



Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

How to enable StorageGRID in your environment

NetApp
October 09, 2024

Inhalt

- Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID 1
 - Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID 1
 - Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID 1
 - Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID 13
 - Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID 25
 - Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID 34

Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

Demo Zur Migration

Dies ist eine Demonstration zur Migration von Benutzern und Buckets von ONTAP S3 zu StorageGRID.

Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

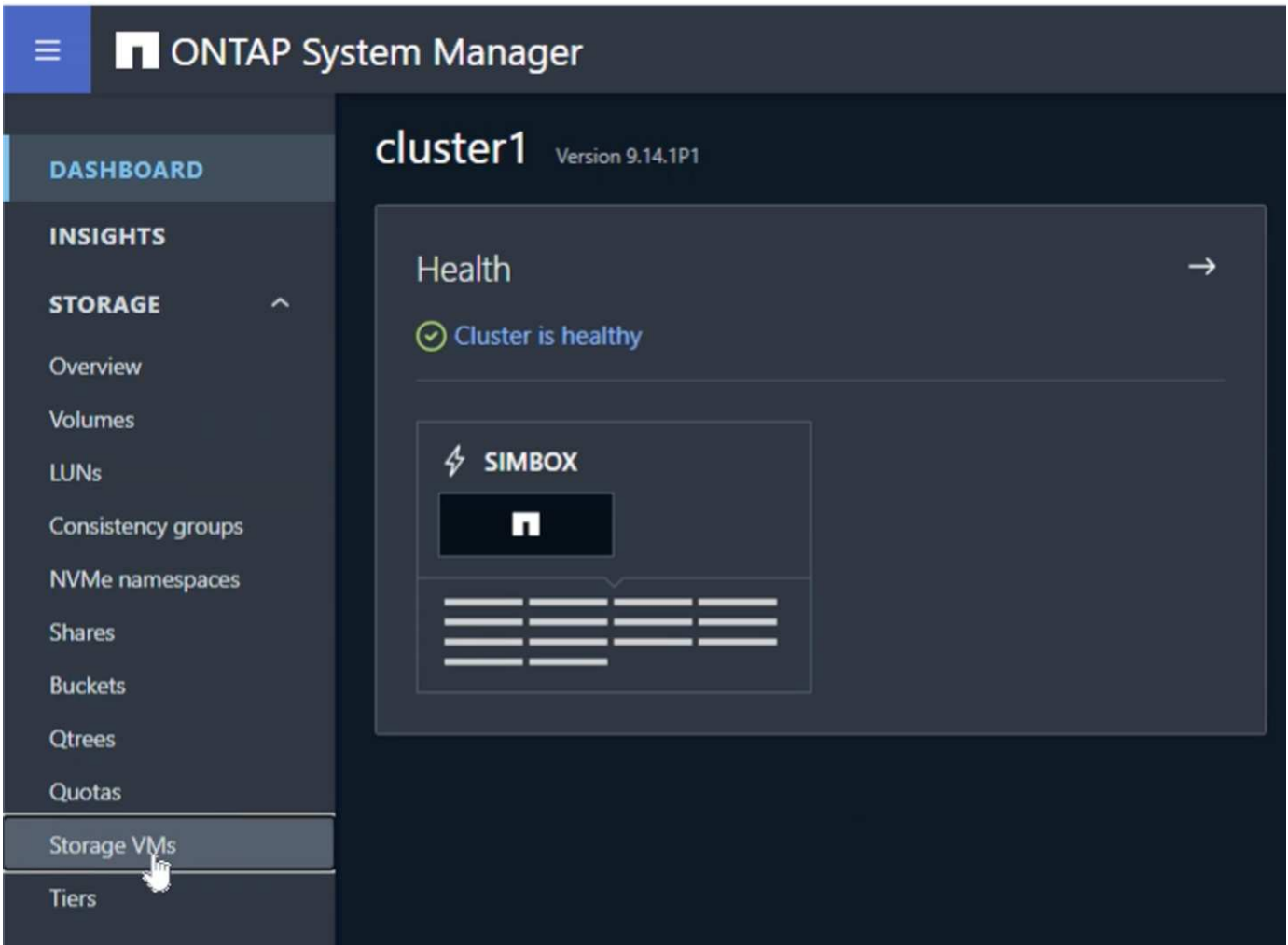
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

ONTAP wird vorbereitet

Für Demonstrationszwecke werden ein SVM Objektspeicher-Server, Benutzer, Gruppen, Gruppenrichtlinien und Buckets erstellt.

Erstellen Sie die virtuelle Speichermaschine

Navigieren Sie im ONTAP System Manager zu Storage VMs und fügen Sie eine neue Storage VM hinzu.



Aktivieren Sie die Kontrollkästchen „S3 aktivieren“ und „TLS aktivieren“, und konfigurieren Sie die HTTP(S)-Ports. Definieren Sie die IP-Adresse und die Subnetzmaske und definieren Sie das Gateway und die Broadcast-Domäne, wenn Sie nicht den Standard oder die in Ihrer Umgebung erforderlichen Standards verwenden.

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

Im Rahmen der SVM-Erstellung wird ein Benutzer erstellt. Laden Sie die S3-Schlüssel für diesen Benutzer herunter, und schließen Sie das Fenster.


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](#)


Sobald die SVM erstellt wurde, bearbeiten Sie die SVM und fügen Sie die DNS-Einstellungen hinzu.

Services

NIS  

Not configured

Name service switch  



Services lookup order 

HOSTS
Files, then DNS

GROUP
Files

NAME MAP
Files

NETGROUP
Files

DNS  

Not configured

Definieren Sie den DNS-Namen und die IP-Adresse.

Add DNS domain ✕

DNS domains

demo.netapp.com

+ Add

Name servers

192.168.0.253

+ Add

Cancel

Cancel **Save**

SVM S3-Benutzer erstellen

Jetzt können wir die S3-Benutzer und -Gruppe konfigurieren. Bearbeiten Sie die S3-Einstellungen.

Protocols

NFS



Not configured

SMB/CIFS



Not configured

NVMe



Not configured

S3



STATUS
✓ Enabled

TLS
Disabled

HTTP
Enabled

Neuen Benutzer hinzufügen.

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

Geben Sie den Benutzernamen und den Ablauf des Schlüssels ein.

Storage VMs

+ Add More

- Name
- svm_demo

S3 All settings

Enabled

Server Edit

FQDN
s3portal.demo.netapp.com

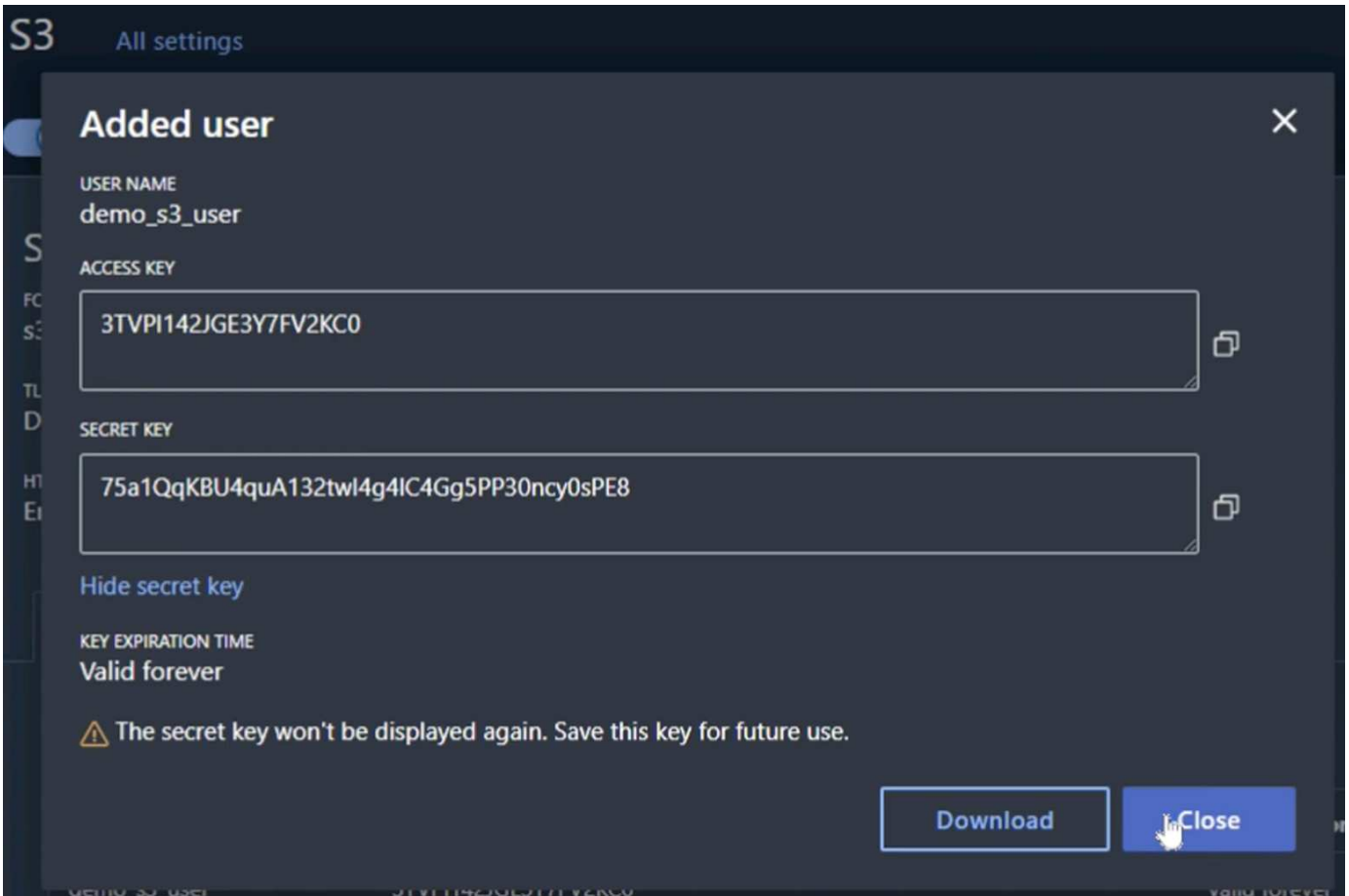
TLS	Disabled	TLS PORT	443
HTTP	Enabled	HTTP PORT	8080

Users Groups Policies

+ Add

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

Laden Sie die S3-Schlüssel für den neuen Benutzer herunter.



SVM S3-Gruppe erstellen

Fügen Sie in den SVM S3-Einstellungen auf der Registerkarte Groups eine neue Gruppe mit dem oben erstellten Benutzer und FullAccess-Berechtigungen hinzu.

Add group ✕

NAME

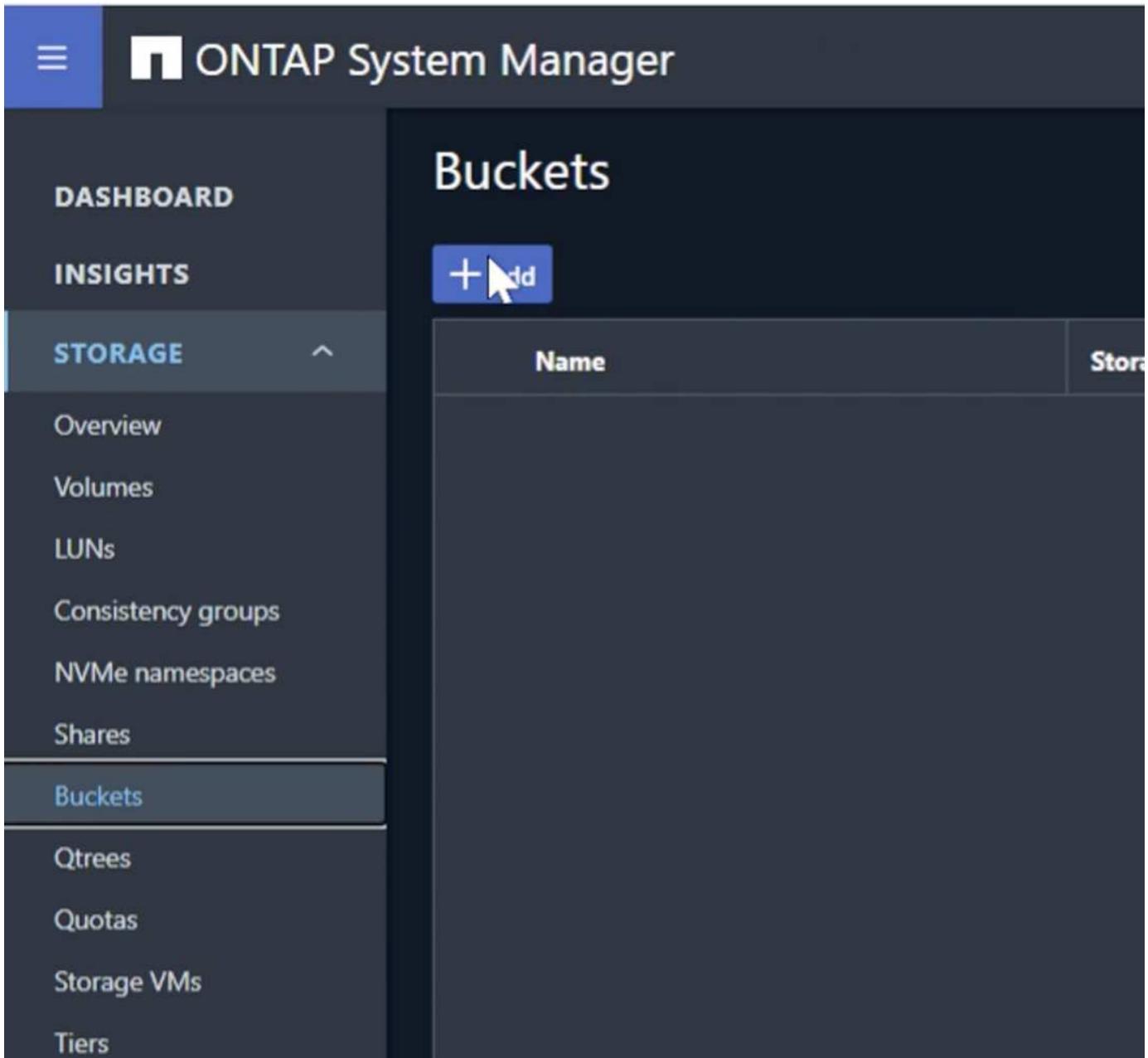
USERS

POLICIES

Cancel **Save**

Erstellung von SVM S3 Buckets

Navigieren Sie zum Bereich „Buckets“, und klicken Sie auf die Schaltfläche „+Hinzufügen“.



Geben Sie einen Namen und eine Kapazität ein, und deaktivieren Sie das Kontrollkästchen „Zugriff auf ListBucket aktivieren...“. Klicken Sie anschließend auf die Schaltfläche „Weitere Optionen“.

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

Aktivieren Sie im Bereich "Weitere Optionen" das Kontrollkästchen Versionierung aktivieren und klicken Sie auf die Schaltfläche "Speichern".

Add bucket



NAME

FOLDER (OPTIONAL)

Browse

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

CAPACITY



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



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

Wiederholen Sie den Prozess, und erstellen Sie einen zweiten Bucket ohne aktivierte Versionierung. Geben Sie einen Namen ein, der mit der gleichen Kapazität wie Bucket One identisch ist, und deaktivieren Sie das Kontrollkästchen „Zugriff auf ListBucket aktivieren...“. Klicken Sie anschließend auf die Schaltfläche „Speichern“.

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

Von Rafael Guedes und Aron Klein

Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

StorageGRID wird vorbereitet

Wenn Sie mit der Konfiguration für diese Demo fortfahren, erstellen wir einen Mandanten, Benutzer, Sicherheitsgruppe, Gruppenrichtlinie und Bucket.

Erstellen Sie die Serviceeinheit

Navigieren Sie zur Registerkarte „Tenants“ und klicken Sie auf die Schaltfläche „Create“

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

Geben Sie die Details für den Mandanten ein, indem Sie einen Mandantennamen angeben, und wählen Sie S3 für den Clienttyp aus. Es ist kein Kontingent erforderlich. Plattfordmdienste müssen nicht ausgewählt oder S3-Auswahl zugelassen werden. Sie können wählen, ob Sie eine eigene Identitätsquelle verwenden möchten. Legen Sie das Root-Passwort fest und klicken Sie auf die Schaltfläche „Fertigstellen“.

Klicken Sie auf den Namen der Serviceeinheit, um die Details der Serviceeinheit anzuzeigen. **Sie brauchen die Mieter-ID später, also kopieren Sie sie ab.** Klicken Sie auf die Schaltfläche Anmelden. Dadurch gelangen Sie zur Anmeldung beim Mandantenportal. Speichern Sie die URL für die spätere Verwendung.

Tenants

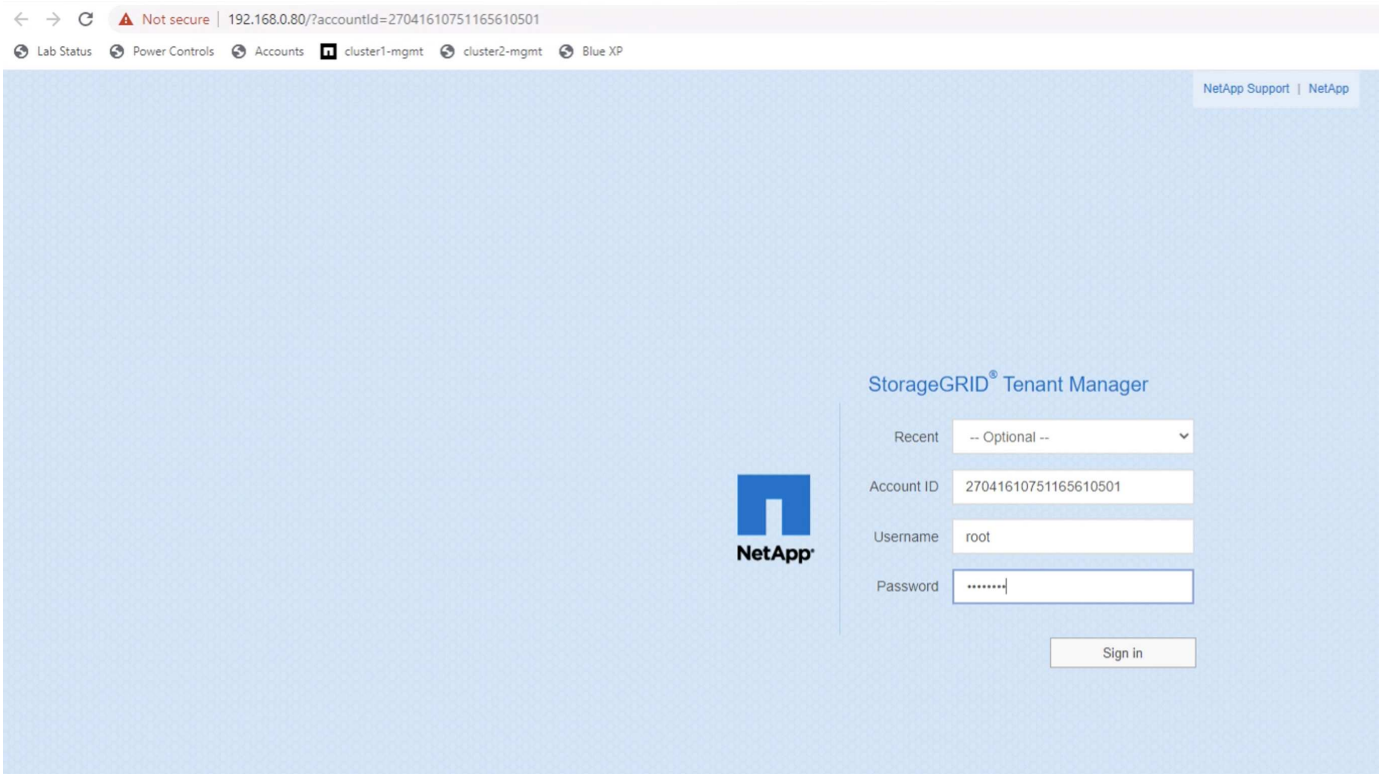
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

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
tenant_demo	0 bytes	—	—	0	Sign in Copy URL

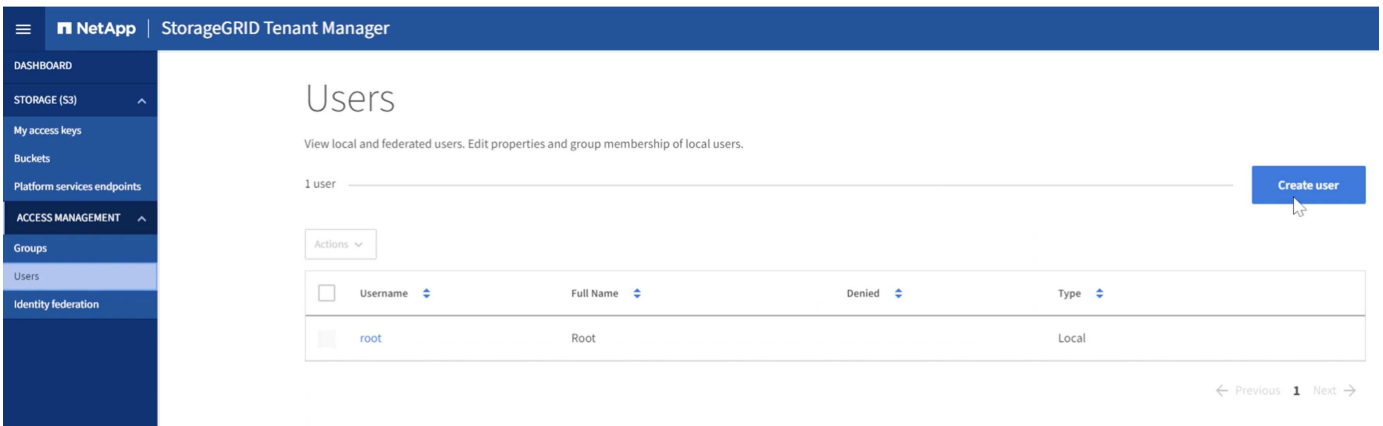
← Previous 1 Next →

Dadurch gelangen Sie zur Anmeldung beim Mandantenportal. Speichern Sie die URL für die zukünftige Verwendung, und geben Sie die Anmeldedaten des Stammbenutzers ein.



Erstellen Sie den Benutzer

Navigieren Sie zur Registerkarte Benutzer, und erstellen Sie einen neuen Benutzer.



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](#)

Nachdem der neue Benutzer erstellt wurde, klicken Sie auf den Benutzernamen, um die Details des Benutzers zu öffnen.

Kopieren Sie die Benutzer-ID aus der URL, die später verwendet werden soll.

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

[Password](#)
[Access](#)
[Access keys](#)
[Groups](#)

Change password

Change this user's password.

Um die S3-Schlüssel zu erstellen, klicken Sie auf den Benutzernamen.

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.

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 →

Wählen Sie die Registerkarte „Zugriffsschlüssel“ aus und klicken Sie auf die Schaltfläche „Schlüssel erstellen“. Es ist nicht notwendig, eine Verfallszeit einzustellen. Laden Sie die S3-Schlüssel herunter, da sie nach dem Schließen des Fensters nicht mehr abgerufen werden können.

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.

i 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

Erstellen Sie die Sicherheitsgruppe

Gehen Sie nun zur Seite Gruppen und erstellen Sie eine neue Gruppe.

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](#)

Legen Sie die Gruppenberechtigungen auf schreibgeschützt fest. Dies sind die Berechtigungen der Mandanten-UI, nicht die S3-Berechtigungen.



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 Berechtigungen werden über die Gruppenrichtlinie (IAM-Richtlinie) gesteuert. Legen Sie die Gruppenrichtlinie auf Benutzerdefiniert fest, und fügen Sie die json-Richtlinie in das Feld ein. Diese Richtlinie ermöglicht Benutzern dieser Gruppe, die Buckets des Mandanten aufzulisten und alle S3-Vorgänge in dem Bucket mit dem Namen „Bucket“ oder Unterordner im Bucket mit dem Namen „Bucket“ auszuführen.

```

{
  "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

Fügen Sie schließlich den Benutzer zur Gruppe hinzu, und beenden Sie den Vorgang.

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](#)

Erstellen Sie zwei Buckets

Navigieren Sie zur Registerkarte „Buckets“, und klicken Sie auf die Schaltfläche „Bucket erstellen“.

Definieren Sie den Bucket-Namen und die 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 ?

Region ?

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

Aktivieren Sie in diesem ersten Bucket die Versionierung.

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](#)

Erstellen Sie nun einen zweiten Bucket ohne aktivierte Versionierung.

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

Aktivieren Sie die Versionierung für diesen zweiten Bucket nicht.

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

Von Rafael Guedes und Aron Klein

Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID


Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

Füllen Sie den Quelleimer aus

Lassen Sie uns einige Objekte in den Quell-ONTAP-Bucket legen. Wir verwenden S3Browser für diese Demo, aber Sie können jedes Tool verwenden, mit dem Sie vertraut sind.

Konfigurieren Sie S3Browser mithilfe der oben erstellten ONTAP-Benutzer-s3-Schlüssel, um eine Verbindung zu Ihrem ONTAP-System herzustellen.

Add New Account — □ ×

 **Add New Account** [online help](#)

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:

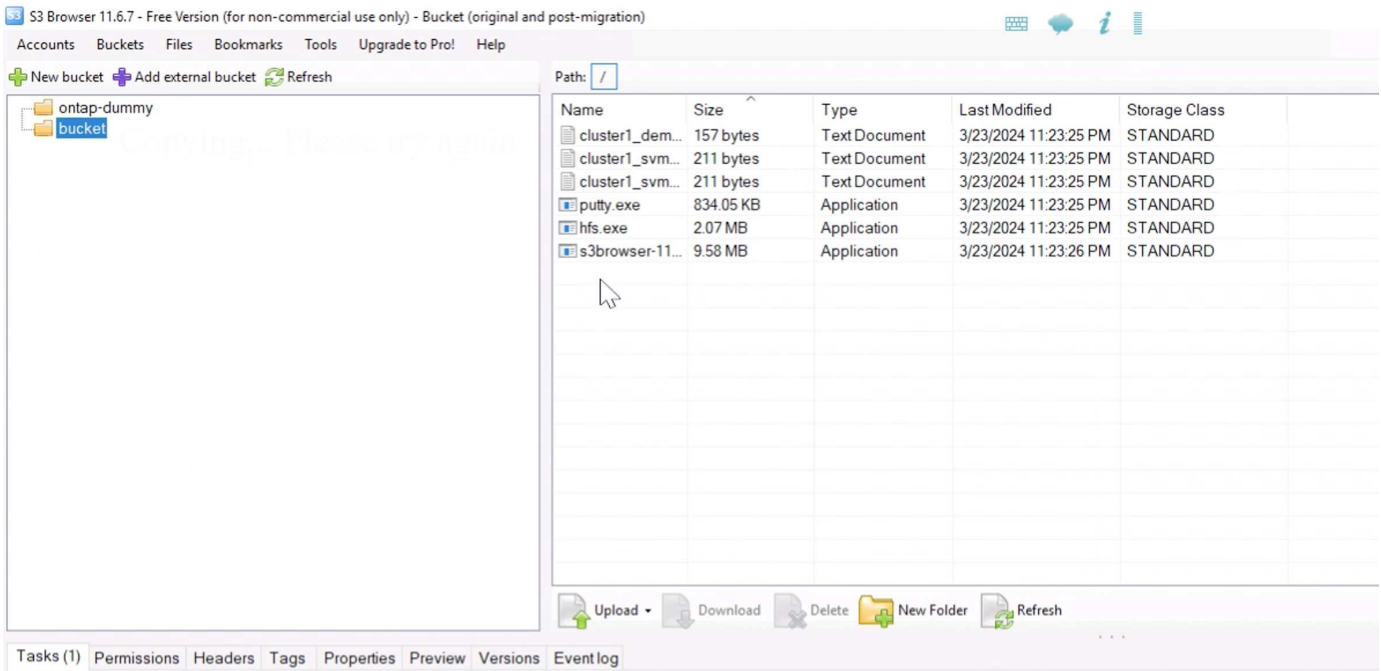
Turn this option on if you want to protect your Access Keys with a master password.

Use secure transfer (SSL/TLS)

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

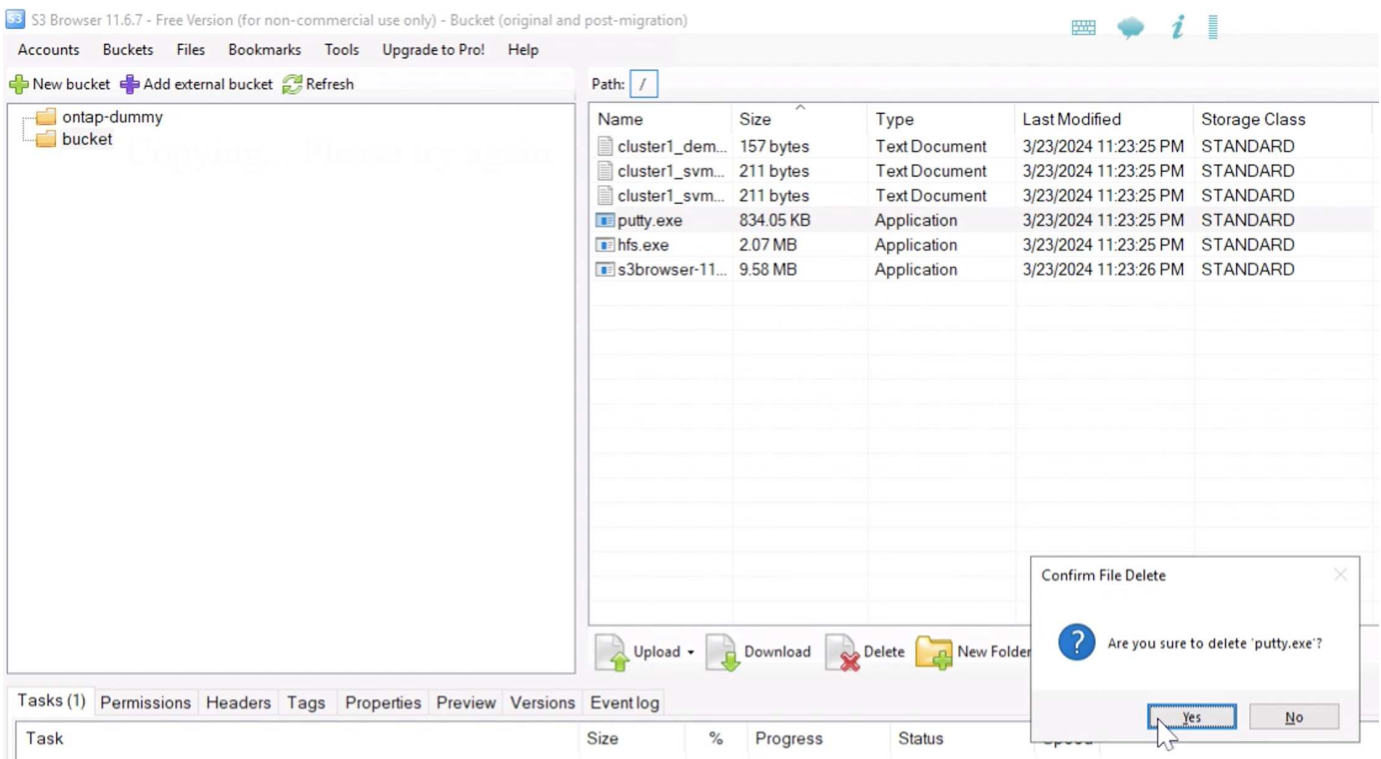
[advanced settings..](#)

Nun können einige Dateien in den Bucket mit aktivierter Versionierung hochgeladen werden.

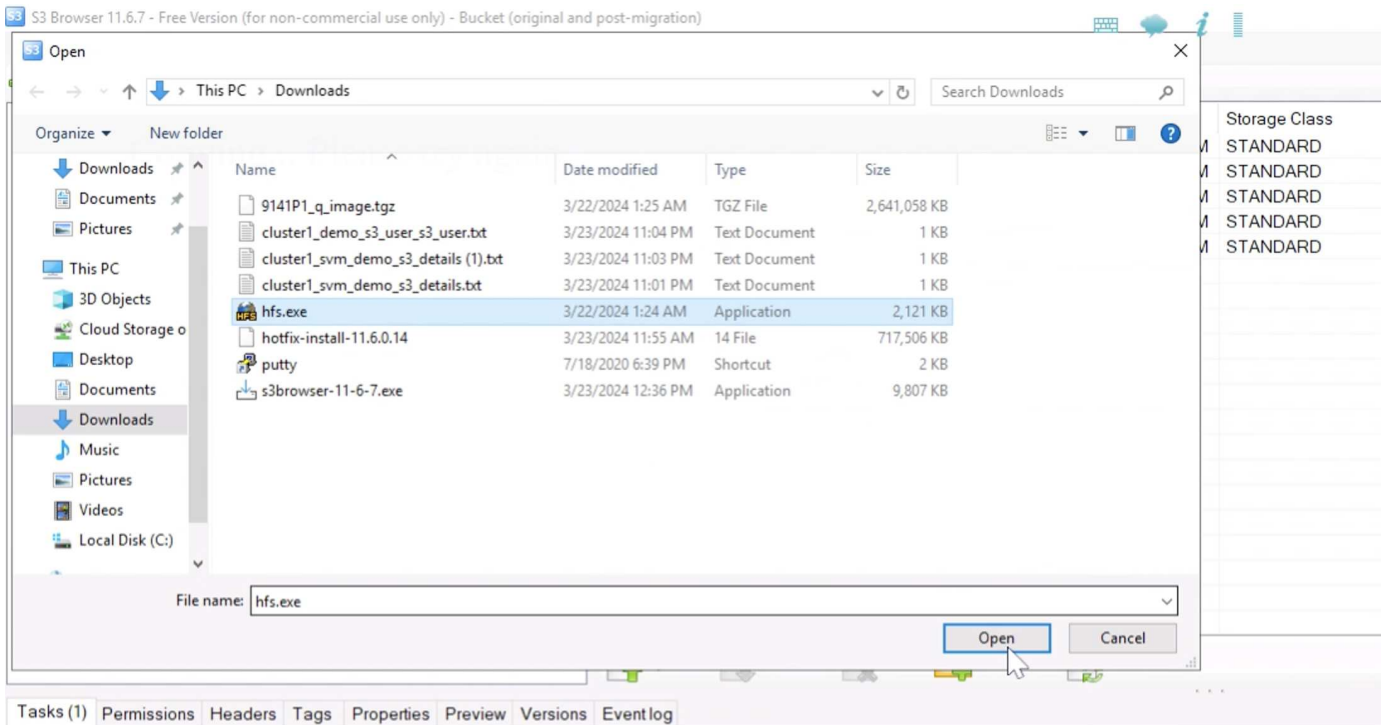


Lassen Sie uns nun einige Objektversionen im Bucket erstellen.

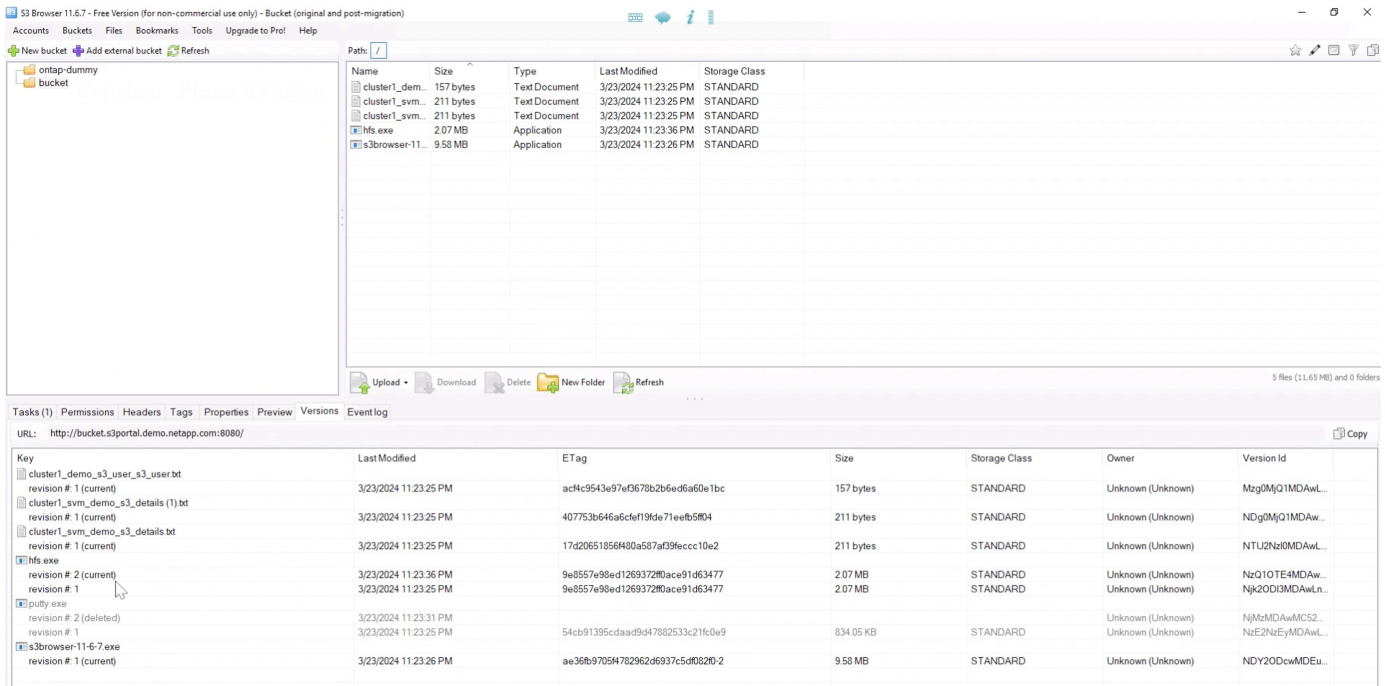
Eine Datei löschen.



Laden Sie eine Datei hoch, die bereits im Bucket vorhanden ist, um die Datei über sich selbst zu kopieren und eine neue Version davon zu erstellen.



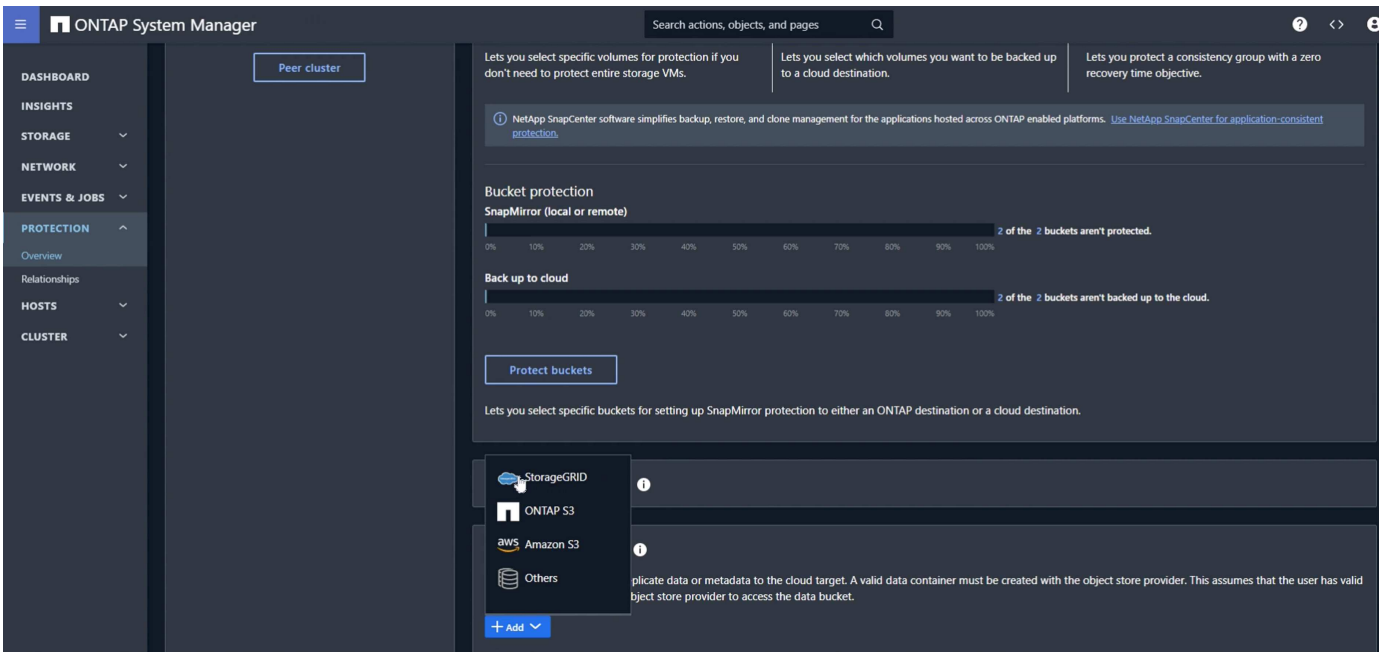
In S3Browser können wir die Versionen der Objekte anzeigen, die wir gerade erstellt haben.



Festlegen der Replikationsbeziehung

Beginnen Sie damit, Daten von ONTAP an StorageGRID zu senden.

Navigieren Sie im ONTAP Systemmanager zu „Schutz/Übersicht“. Scrollen Sie nach unten zu "Cloud object Stores" und klicken Sie auf "Add" und wählen Sie "StorageGRID".



Geben Sie die StorageGRID-Informationen ein, indem Sie einen Namen, URL-Stil (für diese Demo verwenden wir Pfad-styl URLs). Setzen Sie den Umfang des Objektspeichers auf „Storage VM“.

Add cloud object store

NAME

URL STYLE

OBJECT STORE SCOPE

Cluster
 Storage VM

USE BY ⓘ

SnapMirror
 ONTAP S3 SnapMirror

SERVER NAME (FQDN)

Wenn Sie SSL verwenden, legen Sie hier den Load Balancer-Endpunkt-Port fest und kopieren Sie das

StorageGRID-Endpointzertifikat. Andernfalls deaktivieren Sie das SSL-Kontrollkästchen und geben den HTTP-Endpoint-Port hier ein.

Geben Sie die S3-Benutzerschlüssel und den Bucket-Namen der StorageGRID aus der obigen StorageGRID-Konfiguration für das Ziel ein.

ACCESS KEY

7CT7L1X5MIO5091E86TR

SECRET KEY

.....

CONTAINER NAME ⓘ

bucket

Network for cloud object store

Considerations

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

Nachdem jetzt ein Ziel konfiguriert ist, können wir die Richtlinieneinstellungen für das Ziel konfigurieren. Erweitern Sie „Lokale Richtlinieneinstellungen“, und wählen Sie „kontinuierlich“ aus.

ONTAP System Manager

Search actions, objects, and pages

Back up to cloud

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

Protect buckets

Lets you select specific buckets for setting up SnapMirror protection to either an ONTAP destination or a cloud destination.

Local policy settings ⓘ

Protection policies

Applicable when this cluster is the destination

- Asynchronous
At 5 minutes past the hour, every hour
- AutomatedFailOver
No schedules
- CloudBackupDefault
No schedules
- Continuous**
No schedules

Snapshot policies

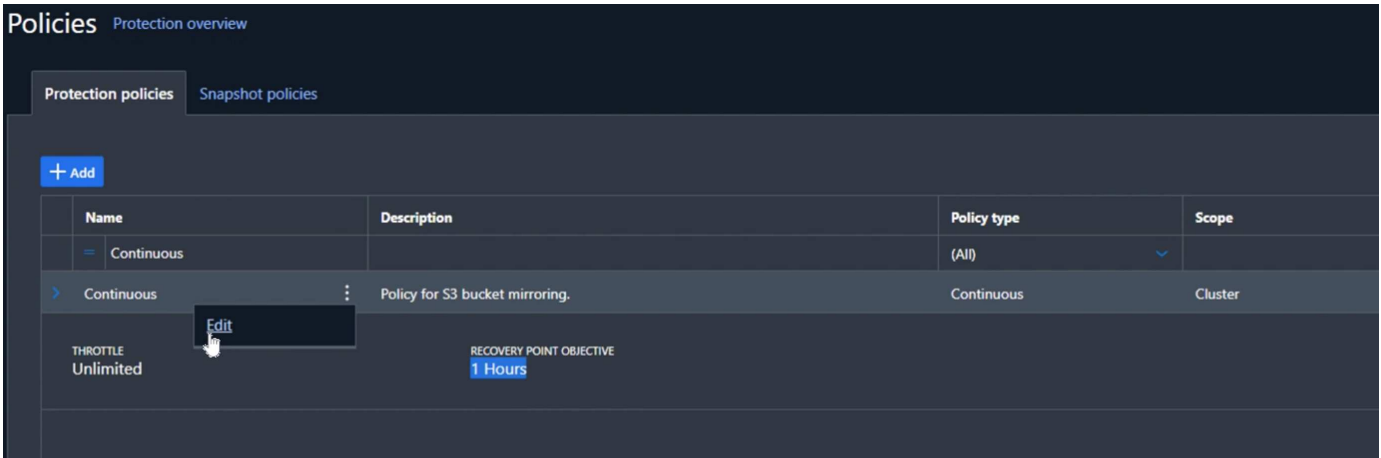
Applicable when this cluster is the source or wh...

- default
3 Schedules
- default-1weekly
3 Schedules
- none
No schedules

Schedules

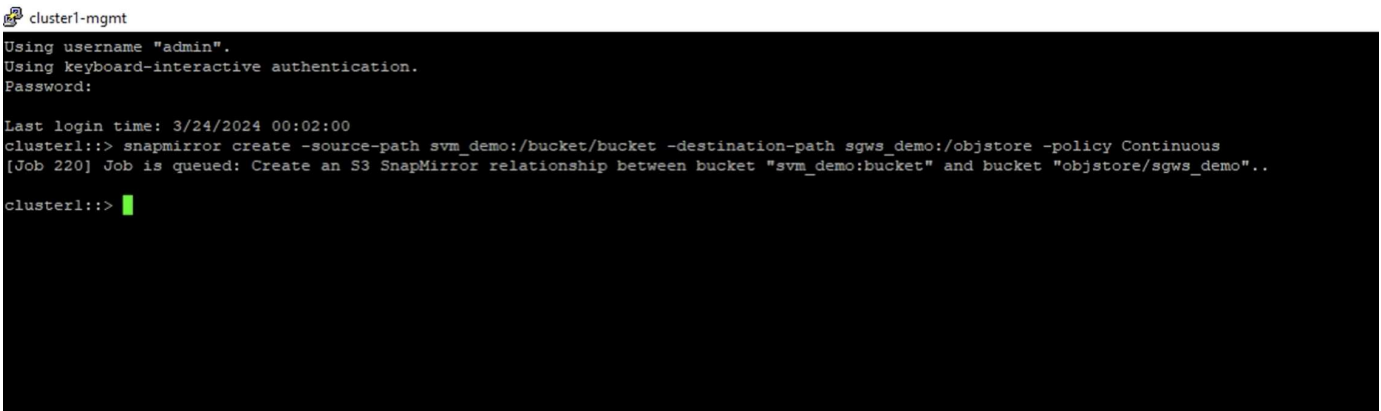
- 5min
At 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, and 55 minutes past the hour, every hour
- 6-hourly
At 12:15 AM, 06:15 AM, 12:15 PM and 06:15 PM, every day
- 8hour
At 02:15 AM, 10:15 AM and 06:15 PM, every day
- 10min
- 12-hourly

Bearbeiten Sie die kontinuierliche Richtlinie, und ändern Sie die „Recovery Point Objective“ von „1 Stunde“ auf „3 Sekunden“.



Jetzt können wir SnapMirror konfigurieren, um den Bucket zu replizieren.

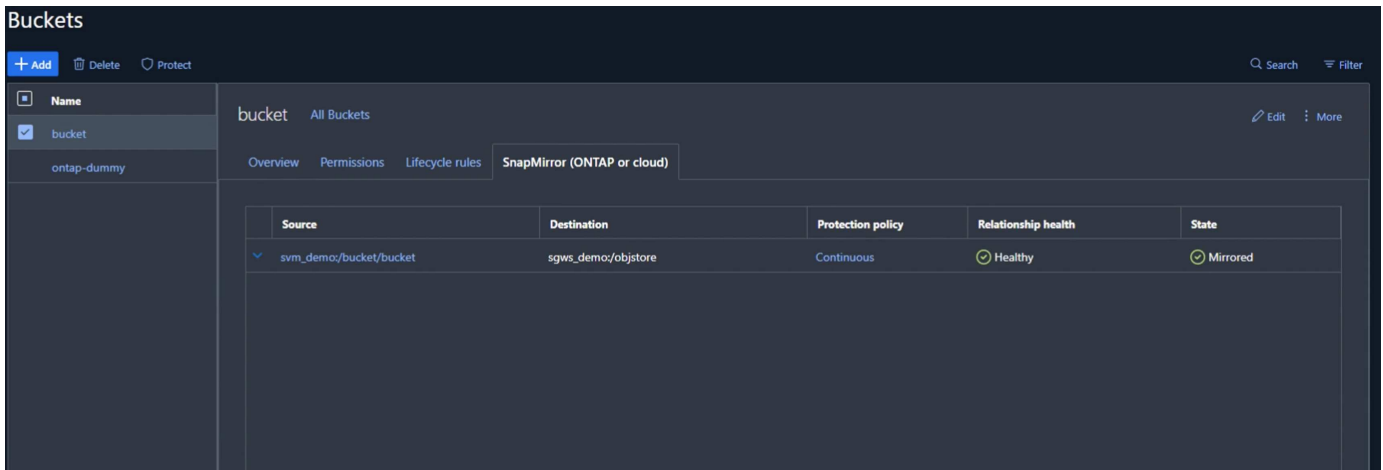
```
SnapMirror create -source-path sv_Demo: /Bucket/bucket -Destination-path sgws_Demo: /Objstore
-Policy kontinuierlich
```



Der Bucket zeigt nun ein Wolkensymbol in der Bucket-Liste unter Schutz an.

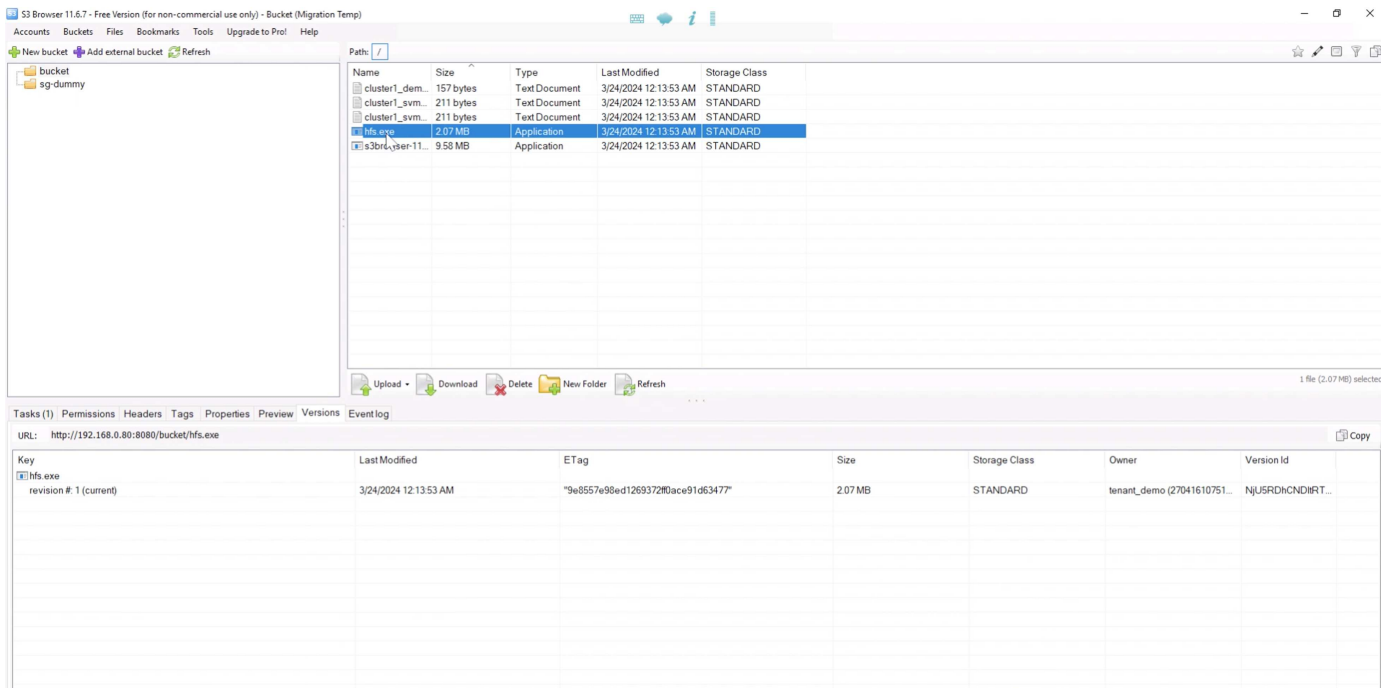


Wenn wir den Bucket auswählen und die Registerkarte „SnapMirror (ONTAP oder Cloud)“ aufrufen, wird der Status der SnapMirror-Umsendung angezeigt.



Details zur Replikation

Wir verfügen jetzt über einen erfolgreich replizierenden Bucket von ONTAP zu StorageGRID. Aber was ist eigentlich Replikation? Unsere Quelle und unser Ziel sind beide versionierte Buckets. Replizieren die vorherigen Versionen auch an das Zielsystem? Wenn wir uns unseren StorageGRID-Bucket mit S3Browser ansehen, sehen wir, dass die bestehenden Versionen nicht repliziert wurden und unser gelöschttes Objekt nicht vorhanden ist, und es gibt auch keine Löschmarkierungen für dieses Objekt. Unser dupliziertes Objekt hat nur eine Version im StorageGRID Bucket.



Fügen Sie in unserem ONTAP Bucket eine neue Version zu demselben Objekt hinzu, das wir zuvor verwendet haben, und sehen Sie sich an, wie es repliziert wurde.

The screenshot shows the S3 Browser interface for a bucket named 'bucket'. The file list includes:

Name	Size	Type	Last Modified	Storage Class
cluster1_dem...	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

The 'Versions' tab for 'hfs.exe' shows the following data:

Key	Last Modified	ETag	Size	Storage Class	Owner	Version Id
revision # 3 (current)	3/24/2024 12:14:52 AM	9e8557e98ed1269372f0ace91d63477	2 07 MB	STANDARD	Unknown (Unknown)	NTUYN0gMDAw...
revision # 2	3/23/2024 11:23:36 PM	9e8557e98ed1269372f0ace91d63477	2 07 MB	STANDARD	Unknown (Unknown)	NzQ1OTE4MDAw...
revision # 1	3/23/2024 11:23:25 PM	9e8557e98ed1269372f0ace91d63477	2 07 MB	STANDARD	Unknown (Unknown)	Njk2ODI3MDAwLn...

Wenn wir uns die StorageGRID-Seite ansehen, sehen wir, dass auch in diesem Bucket eine neue Version erstellt wurde, aber die erste Version vor der SnapMirror-Beziehung fehlt.

The screenshot shows the S3 Browser interface for a bucket named 'sg-dummy'. The file list includes:

Name	Size	Type	Last Modified	Storage Class
cluster1_dem...	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

The 'Versions' tab for 'hfs.exe' shows the following data:

Key	Last Modified	ETag	Size	Storage Class	Owner	Version Id
revision # 2 (current)	3/24/2024 12:14:56 AM	"9e8557e98ed1269372f0ace91d63477"	2 07 MB	STANDARD	tenant_demo (27041610751...	OEHRjY4NDgRT...
revision # 1	3/24/2024 12:13:53 AM	"9e8557e98ed1269372f0ace91d63477"	2 07 MB	STANDARD	tenant_demo (27041610751...	NjUR5RdHcNDIIR...

Dies liegt daran, dass der ONTAP SnapMirror S3-Prozess nur die aktuelle Version des Objekts repliziert. Aus diesem Grund haben wir auf der StorageGRID-Seite einen versionierten Bucket erstellt, um das Ziel zu sein. Auf diese Weise kann StorageGRID einen Versionsverlauf der Objekte verwalten.

Von Rafael Guedes und Aron Klein

Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

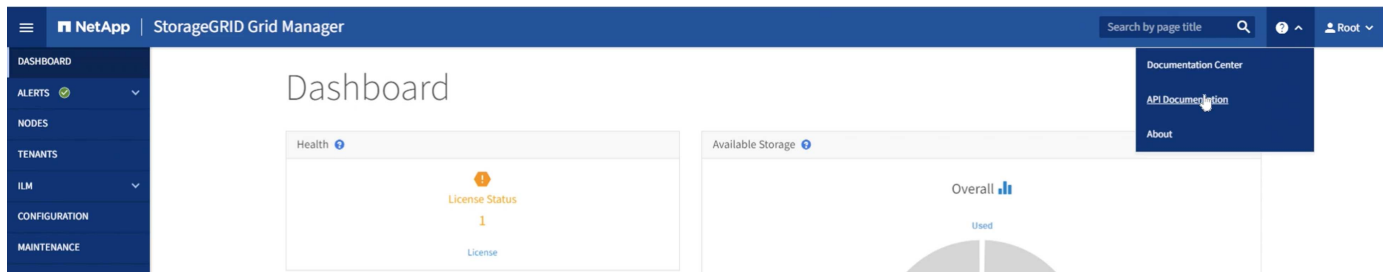
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von

objektbasiertem Storage von ONTAP S3 zu StorageGRID

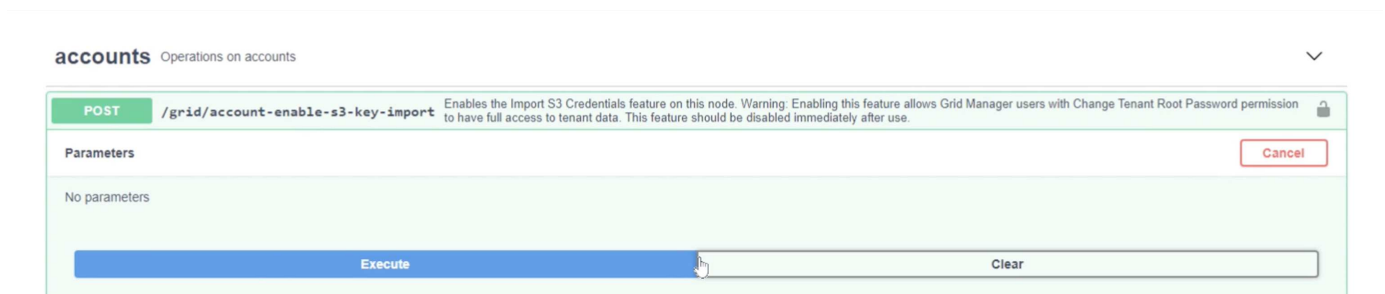
Migrieren Sie S3 Schlüssel

Bei einer Migration sollten Sie die Anmeldeinformationen für die Benutzer meistens migrieren, statt auf der Zielseite neue Anmeldeinformationen zu generieren. StorageGRID stellt API's bereit, mit denen s3 Schlüssel in einen Benutzer importiert werden können.

Durch die Anmeldung bei der StorageGRID-Management-UI (nicht der Mandanten-Manager-UI) wird die Seite „API Documentation“ geöffnet.



Erweitern Sie den Abschnitt "Accounts", wählen Sie "POST /Grid/Account-enable-s3-key-Import", klicken Sie auf "Try it out" und klicken Sie dann auf die Schaltfläche Ausführen.



Scrollen Sie jetzt noch unter „Accounts“ nach unten zu „POST /Grid/Accounts/{id}/users/{user_id}/s3-Access-keys“

Hier werden wir die Mieter-ID und die Benutzer-Konto-ID eingeben, die wir zuvor gesammelt haben. Füllen Sie die Felder und die Schlüssel von unserem ONTAP-Benutzer in der json-Box. Sie können den Ablauf der Schlüssel einstellen, oder entfernen Sie die " , "läuft ab": 123456789" und klicken Sie auf Ausführen.

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>

Nachdem Sie alle Benutzerschlüsselimporte abgeschlossen haben, sollten Sie die Schlüsselimportfunktion in „Accounts“ „POST /Grid/Account-disable-s3-key-Import“ deaktivieren.

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

Wenn wir uns das Benutzerkonto in der Mandantenmanager-UI ansehen, sehen wir, dass der neue Schlüssel hinzugefügt wurde.

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

Der letzte Cut-Over

Wenn beabsichtigt ist, einen ständig replizierenden Bucket von ONTAP auf StorageGRID zu haben, können Sie hier enden. Wenn es sich um eine Migration von ONTAP S3 zu StorageGRID handelt, ist es an der Zeit, diese zu beenden und sie zu übernehmen.

Bearbeiten Sie im ONTAP System Manager die S3-Gruppe und stellen Sie sie auf „ReadOnly Access“ ein. Dadurch wird verhindert, dass Benutzer Daten in den ONTAP S3-Bucket schreiben.

Edit group ✕

NAME

USERS

POLICIES

Cancel **Save**

Jetzt müssen Sie nur noch DNS konfigurieren, der vom ONTAP Cluster zum StorageGRID-Endpunkt führt. Stellen Sie sicher, dass Ihr Endpunktzertifikat korrekt ist, und fügen Sie die Domännennamen des Endpunkts in StorageGRID hinzu, wenn Anforderungen nach virtuellem Hosted-Stil erforderlich sind

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 +

Ihre Clients müssen entweder warten, bis die TTL abläuft, oder DNS bereinigen, um das neue System aufzulösen, damit Sie testen können, ob alles funktioniert. Alles, was noch übrig ist, ist die Bereinigung der anfänglichen temporären S3-Schlüssel, die wir zum Testen des StorageGRID-Datenzugriffs (NICHT der importierten Schlüssel) verwendet haben, um die SnapMirror-Beziehungen zu entfernen und die ONTAP-Daten zu entfernen.

Von Rafael Guedes und Aron Klein

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.