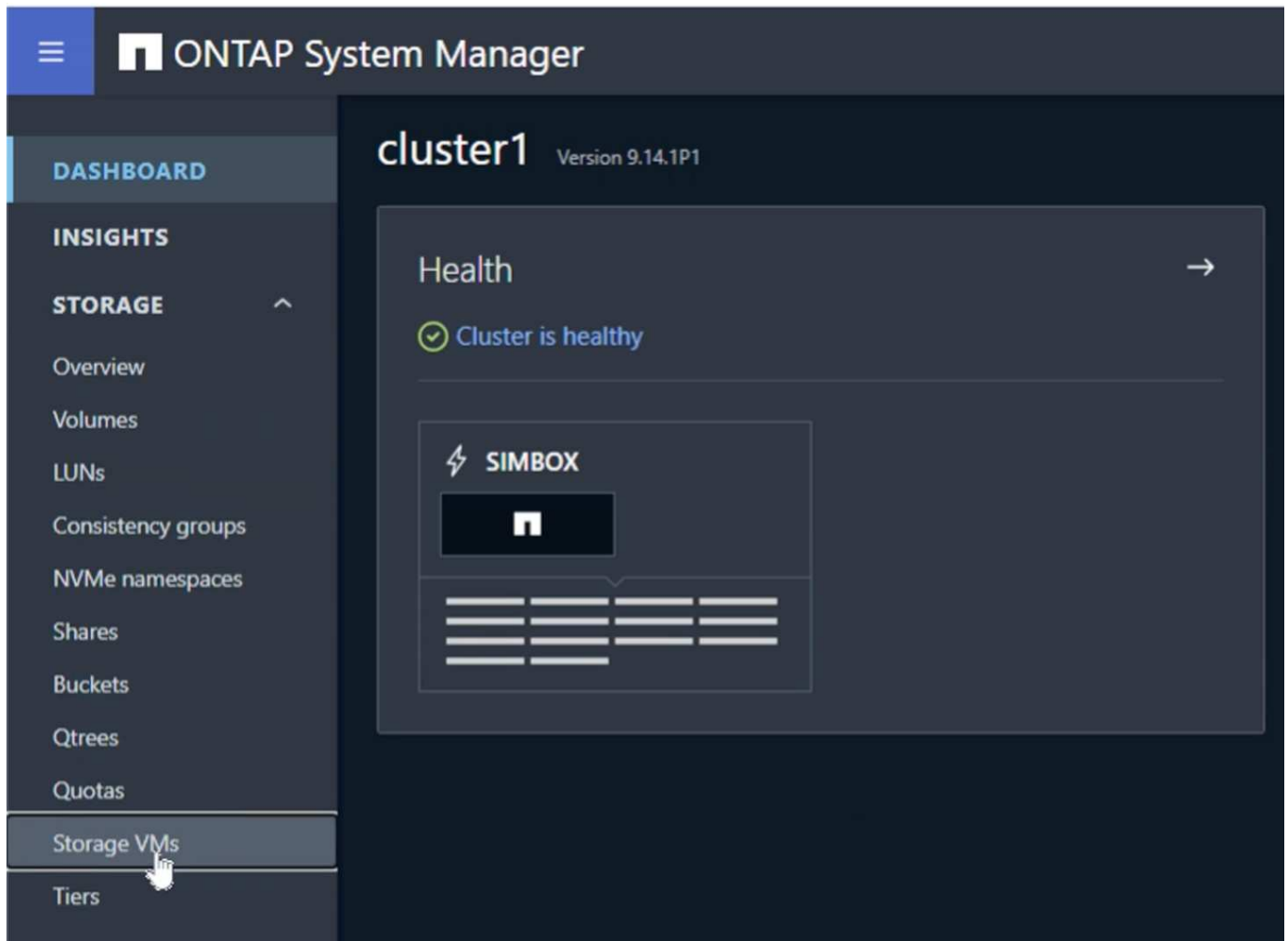
Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

### Preparing ONTAP

For demonstration purposes we will create an SVM object store server, user, group, group policy and buckets.

#### Create the Storage Virtual Machine

In ONTAP System Manager, navigate to Storage VM's and add a new storage VM.



Select the "Enable S3" and "Enable TLS" check boxes and configure the HTTP(S) ports. Define the IP, subnet mask and define the gateway and broadcast domain if not using the default or required in your environment.

## 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

As part of the SVM creation a user will be created. Download the S3 keys for this user and close the window.

## 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

Once the SVM has been created, edit the SVM and add the DNS settings.



## Services


NIS



Not configured

Name service switch



Services lookup order 

HOSTS

Files, then DNS

GROUP

Files



NAME MAP

Files

NETGROUP

Files

DNS



Not configured

Define the DNS name and IP.

**Add DNS domain** ✕

DNS domains

demo.netapp.com

+ Add

Name servers

192.168.0.253

+ Add










Cancel

Cancel **Save**

#### Create SVM S3 User

Now we can configure the S3 users and group. Edit the S3 settings.

## Protocols

<b>NFS</b> Not configured	 	<b>SMB/CIFS</b> Not configured	 	<b>iSCSI</b> Not configured
<b>NVMe</b> Not configured	 	<b>S3</b> STATUS  Enabled TLS Disabled HTTP Enabled	 	

Add a new user.



Storage VMs

[+ Add](#) [More](#)

☒ Name

☒ svm\_demo

S3 [All settings](#)

☒ Enabled

Server [Edit](#)

FQDN  
s3portal.demo.netapp.com

TLS Disabled TLS PORT 443

HTTP Enabled HTTP PORT 8080

[Users](#) [Groups](#) [Policies](#)

[+ Add](#)

User name	Access key	Key expiration time
root		-
sm_s3_user	34EH21411SMW1YOV3NQY	Valid forever

Input the user name and key expiration.

Storage VMs

[+ Add](#) [More](#)

☒ Name

☒ svm\_demo

S3 [All settings](#)

☒ Enabled

Server [Edit](#)

FQDN  
s3portal.demo.netapp.com

TLS Disabled TLS PORT 443

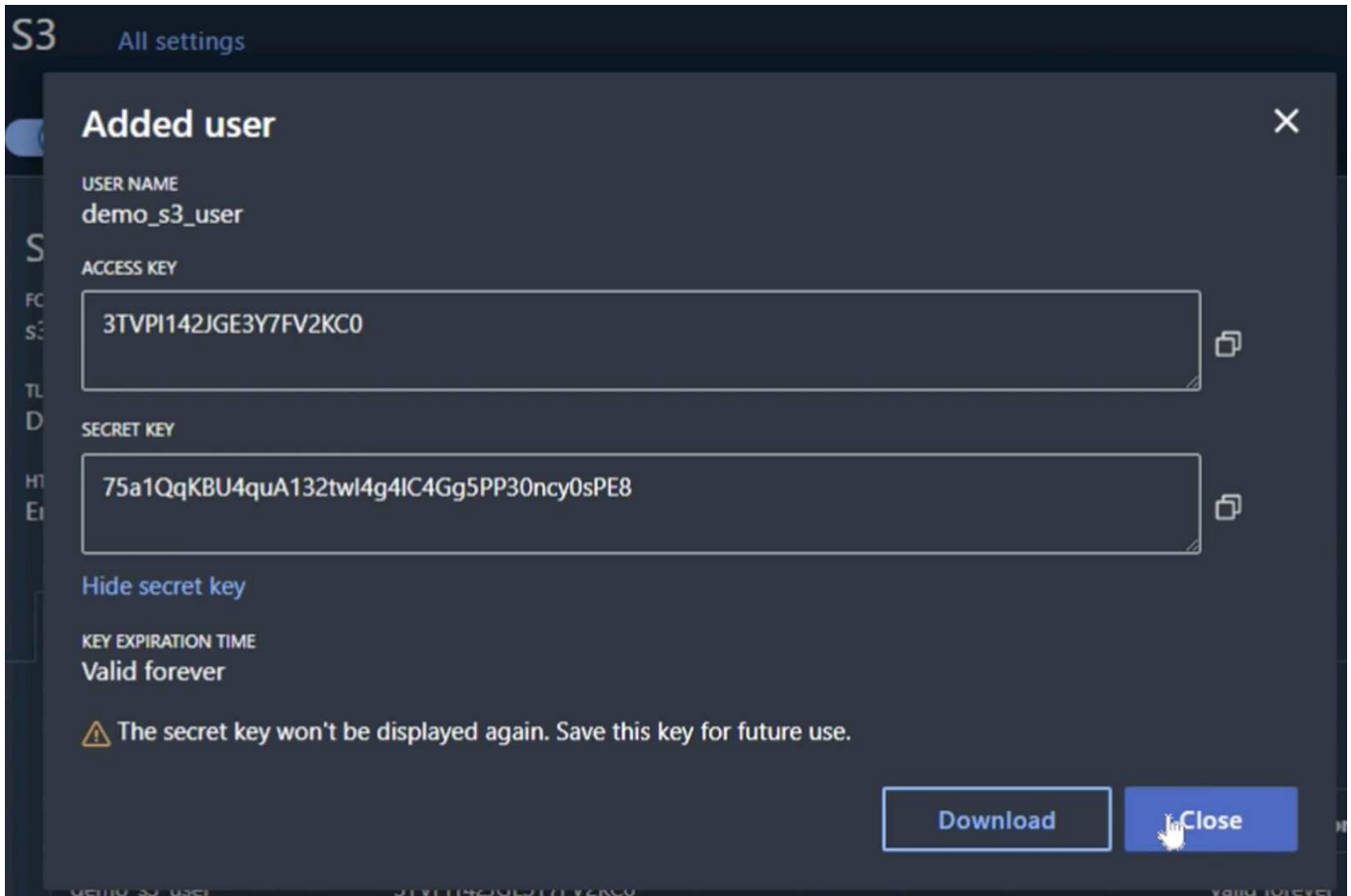
HTTP Enabled HTTP PORT 8080

[Users](#) [Groups](#) [Policies](#)

[+ Add](#)

User name	Access key	Key expiration time
root		-
sm_s3_user	34EH21411SMW1YOV3NQY	Valid forever

Download the S3 keys for the new user.



#### Create SVM S3 group

On the Groups tab of the SVM S3 settings, add a new group with the user created above and FullAccess permissions.

**Add group** ×

NAME

demo\_s3\_group

USERS

demo\_s3\_user ×


POLICIES

FullAccess ×

Cancel Save

#### Create SVM S3 buckets

Navigate to the Buckets section and click the "+Add" button.

 ONTAP System Manager

DASHBOARD

INSIGHTS

STORAGE ^

Overview

Volumes

LUNs

Consistency groups

NVMe namespaces

Shares

Buckets

Qtrees

Quotas

Storage VMs

Tiers

# Buckets

+ Add

Name	Storage
------	---------

Enter a name, capacity, and deselect the "Enable ListBucket access..." check box. and click on the "More options" button.

## Add bucket

NAME

bucket

CAPACITY

100

GiB

☐

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

More options

Cancel

Save

In the "More options" section select the enable versioning check box. and click the "Save" button.

# Add bucket

NAME

bucket

FOLDER (OPTIONAL)

Browse

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

CAPACITY

100

GiB

☐ 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

Extreme

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

Repeat the process and create a second bucket without versioning enabled. Enter a name, the same capacity as bucket one, and deselect the "Enable ListBucket access..." check box. and click on the "Save" button.

**Add bucket** ✕

NAME

ontap-dummy

CAPACITY

100 ▲ ▼ GiB ▼

☐ Enable ListBucket access for all users on the storage VM "svm\_demo".  
Enabling this will allow users to access the bucket.

More options Cancel Save

*By Rafael Guedes, and Aron Klein*

## Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

### Preparing StorageGRID

Continuing the configuration for this demo we will create a Tenant, user, security group, group policy, and bucket.

#### Create the tenant

Navigate to the "Tenants" tab and click on the "create" button

NetApp

StorageGRID Grid Manager

Search by page title

DASHBOARD

ALERTS

NODES

TENANTS

ILM

CONFIGURATION

MAINTENANCE

SUPPORT

# 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.

Create

Export to CSV

Actions

Search tenants by name or ID

No results

	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
No tenants found.						
Create						

Fill in the details for the tenant providing a tenant name, select S3 for the client type, and no quota is required. No need to select platform services or allow S3 select. You can choose to use own Identity source if you choose. Set the root password and click on the finish button.

Click on the tenant name to view the tenant details. **You will need the tenant ID later so copy it off.** Click on the Sign in button. This will bring you to the tenant portal login. Save the URL for future use.

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.

Create

Export to CSV

Actions

Search tenants by name or ID

Displaying one result

	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	tenant_demo	0 bytes	—	—	0	<a href="#">Sign in</a> <a href="#">Copy URL</a>

← Previous

1

Next →

This will bring you to the tenant portal login. Save the URL for future use, and enter the root user credentials.




← → ↻ Not secure | 192.168.0.80/?accountId=27041610751165610501

Lab Status Power Controls Accounts cluster1-mgmt cluster2-mgmt Blue XP

NetApp Support | NetApp

### StorageGRID® Tenant Manager



Recent -- Optional -- ▾

Account ID 27041610751165610501

Username root

Password ••••••

Sign in

## Create the user

Navigate to the Users tab and create a new user.

≡

NetApp | StorageGRID Tenant Manager

DASHBOARD

STORAGE (S3)

My access keys

Buckets

Platform services endpoints

ACCESS MANAGEMENT ▾

Groups

Users

Identity federation

## Users

View local and federated users. Edit properties and group membership of local users.

1 user [Create user](#)

Actions ▾

<input type="checkbox"/>	Username ▾	Full Name ▾	Denied ▾	Type ▾
<input type="checkbox"/>	root	Root		Local

← Previous 1 Next →

Optional

## 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](#)

Now that the new user has been created, click on the users name to open the details of the user.

Copy the user ID from the URL to be used later.

Not secure | https://192.168.0.80/ui/#/users/ebc132e2-cfc3-42c0-a445-3b4465cb523c

Power Controls Accounts cluster1-mgmt cluster2-mgmt Blue XP

## NetApp | StorageGRID Tenant Manager

Users > Demo S3 User

### Overview

Full name: ?	Demo S3 User
Username: ?	demo_s3_user
User type: ?	Local
Denied access: ?	Yes
Access mode: ?	No Groups
Group membership: ?	None

Change password

Change this user's password.

\*\*\*\*\*

To create the S3 keys click on the user name.

NetApp | StorageGRID Tenant Manager

## Users

View local and federated users. Edit properties and group membership of local users.

2 users

Actions ▾

<input type="checkbox"/>	Username ▾	Full Name ▾	Denied ▾	Type ▾
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	demo_s3_user	Demo S3 User	✓	Local

← Previous 1 Next →

Select the "Access keys" tab and click on the "Create Key" button. There is no need to set an expiration time. Download the S3 keys as they cannot be retrieved again once the window is closed.

Create access key

✓ 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

RIJnC5N5FX9RSWgFdj6SQ7wMrfRZYu5bQLdNQTOc



 Download .csv

Finish

### Create the security group

Now go to the Groups page and create a new group.

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

Demo S3 Group

Must contain at least 1 and no more than 32 characters

Unique name ?

demo\_s3\_group

Cancel

Continue

Set the group permissions to Read-Only. This is the Tenant UI permissions, not the S3 permissions.

✓ 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 permissions are controlled with the group policy (IAM Policy). Set the Group policy to custom and paste the json policy in the box. This policy will allow users of this group to list the buckets of the tenant and perform any S3 operations in the bucket named "bucket" or sub-folders in the bucket named "bucket".

```
{
  "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 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

Finally, add the user to the group and finish.

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

### Create two buckets

Navigate to the buckets tab and click on the Create bucket button.

NetApp | StorageGRID Tenant Manager

DASHBOARD

STORAGE (S3)

My access keys

Buckets

Platform services endpoints

ACCESS MANAGEMENT

Groups

Users

Identity federation

## Buckets

Create buckets and manage bucket settings.

0 buckets

Create bucket

Actions

☐

Name

Region

Object Count

Space Used

Date Created

No buckets found

Create bucket

Experimental S3 Console

Define the bucket name and region.



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 ?

bucket

Region ?

us-east-1

Cancel

Continue

On this first bucket enable versioning.

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

Now create a second bucket without versioning enabled.

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 ?

sg-dummy

Region ?

us-east-1

Cancel

Continue

Do not enable versioning on this second bucket.

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

By Rafael Guedes, and Aron Klein


# Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID


Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

## Populate the Source Bucket

Lets put some objects in the source ONTAP bucket. We will use S3Browser for this demo but you could use any tool you are comfortable with.

Using the ONTAP user s3 keys created above, configure S3Browser to connect to your ontap system.

 Add New Account



Add New Account

Enter new account details and click Add new account

[online help](#)

Display name:

Bucket (original and post-migration)

Assign any name to your account.

Account type:

S3 Compatible Storage

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

REST Endpoint:

s3portal.demo.netapp.com:8080

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

Access Key ID:

3TVPI142JGE3Y7FV2KC0

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)

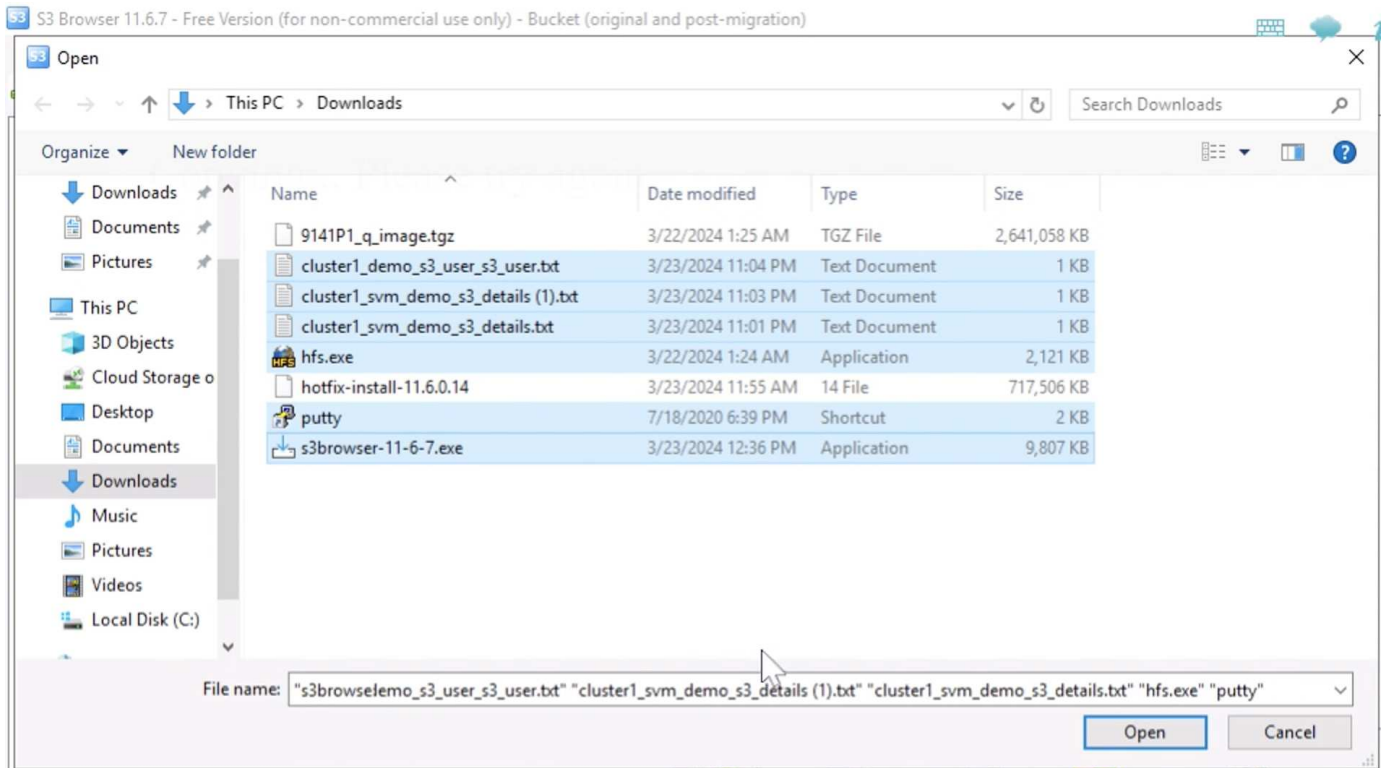
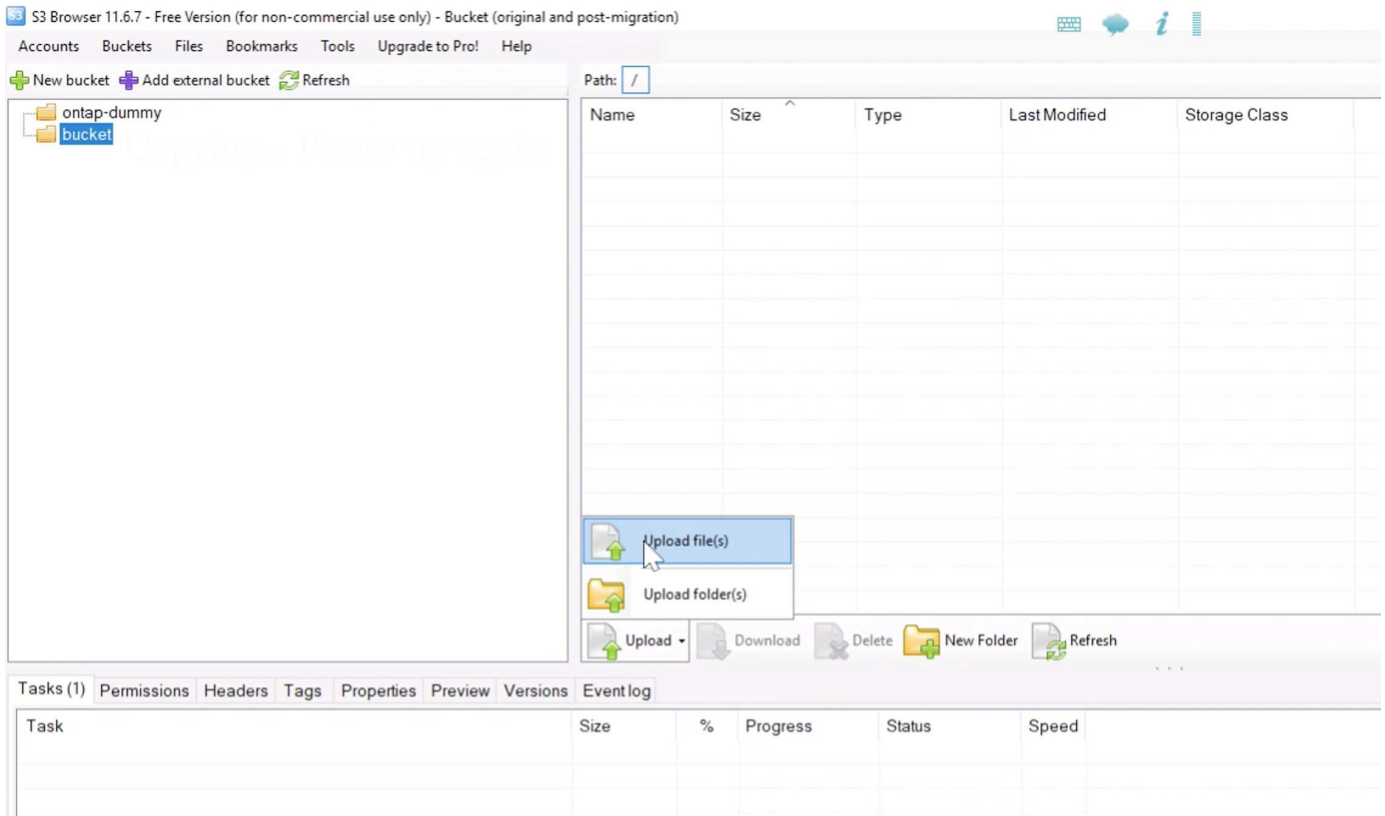
If checked, all communications with the storage will go through encrypted SSL/TLS channel

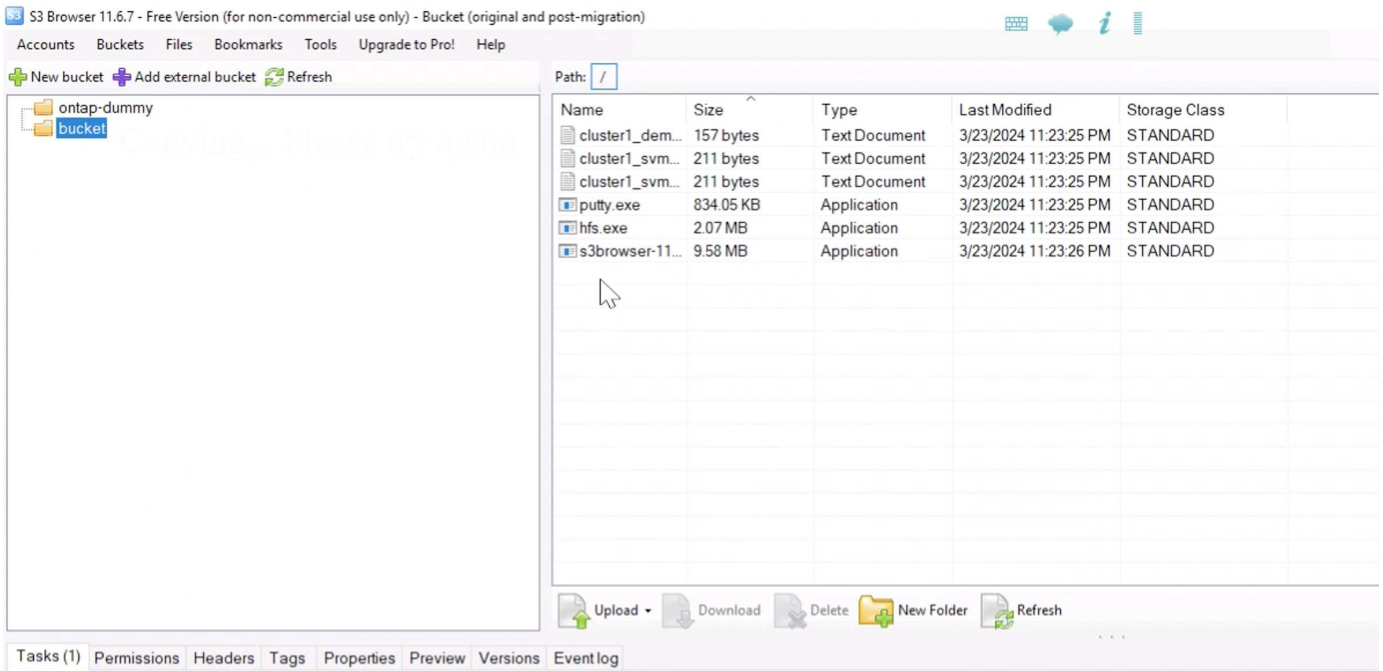
[advanced settings..](#)

 Add new account

 Cancel

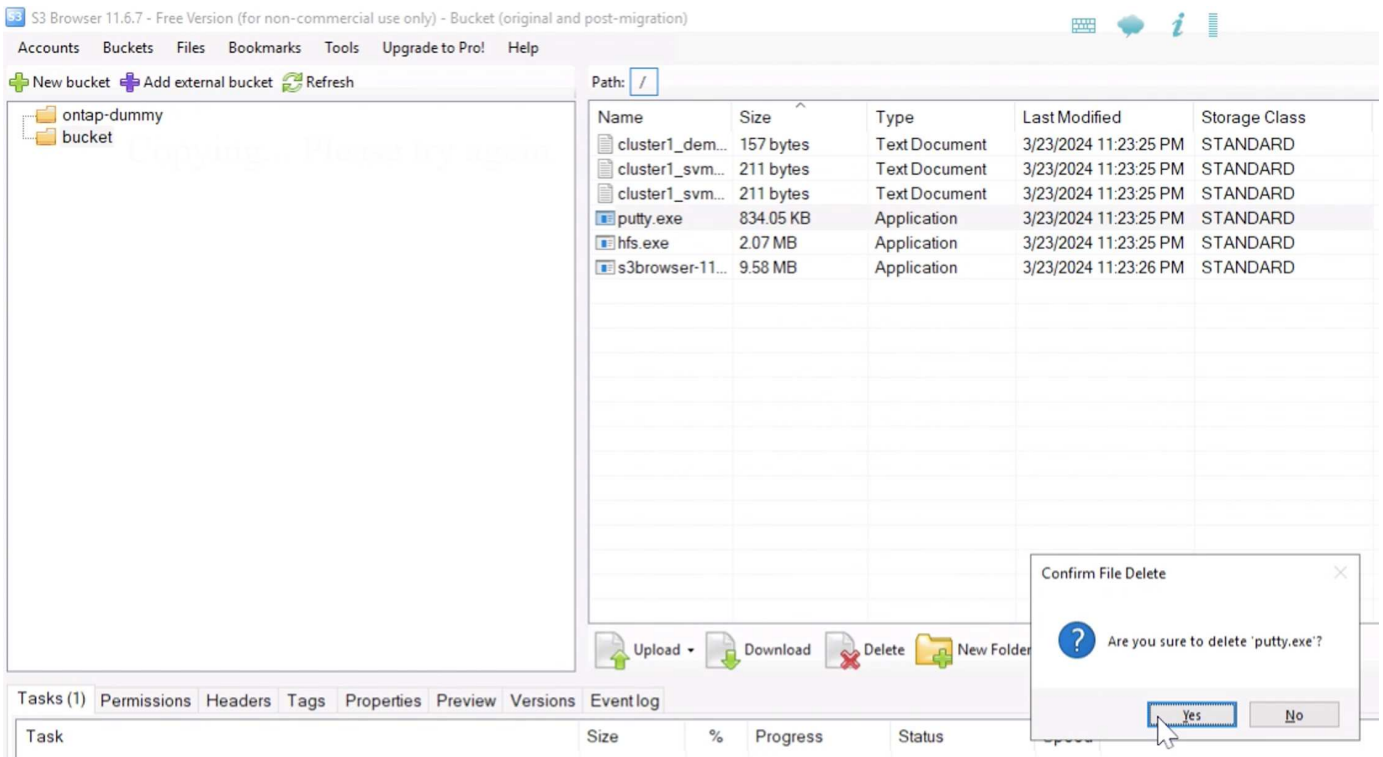
Now lets upload some files to the versioning enabled bucket.



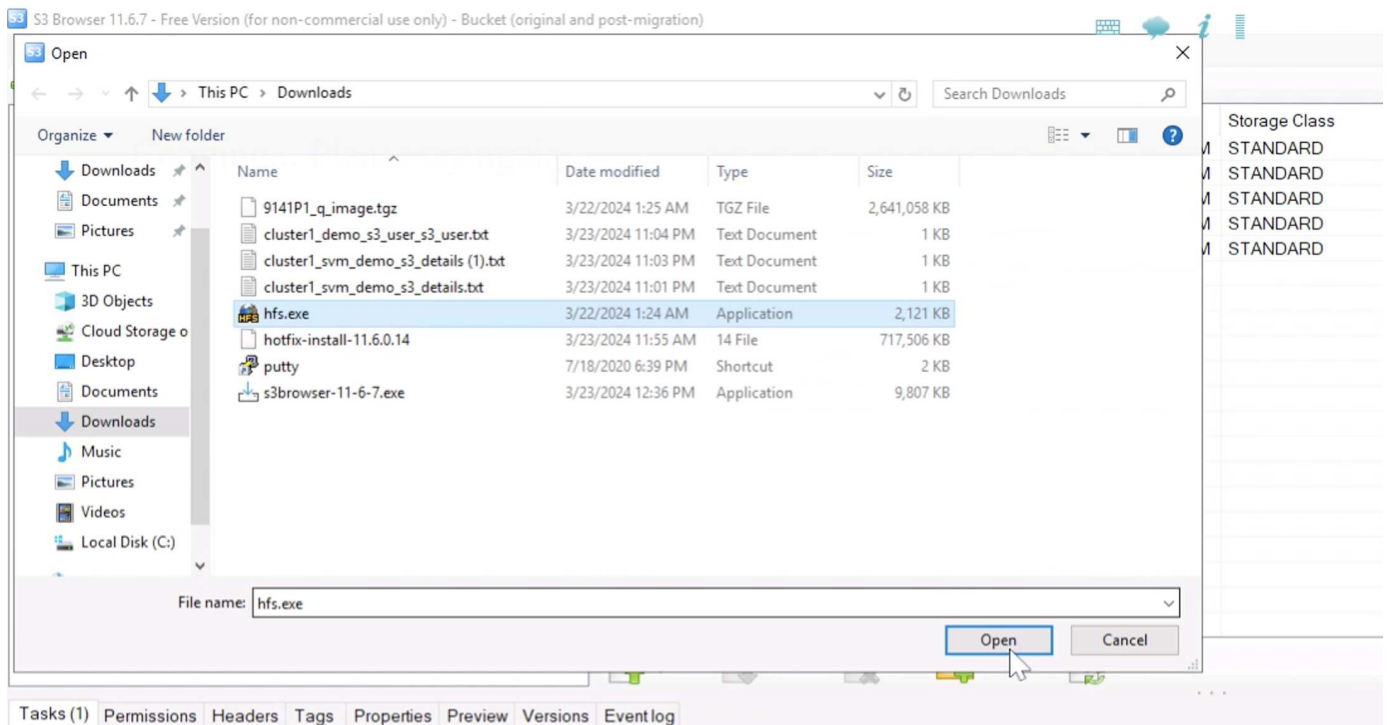


Now lets create some object versions in the bucket.

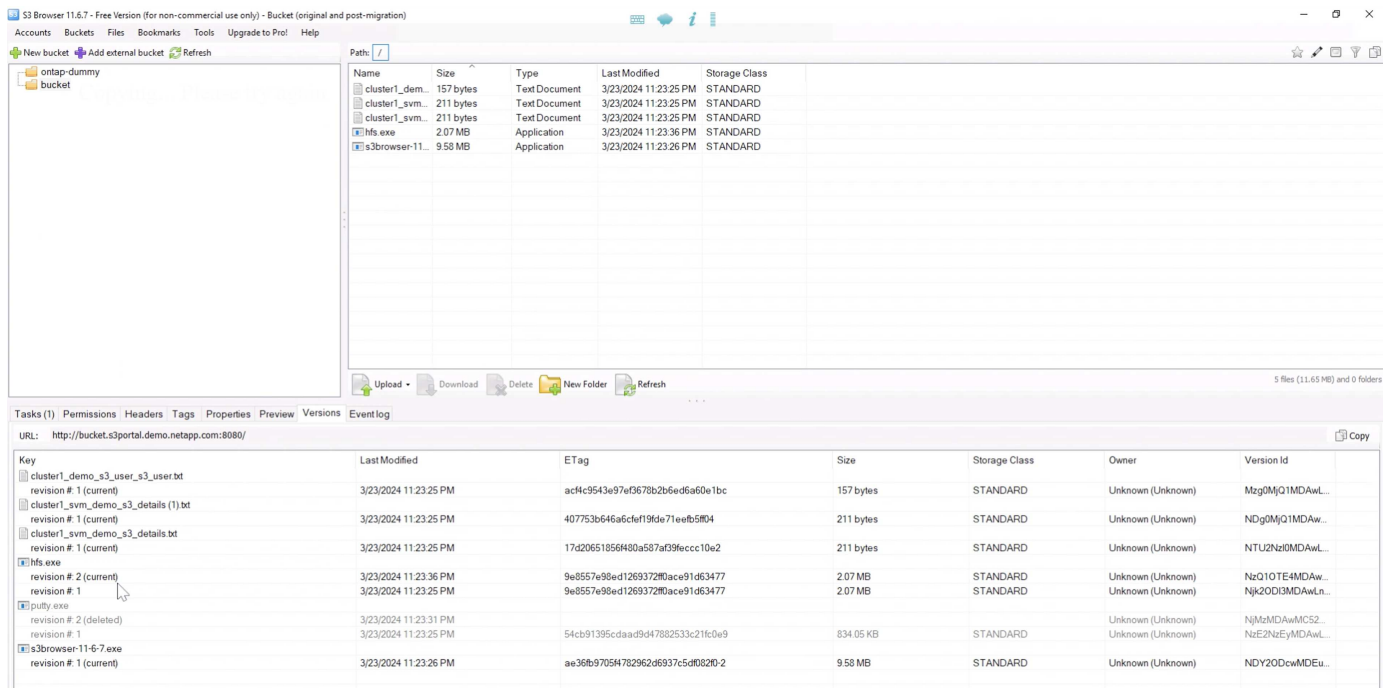
Delete a file.



Upload a file that already exists in the bucket to copy the file over itself and create a new version of it.



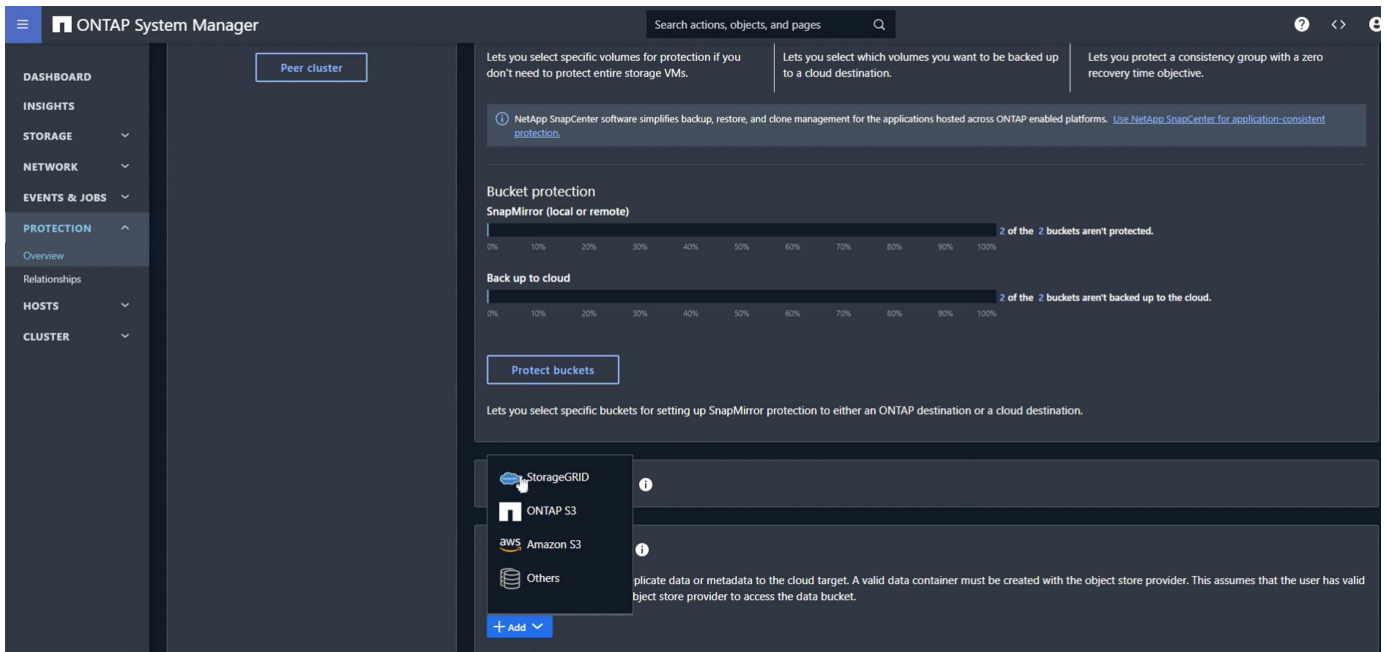
In S3Browser we can view the versions of the objects we just created.



## Establish the replication relationship

Lets start sending data from ONTAP to StorageGRID.

In ONTAP System Manager navigate to "Protection/Overview". Scroll down to "Cloud object stores". and click the "Add" button and select "StorageGRID".



Input the StorageGRID information by providing a name, URL style (for this demo we will use Path-styl URLs). Set the object store scope to "Storage VM".

# Add cloud object store

NAME

sgws\_demo

URL STYLE

Path-style URL

OBJECT STORE SCOPE

☐ Cluster ☒ Storage VM

USE BY

☐ SnapMirror ☒ ONTAP S3 SnapMirror

SERVER NAME (FQDN)

192.168.0.80

If you are using SSL, set the load balancer endpoint port and copy in the StorageGRID endpoint certificate



here. otherwise uncheck the SSL box and input the HTTP endpoint port here.

Input the StorageGRID user S3 keys and bucket name from the StorageGRID configuration above for the destination.

The screenshot shows a configuration window for a cloud object store. It has three input fields at the top: 'ACCESS KEY' with the value '7CT7L1X5MIO5091E86TR', 'SECRET KEY' with a masked value of dots, and 'CONTAINER NAME' with the value 'bucket'. Below these is a section titled 'Network for cloud object store' which contains a table with the following data:

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

Below the table is a checkbox labeled 'Use HTTP proxy' which is currently unchecked. At the bottom left are 'Save' and 'Cancel' buttons. A 'Considerations' link is visible on the right side of the network section.

Now that we have a destination target configured, we can configure the policy settings for the target. Expand "Local policy settings" and select "continuous".

The screenshot shows the ONTAP System Manager interface. On the left is a navigation sidebar with categories like DASHBOARD, INSIGHTS, STORAGE, NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. The main area is titled 'Back up to cloud' and shows a progress bar indicating that 2 of 2 buckets are backed up. Below this is a 'Protect buckets' button and a note about selecting buckets for SnapMirror protection. The 'Local policy settings' section is expanded, showing three panels: 'Protection policies', 'Snapshot policies', and 'Schedules'. In the 'Protection policies' panel, the 'Continuous' policy is selected under the 'Applicable when this cluster is the destination' section.

Edit the continuous policy and change the "Recovery point objective" from "1 Hours" to "3 Seconds".

**Policies** [Protection overview](#)

Protection policies Snapshot policies

[+ Add](#)

Name	Description	Policy type	Scope
Continuous		(All)	
Continuous	Policy for S3 bucket mirroring.	Continuous	Cluster

THROTTLING: Unlimited

RECOVERY POINT OBJECTIVE: 1 Hours

[Edit](#)

Now we can configure snapmirror to replicate the bucket.

```
snapmirror create -source-path sv_demo: /bucket/bucket -destination-path sgws_demo: /objstore -policy Continuous
```

```
cluster1-mgmt
Using username "admin".
Using keyboard-interactive authentication.
Password:

Last login time: 3/24/2024 00:02:00
cluster1::> snapmirror create -source-path svm_demo:/bucket/bucket -destination-path sgws_demo:/objstore -policy Continuous
[Job 220] Job is queued: Create an S3 SnapMirror relationship between bucket "svm_demo:bucket" and bucket "objstore/sgws_demo"..
cluster1::>
```

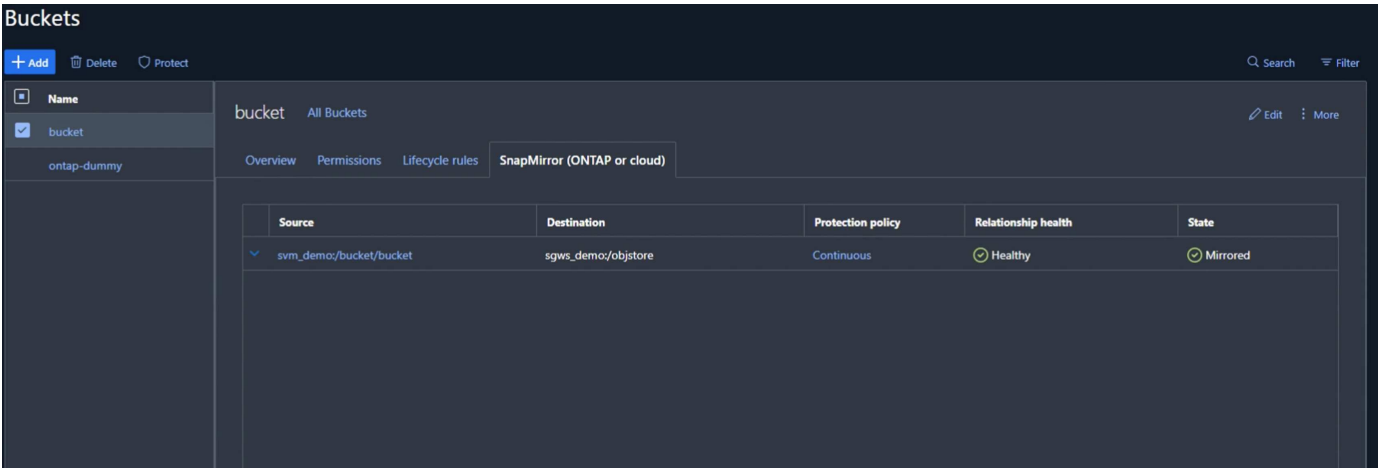
The bucket will now show a cloud symbol in the bucket list under protection.

**Buckets**

[+ Add](#) [Search](#) [Download](#) [Show/hide](#) [Filter](#)

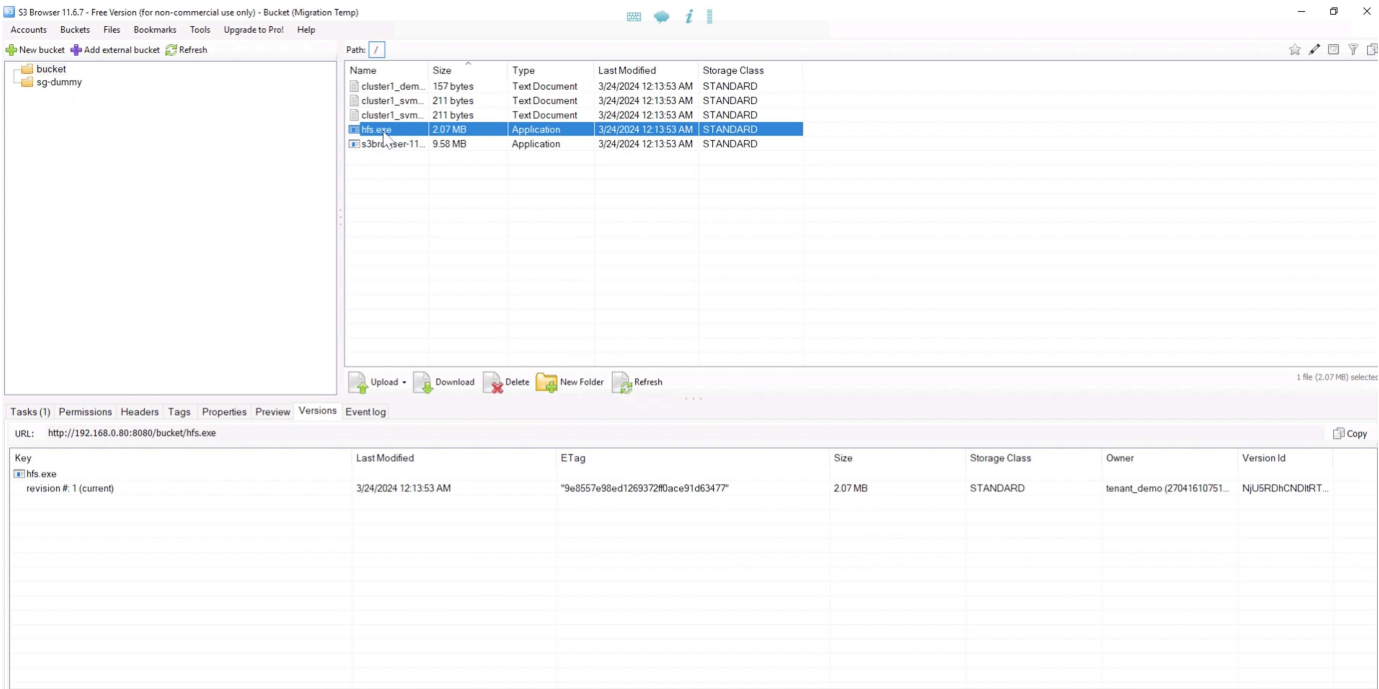
Name	Storage VM	Lifecycle rules	Capacity (available   total)	Protection	Path
bucket	svm_demo	0	100 GiB 100 GiB		-
ontap-dummy	svm_demo	0	100 GiB 100 GiB		-

If we select the bucket and go to the "SnapMirror (ONTAP or Cloud)" tab we will see the snapmirror relationship status.



The replication details

We now have a successfully replicating bucket from ONTAP to StorageGRID. But what is actually replicating? Our source and destination are both versioned buckets. Do the previous versions also replicate to the destination? If we look at our StorageGRID bucket with S3Browser we see that the existing versions did not replicate and our deleted object does not exist, nor does a delete marker for that object. Our duplicated object only has 1 version in the StorageGRID bucket.



In our ONTAP bucket, lets add a new version to our same object that we used previously and see how it replicates.

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)

Accounts Buckets Files Bookmarks Tools Upgrade to Pro! Help

New bucket Add external bucket Refresh

Path: /

Name	Size	Type	Last Modified	Storage Class
cluster1_demo...	157 bytes	Text Document	3/23/2024 11:23:25 PM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/23/2024 11:23:25 PM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/23/2024 11:23:25 PM	STANDARD
putty.exe	834.05 KB	Application	3/23/2024 11:23:25 PM	STANDARD
hfs.exe	2.07 MB	Application	3/24/2024 12:14:52 AM	STANDARD
s3browser-11...	9.58 MB	Application	3/23/2024 11:23:26 PM	STANDARD

Upload Download Delete New Folder Refresh

6 files (12.46 MB) and 0 folders

Tasks (1) Permissions Headers Tags Properties Preview Versions Event log

URL: http://bucket.s3portal.demo.netapp.com:8080/

Key	Last Modified	ETag	Size	Storage Class	Owner	Version Id
cluster1_demo_s3_user_s3_user.txt						
revision # 1 (current)	3/23/2024 11:23:25 PM	ac4c9543e97ef0678b2b6d6a60e1bc	157 bytes	STANDARD	Unknown (Unknown)	Mzg0MjQ1MDAw...
cluster1_svm_demo_s3_details (1).txt	3/23/2024 11:23:25 PM	407753b646a6cfe1f9de71eebf5f04	211 bytes	STANDARD	Unknown (Unknown)	NDg0MjQ1MDAw...
revision # 1 (current)	3/23/2024 11:23:25 PM	17d20651856480a587af39fccc10e2	211 bytes	STANDARD	Unknown (Unknown)	NTU2Nz00MDAw...
hfs.exe						
revision # 3 (current)	3/24/2024 12:14:52 AM	9e8557e98ed1269372f0ace91d63477	2.07 MB	STANDARD	Unknown (Unknown)	NTY0NDg0MDAw...
revision # 2	3/23/2024 11:23:36 PM	9e8557e98ed1269372f0ace91d63477	2.07 MB	STANDARD	Unknown (Unknown)	NzQ1OTI0MDAw...
revision # 1	3/23/2024 11:23:25 PM	9e8557e98ed1269372f0ace91d63477	2.07 MB	STANDARD	Unknown (Unknown)	Njk2ODI0MDAw...
putty.exe						
revision # 1 (current)	3/23/2024 11:23:25 PM	54cb91395cdaad94788253c21fc0e9	834.05 KB	STANDARD	Unknown (Unknown)	NzE2NzE0MDAw...
s3browser-11-6-7.exe						
revision # 1 (current)	3/23/2024 11:23:26 PM	ae36be97054782962d6937c5d0820-2	9.58 MB	STANDARD	Unknown (Unknown)	NDY2ODcwMDEu...

If we look on the StorageGRID side we see that a new version has been created in this bucket too, but is missing the initial version from before the snapmirror relationship.

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (Migration Temp)

Accounts Buckets Files Bookmarks Tools Upgrade to Pro! Help

New bucket Add external bucket Refresh

Path: /

Name	Size	Type	Last Modified	Storage Class
cluster1_demo...	157 bytes	Text Document	3/24/2024 12:13:53 AM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/24/2024 12:13:53 AM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/24/2024 12:13:53 AM	STANDARD
putty.exe	834.05 KB	Application	3/24/2024 12:14:28 AM	STANDARD
hfs.exe	2.07 MB	Application	3/24/2024 12:14:56 AM	STANDARD
s3browser-11...	9.58 MB	Application	3/24/2024 12:13:53 AM	STANDARD

Upload Download Delete New Folder Refresh

1 file (2.07 MB)

Tasks (1) Permissions Headers Tags Properties Preview Versions Event log

URL: http://192.168.0.80:8080/bucket/hfs.exe

Key	Last Modified	ETag	Size	Storage Class	Owner	Version Id
hfs.exe						
revision # 2 (current)	3/24/2024 12:14:56 AM	"9e8557e98ed1269372f0ace91d63477"	2.07 MB	STANDARD	tenant_demo (27041610751...	OEHRyY4NDgRT...
revision # 1	3/24/2024 12:13:53 AM	"9e8557e98ed1269372f0ace91d63477"	2.07 MB	STANDARD	tenant_demo (27041610751...	NjU5RDhjcNDIIR...

This is because the ONTAP SnapMirror S3 process only replicates the current version of the object. This is why we created a versioned bucket on the StorageGRID side to be the destination. This way StorageGRID can maintain a version history of the objects.

By Rafael Guedes, and Aron Klein

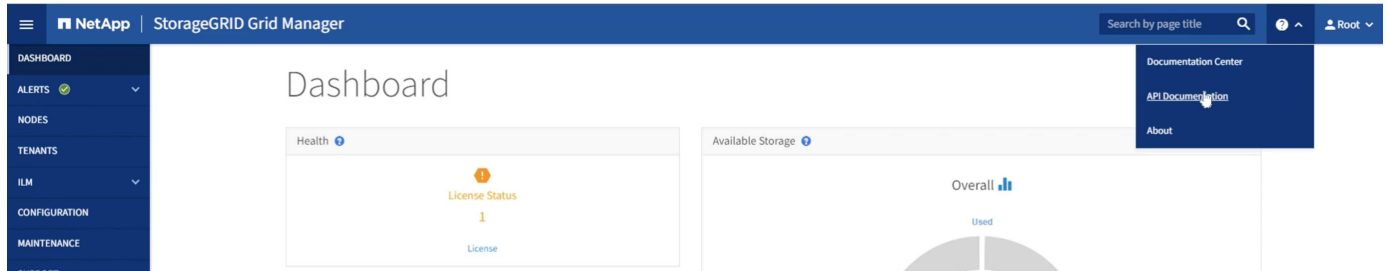
## Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

Enabling enterprise-grade S3 by seamlessly migrating object-based storage from ONTAP S3 to StorageGRID

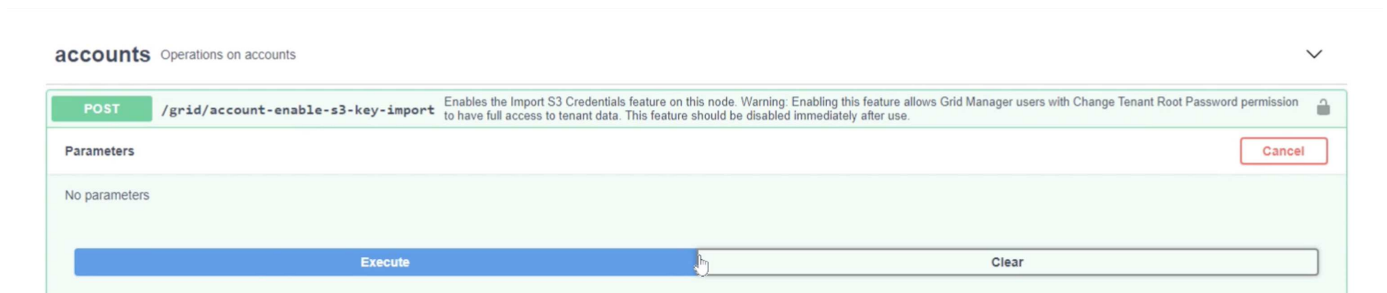
## Migrate S3 Keys

For a migration, most of the time you will want to migrate the credentials for the users rather than generate new credentials on the destination side. StorageGRID provides api's to allow s3 keys to be imported to a user.

Logging into the StorageGRID management UI (not the tenant manager UI) open the API Documentation swagger page.



Expand the "accounts" section, select the "POST /grid/account-enable-s3-key-import", click the "Try it out" button, then click on the execute button.



Now scroll down still under "accounts" to "POST /grid/accounts/{id}/users/{user\_id}/s3-access-keys"

Here is where we are going to input the tenant ID and user account ID we collected earlier. fill in the fields and the keys from our ONTAP user in the json box. you can set the expiration of the keys, or remove the " , "expires": 123456789" and click on execute.

POST

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

Parameters

Name	Description
<b>id</b> * required string (path)	ID of Storage Tenant Account <input type="text" value="27041610751165610501"/>
<b>user_id</b> * required string (path)	ID of user in tenant account. <input type="text" value="ebc132e2-cfc3-42c0-a445-3b4465cb523c"/>
<b>body</b> * required (body)	<div>Edit Value   Model</div> <pre>{   "accessKey": "3TVPI142JGE3Y7FV2KC0",   "secretAccessKey": "75a1QqKBU4quA132twI4g41C4Gg5PP30ncy0sPE8" }</pre>

Once you have completed all of your user key imports you should disable the key import function in "accounts" "POST /grid/account-disable-s3-key-import"

POST

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

Parameters

No parameters

Execute


Responses

Response content type application/json

Cancel

If we look at the user account in the tenant manager UI, we can see the new key has been added.

## 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

### The final cut-over

If the intention is to have a perpetually replicating bucket from ONTAP to StorageGRID, you can end here. If this is a migration from ONTAP S3 to StorageGRID, then its time to put an end to it and cut over.

Inside ONTAP system manager, edit the S3 group and set it to "ReadOnlyAccess". This will prevent the users from writing to the ONTAP S3 bucket anymore.

37

# Edit group

NAME

demo\_s3\_group

USERS

demo\_s3\_user ×

POLICIES

ReadOnlyAccess ×

Cancel

Save

All that is left to do is configure DNS to point from the ONTAP cluster to the StorageGRID endpoint. Make sure your endpoint certificate is correct and if you need virtual hosted style requests then add the endpoint domain names in storageGRID



# 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  +

Your clients will either need to wait for the TTL to expire, or flush DNS to resolve to the new system so you can test that everything is working. All that is left is to clean up the initial temporary S3 keys we used to test the StorageGRID data access (NOT the imported keys), remove the snapmirror relationships, and remove the ONTAP data.

*By Rafael Guedes, and Aron Klein*

## Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.