StorageGRID Lösungen und Ressourcen

StorageGRID solutions and resources

NetApp
December 12, 2025

Inhalt

StorageGRID Lösungen und Ressourcen

Schritte, um auf die StorageGRID Evaluierungssoftware zuzugreifen

Diese Schulung richtet sich an NetApp Vertriebsmitarbeiter, Partner und potenzielle Kunden, die mit NetApp zusammenarbeiten.

Für ein Konto registrieren

1. Registrieren Sie sich für ein Konto auf der "NetApp Support Website" mit Ihrer geschäftlichen E-Mail-Adresse.
   a. Stellen Sie sicher, dass Sie nicht mit dem neu erstellten Konto angemeldet sind.
   b. Wenn Sie bereits über ein Konto verfügen, stellen Sie sicher, dass Sie nicht angemeldet sind, und fahren Sie mit dem nächsten Schritt fort.
2. Erstellen Sie einen nicht-technischen Support-Fall, um die Zugriffsebenen auf „Interessenten“ zu erhöhen. Klicken Sie dazu auf den ""Problem melden"Link „ in der Fußzeile der Website.
3. Wählen Sie als Feedback-Kategorie „Registrierungsproblem“ aus.
4. Schreiben Sie im Kommentarbereich: "Meine Konto-E-Mail-Adresse ist *Your-Email-Adresse*. Ich möchte potenziellen Kunden Zugang erhalten, um die StorageGRID Evaluierungssoftware herunterzuladen.“
   a. Nennen Sie den Namen der internen Person von NetApp, die den Antrag auf Zugang für einen potenziellen Kunden vorgeschlagen hat.

Laden Sie StorageGRID herunter

1. Nachdem Ihr Support-Fall geprüft und genehmigt wurde, werden Sie vom NetApp Support per E-Mail darüber informiert, dass Ihr Konto potenziellen Kunden Zugang gewährt wurde.
2. Laden Sie die herunter "StorageGRID Evaluierungssoftware".

Die Evaluierungslizenzdatei befindet sich in der ZIP-Datei. Es handelt sich um StorageGRID-Webscale-<version>, die nach der ZIP-Datei\vsphere\NLF000000.txt verwendet wurde.

Beim Herunterladen der Software handelt es sich um einen Prozess, der Maßnahmen zur Einhaltung der gesetzlichen Vorschriften beinhaltet. Um die Compliance sicherzustellen, müssen Benutzer ein Konto erstellen und einen Support-Fall eröffnen, bevor sie Zugang erhalten. Dieser Prozess hilft uns dabei, die Kontrolle und Dokumentation aufrechtzuerhalten und Interessenten die für die Produktion benötigte Software zur Verfügung zu stellen.

Wir stellen die „produktionsbereite“ Version von StorageGRID bereit, die weder eine Open Source noch eine alternative Version ist. Es ist wichtig zu beachten, dass **Support nicht zur Verfügung gestellt wird** es sei denn, der potenzielle Kunde aktualisiert auf eine Produktionslizenz.

Bitte wenden Sie sich an StorageGRID.Feedback@netapp.com, wenn Sie Probleme mit den oben genannten Schritten haben.

Validierte Lösungen von Drittanbietern

Validierte Lösungen von Drittanbietern: Überblick

In Zusammenarbeit mit unseren Partnern hat NetApp diese Lösungen zur Verwendung mit StorageGRID validiert. Lesen Sie die Informationen in diesem Abschnitt, um zu erfahren, welche Lösungen validiert wurden, und um weitere Anweisungen, falls zutreffend, zu erhalten.

Im Team mit NetApp erweitern Sie Ihr Portfolio schneller, erzielen einen höheren Bekanntheitsgrad und generieren Umsätze, indem Sie getestete, erstklassige NetApp Lösungen entwickeln. "Werden Sie noch heute Alliance-Partner".

Für StorageGRID 12.0 validierte Lösungen von Drittanbietern

Die folgenden Lösungen von Drittanbietern wurden für die Verwendung mit StorageGRID 12.0 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Kundenbetreuer.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Alluxio
- Apache Kafka
- AWS Bereitstellungspunkt
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Collibra (Minimum Collibra Data Quality Version 2024.02)
- Commvault 11
- Couchbase Enterprise Analytics 2.0
- Ctera Portal 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover-Daten
- Dremio
- Elasticsearch-Snapshot (einschließlich eingefrorener Tier)
- Emam

- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet
- IBM Storage Protect
- Interica
- Komprise
- Microsoft SQL Server Big Data-Cluster
- Model9
- Modzy
- Moonwalk Universal
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 Build 220706 oder höher
- Rubrik CDM
- s3a
- Signiant
- Schneeflocke
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Starburst
- Storage Leicht Gemacht
- Trino
- Lack Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 und höher
- Vertica 10.x

- Vidispine
- Virtalica StorageFabric
- WEKA v3.10 oder höher

Lösungen von Drittanbietern, die auf StorageGRID mit Objektsperre validiert wurden

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Commvault 11, Feature Release 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 und höher

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Auf StorageGRID unterstützte Schlüsselmanager

Diese Lösungen wurden getestet.

- Entrust Kryptografische Sicherheitsplattform v10.4.5
- Vertrauen Sie KeyControl 10.2 an
- Hashicorp Vault 1.20.2
- Thales CipherTrust Manager 2.20

StorageGRID 11.9 validierte Lösungen von Drittanbietern

Die folgenden Drittanbieterlösungen wurden für die Verwendung mit StorageGRID 11.9 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Alluxio
- Apache Kafka
- AWS Bereitstellungspunkt
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Collibra (Minimum Collibra Data Quality Version 2024.02)
- Commvault 11
- Couchbase Enterprise Analytics 2.0
- Ctera Portal 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover-Daten
- Dremio
- Elasticsearch-Snapshot (einschließlich eingefrorener Tier)
- Emam
- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet

- IBM Storage Protect
- Interica
- Komprise
- Microsoft SQL Server Big Data-Cluster
- Model9
- Modzy
- Moonwalk Universal
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 Build 220706 oder höher
- Rubrik CDM
- s3a
- Signiant
- Schneeflocke
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Starburst
- Storage Leicht Gemacht
- Trino
- Lack Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 und höher
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric
- WEKA v3.10 oder höher

Lösungen von Drittanbietern, die auf StorageGRID mit Objektsperre validiert wurden

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Commvault 11, Feature Release 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 und höher

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Auf StorageGRID unterstützte Schlüsselmanager

Diese Lösungen wurden getestet.

- Entrust Kryptografische Sicherheitsplattform v10.4.5

- Vertrauen Sie KeyControl 10.2 an
- Hashicorp Vault 1.15.0
- Thales CipherTrust Manager 2.0
- Thales CipherTrust Manager 2.1
- Thales CipherTrust Manager 2.2
- Thales CipherTrust Manager 2.3
- Thales CipherTrust Manager 2.4
- Thales CipherTrust Manager 2.8
- Thales CipherTrust Manager 2.9
- Thales CipherTrust Manager 2.10
- Thales CipherTrust Manager 2.11
- Thales CipherTrust Manager 2.12
- Thales CipherTrust Manager 2.13
- Thales CipherTrust Manager 2.14
- Thales CipherTrust Manager 2.15
- Thales CipherTrust Manager 2.16
- Thales CipherTrust Manager 2.20

StorageGRID 11.8 validierte Lösungen von Drittanbietern

Die folgenden Drittanbieterlösungen wurden für die Verwendung mit StorageGRID 11.8 validiert.
Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Alluxio
- Apache Kafka
- AWS Bereitstellungspunkt
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Collibra (Minimum Collibra Data Quality Version 2024.02)
- Commvault 11
- Ctera Portal 6
- Dalet

- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover-Daten
- Dremio
- Elasticsearch-Snapshot (einschließlich eingefrorener Tier)
- Emam
- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet
- IBM Storage Protect
- Interica
- Komprise
- Microsoft SQL Server Big Data-Cluster
- Model9
- Modzy
- Moonwalk Universal
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 Build 220706 oder höher
- Rubrik CDM
- s3a
- Signiant
- Schneeflocke
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Starburst

- Storage Leicht Gemacht
- Trino
- Lack Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 und höher
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric
- WEKA v3.10 oder höher

Lösungen von Drittanbietern, die auf StorageGRID mit Objektsperre validiert wurden

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Commvault 11, Feature Release 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 und höher

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Milestone Systems

- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Auf StorageGRID unterstützte Schlüsselmanager

Diese Lösungen wurden getestet.

- Vertrauen Sie KeyControl 10.2 an
- Hashicorp Vault 1.15.0
- Thales CipherTrust Manager 2.0
- Thales CipherTrust Manager 2.1
- Thales CipherTrust Manager 2.2
- Thales CipherTrust Manager 2.3
- Thales CipherTrust Manager 2.4
- Thales CipherTrust Manager 2.8
- Thales CipherTrust Manager 2.9
- Thales CipherTrust Manager 2.10
- Thales CipherTrust Manager 2.11
- Thales CipherTrust Manager 2.12
- Thales CipherTrust Manager 2.13
- Thales CipherTrust Manager 2.14

StorageGRID 11.7 validierte Lösungen von Drittanbietern

Die folgenden Drittanbieterlösungen wurden für die Verwendung mit StorageGRID 11.7 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Alluxio
- Apache Kafka
- AWS Bereitstellungspunkt
- Bridgestor
- Cantemo

- Citrix Content Collaboration
- Collibra (Minimum Collibra Data Quality Version 2024.02)
- Commvault 11
- Ctera Portal 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover-Daten
- Dremio
- Elasticsearch-Snapshot (einschließlich eingefrorener Tier)
- Emam
- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet
- IBM Spectrum Protect Plus
- IBM Storage Protect
- Interica
- Komprise
- Microsoft SQL Server Big Data-Cluster
- Model9
- Modzy
- Moonwalk Universal
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 Build 220706 oder höher
- Rubrik CDM

- s3a
- Signiant
- Schneeflocke
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Storage Leicht Gemacht
- Trino
- Lack Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 10.1.1 und höher
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric
- WEKA v3.10 oder höher

Lösungen von Drittanbietern, die auf StorageGRID mit Objektsperre validiert wurden

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Commvault 11, Feature Release 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 und höher

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive

- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Auf StorageGRID unterstützte Schlüsselmanager

Diese Lösungen wurden getestet.

- Thales CipherTrust Manager 2.0
- Thales CipherTrust Manager 2.1
- Thales CipherTrust Manager 2.2
- Thales CipherTrust Manager 2.3
- Thales CipherTrust Manager 2.4
- Thales CipherTrust Manager 2.8
- Thales CipherTrust Manager 2.9

StorageGRID 11.6 validierte Drittanbieterlösungen

Die folgenden Drittanbieterlösungen wurden zur Verwendung mit StorageGRID 11.6 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Alluxio
- Apache Kafka
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Commvault 11
- Ctera Portal 6

- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Diskover-Daten
- Dremio
- Emam
- Fujifilm Object Archive
- GitHub Enterprise Server
- IBM FileNet
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Microsoft SQL Server Big Data-Cluster
- Model9
- Modzy
- Moonwalk Universal
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 Build 220706 oder höher
- Rubrik CDM
- s3a
- Signiant
- Schneeflocke
- Spectra Logic On-Prem Glacier
- Splunk Smartstore
- Storage Leicht Gemacht

- Trino
- Lack Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric
- WEKA v3.10 oder höher

Lösungen von Drittanbietern, die auf StorageGRID mit Objektsperre validiert wurden

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Commvault 11, Feature Release 26
- IBM FileNet
- OpenText Documentum 21.4
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 und höher

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak

- SoftNAS
- QStar
- Velasea

StorageGRID 11.5 validierte Drittanbieterlösungen

Die folgenden Drittanbieterlösungen wurden zur Verwendung mit StorageGRID 11.5 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Alluxio
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Commvault 11
- Ctera Portal 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Interica
- Komprise
- Moonwalk Universal
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM

- s3a
- Signiant
- Splunk Smartstore
- Trino
- Lack Enterprise 6.0.4
- Veeam 11
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric

Lösungen von Drittanbietern, die auf StorageGRID mit Objektsperre validiert wurden

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- OpenText Documentum 21.4
- Veeam 11

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS

- QStar
- Velasea

StorageGRID 11.4 validierte Drittanbieterlösungen

Die folgenden Drittanbieterlösungen wurden zur Verwendung mit StorageGRID 11.4 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Commvault 11
- Ctera Portal 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Interica
- Komprise
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM
- Signiant
- Splunk Smartstore
- Lack Enterprise 6.0.4
- Veeam 9.5.4

- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 11.3 validierte Drittanbieterlösungen

Die folgenden Drittanbieterlösungen wurden zur Verwendung mit StorageGRID 11.3 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Bridgestor
- Cantemo
- Citrix Content Collaboration

- Commvault 11
- Ctera Portal 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Interica
- Komprise
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- Splunk Smartstore
- Lack Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vidispine

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive

- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 11.2 validierte Drittanbieterlösungen

Die folgenden Drittanbieterlösungen wurden zur Verwendung mit StorageGRID 11.2 validiert. + Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Drittanbieterlösungen, die auf StorageGRID validiert sind

Diese Lösungen wurden in Zusammenarbeit mit den jeweiligen Partnern getestet.

- Actifio
- Bridgestor
- Cantemo
- Citrix Content Collaboration
- Commvault 11
- Ctera Portal 6
- Dalet
- Datadobi
- Data Dynamics StorageX
- DefendX
- Interica
- Komprise
- SCHÖN
- Nasuni
- OpenText Documentum 16.4
- OpenText Media Management 16.5 mit CyanGate Cloud
- Panzura
- Gateway für die Archivierung 2.0
- Punkt Storage Manager 6.4
- Primestream

- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- Splunk Smartstore
- Lack Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vidispine

Von StorageGRID unterstützte Lösungen von Drittanbietern

Diese Lösungen wurden getestet.

- Archiware
- Axis Communications
- Kongruation360
- DataFrameworks
- EcoDigital DIVA-Plattform
- Encoding.com
- Fujifilm Object Archive
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera
- Milestone Systems
- OnSSI
- Schubmotor
- SilverTrak
- SoftNAS
- QStar
- Velasea

Produktfunktionshandbücher

RPO von null mit StorageGRID – Ein umfassender Leitfaden zur Replizierung an mehreren Standorten

Dieser technische Bericht bietet eine umfassende Anleitung zur Implementierung von StorageGRID Replikationsstrategien, um im Falle eines Standortausfalls ein Recovery Point Objective (RPO) von Null zu erreichen. Das Dokument beschreibt detailliert verschiedene Bereitstellungsoptionen für StorageGRID, darunter standortübergreifende synchrone Replikation und standortübergreifende asynchrone Replikation. Darin wird erläutert, wie StorageGRID Information Lifecycle Management (ILM)-Richtlinien konfiguriert werden können, um die Datenbeständigkeit und -verfügbarkeit über mehrere Standorte hinweg zu gewährleisten. Darüber hinaus behandelt der Bericht Leistungsaspekte, Fehlerszenarien und Wiederherstellungsprozesse, um einen ununterbrochenen Kundenbetrieb zu gewährleisten. Ziel dieses Dokuments ist es, Informationen bereitzustellen, die sicherstellen, dass die Daten auch im Falle eines vollständigen Ausfalls der Website zugänglich und konsistent bleiben, indem sowohl synchrone als auch asynchrone Replikationstechniken genutzt werden.

Übersicht über StorageGRID

NetApp StorageGRID ist ein objektbasiertes Storage-System, das die branchenübliche API Amazon Simple Storage Service (Amazon S3) unterstützt.

StorageGRID bietet einen Single Namespace über mehrere Standorte mit variablen Service-Leveln basierend auf Information Lifecycle Management-Richtlinien (ILM). Mit diesen Lebenszyklusrichtlinien können Sie den Speicherort Ihrer Daten während ihres gesamten Lebenszyklus optimieren.

StorageGRID ermöglicht die konfigurierbare Aufbewahrung und Verfügbarkeit Ihrer Daten in lokalen und geografisch verteilten Lösungen. Unabhängig davon, ob sich Ihre Daten vor Ort oder in einer öffentlichen Cloud befinden, ermöglichen integrierte Hybrid-Cloud-Workflows Ihrem Unternehmen die Nutzung von Cloud-Diensten wie Amazon Simple Notification Service (Amazon SNS), Google Cloud, Microsoft Azure Blob, Amazon S3 Glacier, Elasticsearch und mehr.

StorageGRID Scale

Eine minimale StorageGRID Bereitstellung besteht aus einem Admin-Knoten und 3 Speicherknoten an einem einzigen Standort. Ein einzelnes Grid kann auf bis zu 220 Knoten anwachsen. StorageGRID kann als einzelner Standort eingesetzt oder auf bis zu 16 Standorte erweitert werden.

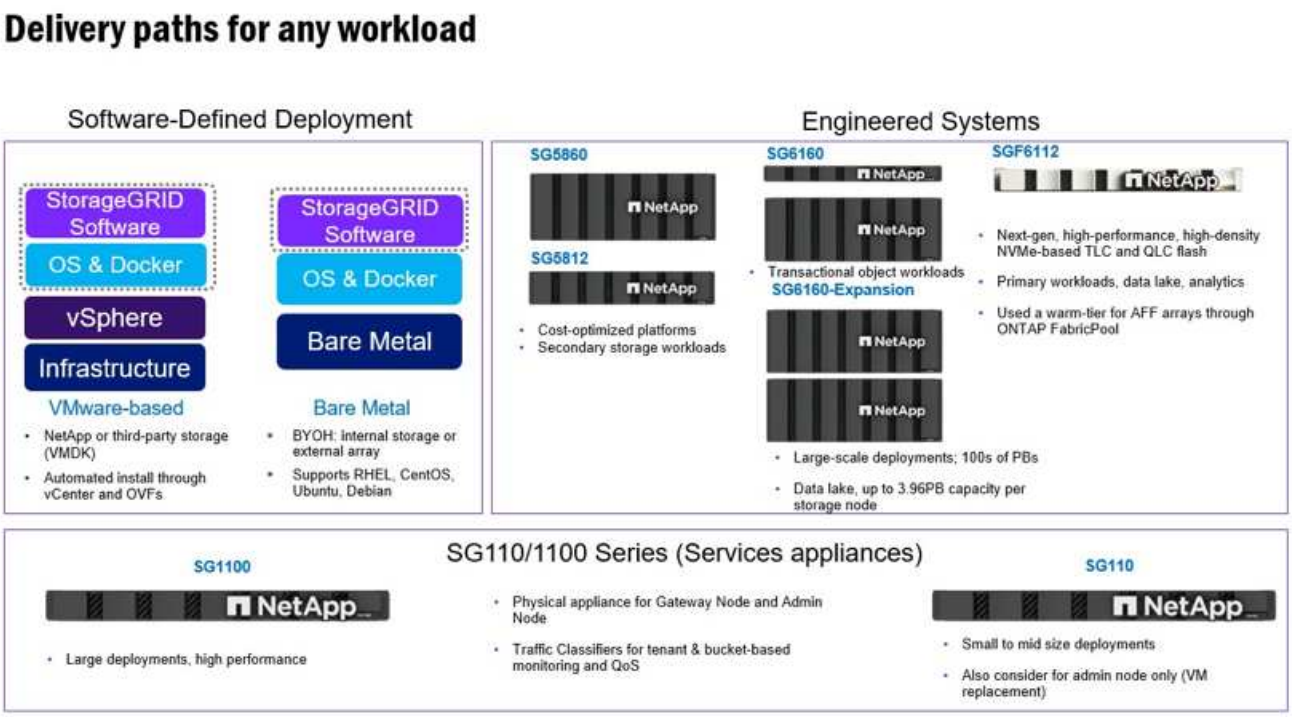
Der Admin-Knoten enthält die Verwaltungsschnittstelle, einen zentralen Punkt für Metriken und Protokollierung und verwaltet die Konfiguration der StorageGRID Komponenten. Der Admin-Knoten enthält außerdem einen integrierten Load Balancer für den S3-API-Zugriff.

StorageGRID kann als reine Software, als VMware Virtual Machine Appliances oder als speziell entwickelte Appliances bereitgestellt werden.

Ein Speicherknoten kann wie folgt bereitgestellt werden:

- Ein reiner Metadatenknoten, der die Objektanzahl maximiert
- Ein reiner Objektspeicherknoten, der den Objektspeicherplatz maximiert
- Ein kombinierter Metadaten- und Objektspeicherknoten, der sowohl die Objektanzahl als auch den Objektspeicherplatz hinzufügt

Jeder Speicherknoten kann für die Objektspeicherung auf eine Kapazität von mehreren Petabyte skaliert werden, wodurch ein einzelner Namespace im Bereich von Hunderten von Petabyte möglich ist. StorageGRID bietet außerdem einen integrierten Load Balancer für S3-API-Operationen, der als Gateway-Knoten bezeichnet wird.



StorageGRID besteht aus einer Sammlung von Knoten, die in einer Site-Topologie platziert sind. Ein Standort in StorageGRID kann ein eindeutiger physischer Standort sein oder sich als logisches Konstrukt an einem gemeinsam genutzten physischen Standort wie andere Standorte im Grid befinden. Eine StorageGRID -Site sollte sich nicht über mehrere physische Standorte erstrecken. Ein Standort stellt eine gemeinsam genutzte Infrastruktur und Fehlerdomäne eines lokalen Netzwerks (LAN) dar.

StorageGRID und Ausfall-Domains

StorageGRID umfasst mehrere Schichten von Ausfall-Domains, die Sie bei der Entscheidung, wie Sie Ihre Lösung planen, wie Sie Ihre Daten speichern und wo Ihre Daten gespeichert werden sollten, um das Risiko von Ausfällen zu mindern.

- Grid-Ebene – Ein Grid, das aus mehreren Standorten besteht, kann einen Standortausfall oder eine Isolierung aufweisen, und der/die zugängliche(n) Standort(e) kann/können weiterhin als Grid betrieben werden.
- Standort-Ebene – Ausfälle innerhalb eines Standorts können den Betrieb dieses Standorts beeinträchtigen, beeinträchtigen aber nicht den Rest des Grids.
- Node-Ebene – Ein Node-Ausfall hat keine Auswirkungen auf den Betrieb des Standorts.

- Festplattenebene – ein Festplattenausfall beeinträchtigt den Betrieb des Node nicht.

Objektdaten und Metadaten

Bei Objekt-Storage ist die Storage-Einheit ein Objekt und nicht eine Datei oder ein Block. Im Gegensatz zur Baumstruktur eines File-Systems oder Block-Storage werden die Daten im Objekt-Storage in einem flachen, unstrukturierten Layout organisiert. Objekt-Storage entkoppelt den physischen Standort der Daten von der Methode zum Speichern und Abrufen dieser Daten.

Jedes Objekt in einem objektbasierten Storage-System besteht aus zwei Teilen: Objekt-Daten und Objekt-Metadaten.

- Objektdaten stellen die eigentlichen zugrunde liegenden Daten dar, zum Beispiel ein Foto, einen Film oder eine Krankenakte.
- Objektmetadaten sind alle Informationen, die ein Objekt beschreiben.

StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im Grid zu verfolgen und den Lebenszyklus eines jeden Objekts mit der Zeit zu managen.

Objektmetadaten enthalten Informationen wie die folgenden:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt, des Objektnamens, des Namens des S3-Buckets, des Mandantenkontonamens oder der ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Erstellung des Objekts sowie des Datums und der Uhrzeit der letzten Änderung des Objekts.
- Der aktuelle Speicherort der Replikatkopie oder des löschcodierten Fragments jedes Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüssel-Wert-Paare vorhanden
- Für segmentierte Objekte und mehrteilige Objekte, Segmentkennungen und Datengrößen.

Objektmetadaten sind individuell anpassbar und erweiterbar und bieten dadurch Flexibilität für die Nutzung von Applikationen. Detaillierte Informationen darüber, wie und wo StorageGRID Objektmetadaten speichert, finden Sie unter "Management von Objekt-Metadaten-Storage".

Das Information Lifecycle Management-System (ILM) von StorageGRID wird zur Orchestrierung der Platzierung, Dauer und Aufnahme aller Objektdaten in Ihrem StorageGRID System verwendet. ILM-Regeln bestimmen, wie StorageGRID Objekte mithilfe von Replikaten der Objekte oder Erasure Coding eines Objekts über Nodes und Standorte hinweg im Zeitverlauf speichert. Dieses ILM-System ist für die Konsistenz der Objektdaten in einem Grid verantwortlich.

Erasure Coding

StorageGRID bietet die Möglichkeit, Codedaten auf Knoten- und Laufwerksebene zu löschen. Mit StorageGRID -Geräten löschen wir die auf jedem Knoten gespeicherten Daten auf allen Laufwerken innerhalb des Knotens und bieten so lokalen Schutz vor mehreren Festplattenausfällen, die zu Datenverlust oder Unterbrechungen führen. Wiederherstellungen nach Laufwerksfehlern erfolgen lokal auf dem Knoten und erfordern keine Datenreplikation über das Netzwerk.

Darüber hinaus verwenden StorageGRID Geräte Erasure-Coding-Schemata, um Objektdaten über die Knoten innerhalb eines Standorts oder verteilt auf drei oder mehr Standorte im StorageGRID -System zu speichern, wobei die ILM-Regeln von StorageGRID vor Knotenausfällen schützen.

Erasure Coding bietet ein Speicherlayout, das gegenüber Knoten- und Standortausfällen robust ist und einen

geringeren Aufwand als die Replikation verursacht. Alle StorageGRID -Erasure-Coding-Verfahren sind an einem einzigen Standort einsetzbar, sofern die Mindestanzahl der Knoten, die zum Speichern der Datenblöcke erforderlich sind, erreicht ist. Das bedeutet, dass für ein EC-Schema von 4+2 mindestens 6 Knoten zur Verfügung stehen müssen, um die Daten zu empfangen.

Erasure-coding scheme (*k+m*)	Minimum number of deployed sites	Recommended number of Storage Nodes at each site	Total recommended number of Storage Nodes	Site loss protection?	Storage overhead
4+2	3	3	9	Yes	50%
6+2	4	3	12	Yes	33%
8+2	5	3	15	Yes	25%
6+3	3	4	12	Yes	50%
9+3	4	4	16	Yes	33%
2+1	3	3	9	Yes	50%
4+1	5	3	15	Yes	25%
6+1	7	3	21	Yes	17%
7+5	3	5	15	Yes	71%

Metadatenkonsistenz

In StorageGRID werden Metadaten normalerweise mit drei Replikaten pro Standort gespeichert, um Konsistenz und Verfügbarkeit zu gewährleisten. Diese Redundanz trägt dazu bei, die Datenintegrität und -Verfügbarkeit auch bei einem Ausfall aufrechtzuerhalten.

Die Standardkonsistenz wird auf einer Grid-weiten Ebene definiert. Benutzer können die Konsistenz auf Bucket-Ebene jederzeit ändern.

Die in StorageGRID verfügbaren Bucket-Konsistenzoptionen sind:

- **All**: Bietet die höchste Konsistenz. Alle Nodes im Grid erhalten die Daten sofort, andernfalls schlägt die Anforderung fehl.
- **Stark-global**:
  - **Legacy Strong Global**: Gewährleistet Lese-nach-Schreib-Konsistenz für alle Client-Anfragen an allen Standorten.
    - Dies ist das Standardverhalten für alle Systeme, die von Version 11.9 oder älter auf Version 12.0 aktualisiert wurden, ohne dass manuell auf das neue Quorum Strong Global umgestellt wurde.
  - **Quorum Strong-global**: Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites. Bietet Konsistenz für mehrere Knoten oder sogar einen Site-Ausfall, wenn das Quorum für die Metadatenreplikation erreicht werden kann.
    - Dies ist das Standardverhalten für alle Systeme, die neu mit Version 12.0 oder höher installiert werden.

    - QUORUM-Konsistenz wird als Quorum von Storage Node-Metadatenreplikaten definiert, wobei jeder Standort über 3 Metadatenreplikate verfügt. Es kann wie folgt berechnet werden: 1+((N*3)/2), wobei N die Gesamtzahl der Standorte ist
    - Beispielsweise müssen aus einem Raster mit 3 Standorten mindestens 5 Replikate erstellt werden, innerhalb eines Standorts dürfen maximal 3 Replikate vorhanden sein.
- **Strong-site**: Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.
- **Read-after-New-write**(default): Bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
- **Verfügbar**: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

Konsistenz von Objektdaten

Metadaten werden automatisch innerhalb von und über Standorte hinweg repliziert, Entscheidungen zur Platzierung von Objektdaten liegen bei Ihnen. Objektdaten können in Replikaten innerhalb und über Standorte hinweg gespeichert werden, in Erasure Coding innerhalb von oder über Standorte hinweg, in einer Kombination oder in Replikaten und in Storage-Schemata, die nach Erasure Coding codiert sind. ILM-Regeln können für alle Objekte angewendet oder so gefiltert werden, dass sie nur für bestimmte Objekte, Buckets oder Mandanten gelten. ILM-Regeln legen fest, wie Objekte gespeichert werden, wie Replikate und/oder Erasure Coding codiert wird, wie lange Objekte an diesen Standorten gespeichert werden, ob sich die Anzahl der Replikate oder Erasure Coding-Schemata ändert oder sich der Standort im Laufe der Zeit ändert.

Jede ILM-Regel wird mit einem von drei Aufnahmeverhalten zum Schutz von Objekten konfiguriert: Dual Commit, Balanced oder Strict.

Die Dual-Commit-Option erstellt sofort zwei Kopien auf zwei beliebigen verschiedenen Speicherknoten im Grid und meldet dem Client, dass die Anfrage erfolgreich war. Die Knotenauswahl erfolgt innerhalb des Standorts der Anfrage, kann aber unter bestimmten Umständen auch Knoten eines anderen Standorts verwenden. Das Objekt wird der ILM-Warteschlange hinzugefügt, um gemäß den ILM-Regeln ausgewertet und platziert zu werden.

Die Option „ausgewogen“ wertet das Objekt sofort anhand der ILM-Richtlinie aus und platziert das Objekt synchron, bevor die Anfrage als erfolgreich an den Client zurückgesendet wird. Kann die ILM-Regel aufgrund eines Ausfalls oder unzureichenden Speicherplatzes zur Erfüllung der Platzierungsanforderungen nicht sofort eingehalten werden, wird stattdessen Dual Commit verwendet. Sobald das Problem behoben ist, platziert ILM das Objekt automatisch gemäß der definierten Regel.

Die strikte Option wertet das Objekt sofort anhand der ILM-Richtlinie aus und platziert das Objekt synchron, bevor die Anfrage als erfolgreich an den Client zurückgesendet wird. Kann die ILM-Regel aufgrund eines Ausfalls oder unzureichenden Speicherplatzes zur Erfüllung der Platzierungsanforderungen nicht sofort erfüllt werden, schlägt die Anfrage fehl und der Kunde muss es erneut versuchen.

Lastverteilung

StorageGRID kann mit Client-Zugriff über die integrierten Gateway-Nodes, einen externen Load Balancer von 3Rd Party, DNS-Round Robin oder direkt zu einem Storage-Node implementiert werden. Mehrere Gateway Nodes können an einem Standort implementiert und in Hochverfügbarkeitsgruppen konfiguriert werden, die für automatisches Failover und Failback bei einem Ausfall des Gateway Node sorgen. Sie können Lastausgleichsmethoden in einer Lösung kombinieren, um einen zentralen Zugriffspunkt für alle Standorte in einer Lösung bereitzustellen.

Die Gateway-Knoten gleichen standardmäßig die Last zwischen den Speicherknoten an dem Standort aus, an dem sich der Gateway-Knoten befindet. StorageGRID kann so konfiguriert werden, dass die Gateway-Knoten die Last mithilfe von Knoten von mehreren Standorten ausgleichen können. Diese Konfiguration würde die Latenz zwischen diesen Standorten zur Antwortlatenz der Clientanfragen addieren. Diese Konfiguration sollte nur vorgenommen werden, wenn die Gesamtlatenz für die Clients akzeptabel ist.

Durch eine Kombination aus lokalem und globalem Lastausgleich kann ein RTO von Null erreicht werden. Um einen unterbrechungsfreien Clientzugriff zu gewährleisten, ist ein Lastausgleich der Clientanfragen erforderlich. Eine StorageGRID Lösung kann an jedem Standort viele Gateway-Knoten und Hochverfügbarkeitsgruppen enthalten. Um einen unterbrechungsfreien Zugriff für Clients an jedem Standort auch bei einem Standortausfall zu gewährleisten, sollten Sie eine externe Load-Balancing-Lösung in Kombination mit StorageGRID Gateway-Knoten konfigurieren. Konfigurieren Sie Hochverfügbarkeitsgruppen für Gateway-Knoten, die die Last innerhalb jedes Standorts verwalten, und verwenden Sie den externen Load Balancer, um die Last auf die Hochverfügbarkeitsgruppen zu verteilen. Der externe Load Balancer muss so konfiguriert sein, dass er eine Zustandsprüfung durchführt, um sicherzustellen, dass Anfragen nur an betriebsbereite Standorte gesendet werden. Weitere Informationen zum Lastausgleich mit StorageGRID finden Sie unter "Technischer Bericht zum StorageGRID Load Balancer"Die

Anforderungen für Zero RPO mit StorageGRID

Um ein Recovery Point Objective (RPO) von null in einem Objekt-Storage-System zu erreichen, ist es bei einem Ausfall entscheidend:

- Sowohl Metadaten als auch Objektinhalte werden synchron betrachtet und als konsistent betrachtet
- Der Zugriff auf den Objektinhalt bleibt trotz des Fehlers erhalten.

Bei einer Bereitstellung an mehreren Standorten ist Quorum Strong Global das bevorzugte Konsistenzmodell, um sicherzustellen, dass Metadaten über alle Standorte hinweg synchronisiert werden. Dies ist für die Erfüllung der Null-RPO-Anforderung unerlässlich.

Objekte im Speichersystem werden auf der Grundlage von Information Lifecycle Management (ILM)-Regeln gespeichert, die vorschreiben, wie und wo Daten während ihres gesamten Lebenszyklus gespeichert werden. Bei der synchronen Replikation kann man zwischen strikter Ausführung und ausgewogener Ausführung abwägen.

- Für ein RPO von null ist eine strikte Ausführung dieser ILM-Regeln nötig, da so sichergestellt wird, dass Objekte ohne Verzögerung oder Fallback an den definierten Standorten platziert werden, sodass die Datenverfügbarkeit und -Konsistenz erhalten bleiben.
- Das ILM-Balance-Aufnahmeverhalten von StorageGRID sorgt für ein Gleichgewicht zwischen Hochverfügbarkeit und Ausfallsicherheit, sodass Benutzer auch bei einem Standortausfall weiterhin Daten aufnehmen können.

Synchrone Implementierungen an mehreren Standorten

Multi-Site-Lösungen: StorageGRID ermöglicht Ihnen die synchrone Replikation von Objekten über mehrere Sites innerhalb des Grids hinweg. Durch das Einrichten von Information Lifecycle Management (ILM)-Regeln mit ausgewogenem oder striktem Verhalten werden Objekte sofort an den angegebenen Orten platziert. Durch Konfigurieren der Bucket-Konsistenzebene auf Quorum Strong Global wird auch die synchrone Metadatenreplikation sichergestellt. StorageGRID verwendet einen einzigen globalen Namespace und speichert die Platzierungsorte der Objekte als Metadaten, sodass jeder Knoten weiß, wo sich alle Kopien oder Erasure-Coded-Teile befinden. Wenn ein Objekt nicht von der Site abgerufen werden kann, von der die Anforderung gestellt wurde, wird es automatisch von einer Remote-Site abgerufen, ohne dass Failover-Verfahren erforderlich sind.

Sobald der Ausfall behoben ist, sind keine manuellen Failback-Prozesse erforderlich. Die Replizierungs-Performance hängt von dem Standort mit dem niedrigsten Netzwerkdurchsatz, der höchsten Latenz und der niedrigsten Performance ab. Die Performance eines Standorts basiert auf der Anzahl der Nodes, der Anzahl und Geschwindigkeit der CPU-Kerne, dem Arbeitsspeicher, der Anzahl der Laufwerke und den Laufwerkstypen.

Multi-Grid-Lösungen: StorageGRID kann Mandanten, Benutzer und Buckets mithilfe von Grid-übergreifender Replikation (CGR) zwischen mehreren StorageGRID-Systemen replizieren. CGR kann ausgewählte Daten auf mehr als 16 Standorte erweitern, die nutzbare Kapazität Ihres Objektspeichers erhöhen und Disaster Recovery bereitstellen. Die Replikation von Buckets mit CGR umfasst Objekte, Objektversionen und Metadaten und kann bidirektional oder einseitig erfolgen. Der Recovery-Zeitpunkt (Recovery Point Objective, RPO) hängt von der Performance des jeweiligen StorageGRID-Systems und der Netzwerkverbindungen zwischen diesen Systemen ab.

Zusammenfassung:

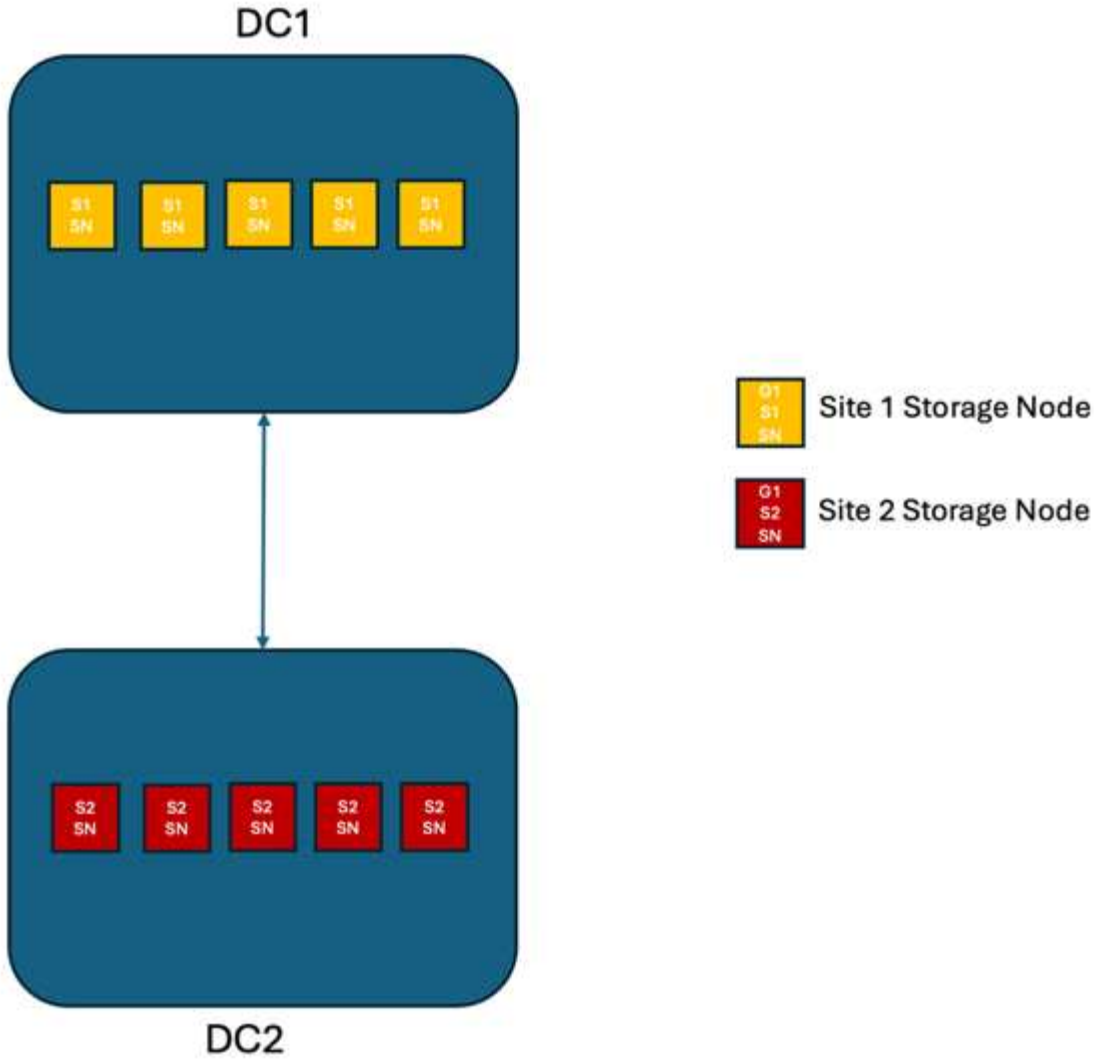
- Die Grid-interne Replizierung umfasst sowohl synchrone als auch asynchrone Replizierung, die mithilfe des ILM-Aufnahmeverhaltens und der Konsistenzkontrolle für Metadaten konfigurierbar ist.
- Die Replizierung zwischen dem Grid erfolgt nur asynchron.

Bereitstellung über mehrere Standorte in einem einzigen Grid

In den folgenden Szenarien werden die StorageGRID Lösungen mit einem optionalen externen Load Balancer konfiguriert, der die Anfragen an die integrierten Load-Balancer-Hochverfügbarkeitsgruppen verwaltet. Dadurch wird sowohl ein RTO von Null als auch ein RPO von Null erreicht. ILM ist mit Balanced Ingest Protection für die synchrone Platzierung konfiguriert. Jeder Bucket ist mit der Quorum-Version des Strong Global-Konsistenzmodells für Grids mit 3 oder mehr Standorten und der Legacy-Version des Strong Global-Konsistenzmodells für 2 Standorte konfiguriert.

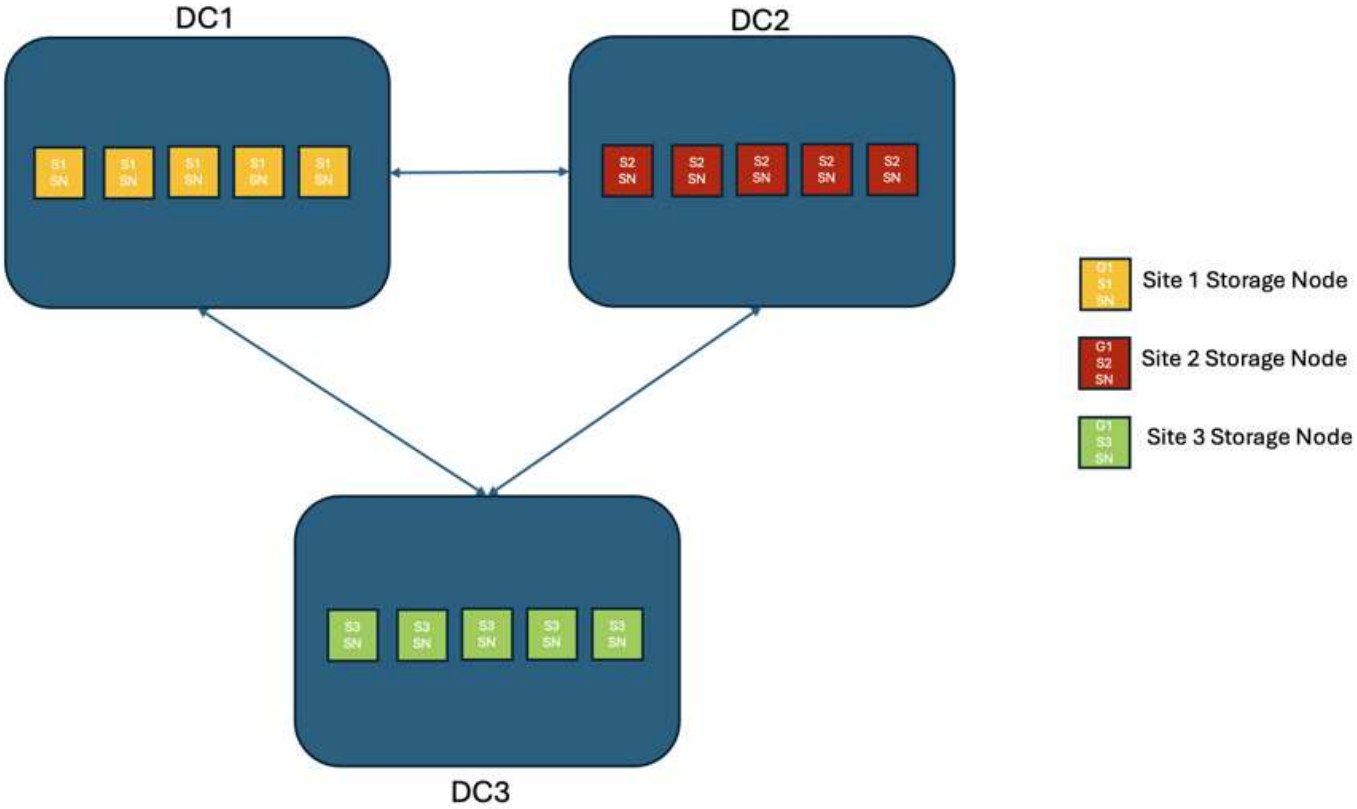
Szenario 1:

Bei einer StorageGRID Lösung mit zwei Standorten gibt es mindestens zwei Replikate jedes Objekts und sechs Replikate aller Metadaten. Nach der Wiederherstellung nach einem Ausfall werden die Aktualisierungen vom Ausfallort automatisch mit dem wiederhergestellten Standort/den wiederhergestellten Knoten synchronisiert. Bei nur zwei Standorten ist es unwahrscheinlich, dass in Ausfallszenarien, die über einen vollständigen Standortausfall hinausgehen, ein RPO von Null erreicht werden kann.



Szenario 2:

In einer StorageGRID Lösung mit drei oder mehr Standorten gibt es mindestens 3 Replikate oder 3 EC-Chunks von jedem Objekt und 9 Replikate aller Metadaten. Nach der Wiederherstellung nach einem Ausfall werden die Aktualisierungen vom Ausfallort automatisch mit dem wiederhergestellten Standort/den wiederhergestellten Knoten synchronisiert. Mit drei oder mehr Standorten ist es möglich, einen RPO von Null zu erreichen.



Ausfallszenarien für mehrere Standorte

Ausfall	Ergebnis an zwei Standorten + Vermächtnis Starke globale Präsenz	Ergebnis von 3 oder mehr Standorten + Quorum Strong Global
Ausfall eines Laufwerks mit einem Node	Jede Appliance nutzt mehrere Festplattengruppen und kann den Ausfall von mindestens einem Laufwerk pro Gruppe ohne Unterbrechung oder Datenverlust überstehen.	Jede Appliance nutzt mehrere Festplattengruppen und kann den Ausfall von mindestens einem Laufwerk pro Gruppe ohne Unterbrechung oder Datenverlust überstehen.
Ausfall eines einzelnen Nodes an einem Standort	Keine Unterbrechung von Prozessen oder Datenverlust:	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall mehrerer Nodes an einem Standort	Auf diesen Standort gerichtete Unterbrechung von Client-Vorgängen, jedoch kein Datenverlust. Der auf den anderen Standort gerichtete Betrieb bleibt ohne Unterbrechung und ohne Datenverlust erhalten.	Der Betrieb wird auf alle anderen Standorte geleitet und erfolgt ohne Unterbrechung und Datenverlust.

Ausfall	Ergebnis an zwei Standorten + Vermächtnis Starke globale Präsenz	Ergebnis von 3 oder mehr Standorten + Quorum Strong Global
Ausfall eines einzelnen Nodes an mehreren Standorten	Keine Unterbrechungen oder Datenverluste bei: • Im Raster existiert mindestens eine Replikatkopie. • Im Raster sind ausreichend EC-Blöcke vorhanden Betriebsausfall und Gefahr von Datenverlusten bei: • Es existieren keine Duplikate. • Es sind nicht genügend EC-Spannfutter vorhanden	Keine Unterbrechungen oder Datenverluste bei: • Im Raster existiert mindestens eine einzige Replikatkopie. • Im Raster sind ausreichend EC-Blöcke vorhanden Betriebsausfall und Gefahr von Datenverlusten bei: • Es existieren keine Duplikate. • Es sind nicht genügend EC-Chucks vorhanden, um das Objekt abzurufen
Ausfall eines einzelnen Standorts	Einige Clientvorgänge werden unterbrochen, bis die Störung behoben ist. GET- und HEAD-Operationen werden ohne Unterbrechung fortgesetzt. Reduzieren Sie die Bucket-Konsistenz auf „Lesen nach neuem Schreiben“ oder niedriger, um den Betrieb in diesem Fehlerzustand ununterbrochen fortzusetzen.	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines Standorts und eines einzelnen Node	Einige Clientvorgänge werden unterbrochen, bis der Fehler behoben ist. Der Betrieb von HEAD wird ohne Unterbrechung fortgesetzt. GET-Operationen werden ohne Unterbrechung fortgesetzt, wenn eine Replikatkopie oder ausreichend viele EC-Chunks vorhanden sind. Reduzieren Sie die Bucket-Konsistenz auf „Lesen nach neuem Schreiben“ oder niedriger, um den Betrieb in diesem Fehlerzustand ununterbrochen fortzusetzen.	Keine Betriebsunterbrechung oder Datenverlust. Möglicher Datenverlust abhängig von der Anzahl der Replikate. Lokales Erasure Coding kann Datenverlust verhindern.

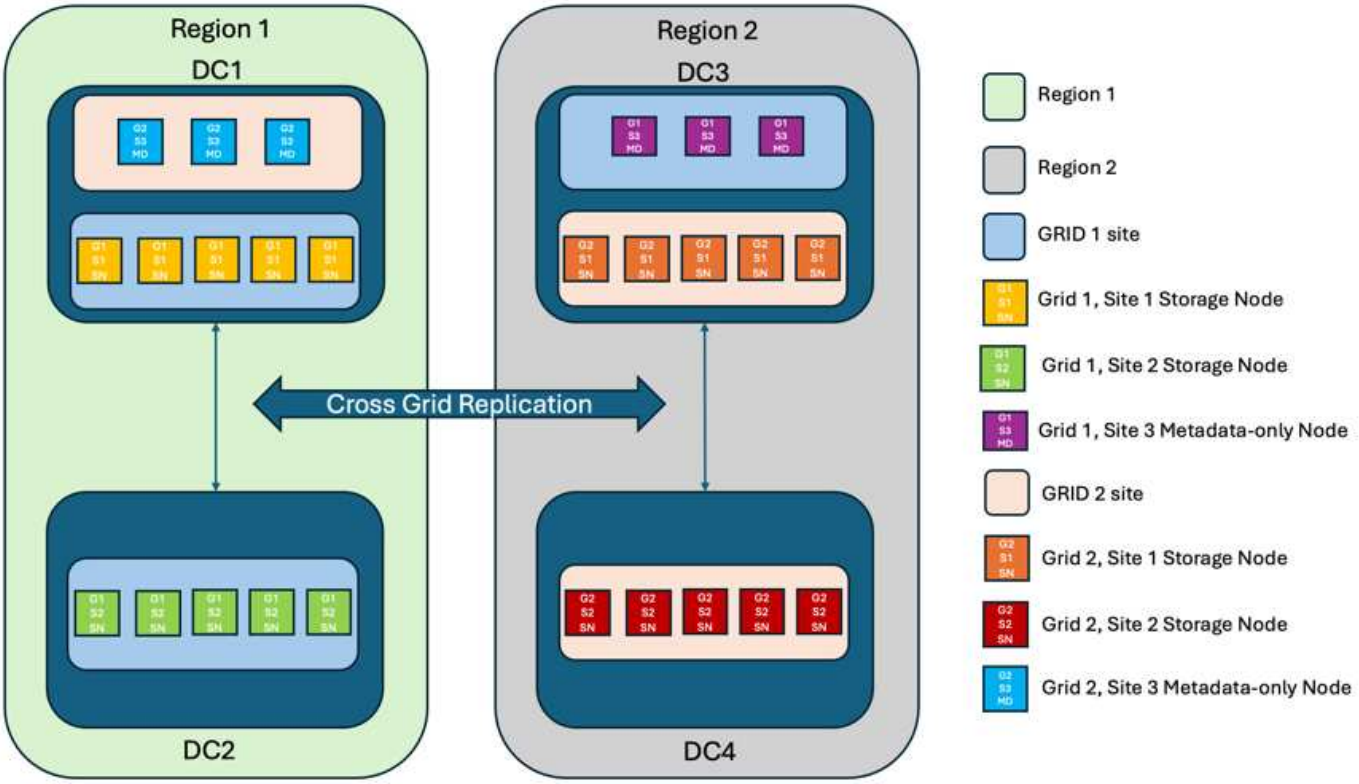
Ausfall	Ergebnis an zwei Standorten + Vermächtnis Starke globale Präsenz	Ergebnis von 3 oder mehr Standorten + Quorum Strong Global
Von jedem verbleibenden Standort aus einen Standort und einen Node	Es existieren nur zwei Standorte. Siehe: Einzelner Standort plus ein einzelner Knoten.	Der Betrieb wird gestört, wenn das Quorum für die Metadatenreplikate nicht erreicht werden kann. Reduzieren Sie die Bucket-Konsistenz auf „Lesen nach neuem Schreiben“ oder niedriger, um den Betrieb in diesem Fehlerzustand ununterbrochen fortzusetzen. Möglicher Datenverlust bei dauerhaftem Ausfall, abhängig von der Anzahl der Replikatkopien. Lokales Erasure Coding kann Datenverlust verhindern.
Ausfall mehrerer Standorte	Es gibt keine betriebsbereiten Standorte mehr. Daten gehen verloren, wenn auch nur ein Standort nicht vollständig wiederhergestellt werden kann.	Der Betrieb wird gestört, wenn das Quorum für die Metadatenreplikate nicht erreicht werden kann. Reduzieren Sie die Bucket-Konsistenz auf „Lesen nach neuem Schreiben“ oder niedriger, um den Betrieb in diesem Fehlerzustand ununterbrochen fortzusetzen. Bei einem permanenten Ausfall ist ein Datenverlust möglich, wenn nicht genügend löschcodierte Datenblöcke übrig bleiben. Lokales Erasure-Coding oder das Erstellen von Replikaten können Datenverlust verhindern.
Netzwerkisolierung eines Standorts	Der Betrieb der Kunden wird unterbrochen, bis der Fehler behoben ist. Reduzieren Sie die Bucket-Konsistenz auf „Lesen nach neuem Schreiben“ oder niedriger, um den Betrieb in diesem Fehlerzustand ununterbrochen fortzusetzen. Kein Datenverlust	Der Betrieb des isolierten Standorts wird beeinträchtigt sein, es wird jedoch keinen Datenverlust geben. Reduzieren Sie die Bucket-Konsistenz auf „Lesen nach neuem Schreiben“ oder niedriger, um den Betrieb in diesem Fehlerzustand ununterbrochen fortzusetzen. Keine Betriebsunterbrechungen an den übrigen Standorten und kein Datenverlust.

Eine Multi-Grid-Implementierung an mehreren Standorten

Um eine zusätzliche Redundanzebene hinzuzufügen, werden in diesem Szenario zwei StorageGRID Cluster eingesetzt und mithilfe der Cross-Grid-Replikation synchron gehalten. Für diese Lösung verfügt jeder StorageGRID Cluster über drei Standorte. Zwei Standorte werden für die Objektspeicherung und Metadaten verwendet, während der dritte Standort ausschließlich für Metadaten genutzt wird. Beide Systeme werden mit einer ausgewogenen ILM-Regel konfiguriert, um die Objekte mithilfe von Erasure Coding an jedem der beiden Datenstandorte synchron zu speichern. Buckets werden mit dem Quorum Strong Global-Konsistenzmodell konfiguriert. Jedes Grid wird mit einer bidirektionalen Cross-Grid-Replikation auf jedem Bucket konfiguriert.

Dies ermöglicht die asynchrone Replikation zwischen den Regionen. Optional kann ein globaler Load Balancer implementiert werden, um Anfragen an die integrierten Load Balancer-Hochverfügbarkeitsgruppen beider StorageGRID -Systeme zu verwalten und so ein RPO von Null zu erreichen.

Die Lösung nutzt vier Standorte, die gleichmäßig in zwei Regionen aufgeteilt sind. Region 1 enthält die 2 Storage-Standorte von Grid 1 als primäres Grid der Region und den Metadaten-Standort von Grid 2. Region 2 enthält die 2 Storage-Standorte von Grid 2 als primäres Grid der Region und den Metadaten-Standort von Grid 1. In jeder Region kann der gleiche Standort den Speicherort des primären Grids der Region sowie den nur-Metadaten-Standort des anderen Regionengitters beherbergen. Wenn Nodes als dritter Standort nur Metadaten verwendet werden, sorgen sie für die erforderliche Konsistenz für die Metadaten und nicht für das Duplizieren des Storage von Objekten an diesem Standort.



Diese Lösung mit vier separaten Standorten bietet vollständige Redundanz von zwei separaten StorageGRID-Systemen mit einem RPO von 0 und nutzt sowohl synchrone Replizierung an mehreren Standorten als auch asynchrone Replizierung in mehreren Grids. Bei jedem einzelnen Standort kann der Client-Betrieb auf beiden StorageGRID Systemen unterbrechungsfrei ausgeführt werden.

In dieser Lösung gibt es vier Kopien, die nach Erasure Coding codiert wurden, und 18 Replikate aller Metadaten. Dies ermöglicht mehrere Ausfallszenarien ohne Auswirkungen auf den Client-Betrieb. Bei einem Ausfall werden die Updates nach dem Ausfall automatisch mit dem ausgefallenen Standort bzw. den ausgefallenen Nodes synchronisiert.

Ausfallszenarien für mehrere Standorte und Grids

Ausfall	Ergebnis
Ausfall eines Laufwerks mit einem Node	Jede Appliance nutzt mehrere Festplattengruppen und kann den Ausfall von mindestens einem Laufwerk pro Gruppe ohne Unterbrechung oder Datenverlust überstehen.

Ausfall	Ergebnis
Ausfall eines einzelnen Nodes an einem Standort in einem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines einzelnen Nodes an einem Standort in jedem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall mehrerer Nodes an einem Standort in einem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall mehrerer Nodes an einem Standort in jedem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines einzelnen Nodes an mehreren Standorten in einem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines einzelnen Nodes an mehreren Standorten in jedem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines einzelnen Standorts in einem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines Standorts in jedem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines einzelnen Standorts und eines einzelnen Node in einem Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ein Standort und ein Node von jedem verbleibenden Standort in einem einzelnen Grid	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines einzelnen Standorts	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines Standorts in jedem Grid DC1 und DC3	Der Betrieb wird unterbrochen, bis entweder der Fehler behoben oder die Bucket-Konsistenz verringert wird; jedes Grid hat 2 Standorte verloren Alle Daten sind noch an 2 Standorten vorhanden
Ausfall eines Standorts in jedem Grid DC1 und DC4 oder DC2 und DC3	Keine Unterbrechung von Prozessen oder Datenverlust:
Ausfall eines Standorts in jedem Grid DC2 und DC4	Keine Unterbrechung von Prozessen oder Datenverlust:
Netzwerkisolierung eines Standorts	Der Betrieb des isolierten Standorts wird unterbrochen, aber es gehen keine Daten verloren Es gibt keine Unterbrechung des Betriebs an den verbleibenden Standorten oder Datenverluste.

Schlussfolgerung

Das Erreichen eines Recovery Point Objective (RPO) von null mit StorageGRID ist ein wichtiges Ziel, um die

Datenaufbewahrung und Verfügbarkeit bei Standortausfällen sicherzustellen. Durch den Einsatz der robusten Replikationsstrategien von StorageGRID, einschließlich synchroner Replizierung an mehreren Standorten und asynchroner Multi-Grid-Replizierung, können Unternehmen den unterbrechungsfreien Client-Betrieb gewährleisten und über mehrere Standorte hinweg für Datenkonsistenz sorgen. Die Implementierung von ILM-Richtlinien (Information Lifecycle Management) und die Verwendung von Nodes, die nur Metadaten enthalten, erhöhen die Ausfallsicherheit und Performance des Systems noch weiter. Mit StorageGRID können Unternehmen ihre Daten zuversichtlich managen, da sie wissen, dass sie auch bei komplexen Ausfallszenarien zugänglich und konsistent bleiben. Dieser umfassende Ansatz für Datenmanagement und -Replikation unterstreicht die Bedeutung einer sorgfältigen Planung und Ausführung bei der Erreichung eines Null-RPO-Ziels und der Sicherung wertvoller Informationen.

Cloud Storage Pool für AWS oder Google Cloud erstellen

Sie können einen Cloud Storage Pool verwenden, wenn Sie StorageGRID-Objekte in einen externen S3-Bucket verschieben möchten. Der externe Bucket kann zu Amazon S3 (AWS) oder Google Cloud gehören.

Was Sie benötigen

- StorageGRID 11.6 wurde konfiguriert.
- Sie haben bereits einen externen S3-Bucket auf AWS oder Google Cloud eingerichtet.

Schritte

1. Navigieren Sie im Grid Manager zu **ILM** > **Storage Pools**.
2. Wählen Sie im Abschnitt Cloud-Speicherpools der Seite **Erstellen** aus.

   Das Popup-Fenster „Cloud-Speicherpool erstellen“ wird angezeigt.

3. Geben Sie einen Anzeigenamen ein.
4. Wählen Sie in der Dropdown-Liste Provider Type * Amazon S3* aus.

   Dieser Provider-Typ funktioniert für AWS S3 oder Google Cloud.

5. Geben Sie den URI für den S3-Bucket ein, der für den Cloud-Storage-Pool verwendet werden soll.

   Es sind zwei Formate zulässig:

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Geben Sie den S3-Bucket-Namen ein.

   Der angegebene Name muss exakt mit dem Namen des S3-Buckets übereinstimmen. Andernfalls schlägt die Erstellung von Cloud-Storage-Pool fehl. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

7. Geben Sie optional die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel ein.
8. Wählen Sie in der Dropdown-Liste * Zertifikat nicht überprüfen* aus.
9. Klicken Sie Auf **Speichern**.

Erwartetes Ergebnis

Es muss sichergestellt werden, dass ein Cloud-Storage-Pool für Amazon S3 oder Google Cloud erstellt wurde.

Von Jonathan Wong

Cloud Storage Pool für Azure Blob Storage erstellen

Sie können einen Cloud Storage Pool verwenden, wenn Sie StorageGRID-Objekte in einen externen Azure Container verschieben möchten.

Was Sie benötigen

- StorageGRID 11.6 wurde konfiguriert.
- Sie haben bereits einen externen Azure-Container eingerichtet.

Schritte

1. Navigieren Sie im Grid Manager zu **ILM** > **Storage Pools**.
2. Wählen Sie im Abschnitt Cloud-Speicherpools der Seite **Erstellen** aus.

   Das Popup-Fenster „Cloud-Speicherpool erstellen“ wird angezeigt.

3. Geben Sie einen Anzeigenamen ein.
4. Wählen Sie in der Dropdown-Liste Provider Type * Azure Blob Storage* aus.
5. Geben Sie den URI für den S3-Bucket ein, der für den Cloud-Storage-Pool verwendet werden soll.

   Es sind zwei Formate zulässig:

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Geben Sie den Azure-Containernamen ein.

   Der angegebene Name muss exakt mit dem Azure-Containernamen übereinstimmen. Andernfalls schlägt die Erstellung des Cloud-Storage-Pools fehl. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

7. Geben Sie optional den zugeordneten Kontonamen und den Kontokschlüssel des Azure-Containers für die Authentifizierung ein.
8. Wählen Sie in der Dropdown-Liste * Zertifikat nicht überprüfen* aus.
9. Klicken Sie Auf **Speichern**.

Erwartetes Ergebnis

Erstellen eines Cloud-Storage-Pools für Azure Blob Storage bestätigen

Von Jonathan Wong

Verwenden Sie einen Cloud Storage Pool für Backups

Sie können eine ILM-Regel erstellen, um Objekte für Backups in einen Cloud Storage-Pool zu verschieben.

Was Sie benötigen

- StorageGRID 11.6 wurde konfiguriert.
- Sie haben bereits einen externen Azure-Container eingerichtet.

Schritte

1. Navigieren Sie im Grid Manager zu **ILM** > **Regeln** > **Erstellen**.
2. Geben Sie eine Beschreibung ein.
3. Geben Sie ein Kriterium ein, um die Regel auszulösen.
4. Klicken Sie Auf **Weiter**.
5. Replizieren Sie das Objekt auf Storage Nodes.
6. Fügen Sie eine Platzierungsregel hinzu.
7. Replizieren des Objekts in den Cloud Storage Pool
8. Klicken Sie Auf **Weiter**.
9. Klicken Sie Auf **Speichern**.

Erwartetes Ergebnis

Vergewissern Sie sich, dass im Aufbewahrungsdiagramm die lokal in StorageGRID gespeicherten Objekte und in einem Cloud-Speicherpool für Backups angezeigt werden.

Vergewissern Sie sich, dass bei Auslösung der ILM-Regel im Cloud Storage Pool eine Kopie vorhanden ist und Sie das Objekt lokal abrufen können, ohne ein Objekt wiederherstellen zu müssen.

Von Jonathan Wong

Konfigurieren Sie den Integrationsservice für die StorageGRID Suche

Dieser Leitfaden enthält detaillierte Anweisungen zum Konfigurieren des NetApp StorageGRID Suchintegrationsservices mit Amazon OpenSearch Service oder On-Premises Elasticsearch.

Einführung

StorageGRID unterstützt drei Arten von Plattform-Services.

- **StorageGRID CloudMirror Replikation**. Spiegeln bestimmter Objekte aus einem StorageGRID-Bucket auf ein angegebenes externes Ziel
- **Benachrichtigungen**. Bucket-spezifische Ereignisbenachrichtigungen senden Benachrichtigungen über bestimmte Aktionen, die an Objekten durchgeführt werden, an einen bestimmten externen Amazon Simple Notification Service (Amazon SNS).
- **Integrationsservice suchen**. Senden von einfachen Storage Service (S3) Objektmetadaten in einen angegebenen Elasticsearch-Index, wo Sie die Metadaten mithilfe des externen Service durchsuchen oder analysieren können.

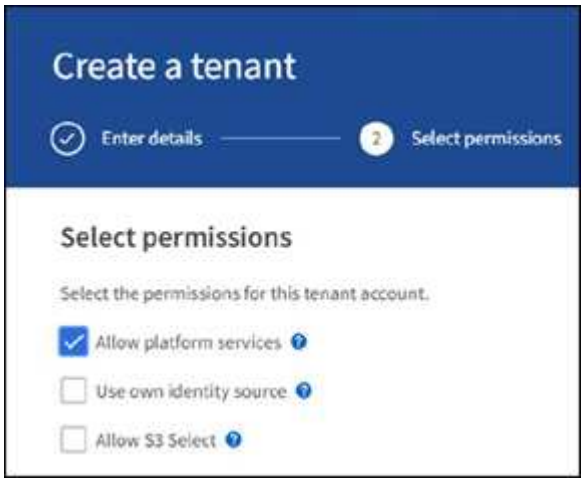
Plattform-Services werden vom S3-Mandanten über die Mandanten-Manager-UI konfiguriert. Weitere Informationen finden Sie unter "Überlegungen bei der Verwendung von Plattform-Services".

Dieses Dokument dient als Ergänzung zum "StorageGRID 11.6 Mandantenleitfaden" Und enthält Schritt-für-Schritt-Anleitungen und Beispiele für die Endpunkt- und Bucket-Konfiguration für Suchintegrations-Services. Die hier enthaltene Anleitung zur Einrichtung von Amazon Web Services (AWS) oder lokalen Elasticsearch-Services dienen nur zu Test- oder Demonstrationszwecken.

Zielgruppen sollten mit Grid Manager, Mandanten-Manager vertraut sein und über den S3-Browser Zugang verfügen, um grundlegende Vorgänge zum Hochladen (PUT) und Herunterladen (GET) für StorageGRID-Suchintegrationstests durchzuführen.

Erstellung von Mandanten und Aktivierung von Plattform-Services

1. Erstellen Sie einen S3-Mandanten mithilfe von Grid Manager, geben Sie einen Anzeigenamen ein und wählen Sie das S3-Protokoll aus.
2. Wählen Sie auf der Berechtigungsseite die Option Plattformdienste zulassen. Wählen Sie ggf. andere Berechtigungen aus.



3. Richten Sie das ursprüngliche Kennwort des Mandanten-Root-Benutzers ein, oder wählen Sie, falls im Raster der Identifikationsverbund aktiviert ist, welche föderierte Gruppe Root-Zugriffsberechtigungen hat, um das Mandantenkonto zu konfigurieren.
4. Klicken Sie auf als Stamm anmelden und wählen Sie Bucket: Erstellen und verwalten.

   Dies führt Sie zur Seite Tenant Manager.

5. Wählen Sie im Tenant Manager My Access Keys aus, um den S3-Zugriffsschlüssel für spätere Tests zu erstellen und herunterzuladen.

Integrationsservices mit Amazon OpenSearch suchen

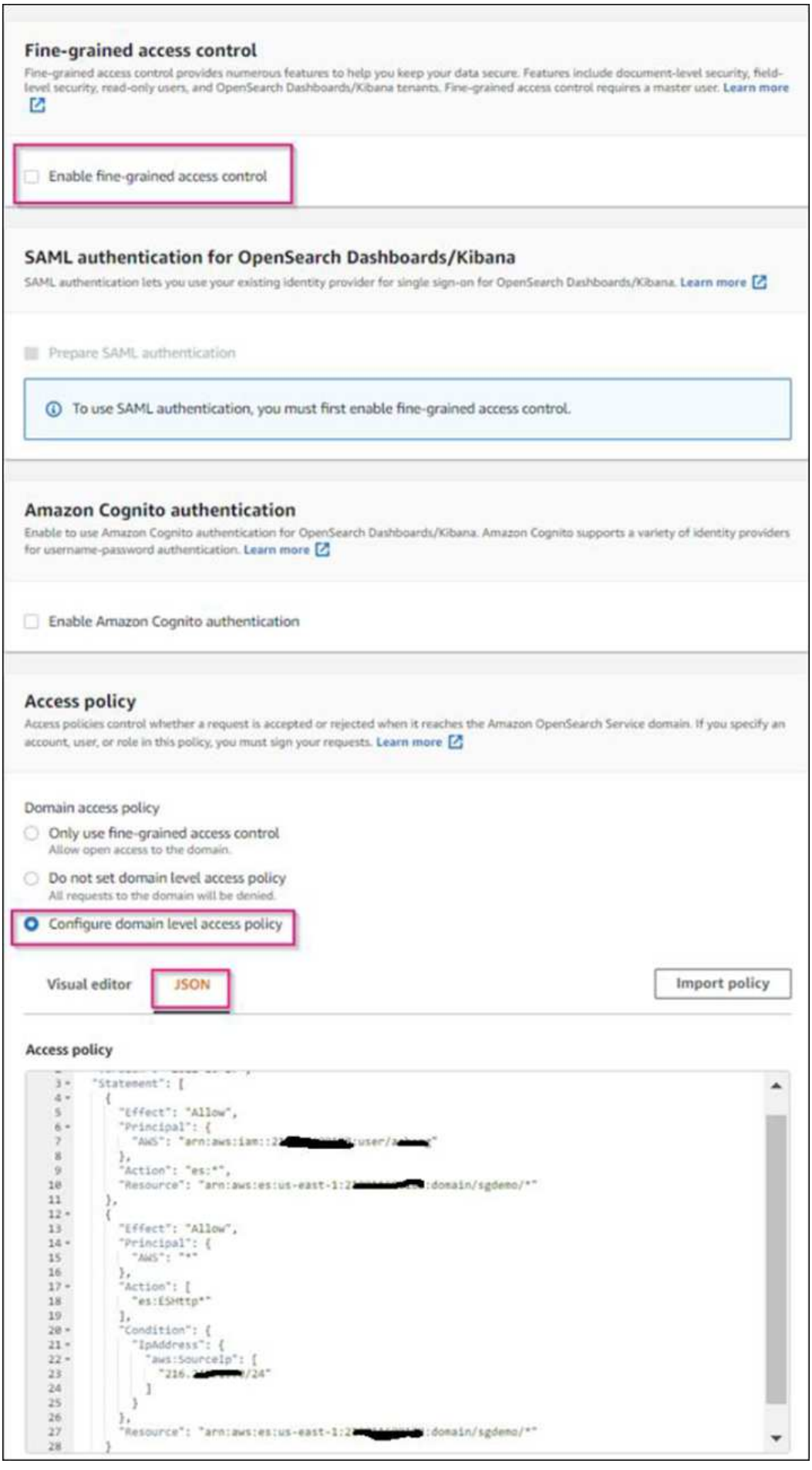
Einrichtung des Amazon OpenSearch Service (ehemals Elasticsearch)

Verwenden Sie dieses Verfahren für eine schnelle und einfache Einrichtung des OpenSearch-Dienstes nur zu Test-/Demo-Zwecken. Wenn Sie On-Premises-Elasticsearch für Suchintegrationsservices verwenden, lesen Sie den Abschnitt Suchintegrations-Services für On-Premises-Elasticsearch.

> Sie müssen über eine gültige Anmeldung für die AWS-Konsole, einen Zugriffsschlüssel, einen geheimen Zugriffsschlüssel und die Berechtigung zum Abonnieren des OpenSearch-Dienstes verfügen.

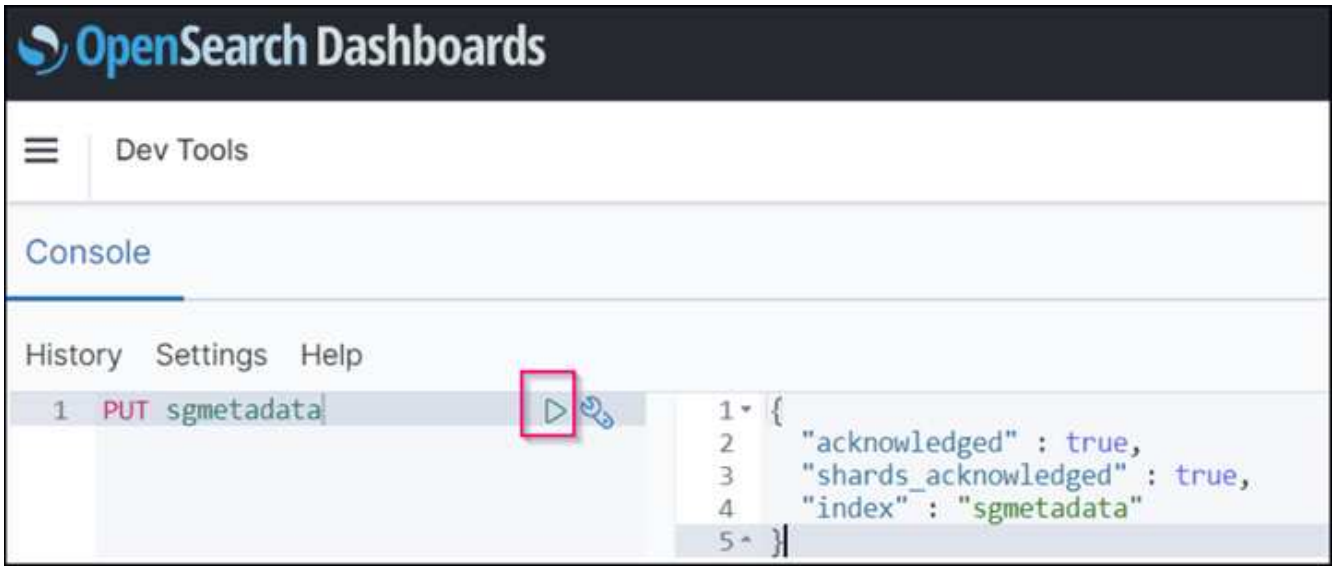
1. Erstellen Sie mithilfe der Anweisungen von eine neue Domäne "AWS OpenSearch Service – erste Schritte", Mit Ausnahme der folgenden:
   - Schritt 4: Domain-Name: Sgdemo
   - Schritt 10: Feinkörnige Zugriffssteuerung: Deaktivieren Sie die Option Enable Fine-genarainable Access Control.
   - Schritt 12: Zugriffsrichtlinie: Wählen Sie Zugriffsrichtlinie auf Zugriffsebene konfigurieren, wählen Sie die Registerkarte JSON aus, um die Zugriffsrichtlinie anhand des folgenden Beispiels zu ändern:
     - Ersetzen Sie den hervorgehobenen Text durch Ihre eigene AWS IAM-ID (Identity and Access Management) und Ihren Benutzernamen.
     - Ersetzen Sie den markierten Text (die IP-Adresse) durch die öffentliche IP-Adresse Ihres lokalen Computers, über den Sie auf die AWS-Konsole zugreifen.
     - Öffnen Sie eine Browserregisterkarte für "https://checkip.amazonaws.com" Um Ihre öffentliche IP zu finden.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal":
        {"AWS": "arn:aws:iam:: nnnnnn:user/xyzabc"},
        "Action": "es:*",
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        },
        {
        "Effect": "Allow",
        "Principal": {"AWS": "*"},
        "Action": [
        "es:ESHttp*"
                ],
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": [ "nnn.nnn.nn.n/nn"
                    ]
                }
        },
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        }
    ]
}
```

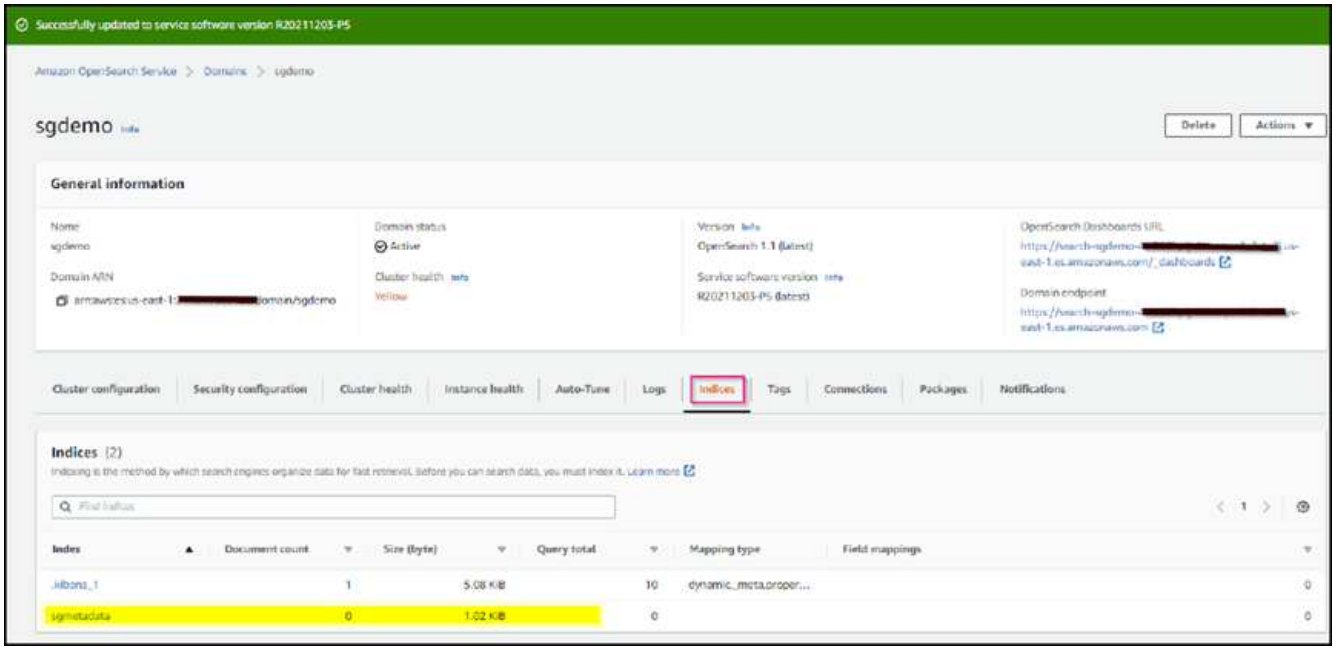

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
Enable fine-grained access control
SAML authentication for OpenSearch Dashboards/Kibana
SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. Learn more
Prepare SAML authentication
To use SAML authentication, you must first enable fine-grained access control.
Amazon Cognito authentication
Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more
Enable Amazon Cognito authentication
Access policy
Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. Learn more
Domain access policy
Only use fine-grained access control
Allow open access to the domain.
Do not set domain level access policy
All requests to the domain will be denied.
Configure domain level access policy
Visual editor
JSON
Import policy
Access policy
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::2[redacted]:user/A[redacted]"
},
"Action": "es:*",
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
},
{
"Effect": "Allow",
"Principal": {
"AWS": "*"
},
"Action": [
"es:ESHttp*"
],
"Condition": {
"IpAddress": {
"aws:SourceIp": [
"216.[redacted]/24"
]
}
},
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
}

2. Warten Sie 15 bis 20 Minuten, bis die Domain aktiv ist.

3. Klicken Sie auf OpenSearch Dashboards URL, um die Domäne in einer neuen Registerkarte zu öffnen, um auf das Dashboard zuzugreifen. Wenn ein Fehler beim Zugriff verweigert wird, überprüfen Sie, ob die Quell-IP-Adresse der Zugriffsrichtlinie korrekt auf Ihre öffentliche IP-Adresse des Computers eingestellt ist, um den Zugriff auf das Domain-Dashboard zu ermöglichen.
4. Wählen Sie auf der Willkommensseite des Dashboards „Explore“ auf eigene Faust aus. Wählen Sie im Menü „Management → Entwicklungstools“
5. Geben Sie unter Dev Tools → Console ein `PUT <index>` Wo Sie den Index zum Speichern von StorageGRID-Objektmetadaten verwenden. Im folgenden Beispiel verwenden wir den Indexnamen 'sgmetadaten'. Klicken Sie auf das kleine Dreieck-Symbol, um den PUT-Befehl auszuführen. Das erwartete Ergebnis wird im rechten Bereich angezeigt, wie im folgenden Beispiel Screenshot dargestellt.



6. Überprüfen Sie, ob der Index über die Benutzeroberfläche von Amazon OpenSearch unter sgdomain > Indizes sichtbar ist.

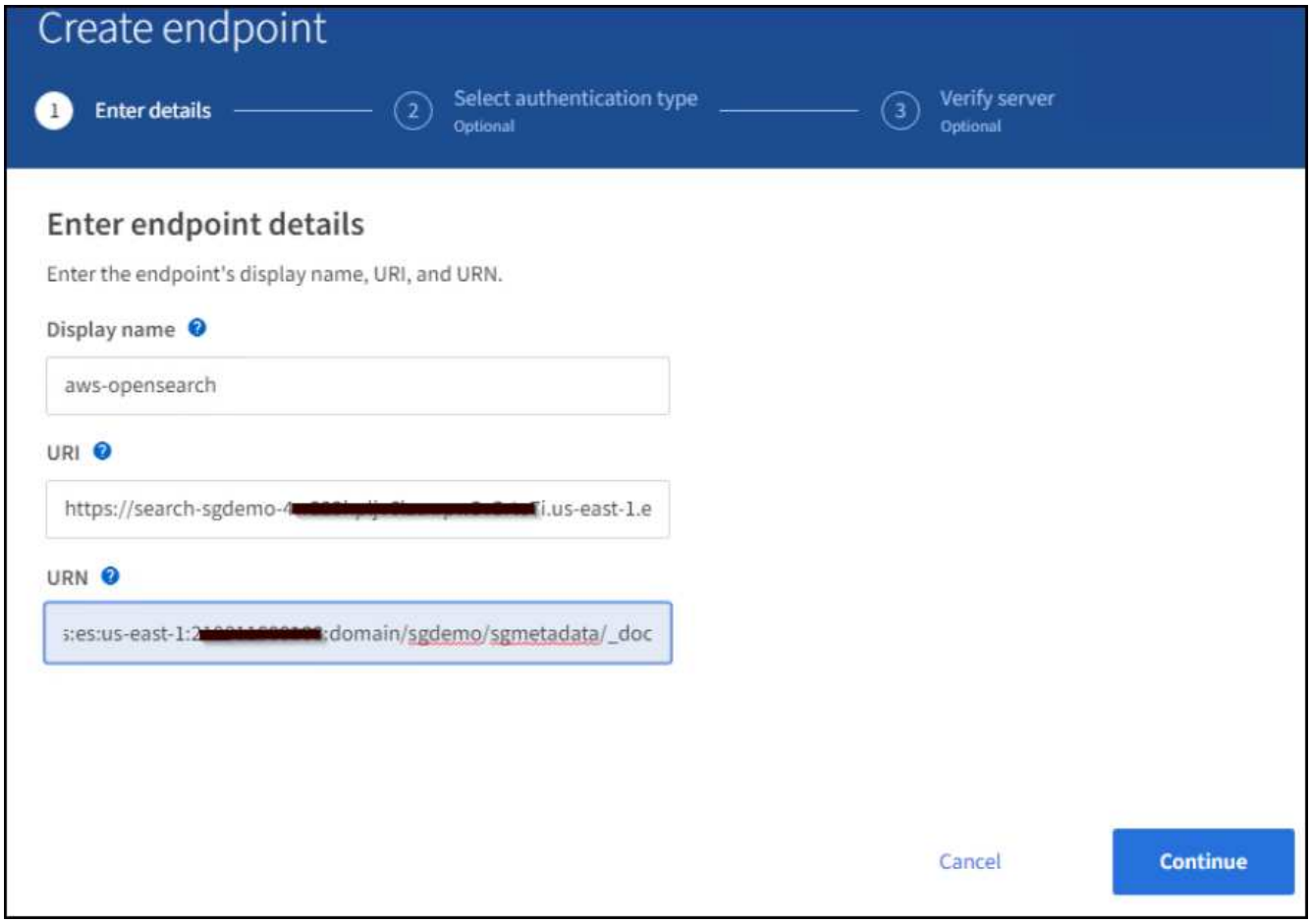


Endpoint-Konfiguration für Plattform-Services

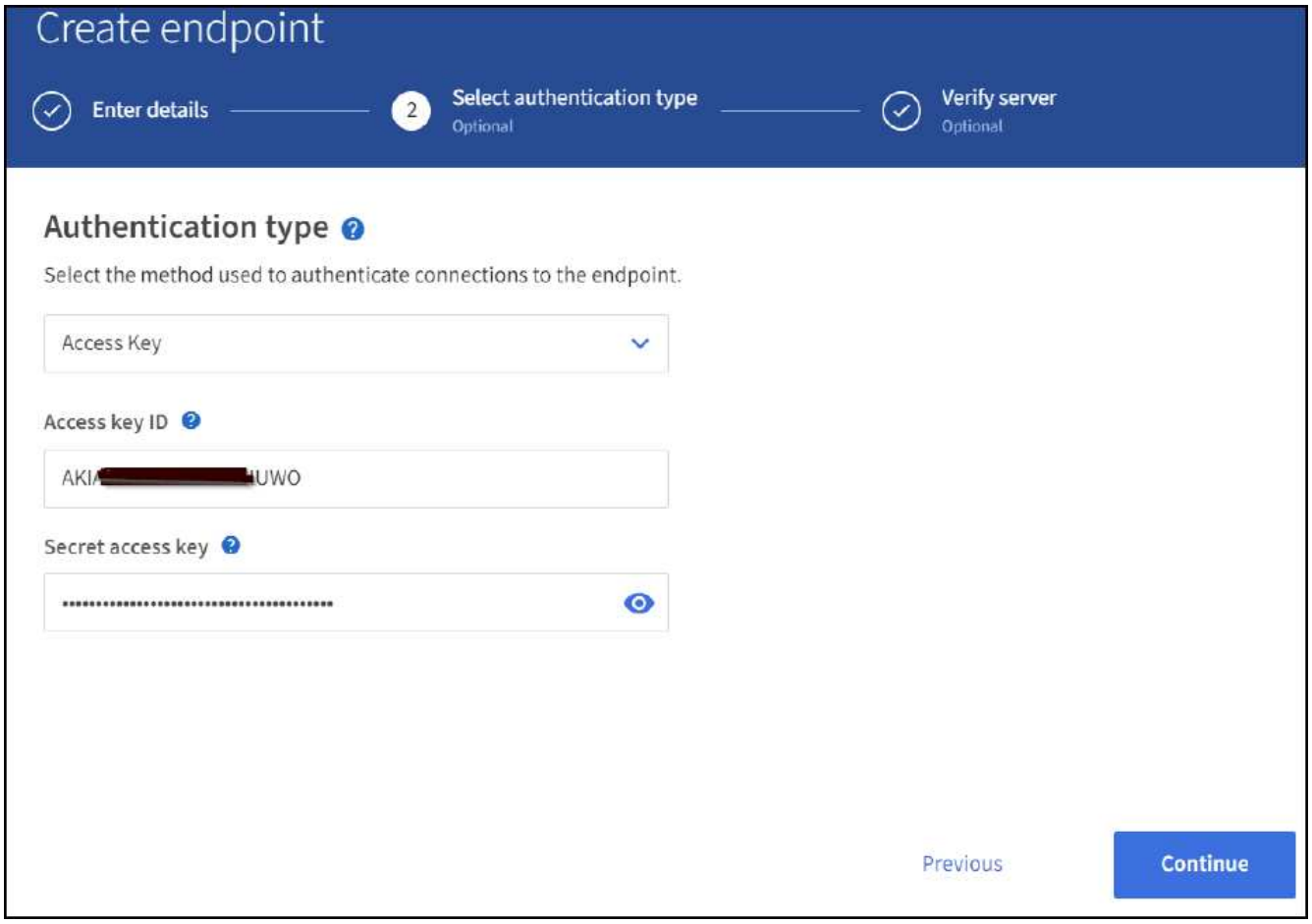
Gehen Sie wie folgt vor, um die Endpunkte der Plattformservices zu konfigurieren:

1. In Tenant Manager wechseln Sie zu STORAGE(S3) > Plattform-Services-Endpunkten.
2. Klicken Sie auf Endpunkt erstellen, geben Sie Folgendes ein und klicken Sie dann auf Weiter:
   - Beispiel für einen Anzeigenamen `aws-opensearch`
   - Der Domänenendpunkt im Beispiel-Screenshot unter Schritt 2 des vorhergehenden Verfahrens im URI-Feld.
   - Die Domäne ARN, die in Schritt 2 des vorhergehenden Verfahrens im Feld URN verwendet wurde und addieren `/<index>/_doc` Bis zum Ende von ARN.

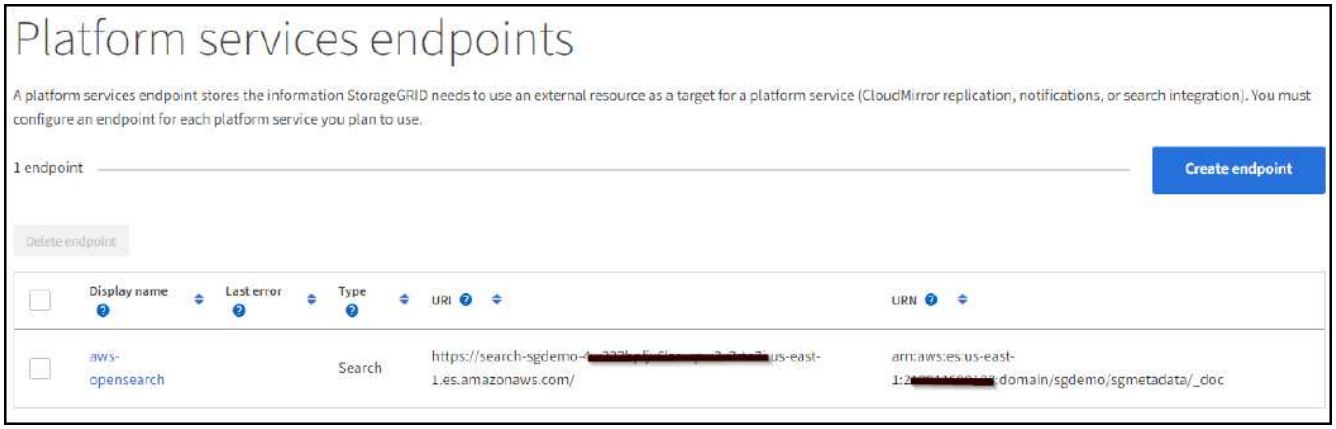
     In diesem Beispiel wird URN `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.



3. Um auf die Amazon OpenSearch sgdomain zuzugreifen, wählen Sie als Authentifizierungstyp den Zugriffsschlüssel aus, und geben Sie dann den Amazon S3-Zugriffsschlüssel und den geheimen Schlüssel ein. Um zur nächsten Seite zu gelangen, klicken Sie auf Weiter.



4. Um den Endpunkt zu überprüfen, wählen Sie Operating System CA Certificate und Test and Create Endpoint aus. Wenn die Überprüfung erfolgreich ist, wird ein Endpunkt-Bildschirm angezeigt, der der folgenden Abbildung entspricht. Wenn die Überprüfung fehlschlägt, überprüfen Sie, ob der URN umfasst `/<index>/_doc` Am Ende des Pfads und der AWS Zugriffsschlüssel und der Geheimschlüssel sind korrekt.



Suchintegrations-Services für On-Premises-Elasticsearch

Elasticsearch-Einrichtung vor Ort

Dieses Verfahren dient der schnellen Einrichtung von vor-Ort-Elasticsearch und Kibana mit Docker nur zu Testzwecken. Wenn Elasticsearch und Kibana-Server bereits vorhanden sind, fahren Sie mit Schritt 5 fort.

1. Folgen Sie diesen Anweisungen "Docker-Installationsvorgang" So installieren Sie den Docker. Wir verwenden den "CentOS Docker Installationsverfahren" In diesem Setup.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io
sudo systemctl start docker
```

   - Um den Docker nach dem Neustart zu starten, geben Sie Folgendes ein:

```
sudo systemctl enable docker
```

   - Stellen Sie die ein `vm.max_map_count` Wert für 262144:

```
sysctl -w vm.max_map_count=262144
```

   - Um die Einstellung nach dem Neustart zu behalten, geben Sie Folgendes ein:

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

2. Folgen Sie den "Elasticsearch Quick Start Guide" Selbstverwalteter Abschnitt zum Installieren und Ausführen der Elasticsearch- und Kibana-Docker. In diesem Beispiel wurde die Version 8.1 installiert.

Beachten Sie den Benutzernamen/das Kennwort und das Token, das Elasticsearch erstellt hat. Sie müssen diese zum Starten der Kibana UI und der StorageGRID-Plattform-Endpunktauthentifizierung verwenden.

Elasticsearch Service | Self-managed

Install and run Elasticsearch

1. Install and start Docker Desktop.
2. Run:

```
docker network create elastic
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.0
docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -it
```

When you start Elasticsearch for the first time, the following security configuration occurs automatically:

- Certificates and keys are generated for the transport and HTTP layers.
- The Transport Layer Security (TLS) configuration settings are written to `elasticsearch.yml`.
- A password is generated for the `elastic` user.
- An enrollment token is generated for Kibana.

NOTE You might need to scroll back a bit in the terminal to view the password and enrollment token.

3. Copy the generated password and enrollment token and save them in a secure location. These values are shown only when you start Elasticsearch for the first time. You'll use these to enroll Kibana with your Elasticsearch cluster and log in.

NOTE If you need to reset the password for the `elastic` user or other built-in users, run the `elasticsearch-reset-password` tool. To generate new enrollment tokens for Kibana or Elasticsearch nodes, run the `elasticsearch-create-enrollment-token` tool. These tools are available in the Elasticsearch `bin` directory.

Install and run Kibana

To analyze, visualize, and manage Elasticsearch data using an intuitive UI, install Kibana.

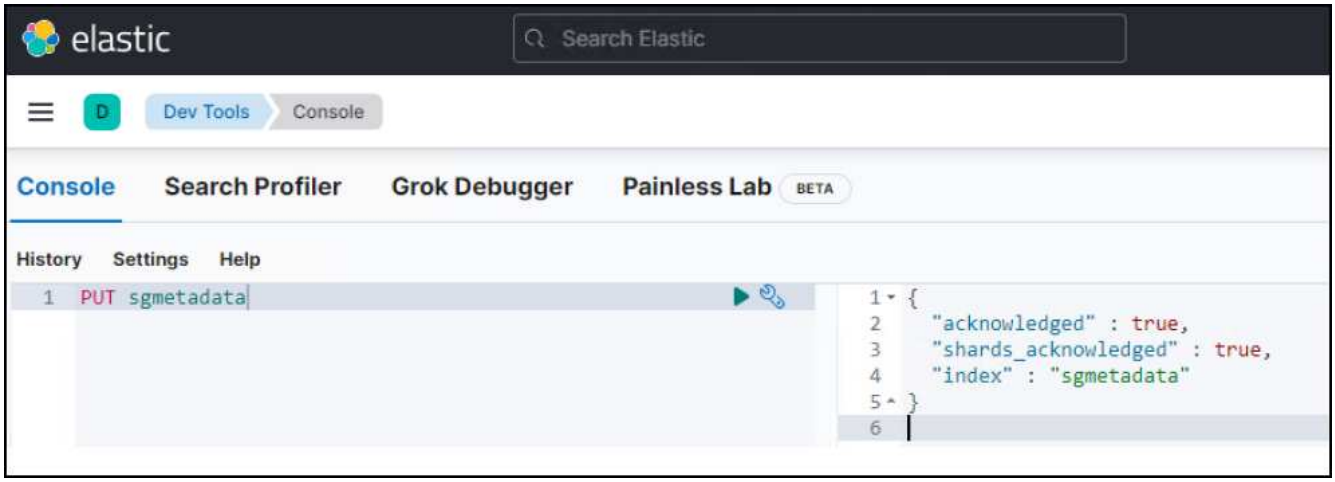
1. In a new terminal session, run:

```
docker pull docker.elastic.co/kibana/kibana:8.1.0
docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/ki
```

When you start Kibana, a unique link is output to your terminal.

2. To access Kibana, click the generated link in your terminal.
   a. In your browser, paste the enrollment token that you copied and click the button to connect your Kibana instance with Elasticsearch.
   b. Log in to Kibana as the `elastic` user with the password that was generated when you started Elasticsearch.

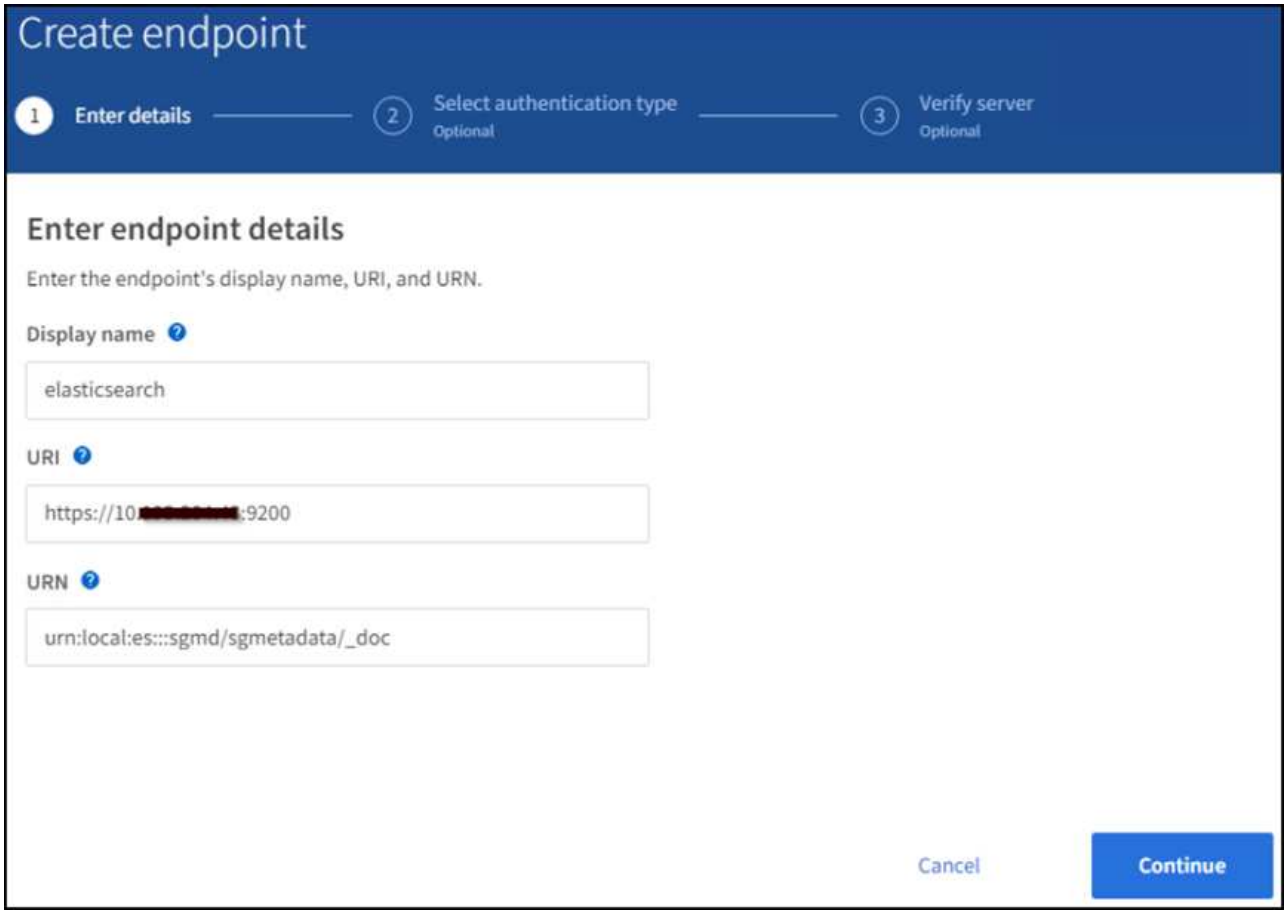
3. Nachdem der Kibana-Docker-Container gestartet wurde, wird der URL-Link aufgerufen `https://0.0.0.0:5601` Wird in der Konsole angezeigt. Ersetzen Sie 0.0.0.0 durch die Server-IP-Adresse in der URL.
4. Melden Sie sich mit dem Benutzernamen bei der Kibana-Benutzeroberfläche an `elastic` Und das Passwort, das im vorherigen Schritt von Elastic generiert wurde.
5. Wenn Sie sich zum ersten Mal anmelden möchten, wählen Sie auf der Begrüßungsseite „Explore“. Wählen Sie im Menü Verwaltung > Entwicklungstools.
6. Geben Sie auf dem Bildschirm Dev Tools Console die Eingabe ein `PUT <index>` Dort, wo Sie diesen Index zum Speichern von StorageGRID-Objektmetadaten verwenden. Wir verwenden den Indexnamen `sgmetadata` In diesem Beispiel. Klicken Sie auf das kleine Dreieck-Symbol, um den PUT-Befehl auszuführen. Das erwartete Ergebnis wird im rechten Bereich angezeigt, wie im folgenden Beispiel Screenshot dargestellt.



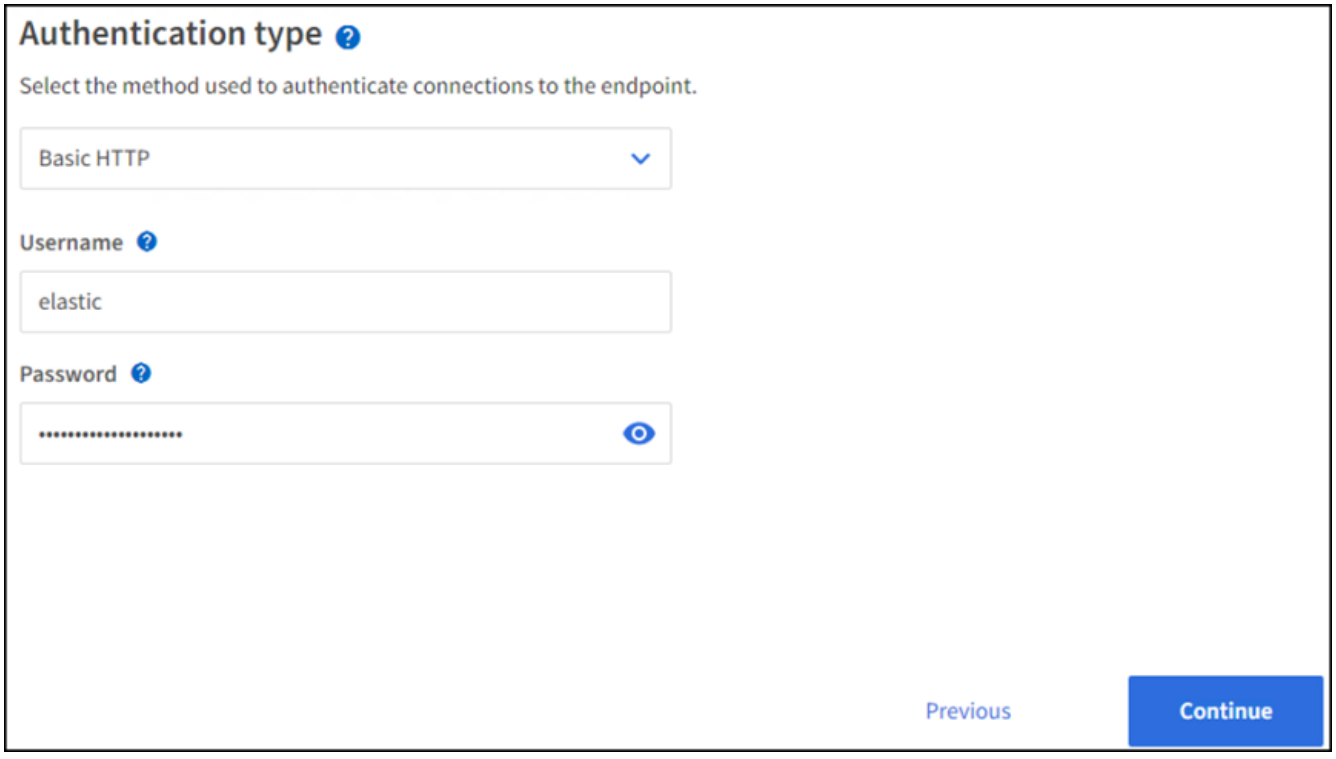
Endpoint-Konfiguration für Plattform-Services

Gehen Sie wie folgt vor, um Endpunkte für Plattformservices zu konfigurieren:

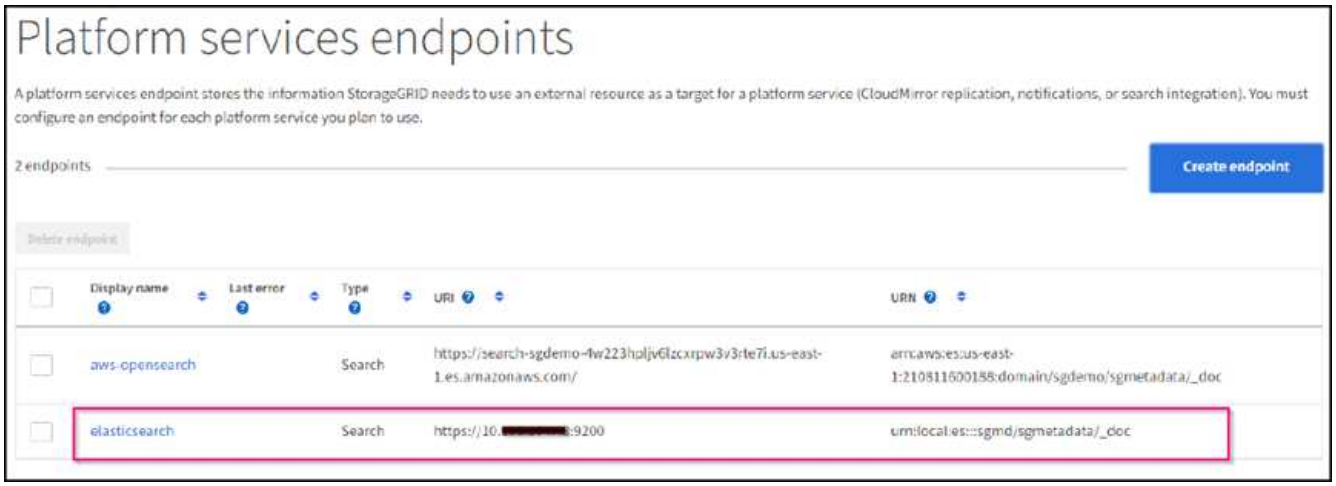
1. In Tenant Manager wechseln Sie zu STORAGE (S3) > Plattform-Services-Endpunkten
2. Klicken Sie auf Endpunkt erstellen, geben Sie Folgendes ein und klicken Sie dann auf Weiter:
   - Beispiel für Anzeigename: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
   - URNE: `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Wobei der Indexname der Name ist, den Sie auf der Kibana-Konsole verwendet haben. Beispiel: `urn:local:es:::sgmd/sgmetadata/_doc`



3. Wählen Sie Basic HTTP als Authentifizierungstyp, geben Sie den Benutzernamen ein `elastic` Und das durch den Elasticsearch-Installationsprozess generierte Passwort. Um zur nächsten Seite zu gelangen, klicken Sie auf Weiter.



4. Wählen Sie Zertifikat nicht überprüfen und Endpunkt erstellen und testen, um den Endpunkt zu überprüfen. Wenn die Überprüfung erfolgreich ist, wird ein Endpunkt-Bildschirm angezeigt, der dem folgenden Screenshot ähnelt. Wenn die Überprüfung fehlschlägt, überprüfen Sie, ob die Einträge für URN, URI und Benutzername/Passwort korrekt sind.



Konfiguration des integrierten Service für die Bucket-Suche

Nachdem der Plattform-Service-Endpunkt erstellt wurde, besteht der nächste Schritt darin, diesen Service auf Bucket-Ebene zu konfigurieren, um Objektmetadaten an den definierten Endpunkt zu senden, sobald ein Objekt erstellt, gelöscht oder seine Metadaten oder Tags aktualisiert werden.

Sie können die Suchintegration mit Tenant Manager konfigurieren, um eine benutzerdefinierte StorageGRID-Konfigurations-XML auf einen Bucket anzuwenden wie folgt:

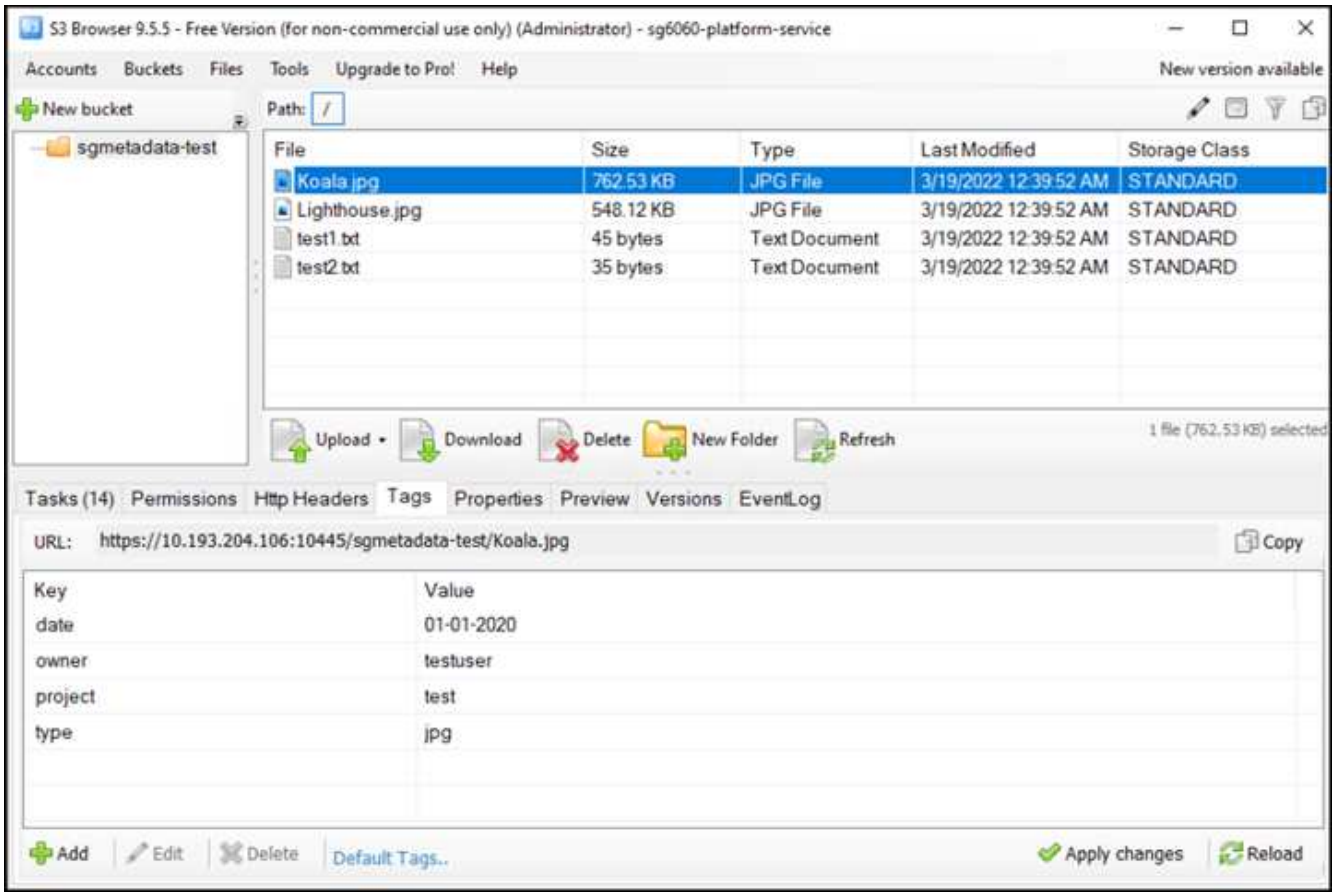
1. Wählen Sie in Tenant Manager „STORAGE(S3)“ > „Buckets“
2. Klicken Sie auf Create Bucket. Geben Sie den Bucket-Namen ein (z. B. `sgmetadata-test`) Und akzeptieren Sie die Standardeinstellung `us-east-1` Werden.
3. Klicken Sie Auf Weiter > Bucket Erstellen.
4. Um die Seite „Bucket-Übersicht“ aufzurufen, klicken Sie auf den Bucket-Namen und wählen Sie „Platform Services“ aus.
5. Wählen Sie das Dialogfeld Integration der Suche aktivieren aus. Geben Sie im angegebenen XML-Feld die Konfigurations-XML-XML-Datei unter Verwendung dieser Syntax ein.

   Der hervorgehobene URN muss mit dem von Ihnen definierten Endpunkt für Plattformservices übereinstimmen. Sie können eine weitere Browserregisterkarte öffnen, um auf den Mandantenmanager zuzugreifen und URN vom definierten Endpunkt der Plattformdienste zu kopieren.

   In diesem Beispiel haben wir kein Präfix verwendet, was bedeutet, dass die Metadaten für jedes Objekt in diesem Bucket an den zuvor definierten Elasticsearch-Endpunkt gesendet werden.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Urn> urn:local:es:::sgmd/sgmetadata/_doc</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

6. Verwenden Sie S3-Browser, um eine Verbindung zu StorageGRID mit dem Mandantenzugriff/geheimen Schlüssel herzustellen und Testobjekte in hochzuladen `sgmetadata-test` Bucket und fügen Sie Tags oder benutzerdefinierte Metadaten zu Objekten hinzu.



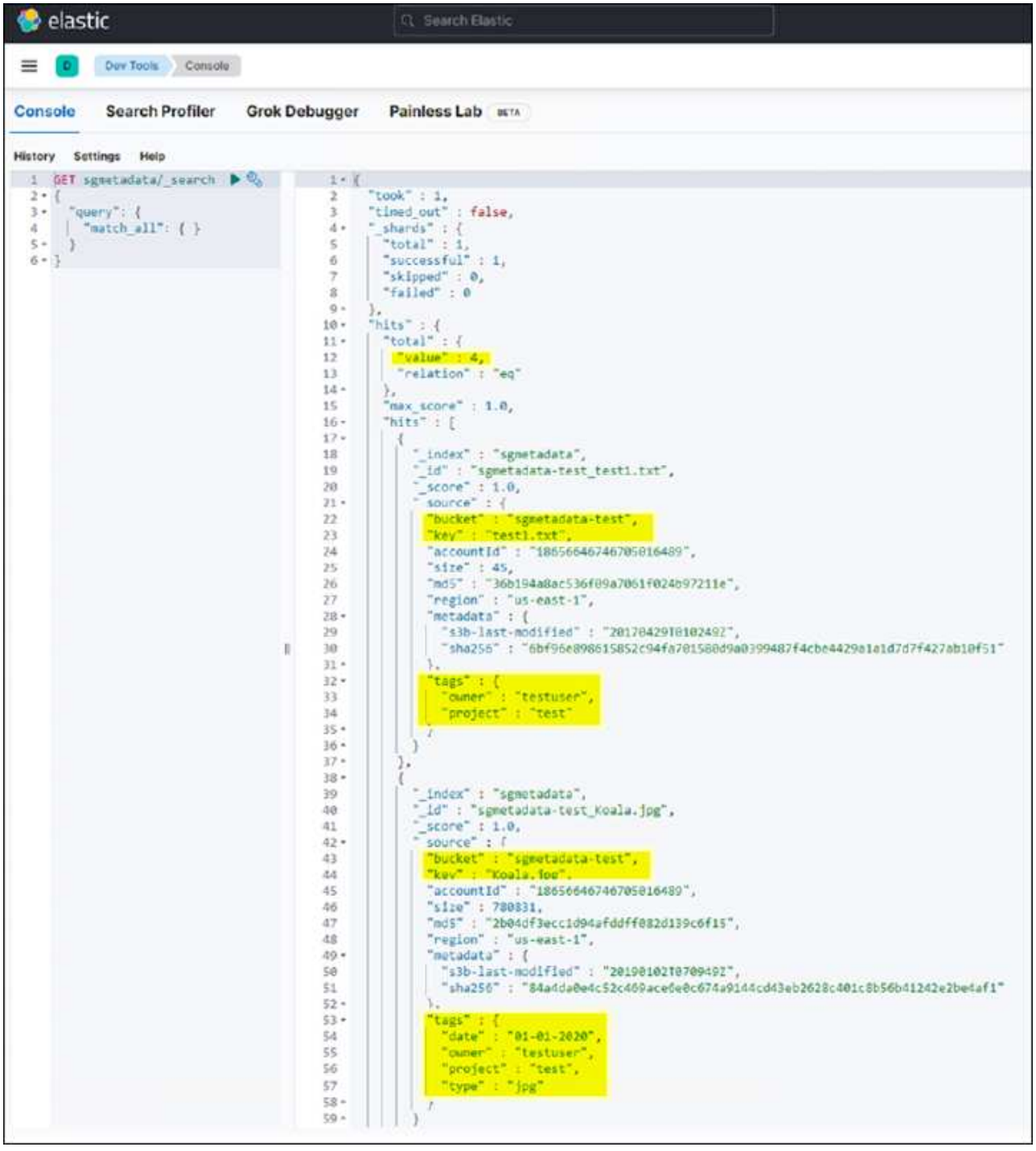
7. Verwenden Sie die Kibana UI, um zu überprüfen, ob die Objektmetadaten in den Index der sgmetadaten geladen wurden.

   a. Wählen Sie im Menü Verwaltung > Entwicklungstools.

   b. Fügen Sie die Beispielabfrage in das Konsolenfenster auf der linken Seite ein, und klicken Sie auf das Dreieckssymbol, um sie auszuführen.

      Das Beispielergebnis für die Abfrage 1 im folgenden Beispiel-Screenshot zeigt vier Datensätze. Dies entspricht der Anzahl der Objekte im Bucket.

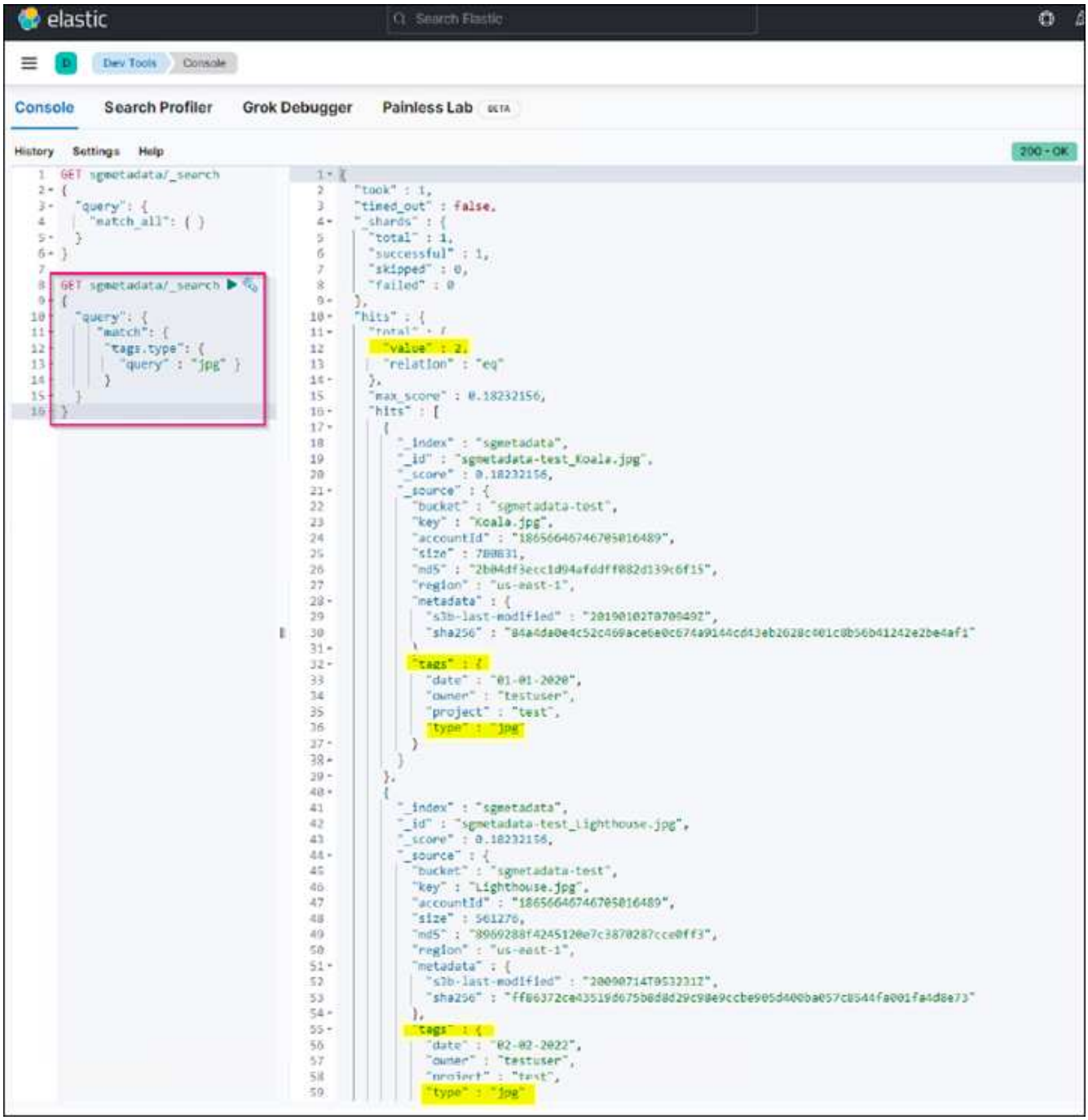
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



Das Beispielergebnis für Abfrage 2 im folgenden Screenshot zeigt zwei Datensätze mit Tag-Typ jpg.

```
GET sgmetadata/_search
{
    "query": {
        "match": {
            "tags.type": {
                "query" : "jpg" }
                }
            }
}
```

+



Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- "Was sind Plattform-Services"
- "StorageGRID 11.6-Dokumentation"

Von Angela Cheng

Node-Klonen

Überlegungen und Performance von Node-Klonen

Überlegungen zu Node-Klonen

Node-Klone können eine schnellere Methode zum Austausch vorhandener Appliance-Nodes für eine Technologieaktualisierung sein, die Kapazität erhöhen oder die Performance Ihres StorageGRID Systems steigern. Node-Klon kann auch für die Konvertierung in Node-Verschlüsselung mit einem KMS oder die Änderung eines Storage-Node von DDP8 zu DDP16 nützlich sein.

- Die genutzte Kapazität des Quell-Node ist nicht relevant für die Zeit, die für den Abschluss des Klonprozesses erforderlich ist. Node-Klon ist eine vollständige Kopie des Node, einschließlich freiem Speicherplatz im Node.
- Quell- und Ziel-Appliances müssen dieselbe PGE-Version aufweisen
- Der Zielknoten muss immer eine größere Kapazität als die Quelle haben
  - Stellen Sie sicher, dass die neue Ziel-Appliance eine größere Laufwerksgröße als die Quelle hat
  - Wenn das Zielgerät über Laufwerke gleicher Größe verfügt und für DDP8 konfiguriert ist, können Sie das Ziel für DDP16 konfigurieren. Wenn die Quelle bereits für DDP16 konfiguriert ist, ist ein Node-Klon nicht möglich.
  - Beachten Sie beim Wechsel von SG5660 oder SG5760 Appliances zu SG6060 Appliances, dass die SG5x60 60 Laufwerke mit Kapazität haben, bei denen die SG6060 nur 58 hat.
- Für den Klonprozess eines Node muss der Quell-Node für die Dauer des Klonens offline im Grid sein. Wenn ein zusätzlicher Knoten während dieser Zeit offline geht, sind möglicherweise die Client-Services betroffen.
- 11.8 und unten: Ein Storage-Node kann nur 15 Tage offline sein. Wenn der Klonprozess fast 15 Tage beträgt oder 15 Tage überschreitet, können Sie das Erweiterungs- und Ausmusterung verwenden.
  - 11.9: Die 15-Tage-Grenze wurde entfernt.
- Bei einem SG6060 oder SG6160 mit Erweiterungs-Shelfs müssen Sie die Zeit für die richtige Shelf-Laufwerksgröße zur Zeit der Basis-Appliance hinzufügen, um die volle Klondauer zu erhalten.
- Die Anzahl der Volumes in einer Ziel-Storage-Appliance muss größer oder gleich der Anzahl der Volumes im Quell-Node sein. Sie können einen Quell-Node mit 16 Objektspeicher-Volumes (rangedb) nicht auf einer Ziel-Storage-Appliance mit 12 Objektspeicher-Volumes klonen, selbst wenn die Ziel-Appliance über eine größere Kapazität als der Quell-Node verfügt. Die meisten Storage Appliances verfügen über 16 Objektspeicher-Volumes, außer der SGF6112 Storage Appliance mit nur 12 Objektspeicher-Volumes. Sie können beispielsweise nicht von einem SG5760 in ein SGF6112 klonen.

Schätzungen der Performance von Node-Klonen

Die folgenden Tabellen enthalten berechnete Schätzungen für die Dauer von Node-Klonen. Die Bedingungen variieren, sodass Einträge in **BOLD** das 15-Tage-Limit für einen Knoten nach unten überschreiten können.

DDP8

SG5612/SG5712/SG5812 → BELIEBIG

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	1 Tag	2 Tage	2.5 Tage	3 Tage	4 Tage	4.5 Tage	5.5 Tage
25 GB	1 Tag	2 Tage	2.5 Tage	3 Tage	4 Tage	4.5 Tage	5.5 Tage

SG5660 → SG5760/SG5860

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	3.5 Tage	7 Tage	8.5 Tage	10.5 Tage	**13,5 Tage**	**15,5 Tage**	**18,5 Tage**
25 GB	3.5 Tage	7 Tage	8.5 Tage	10.5 Tage	**13,5 Tage**	**15,5 Tage**	**18,5 Tage**

SG5660 → SG6060/SG6160

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	2.5 Tage	4.5 Tage	5.5 Tage	6.5 Tage	9 Tage	10 Tage	**12 Tage**
25 GB	2 Tage	4 Tage	5 Tage	6 Tage	8 Tage	9 Tage	10 Tage

SG5760/SG5860 → SG5760/SG5860

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	3.5 Tage	7 Tage	8.5 Tage	10.5 Tage	**13,5 Tage**	**15,5 Tage**	**18,5 Tage**
25 GB	3.5 Tage	7 Tage	8.5 Tage	10.5 Tage	**13,5 Tage**	**15,5 Tage**	**18,5 Tage**

SG5760/SG5860 → SG6060/SG6160

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	2.5 Tage	4.5 Tage	5.5 Tage	6.5 Tage	9 Tage	10 Tage	**12 Tage**
25 GB	2 Tage	3.5 Tage	4.5 Tage	5.5 Tage	7 Tage	8 Tage	9.5 Tage

SG6060/SG6160 → SG6060/SG6160

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	2.5 Tage	4.5 Tage	5.5 Tage	6.5 Tage	8.5 Tage	9.5 Tage	11.5 Tage
25 GB	2 Tage	3 Tage	4 Tage	4.5 Tage	6 Tage	7 Tage	8.5 Tage

DDP16

SG5760/SG5860 → SG5760/SG5860

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	3.5 Tage	6.5 Tage	8 Tage	9.5 Tage	**12,5 Tage**	**14 Tage**	**17 Tage**
25 GB	3.5 Tage	6.5 Tage	8 Tage	9.5 Tage	**12,5 Tage**	**14 Tage**	**17 Tage**

SG5760/SG5860 → SG6060/SG6160

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	2.5 Tage	5 Tage	6 Tage	7.5 Tage	10 Tage	11 Tage	**13 Tage**
25 GB	2 Tage	3.5 Tage	4 Tage	5 Tage	6.5 Tage	7 Tage	8.5 Tage

SG6060/SG6160 → SG6060/SG6160

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	3 Tage	5 Tage	6 Tage	7 Tage	9.5 Tage	10.5 Tage	**13 Tage**

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
25 GB	2 Tage	3.5 Tage	4.5 Tage	5 Tage	7 Tage	7.5 Tage	9 Tage

Erweiterungs-Shelf (oberhalb von SG6060/SG6160 für jedes Shelf auf der Quell-Appliance hinzufügen)

Geschwindigkeit der Netzwerkschnittstelle	Größe des 4-TB-Laufwerks	8-TB-Laufwerke	10-TB-Laufwerkgröße	12-TB-Laufwerksgröße	16-TB-Laufwerkgröße	18 TB Laufwerksgröße	22 TB Laufwerksgröße
10 GBIT	3.5 Tage	5 Tage	6 Tage	7 Tage	9.5 Tage	10.5 Tage	**12 Tage**
25 GB	2 Tage	3 Tage	4 Tage	4.5 Tage	6 Tage	7 Tage	8.5 Tage

Von Aron Klein

Standortverlagerung von Grid-Standorten und standortweites Netzwerkänderungsverfahren

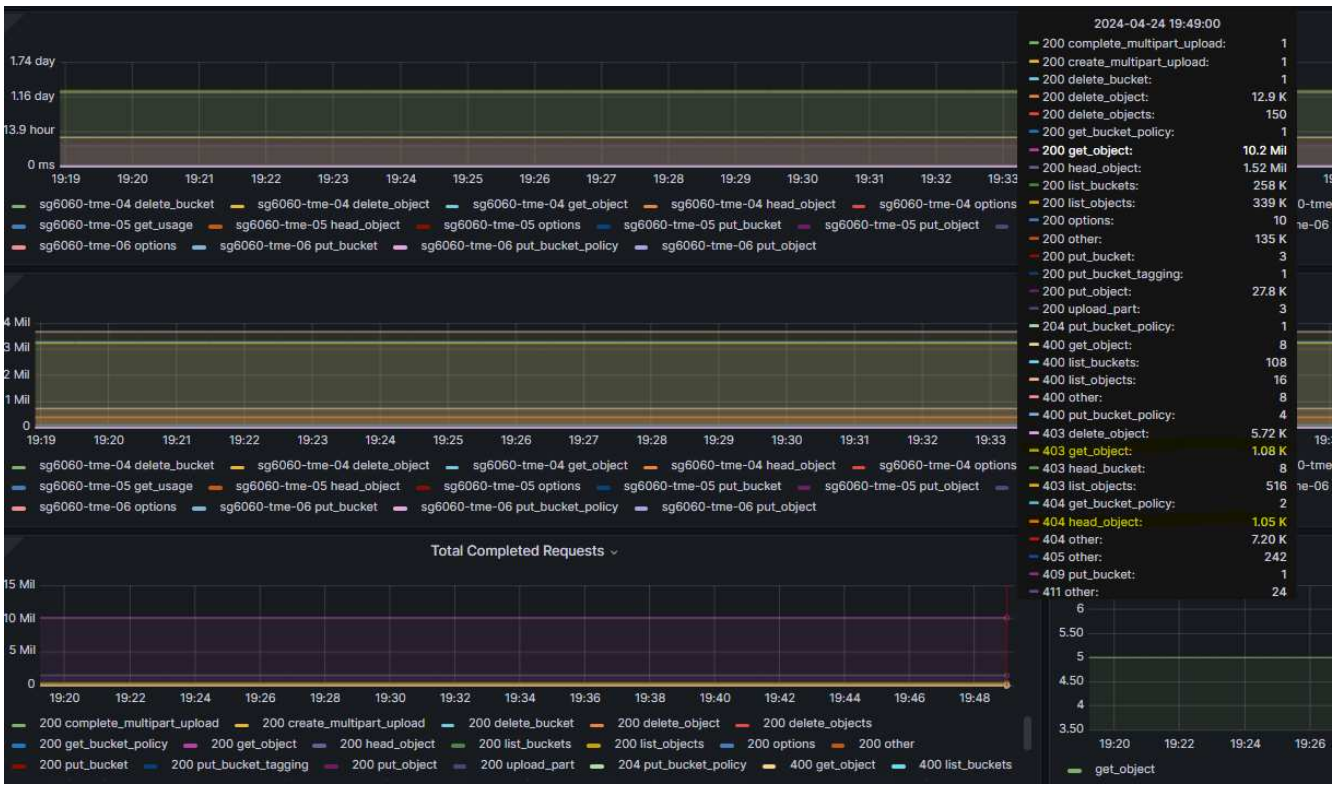
Dieser Leitfaden beschreibt die Vorbereitung und das Verfahren für den Standortwechsel in einem Grid mit mehreren Standorten von StorageGRID. Sie sollten über ein vollständiges Verständnis dieser Vorgehensweise verfügen und im Voraus planen, um einen reibungslosen Prozess zu gewährleisten und Unterbrechungen für Kunden zu minimieren.

Informationen zum Ändern des Grid-Netzwerks des gesamten Grid finden Sie unter "Ändern Sie die IP-Adressen für alle Nodes im Grid".

Überlegungen vor Standortverlagerung

- Die Standortverschiebungen sollten abgeschlossen sein und alle Nodes innerhalb von 15 Tagen online sein, um eine Wiederherstellung der Cassandra-Datenbank zu vermeiden.
  "Stellen Sie Storage Node länger als 15 Tage wieder her"
- Wenn eine ILM-Regel in der aktiven Richtlinie striktes Aufnahmeverhalten verwendet, sollten Sie sie in Erwägung ziehen, um einen Ausgleich oder eine doppelte Provisionierung zu erreichen, wenn der Kunde weiterhin Objekte im Grid bei der Standortverlagerung ABLEGEN möchte.
- Bei Storage Appliances mit 60 oder mehr Laufwerken: Verschieben Sie das Shelf niemals bei installierten Festplatten. Beschriften Sie die einzelnen Laufwerke, und entfernen Sie sie vor dem Verpacken/Verschieben aus dem Speichergehäuse.
- Ändern der StorageGRID-Appliance Grid-Netzwerk-VLAN kann Remote über das Admin-Netzwerk oder das Client-Netzwerk durchgeführt werden. Oder planen Sie, vor Ort zu sein, um die Änderung vor oder nach dem Umzug durchzuführen.
- Prüfen Sie, ob die Kundenanwendung vor dem PUT ein Objekt vom TYP HEAD oder GET Nonexistent verwendet. Wenn ja, ändern Sie die Bucket-Konsistenz in strong-site, um HTTP 500-Fehler zu vermeiden. Wenn Sie sich nicht sicher sind, überprüfen Sie die S3-Übersicht Grafana-Diagramme **Grid-Manager > Support > Metriken**, bewegen Sie die Maus über das Diagramm 'gesamte abgeschlossene Anfrage'.

Wenn eine sehr hohe Anzahl von 404 get Object oder 404 Head Objects vorhanden ist, verwenden wahrscheinlich eine oder mehrere Anwendungen Head oder Get Nonexistence Objects. Die Zählung wird akkumuliert, Maus über verschiedene Zeitachse, um den Unterschied zu sehen.



Verfahren zum Ändern der Grid-IP-Adresse vor Standortverlagerung

Schritte

1. Wenn das neue Netznetz-Subnetz am neuen Standort verwendet wird, "Fügen Sie das Subnetz der Subnetzliste des Netznetzes hinzu"
2. Melden Sie sich beim primären Admin-Knoten an, verwenden Sie Change-IP, um Grid IP-Änderungen vorzunehmen, müssen Sie die Änderung * inszenieren*, bevor Sie den Knoten für die Verlagerung herunterfahren.
   a. Wählen Sie 2 und dann 1 für Grid IP-Änderung

```
Editing: Node IP/subnet and gateway

Use up arrow to recall a previously typed value, which you can then edit
Use d or 0.0.0.0/0 as the IP/mask to delete the network from the node
Use q to complete the editing session early and return to the previous menu
Press <enter> to use the value shown in square brackets

================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP/mask [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP/mask [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP/mask [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP/mask [     10.45.74.18/26 ]: 10.45.74.28/26
================================================================================
LONDON-ADM1 Grid    Gateway [         10.45.74.1 ]:
LONDON-S1   Grid    Gateway [         10.45.74.1 ]:
LONDON-S2   Grid    Gateway [         10.45.74.1 ]:
LONDON-S3   Grid    Gateway [         10.45.74.1 ]:
================================================================================
================================================================================
Site: OXFORD
================================================================================
OXFORD-ADM1 Grid    IP/mask [     10.45.75.14/26 ]:
OXFORD-S1   Grid    IP/mask [     10.45.75.16/26 ]:
OXFORD-S2   Grid    IP/mask [     10.45.75.17/26 ]:
OXFORD-S3   Grid    IP/mask [     10.45.75.18/26 ]:
================================================================================
OXFORD-ADM1 Grid    Gateway [         10.45.75.1 ]:
OXFORD-S1   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S2   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S3   Grid    Gateway [         10.45.75.1 ]:
================================================================================
Finished editing. Press Enter to return to menu.
```

b. Wählen Sie 5, um die Änderungen anzuzeigen

```
================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP      [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP      [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP      [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP      [     10.45.74.18/26 ]: 10.45.74.28/26
Press Enter to continue
```

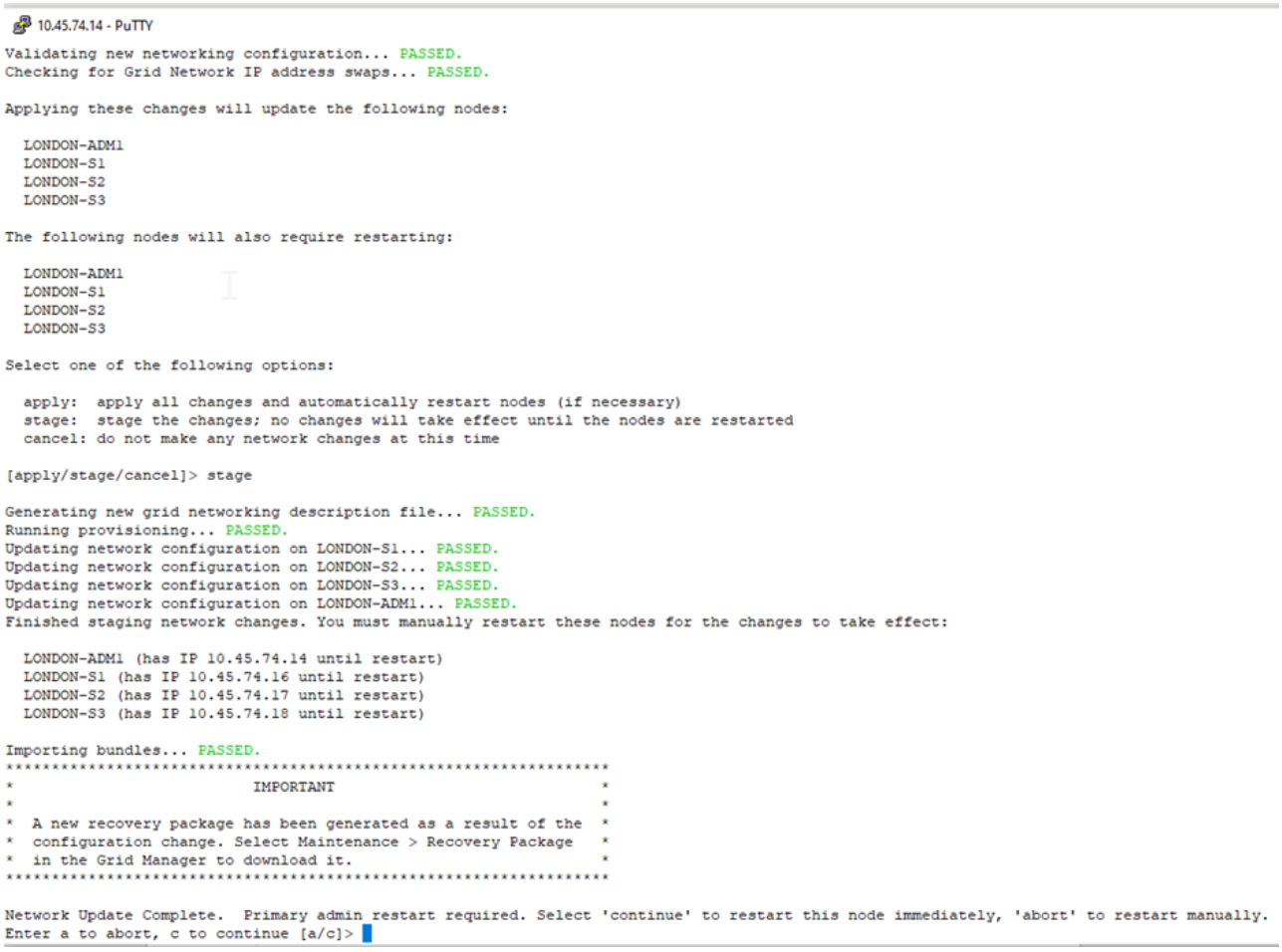
c. Wählen Sie 10, um die Änderung zu validieren und anzuwenden.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask and gateway
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection: 10
```

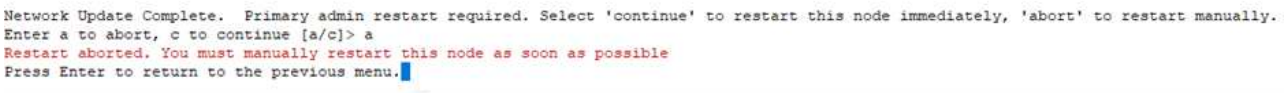
d. In diesem Schritt muss **Stufe** ausgewählt werden.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

The following nodes will also require restarting:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

Select one of the following options:

  apply:  apply all changes and automatically restart nodes (if necessary)
  stage:  stage the changes; no changes will take effect until the nodes are restarted
  cancel: do not make any network changes at this time

[apply/stage/cancel]> stage
```

e. Wenn der primäre Admin-Knoten in der obigen Änderung enthalten ist, geben Sie **'a' ein, um den primären Admin-Knoten manuell neu zu starten**



f. Drücken Sie ENTER, um zum vorherigen Menü zurückzukehren und die Change-ip-Schnittstelle zu verlassen.



3. Laden Sie das neue Wiederherstellungspaket vom Grid Manager herunter. **Grid-Manager** > **Wartung** > **Recovery-Paket**
4. Wenn eine VLAN-Änderung auf der StorageGRID-Appliance erforderlich ist, lesen Sie den Abschnitt VLAN-Änderung der Appliance.
5. Fahren Sie alle Knoten und/oder Geräte am Standort herunter, kennzeichnen/entfernen Sie ggf. Festplattenlaufwerke, und entfernen Sie sie aus dem Rack, packen Sie sie aus, und verschieben Sie sie.
6. Wenn Sie die ip-Adresse des Admin-Netzwerks und/oder des Client-VLAN und der ip-Adresse ändern möchten, können Sie die Änderung nach der Verlagerung vornehmen.

VLAN-Änderung der Appliance

Bei der folgenden Vorgehensweise wird davon ausgegangen, dass Sie Remote-Zugriff auf das Admin- oder Client-Netzwerk der StorageGRID Appliance haben, um die Änderung Remote durchzuführen.

Schritte

1. Vor dem Herunterfahren des Geräts "Stellen Sie das Gerät in den Wartungsmodus".

2. Verwenden eines Browsers für den Zugriff auf die StorageGRID-Appliance-Installer-GUI mit https://<admin-or-client-network-ip>:8443. Grid IP kann nicht verwendet werden, da die neue Grid-IP bereits vorhanden ist, sobald die Appliance im Wartungsmodus gestartet wird.
3. Ändern Sie das VLAN für das Grid-Netzwerk. Wenn Sie über das Client-Netzwerk auf die Appliance zugreifen, können Sie das Client-VLAN derzeit nicht ändern. Sie können es nach dem Umzug ändern.
4. ssh zur Appliance und Herunterfahren des Node mit 'shutdoown -h now'
5. Sobald die Appliances an einem neuen Standort bereit sind, können Sie über die Benutzeroberfläche des StorageGRID-Appliance-Installationsprogramms auf zugreifen https://<grid-network-ip>:8443. Überprüfen Sie mithilfe der Ping/nmap-Tools in der GUI, ob sich der Speicher im optimalen Zustand und der Netzwerkverbindung zu anderen Grid-Nodes befindet.
6. Wenn Sie planen, die Client-Netzwerk-IP zu ändern, können Sie das Client-VLAN zu diesem Zeitpunkt ändern. Das Client-Netzwerk ist erst bereit, wenn Sie die Client-Netzwerk-ip-Adresse mit dem Change-ip-Tool in einem späteren Schritt aktualisieren.
7. Beenden Sie den Wartungsmodus. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann **Neustart in StorageGRID** aus.
8. Wenn alle Nodes eingeschaltet sind und Grid kein Verbindungsproblem zeigt, aktualisieren Sie ggf. das Admin-Netzwerk und das Client-Netzwerk der Appliance mithilfe von Change-ip.

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

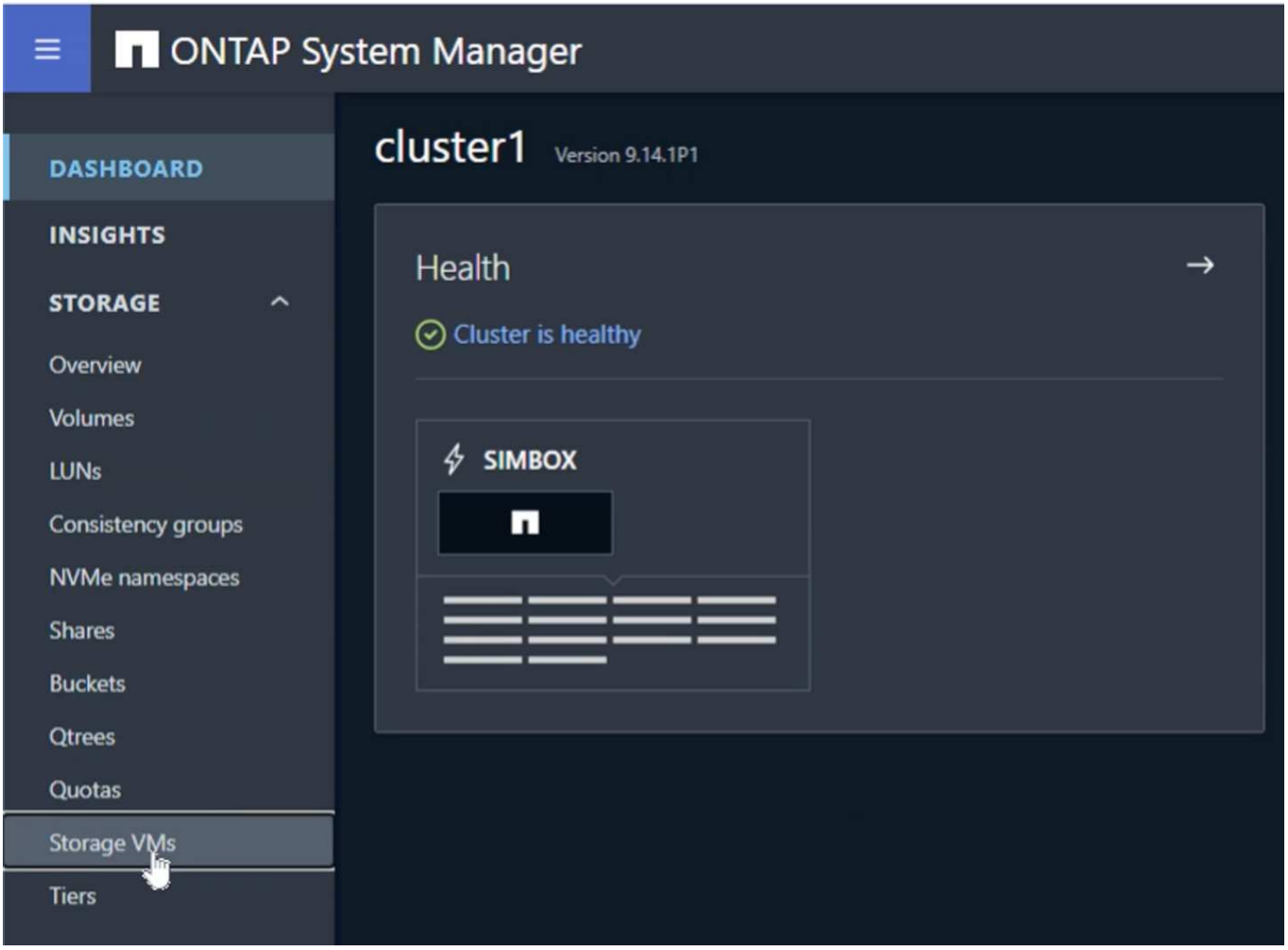
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

ONTAP wird vorbereitet

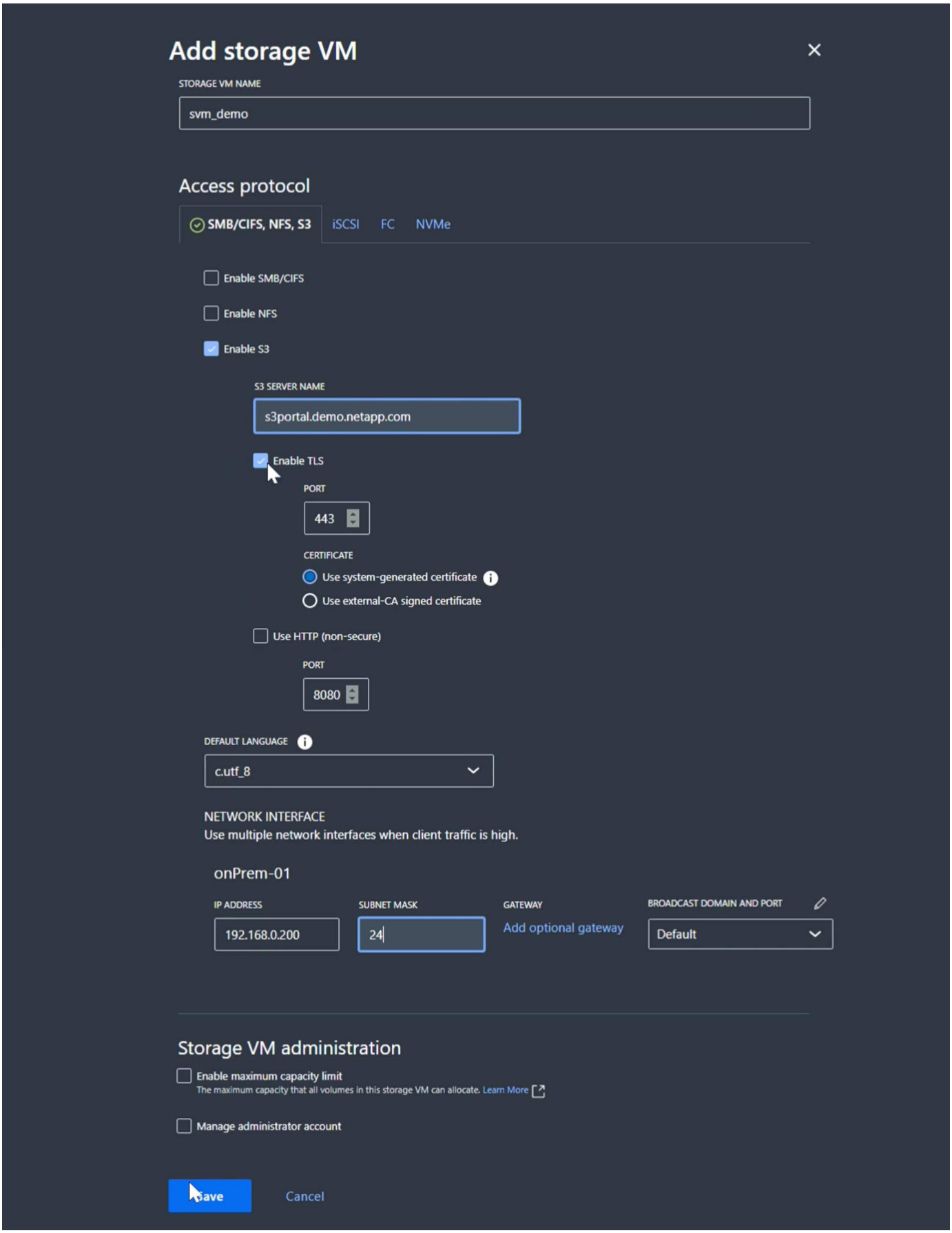
Für Demonstrationszwecke werden ein SVM Objektspeicher-Server, Benutzer, Gruppen, Gruppenrichtlinien und Buckets erstellt.

Erstellen Sie die virtuelle Speichermaschine

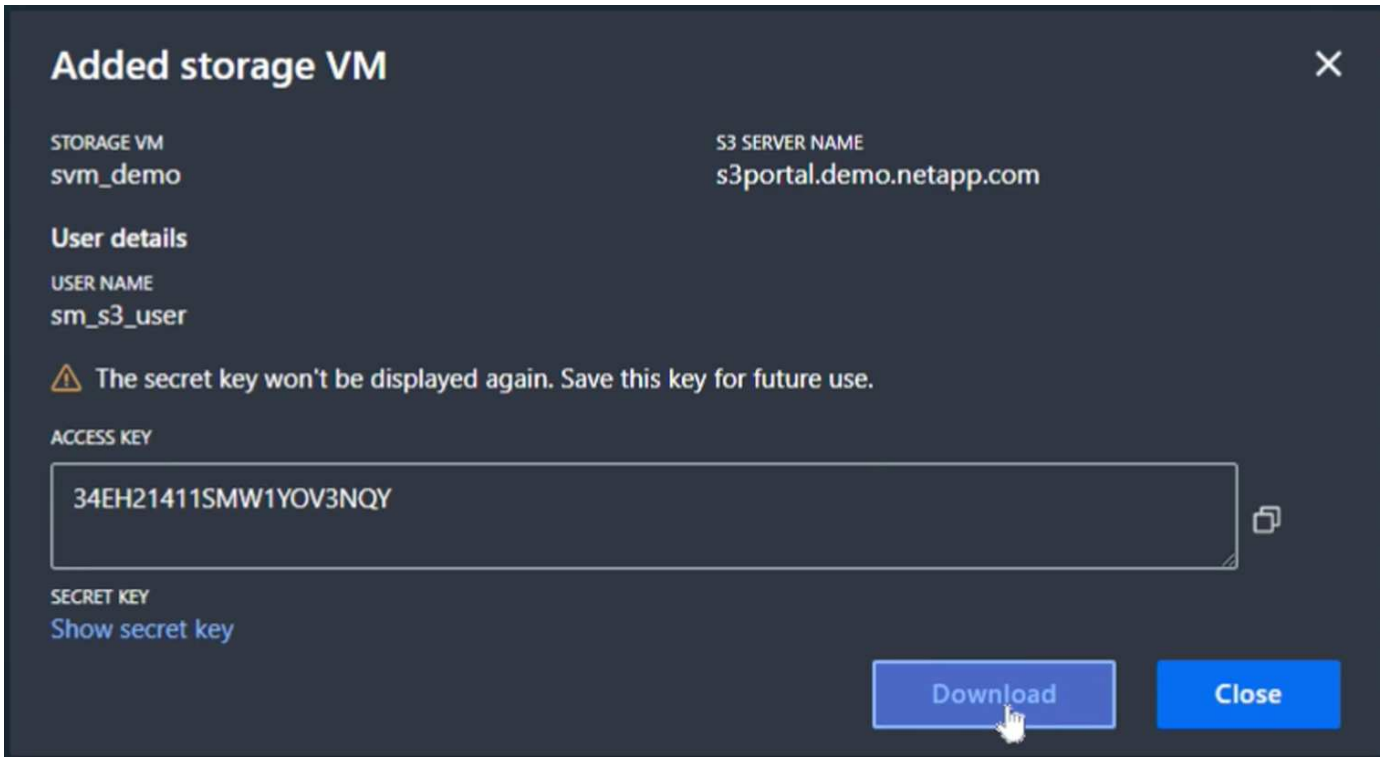
Navigieren Sie im ONTAP System Manager zu Storage VMs und fügen Sie eine neue Storage VM hinzu.



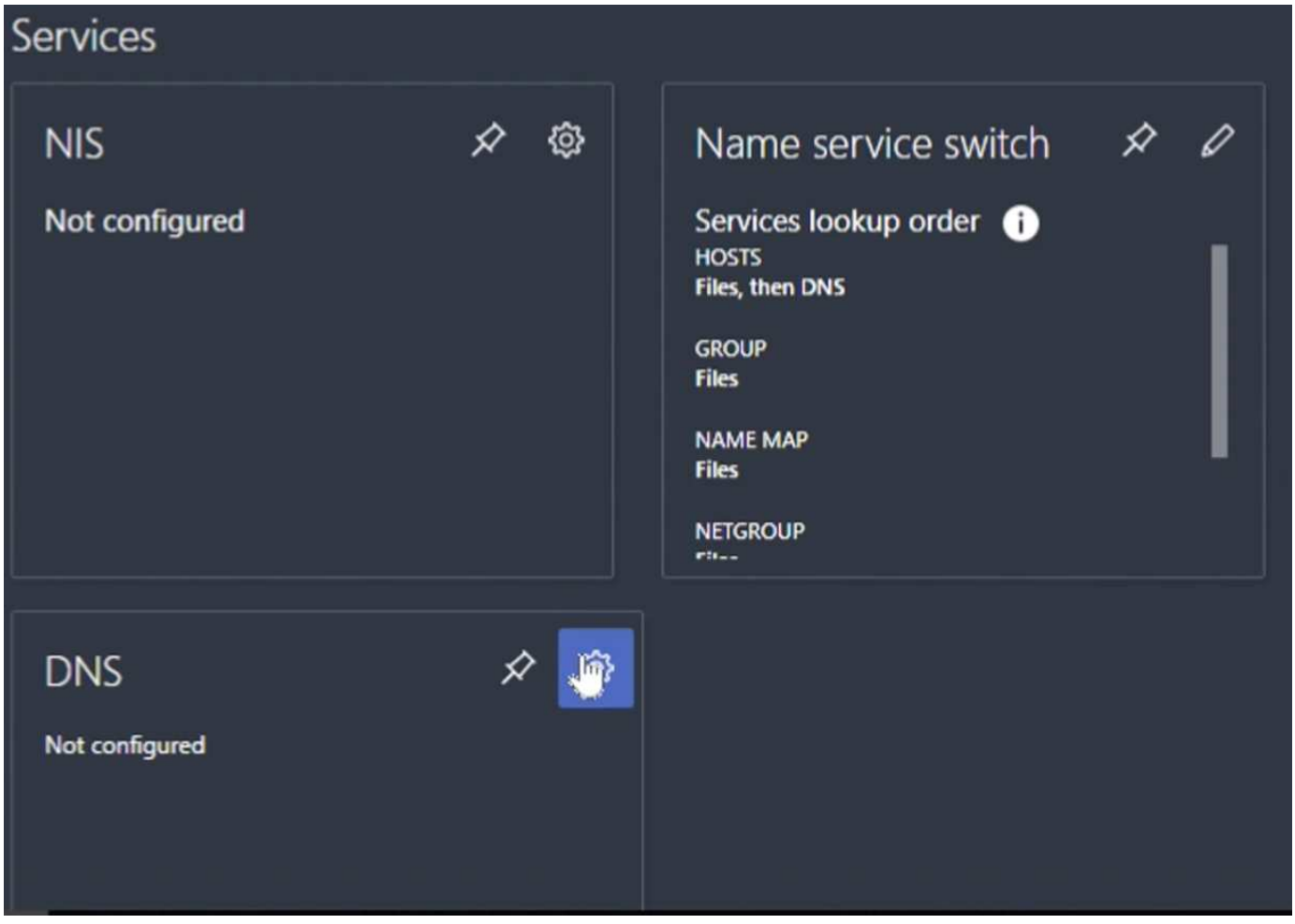
Aktivieren Sie die Kontrollkästchen „S3 aktivieren“ und „TLS aktivieren“, und konfigurieren Sie die HTTP(S)-Ports. Definieren Sie die IP-Adresse und die Subnetzmaske und definieren Sie das Gateway und die Broadcast-Domäne, wenn Sie nicht den Standard oder die in Ihrer Umgebung erforderlichen Standards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



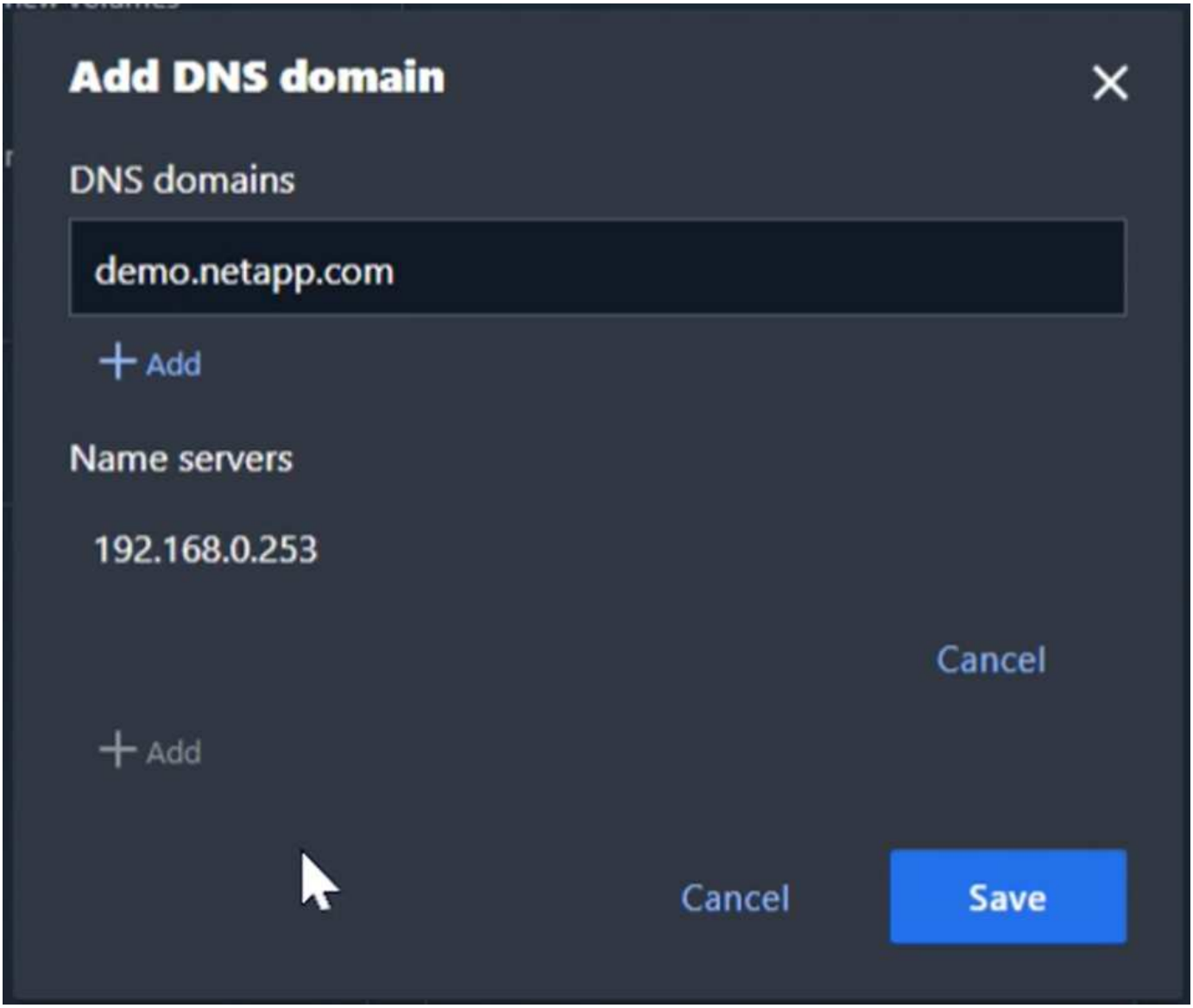
Im Rahmen der SVM-Erstellung wird ein Benutzer erstellt. Laden Sie die S3-Schlüssel für diesen Benutzer herunter, und schließen Sie das Fenster.



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

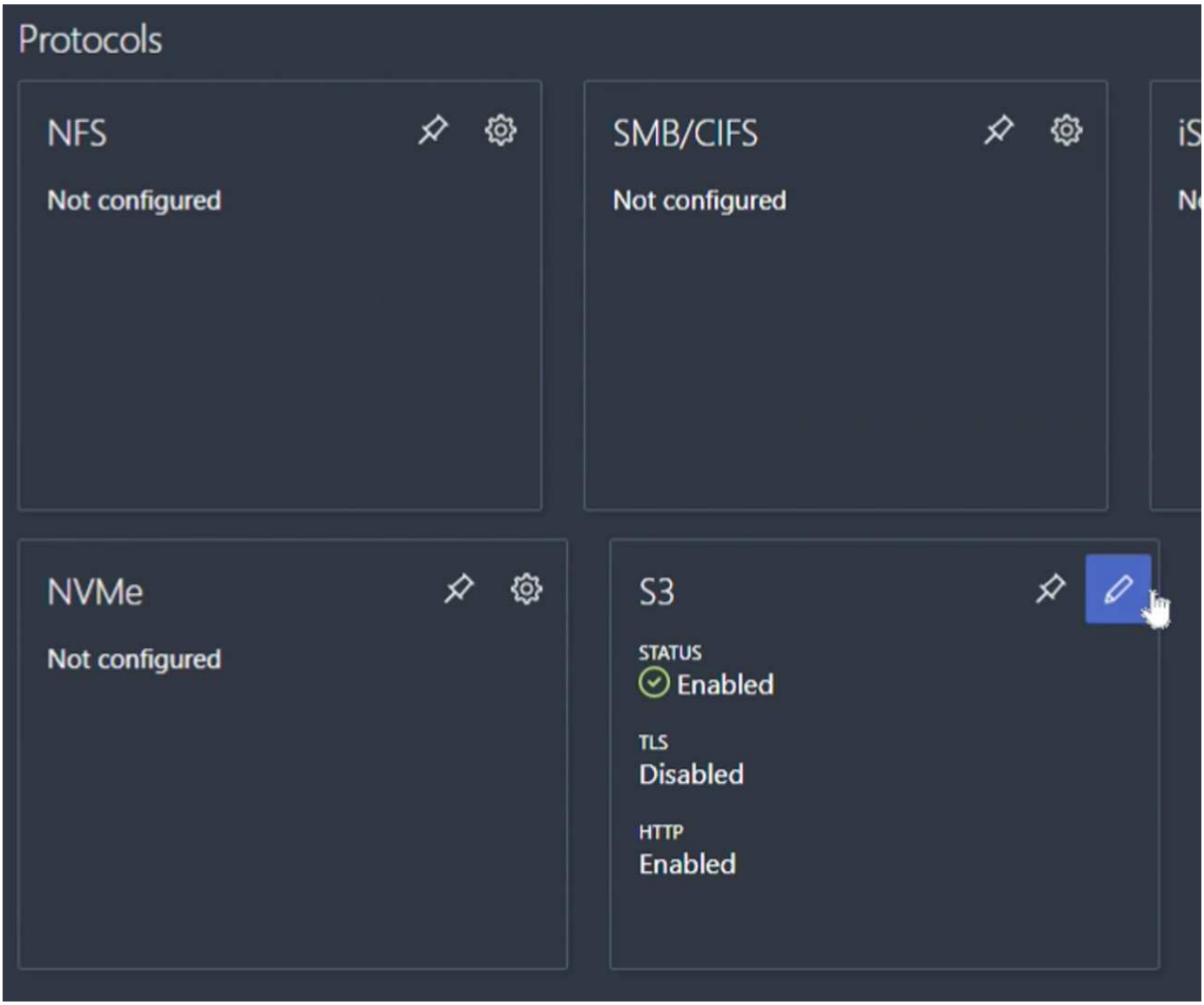


Definieren Sie den DNS-Namen und die IP-Adresse.

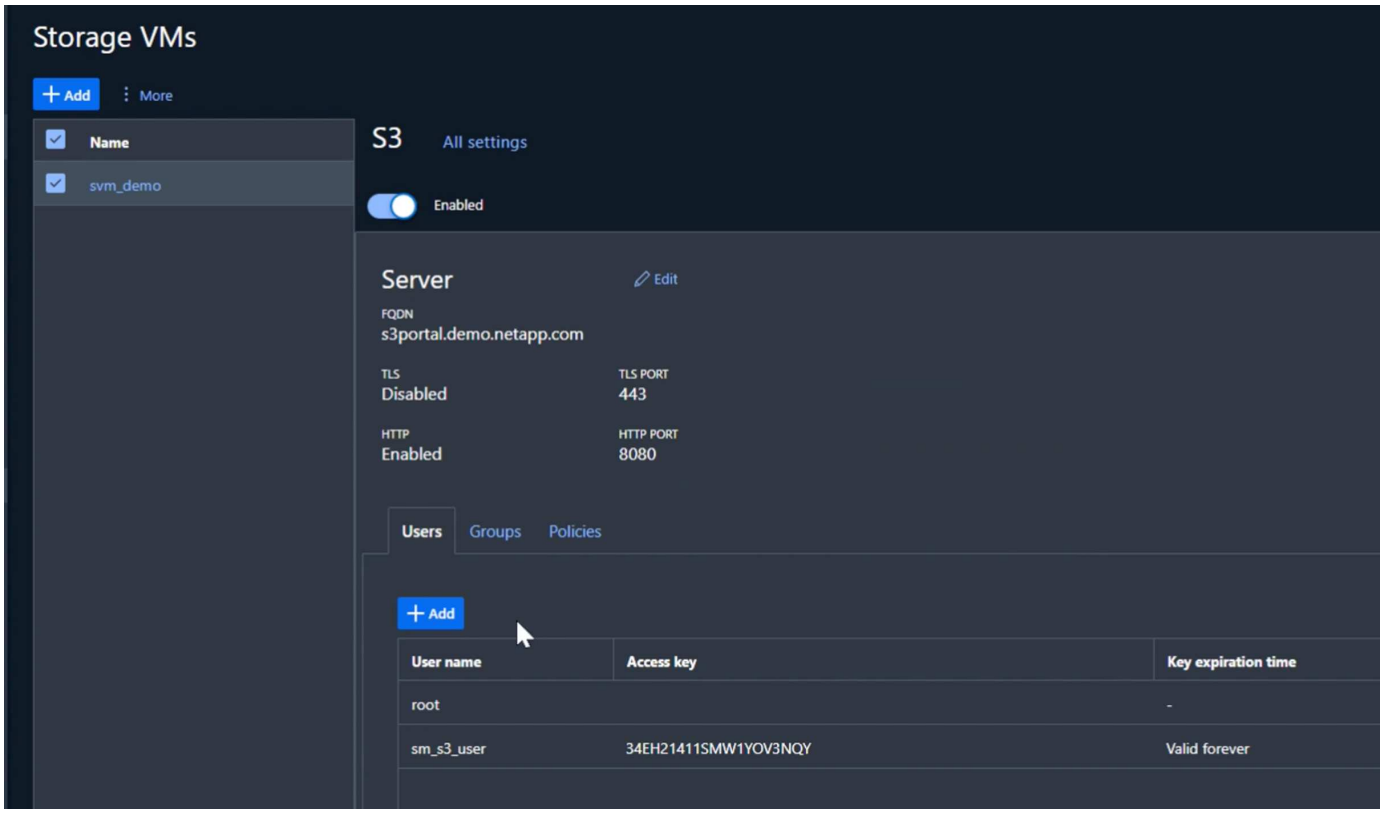


SVM S3-Benutzer erstellen

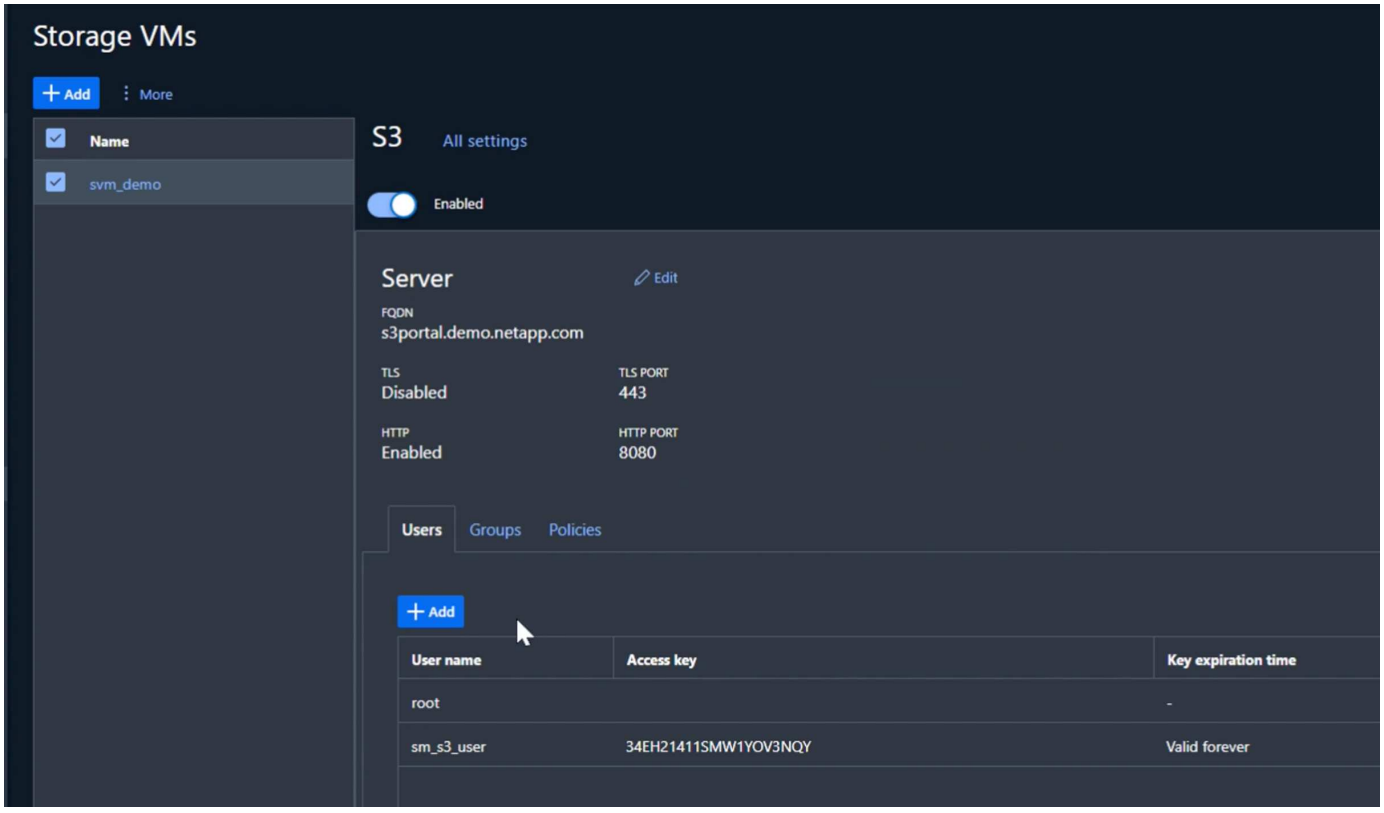
Jetzt können wir die S3-Benutzer und -Gruppe konfigurieren. Bearbeiten Sie die S3-Einstellungen.



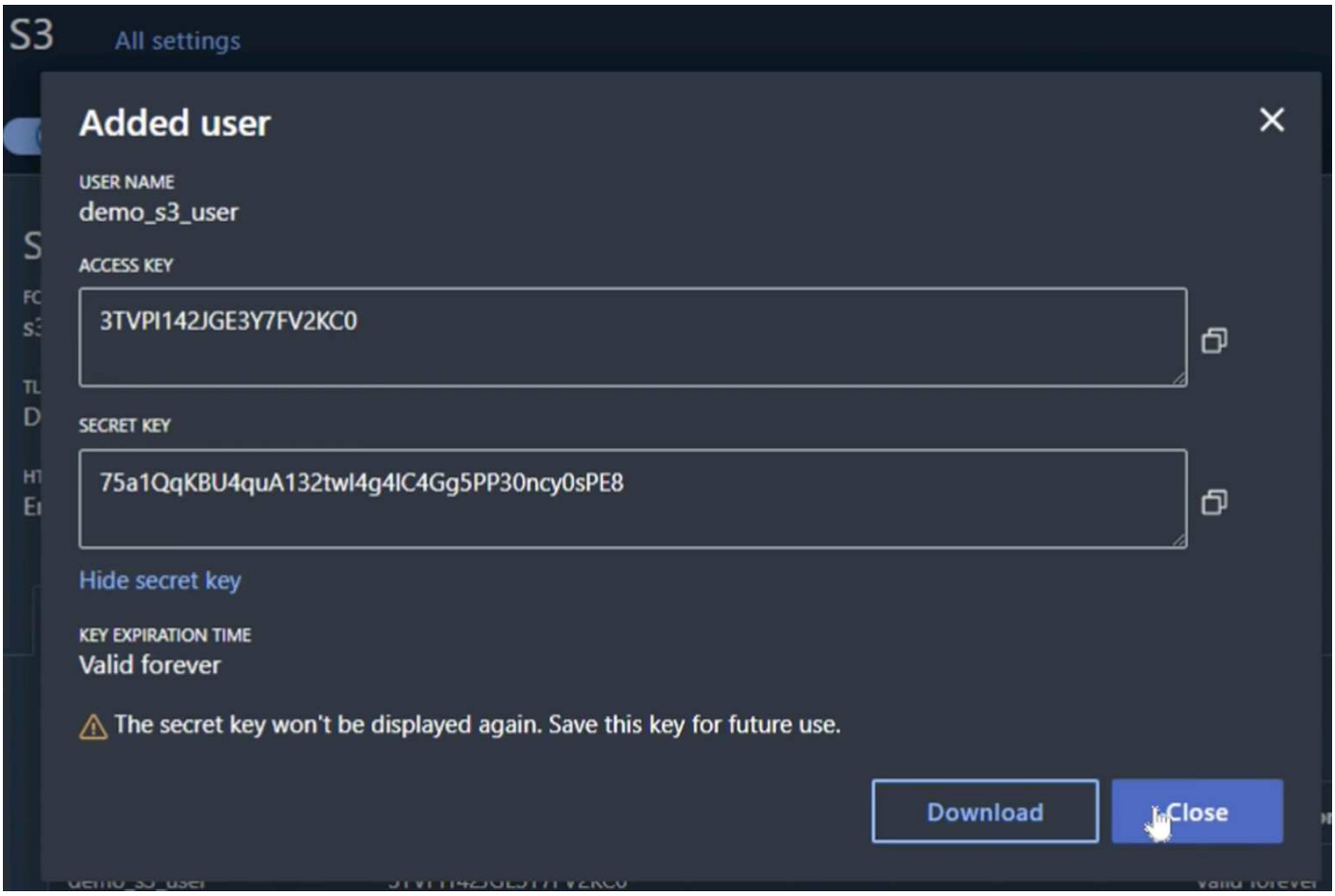
Neuen Benutzer hinzufügen.



Geben Sie den Benutzernamen und den Ablauf des Schlüssels ein.

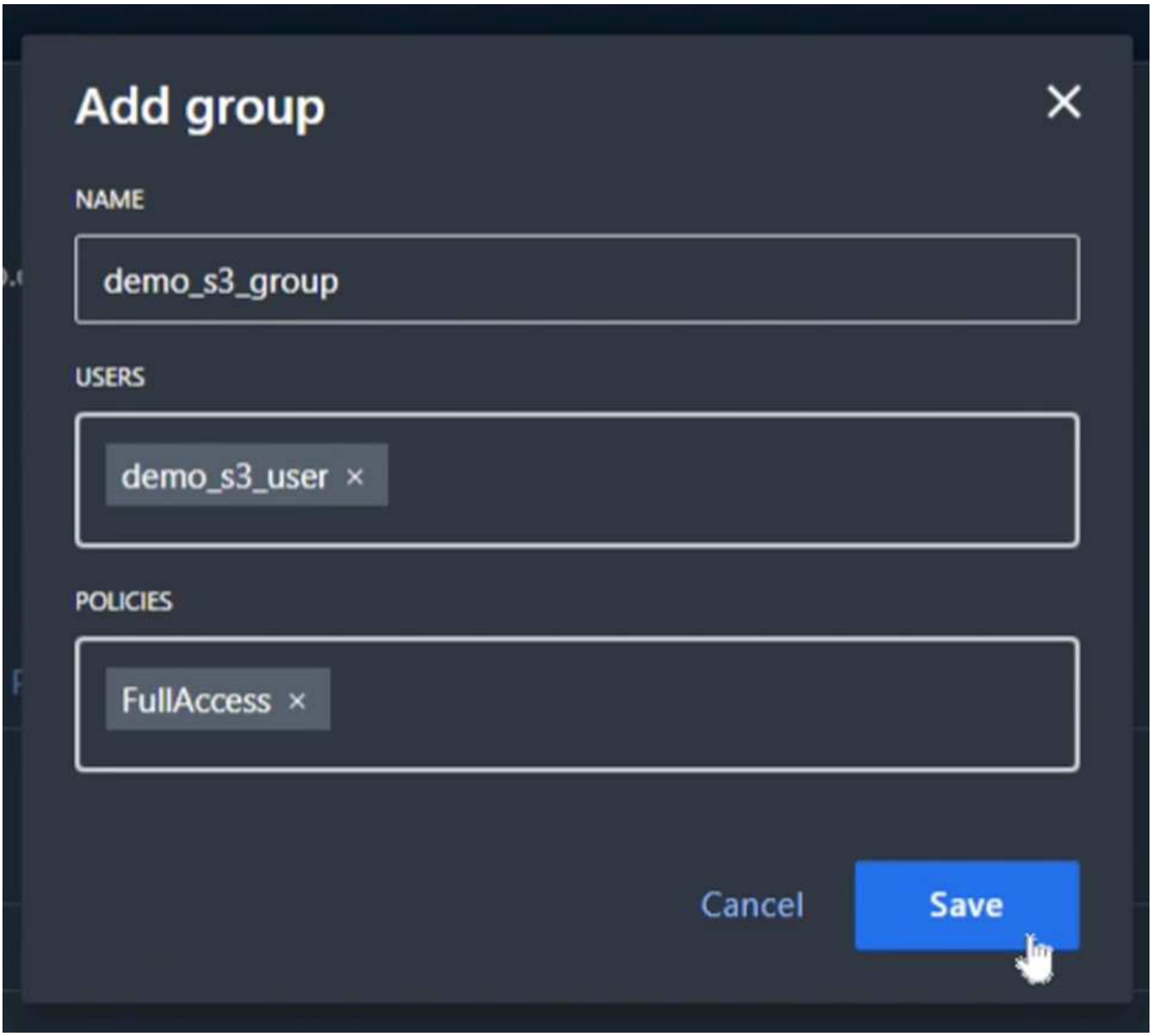


Laden Sie die S3-Schlüssel für den neuen Benutzer herunter.



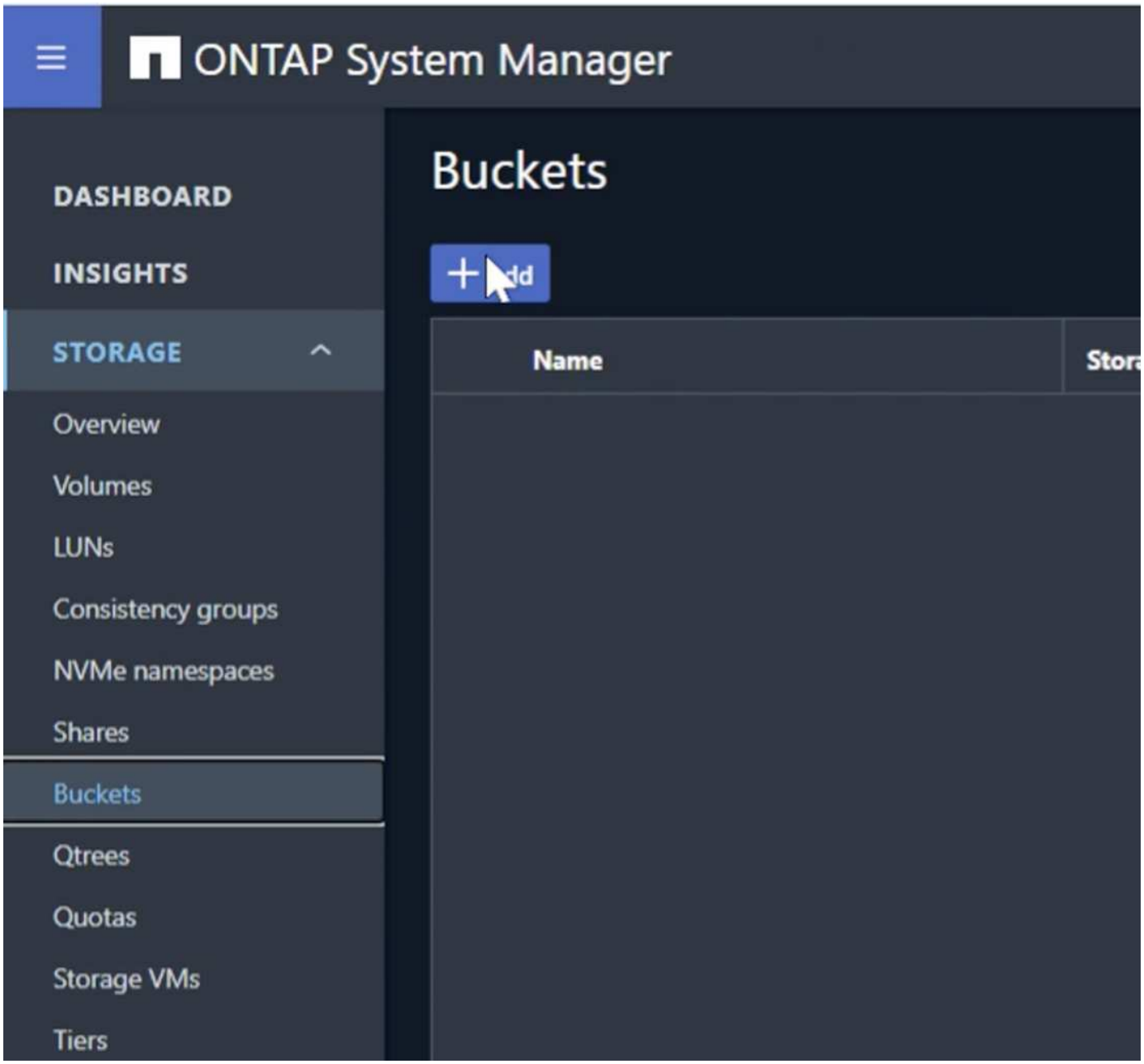
SVM S3-Gruppe erstellen

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

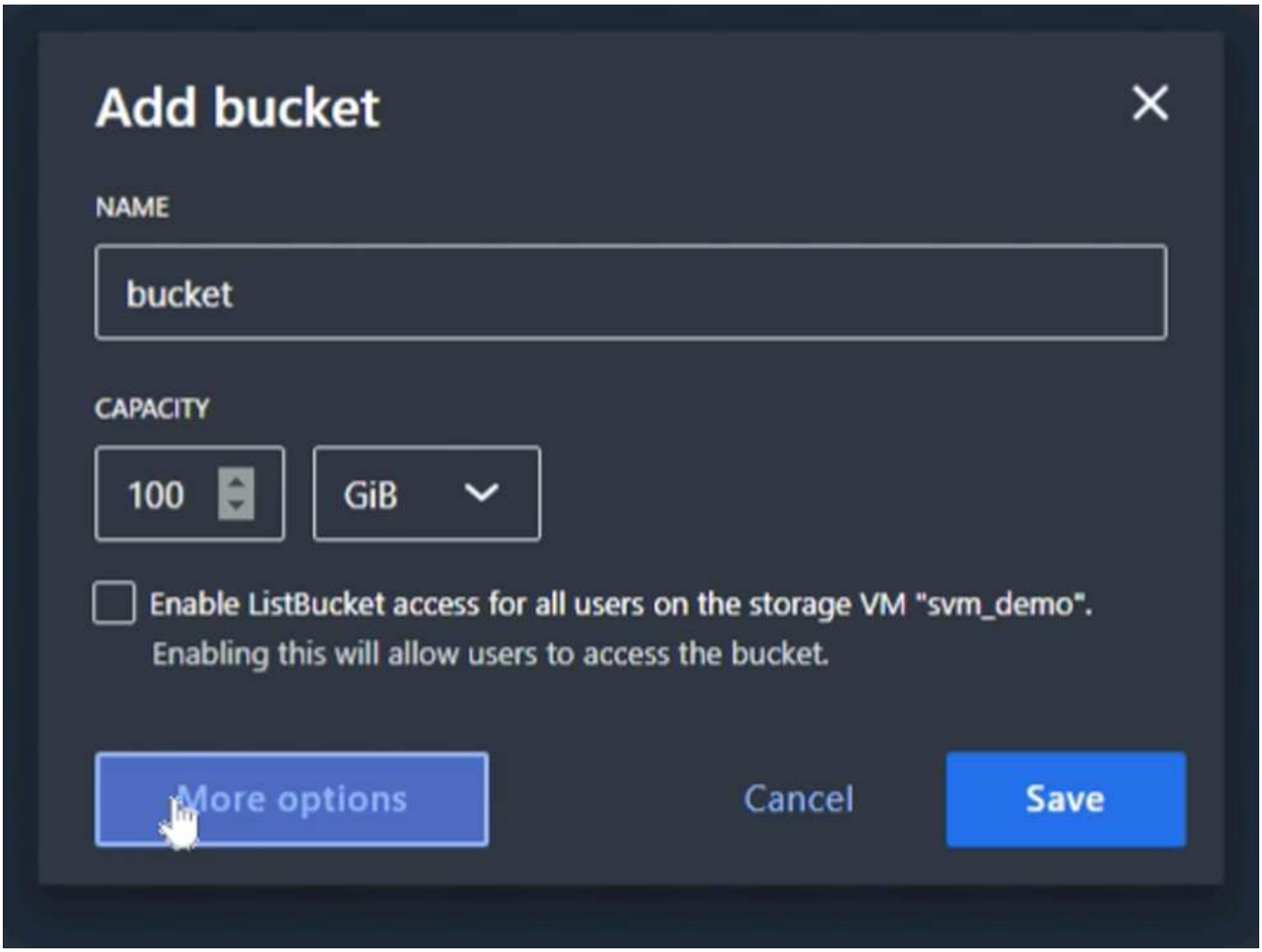


Erstellung von SVM S3 Buckets

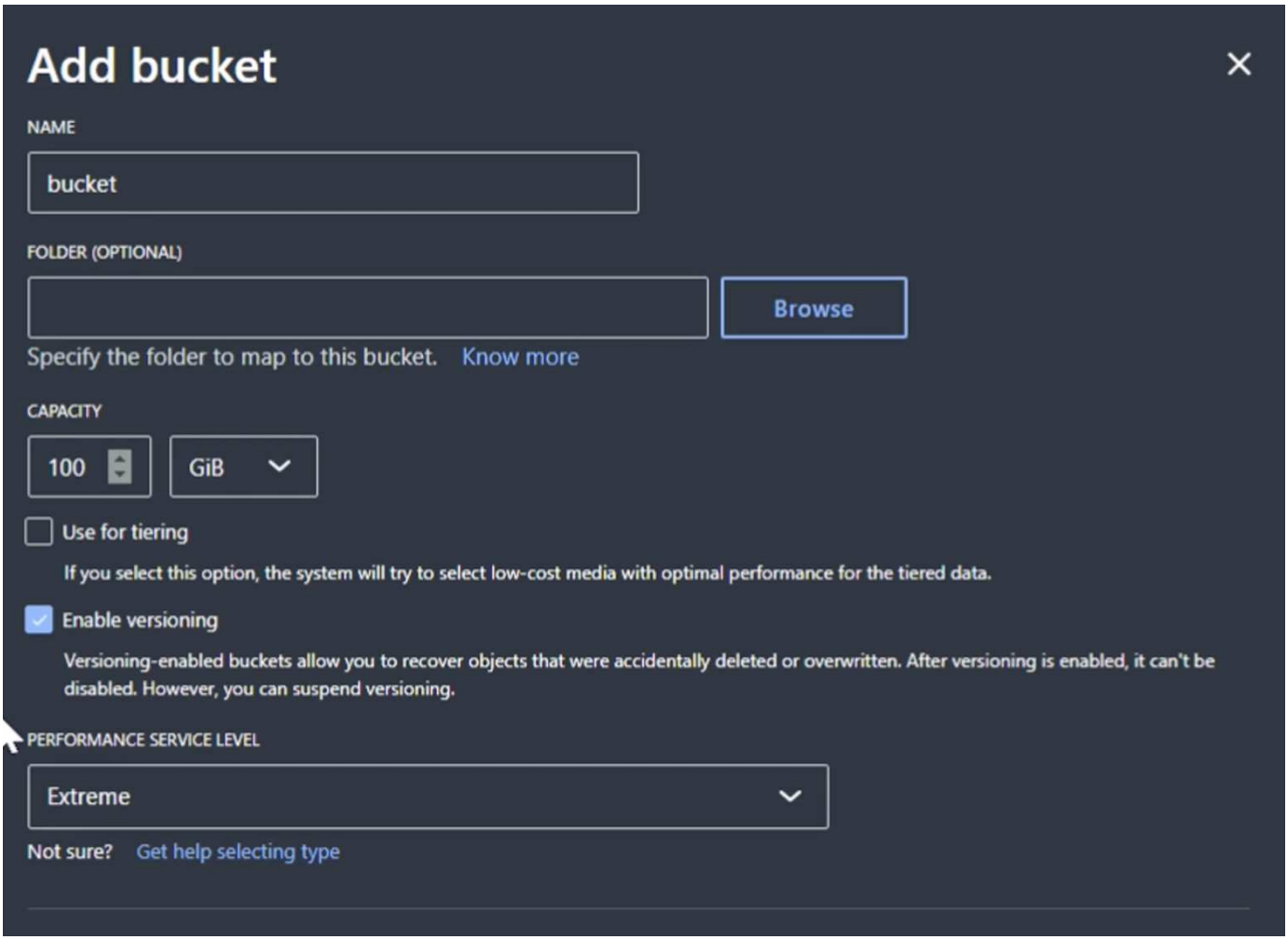
Navigieren Sie zum Bereich „Buckets“, und klicken Sie auf die Schaltfläche „+Hinzufügen“.



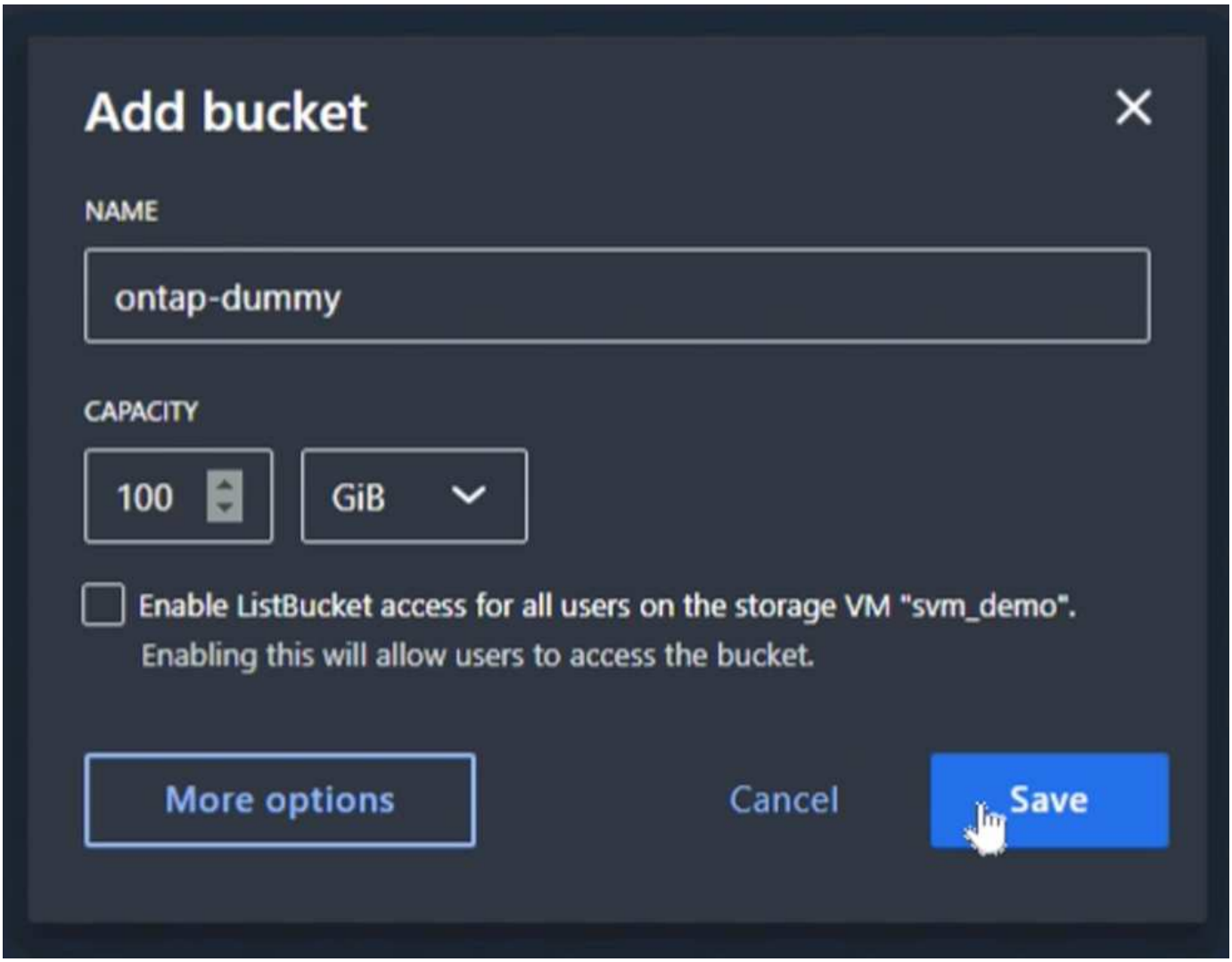
Geben Sie einen Namen und eine Kapazität ein, und deaktivieren Sie das Kontrollkästchen „Zugriff auf ListBucket aktivieren…“. Klicken Sie anschließend auf die Schaltfläche „Weitere Optionen“.



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



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“.



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

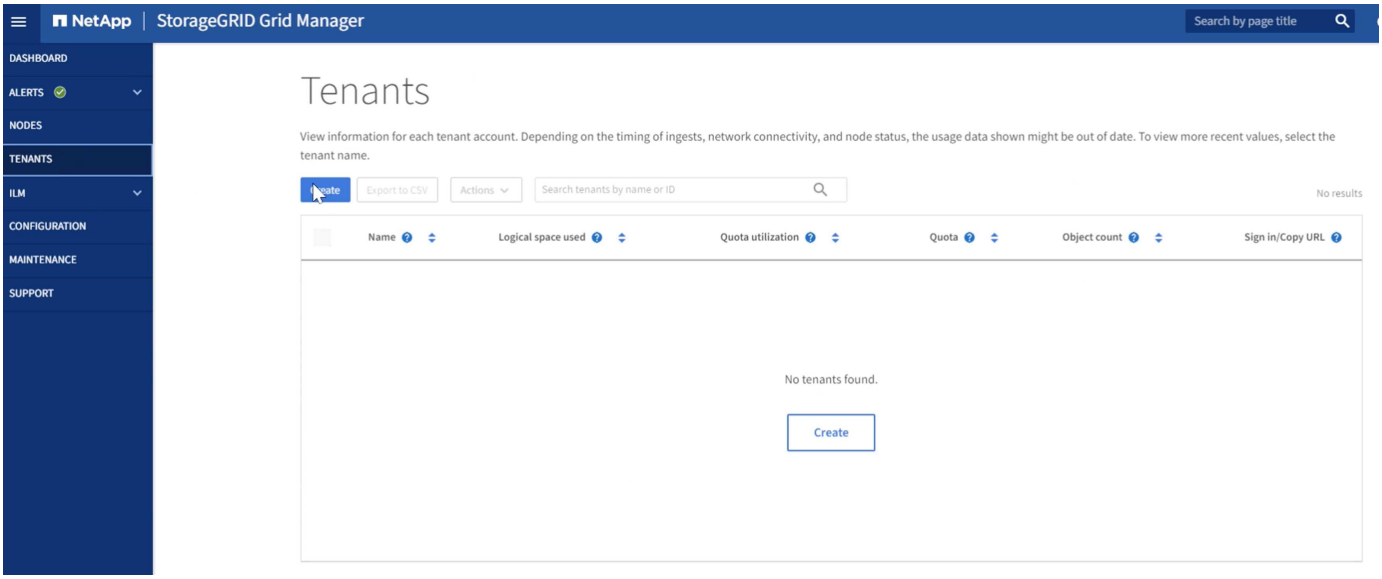
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

StorageGRID wird vorbereitet

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

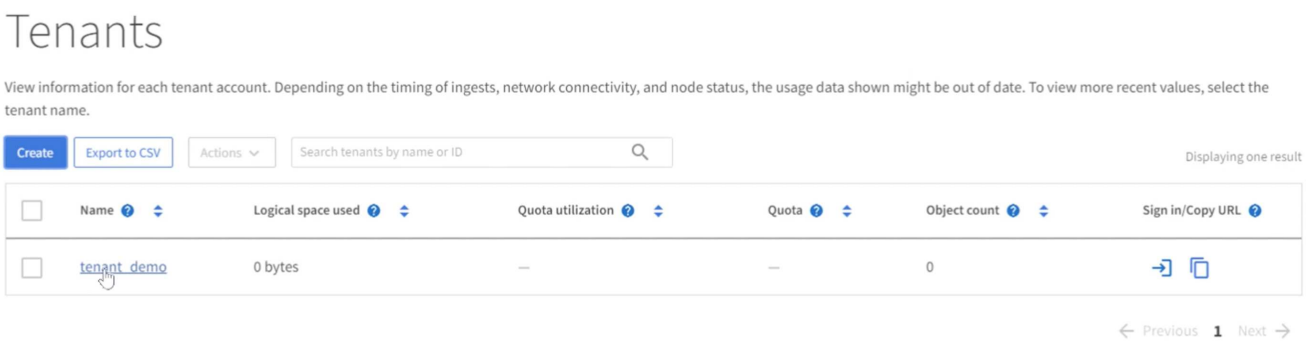
Erstellen Sie die Serviceeinheit

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

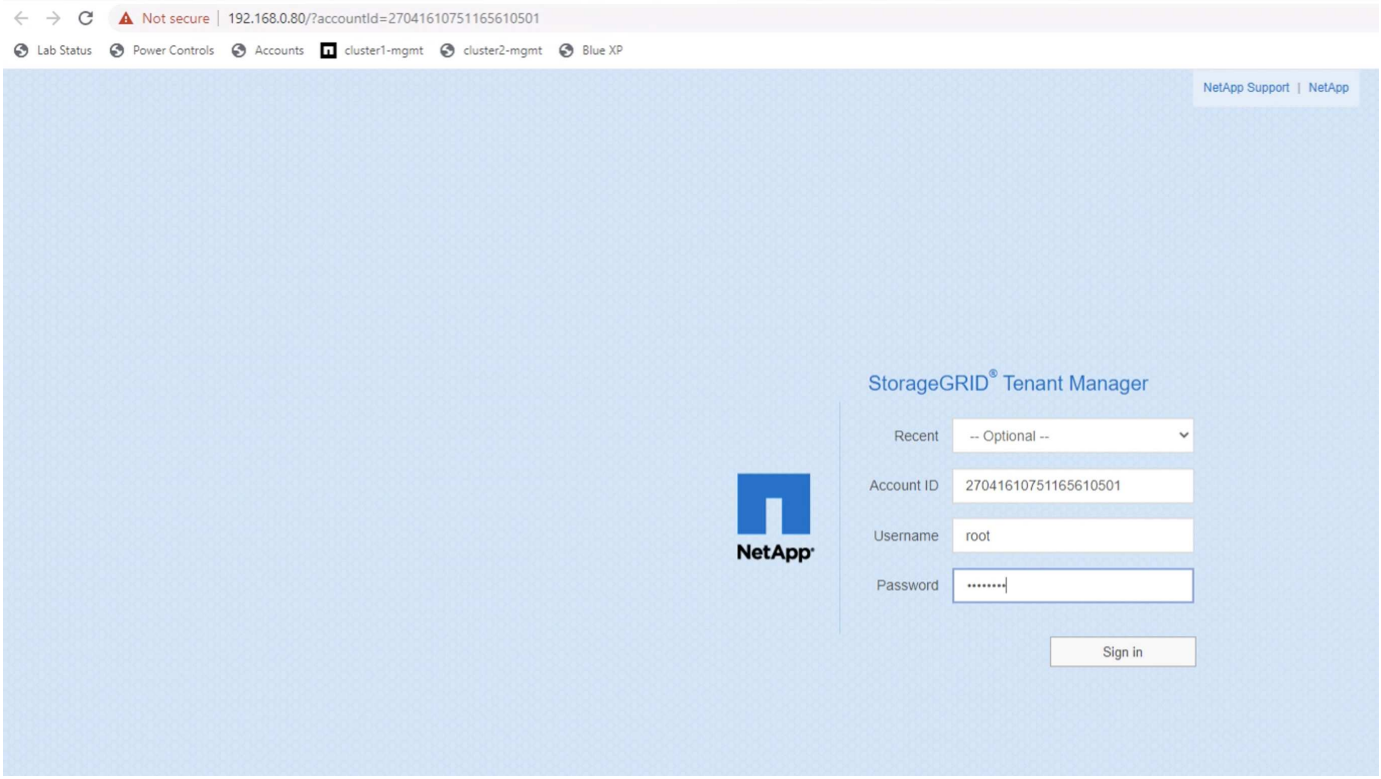


Geben Sie die Details für den Mandanten ein, indem Sie einen Mandantennamen angeben, und wählen Sie S3 für den Clienttyp aus. Es ist kein Kontingent erforderlich. Plattformdienste müssen nicht ausgewählt oder S3-Auswahl zugelassen werden. Sie können wählen, ob Sie eine eigene Identitätsquelle verwenden 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.

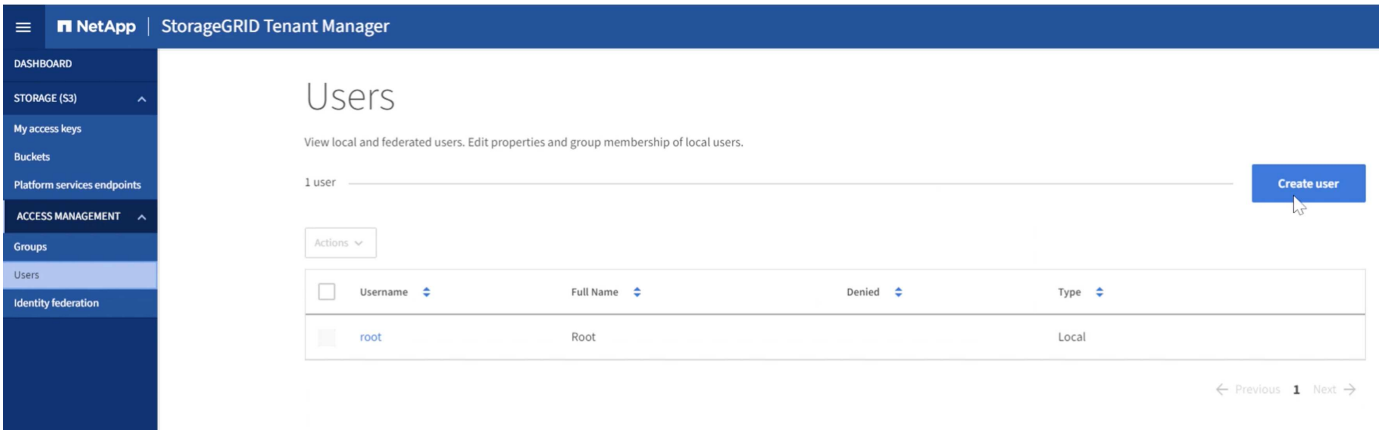


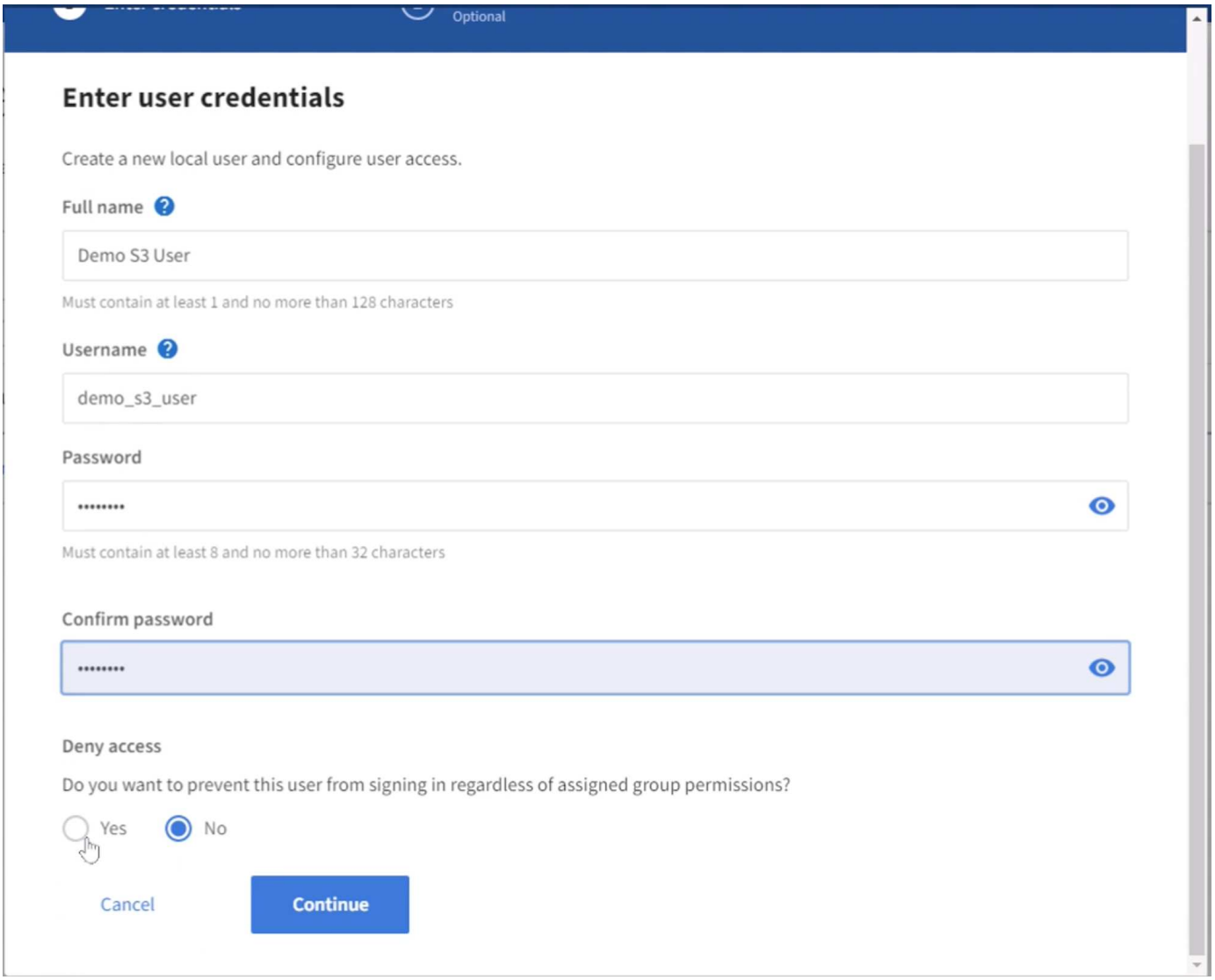
Dadurch gelangen Sie zur Anmeldung beim Mandantenportal. Speichern Sie die URL für die zukünftige Verwendung, und geben Sie die Anmeldedaten des Stammbenutzers ein.



Erstellen Sie den Benutzer

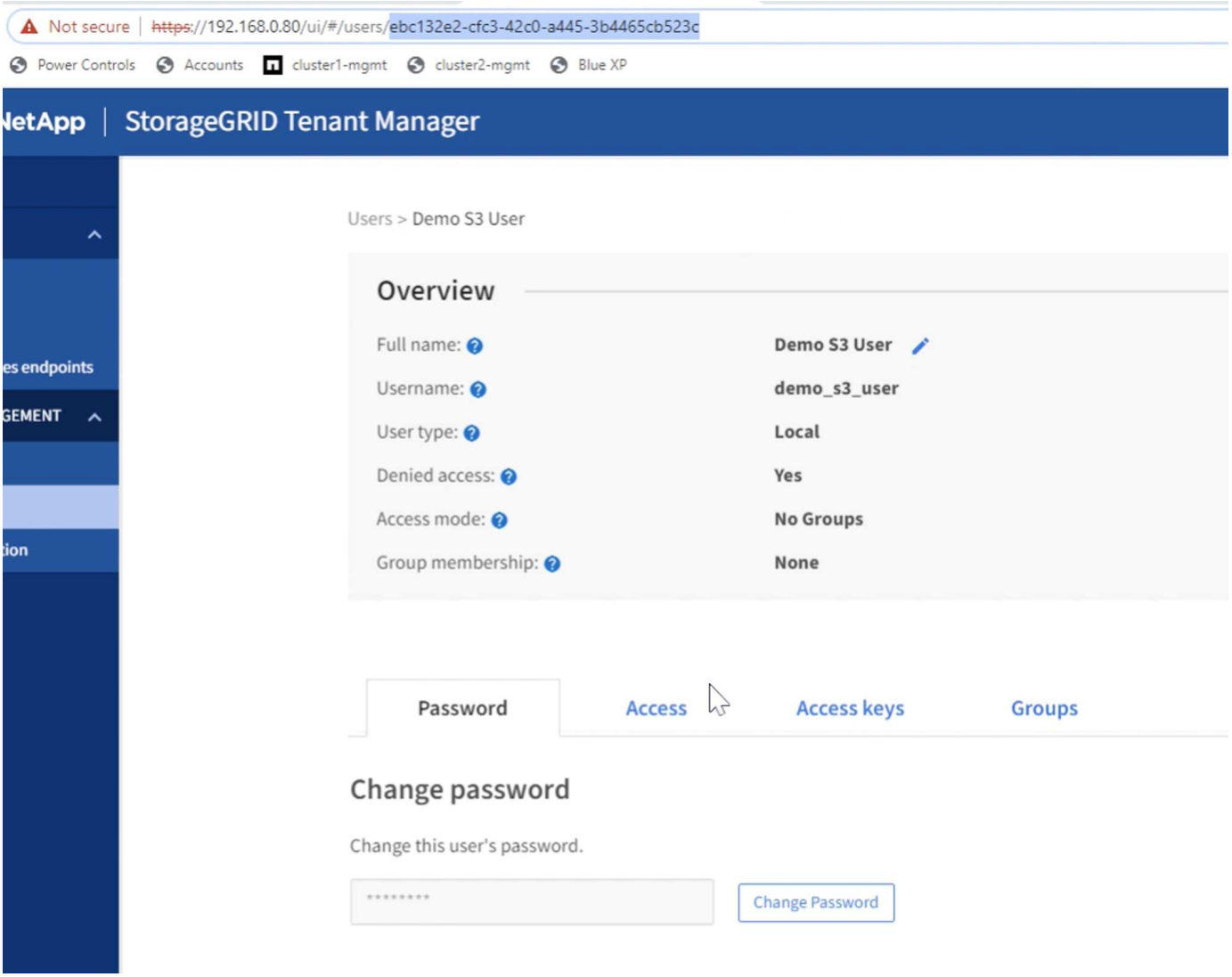
Navigieren Sie zur Registerkarte Benutzer, und erstellen Sie einen neuen Benutzer.



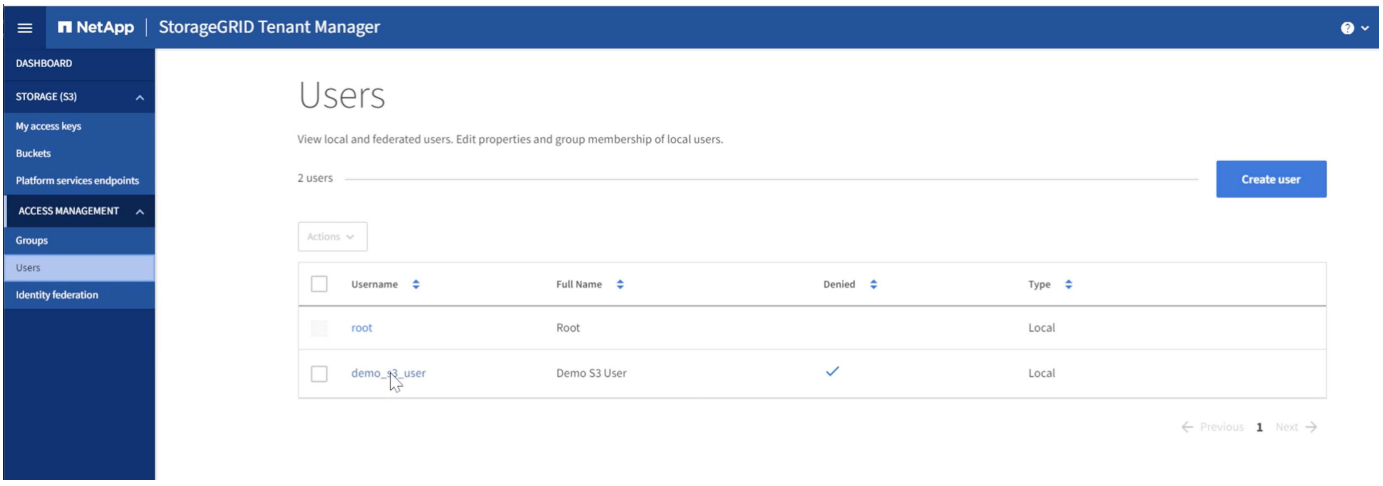


Nachdem der neue Benutzer erstellt wurde, klicken Sie auf den Benutzernamen, um die Details des Benutzers zu öffnen.

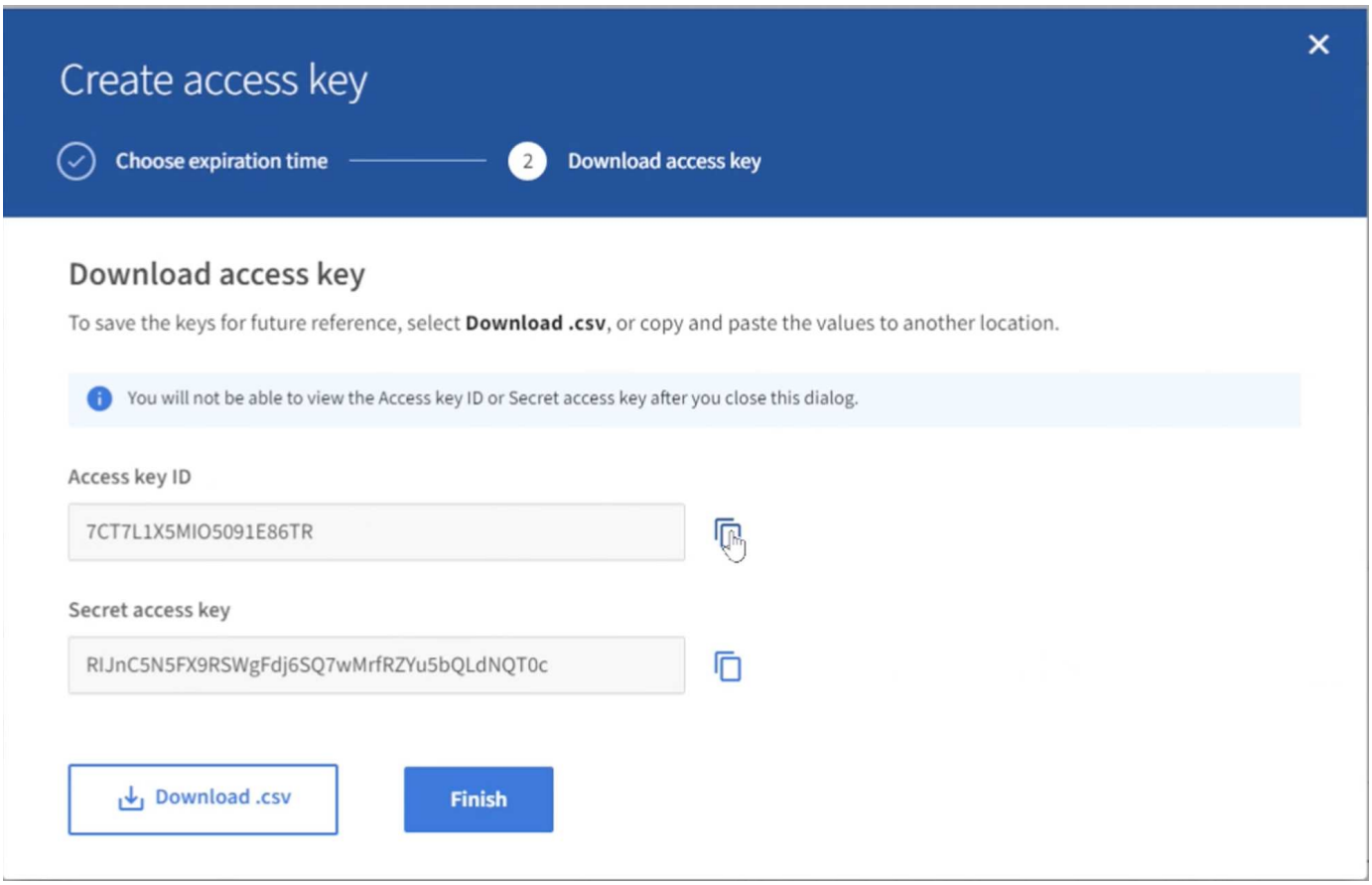
Kopieren Sie die Benutzer-ID aus der URL, die später verwendet werden soll.



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

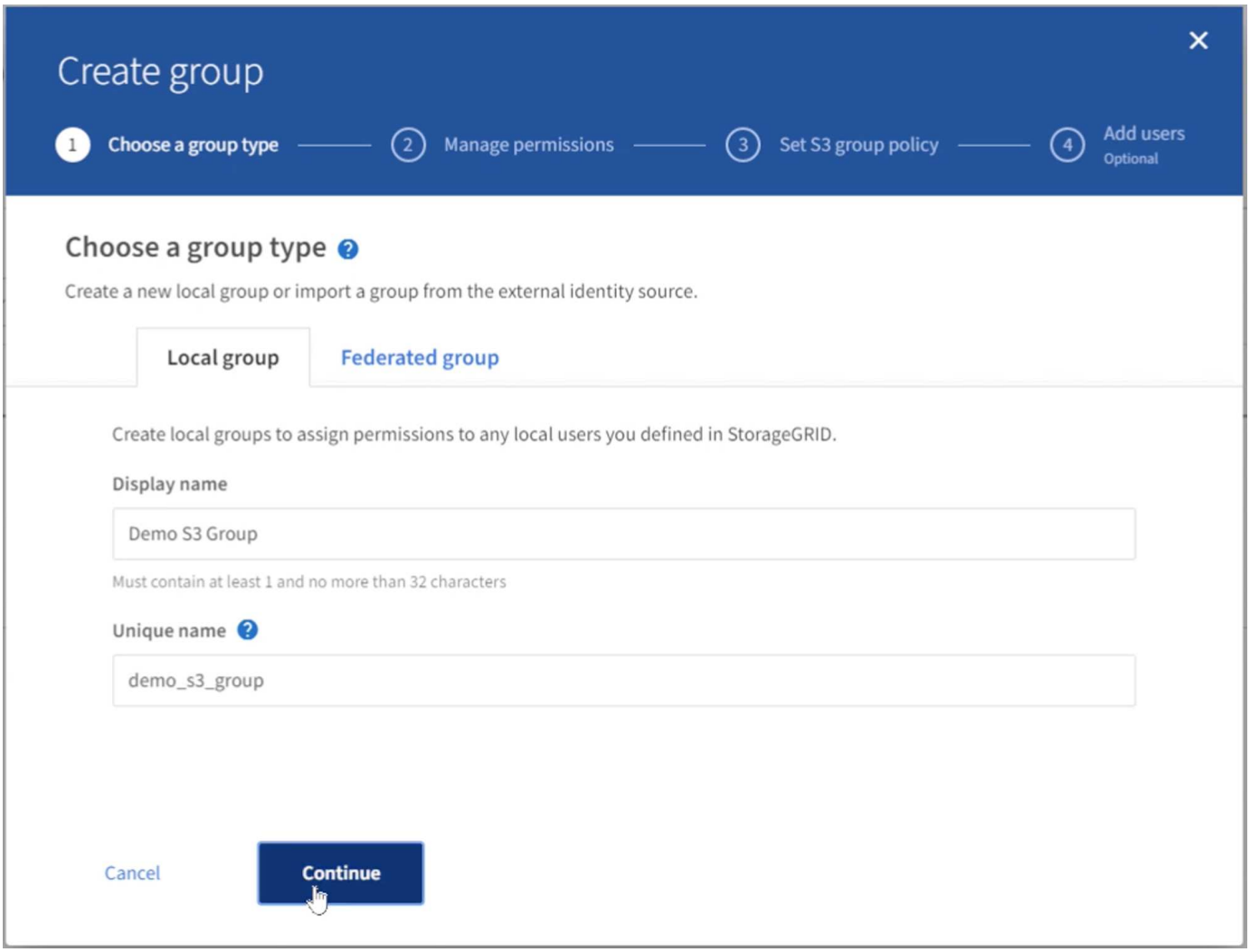


Wählen Sie die Registerkarte „Zugriffsschlüssel“ aus und klicken Sie auf die Schaltfläche „Schlüssel erstellen“. Es ist nicht notwendig, eine Verfallszeit einzustellen. Laden Sie die S3-Schlüssel herunter, da sie nach dem Schließen des Fensters nicht mehr abgerufen werden können.

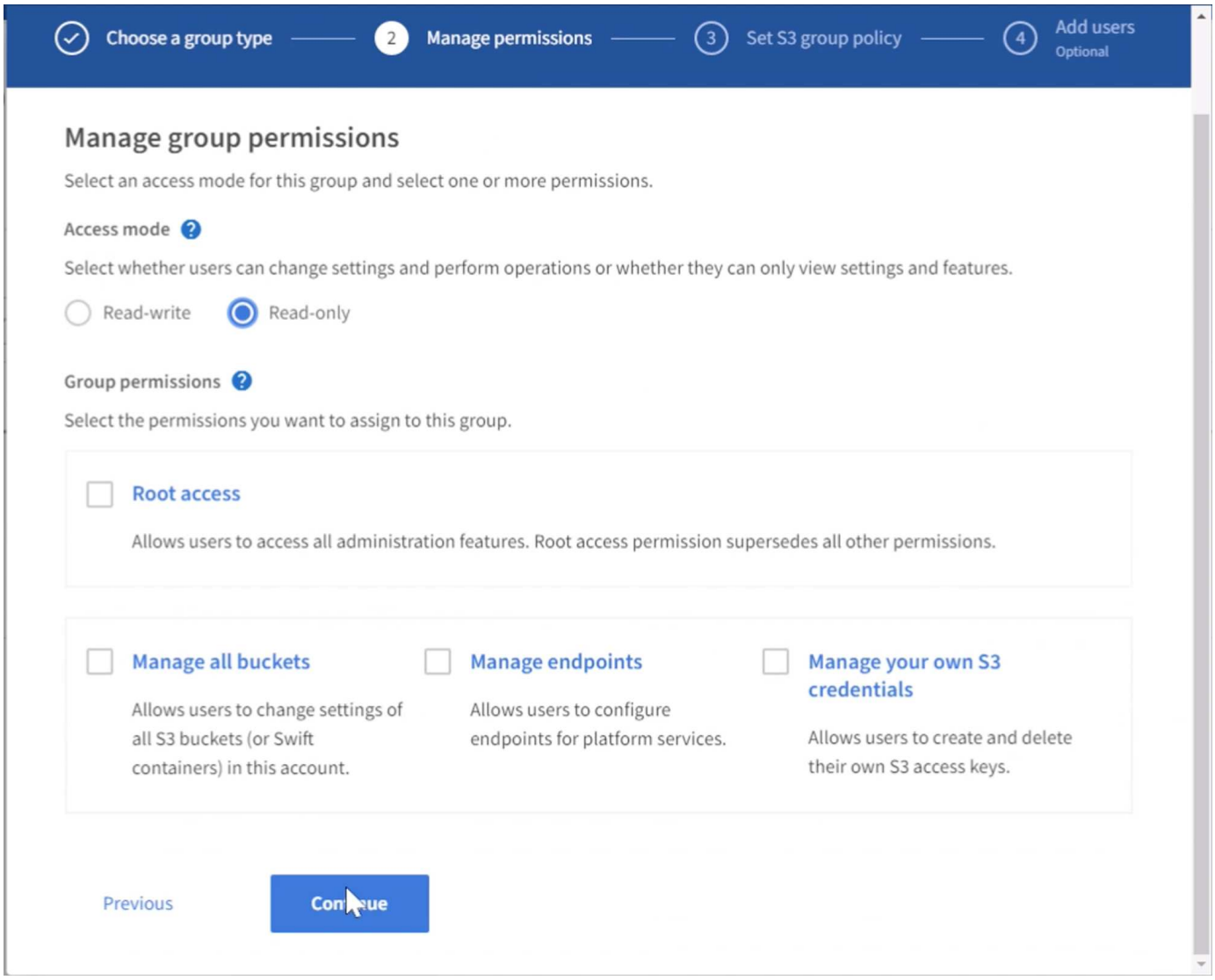


Erstellen Sie die Sicherheitsgruppe

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

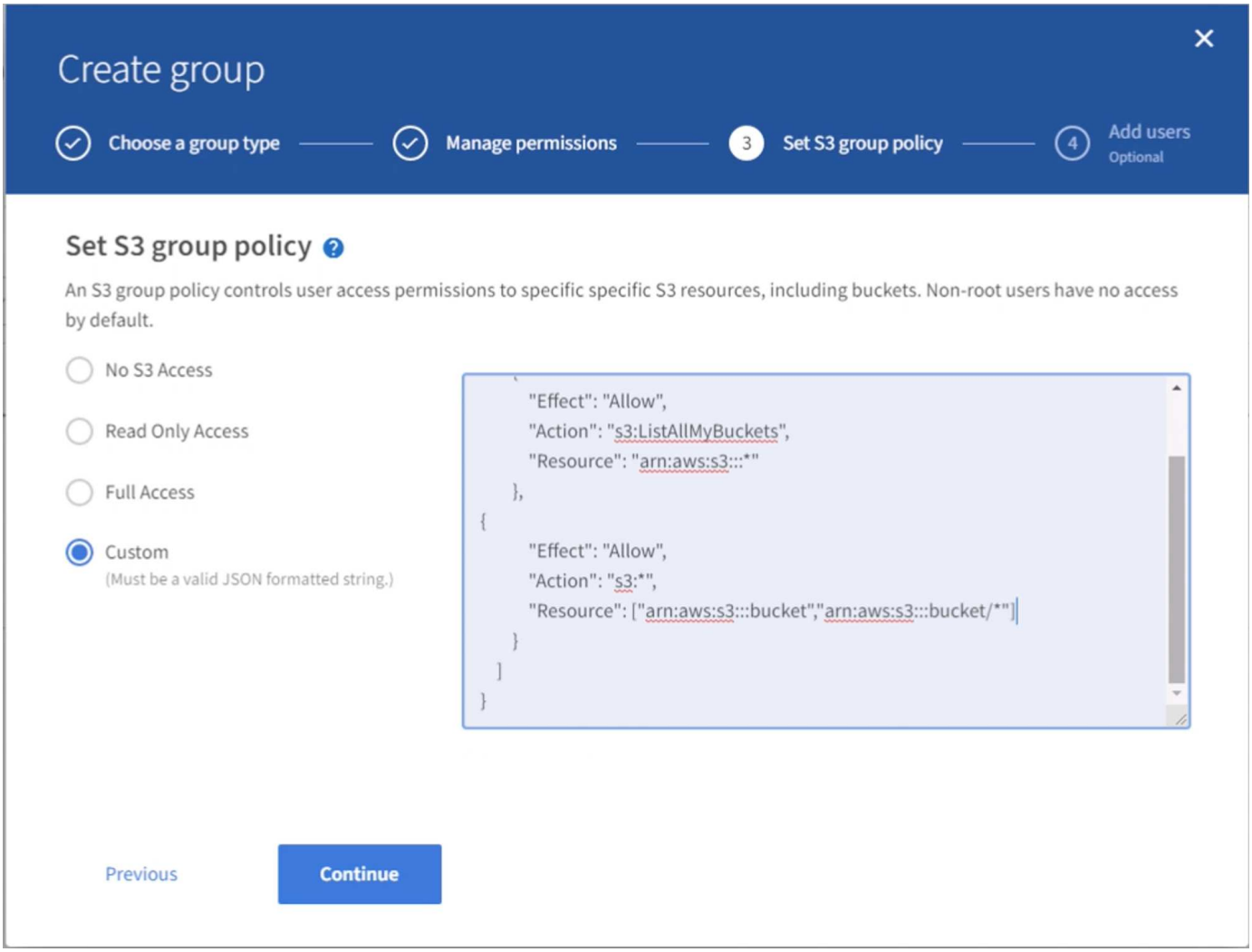


Legen Sie die Gruppenberechtigungen auf schreibgeschützt fest. Dies sind die Berechtigungen der Mandanten-UI, nicht die S3-Berechtigungen.

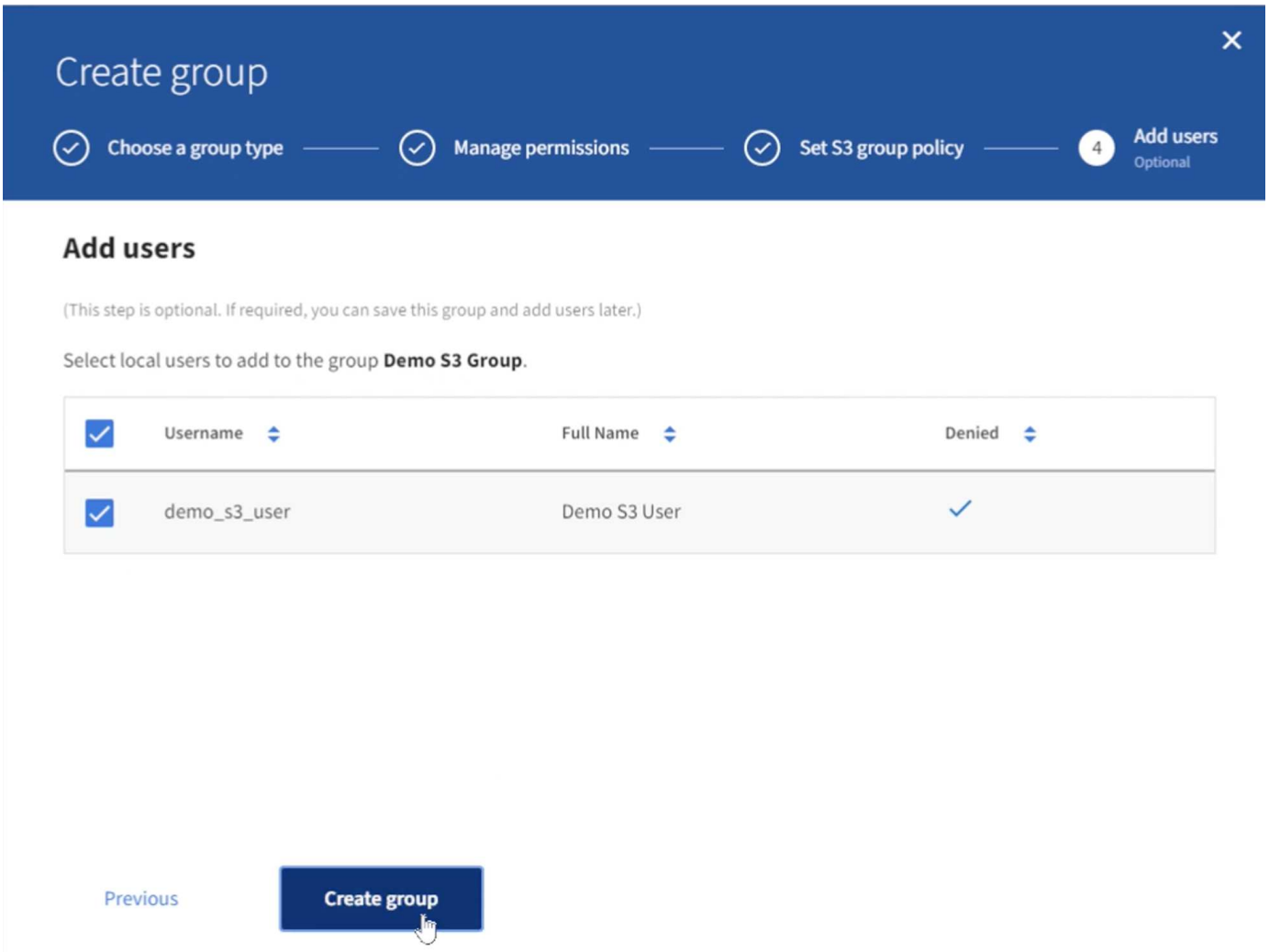


S3 Berechtigungen werden über die Gruppenrichtlinie (IAM-Richtlinie) gesteuert. Legen Sie die Gruppenrichtlinie auf Benutzerdefiniert fest, und fügen Sie die json-Richtlinie in das Feld ein. Diese Richtlinie ermöglicht Benutzern dieser Gruppe, die Buckets des Mandanten aufzulisten und alle S3-Vorgänge 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/*"]
      }
    ]
}
```

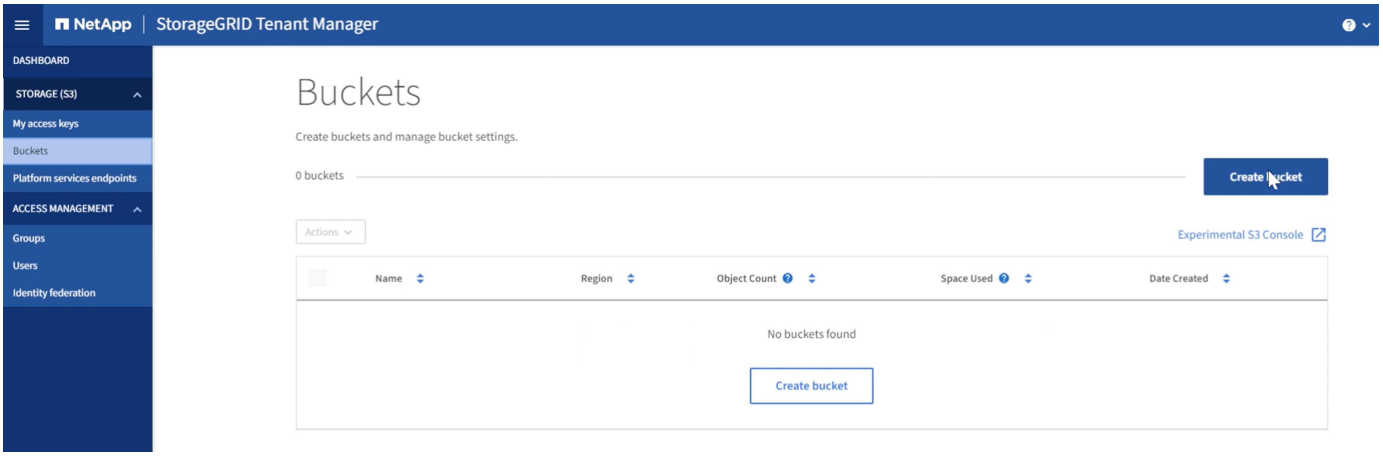


Fügen Sie schließlich den Benutzer zur Gruppe hinzu, und beenden Sie den Vorgang.

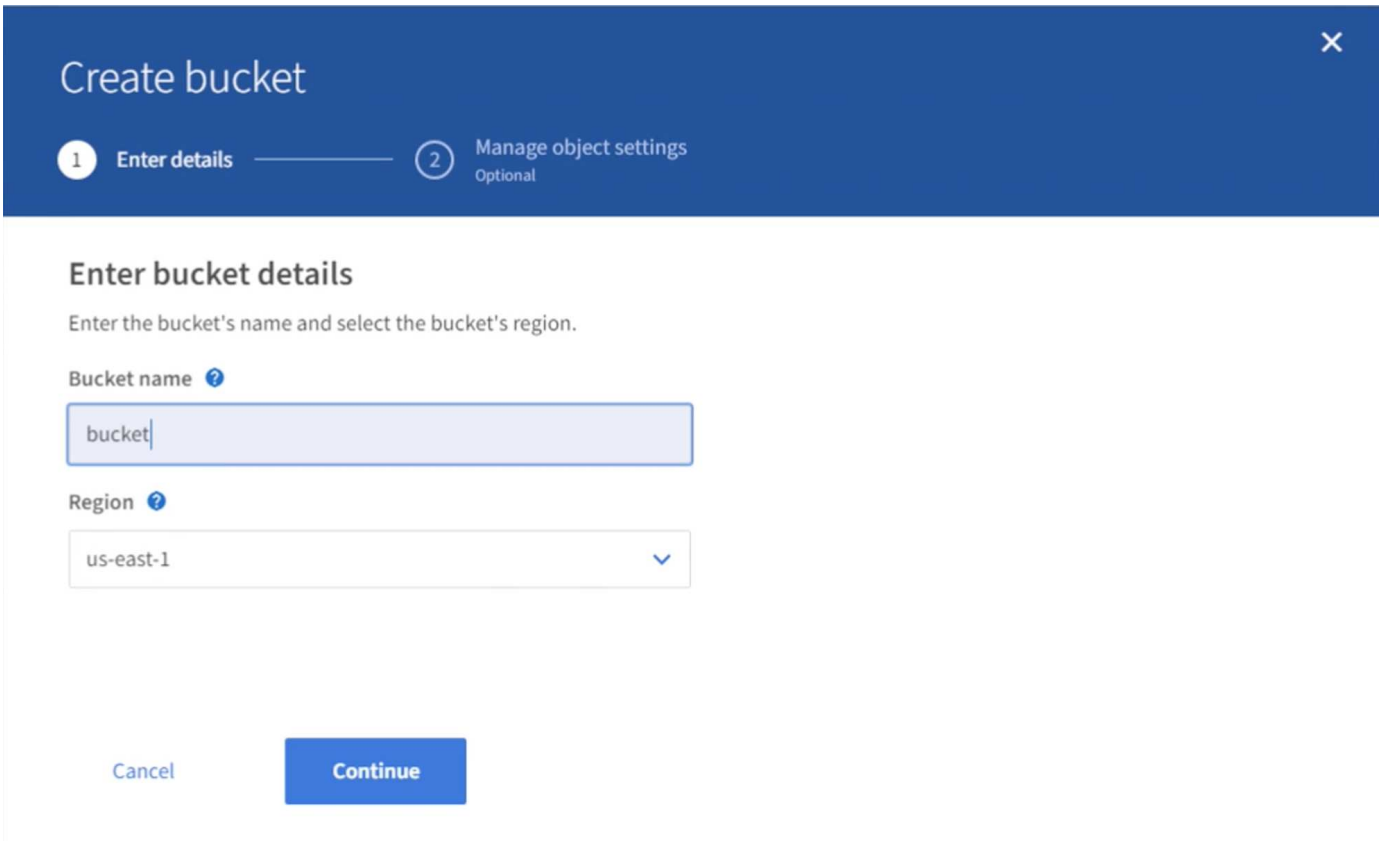


Erstellen Sie zwei Buckets

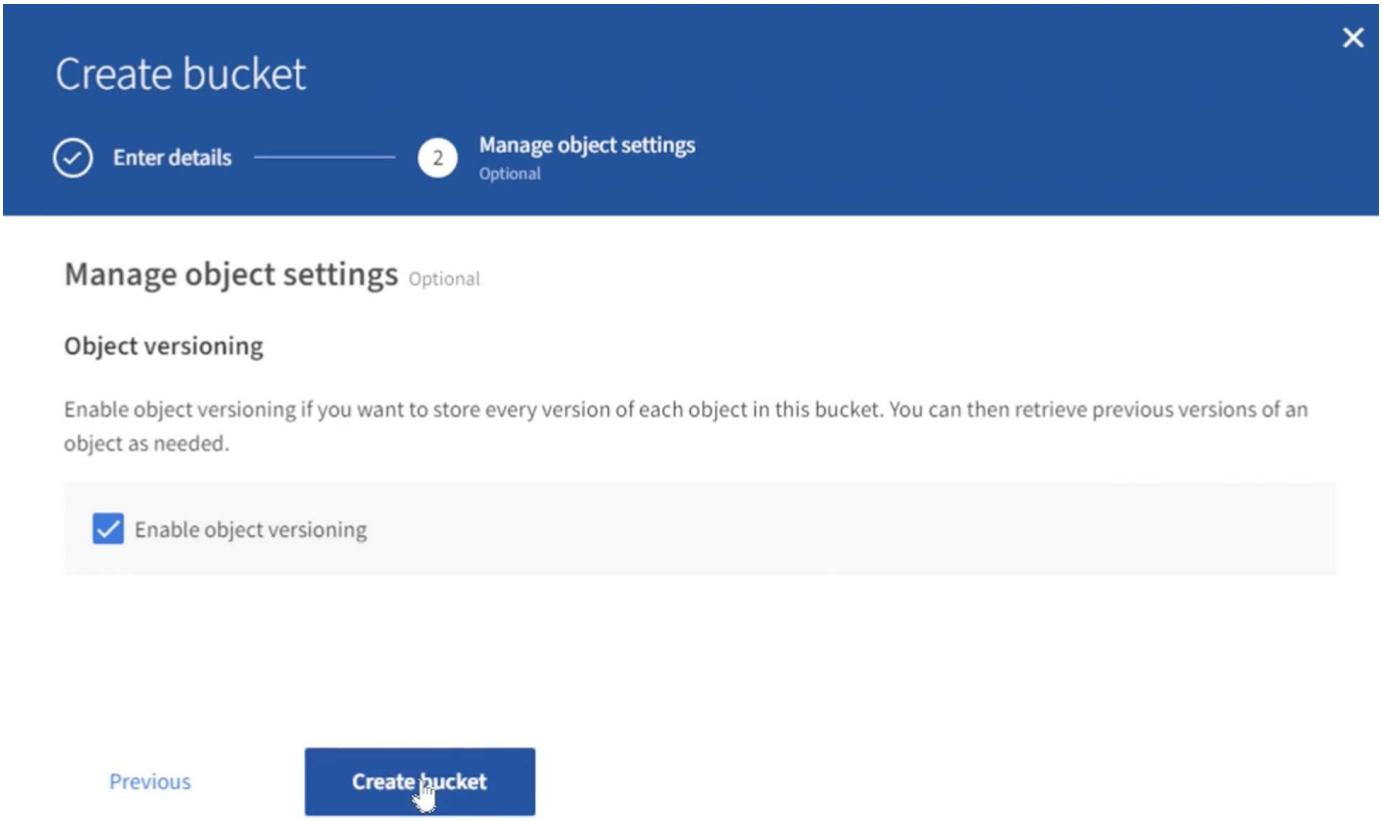
Navigieren Sie zur Registerkarte „Buckets“, und klicken Sie auf die Schaltfläche „Bucket erstellen“.



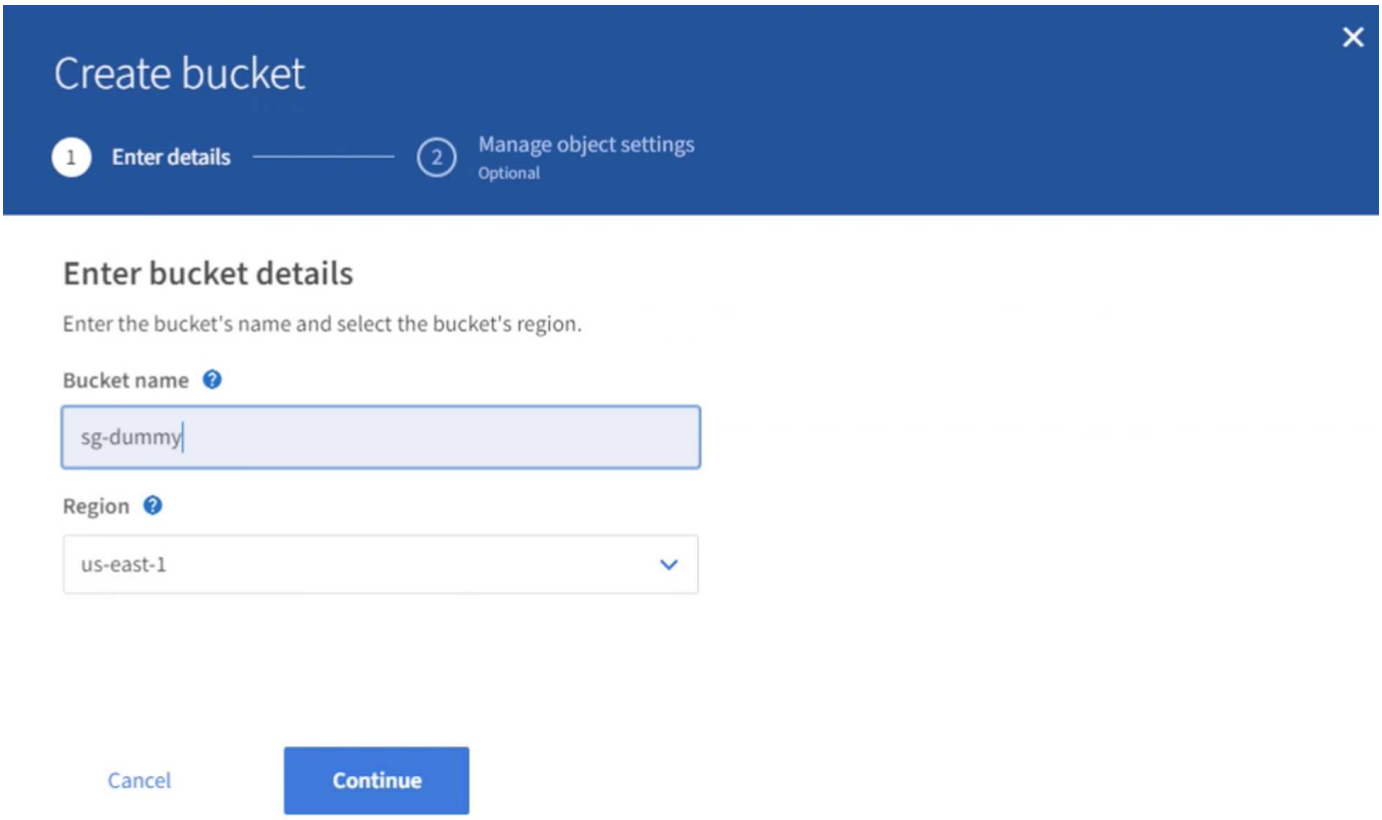
Definieren Sie den Bucket-Namen und die Region.



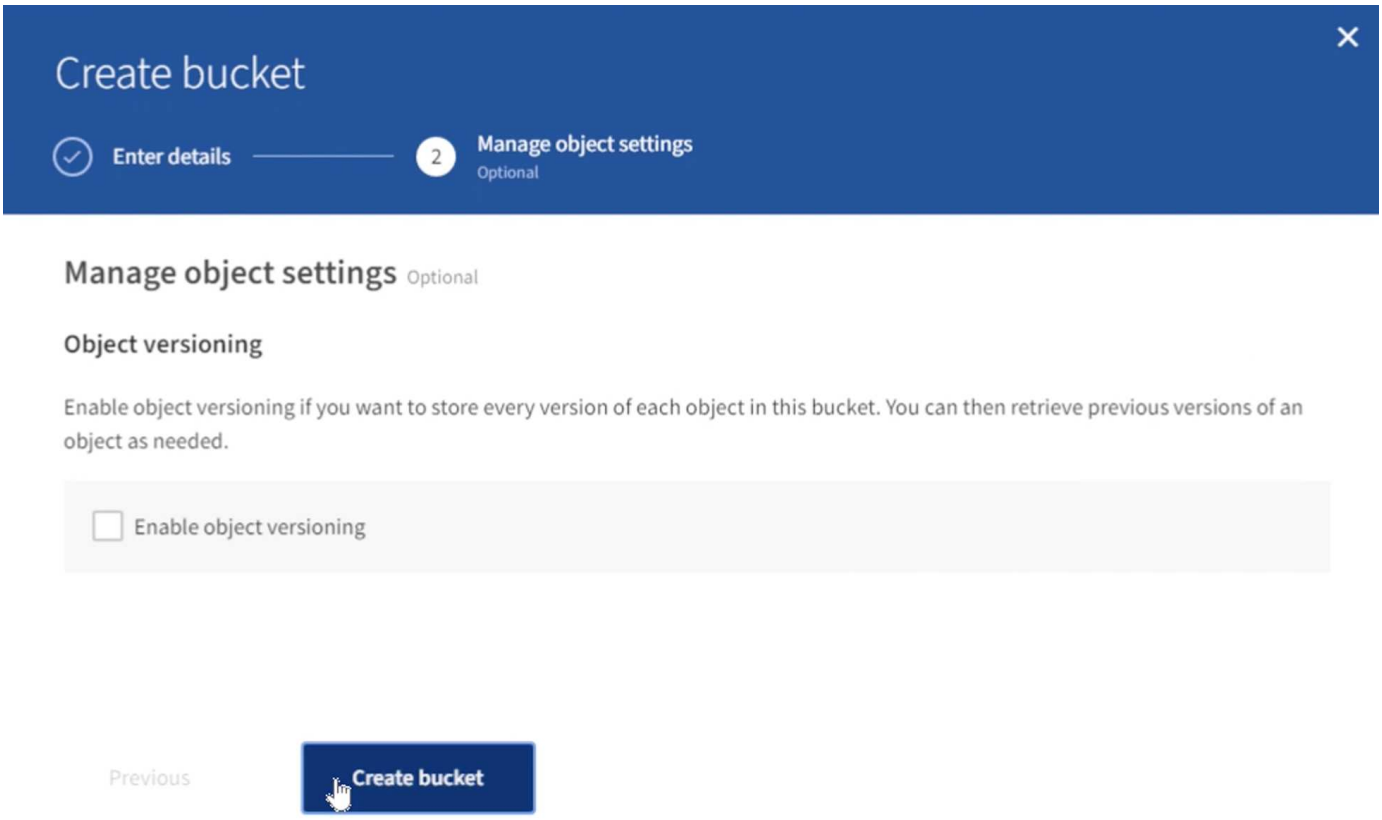
Aktivieren Sie in diesem ersten Bucket die Versionierung.



Erstellen Sie nun einen zweiten Bucket ohne aktivierte Versionierung.



Aktivieren Sie die Versionierung für diesen zweiten Bucket nicht.



Von Rafael Guedes und Aron Klein

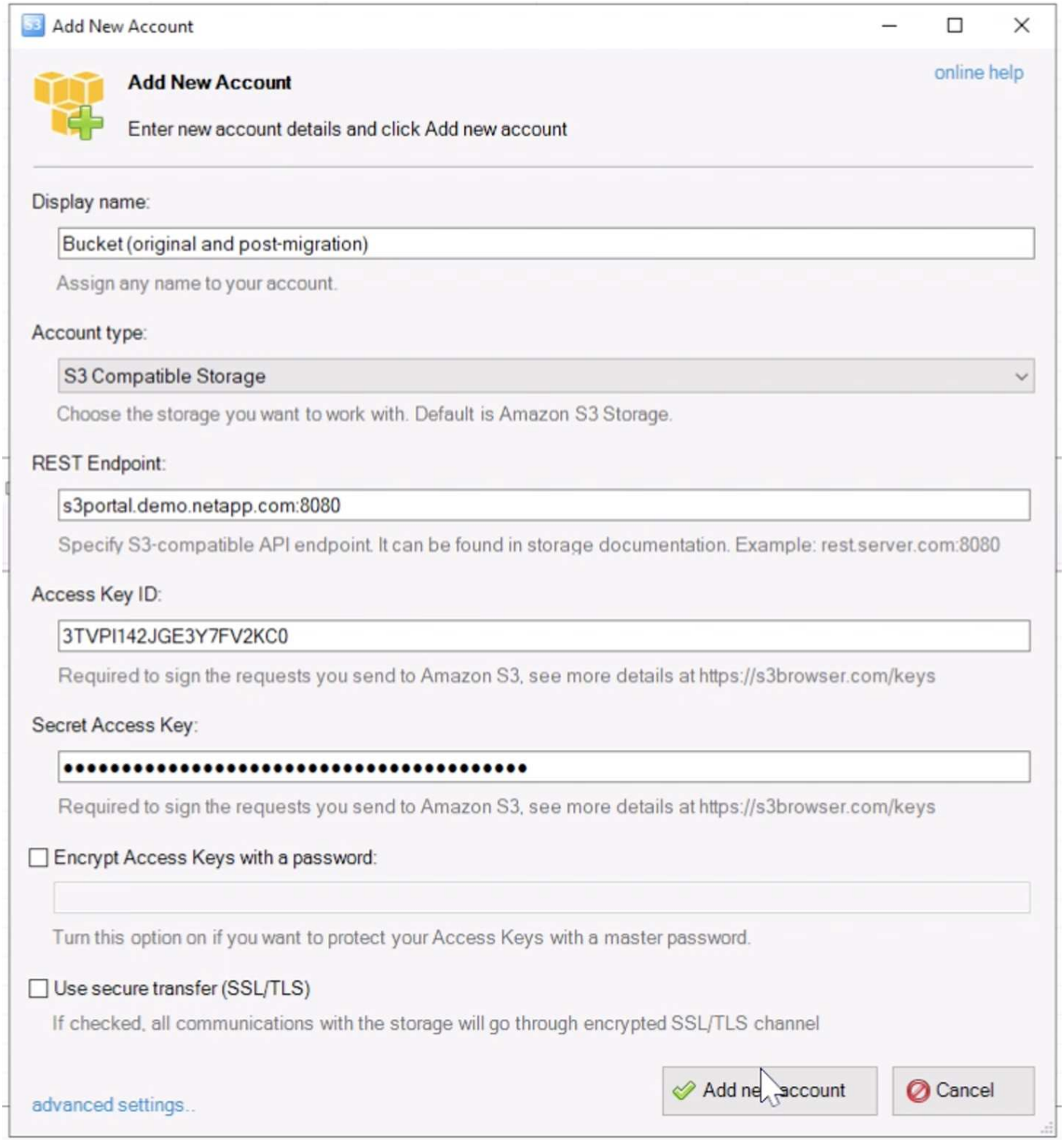
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

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

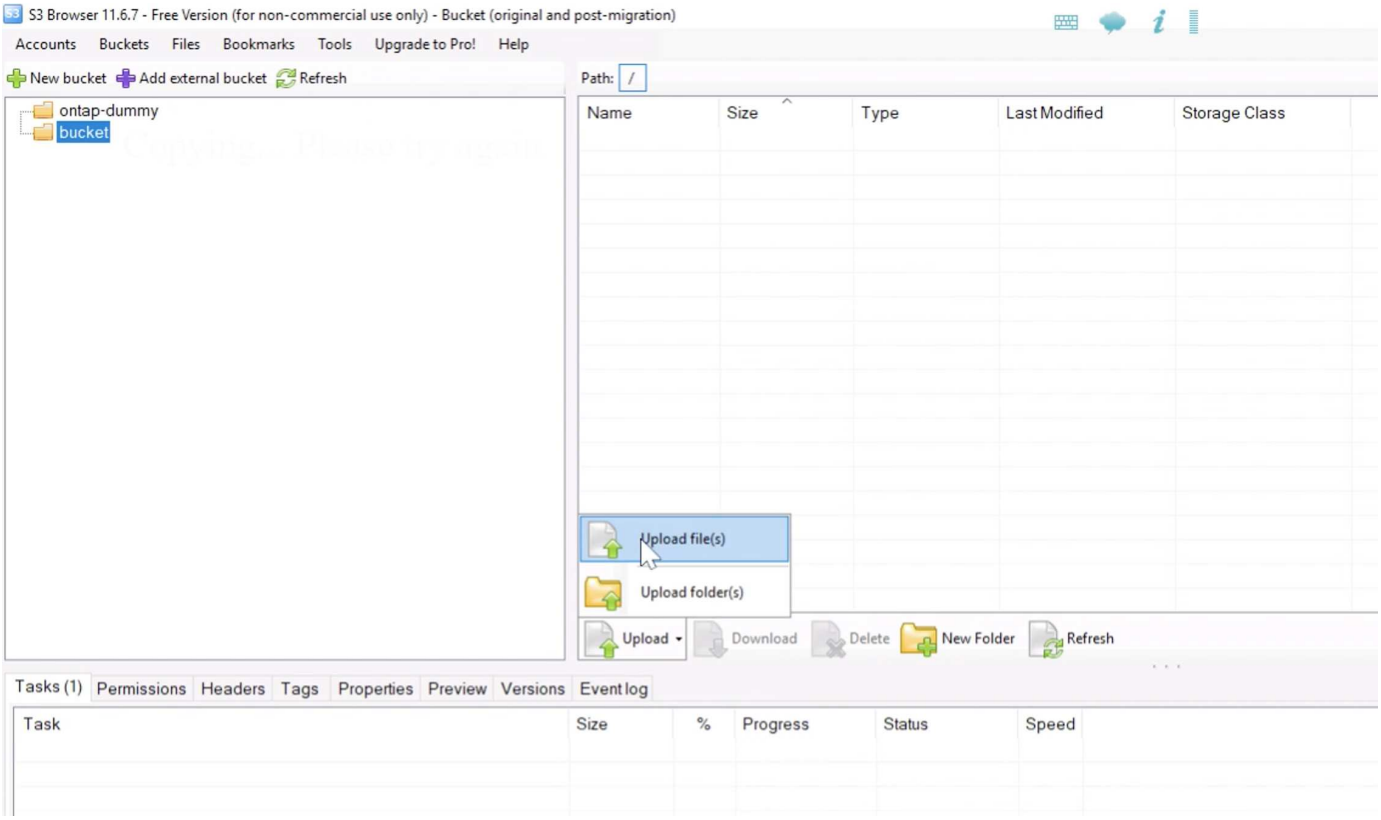
Füllen Sie den Quelleimer aus

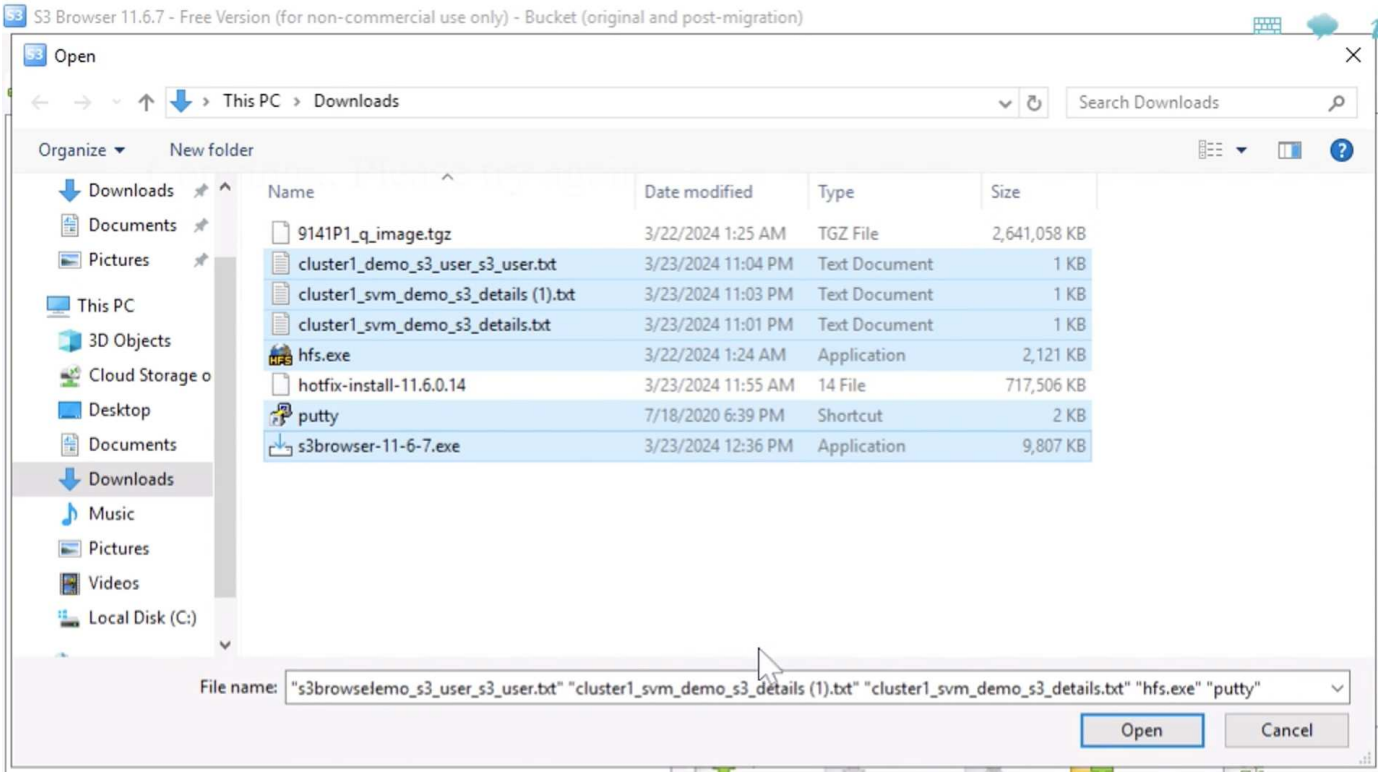
Lassen Sie uns einige Objekte in den Quell-ONTAP-Bucket legen. Wir verwenden S3Browser für diese Demo, aber Sie können jedes Tool verwenden, mit dem Sie vertraut sind.

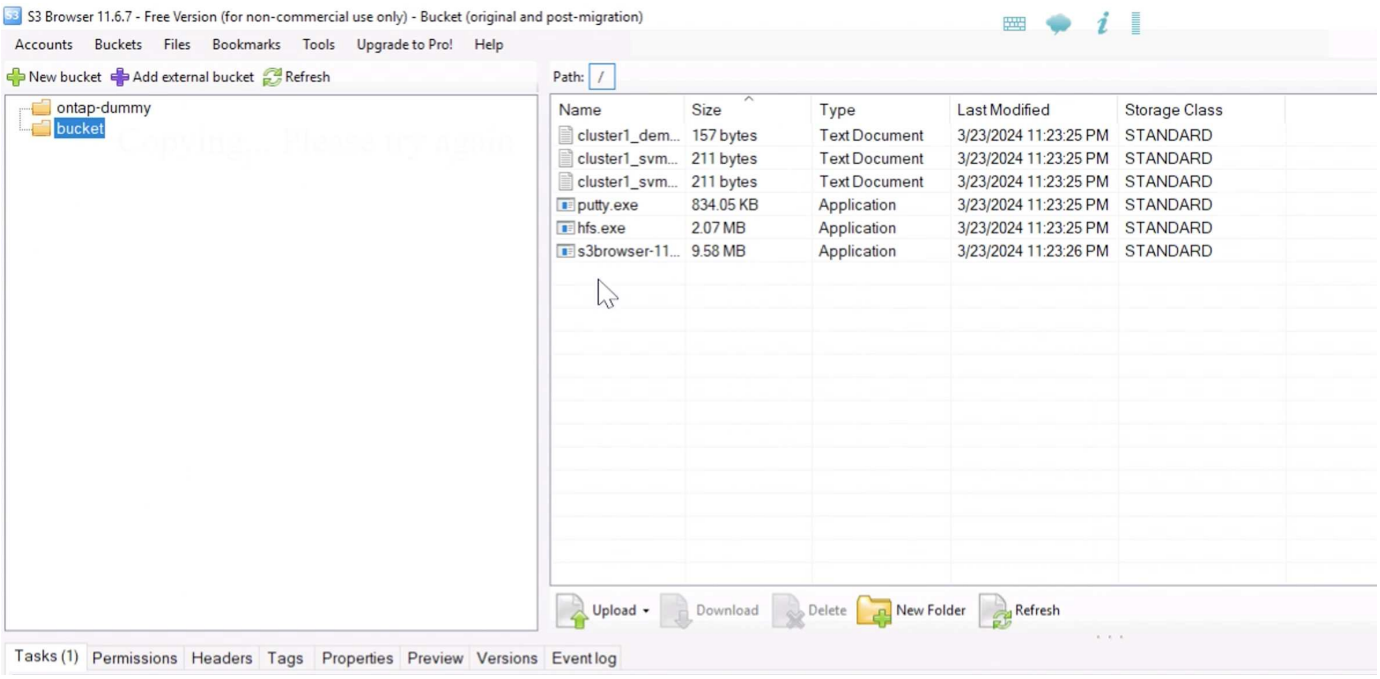
Konfigurieren Sie S3Browser mithilfe der oben erstellten ONTAP-Benutzer-s3-Schlüssel, um eine Verbindung zu Ihrem ONTAP-System herzustellen.



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

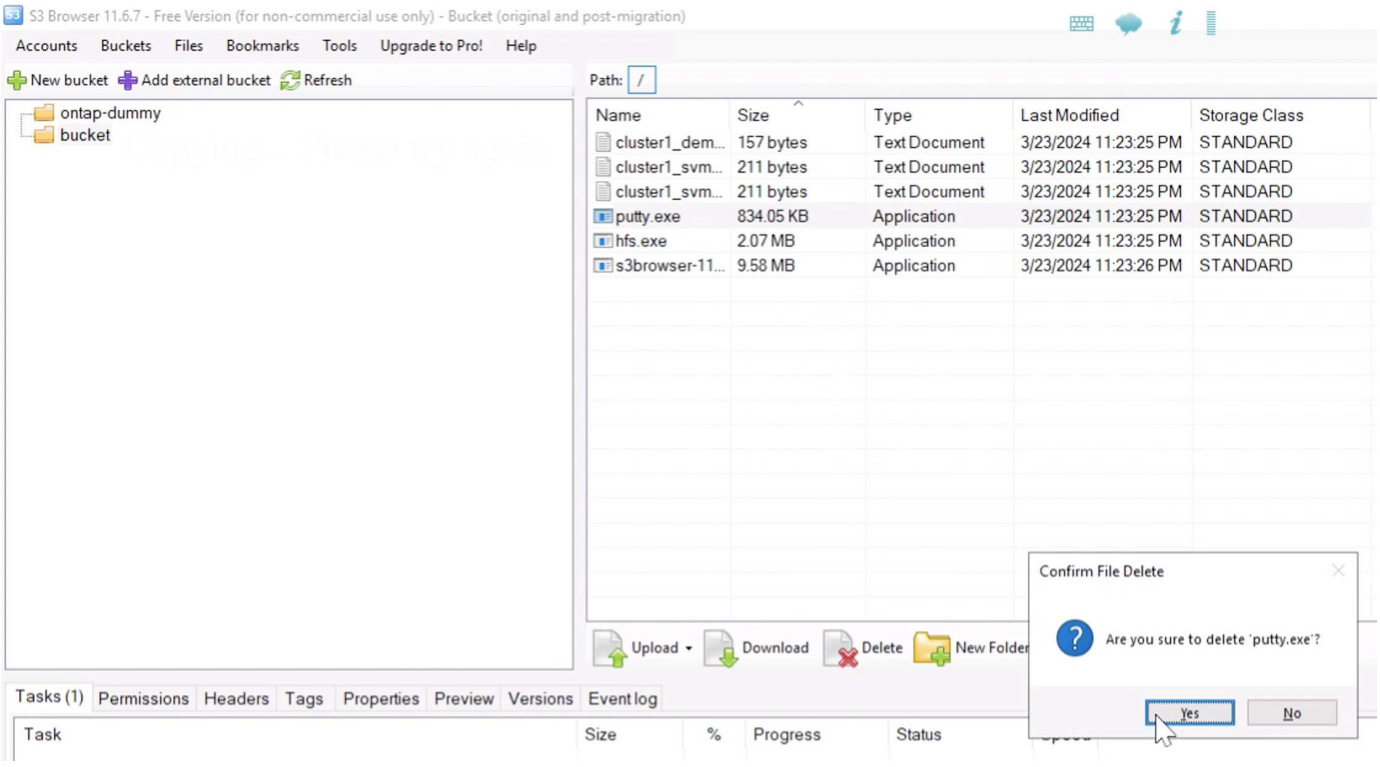

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)
Upload
Download
Delete
New Folder
Refresh
Tasks (1)
Permissions
Headers
Tags
Properties
Preview
Versions
Event log
Task
Size
%
Progress
Status
Speed


S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Open
This PC
Downloads
Search Downloads
Organize
New folder
Downloads
Documents
Pictures
This PC
3D Objects
Cloud Storage o
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
9141P1_q_image.tgz
3/22/2024 1:25 AM
TGZ File
2,641,058 KB
cluster1_demo_s3_user_s3_user.txt
3/23/2024 11:04 PM
Text Document
1 KB
cluster1_svm_demo_s3_details (1).txt
3/23/2024 11:03 PM
Text Document
1 KB
cluster1_svm_demo_s3_details.txt
3/23/2024 11:01 PM
Text Document
1 KB
hfs.exe
3/22/2024 1:24 AM
Application
2,121 KB
hotfix-install-11.6.0.14
3/23/2024 11:55 AM
14 File
717,506 KB
putty
7/18/2020 6:39 PM
Shortcut
2 KB
s3browser-11-6-7.exe
3/23/2024 12:36 PM
Application
9,807 KB
File name:
"s3browselemo_s3_user_s3_user.txt" "cluster1_svm_demo_s3_details (1).txt" "cluster1_svm_demo_s3_details.txt" "hfs.exe" "putty"
Open
Cancel

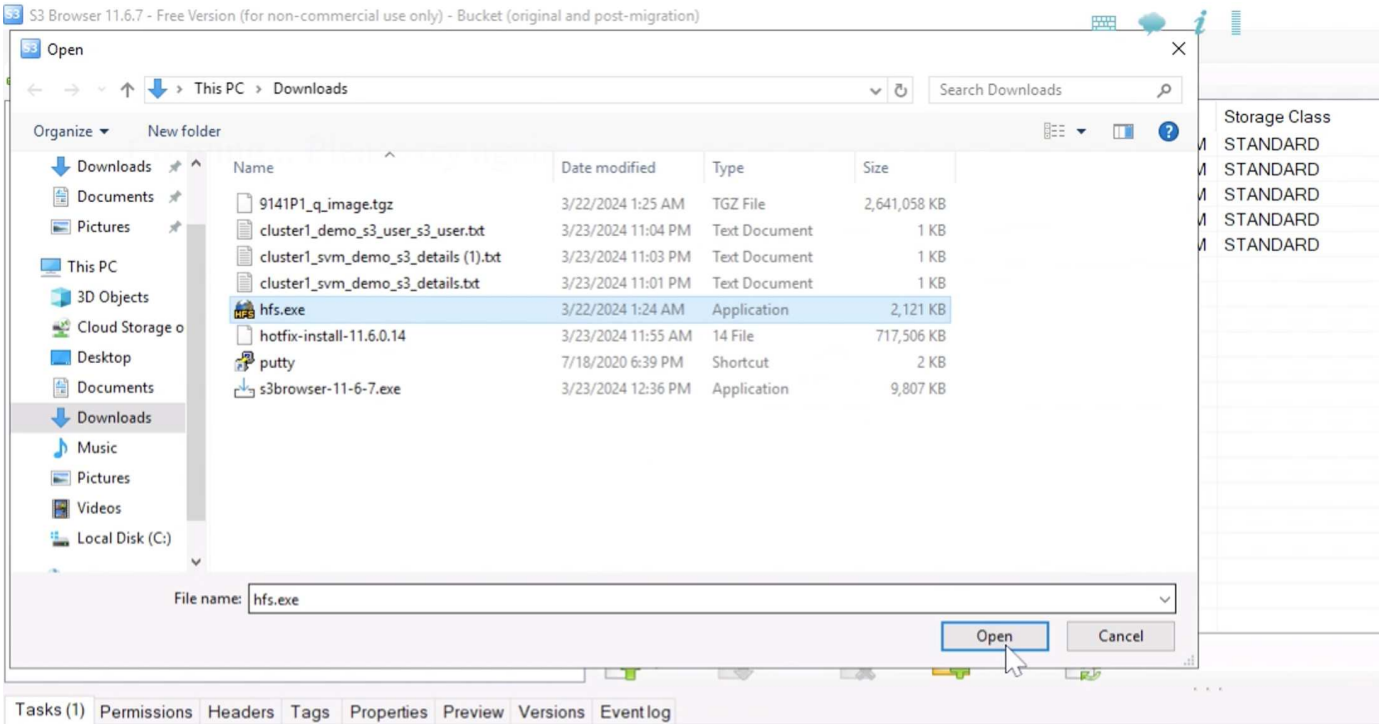


Lassen Sie uns nun einige Objektversionen im Bucket erstellen.

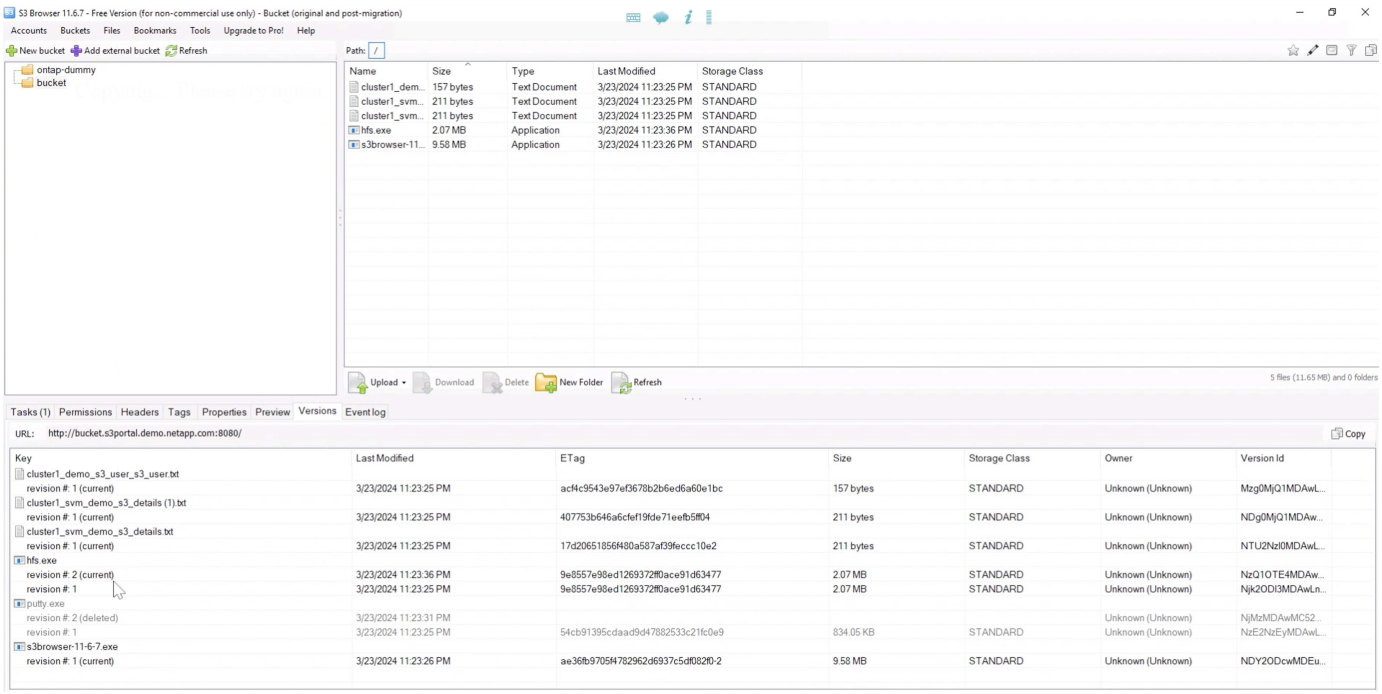
Eine Datei löschen.



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.



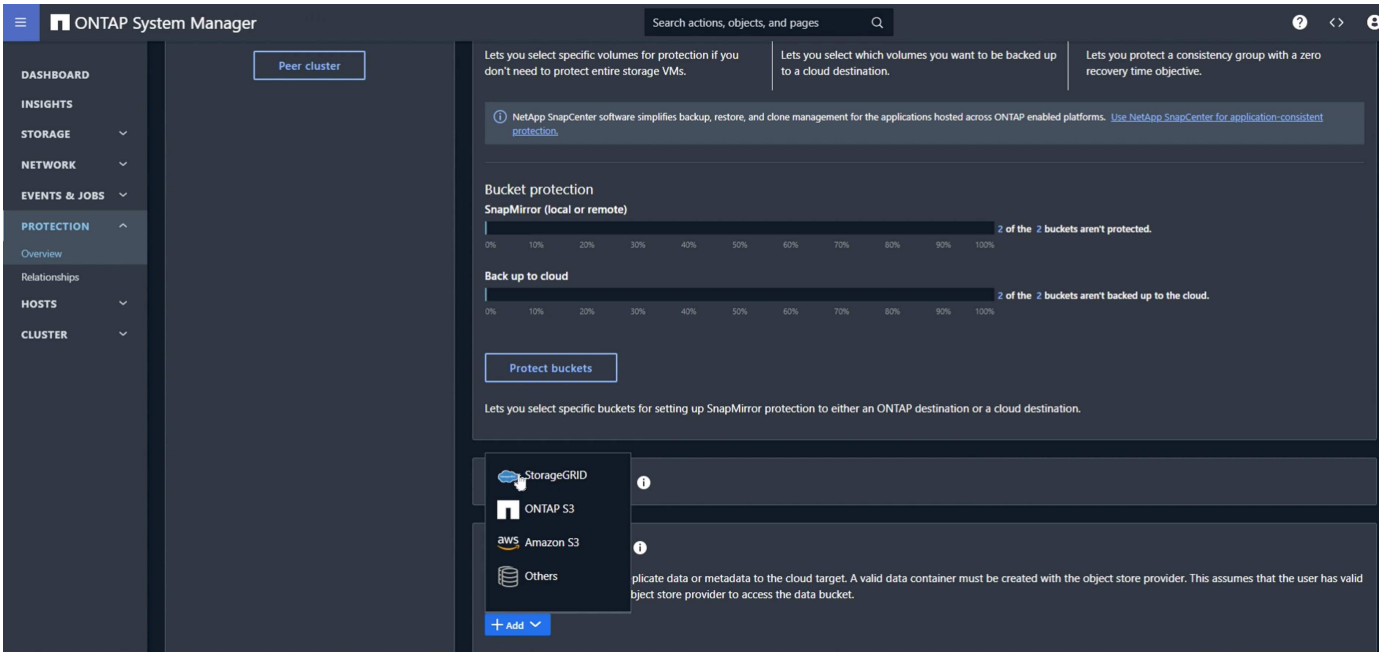
In S3Browser können wir die Versionen der Objekte anzeigen, die wir gerade erstellt haben.



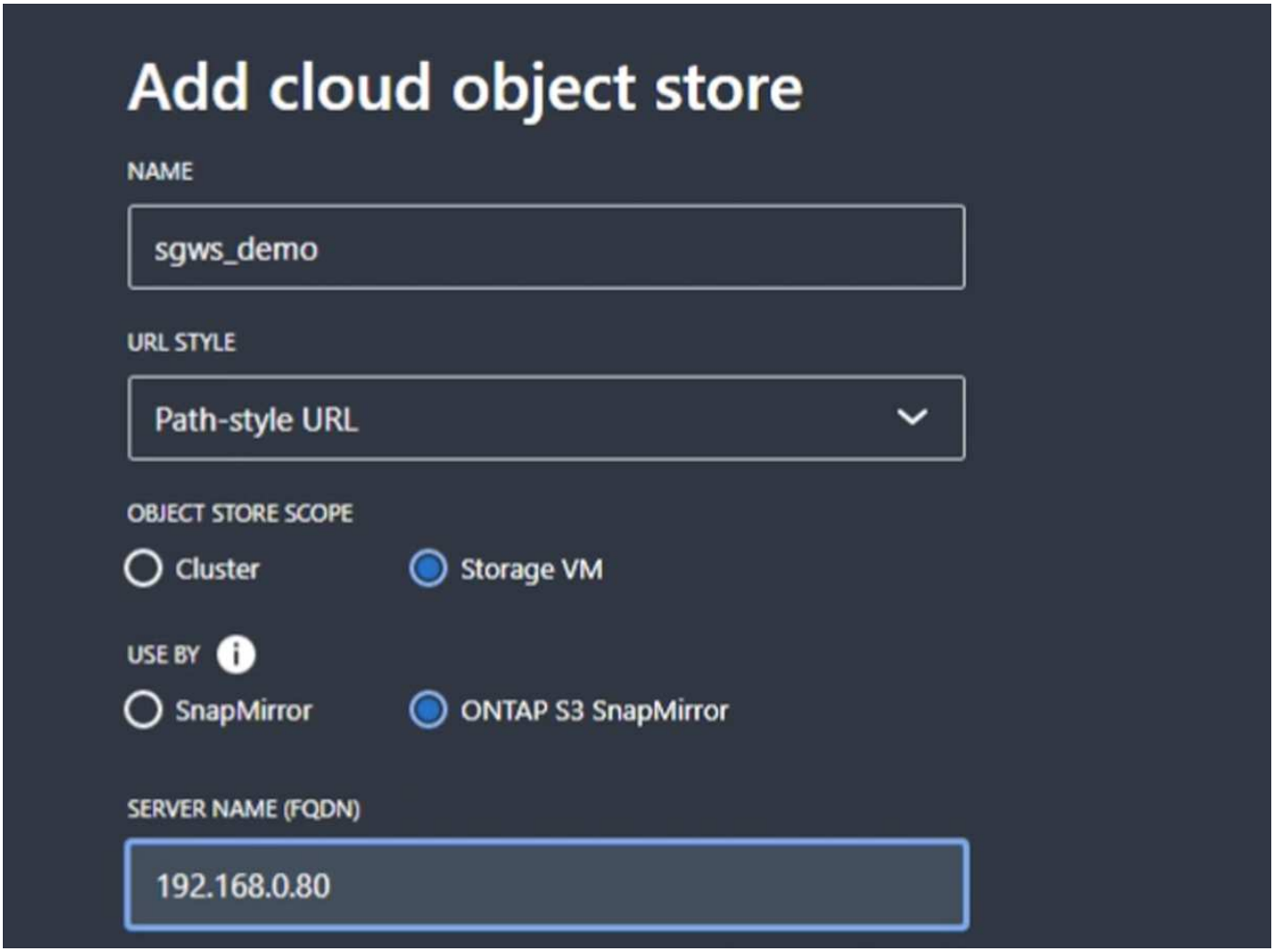
Festlegen der Replikationsbeziehung

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".



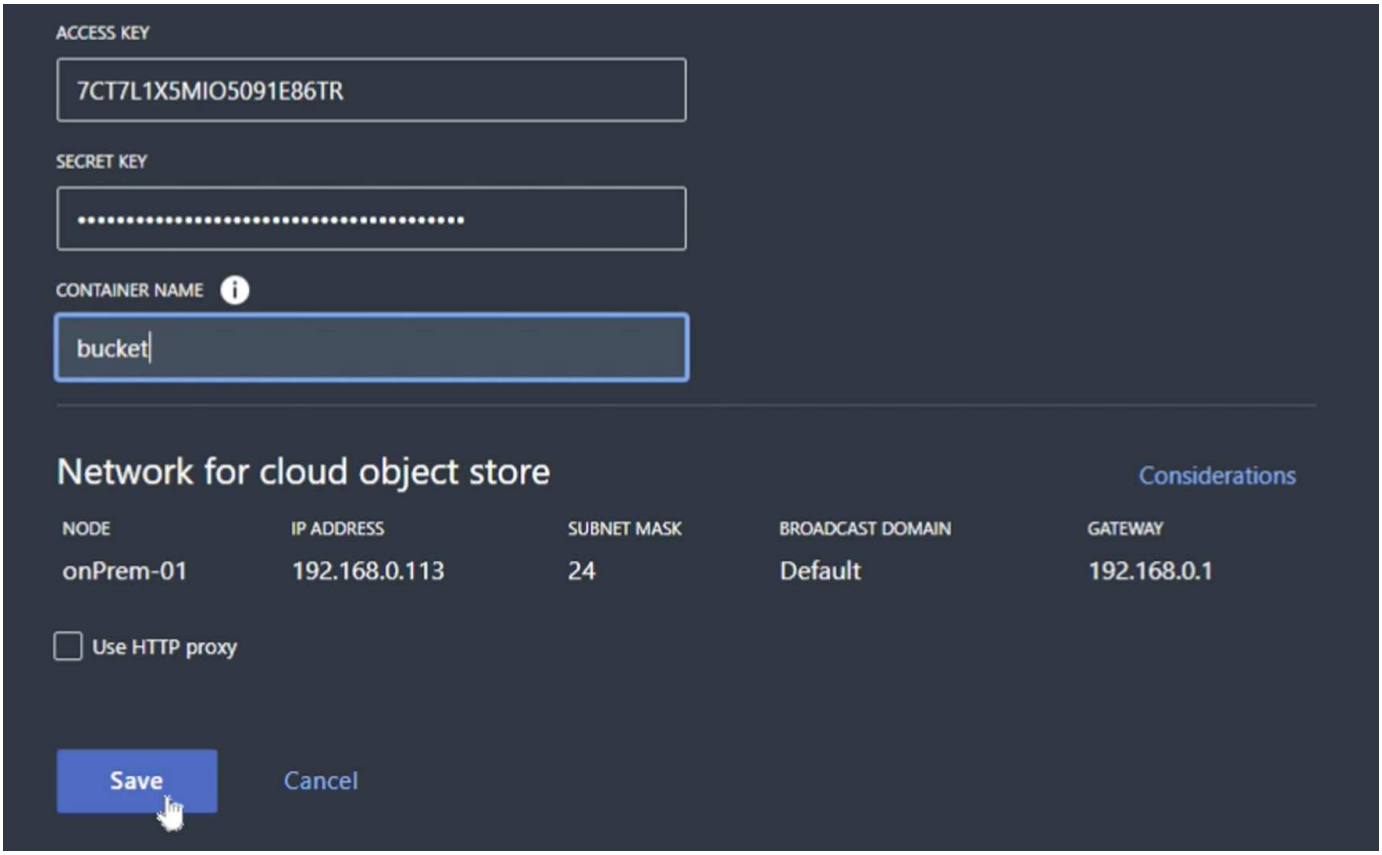
Geben Sie die StorageGRID-Informationen ein, indem Sie einen Namen, URL-Stil (für diese Demo verwenden wir Pfad-styl URLs). Setzen Sie den Umfang des Objektspeichers auf „Storage VM“.



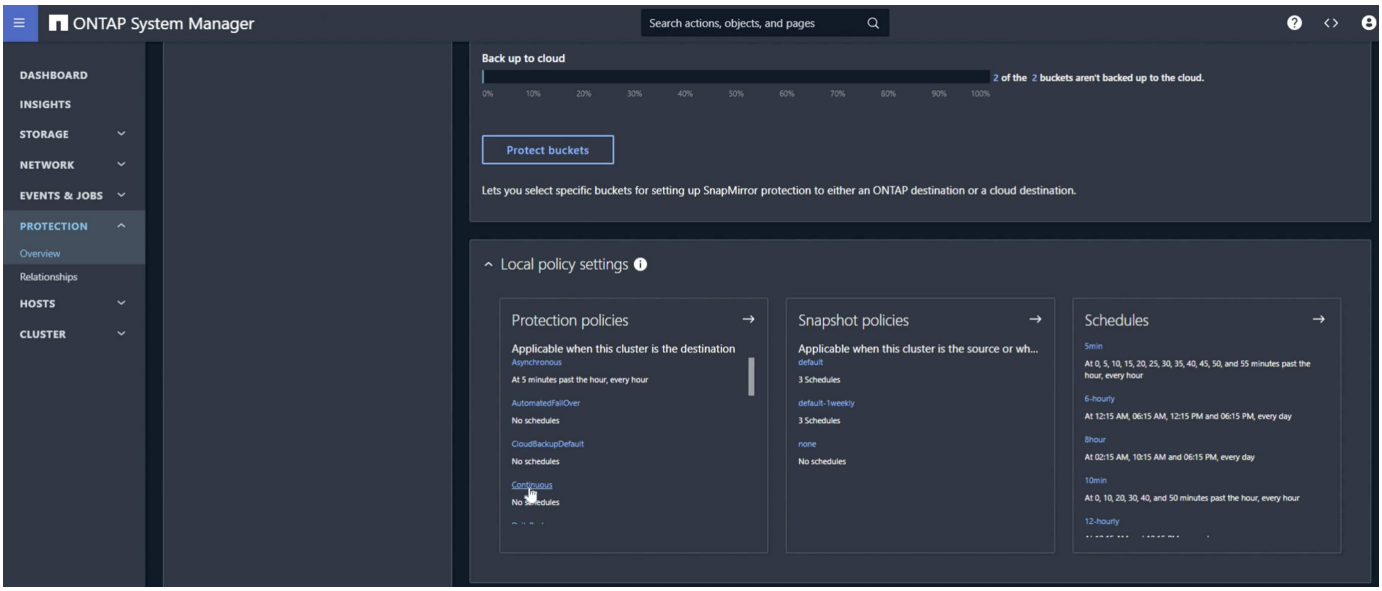
Wenn Sie SSL verwenden, legen Sie hier den Load Balancer-Endpunkt-Port fest und kopieren Sie das

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

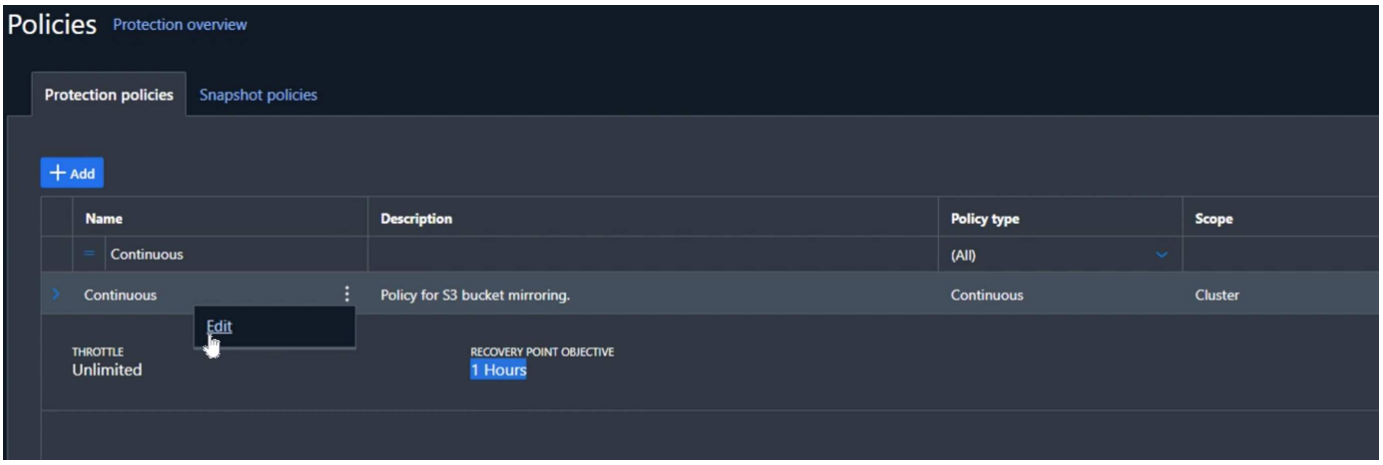
Geben Sie die S3-Benutzerschlüssel und den Bucket-Namen der StorageGRID aus der obigen StorageGRID-Konfiguration für das Ziel ein.



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



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

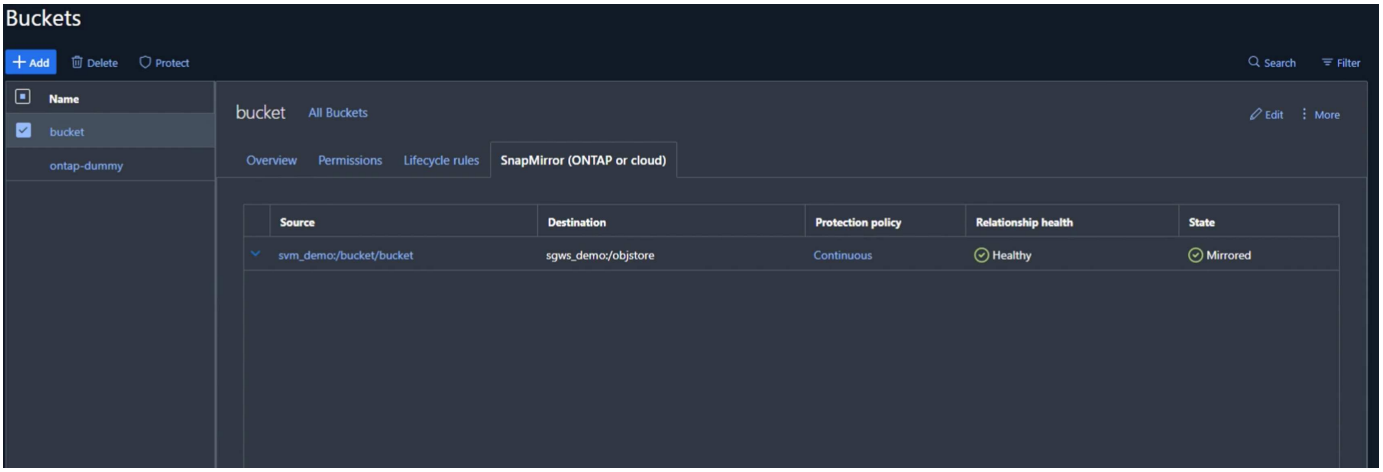


Jetzt können wir SnapMirror konfigurieren, um den Bucket zu replizieren.

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

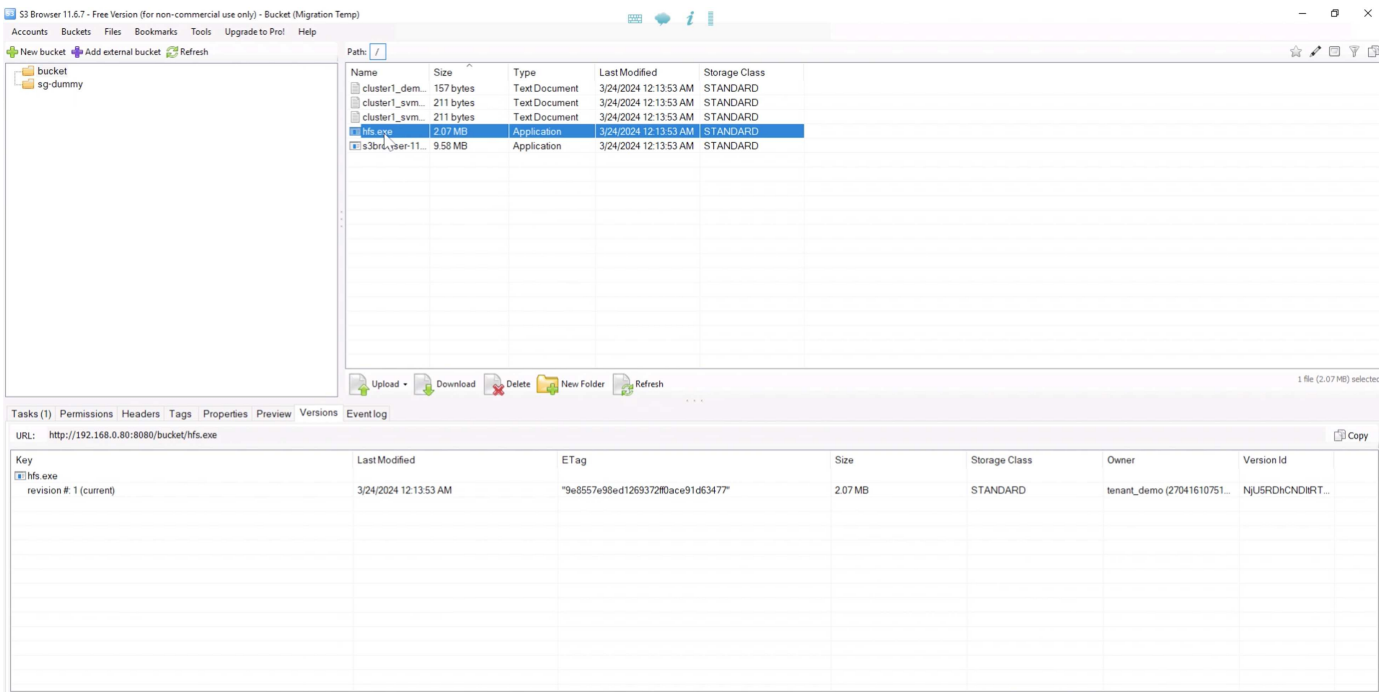
Der Bucket zeigt nun ein Wolkensymbol in der Bucket-Liste unter Schutz an.

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

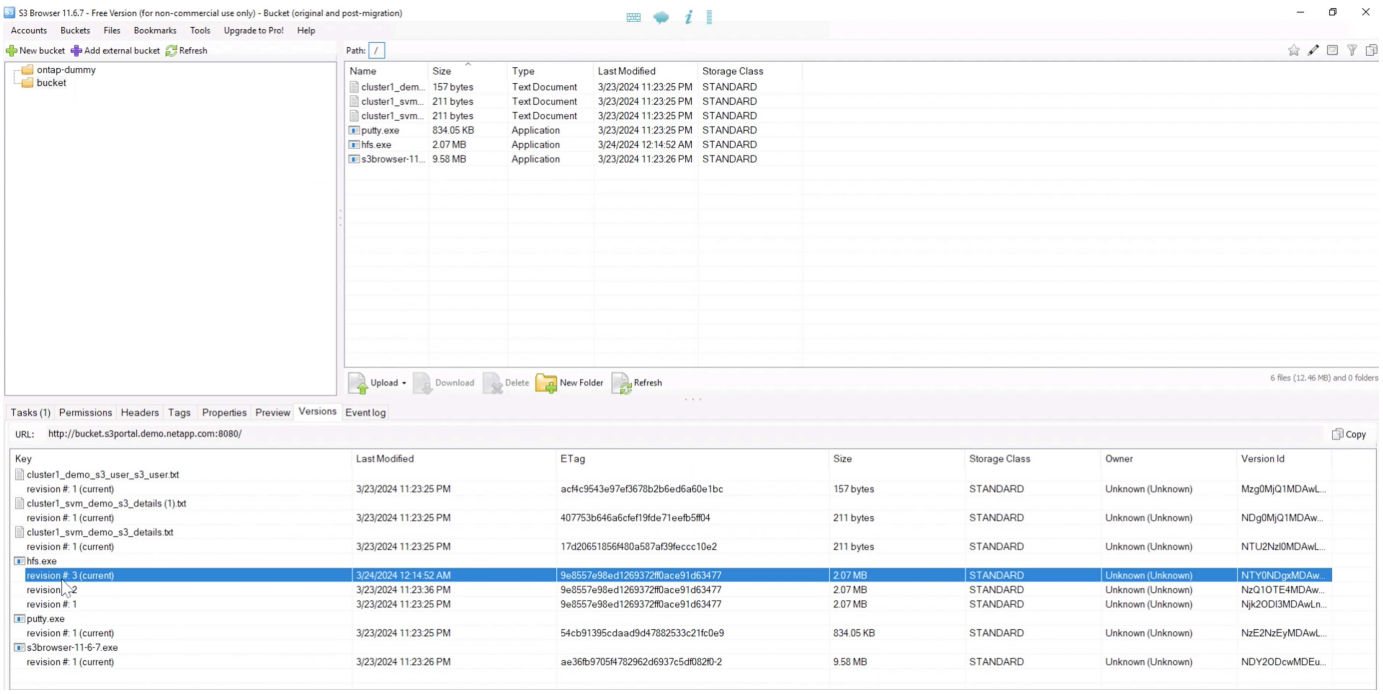


Details zur Replikation

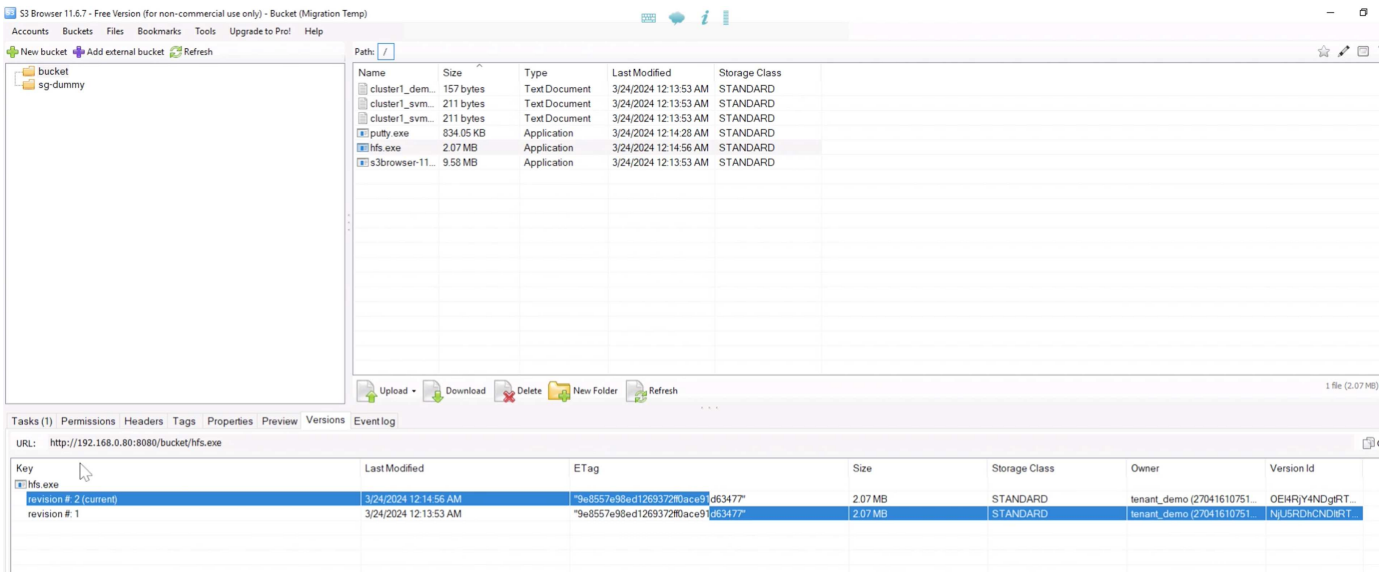
Wir verfügen jetzt über einen erfolgreich replizierenden Bucket von ONTAP zu StorageGRID. Aber was ist eigentlich Replikation? Unsere Quelle und unser Ziel sind beide versionierte Buckets. Replizieren die vorherigen Versionen auch an das Zielsystem? Wenn wir uns unseren StorageGRID-Bucket mit S3Browser ansehen, sehen wir, dass die bestehenden Versionen nicht repliziert wurden und unser gelöschtes 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.



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.



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

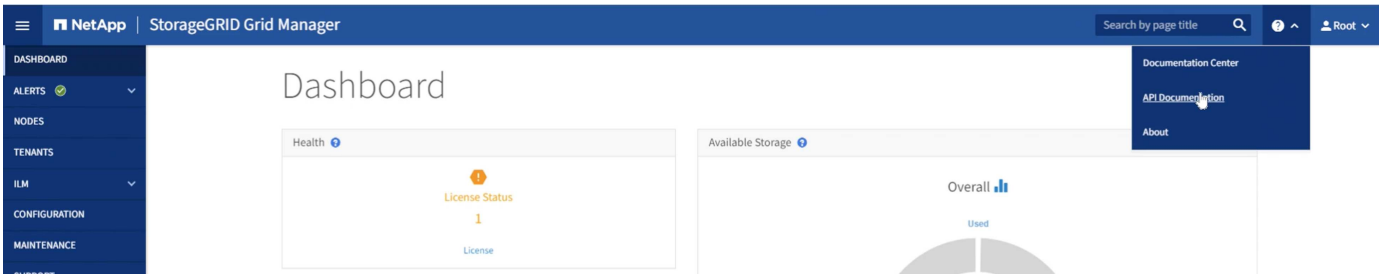
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

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

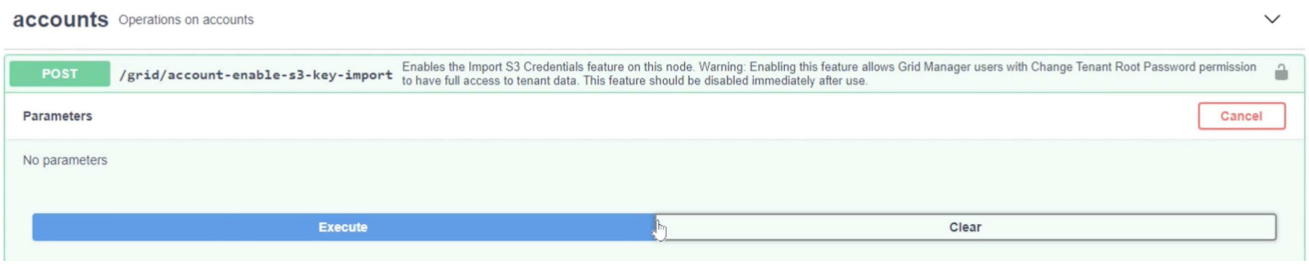
Migrieren Sie S3 Schlüssel

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.

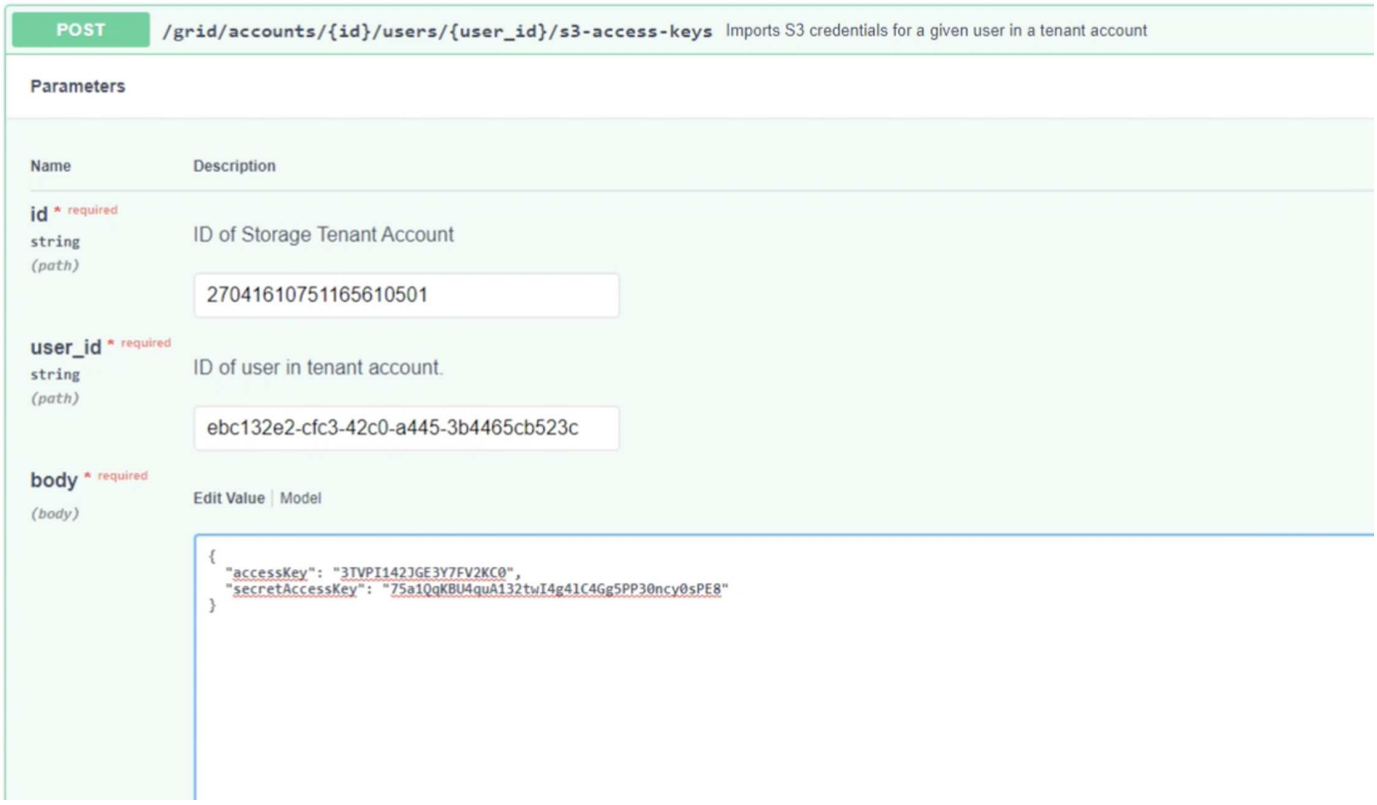


Erweitern Sie den Abschnitt "Accounts", wählen Sie "POST /Grid/Account-enable-s3-key-Import", klicken Sie auf "Try it out" und klicken Sie dann auf die Schaltfläche Ausführen.

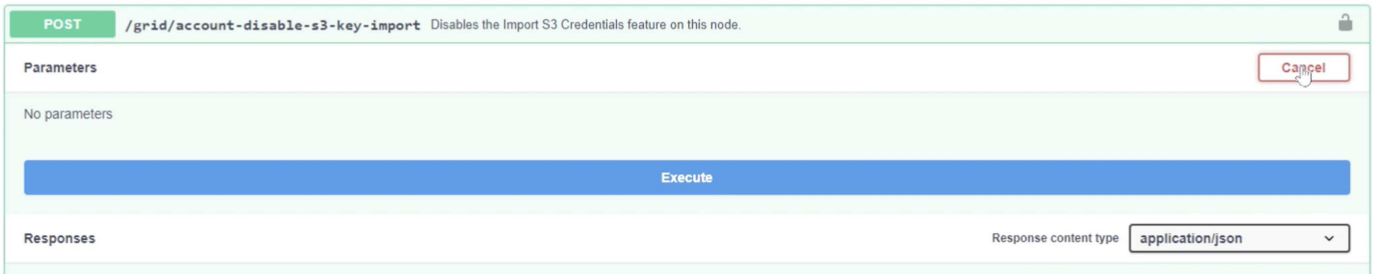


Scrollen Sie jetzt noch unter „Accounts" nach unten zu „POST /Grid/Accounts/{id}/users/{user_id}/s3-Access-keys"

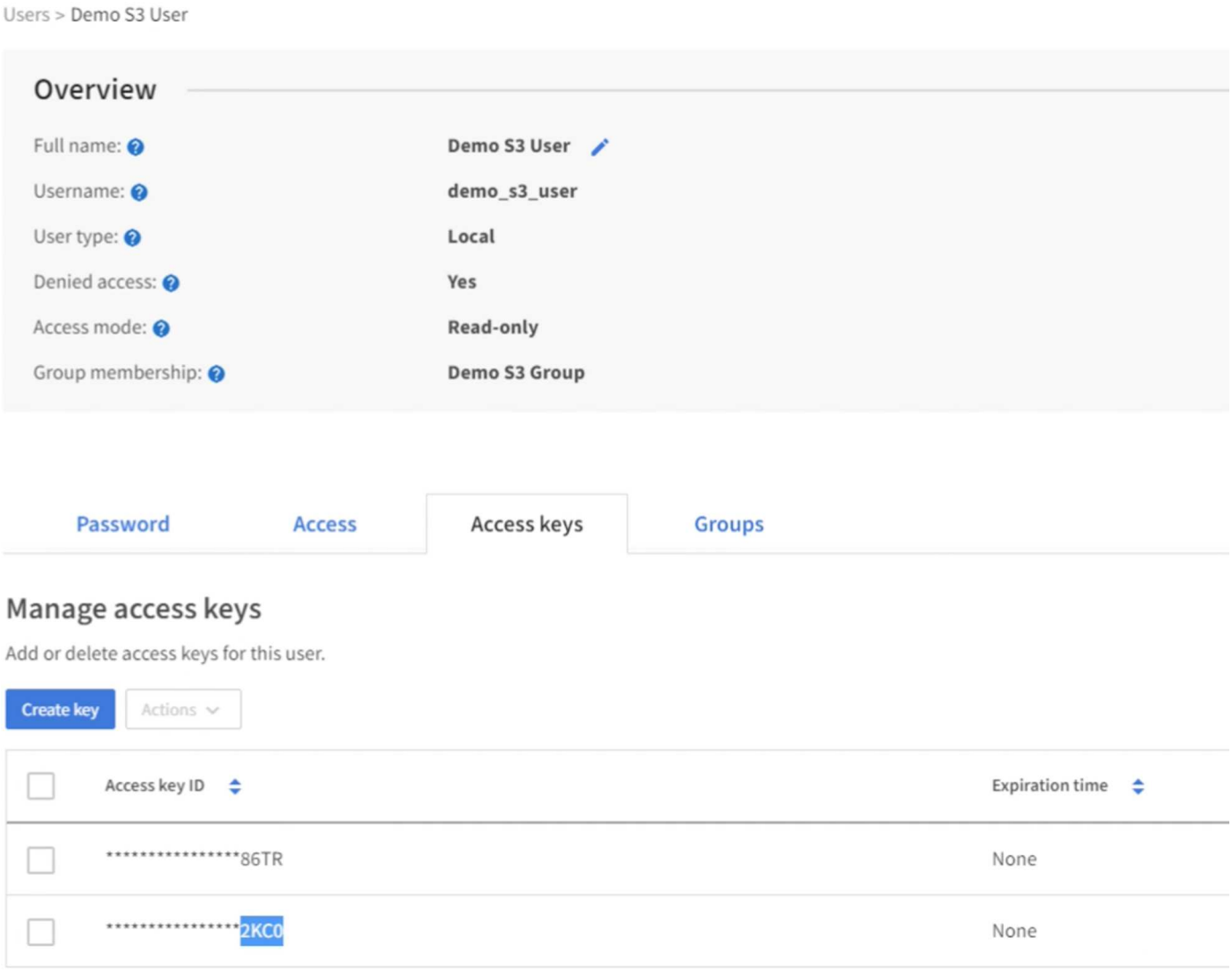
Hier werden wir die Mieter-ID und die Benutzer-Konto-ID eingeben, die wir zuvor gesammelt haben. Füllen Sie die Felder und die Schlüssel von unserem ONTAP-Benutzer in der json-Box. Sie können den Ablauf der Schlüssel einstellen, oder entfernen Sie die " , "läuft ab": 123456789" und klicken Sie auf Ausführen.



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



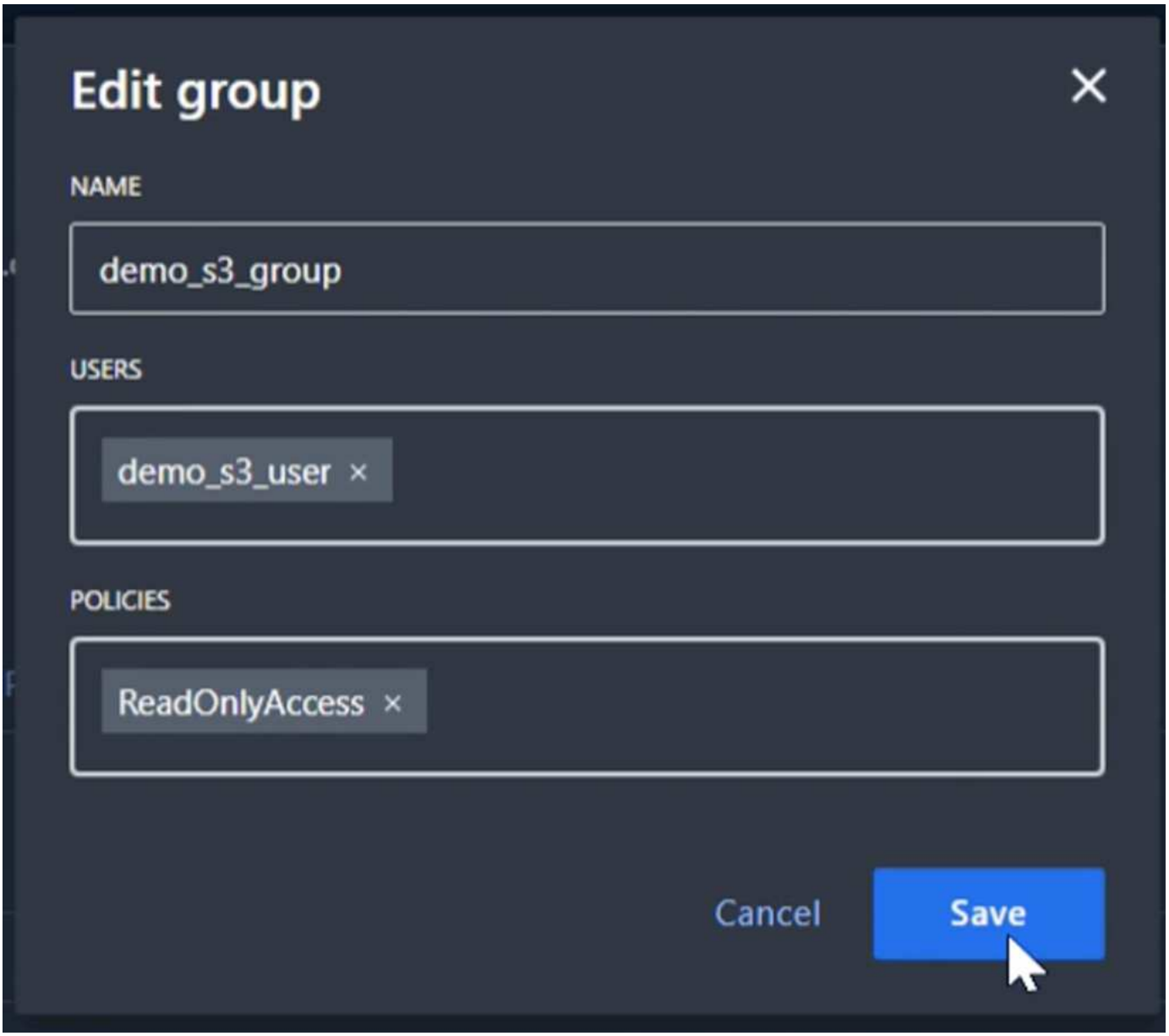
Wenn wir uns das Benutzerkonto in der Mandantenmanager-UI ansehen, sehen wir, dass der neue Schlüssel hinzugefügt wurde.



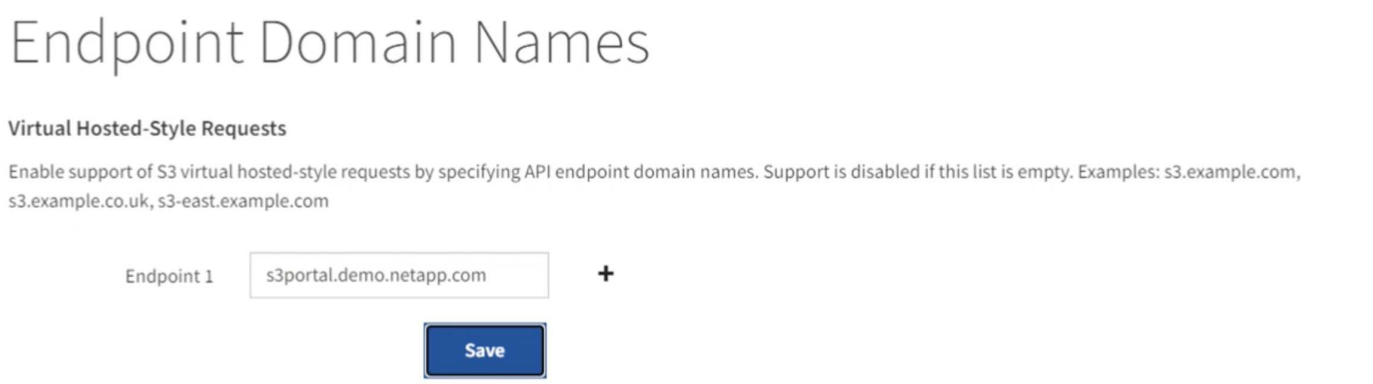
Der letzte Cut-Over

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.



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 Domänennamen des Endpunkts in StorageGRID hinzu, wenn Anforderungen nach virtuellem Hosted-Stil erforderlich sind



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

Tool- und Anwendungsleitfäden

Nutzen Sie Hadoop S3A-Connector von Cloudera mit StorageGRID

Von Angela Cheng

Hadoop ist bereits seit einiger Zeit ein beliebtes Datenwissenschaftlerteam. Hadoop ermöglicht die verteilte Verarbeitung großer Datensätze über Computer-Cluster mithilfe von einfachen ProgrammierFrameworks. Hadoop wurde entwickelt, um von einzelnen Servern auf Tausende von Machines zu skalieren, wobei jede Maschine über lokale Computing- und Storage-Ressourcen verfügt.

Vorteile von S3A für Hadoop Workflows

Mit der Zeit hat das Datenvolumen zugenommen, aber die Nutzung der IT-Infrastruktur mit eigenen Computing- und Storage-Ressourcen ist ineffizient. Lineare Skalierung führt zu Herausforderungen bei der effizienten Nutzung von Ressourcen und dem Management der Infrastruktur.

Zur Bewältigung dieser Herausforderungen bietet der Hadoop S3A-Client hochperformante I/O-Vorgänge im Vergleich zu S3-Objekt-Storage. Durch die Implementierung eines Hadoop Workflows mit S3A können Sie Objekt-Storage als Daten-Repository nutzen und Computing- und Storage-Ressourcen separat voneinander skalieren. Dadurch wiederum können Sie Computing- und Storage-Ressourcen unabhängig voneinander skalieren. Die Abkopplung von Computing und Storage eröffnet Ihnen auch die Möglichkeit, die passende Menge an Ressourcen für Ihre Rechneraufgaben zu beanspruchen und Kapazitäten basierend auf der Größe Ihres Datensatzes zu bereitstellen. Somit lassen sich die Gesamtbetriebskosten für Hadoop Workflows verringern.

S3A-Anschluss für die Verwendung von StorageGRID konfigurieren

Voraussetzungen

- Einen StorageGRID S3-Endpunkt-URL, einen S3-Zugriffsschlüssel für Mandanten und einen geheimen Schlüssel für Hadoop S3A-Verbindungstests.
- Ein Cloudera Cluster und Root- oder sudo-Berechtigung für jeden Host im Cluster, um das Java-Paket zu installieren.

Seit April 2022 wurde Java 11.0.14 mit Cloudera 7.1.7 gegen StorageGRID 11.5 und 11.6 getestet. Die Java-Versionsnummer kann jedoch bei einer neuen Installation unterschiedlich sein.

Installieren Sie das Java-Paket

1. Prüfen Sie die "Cloudera Support-Matrix" Für die unterstützte JDK-Version.
2. Laden Sie die herunter "Java 11.x-Paket" Das dem Cloudera Cluster-Betriebssystem entspricht. Kopieren Sie dieses Paket auf jeden Host im Cluster. In diesem Beispiel wird das rpm-Paket für CentOS verwendet.
3. Melden Sie sich bei jedem Host als Root an oder verwenden Sie ein Konto mit sudo-Berechtigung. Führen Sie für jeden Host folgende Schritte durch:
   a. Installieren Sie das Paket:

```
$ sudo rpm -Uvh jdk-11.0.14_linux-x64_bin.rpm
```

b. Überprüfen Sie, wo Java installiert ist. Wenn mehrere Versionen installiert sind, legen Sie die neu installierte Version als Standard fest:

```
alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 +1           /usr/java/jre1.8.0_291-amd64/bin/java
  2           /usr/java/jdk-11.0.14/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

c. Fügen Sie diese Zeile am Ende von hinzu `/etc/profile`. Der Pfad sollte dem Pfad der obigen Auswahl entsprechen:

```
export JAVA_HOME=/usr/java/jdk-11.0.14
```

d. Führen Sie den folgenden Befehl aus, damit das Profil wirksam wird:

```
source /etc/profile
```

Konfiguration von Cloudera HDFS S3A

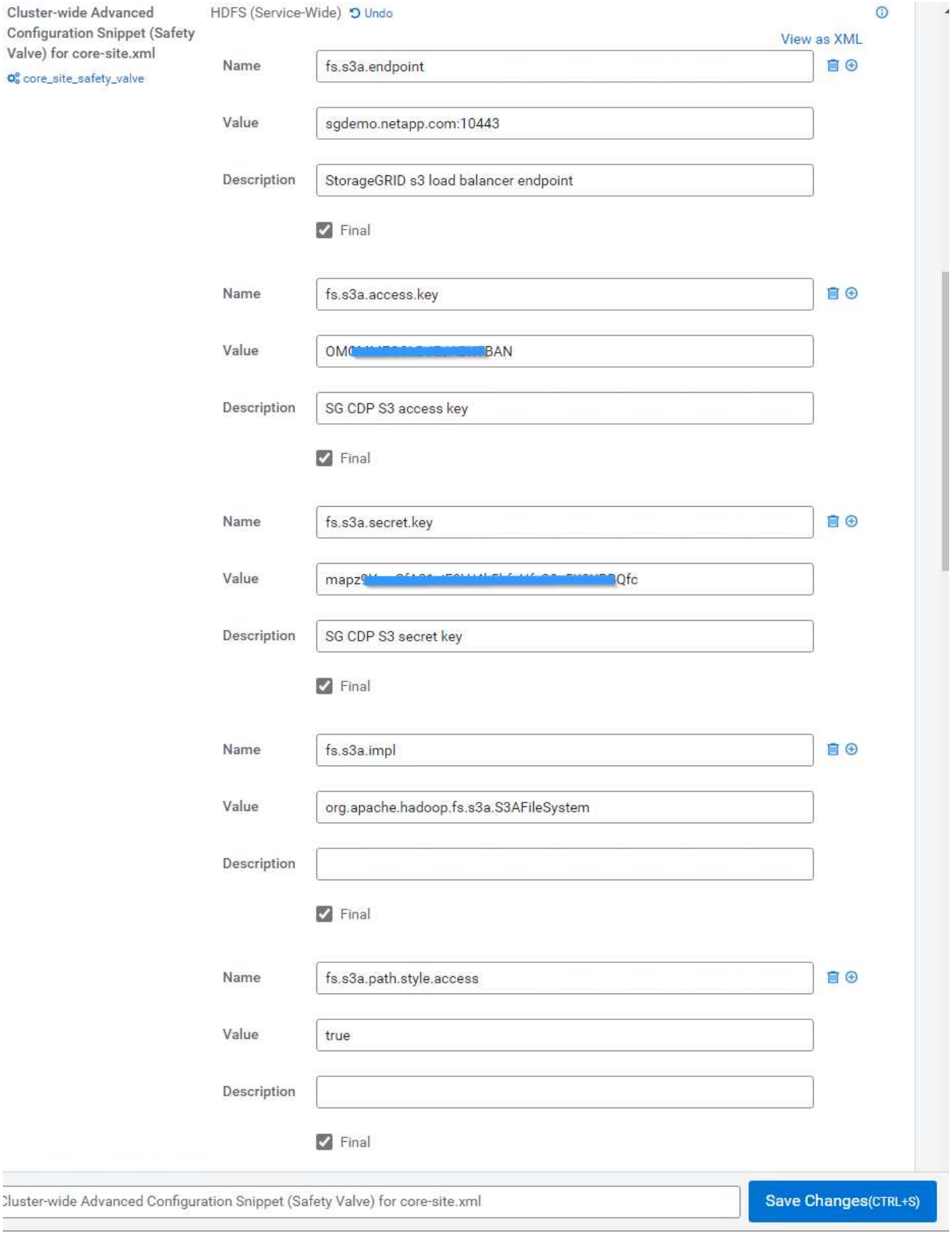
Schritte

1. Wählen Sie in der Cloudera Manager GUI Cluster > HDFS aus, und wählen Sie Konfiguration aus.
2. Wählen Sie unter KATEGORIE die Option Erweitert aus, und blättern Sie nach unten, um zu suchen `Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml`.
3. Klicken Sie auf das (+)-Zeichen und fügen Sie folgende Wertpaare hinzu.

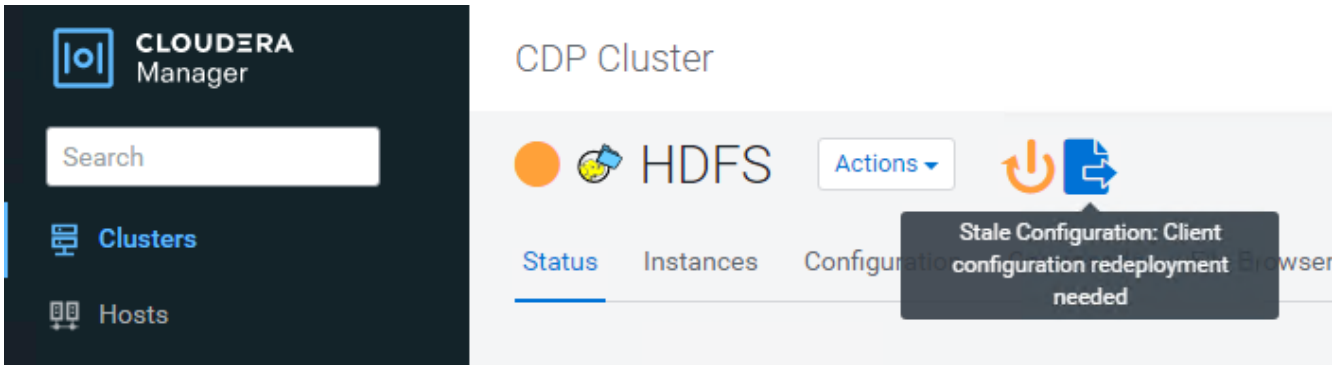
Name	Wert
fs.s3a.access.key	*<S3-Zugriffsschlüssel des Mandanten von StorageGRID>*
fs.s3a.secret.key	*<Mandant s3 geheimen Schlüssel von StorageGRID>*
fs.s3a.connection.ssl.enabled	[Wahr oder falsch] (Standardeinstellung: Https, wenn dieser Eintrag fehlt)

Name	Wert
fs.s3a.Endpunkt	*<StorageGRID S3 Endpunkt:Port>*
fs.s3a.mpl	Org.apache.hadoop.fs.s3a.S3AFileSystem
fs.s3a.path.style.Access	[True oder false] (Standard ist der Stil des virtuellen Hosts, wenn dieser Eintrag fehlt)

Beispiel Screenshot



4. Klicken Sie auf die Schaltfläche Änderungen speichern. Wählen Sie in der HDFS-Menüleiste das Symbol „veraltete Konfiguration“ aus, wählen Sie auf der nächsten Seite „veraltete Dienste neu starten“ und anschließend „Jetzt neu starten“ aus.



S3A-Verbindung mit StorageGRID testen

Führen Sie einen grundlegenden Verbindungstest durch

Melden Sie sich bei einem der Hosts im Cloudera Cluster an, und geben Sie ein `hadoop fs -ls s3a://<bucket-name>/`.

Im folgenden Beispiel wird Pfadsyle mit einem vorhandenen hdfs-Test-Bucket und einem Testobjekt verwendet.

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:24:37 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:24:37 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
Found 1 items
-rw-rw-rw-   1 root root       1679 2022-02-14 16:03 s3a://hdfs-test/test
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
```

Fehlerbehebung

Szenario 1

Verwenden Sie eine HTTPS-Verbindung zu StorageGRID, und holen Sie ein `handshake_failure` Fehler nach einem Timeout von 15 Minuten.

Grund: alte JRE/JDK-Version mit veralteter oder nicht unterstützter TLS-Chiffre-Suite für die Verbindung zu

StorageGRID.

Beispiel-Fehlermeldung

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:52:34 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:52:35 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/02/15 19:04:51 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
ls: doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
```

Auflösung: stellen Sie sicher, dass JDK 11.x oder höher installiert ist und auf die Java-Bibliothek eingestellt ist. Siehe Installieren Sie das Java-Paket Weitere Informationen finden Sie in.

Szenario 2:

Fehler beim Herstellen der Verbindung zum StorageGRID mit Fehlermeldung `Unable to find valid certification path to requested target`.

Grund: StorageGRID S3-Endpoint-Server-Zertifikat wird nicht von Java-Programm vertrauenswürdig.

Beispielfehlermeldung:

```
[root@hdp6 ~]# hadoop fs -ls s3a://hdfs-test/
22/03/11 20:58:12 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/03/11 20:58:13 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/03/11 21:12:25 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target: Unable to execute HTTP
request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

Auflösung: NetApp empfiehlt die Verwendung eines Serverzertifikats, das von einer bekannten öffentlichen Zertifizierungsstelle ausgestellt wurde, um die Sicherheit der Authentifizierung sicherzustellen. Alternativ können Sie dem Java Trust Store ein benutzerdefiniertes CA- oder Serverzertifikat hinzufügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte StorageGRID-Zertifizierungsstelle oder ein Serverzertifikat zum Java-Treuhandspeicher hinzuzufügen.

1. Sichern Sie die vorhandene Standard-Java-Cacaerts-Datei.

```
cp -ap $JAVA_HOME/lib/security/cacerts
$JAVA_HOME/lib/security/cacerts.orig
```

2. Importieren Sie das StorageGRID S3-Endpunktcert in den Java-Treuhandspeicher.

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts
-storepass changeit -noprompt -alias sg-lb -file <StorageGRID CA or
server cert in pem format>
```

Tipps zur Fehlerbehebung

1. Erhöhen sie den hadoop Protokolllevel zum DEBUGGEN.

   ```
   export HADOOP_ROOT_LOGGER=hadoop.root.logger=DEBUG,console
   ```

2. Führen Sie den Befehl aus und leiten Sie die Protokollmeldungen an ERROR.log.

   ```
   hadoop fs -ls s3a://<bucket-name>/ &>error.log
   ```

Von Angela Cheng

Verwenden Sie S3cmd, um den S3-Zugriff auf StorageGRID zu testen und zu demonstrieren

Von Aron Klein

S3cmd ist ein kostenloses Befehlszeilen-Tool und Client für S3-Vorgänge. Sie können s3cmd verwenden, um den s3-Zugriff auf StorageGRID zu testen und zu demonstrieren.

S3cmd installieren und konfigurieren

Um S3cmd auf einer Workstation oder einem Server zu installieren, laden Sie ihn von herunter "Kommandozeile S3-Client". S3cmd ist vorinstalliert auf jedem StorageGRID-Knoten als Tool zur Unterstützung der Fehlerbehebung.

Erste Konfigurationsschritte

1. S3cmd --configure
2. Geben Sie nur Access_Key und Secret_Key an, für den Rest behalten Sie die Standardeinstellungen.
3. Zugriff mit den angegebenen Zugangsdaten testen? [J/n]: n (den Test umgehen, da er fehlschlägt)
4. Einstellungen speichern? [J/N] J
   a. Konfiguration in '/root/.s3cfg' gespeichert
5. In .s3cfg make fields Host_base and Host_bucket leerer nach dem "=" Zeichen :
   a. Host_Base =
   b. Host_Bucket =

Wenn Sie in Schritt 4 Host_Base und Host_Bucket angeben, müssen Sie in der CLI keinen Endpunkt mit --Host angeben. Beispiel:

```
host_base = 192.168.1.91:8082
host_bucket = bucketX.192.168.1.91:8082
s3cmd ls s3://bucketX --no-check-certificate
```

Beispiele für grundlegende Befehle

- **Erstellen Sie einen Eimer:**

```
s3cmd mb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Alle Buckets auflisten:**

```
s3cmd ls --host=<endpoint>:<port> --no-check-certificate
```

- **Alle Eimer und deren Inhalt auflisten:**

```
s3cmd la --host=<endpoint>:<port> --no-check-certificate
```

- **Objekte in einem bestimmten Bucket auflisten:**

```
s3cmd ls s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Ein Eimer löschen:**

```
s3cmd rb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Legen Sie ein Objekt:**

```
s3cmd put <file> s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Holen Sie sich ein Objekt:**

```
s3cmd get s3://<bucket>/<object> <file> --host=<endpoint>:<port> --no-check
-certificate
```

- **Ein Objekt löschen:**

```
s3cmd del s3://<bucket>/<object> --host=<endpoint>:<port> --no-check
-certificate
```

Vertica Eon-Modus-Datenbank mit NetApp StorageGRID als gemeinschaftliche Storage-Lösung

Von Angela Cheng

In diesem Leitfaden werden die Verfahren zum Erstellen einer Vertica Eon-Modus-Datenbank mit gemeinsamem Speicher auf NetApp StorageGRID beschrieben.

Einführung

Vertica ist eine Software für das Analyse-Datenbankmanagement. Es handelt sich um eine spaltenbasierte Storage-Plattform zur Verarbeitung großer Datenvolumen. Damit ermöglicht sie eine sehr schnelle Abfrage-Performance in einem klassisch intensiven Szenario. Eine Vertica-Datenbank läuft in einem der beiden Modi: Eon oder Enterprise. Beide Modi können sowohl lokal als auch in der Cloud implementiert werden.

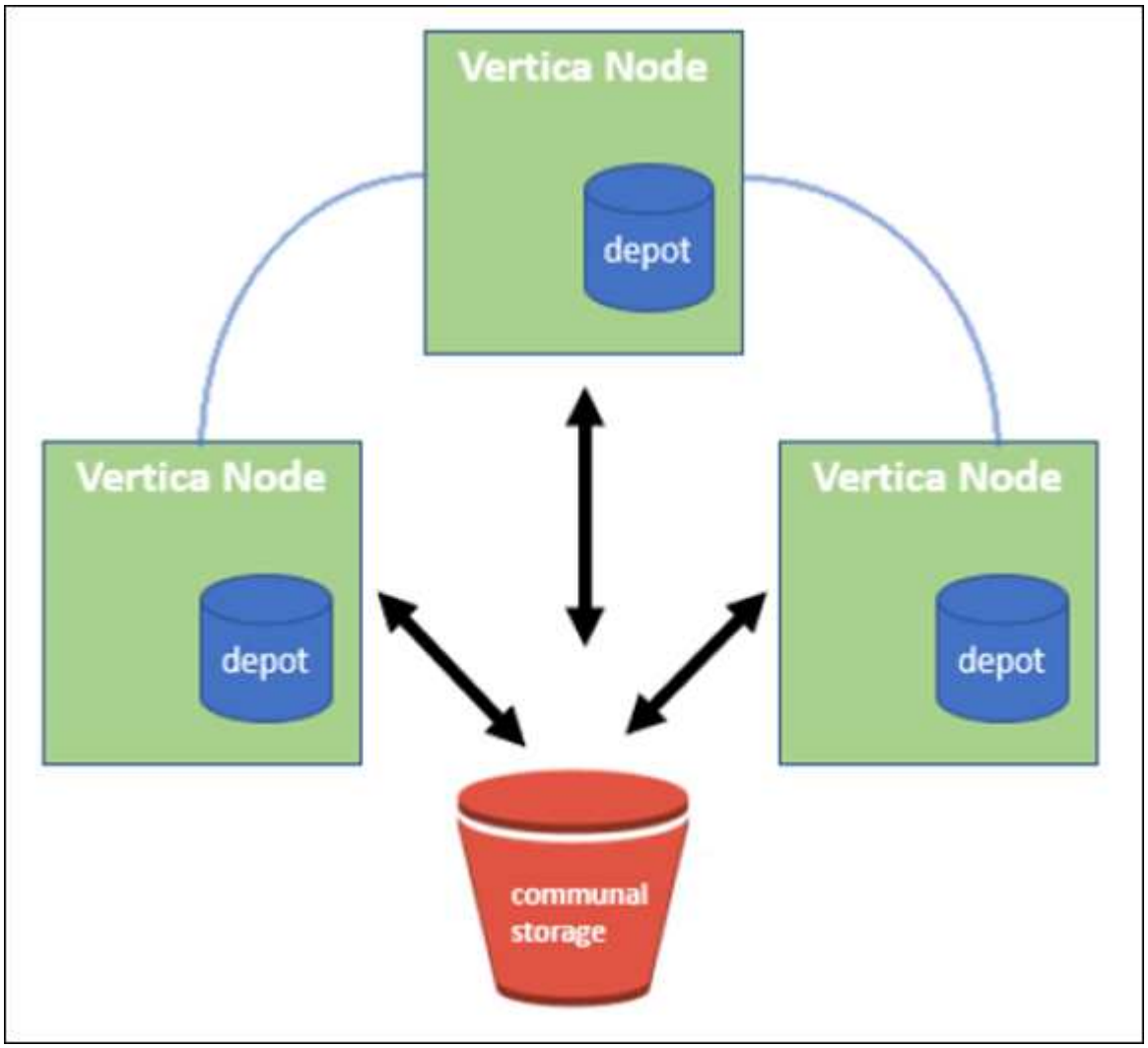
Eon- und Enterprise-Modi unterscheiden sich hauptsächlich darin, wo sie Daten speichern:

- Die Eon-Modus-Datenbanken verwenden einen gemeinsamen Speicher für ihre Daten. Dies wird von Vertica empfohlen.
- Die Enterprise-Mode-Datenbanken speichern die Daten lokal im Dateisystem der Knoten, aus denen die Datenbank besteht.

Eon-Mode-Architektur

Eon-Modus trennt die Computing-Ressourcen von der gemeinsamen Storage-Schicht der Datenbank, wodurch Computing- und Storage-Ressourcen getrennt skaliert werden können. Vertica im Eon-Modus ist für variable Workloads optimiert und kann durch die Nutzung separater Computing- und Storage-Ressourcen voneinander isoliert werden.

Eon-Modus speichert Daten in einem gemeinsam genutzten Objektspeicher, dem sogenannten Communal Storage – einem S3-Bucket, der entweder lokal oder in Amazon S3 gehostet wird.



Gemeinschaftsspeicher

Statt Daten lokal zu speichern, verwendet der Eon-Modus einen einzigen gemeinsamen Speicherort für alle Daten und den Katalog (Metadaten). Der zentrale Speicherort der Datenbank, der von den Datenbank-Nodes gemeinsam genutzt wird, ist die gemeinsame Speicherung.

Kommunale Lagerung hat folgende Eigenschaften:

- Kommunaler Storage in der Cloud oder On-Premises-Objekt-Storage ist ausfallsicherer und anfällig für Datenverluste aufgrund von Storage-Ausfällen als Storage auf Festplatte an individuellen Maschinen.
- Alle Daten können von jedem Node aus denselben Pfad gelesen werden.
- Die Kapazität ist nicht durch den Festplattenspeicher auf Nodes begrenzt.
- Da Daten communal gespeichert werden, können Sie den Cluster flexibel skalieren, um den sich ändernden Anforderungen gerecht zu werden. Falls die Daten lokal auf den Nodes gespeichert wurden, müssten beim Hinzufügen oder Entfernen von Nodes umfangreiche Datenmengen zwischen Nodes verschoben werden, um sie entweder von entfernten Nodes oder auf neu erstellte Nodes zu verschieben.

Das Depot

Ein Nachteil der kommunalen Lagerung ist seine Geschwindigkeit. Der Zugriff auf Daten von einem gemeinsam genutzten Cloud-Speicherort ist langsamer als das Lesen von einer lokalen Festplatte. Darüber hinaus kann die Verbindung zu kommunalem Storage zu einem Engpass werden, wenn viele Nodes die Daten gleichzeitig lesen. Zur Verbesserung der Zugriffsgeschwindigkeit für Daten führen die Knoten in einer Eon-Modus-Datenbank einen lokalen Festplatten-Cache mit Daten, die als Depot bezeichnet werden. Bei der Ausführung einer Abfrage prüfen die Knoten zunächst, ob sich die erforderlichen Daten im Depot befinden. Ist dies der Fall, wird die Abfrage beendet, indem die lokale Kopie der Daten verwendet wird. Wenn sich die Daten nicht im Depot befindet, ruft der Knoten die Daten aus dem gemeinsamen Lager ab und speichert eine Kopie im Depot.

NetApp StorageGRID-Empfehlungen

Vertica speichert Datenbankdaten im Objekt-Storage als Tausende (oder Millionen) komprimierter Objekte (die beobachtete Größe beträgt 200 bis 500 MB pro Objekt. Wenn ein Benutzer Datenbankabfragen ausführt, ruft Vertica den ausgewählten Datenbereich aus diesen komprimierten Objekten parallel mit dem GET-Aufruf des Byte-Bereichs ab. Jeder Byte-Bereich HAT ca. 8 KB.

Während des 10-TB-Datenbankdepots zur Prüfung von Benutzeranfragen wurden 4,000 bis 10,000 GET-Anforderungen (Byte-Bereich GET) pro Sekunde an das Grid gesendet. Bei diesem Test werden SG6060 Appliances eingesetzt, obwohl die CPU-Auslastung des % pro Appliance-Node niedrig ist (etwa 20 bis 30 %), warten 2/3 der CPU-Zeit auf I/O Bei SGF6024 wird ein sehr kleiner Prozentsatz (0 % bis 0.5 %) des I/O-Wartens beobachtet.

Aufgrund der hohen Anforderungen an kleine IOPS mit sehr niedrigen Latenzanforderungen (der Durchschnitt liegt bei weniger als 0.01 Sekunden) empfiehlt NetApp die Verwendung von SFG6024 für Objekt-Storage-Services. Falls das SG6060 für sehr große Datenbanken benötigt wird, sollte der Kunde mit dem Vertica Account-Team zusammenarbeiten, um den aktiv abgefragten Datensatz zu unterstützen.

Für den Admin-Node und den API-Gateway-Node kann der Kunde das SG100 oder SG1000 verwenden. Die Wahl hängt von der Anzahl der Abfragen der Benutzer in paralleler und Datenbank-Größe ab. Wenn der Kunde einen Drittanbieter-Load-Balancer einsetzen möchte, empfiehlt NetApp einen dedizierten Load Balancer für Workloads mit hohen Performance-Anforderungen. Informationen zur StorageGRID Dimensionierung erhalten Sie vom NetApp Account Team.

Weitere Empfehlungen für die StorageGRID-Konfiguration:

- **Grid-Topologie**. Kombinieren Sie SGF6024 nicht mit anderen Storage Appliance-Modellen am selben Grid-Standort. Wenn Sie den SG6060 für den langfristigen Archivierungsschutz verwenden möchten, sollten Sie den SGF6024 mit einem dedizierten Grid Load Balancer am eigenen Grid-Standort (entweder am physischen oder logischen Standort) für eine aktive Datenbank aufbewahren, um die Performance zu steigern. Die Kombination verschiedener Appliance-Modelle am selben Standort verringert die Gesamtleistung am Standort.

- **Datenschutz**. Verwenden Sie Replizieren-Kopien für die Sicherheit. Verwenden Sie kein Erasure Coding für eine aktive Datenbank. Der Kunde kann das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verwenden, um inaktive Datenbanken langfristig zu schützen.
- **Gitterkompression nicht aktivieren**. Vertica komprimiert Objekte, bevor sie in Objekt-Storage gespeichert werden. Durch die Aktivierung der Grid-Komprimierung wird die Storage-Auslastung nicht weiter gesenkt und DIE GET-Performance im Byte-Bereich wird deutlich verringert.
- **HTTP im Vergleich zu HTTPS S3-Endpunktverbindung**. Während des Benchmark-Tests konnten wir bei der Verwendung einer HTTP S3-Verbindung vom Vertica Cluster zum StorageGRID Load Balancer-Endpunkt eine Performance-Steigerung von ca. 5 % feststellen. Diese Auswahl sollte auf den Sicherheitsanforderungen des Kunden basieren.

Empfehlungen für eine Vertica Konfiguration sind:

- **Die Standardeinstellungen des Vertica Datenbank-Depots sind aktiviert (Wert = 1) für Lese- und Schreibvorgänge**. NetApp empfiehlt dringend, diese Depoteinstellungen für die Performance-Steigerung zu aktivieren.
- **Streaming-Einschränkungen deaktivieren**. Weitere Informationen zur Konfiguration finden Sie im Abschnitt Deaktivieren von Streaming-Einschränkungen.

Installation von Eon-Modus vor Ort mit kommunalem Speicher auf StorageGRID

In den folgenden Abschnitten wird das Verfahren beschrieben, um den Eon-Modus vor Ort mit kommunalem Speicher auf StorageGRID zu installieren. Das Verfahren zur Konfiguration von S3-kompatiblem Objektspeicher (Simple Storage Service) ähnelt dem Verfahren im Vertica-Leitfaden. "Installation einer On-Premises-Eon-Mode-Datenbank".

Für den Funktionstest wurde folgendes Setup verwendet:

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- Drei Virtual Machines (VMs) mit CentOS 7.x OS für Vertica Nodes zu einem Cluster bilden. Dieses Setup gilt nur für den Funktionstest, nicht für das Produktions-Datenbank-Cluster der Vertica.

Diese drei Nodes sind mit einem SSH-Schlüssel (Secure Shell) eingerichtet, um SSH ohne Passwort zwischen den Nodes innerhalb des Clusters zuzulassen.

Erforderliche Informationen von NetApp StorageGRID

Um den Eon-Modus vor Ort mit kommunalem Speicher auf StorageGRID zu installieren, müssen Sie die folgenden Vorbedingung-Informationen haben.

- IP-Adresse oder vollständig qualifizierter Domain-Name (FQDN) und Portnummer des StorageGRID S3-Endpunkts. Wenn Sie HTTPS verwenden, verwenden Sie eine CA (Custom Certificate Authority) oder ein selbstsigniertes SSL-Zertifikat, das am StorageGRID S3-Endpunkt implementiert wurde.
- Bucket-Name Er muss vorexistieren und leer sein.
- Schlüssel-ID und geheimer Zugriffsschlüssel mit Lese- und Schreibzugriff auf den Bucket

Erstellen einer Autorisierungsdatei für den Zugriff auf den S3-Endpunkt

Beim Erstellen einer Autorisierungsdatei für den Zugriff auf den S3-Endpunkt gelten die folgenden Voraussetzungen:

- Vertica ist installiert.
- Ein Cluster ist für die Datenbankerstellung eingerichtet, konfiguriert und bereit.

So erstellen Sie eine Autorisierungsdatei für den Zugriff auf den S3-Endpunkt:

1. Melden Sie sich beim Vertica-Knoten an, auf dem Sie ausgeführt werden `admintools` So erstellen Sie die Eon-Modus-Datenbank.

   Der Standardbenutzer ist `dbadmin`, Erstellt während der Vertica Cluster Installation.

2. Verwenden Sie einen Texteditor, um eine Datei unter dem zu erstellen `/home/dbadmin` Verzeichnis. Der Dateiname kann alles sein, was Sie wollen, z. B. `sg_auth.conf`.
3. Wenn der S3-Endpunkt einen Standard-HTTP-Port 80 oder HTTPS-Port 443 verwendet, überspringen Sie die Portnummer. Um HTTPS zu verwenden, legen Sie die folgenden Werte fest:

   ◦ `awsenablehttps = 1`, Sonst setzen Sie den Wert auf `0`.

   ◦ `awsauth = <s3 access key ID>:<secret access key>`

   ◦ `awsendpoint = <StorageGRID s3 endpoint>:<port>`

   Um eine benutzerdefinierte CA oder ein selbstsigniertes SSL-Zertifikat für die HTTPS-Verbindung des StorageGRID S3-Endpunkts zu verwenden, geben Sie den vollständigen Dateipfad und den Dateinamen des Zertifikats an. Diese Datei muss sich am selben Speicherort auf jedem Vertica-Knoten befinden und über Leseberechtigung für alle Benutzer verfügen. Überspringen Sie diesen Schritt, wenn das StorageGRID S3 Endpoint SSL-Zertifikat von einer öffentlich bekannten CA signiert wurde.

   - `awscafile = <filepath/filename>`

   Informationen hierzu finden Sie beispielsweise in der folgenden Beispieldatei:

```
awsauth = MNVU4OYFAY2xyz123:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wANabcxyz
awsendpoint = s3.england.connectlab.io:10443
awsenablehttps = 1
awscafile = /etc/custom-cert/grid.pem
```

+

> In einer Produktionsumgebung muss der Kunde ein Serverzertifikat implementieren, das von einer öffentlich bekannten CA auf einem StorageGRID S3 Load Balancer-Endpunkt unterzeichnet wurde.

Auswählen eines Depotpfads auf allen Vertica-Knoten

Wählen Sie auf jedem Knoten ein Verzeichnis für den Depot-Speicherpfad aus oder erstellen Sie ein Verzeichnis. Das Verzeichnis, das Sie für den Parameter Depot-Speicherpfad bereitstellen, muss Folgendes haben:

- Derselbe Pfad auf allen Nodes im Cluster (z. B. `/home/dbadmin/depot`)
- Vom dbadmin-Benutzer lesbar und beschreibbar sein

- Ausreichende Lagerung

  Standardmäßig verwendet Vertica 60 % des Dateisystemspeichers, der das Verzeichnis für die Depotspeicherung enthält. Sie können die Größe des Depots mithilfe der begrenzen `--depot-size` Argument in `create_db` Befehl. Siehe "Dimensionierung des Vertica Clusters für eine Eon-Mode-Datenbank" Artikel für allgemeine Vertica Größenrichtlinien oder wenden Sie sich an Ihren Vertica Account Manager.

  Der `admintools create_db` Das Tool versucht, den Depotpfad für Sie zu erstellen, wenn dieser nicht vorhanden ist.

Erstellen der On-Premises-Datenbank von Eon

So erstellen Sie die On-Premises-Datenbank von Eon:

1. Verwenden Sie zum Erstellen der Datenbank die `admintools create_db` Werkzeug.

   Die folgende Liste enthält eine kurze Erläuterung der Argumente, die in diesem Beispiel verwendet werden. Eine detaillierte Erläuterung aller erforderlichen und optionalen Argumente finden Sie im Dokument Vertica.

   - -X <Pfad/Dateiname der in erstellten Autorisierungsdatei „Erstellen einer Autorisierungsdatei für den Zugriff auf den S3-Endpunkt“ >.

     Die Autorisierungsdetails werden nach erfolgreicher Erstellung in der Datenbank gespeichert. Sie können diese Datei entfernen, um zu vermeiden, dass der S3-Geheimschlüssel offengelegt wird.

   - --communal-Storage-location <s3://storagegrid buchname>
   - -S <kommagetrennte Liste der Vertica-Knoten, die für diese Datenbank verwendet werden sollen>
   - -D <Name der zu erstellenden Datenbank>
   - -P <Kennwort für diese neue Datenbank> festlegen. Den folgenden Beispielbefehl können Sie z. B. einsehen:

     ```
     admintools -t create_db -x sg_auth.conf --communal-storage
     -location=s3://vertica --depot-path=/home/dbadmin/depot --shard
     -count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
     '<password>'
     ```

     Das Erstellen einer neuen Datenbank dauert abhängig von der Anzahl der Nodes für die Datenbank mehrere Minuten. Wenn Sie die Datenbank zum ersten Mal erstellen, werden Sie aufgefordert, die Lizenzvereinbarung zu akzeptieren.

Informationen hierzu finden Sie z. B. in der folgenden Beispielautorisierungsdatei und `create db` Befehl:

```
[dbadmin@vertica-vm1 ~]$ cat sg_auth.conf
awsauth = MNVU4OYFAY2CPKVXVxxxx:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wAN+xxxx
awsendpoint = s3.england.connectlab.io:10445
awsenablehttps = 1
```

```
[dbadmin@vertica-vm1 ~]$ admintools -t create_db -x sg_auth.conf
--communal-storage-location=s3://vertica --depot-path=/home/dbadmin/depot
--shard-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'xxxxxxxx'
Default depot size in use
Distributing changes to cluster.
    Creating database vmart
    Starting bootstrap node v_vmart_node0007 (10.45.74.19)
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (UP)
    Creating database nodes
    Creating node v_vmart_node0008 (host 10.45.74.29)
    Creating node v_vmart_node0009 (host 10.45.74.39)
    Generating new configuration information
    Stopping single node db before adding additional nodes.
    Database shutdown complete
    Starting all nodes
Start hosts = ['10.45.74.19', '10.45.74.29', '10.45.74.39']
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
        v_vmart_node0008 (10.45.74.29)
        v_vmart_node0009 (10.45.74.39)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (UP) v_vmart_node0008: (UP)
v_vmart_node0009: (UP)
Creating depot locations for 3 nodes
Communal storage detected: rebalancing shards

Waiting for rebalance shards. We will wait for at most 36000 seconds.
Installing AWS package
```

```
    Success: package AWS installed
Installing ComplexTypes package
    Success: package ComplexTypes installed
Installing MachineLearning package
    Success: package MachineLearning installed
Installing ParquetExport package
    Success: package ParquetExport installed
Installing VFunctions package
    Success: package VFunctions installed
Installing approximate package
    Success: package approximate installed
Installing flextable package
    Success: package flextable installed
Installing kafka package
    Success: package kafka installed
Installing logsearch package
    Success: package logsearch installed
Installing place package
    Success: package place installed
Installing txtindex package
    Success: package txtindex installed
Installing voltagesecure package
    Success: package voltagesecure installed
Syncing catalog on vmart with 2000 attempts.
Database creation SQL tasks completed successfully. Database vmart created
successfully.
```

Objektgröße (Byte)	Bucket/Objektschlüssel vollständiger Pfad
61	s3://vertica/051/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07_0_0.dfs
145	s3://vertica/2c4/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d_0_0.dfs
146	s3://vertica/33c/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d_0_0.dfs

Objektgröße (Byte)	Bucket/Objektschlüssel vollständiger Pfad
40	s3://vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31_0_0.dfs
145	s3://vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21_0_0.dfs
34	s3://vertica/472/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25_0_0.dfs
41	s3://vertica/476/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d_0_0.dfs
61	s3://vertica/52a/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d_0_0.dfs
131	s3://vertica/5d2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19_0_0.dfs
91	s3://vertica/5f7/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11_0_0.dfs
118	s3://vertica/82d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15_0_0.dfs
115	s3://vertica/9a2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61_0_0.dfs

Objektgröße (Byte)	Bucket/Objektschlüssel vollständiger Pfad
33	s3://vertica/acd/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29_0_0.dfs
133	s3://vertica/b98/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d_0_0.dfs
38	s3://vertica/db3/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49_0_0.dfs
38	s3://vertica/eba/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59_0_0.dfs
21521920	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2.tar
6865408	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602.tar
204217344	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610.tar
16109056	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0.tar
12853248	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800.tar

Objektgröße (Byte)	Bucket/Objektschlüssel vollständiger Pfad
8937984	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a.tar
56260608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2.tar
53947904	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000000219ba/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219ba.tar
44932608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de.tar
256306688	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e.tar
8062464	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34.tar
20024832	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70.tar
10444	s3://vertica/metadata/VMart/cluster_config.json
823266	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/chkpt_1.cat.gz

Objektgröße (Byte)	Bucket/Objektschlüssel vollständiger Pfad
254	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/completed
2958	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/completed
822521	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/completed
746513	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat
2596	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz
821065	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz
6440	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat
8518	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat

Objektgröße (Byte)	Bucket/Objektschlüssel vollständiger Pfad
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Deaktivieren von Streaming-Einschränkungen

Dieses Verfahren basiert auf dem Vertica-Leitfaden für andere On-Premises-Objektspeicher und sollte für StorageGRID angewendet werden.

1. Deaktivieren Sie nach dem Erstellen der Datenbank das `AWSStreamingConnectionPercentage` Konfigurationsparameter durch Festlegen auf `0`. Diese Einstellung ist für eine On-Premises-Installation im Eon-Modus mit kommunalem Speicher nicht erforderlich. Dieser Konfigurationsparameter steuert die Anzahl der Verbindungen zu dem Objektspeicher, den Vertica für das Streaming von Lesevorgängen verwendet. In einer Cloud-Umgebung verhindert diese Einstellung, dass aus dem Objektspeicher Daten gestreamt werden, alle verfügbaren Datei-Handles nutzen. Einige Datei-Handles stehen für andere Objektspeichervorgänge zur Verfügung. Aufgrund der niedrigen Latenz von On-Premises-Objektspeichern ist diese Option nicht erforderlich.
2. Verwenden Sie A `vsql` Anweisung zum Aktualisieren des Parameterwerts. Das Passwort ist das Datenbank-Passwort, das Sie unter „Erstellen der On-Premises-Datenbank von Eon“ festgelegt haben. Informationen hierzu finden Sie z. B. in der folgenden Beispielausgabe:

```
[dbadmin@vertica-vm1 ~]$ vsql
Password:
Welcome to vsql, the Vertica Analytic Database interactive terminal.
Type:   \h or \? for help with vsql commands
        \g or terminate with semicolon to execute query
        \q to quit
dbadmin=> ALTER DATABASE DEFAULT SET PARAMETER
AWSStreamingConnectionPercentage = 0; ALTER DATABASE
dbadmin=> \q
```

Depot-Einstellungen werden überprüft

Standarddepot-Einstellungen der Vertica-Datenbank sind aktiviert (Wert = 1) für Lese- und Schreibvorgänge. NetApp empfiehlt dringend, diese Depoteinstellungen für die Performance-Steigerung zu aktivieren.

```
vsql -c 'show current all;' | grep -i UseDepot
DATABASE | UseDepotForReads | 1
DATABASE | UseDepotForWrites | 1
```

Laden von Probendaten (optional)

Wenn diese Datenbank zu Testzwecken bereit ist und entfernt werden wird, können Sie Beispieldaten zu Testzwecken in diese Datenbank laden. Vertica kommt mit Probendatensatz, VMart, gefunden unter `/opt/vertica/examples/VMart_Schema/` Auf jedem Vertica-Knoten. Weitere Informationen zu diesem Beispieldatensatz finden Sie hier "Hier".

Führen Sie die folgenden Schritte aus, um die Probendaten zu laden:

1. Melden Sie sich als dbadmin an einem der Vertica-Knoten an: cd /opt/vertica/examples/VMart_Schema/
2. Laden Sie Beispieldaten in die Datenbank, und geben Sie das Datenbank-Passwort ein, wenn Sie in den Unterschritten c und d aufgefordert werden:

a. `cd /opt/vertica/examples/VMart_Schema`

b. `./vmart_gen`

c. `vsql < vmart_define_schema.sql`

d. `vsql < vmart_load_data.sql`

3. Es gibt mehrere vordefinierte SQL-Abfragen. Sie können einige davon ausführen, um zu bestätigen, dass die Testdaten erfolgreich in die Datenbank geladen wurden. Beispiel: `vsql < vmart_queries1.sql`

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- "NetApp StorageGRID 11.7 Produktdokumentation"
- "Datenblatt zu StorageGRID"
- "Vertica 10.1 Produktdokumentation"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	September 2021	Erste Version.

Von Angela Cheng

StorageGRID-Protokollanalyse mit ELK-Stack

Von Angela Cheng

Mit der StorageGRID syslog Forward-Funktion können Sie einen externen Syslog-Server konfigurieren, um StorageGRID-Protokollmeldungen zu sammeln und zu analysieren. ELK (Elasticsearch, Logstash, Kibana) hat sich zu einer der beliebtesten Log-Analytics-Lösungen entwickelt. Im sehen Sie "StorageGRID-Protokollanalyse mit ELK-Video" sich eine Beispielkonfiguration für ELK an und erfahren, wie diese verwendet werden kann, um fehlgeschlagene S3-Anfragen zu identifizieren und Fehler zu beheben. StorageGRID 11.9 unterstützt den Export des Load Balancer-Endpunktzugriffsprotokolls auf externen Syslog-Server. Hier "Youtube-Video" erfahren Sie mehr über diese neue Funktion. Dieser Artikel enthält Beispieldateien der Logstash-Konfiguration, Kibana-Abfragen, Diagramme und Dashboard, die Ihnen einen schnellen Einstieg in die StorageGRID-Protokollverwaltung und -Analyse ermöglichen.

Anforderungen

- StorageGRID 11.6.0.2 oder höher
- ELK (Elasticsearch, Logstash und Kibana) 7.1x oder höher installiert und in Betrieb

Beispieldateien

- "Laden Sie das Paket Logstash 7.x Beispieldateien herunter" + **md5 Prüfsumme** 148c23d0021d9a4bb4a6c0287464deab + **sha256 Prüfsumme** f51ec9e2e3f842d5a786156b167a561beb4373038b4e7bb3c8be3d522adf2d6

- "Laden Sie das Paket Logstash 8.x Beispieldateien herunter" + **md5 Prüfsumme** e11bae3a662f87c310ef363d0fe06835 + **sha256 Prüfsumme** 5c670755742cfd5aa723a596ba087e0153a65bcae3934afddddddddd68d
- "Laden Sie das Paket mit den Logstash 8.x-Beispieldateien für StorageGRID 11.9 herunter" + **md5-Prüfsumme** 41272857c4a54600f95995f6ed74800d + **Sha256-Prüfsumme** 67048ee8661052719990851e1ad960d4902fe537a6e135e8600177188da677c9

Annahme

Leser kennen die Terminologie und den Betrieb von StorageGRID und ELK.

Anweisung

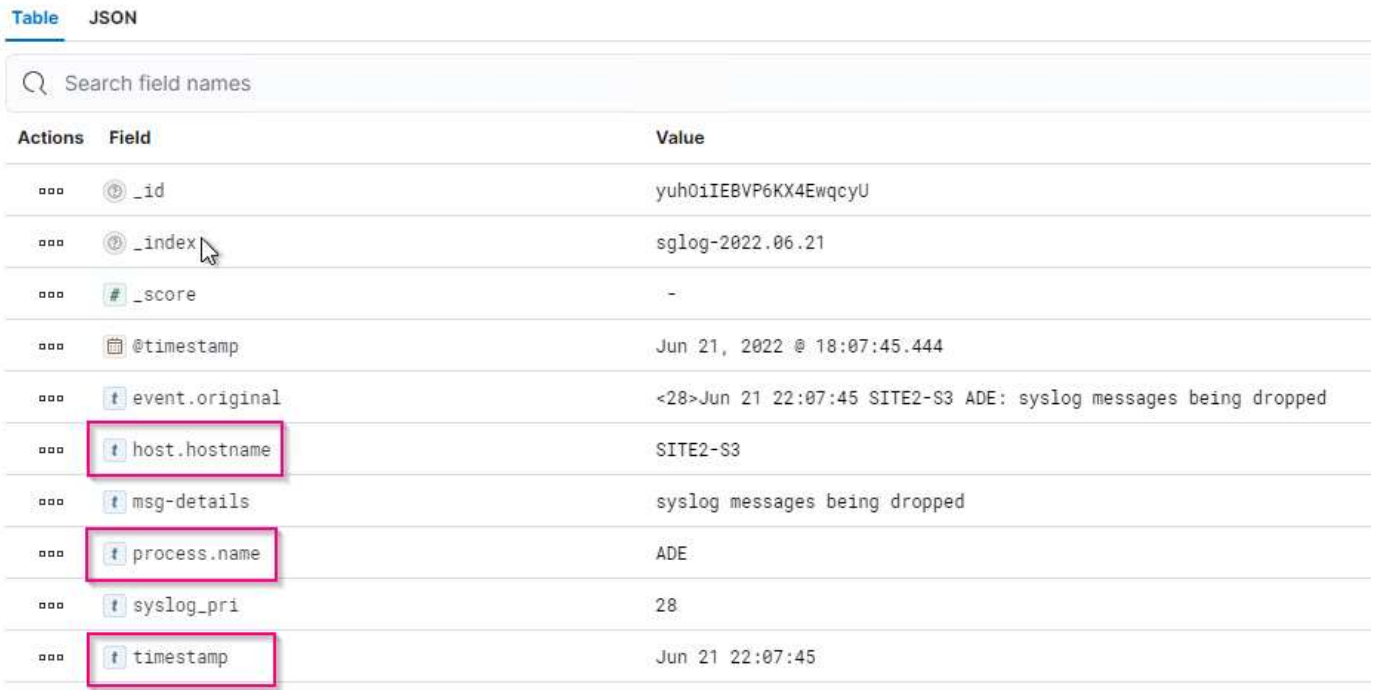
Zwei Beispielversionen werden aufgrund von Unterschieden in Namen bereitgestellt, die durch grok-Muster definiert wurden. + zum Beispiel definiert das SYSLOGBASE-grok-Muster in der Logstash config-Datei Feldnamen je nach installierter Logstash-Version unterschiedlich.

```
match => {"message" => '<%{POSINT:syslog_pri}>%{SYSLOGBASE}
%{GREEDYDATA:msg-details}'}
```

Logstash 7.17 Beispiel

Field	Value
t _id	7C1MaYEBRH8UbfKnIls8
t _index	sgrid2-2022.06.15
# _score	-
t _type	_doc
@timestamp	Jun 15, 2022 @ 17:36:46.038
t host	grid2-site2-s1
t logsource	SITE2-S1
t msg-details	Reloading syslog service
t pid	628
t program	update-sysl
t syslog_pri	37
t timestamp	Jun 15 21:36:46

Logstash 8.23 Beispiel



Schritte

1. Entpacken Sie das angegebene Muster anhand Ihrer installierten ELK-Version. + der Beispielordner enthält zwei Logstash-Konfigurationsbeispiele: + **sglog-2-file.conf:** Diese Konfigurationsdatei gibt StorageGRID-Protokollnachrichten ohne Datentransformation in eine Datei auf Logstash aus. Sie können auf diese Weise bestätigen, dass Logstash StorageGRID Nachrichten empfangen oder StorageGRID-Protokollmuster verstehen. + **sglog-2-es.conf:** Diese Konfigurationsdatei wandelt StorageGRID-Protokollmeldungen mithilfe verschiedener Muster und Filter um. Dazu gehören beispielsweise Drop-Statements, die Meldungen basierend auf Mustern oder Filtern ablegen. Die Ausgabe wird zur Indizierung an Elasticsearch gesendet. + Passen Sie die ausgewählte Konfigurationsdatei entsprechend der Anweisung in der Datei an.
2. Testen Sie die benutzerdefinierte Konfigurationsdatei:

   ```
   /usr/share/logstash/bin/logstash --config.test_and_exit -f <config-file-path/file>
   ```

   Wenn die letzte zurückgegebene Zeile der unten angegebenen Zeile ähnelt, weist die Konfigurationsdatei keine Syntaxfehler auf:

   ```
   [LogStash::Runner] runner - Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
   ```

3. Benutzerdefinierte conf-Datei auf den Logstash-Server kopieren.config: /Etc/logstash/conf.d + Wenn Sie config.reload.automatic in /etc/logstash/logstash.yml nicht aktiviert haben, starten Sie den Logstash-Dienst neu. Andernfalls warten Sie, bis das Neueintervall der Konfiguration abgelaufen ist.

```
 grep reload /etc/logstash/logstash.yml
# Periodically check if the configuration has changed and reload the
pipeline
config.reload.automatic: true
config.reload.interval: 5s
```

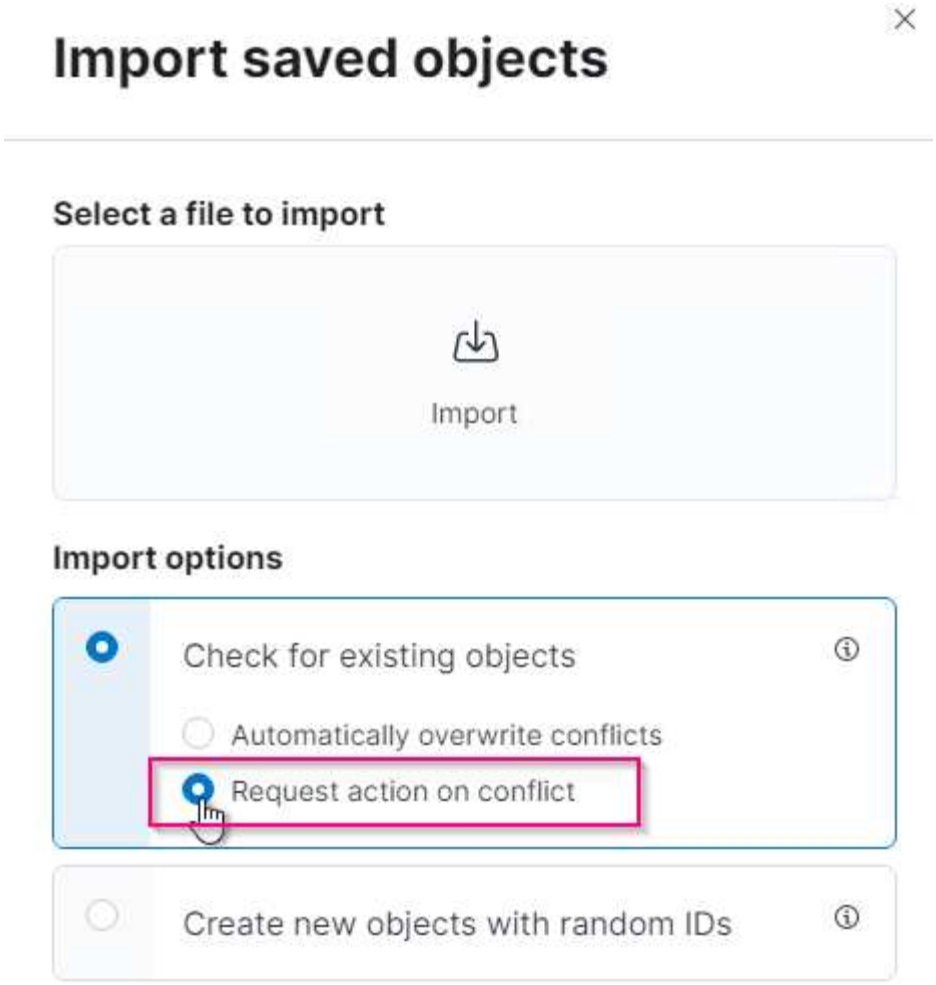
4. Prüfen Sie /var/log/logstash/logstash-plain.log und vergewissern Sie sich, dass beim Starten von Logstash mit der neuen Konfigurationsdatei keine Fehler auftreten.
5. Bestätigen Sie, dass der TCP-Port gestartet wurde und Sie zuhören. + in diesem Beispiel wird der TCP-Port 5000 verwendet.

```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

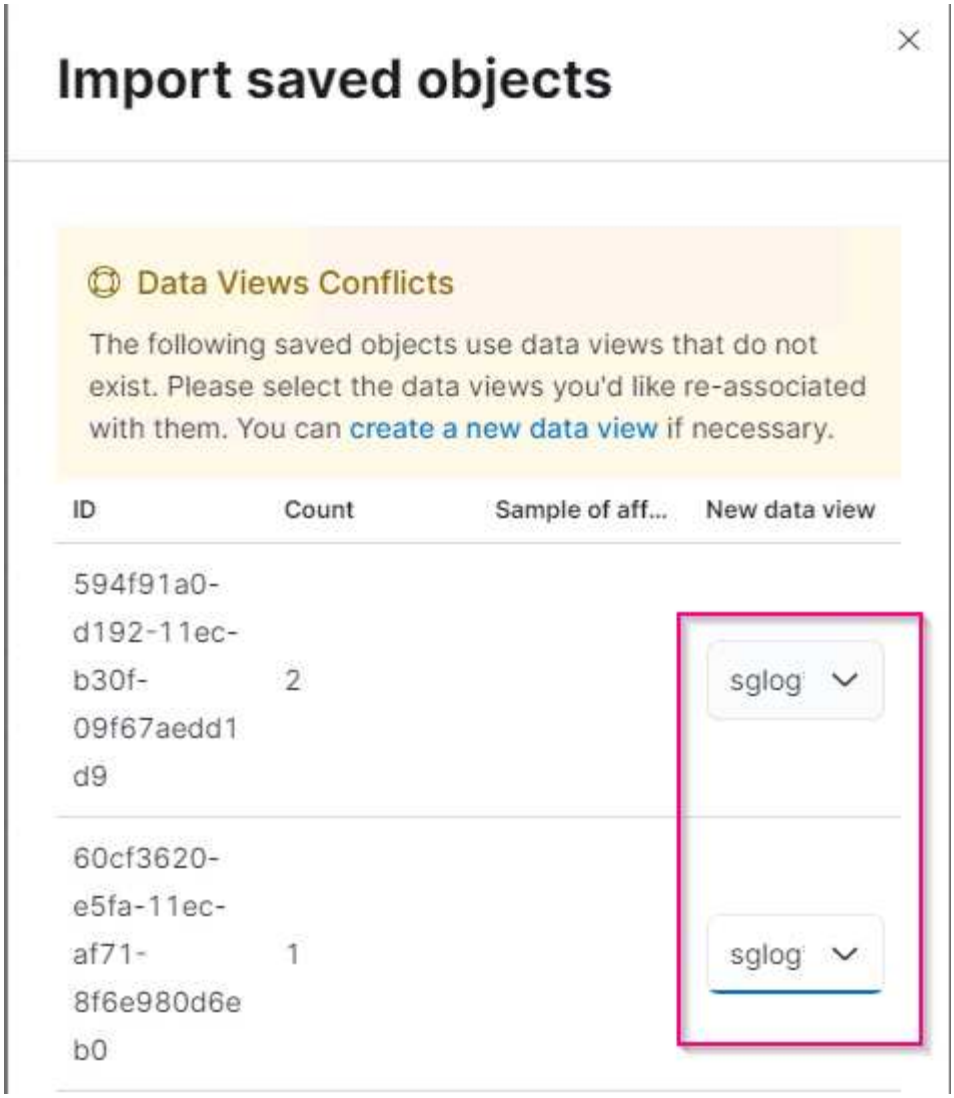
6. Konfigurieren Sie über die StorageGRID Manager-GUI einen externen Syslog-Server, um Protokollmeldungen an Logstash zu senden. Weitere Informationen finden Sie im "Demovideo" .
7. Sie müssen die Firewall auf dem Logstash-Server konfigurieren oder deaktivieren, damit StorageGRID-Knoten eine Verbindung zum definierten TCP-Port herstellen können.
8. Wählen Sie in der Kibana GUI die Option Management → Dev Tools. Führen Sie auf der Konsolenseite diesen BEFEHL GET aus, um zu bestätigen, dass neue Indizes auf Elasticsearch erstellt werden.

```
GET /_cat/indices/*?v=true&s=index
```

9. Erstellen Sie in der Kibana GUI Indexmuster (ELK 7.x) oder Datenansicht (ELK 8.x).
10. Geben Sie in der Kibana GUI in das Suchfeld, das sich in der oberen Mitte befindet, „abgetackte Objekte“ ein. + Wählen Sie auf der Seite gespeicherte Objekte die Option Importieren. Wählen Sie unter „Importoptionen“ die Option „Aktion für Konflikt anfordern“ aus.



Importieren Sie elk<Version>-query-Chart-sample.ndjson. + Wählen Sie bei Aufforderung zur Lösung des Konflikts das in Schritt 8 erstellte Indexmuster oder die Datenansicht aus.



Die folgenden Kibana-Objekte werden importiert: + **Query** + * Audit-msg-s3rq-orlm + * bycast log s3-bezogene Nachrichten + * Loglevel Warnung oder höher + * fehlgeschlagenes Sicherheitsereignis bycast.log + * nginx-gw-Endpunkt-Zugriffsprotokoll (nur verfügbar in elk8-sample-for-sg119.zip) + * Dashboard Chart* + * S3-Fehlerstatusdiagramme über S3 * Meldungsdaten *

Sie können nun die StorageGRID-Protokollanalyse mit Kibana durchführen.

Weitere Ressourcen

- "Syslog101"
- "Was ist der ELK-Stack"
- "Liste der Tülenmuster"
- "Ein Anfängerführer zum Logstash: Grok"
- "Eine praktische Anleitung zum Logstash: Syslog Deep Dive"
- "Kibana Guide – Erkunden Sie das Dokument"
- "Referenz für StorageGRID-Prüfprotokolle"

Mit Prometheus und Grafana können Sie die Aufbewahrung Ihrer Kennzahlen erweitern

Von Aron Klein

Dieser technische Bericht enthält detaillierte Anweisungen zur Konfiguration von NetApp StorageGRID mit externen Prometheus- und Grafana-Diensten.

Einführung

StorageGRID speichert Kennzahlen mithilfe von Prometheus und visualisiert diese Kennzahlen über integrierte Grafana Dashboards. Die Kennzahlen von Prometheus können über StorageGRID sicher abgerufen werden, indem Client-Zugriffszertifikate konfiguriert und prometheus-Zugriff für den angegebenen Client ermöglicht wird. Derzeit wird die Aufbewahrung dieser metrischen Daten durch die Storage-Kapazität des Administrations-Nodes begrenzt. Um eine längere Dauer zu erreichen und individuelle Visualisierungen dieser Kennzahlen zu erstellen, werden wir einen neuen Prometheus- und Grafana-Server einsetzen, unseren neuen Server für die Scrape der Kennzahlen aus der StorageGRIDs-Instanz konfigurieren und ein Dashboard mit den für uns wichtigen Kennzahlen erstellen. Weitere Informationen zu den in der erfassten Prometheus-Kennzahlen finden Sie unter "StorageGRID-Dokumentation".

Föderate Prometheus

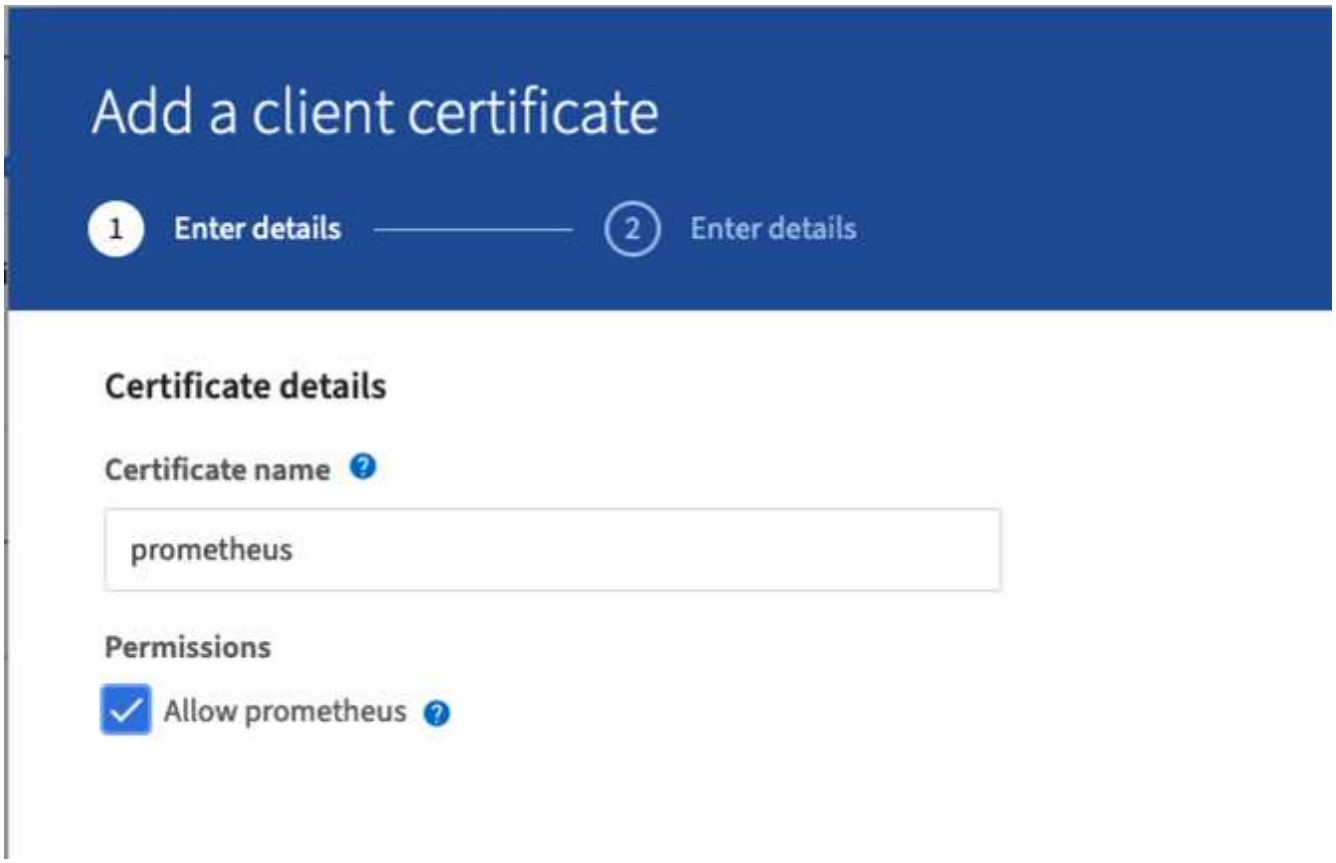
Labordetails

Für die Zwecke dieses Beispiels werde ich alle virtuellen Maschinen für StorageGRID 11.6 Knoten und einen Debian 11-Server verwenden. Die StorageGRID-Managementoberfläche ist mit einem öffentlich vertrauenswürdigen CA-Zertifikat konfiguriert. Dieses Beispiel wird die Installation und Konfiguration des StorageGRID-Systems oder der Debian linux-Installation nicht durchlaufen. Sie können jeden gewünschten Linux-Geschmack verwenden, der von Prometheus und Grafana unterstützt wird. Sowohl Prometheus als auch Grafana können als Docker-Container installiert, aus der Quelle erstellt oder vorkompilierte Binärdateien erstellt werden. In diesem Beispiel werde ich sowohl Prometheus- als auch Grafana-Binärdateien direkt auf dem gleichen Debian-Server installieren. Laden Sie sich die grundlegenden Installationsanweisungen von herunter https://prometheus.io Und https://grafana.com/grafana/ Jeweils.

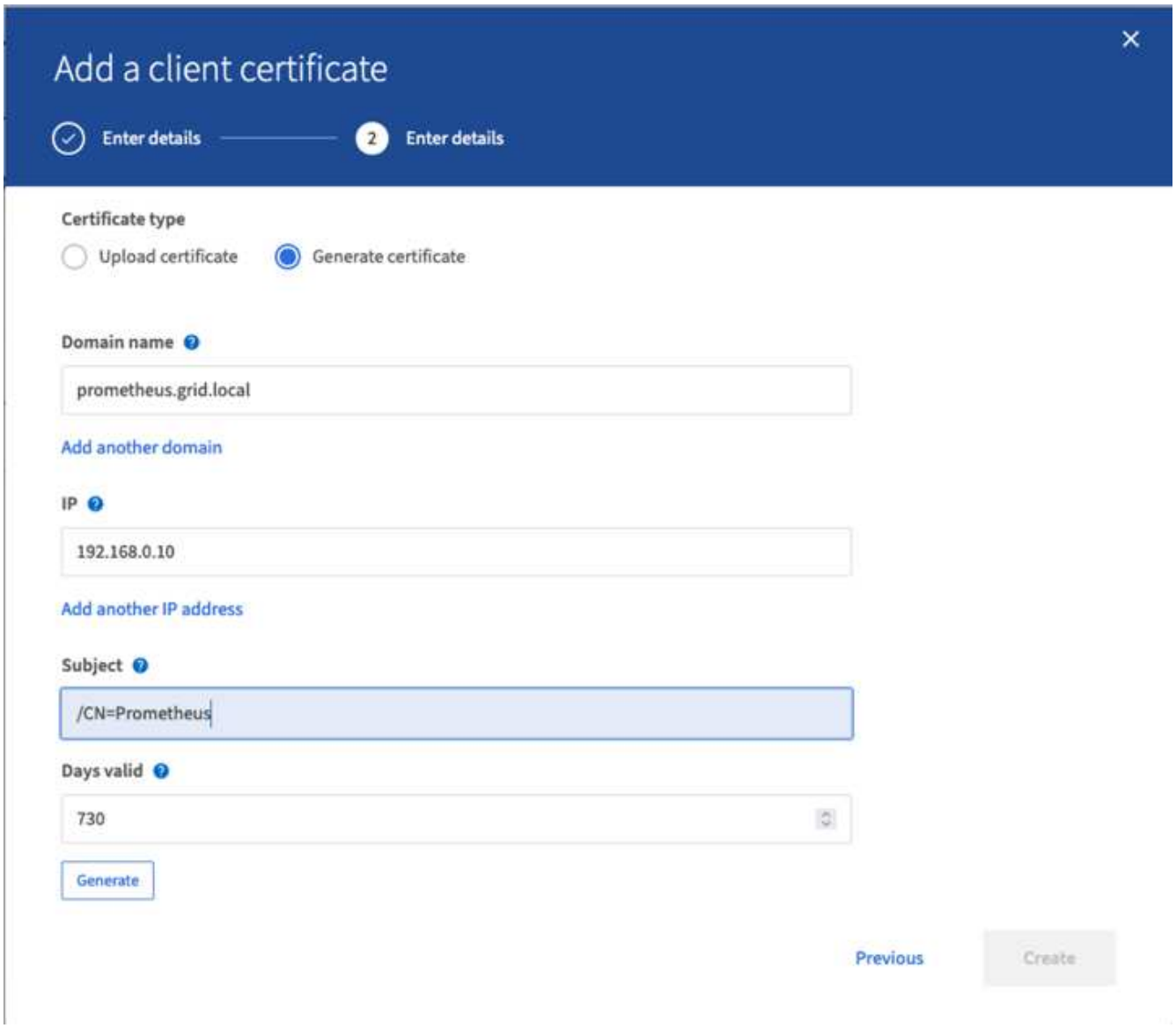
Konfigurieren Sie StorageGRID für Prometheus Client-Zugriff

Um Zugriff auf gespeicherte prometheus-Kennzahlen zu StorageGRIDs zu erhalten, müssen Sie ein Clientzertifikat mit privatem Schlüssel generieren oder hochladen und die Berechtigung für den Client aktivieren. Die StorageGRID-Schnittstelle muss ein SSL-Zertifikat haben. Dieses Zertifikat muss vom prometheus-Server entweder von einer vertrauenswürdigen CA oder manuell vertrauenswürdig sein, wenn es selbst signiert ist. Weitere Informationen finden Sie auf der "StorageGRID-Dokumentation".

1. Wählen Sie in der StorageGRID-Managementoberfläche unten links die Option „KONFIGURATION“ und klicken Sie in der zweiten Spalte unter „Sicherheit“ auf Zertifikate.
2. Wählen Sie auf der Seite Zertifikate die Registerkarte „Client“ aus und klicken Sie auf die Schaltfläche „Add“.
3. Geben Sie einen Namen für den Client an, dem Zugriff gewährt wird, und verwenden Sie dieses Zertifikat. Klicken Sie auf das Feld unter „Berechtigungen“ vor „Prometheus zulassen“ und klicken Sie auf die Schaltfläche „Weiter“.

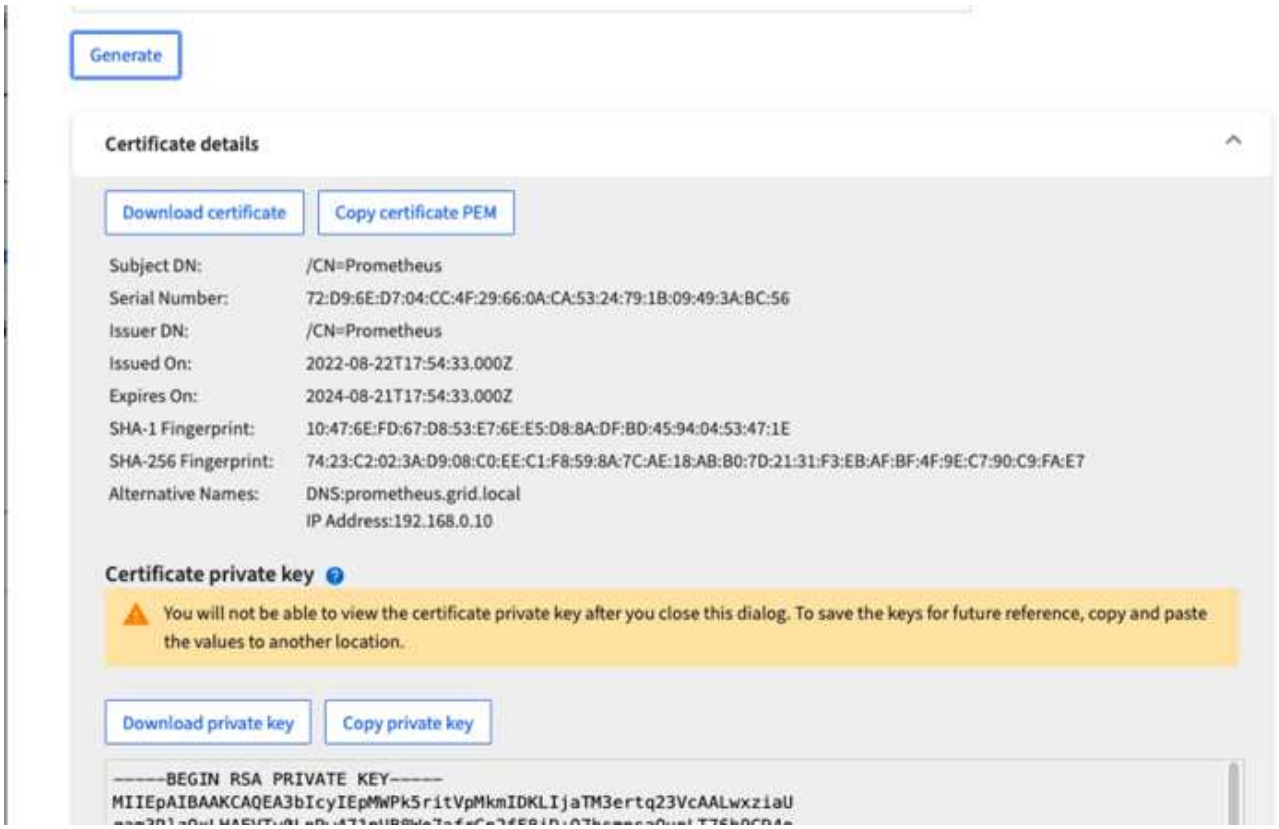


4. Wenn Sie ein CA-signiertes Zertifikat haben, können Sie das Optionsfeld für "Zertifikat hochladen" wählen, aber in unserem Fall werden wir StorageGRID das Client-Zertifikat generieren lassen, indem Sie das Optionsfeld für "Zertifikat generieren". Die Pflichtfelder werden angezeigt, in die ausgefüllt werden soll. Geben Sie den FQDN für den Client-Server, die IP des Servers, den Betreff und die gültigen Tage ein. Dann klicken Sie auf die Schaltfläche „Erzeugen“.



> Be mindful of the certificate days valid entry as you will need to renew this certificate in both StorageGRID and the Prometheus server before it expires to maintain uninterrupted collection.

1. Laden Sie die Pem-Datei des Zertifikats und die Pem-Datei des privaten Schlüssels herunter.



This is the only time you can download the private key, so make sure you do not skip this step.

Bereiten Sie den Linux-Server für die Prometheus-Installation vor

Vor der Installation von Prometheus möchte ich meine Umgebung mit einem Prometheus-Benutzer, der Verzeichnisstruktur vorbereiten und die Kapazität für den Speicherort der Kennzahlen konfigurieren.

1. Erstellen Sie den Prometheus-Benutzer.

```
sudo useradd -M -r -s /bin/false Prometheus
```

2. Erstellen Sie die Verzeichnisse für Prometheus, Clientzertifikat und Kennzahlendaten.

```
sudo mkdir /etc/Prometheus /etc/Prometheus/cert /var/lib/Prometheus
```

3. Ich formatierte die Festplatte, die ich für die Aufbewahrung der Kennzahlen mit einem ext4 Dateisystem verwende.

```
mkfs -t ext4 /dev/sdb
```

4. Ich montierte dann das Dateisystem in das Prometheus-Kennzahlenverzeichnis.

```
sudo mount -t auto /dev/sdb /var/lib/prometheus/
```

5. Holen Sie die UUID der Festplatte, die Sie für Ihre Kennzahlendaten verwenden.

```
sudo ls -al /dev/disk/by-uuid/
   lrwxrwxrwx 1 root root   9 Aug 18 17:02 9af2c5a3-bfc2-4ec1-85d9-
ebab850bb4a1 -> ../../sdb
```

6. Hinzufügen eines Eintrags in /etc/fstab/ das Hinzufügen des Mount bei Neustarts mit der UUID von /dev/sdb.

```
/etc/fstab
UUID=9af2c5a3-bfc2-4ec1-85d9-ebab850bb4a1 /var/lib/prometheus   ext4
defaults    0   0
```

Installation und Konfiguration von Prometheus

Nachdem der Server nun bereit ist, kann ich die Prometheus-Installation starten und den Service konfigurieren.

1. Extrahieren Sie das Prometheus Installationspaket

```
tar xzf prometheus-2.38.0.linux-amd64.tar.gz
```

2. Kopieren Sie die Binärdateien in /usr/local/bin, und ändern Sie das Eigentumsrecht in den zuvor erstellten prometheus-Benutzer

```
sudo cp prometheus-2.38.0.linux-amd64/{prometheus,promtool}
/usr/local/bin
sudo chown prometheus:prometheus /usr/local/bin/{prometheus,promtool}
```

3. Kopieren Sie die Konsolen und Bibliotheken auf /etc/prometheus

```
sudo cp -r prometheus-2.38.0.linux-amd64/{consoles,console_libraries}
/etc/prometheus/
```

4. Kopieren Sie das Clientzertifikat und die pem-Dateien mit privaten Schlüsseln, die zuvor von StorageGRID heruntergeladen wurden, in /etc/prometheus/certs
5. Erstellen Sie die yaml-Konfigurationsdatei für prometheus

```
sudo nano /etc/prometheus/prometheus.yml
```

6. Geben Sie die folgende Konfiguration ein. Der Jobname kann alles sein, was Sie wünschen. Ändern Sie die „-Targets: ['']“ in den FQDN des Admin-Knotens. Wenn Sie die Namen des Zertifikats und der Dateinamen des privaten Schlüssels geändert haben, aktualisieren Sie bitte den abschnitt tls_config, um mit dem Eintrag übereinstimmen. Speichern Sie anschließend die Datei. Wenn Ihre Grid-Management-Schnittstelle ein selbstsigniertes Zertifikat verwendet, laden Sie das Zertifikat herunter und legen Sie es mit dem Clientzertifikat mit einem eindeutigen Namen ab, und fügen Sie im Abschnitt tls_config Ca_file: /Etc/prometheus/cert/UICert.pem hinzu

   a. In diesem Beispiel sammle ich alle Kennzahlen, die mit alertmanager, cassandra, Node und StorageGRID beginnen. Weitere Informationen zu den Prometheus-Kennzahlen finden Sie im "StorageGRID-Dokumentation".

```
# my global config
global:
  scrape_interval: 60s # Set the scrape interval to every 15 seconds.
Default is every 1 minute.

scrape_configs:
  - job_name: 'StorageGRID'
    honor_labels: true
    scheme: https
    metrics_path: /federate
    scrape_interval: 60s
    scrape_timeout: 30s
    tls_config:
      cert_file: /etc/prometheus/cert/certificate.pem
      key_file: /etc/prometheus/cert/private_key.pem
    params:
      match[]:
        -
'{__name__=~"alertmanager_.*|cassandra_.*|node_.*|storagegrid_.*"}'
    static_configs:
    - targets: ['sgdemo-rtp.netapp.com:9091']
```

Wenn Ihre Grid-Managementoberfläche ein selbstsigniertes Zertifikat verwendet, laden Sie das Zertifikat herunter, und legen Sie es mit dem Clientzertifikat mit einem eindeutigen Namen ab. Fügen Sie im Abschnitt tls_config das Zertifikat über dem Clientzertifikat und den privaten Schlüsselzeilen hinzu

```
        ca_file: /etc/prometheus/cert/UIcert.pem
```

1. Ändern Sie das Eigentum aller Dateien und Verzeichnisse in /etc/prometheus und /var/lib/prometheus in den prometheus-Benutzer

```
sudo chown -R prometheus:prometheus /etc/prometheus/
sudo chown -R prometheus:prometheus /var/lib/prometheus/
```

2. Erstellen Sie eine prometheus-Servicedatei in /etc/systemd/System

```
sudo nano /etc/systemd/system/prometheus.service
```

3. Fügen Sie die folgenden Zeilen ein, beachten Sie die --Storage.tsdb.Retention.time=1y, welche die Aufbewahrung der metrischen Daten auf 1 Jahr festlegt. Alternativ können Sie zur Basis-Aufbewahrung auf Storage-Beschränkungen --Storage.tsdb.Retention.size=300gib verwenden. Dies ist der einzige Speicherort, der die Aufbewahrung von Kennzahlen vornimmt.

```
[Unit]
Description=Prometheus Time Series Collection and Processing Server
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
        --config.file /etc/prometheus/prometheus.yml \
        --storage.tsdb.path /var/lib/prometheus/ \
        --storage.tsdb.retention.time=1y \
        --web.console.templates=/etc/prometheus/consoles \
        --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

4. Laden Sie den systemd-Dienst erneut, um den neuen prometheus-Service zu registrieren. Dann starten und aktivieren sie den prometheus Service.

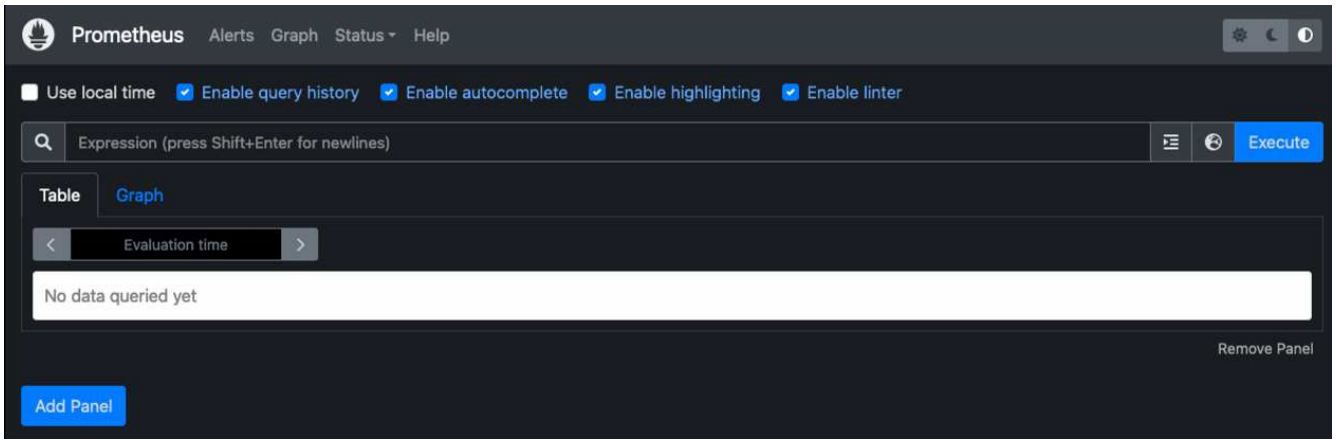
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. Überprüfen Sie, ob der Service ordnungsgemäß läuft

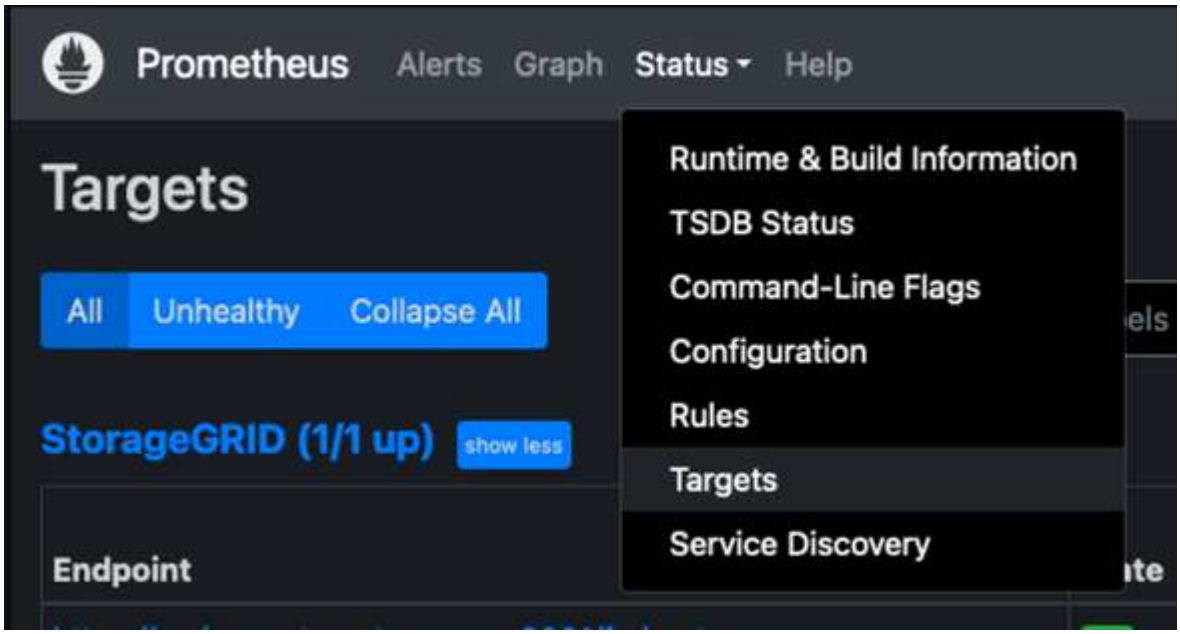
```
sudo systemctl status prometheus
```

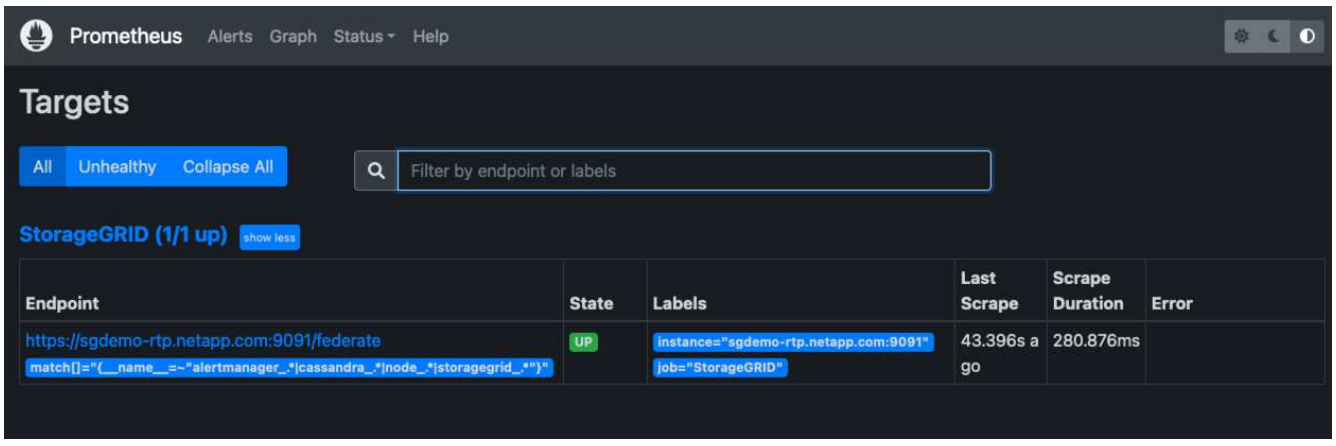
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 28818)
     Memory: 107.7M
        CPU: 1.143s
     CGroup: /system.slice/prometheus.service
             └─6498 /usr/local/bin/prometheus --config.file
/etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
--web.console.templates=/etc/prometheus/consoles --web.con>

Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.510Z caller=head.go:544 level=info component=tsdb
msg="Replaying WAL, this may take a while"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=0 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=1 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:621 level=info component=tsdb msg="WAL
replay completed" checkpoint_replay_duration=55.57µs wal_rep>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:997 level=info fs_type=EXT4_SUPER_MAGIC
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1000 level=info msg="TSDB started"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1181 level=info msg="Loading
configuration file" filename=/etc/prometheus/prometheus.yml
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:1218 level=info msg="Completed loading
of configuration file" filename=/etc/prometheus/prometheus.y>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:961 level=info msg="Server is ready to
receive web requests."
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=manager.go:941 level=info component="rule
manager" msg="Starting rule manager..."
```

6. Sie sollten nun in der Lage sein, auf die Benutzeroberfläche Ihres prometheus-Servers zu navigieren http://Prometheus-server:9090 Und siehe UI

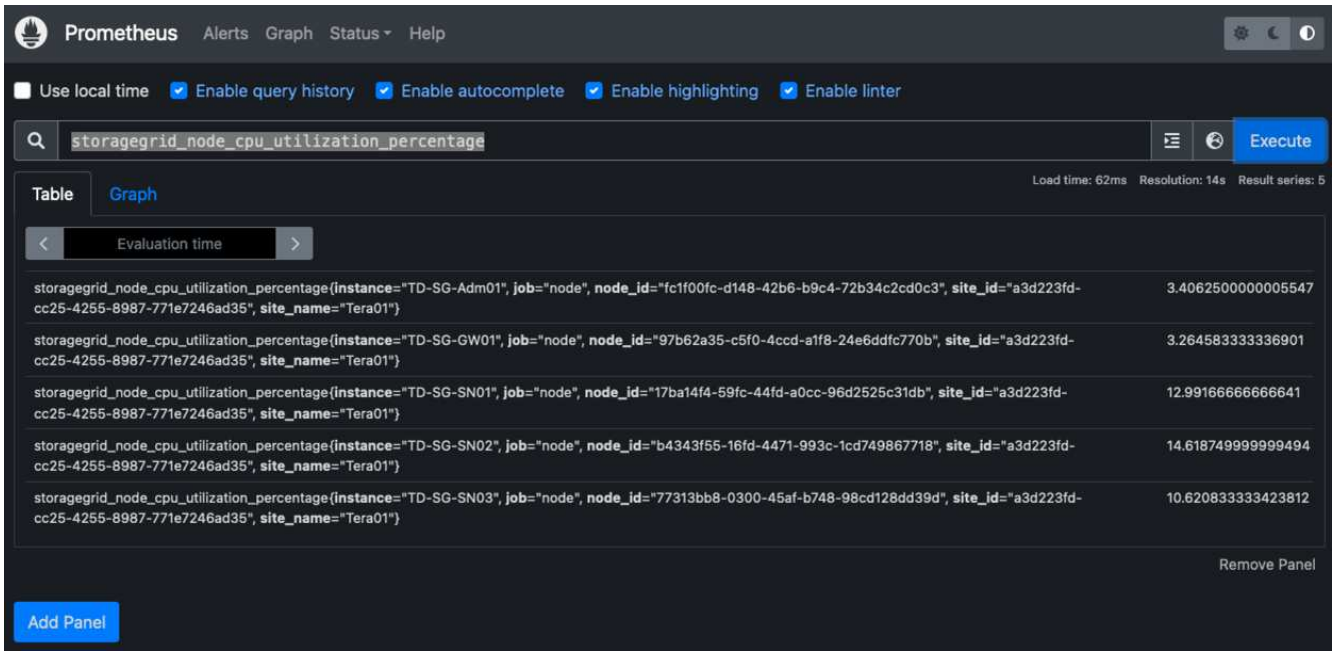


7. Unter "Status" Targets sehen Sie den Status des StorageGRID Endpunkts, den wir in prometheus.yml konfiguriert haben





8. Auf der Seite Diagramm können Sie eine Testabfrage ausführen und überprüfen, ob die Daten erfolgreich abgefangen wurden. Geben Sie beispielsweise „storagegrid_Node_cpu_Utiltiy_percenty“ in die Abfrageleiste ein und klicken Sie auf die Schaltfläche Ausführen.



Installation und Konfiguration von Grafana

Nach der Installation und dem Betrieb von prometheus können wir nun zur Installation von Grafana und zur Konfiguration eines Dashboards wechseln

Grafana-Instalation

1. Installieren Sie die neueste Enterprise Edition von Grafana

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key
https://packages.grafana.com/gpg.key
```

2. Dieses Repository für stabile Versionen hinzufügen:

```
echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://packages.grafana.com/enterprise/deb stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
```

3. Nachdem Sie das Repository hinzugefügt haben.

```
sudo apt-get update
sudo apt-get install grafana-enterprise
```

4. Laden Sie den systemd-Dienst neu, um den neuen grafana-Dienst zu registrieren. Starten und aktivieren Sie dann den Grafana-Service.

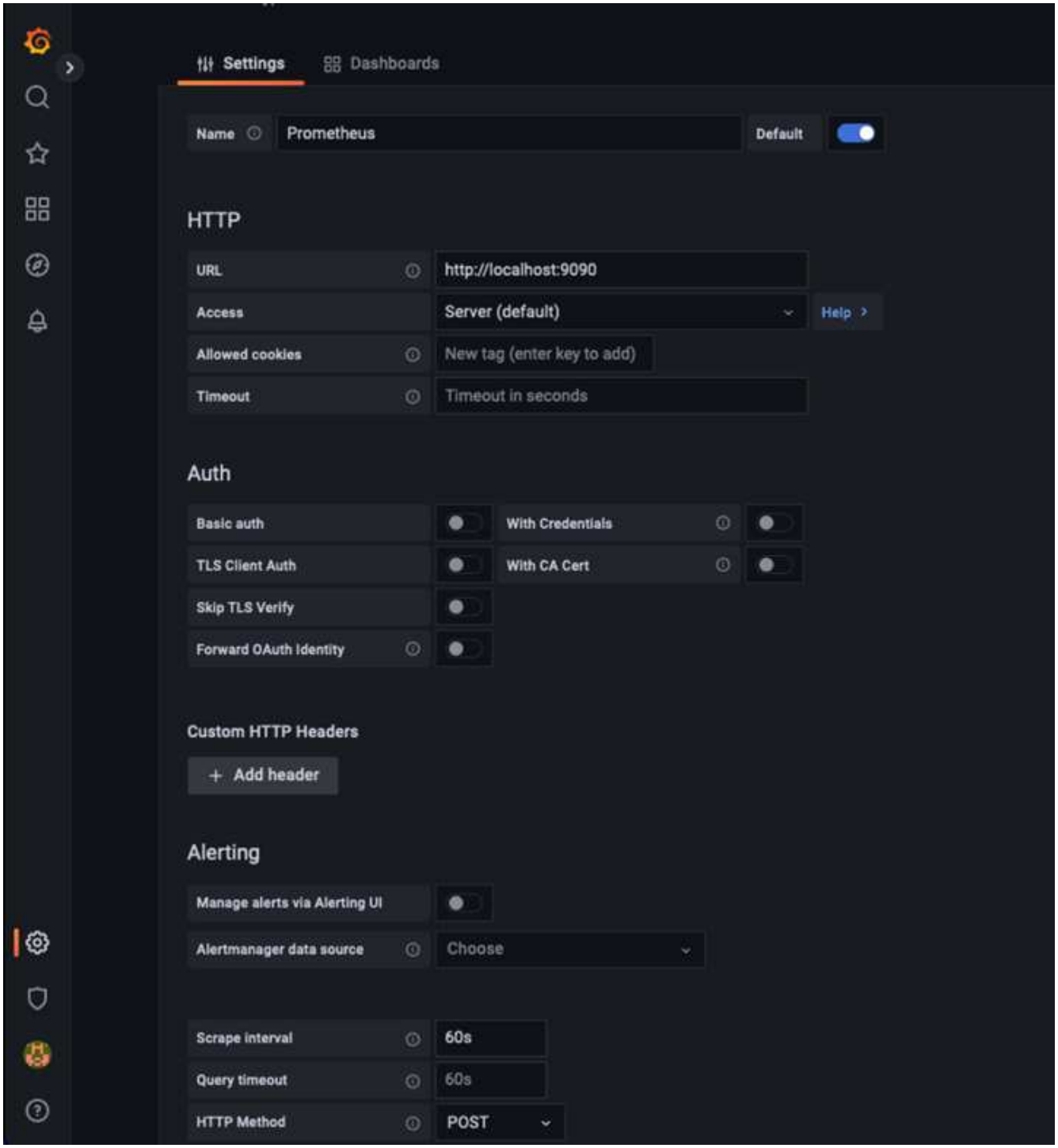
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafana wird jetzt installiert und ausgeführt. Wenn Sie einen Browser zu HTTP://Prometheus-Server:3000 öffnen, werden Sie mit der Grafana-Anmeldeseite begrüßt.
6. Die Standard-Anmeldeinformationen sind admin/admin. Sie sollten ein neues Passwort festlegen, wenn Sie dazu aufgefordert werden.

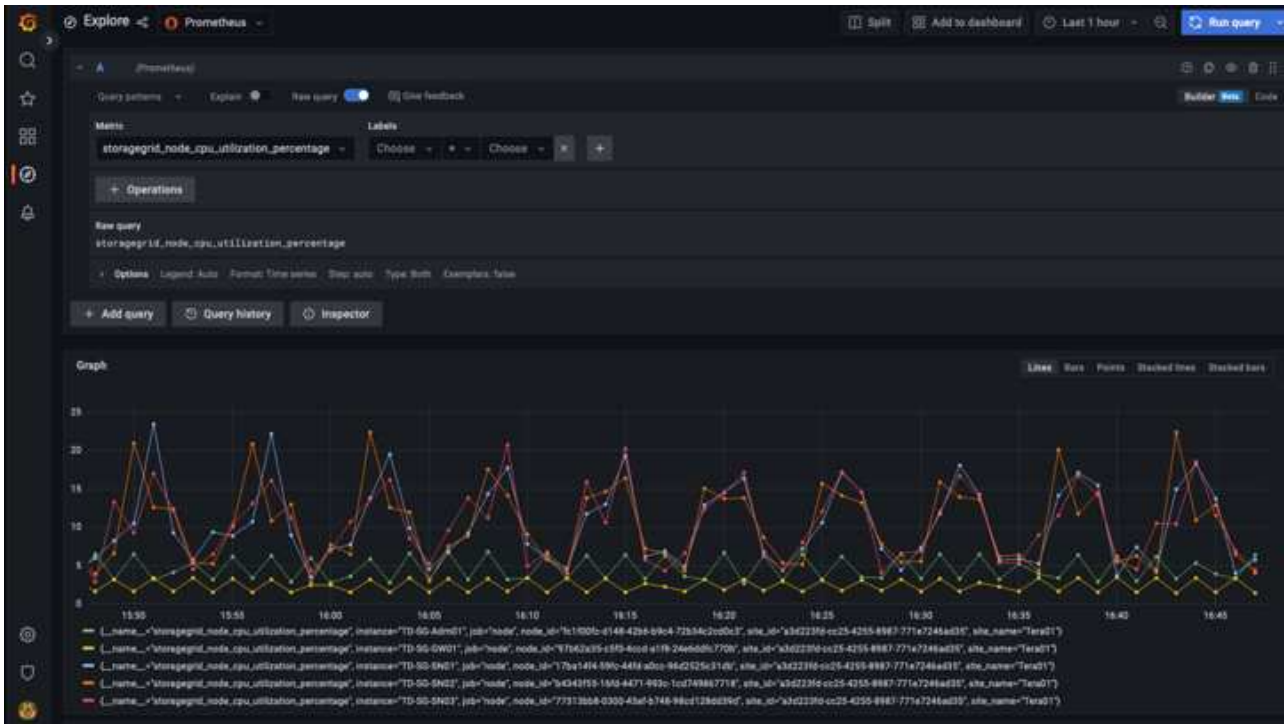
Erstellen eines Grafana Dashboards für StorageGRID

Mit der Installation und dem Betrieb von Grafana und Prometheus ist es jetzt an der Zeit, beide zu verbinden. Dazu wird eine Datenquelle erstellt und ein Dashboard erstellt

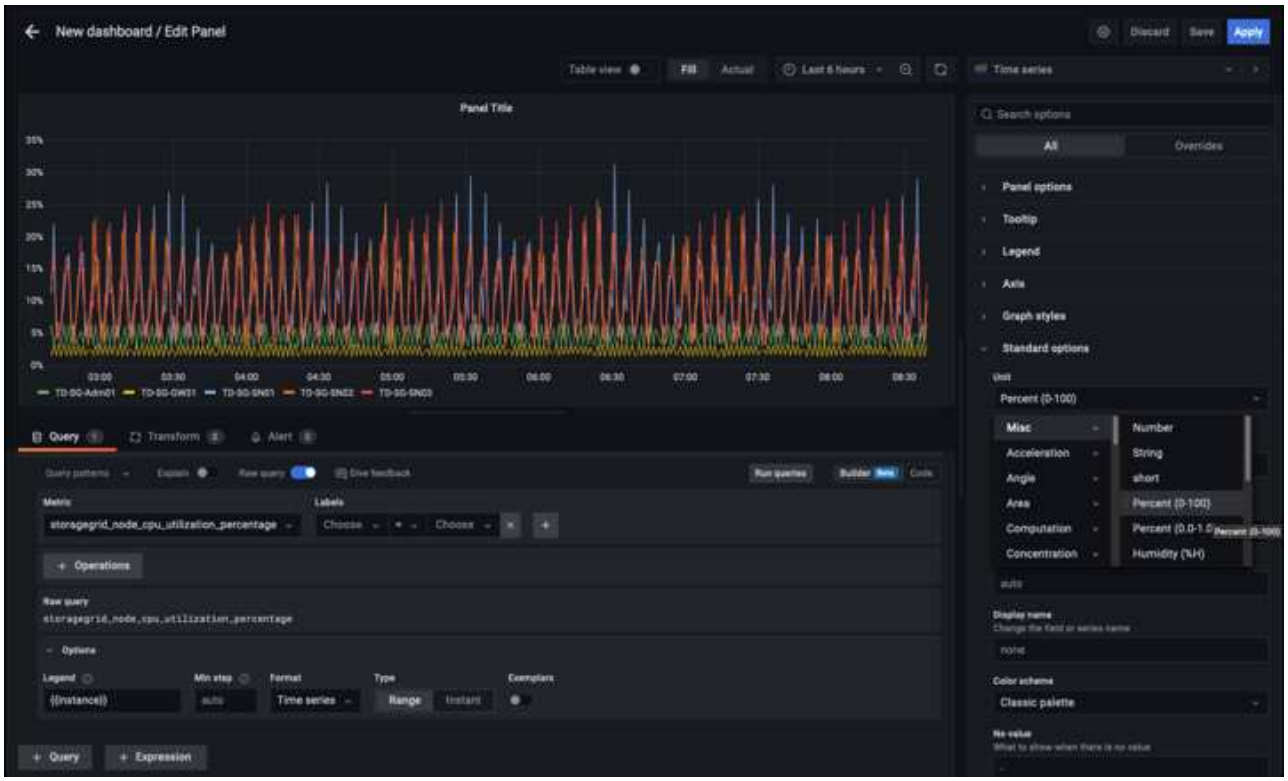
1. Erweitern Sie im linken Fensterbereich „Konfiguration“ und wählen Sie „Datenquellen“, und klicken Sie dann auf die Schaltfläche „Datenquelle hinzufügen“
2. Prometheus wird eine der wichtigsten Datenquellen zur Auswahl sein. Wenn nicht, dann verwenden Sie die Suchleiste zu finden "Prometheus"
3. Konfigurieren Sie die Prometheus-Quelle, indem Sie die URL der prometheus-Instanz und das Scrape-Intervall eingeben, um das Prometheus-Intervall zu entsprechen. Ich habe auch den Abschnitt „Warnungen“ deaktiviert, da ich den Alarmmanager auf prometheus nicht konfiguriert habe.



4. Blättern Sie nach unten, und klicken Sie auf „Speichern & Testen“, wenn Sie die gewünschten Einstellungen eingegeben haben.
5. Nachdem der Konfigurationstest erfolgreich abgeschlossen wurde, klicken Sie auf die Schaltfläche Explore.
   a. Im Erkundungs-Fenster können Sie die gleiche Metrik verwenden, die wir Prometheus mit „storagegrid_Node_cpu_Utifficienty_percenty“ getestet haben, und auf die Schaltfläche „Run query“ klicken



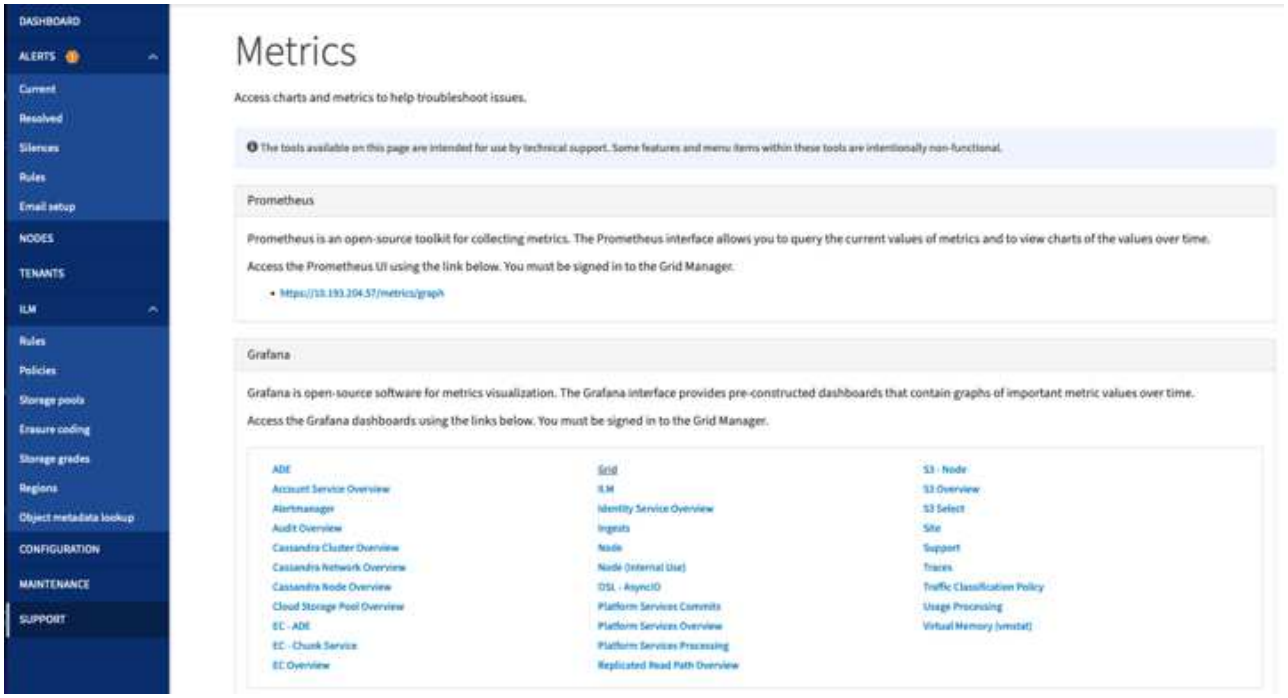
6. Nachdem die Datenquelle konfiguriert ist, können wir jetzt ein Dashboard erstellen.
   a. Erweitern Sie im linken Fensterbereich „Dashboards“ und wählen Sie „+ neues Dashboard“ aus.
   b. Wählen Sie „Neues Bedienfeld hinzufügen“ aus.
   c. Konfigurieren Sie das neue Panel durch Auswahl einer Metrik, wieder werde ich "storagegrid_Node_cpu_Utilement_percenty" verwenden, einen Titel für das Panel eingeben, unten "Optionen" erweitern und für Legende ändern zu Custom und geben Sie "{{instance}}" ein, um die Knotennamen zu definieren, und im rechten Fensterbereich unter "Standardoptionen" setzen "Einheit" auf "Misc/Prozent(0-100)". Klicken Sie dann auf „Übernehmen“, um das Panel im Dashboard zu speichern.



7. Wir könnten unser Dashboard für jede gewünschte Metrik weiter ausbauen, aber glücklicherweise verfügt StorageGRID bereits über Dashboards mit Panels, die wir in unsere benutzerdefinierten Dashboards kopieren können.

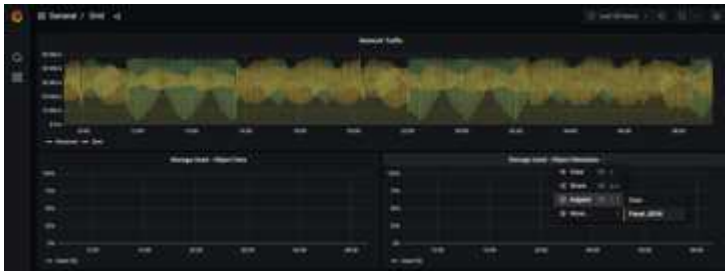
   a. Wählen Sie im linken Fensterbereich der StorageGRID-Managementoberfläche „Support“ und klicken Sie unten in der Spalte „Tools“ auf „Metriken“.

   b. Innerhalb von Kennzahlen wähle ich den Link „Grid“ oben in der mittleren Spalte aus.



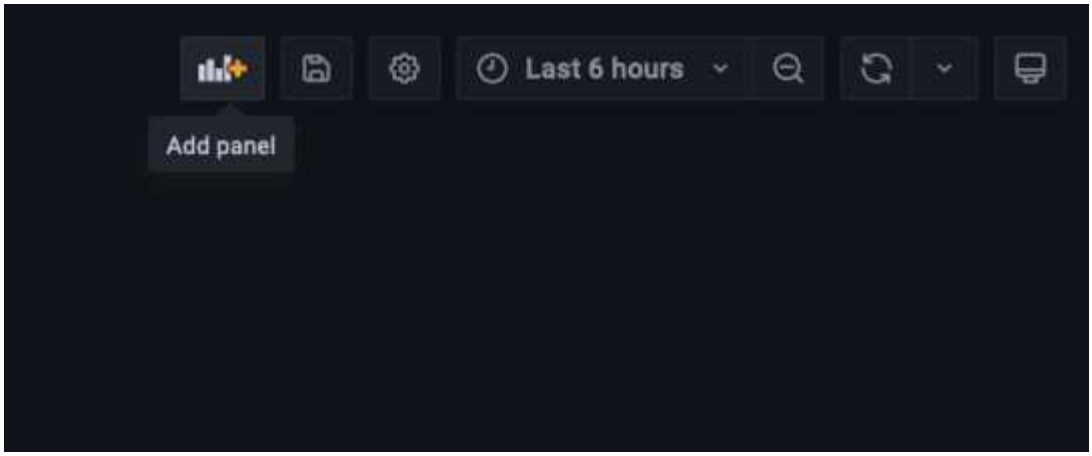
   c. Wählen Sie im Grid-Dashboard den Bereich „Storage Used - Object Metadata“ aus. Klicken Sie auf

den kleinen Pfeil nach unten und auf das Ende des Bedienfeldtitels, um ein Menü zu öffnen. Wählen Sie in diesem Menü „Inspect“ und „Panel JSON“ aus.



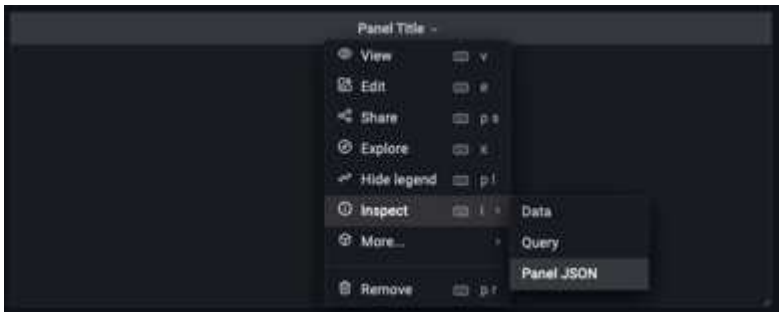
d. Kopieren Sie den JSON-Code und schließen Sie das Fenster.

e. Klicken Sie in unserem neuen Dashboard auf das Symbol, um ein neues Panel hinzuzufügen.

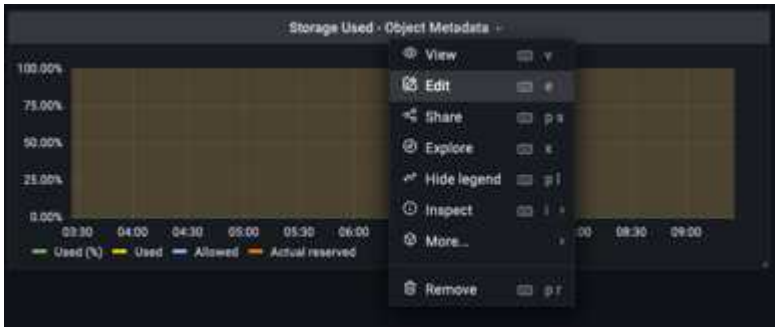


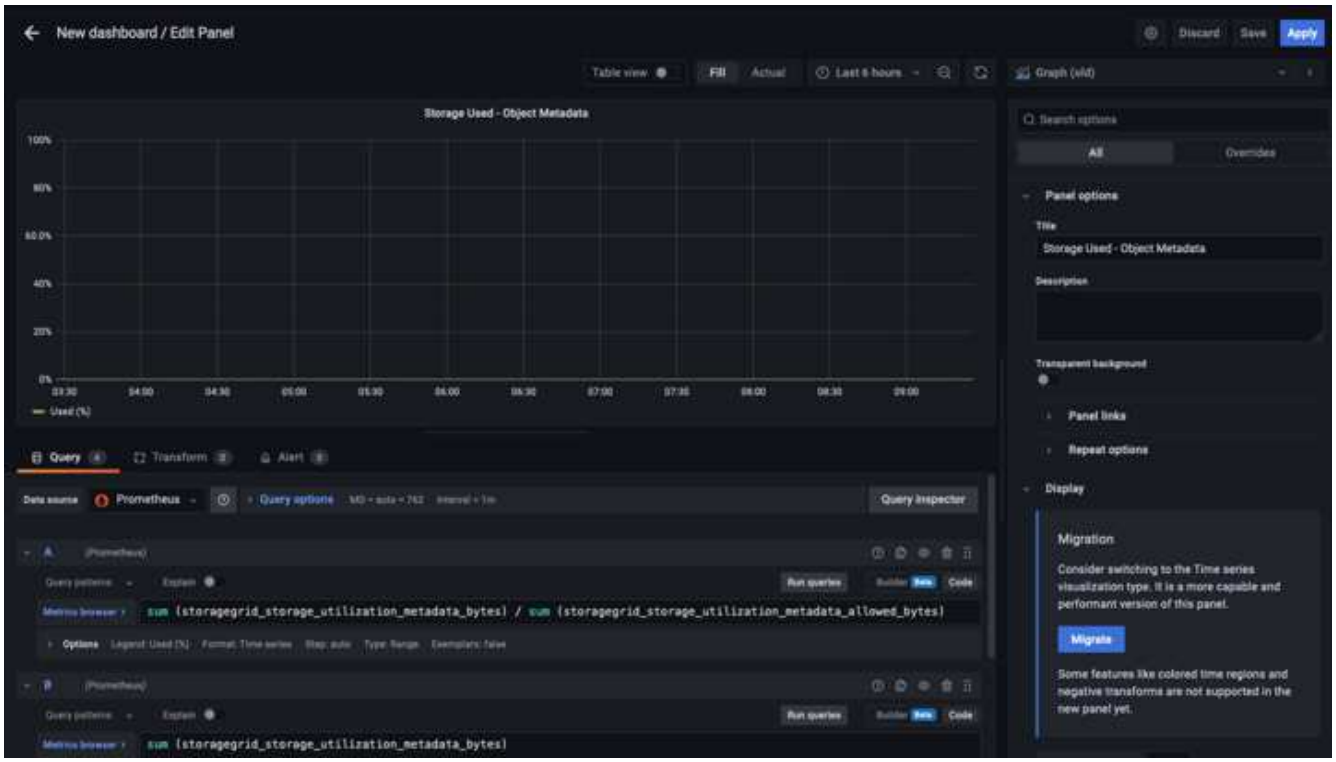
f. Wenden Sie das neue Bedienfeld an, ohne Änderungen vorzunehmen

g. Wie bei dem StorageGRID-Panel sollten Sie auch die JSON überprüfen. Entfernen Sie den gesamten JSON-Code, und ersetzen Sie ihn durch den kopierten Code aus dem StorageGRID-Fenster.



h. Bearbeiten Sie das neue Bedienfeld, und auf der rechten Seite sehen Sie eine Migrationsmeldung mit einem "Migrate"-Button. Klicken Sie auf die Schaltfläche und dann auf die Schaltfläche „Übernehmen“.





8. Sobald Sie alle Panels eingerichtet und so konfiguriert haben, wie Sie möchten. Speichern Sie das Dashboard, indem Sie oben rechts auf das Festplatten-Symbol klicken und Ihrem Dashboard einen Namen geben.

Schlussfolgerung

Jetzt verfügen wir über einen Prometheus Server mit anpassbarer Datenaufbewahrung und Storage-Kapazität. Damit können wir unsere eigenen Dashboards mit den für unsere Betriebsabläufe wichtigsten Kennzahlen weiterentwickeln. Weitere Informationen zu den in der erfassten Prometheus-Kennzahlen finden Sie unter "StorageGRID-Dokumentation".

Verwenden Sie F5 DNS für den globalen Lastausgleich von StorageGRID.

Von Steve Gorman (F5)

Dieser technische Bericht enthält detaillierte Anweisungen zur Konfiguration von NetApp StorageGRID mit F5 DNS-Diensten für den globalen Lastausgleich, um eine bessere Datenverfügbarkeit und höhere Datenkonsistenz zu erreichen sowie das S3-Transaktionsrouting zu optimieren, wenn Ihr Grid über mehrere Standorte und/oder HA-Gruppen verteilt ist.

Einführung

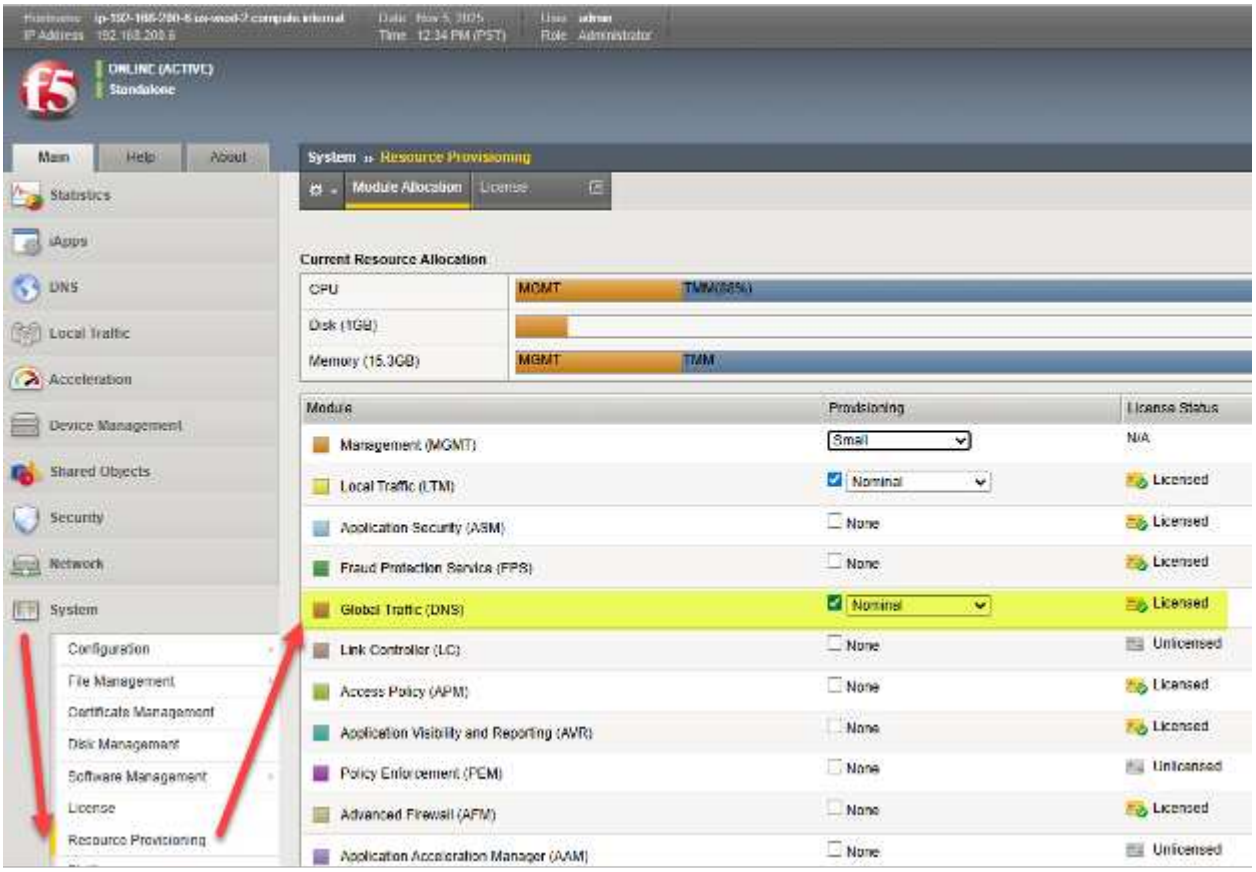
Die F5 BIG-IP DNS-Lösung, die früher BIG-IP GTM (Global Traffic Manager) und informell GSLB (Global Server Load Balancing) genannt wurde, ermöglicht einen nahtlosen Zugriff über mehrere aktive HA-Gruppen und aktive, standortübergreifende StorageGRID Lösungen hinweg.

F5 BIG-IP Multi-Site StorageGRID -Konfiguration

Unabhängig von der Anzahl der zu unterstützenden StorageGRID Standorte müssen mindestens zwei BIG-IP-Appliances, physisch oder virtuell, über das aktivierte und eingerichtete BIG-IP-DNS-Modul verfügen. Je mehr DNS-Appliances, desto größer ist der Grad an Redundanz, von dem ein Unternehmen profitiert.

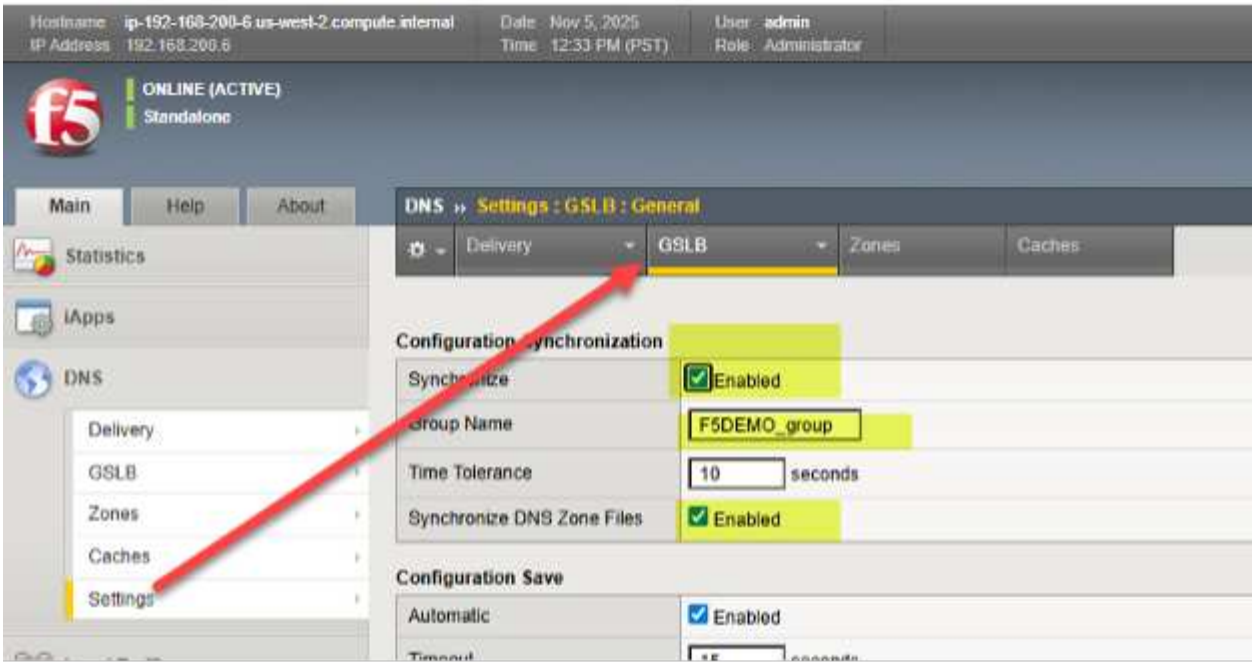
BIG-IP DNS – Erste Schritte bei der Ersteinrichtung

Sobald die BIG-IP-Appliance mindestens initial provisioniert wurde, verwenden Sie einen Webbrowser, um sich in die TMUI (BIG-IP GUI)-Oberfläche einzuloggen und wählen Sie System → Ressourcenbereitstellung. Wie bereits erwähnt, muss sichergestellt werden, dass das Modul „Global Traffic (DNS)“ ein Häkchen aufweist und als lizenziert angezeigt wird. Beachten Sie, dass es, wie im Bild dargestellt, üblich ist, dass „Local Traffic (LTM)“ auf demselben Gerät bereitgestellt werden kann.

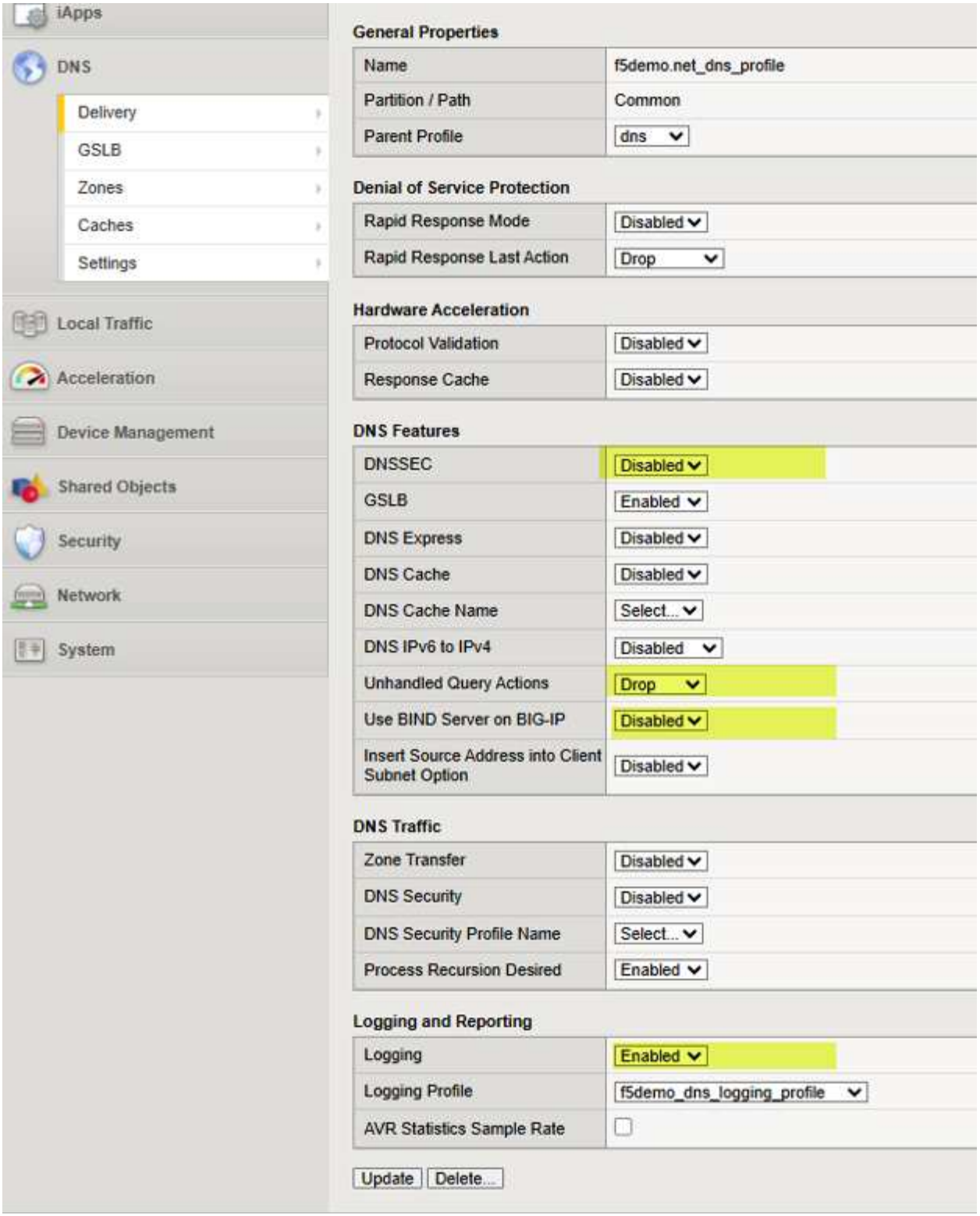


DNS-Protokoll-Grundelemente konfigurieren

Der erste Schritt zur globalen Verkehrssteuerung für StorageGRID -Sites besteht darin, die Registerkarte DNS auszuwählen, wo praktisch die gesamte globale Verkehrssteuerung konfiguriert wird, und dann Einstellungen→ GLSB auszuwählen. Aktivieren Sie die beiden Synchronisierungsoptionen und wählen Sie einen DNS-Gruppennamen, der von allen teilnehmenden BIG-IP-Appliances gemeinsam genutzt werden soll.



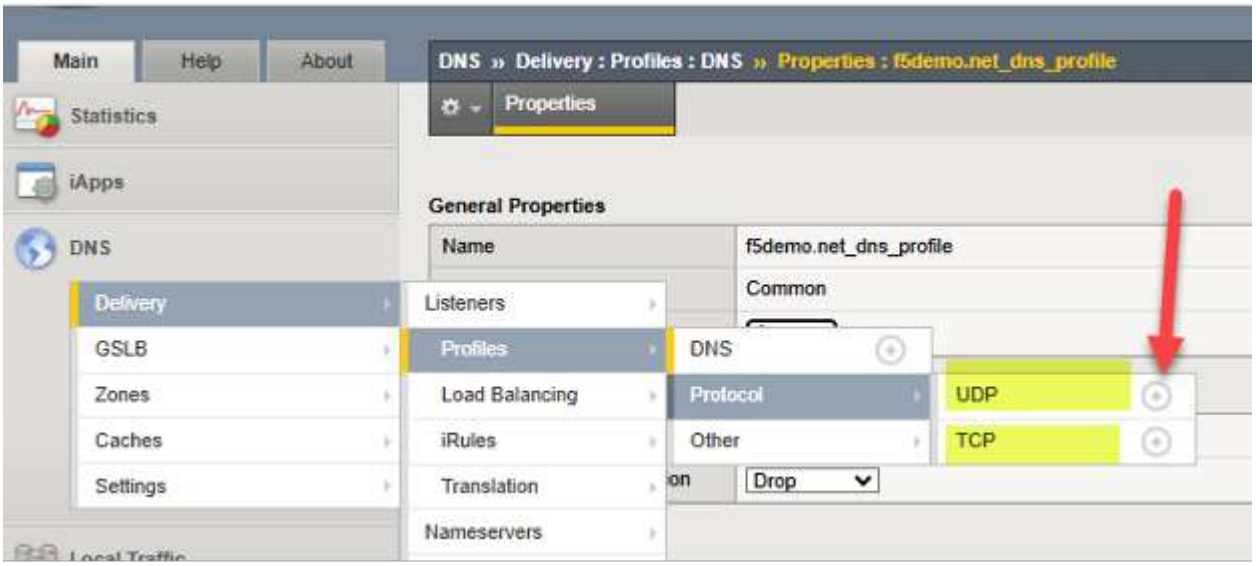
Navigieren Sie anschließend zu DNS > Zustellung > Profile > DNS: Erstellen und erstellen Sie ein Profil, das die DNS-Funktionen steuert, die Sie aktivieren oder deaktivieren möchten. Wenn Sie an der Generierung spezifischer DNS-Protokolle interessiert sind, finden Sie den vorherigen Link zum DNS-Schulungsleitfaden. Hier ist ein Beispiel für ein funktionierendes DNS-Profil. Beachten Sie die vier Hervorhebungen, die wichtige Werte für die Einstellungen darstellen. Zur Verdeutlichung wird jede mögliche Einstellung im folgenden F5 KB-Artikel (Wissensdatenbank) erläutert. "Hier"Die



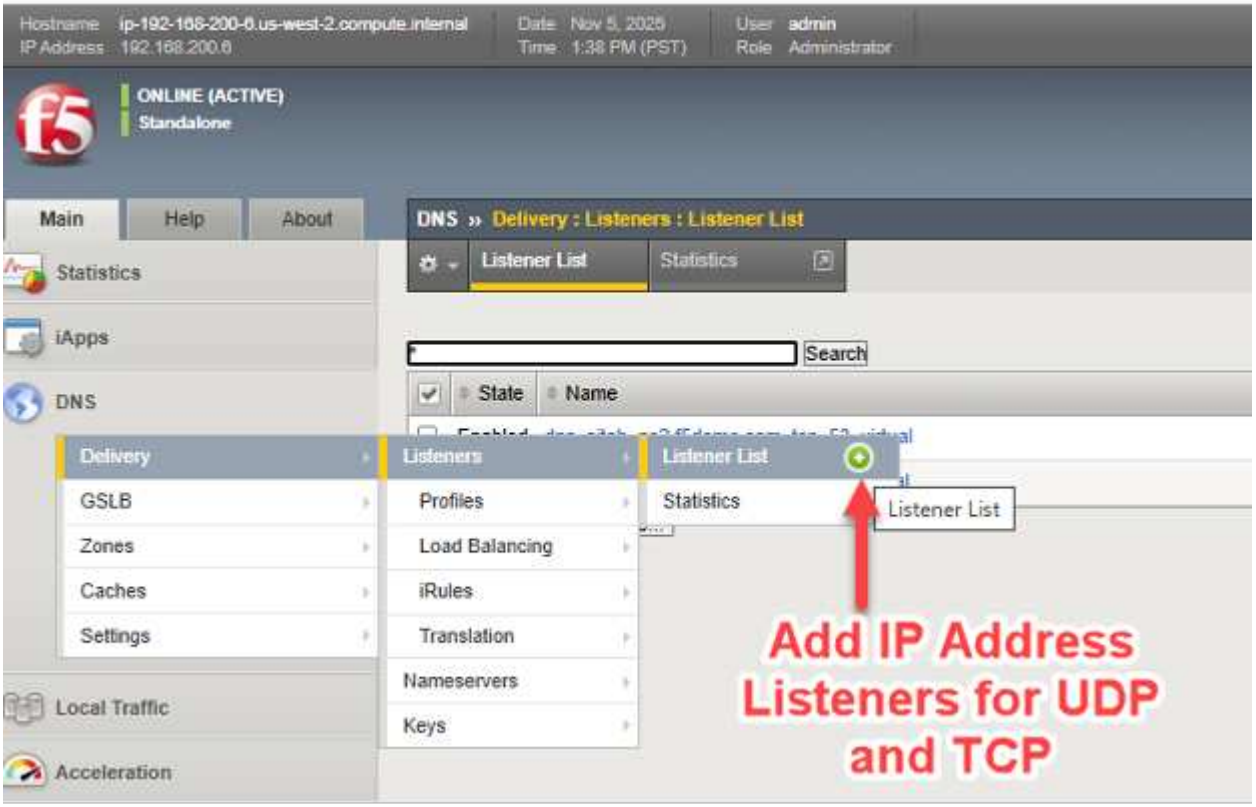
An dieser Stelle können wir die Eigenschaften der UDP- und TCP-Protokolle über erstellte „Profile“ anpassen, die beide DNS-Verkehr mit BIG-IP übertragen können. Erstellen Sie einfach ein neues Profil für UDP und TCP. Unter der Annahme, dass der DNS-Datenverkehr WAN-Verbindungen durchläuft, ist es eine gute Vorgehensweise, einfach die UDP- und TCP-Eigenschaften zu übernehmen, die bekanntermaßen in WAN-Umgebungen gut funktionieren. Um ein Protokoll hinzuzufügen, klicken Sie einfach auf das „+“-Symbol neben dem jeweiligen Protokoll und legen Sie das übergeordnete Profil wie folgt fest:

UDP → Verwende das „übergeordnete“ Profil „udp_gtm_dns“

TCP → Verwenden Sie das „übergeordnete“ Profil „f5-tcp-wan“

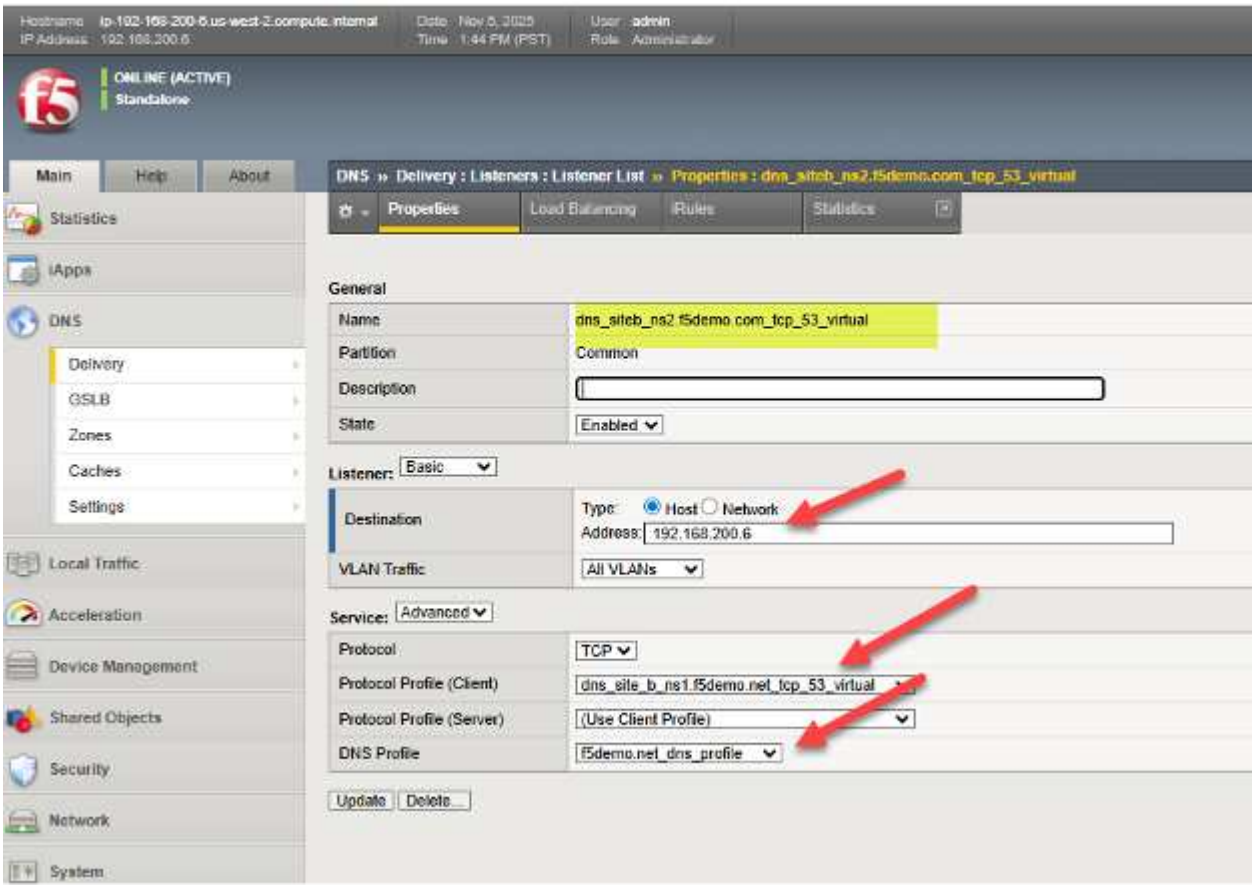


Jetzt müssen wir nur noch dem BIG-IP DNS eine IP-Adresse für den UDP- und TCP-Datenverkehr zuweisen. Für diejenigen, die mit BIG-IP LTM vertraut sind, handelt es sich im Wesentlichen um die Erstellung virtueller DNS-Server, und virtuelle Server benötigen „Listener“-IP-Adressen. Folgen Sie, wie im Screenshot dargestellt, den Pfeilen, um Listener/virtuelle Server für DNS/UDP und DNS/TCP zu erstellen.



Nachfolgend ein Beispiel aus einem laufenden BIG-IP DNS-System. Darin sehen wir die Einstellungen des virtuellen TCP-Server-Listeners und können erkennen, wie viele der vorherigen Schritte miteinander verknüpft sind. Dies umfasst das Referenzieren des DNS-Profils und des Protokollprofils (TCP) sowie die Konfiguration einer gültigen IP-Adresse für die Verwendung durch DNS. Wie bei allen Objekten, die man mit BIG-IP erstellt, ist es hilfreich, einen aussagekräftigen Namen zu verwenden, der dazu dient, das Objekt selbst zu

identifizieren, wie zum Beispiel dns/siteb/TCP53 im zugewiesenen Beispielnamen.



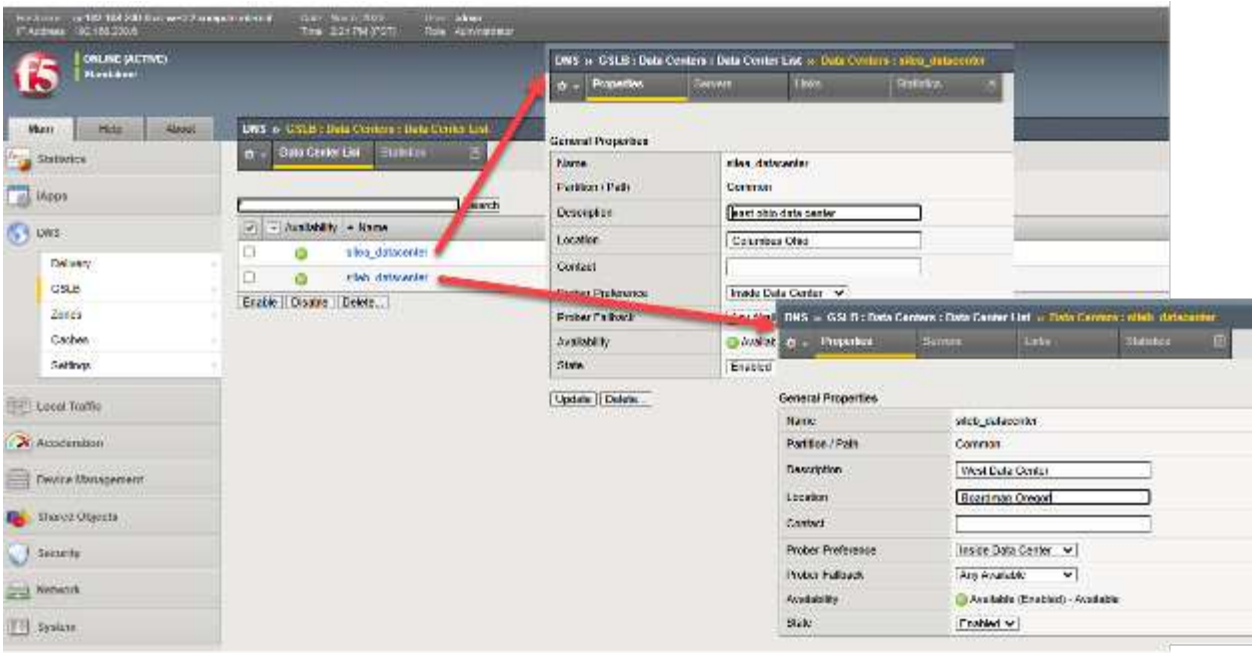
Hiermit sind die vorbereitenden, in der Regel einmaligen Einrichtungsschritte einer BIG-IP-Appliance mit aktiviertem DNS-Modul abgeschlossen. An diesem Punkt sind wir bereit, uns den Details der Einrichtung einer globalen Traffic-Management-Lösung mit unseren Appliances zuzuwenden, die selbstverständlich mit den Eigenschaften der StorageGRID Standorte verknüpft sein wird.

Einrichtung von Rechenzentrumsstandorten und Etablierung der Inter-BIG-IP-Kommunikation in vier Schritten

Schritt eins: Rechenzentren erstellen

Jeder Standort, der Cluster von Knoten beherbergen soll, die lokal von BIG-IP LTM lastverteilt werden sollen, muss in BIG-IP DNS eingetragen werden. Dies muss nur auf einem BIG-IP DNS-Server erfolgen, da wir eine DNS-synchronisierte Gruppe zur Unterstützung des Traffic-Managements erstellen. Daher wird diese Konfiguration von allen DNS-Mitgliedern der Gruppe gemeinsam genutzt.

Wählen Sie über die TMUI-Benutzeroberfläche DNS > GSLB > Rechenzentren > Rechenzentrumsliste und erstellen Sie einen Eintrag für jeden StorageGRID Standort. Bei Verwendung eines Netzwerkaufbaus gemäß Abbildung 1 und DNS-Appliances an anderen Standorten als StorageGRID müssen zusätzlich zu den Speicherstandorten auch Rechenzentren für diese Standorte hinzugefügt werden. In diesem Beispiel werden die Standorte a und b in Ohio und Oregon erstellt, die BIG-IPs sind Dual-DNS- und LTM-Appliances.



Schritt zwei: Server erstellen (Liste aller BIG-IP-Appliances in der Lösung)

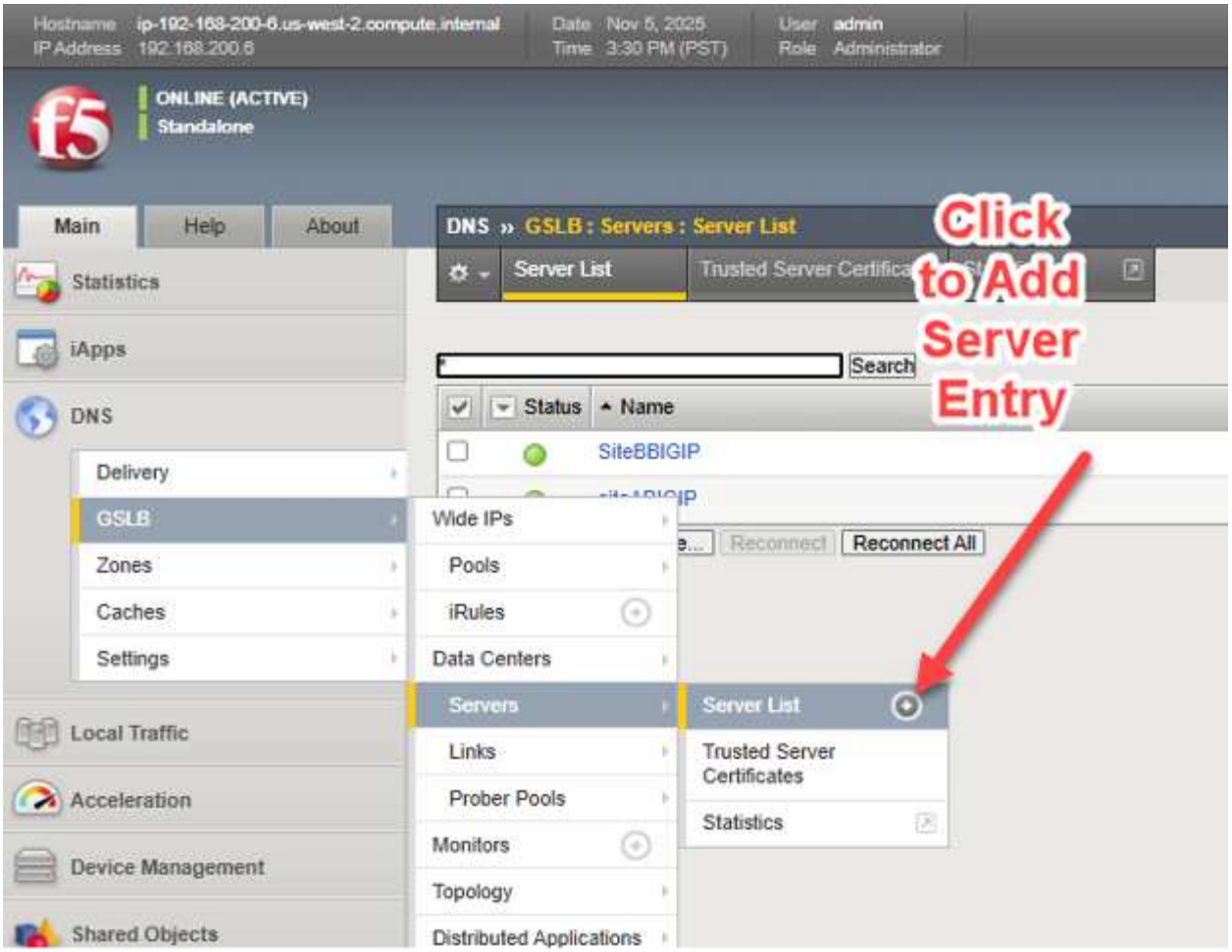
Wir sind nun bereit, die einzelnen StorageGRID Standortcluster mit der BIG-IP-DNS-Konfiguration zu verbinden. Zur Erinnerung: Die BIG-IP-Appliance an jedem Standort übernimmt den eigentlichen Lastausgleich des S3-Datenverkehrs durch die Konfiguration virtueller Server, die eine erreichbare IP-Adresse/einen Port des „Front-Ends“ mit einem Satz von Back-End-„Pools“ von Storage Node-Appliances verbinden, wobei „Back-End“-IP-Adressen/Ports verwendet werden.

Sollten beispielsweise alle Speicherknoten in einem Pool aus administrativen Gründen offline genommen werden, etwa wegen der Stilllegung eines Standorts, oder unerwartet aufgrund fehlgeschlagener Echtzeit-Zustandsprüfungen, wird der Datenverkehr durch Änderung der DNS-Abfrageantworten auf andere Standorte umgeleitet.

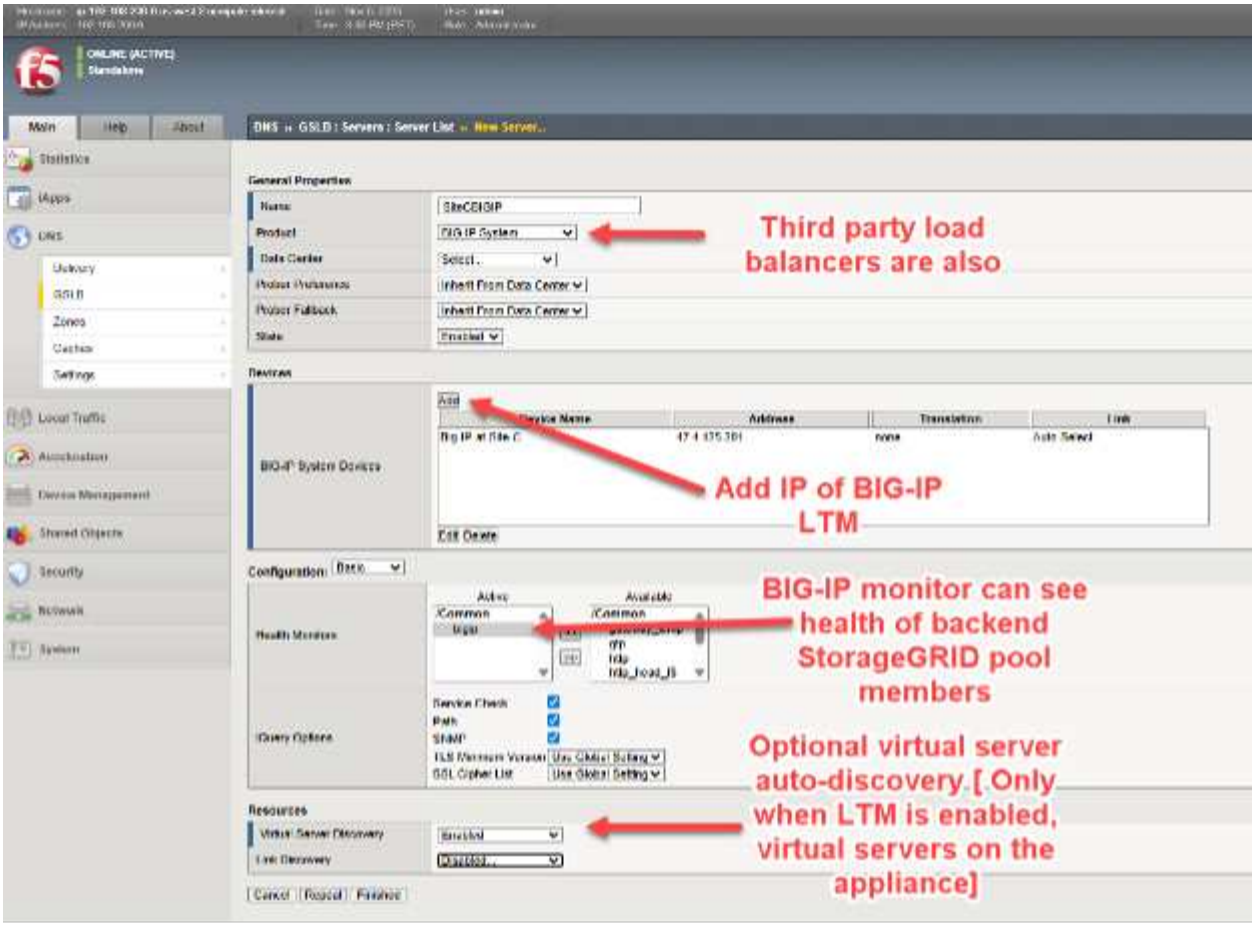
Um die StorageGrid-Sites, insbesondere die lokalen virtuellen Server, mit der BIG-IP-DNS-Konfiguration auf jedem Gerät zu verknüpfen, muss die Einrichtung nur einmal durchgeführt werden. In einem nächsten Schritt werden die Konfigurationen aller BIG-IP DNS-Geräte synchronisiert.

Vereinfacht ausgedrückt erstellen wir eine Liste, die als Serverliste bezeichnet wird, aller unserer BIG-IP-Appliances, unabhängig davon, ob sie für DNS, LTM oder sowohl DNS als auch LTM lizenziert sind. Diese Masterliste wird nach Fertigstellung der Liste mit allen BIG-IP DNS-Appliances synchronisiert.

Auf einem BIG-IP DNS-lizenzierten Gerät wählen Sie DNS > GSLB > Server > Serverliste und klicken Sie auf die Schaltfläche "Hinzufügen" (+).



Zu den vier wichtigsten Elementen beim Hinzufügen jedes BIG-IP gehören: * Die Auswahl von BIG-IP aus dem Produkt-Dropdown-Menü; andere Load Balancer sind zwar möglich, bieten aber im Allgemeinen nicht die Echtzeit-Transparenz und Reaktionsfähigkeit, wenn sich der Zustand der Backend-Knoten an den einzelnen Standorten verschlechtert. * Fügen Sie die IP-Adresse der BIG-IP DNS-Appliance hinzu. Beim erstmaligen Hinzufügen einer BIG-IP DNS-Appliance wird wahrscheinlich die Adresse der aktuell über die grafische Benutzeroberfläche aufgerufenen Appliance verwendet; zukünftige Appliances werden die Adressen der anderen Appliances in der Lösung verwenden. * Wählen Sie einen Health Monitor aus. Verwenden Sie immer „BIG-IP“, wenn der hinzuzufügende Load Balancer eine BIG-IP Appliance ist, um den Zustand der StorageGRID Knoten im Backend zu berücksichtigen. * Optional kann die automatische Erkennung virtueller Server angefordert werden, wenn es sich bei dem Gerät um ein Dual-DNS/LTM-Gerät handelt.

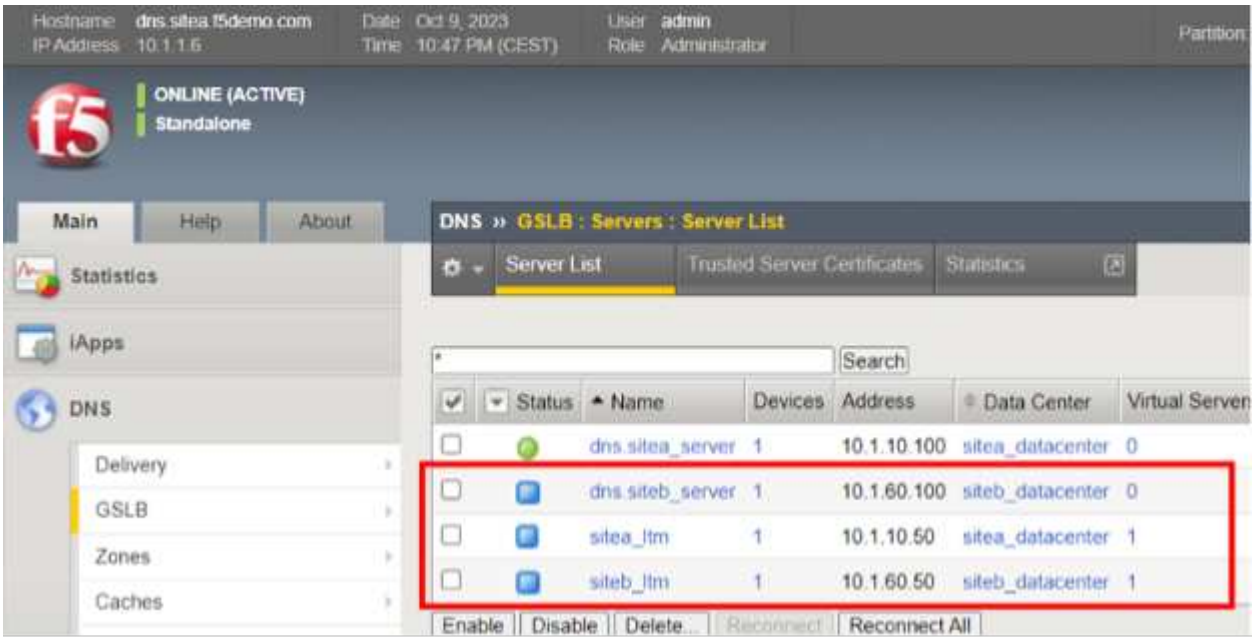


In bestimmten Situationen, wie z. B. bei vorübergehenden Netzwerkproblemen oder Firewall-ACL-Regeln zwischen Netzwerkstandorten, werden bei der Hinzufügung einer Remote-Appliance in diesem Stadium möglicherweise keine Einträge für Remote-Appliances mit konfiguriertem LTM bei der virtuellen Servererkennung angezeigt. In solchen Fällen können nach dem Hinzufügen des neuen Geräts („Servers“) die virtuellen Server wie unten angegeben manuell hinzugefügt werden. Wenn Sie eine reine BIG-IP-DNS-Appliance hinzufügen, werden keine virtuellen Server erkannt oder diesem Gerät hinzugefügt.

Wir müssen diese Servereinträge für jedes Gerät in unserer Lösung an allen Standorten hinzufügen, einschließlich BIG-IP DNS-Geräte, BIG-IP LTM-Geräte und aller Geräte, die die Doppelrolle sowohl als DNS- als auch als LTM-Einheiten übernehmen.

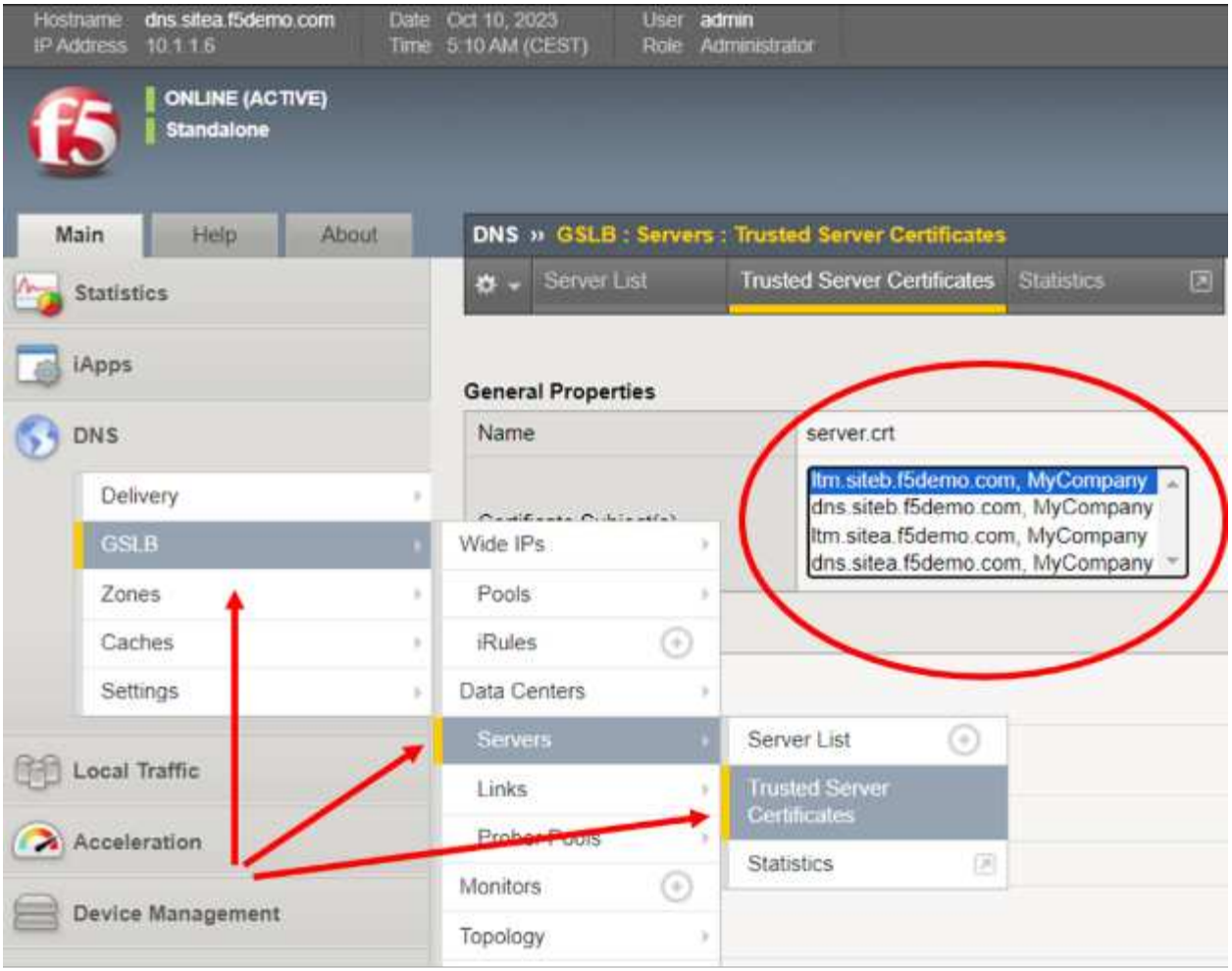
Schritt drei: Vertrauensverhältnis zwischen allen BIG-IP-Appliances herstellen

Im folgenden Beispiel wurden vier Appliances als Server hinzugefügt; sie sind auf zwei Standorte verteilt. Beachten Sie, dass jeder Standort über einen eigenen BIG-IP DNS-Server und BIG-IP LTM verfügt. Allerdings werden bei allen Geräten außer dem aktuell angemeldeten Gerät blaue Symbole in der Spalte „Status“ angezeigt. Dies bedeutet, dass noch keine Vertrauensbeziehung zu den anderen BIG-IP-Appliances hergestellt wurde.



Um Vertrauen zu schaffen, stellen Sie eine SSH-Verbindung zum BIG-IP her, auf dem die Konfigurationsdetails soeben über die GUI eingegeben wurden, und verwenden Sie das Konto „root“, um auf die BIG-IP-Befehlszeilenschnittstelle zuzugreifen. Geben Sie an der Eingabeaufforderung folgenden einzelnen Befehl ein: *bigip_add*

Der Befehl „bigip_add“ lädt das Verwaltungszertifikat von den Ziel-BIG-IP-Geräten herunter, um es beim Aufbau des verschlüsselten „iQuery“-Kanals zwischen den GSLB-Servern im Cluster zu verwenden. iQuery läuft standardmäßig über TCP-Port 4353 und dient als Heartbeat, um die Synchronisierung der BOG-IP-DNS-Mitglieder zu gewährleisten. Es verwendet XML und Gzip im verschlüsselten Kanal. Wenn "bigip_add" ohne Optionen ausgeführt wird, wird der Befehl für alle BIGIP-Geräte in der GSLB-Serverliste ausgeführt, wobei der aktuelle Benutzername verwendet wird, um eine Verbindung zu den Endpunkten herzustellen. Um den Erfolg schnell zu überprüfen, kehren Sie einfach zur BIG-IP-Benutzeroberfläche zurück und vergewissern Sie sich, dass alle Server nun Zertifikate im angezeigten Dropdown-Menü aufweisen.



Schritt vier: Synchronisieren Sie alle BIG-IP DNS-Appliances mit der DNS-Gruppe

Im letzten Schritt können alle BIG-IP DNS-Appliances vollständig über die TMUI-Benutzeroberfläche eines einzigen Geräts konfiguriert werden. In einem Beispiel, in dem es zwei StorageGRID Standorte gibt, bedeutet dies, dass man nun per SSH auf die Befehlszeile des BIG-IP-DNS des **anderen** Standorts zugreifen muss. Nachdem Sie sich als Root angemeldet und sichergestellt haben, dass die Firewall-Richtlinien/ACLs die Kommunikation der beiden BIG-IP-DNS-Geräte über die TCP-Ports 22 (SSH), 443 (HTTPS) und 4354 (F5 iQuery-Protokoll) erlauben, geben Sie an der Eingabeaufforderung folgenden Befehl ein: *gtm_add <IP-Adresse des ersten BIG-IP-DNS-Servers, an dem zuvor alle GUI-Schritte durchgeführt wurden>*

An diesem Punkt können alle weiteren DNS-Konfigurationsarbeiten auf jedem BIG-IP DNS-Gerät durchgeführt werden, das der Gruppe hinzugefügt wurde. Der obige Befehl gtm_add muss nicht auf Appliance-Mitgliedern angewendet werden, die ausschließlich LTM sind. Nur Appliances, die DNS unterstützen, benötigen diesen Befehl, um Teil der synchronisierten DNS-Gruppe zu werden.

Einrichtung von Rechenzentrumsstandorten und Aufbau der Inter-BIG-IP-Kommunikation

An diesem Punkt sind alle Schritte zur Erstellung der zugrunde liegenden, fehlerfreien BIG-IP DNS-Appliance-Gruppe abgeschlossen. Wir können nun mit der Erstellung von Namen, FQDNs, fortfahren, die auf unsere verteilten Web-/S3-Dienste verweisen, die in jedem StorageGRID Rechenzentrum bereitgestellt werden.

Diese Namen werden als „Wide IPs“ oder kurz WIPs bezeichnet und sind normale DNS-FQDNs mit DNS-A-Ressourceneinträgen. Anstatt jedoch wie ein herkömmlicher A-Ressourceneintrag auf einen Server zu verweisen, verweisen sie intern auf Pools von virtuellen BIG-IP-Servern. Jeder Pool kann einzeln aus einem oder mehreren virtuellen Servern bestehen. Ein S3-Client, der eine IP-Adresse zur Namensauflösung

anfordert, erhält die Adresse des virtuellen S3-Servers am optimalen, gemäß den Richtlinien ausgewählten StorageGRID Standort.

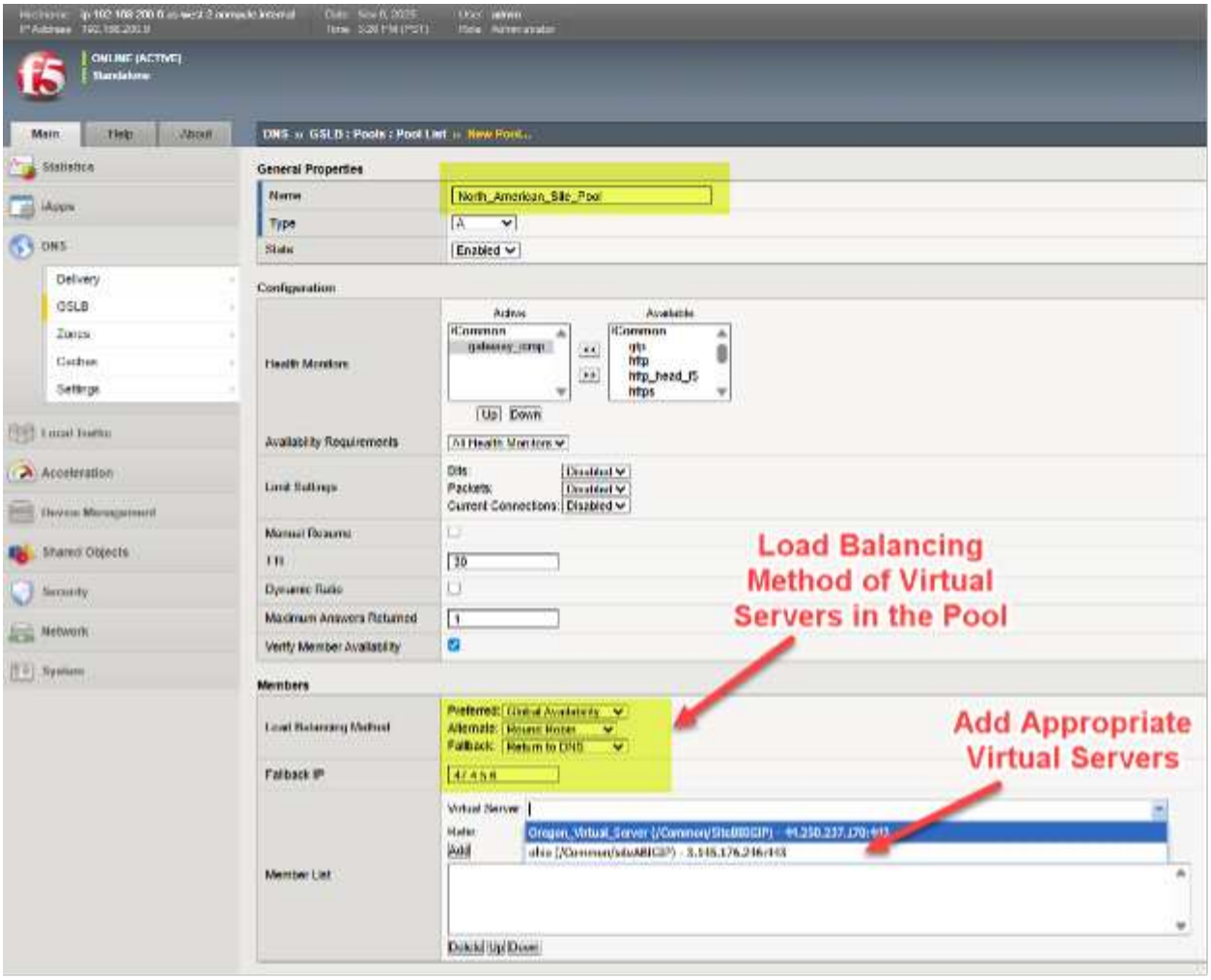
Weite IP-Adressen, Adresspools und virtuelle Server kurz erklärt

Um ein einfaches, fiktives Beispiel zu nennen: Bei einem WIP für den Namen **storage.quantumvault.com** könnte die BIG-IP DNS-Lösung mit zwei Pools potenzieller virtueller Server verknüpft sein. Der erste Pool könnte aus 4 Standorten in Nordamerika bestehen; der zweite Pool könnte aus 3 Standorten in Europa bestehen.

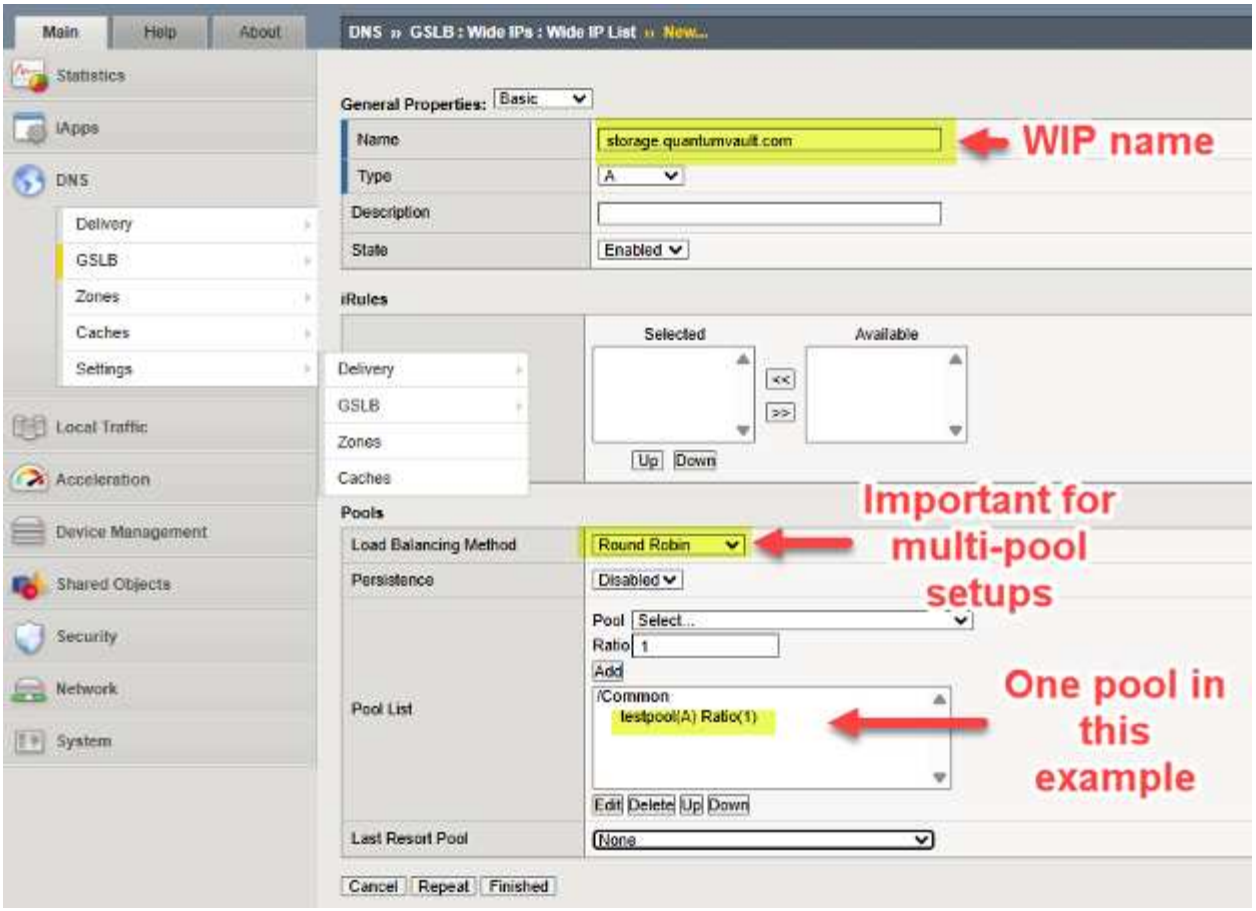
Die Auswahl des Pools könnte durch eine Reihe von politischen Entscheidungen erfolgen; vielleicht könnte ein einfaches Verhältnis von 5:1 verwendet werden, um den Großteil des Datenverkehrs auf nordamerikanische StorageGRID Standorte zu lenken. Wahrscheinlicher ist vielleicht eine topologiebasierte Wahl, bei der der Pool so gewählt wird, dass beispielsweise der gesamte aus Europa stammende S3-Datenverkehr an europäische Standorte geleitet wird und der übrige weltweite S3-Datenverkehr an nordamerikanische Rechenzentren.

Sobald BIG-IP DNS einen Pool ermittelt hat – nehmen wir an, es wurde der nordamerikanische Pool ausgewählt –, kann der tatsächliche DNS-A-Ressourceneintrag, der zur Auflösung von storage.quantumvault.com zurückgegeben wird, einer der vier virtuellen Server sein, die von BIG-IP LTM an einem der vier nordamerikanischen Standorte unterstützt werden. Auch hier ist die Wahl des Standorts richtlinienbasiert. Es gibt einfache „statische“ Verfahren wie Round-Robin, während fortgeschrittenere „dynamische“ Auswahlverfahren wie Leistungstests zur Messung der Latenz jedes Standorts von lokalen DNS-Resolvern durchgeführt und als Kriterium für die Standortauswahl verwendet werden.

Um einen Pool von virtuellen Servern auf einem BIG-IP DNS einzurichten, folgen Sie dem Menüpfad **DNS > GSLB > Pools > Pool List > Add (+)**. In diesem Beispiel sehen wir, wie verschiedene nordamerikanische virtuelle Server zu einem Pool hinzugefügt werden und dass die bevorzugte Methode zum Lastausgleich, wenn dieser Pool ausgewählt wird, nach dem Tiering-Prinzip gewählt wird.



Wir fügen die WIP (Wide IP), den Namen unseres Dienstes, der per DNS aufgelöst wird, einer Bereitstellung hinzu, indem wir dem Pfad DNS > GSLB > Wide IPs > Wide IP List > Create (+) folgen. Im folgenden Beispiel stellen wir einen beispielhaften WIP für einen S3-fähigen Speicherdienst bereit.



DNS zur Unterstützung des globalen Datenverkehrsmanagements anpassen

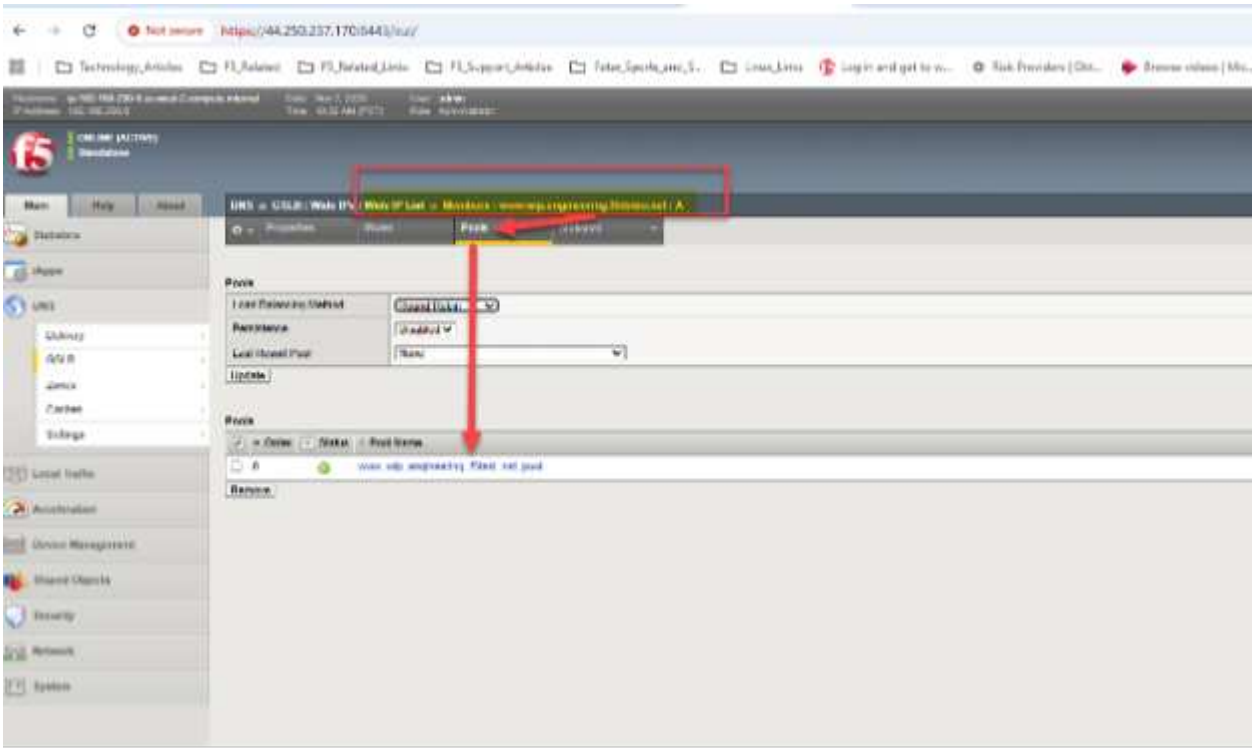
An diesem Punkt sind alle unsere zugrunde liegenden BIG-IP-Appliances bereit, GSLB (Global Server Load Balancing) durchzuführen. Wir müssen lediglich die für die S3-Datenflüsse verwendeten Namen anpassen und zuweisen, um die Lösung optimal nutzen zu können. Der allgemeine Ansatz besteht darin, einen Teil der bestehenden DNS-Domäne eines Unternehmens an die Kontrolle von BIG-IP DNS zu delegieren. Dies bedeutet, einen Abschnitt des Namensraums, eine Subdomain, zu „exkl.) und die Kontrolle über diese Subdomain an die BIG-IP DNS-Appliances zu delegieren. Technisch gesehen geschieht dies dadurch, dass sichergestellt wird, dass die BIG-IP DNS-Appliances über A-DNS-Ressourceneinträge (RRs) im Unternehmens-DNS verfügen und diese Namen/Adressen dann zu Name Server (NS)-DNS-Ressourceneinträgen für die delegierte Domäne gemacht werden.

Es gibt heutzutage verschiedene Möglichkeiten für Unternehmen, ihr DNS zu verwalten; eine Methode ist eine vollständig gehostete Lösung. Ein Beispiel hierfür wäre der Betrieb und die Verwaltung von DNS über Windows Server 2025. Eine alternative Vorgehensweise für ein Unternehmen kann darin bestehen, Cloud-DNS-Anbieter wie AWS Route53 oder Squarespace zu nutzen.

Hier ist ein fiktives Beispiel zur Veranschaulichung. Wir haben StorageGRID, das das Lesen und Schreiben von Objekten über das S3-Protokoll mit einer bestehenden, von AWS Route53 verwalteten Domäne unterstützt; die bestehende Beispieldomäne ist f5demo.net.

Wir möchten die Subdomain engineering.f5demo.net den BIG-IP DNS-Appliances für das globale Traffic-Management zuweisen. Dazu erstellen wir einen neuen NS-Ressourceneintrag (Nameserver) für engineering.f5demo.net und verweisen diesen auf die Liste der BIG-IP DNS-Appliance-Namen. In unserem Beispiel haben wir zwei BIG-IP DNS-Appliances, und daher erstellen wir zwei A-Ressourceneinträge dafür.

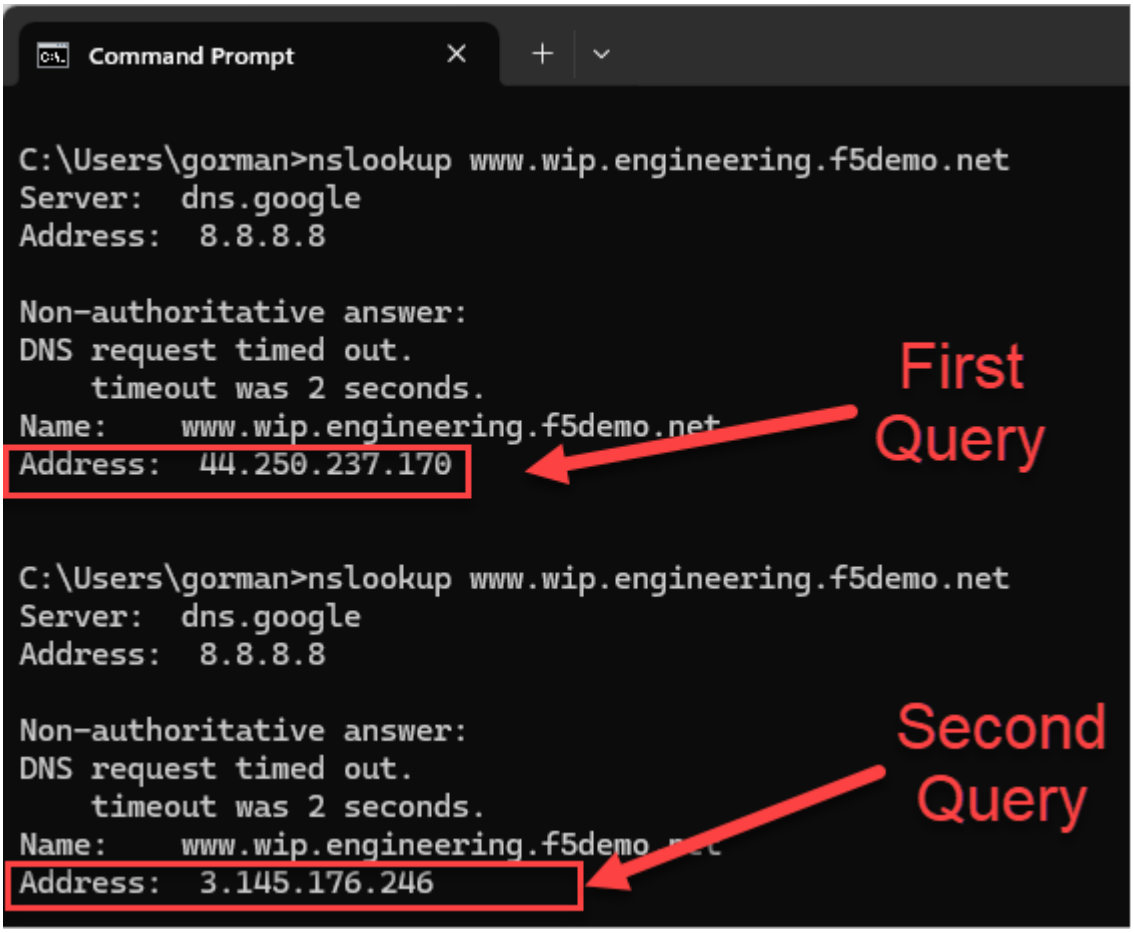
Als Beispiel richten wir nun eine Wide IP (WIP) in unserem BIG-IP DNS ein. Da DNS die Gruppensynchronisierung nutzt, müssen wir die Einstellungen nur über die GUI eines Geräts anpassen. Innerhalb der BIG-IP DNS GUI gehen Sie zu **DNS > GSLB > Wide IPs > Wide IP List (+)**. Zur Erinnerung: Bei einer herkömmlichen DNS-FQDN-Konfiguration müsste man eine oder mehrere IPv4-Adressen eingeben; in unserem Fall verweisen wir einfach auf einen oder mehrere Pools von StorageGRID Virtual-Servern.



In unserem Beispiel verwenden wir generische HTTPS-Webserver, die sich sowohl an Standorten in Ohio als auch in Oregon befinden. Mit einem einfachen „Round-Robin“-Verfahren sollten wir sehen können, wie der globale DNS-Server auf Anfragen nach den A-Resource-Record-Zuordnungen für *www.wip.engineering.f5demo.net* mit beiden virtuellen Server-IPs antwortet.

Ein einfacher Test kann mit Webbrowsern durchgeführt werden oder, im Falle von S3 mit StorageGRID, gegebenenfalls mit grafischen Tools wie S3Browser. Bei jeder DNS-Abfrage wird aufgrund unserer Wahl des Round-Robin-Verfahrens innerhalb des Pools der nächste Rechenzentrumsstandort im Pool als Ziel für den nachfolgenden Datenverkehr verwendet.

In unserem Beispiel-Setup können wir dig oder nslookup verwenden, um schnell eine Reihe von zwei DNS-Abfragen zu generieren und sicherzustellen, dass BIG-IP DNS tatsächlich einen Round-Robin-Lastausgleich durchführt, sodass beide Websites im Laufe der Zeit Datenverkehr erhalten.

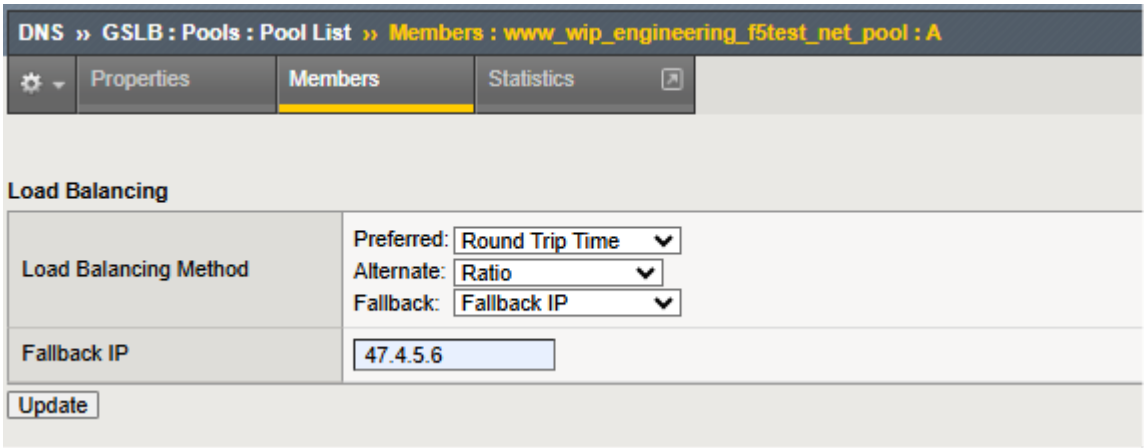


Vorschläge zur Erkundung fortgeschrittenerer Techniken

Eine von vielen möglichen Vorgehensweisen wäre die Verwendung des Modus „Globale Verfügbarkeit“

anstelle des oben genannten einfachen Beispiels „Round Robin“. Mit Global Availability kann der Datenverkehr gezielt auf die Reihenfolge der Pools oder virtuellen Server innerhalb eines einzelnen Pools geleitet werden. Auf diese Weise könnte der gesamte S3-Datenverkehr standardmäßig beispielsweise auf einen Standort in New York City umgeleitet werden.

Wenn die Integritätsprüfungen ein Problem mit der Verfügbarkeit von StorageGRID -Knoten an diesem Standort anzeigen, könnte der Datenverkehr zu diesem Zeitpunkt nach St. Louis umgeleitet werden. Sollten in St. Louis gesundheitliche Probleme auftreten, könnte im Gegenzug ein Standort in Frankfurt S3-Lese- oder Schreibvorgänge empfangen. Globale Verfügbarkeit ist somit ein Ansatz zur Gewährleistung der Ausfallsicherheit der gesamten S3 StorageGRID Lösung. Ein anderer Ansatz besteht darin, verschiedene Load-Balancing-Verfahren zu kombinieren, wobei ein gestaffeltes Verfahren zum Einsatz kommt.



In diesem Beispiel ist die Option „dynamisch“ die erste Load-Balancing-Option für die Standorte im konfigurierten Pool. Im gezeigten Beispiel wird ein kontinuierlicher Messansatz beibehalten, bei dem die Leistung des lokalen DNS-Resolvers aktiv überwacht wird und der Auslöser für die Standortauswahl ist. Sollte dieser Ansatz nicht verfügbar sein, können die einzelnen Standorte anhand des ihnen jeweils zugeordneten Verhältnisses ausgewählt werden. Durch das Verhältnis können größere StorageGRID Standorte mit höherer Bandbreite mehr S3-Transaktionen empfangen als kleinere Standorte. Schließlich wird, falls im Falle eines Notfalls alle Standorte im Pool ausfallen sollten, die angegebene Fallback-IP-Adresse als letzter Ausweg genutzt. Eine der interessantesten Load-Balancing-Methoden von BIG-IP DNS ist die „Topologie“. Dabei wird die eingehende Quelle der DNS-Anfragen, der lokale DNS-Resolver des S3-Benutzers, beobachtet und anhand von Informationen zur Internettopologie der scheinbar „nächstgelegene“ Standort aus dem Pool ausgewählt.

Schließlich, wenn sich die Standorte über den gesamten Globus erstrecken, lohnt es sich möglicherweise, die Verwendung der dynamischen „Probe“-Technologie in Betracht zu ziehen, die im F5 BIG-IP DNS-Handbuch ausführlich beschrieben wird. Mithilfe von Sonden können häufige Quellen von DNS-Anfragen überwacht werden, beispielsweise ein Geschäftspartner, dessen Datenverkehr im Allgemeinen denselben lokalen DNS-Resolver verwendet. BIG-IP DNS-Probes können vom BIG-IP LTM an jedem Standort weltweit gestartet werden, um allgemein zu ermitteln, welcher potenzielle Standort voraussichtlich die niedrigste Latenz für S3-Transaktionen bietet. Daher könnte der Datenverkehr aus Asien besser von asiatischen StorageGRID Standorten bedient werden als von Standorten in Nordamerika oder Europa.

Schlussfolgerung

Die Integration von F5 BIG-IP mit NetApp StorageGRID adressiert technische Herausforderungen im Zusammenhang mit der Datenverfügbarkeit und -konsistenz über mehrere Standorte hinweg sowie der Optimierung des S3-Transaktionsroutings. Durch den Einsatz dieser Lösung werden Speicherstabilität, Leistung und Zuverlässigkeit verbessert, wodurch sie sich ideal für Unternehmen eignet, die eine robuste, skalierbare und flexible Speicherinfrastruktur suchen.

Weitere Informationen finden Sie in der offiziellen F5-Dokumentation für BIG-IP DNS unter diesem Link. "Link"Die Ein geführter Leitfaden für den Unterricht, der Schritt-für-Schritt-Anleitungen für ein Beispiel-Setup bietet, ist ebenfalls verfügbar. "Hier"Die

Datadog SNMP-Konfiguration

Von Aron Klein

Konfigurieren Sie Datadog, um StorageGRID-snmp-Metriken und Traps zu erfassen.

Konfigurieren Sie Das Datadog

Datadog ist eine Überwachungslösung, die Metriken, Visualisierungen und Warnmeldungen bereitstellt. Die folgende Konfiguration wurde mit linux Agent Version 7.43.1 auf einem lokalen Ubuntu 22.04.1-Host auf dem StorageGRID-System implementiert.

Datadog-Profil- und Trap-Dateien, die aus der StorageGRID-MIB-Datei generiert wurden

Datadog bietet eine Methode zum Konvertieren von Produkt-MIB-Dateien in Datadog-Referenzdateien, die für die Zuordnung der SNMP-Meldungen erforderlich sind.

Diese StorageGRID-yaml-Datei für die Datadog-Trap-Auflösungszuordnung wurde nach der gefundenen Anweisung erstellt "Hier". + Platzieren Sie diese Datei in /etc/datadog-Agent/conf.d/snmp.d/Traps_db/ +

- "Laden Sie die Trap yaml-Datei herunter" +
  - **md5-Prüfsumme** 42e27e4210719945a46172b98c379517 +
  - **Sha256 Prüfsumme** d0fe5c8e6ca3c902d054f854b70a85f928cba8b7c76391d356f05d2cf73b6887 +

Diese yaml-Datei für das StorageGRID-Profil für die Datadog-Metrikzuordnung wurde nach der gefundenen Anweisung generiert "Hier". + Platzieren Sie diese Datei in /etc/datadog-Agent/conf.d/snmp.d/profiles/ +

- "Laden Sie die Profil-yaml-Datei herunter" +
  - **md5-Prüfsumme** 72bb7784f4801adda4e0c3ea77df19aa +
  - **Sha256 Prüfsumme** b6b7fadd33063422a8bb8e39b3ead8ab38349ee0229926eadc8585f0087b8cee +

SNMP-Datadog-Konfiguration für Metriken

Die Konfiguration von SNMP für Metriken kann auf zwei Arten verwaltet werden. Sie können für die automatische Erkennung konfigurieren, indem Sie einen Netzwerkadressbereich bereitstellen, der die StorageGRID-Systeme enthält, oder die IP-Adressen der einzelnen Geräte definieren. Der Konfigurationsposition unterscheidet sich je nach getroffenen Entscheidungen. Die automatische Erkennung wird in der Datei des Datadog-Agenten yaml definiert. Explizite Gerätedefinitionen werden in der snmp-yaml-Konfigurationsdatei konfiguriert. Im Folgenden finden Sie Beispiele für jedes System eines StorageGRID.

Automatische Erkennung

Konfiguration befindet sich in /etc/datadog-Agent/datadog.yaml

```
listeners:
  - name: snmp
snmp_listener:
  workers: 100  # number of workers used to discover devices concurrently
  discovery_interval: 3600  # interval between each autodiscovery in
seconds
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
  configs:
    - network_address: 10.0.0.0/24  # CIDR subnet
      snmp_version: 2
      port: 161
      community_string: 'st0r@gegrid'  # enclose with single quote
      profile: netapp-storagegrid
```

Einzelne Geräte

/Etc/datadog-Agent/conf.d/snmp.d/conf.yaml

```
init_config:
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
instances:
- ip_address: '10.0.0.1'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'  # enclose with single quote
- ip_address: '10.0.0.2'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
- ip_address: '10.0.0.3'
  profile: netapp-storagegrid
 community_string: 'st0r@gegrid'
- ip_address: '10.0.0.4'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
```

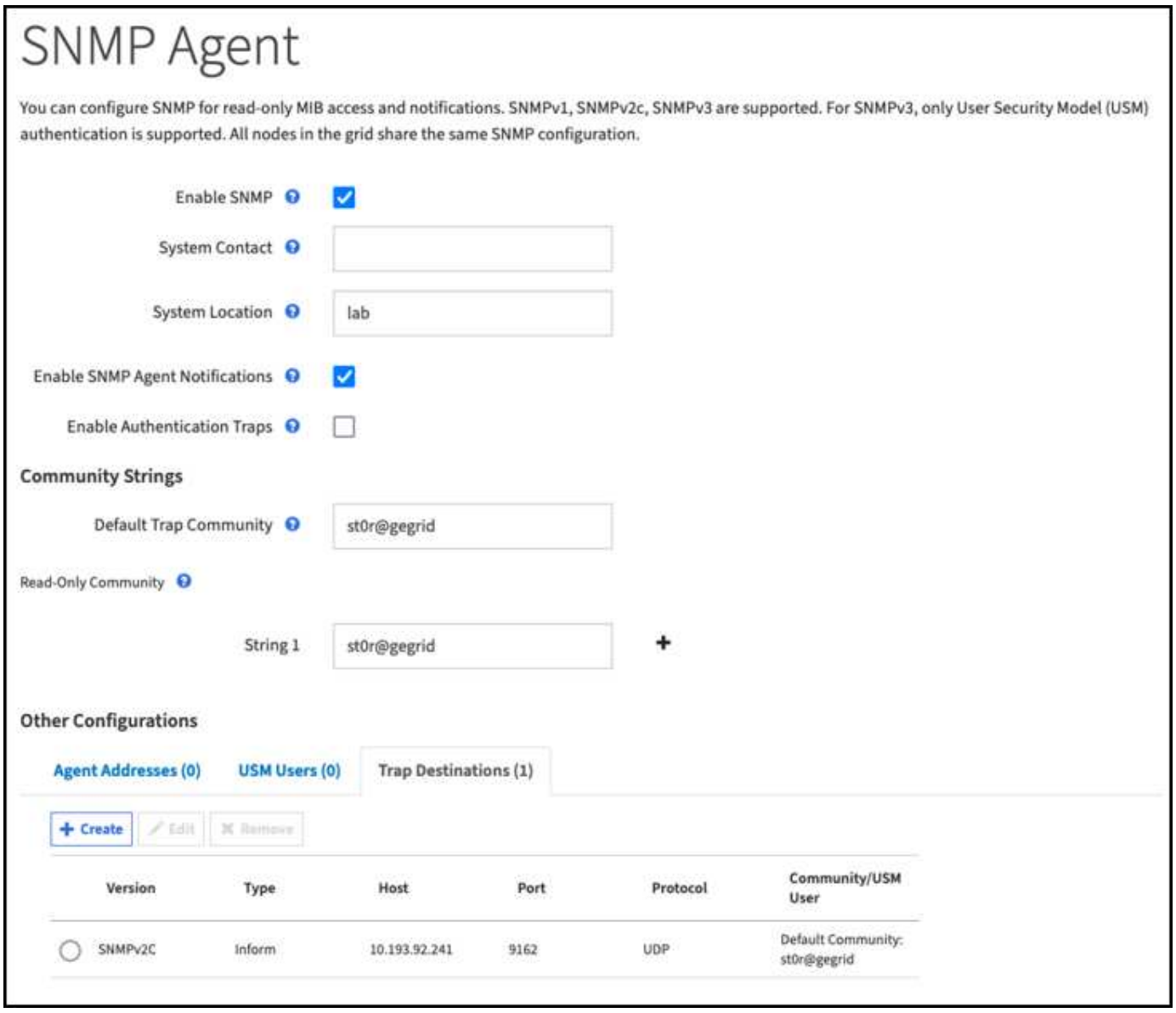
SNMP-Konfiguration für Traps

Die Konfiguration für SNMP-Traps wird in der Datei /etc/datadog-Agent/datadog.yaml der Datendog-Konfiguration definiert

```
network_devices:
  namespace:  # optional, defaults to "default".
  snmp_traps:
    enabled: true
    port: 9162 # on which ports to listen for traps
    community_strings: # which community strings to allow for v2 traps
      - st0r@gegrid
```

Beispiel für eine StorageGRID-SNMP-Konfiguration

Der SNMP-Agent in Ihrem StorageGRID-System befindet sich auf der Registerkarte Konfiguration in der Spalte Überwachung. Aktivieren Sie SNMP und geben Sie die gewünschten Informationen ein. Wenn Sie Traps konfigurieren möchten, wählen Sie „Traps-Ziele“ und erstellen Sie ein Ziel für den Datadog-Agent-Host, der die Trap-Konfiguration enthält.



Mit rclone können Sie Objekte auf StorageGRID migrieren, VERSCHIEBEN und LÖSCHEN

Von Siegfried Hepp und Aron Klein

Rclone ist ein kostenloses Kommandozeilen-Tool und Client für S3-Vorgänge. Sie können rclone verwenden, um Objektdaten auf StorageGRID zu migrieren, zu kopieren und zu löschen. Rclone bietet die Möglichkeit, Buckets auch dann zu löschen, wenn es nicht leer ist. Die Funktion „purge“ ist in einem Beispiel unten dargestellt.

Installieren und Konfigurieren von rclone

Um rclone auf einer Workstation oder einem Server zu installieren, laden Sie es von herunter "rclone.org".

Erste Konfigurationsschritte

1. Erstellen Sie die rclone-Konfigurationsdatei, indem Sie entweder das Konfigurationsskript ausführen oder die Datei manuell erstellen.
2. In diesem Beispiel verwende ich sgdemo für den Namen des entfernten StorageGRID S3-Endpunkts in der rclone-Konfiguration.
   a. Erstellen Sie die Konfigurationsdatei ~/.config/rclone/rclone.conf

```
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com
```

   b. Führen Sie rclone config aus

Rclone config

```
2023/04/13 14:22:45 NOTICE: Config file
"/root/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> sgdemo
```

```
Option Storage.
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Providers including AWS,
Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio,
SeaweedFS, and Tencent COS
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Better checksums for other remotes
   \ "hasher"
 7 / Box
   \ "box"
 8 / Cache a remote
   \ "cache"
 9 / Citrix Sharefile
   \ "sharefile"
10 / Compress a remote
   \ "compress"
11 / Dropbox
   \ "dropbox"
12 / Encrypt/Decrypt a remote
   \ "crypt"
13 / Enterprise File Fabric
   \ "filefabric"
14 / FTP Connection
```

```
   \ "ftp"
15 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
16 / Google Drive
   \ "drive"
17 / Google Photos
   \ "google photos"
18 / Hadoop distributed file system
   \ "hdfs"
19 / Hubic
   \ "hubic"
20 / In memory object storage system.
   \ "memory"
21 / Jottacloud
   \ "jottacloud"
22 / Koofr
   \ "koofr"
23 / Local Disk
   \ "local"
24 / Mail.ru Cloud
   \ "mailru"
25 / Mega
   \ "mega"
26 / Microsoft Azure Blob Storage
   \ "azureblob"
27 / Microsoft OneDrive
   \ "onedrive"
28 / OpenDrive
   \ "opendrive"
29 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore,
OVH)
   \ "swift"
30 / Pcloud
   \ "pcloud"
31 / Put.io
   \ "putio"
32 / QingCloud Object Storage
   \ "qingstor"
33 / SSH/SFTP Connection
   \ "sftp"
34 / Sia Decentralized Cloud
   \ "sia"
35 / Sugarsync
   \ "sugarsync"
36 / Tardigrade Decentralized Cloud Storage
   \ "tardigrade"
```

```
37 / Transparently chunk/split large files
   \ "chunker"
38 / Union merges the contents of several upstream fs
   \ "union"
39 / Uptobox
   \ "uptobox"
40 / Webdav
   \ "webdav"
41 / Yandex Disk
   \ "yandex"
42 / Zoho
   \ "zoho"
43 / http Connection
   \ "http"
44 / premiumize.me
   \ "premiumizeme"
45 / seafile
   \ "seafile"
```

```
Storage> 4
```

```
Option provider.
Choose your S3 provider.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / Amazon Web Services (AWS) S3
   \ "AWS"
 2 / Alibaba Cloud Object Storage System (OSS) formerly Aliyun
   \ "Alibaba"
 3 / Ceph Object Storage
   \ "Ceph"
 4 / Digital Ocean Spaces
   \ "DigitalOcean"
 5 / Dreamhost DreamObjects
   \ "Dreamhost"
 6 / IBM COS S3
   \ "IBMCOS"
 7 / Minio Object Storage
   \ "Minio"
 8 / Netease Object Storage (NOS)
   \ "Netease"
 9 / Scaleway Object Storage
   \ "Scaleway"
10 / SeaweedFS S3
   \ "SeaweedFS"
11 / StackPath Object Storage
   \ "StackPath"
12 / Tencent Cloud Object Storage (COS)
   \ "TencentCOS"
13 / Wasabi Object Storage
   \ "Wasabi"
14 / Any other S3 compatible provider
   \ "Other"
provider> 14
```

```
Option env_auth.
Get AWS credentials from runtime (environment variables or
EC2/ECS meta data if no env vars).
Only applies if access_key_id and secret_access_key is blank.
Enter a boolean value (true or false). Press Enter for the
default ("false").
Choose a number from below, or type in your own value.
 1 / Enter AWS credentials in the next step.
   \ "false"
 2 / Get AWS credentials from the environment (env vars or IAM).
   \ "true"
env_auth> 1
```

```
Option access_key_id.
AWS Access Key ID.
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
access_key_id> ABCDEFGH123456789JKL
```

```
Option secret_access_key.
AWS Secret Access Key (password).
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
secret_access_key> 123456789ABCDEFGHIJKLMN0123456789PQRST+V
```

```
Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a
region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Use this if unsure.
 1 | Will use v4 signatures and an empty region.
   \ ""
   / Use this only if v4 signatures don't work.
 2 | E.g. pre Jewel/v10 CEPH.
   \ "other-v2-signature"
region> 1
```

```
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> sgdemo.netapp.com
```

```
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
location_constraint>
```

```
Option acl.
Canned ACL used when creating buckets and storing or copying
objects.
This ACL is used for creating objects and if bucket_acl isn't
set, for creating buckets too.
For more info visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-
overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as
S3
doesn't copy the ACL from the source but rather writes a fresh
one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Owner gets FULL_CONTROL.
 1 | No one else has access rights (default).
   \ "private"
   / Owner gets FULL_CONTROL.
 2 | The AllUsers group gets READ access.
   \ "public-read"
   / Owner gets FULL_CONTROL.
 3 | The AllUsers group gets READ and WRITE access.
   | Granting this on a bucket is generally not recommended.
   \ "public-read-write"
   / Owner gets FULL_CONTROL.
 4 | The AuthenticatedUsers group gets READ access.
   \ "authenticated-read"
   / Object owner gets FULL_CONTROL.
 5 | Bucket owner gets READ access.
   | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-read"
   / Both the object owner and the bucket owner get FULL_CONTROL
over the object.
 6 | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-full-control"
acl>
```

```
Edit advanced config?
y) Yes
n) No (default)
y/n> n
```

```
--------------------
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com:443
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>
```

```
Current remotes:
```

```
Name                 Type
====                 ====
sgdemo               s3
```

```
e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

Beispiele für grundlegende Befehle

- **Erstellen Sie einen Eimer:**

  `rclone mkdir remote:bucket`

  ```
  # Rclone mkdir sgdemo:test01
  ```

  Verwenden Sie --no-Check-Certificate, wenn Sie SSL-Zertifikate ignorieren müssen.

- **Alle Buckets auflisten:**

```
rclone lsd remote:
```

```
# Rclone lsd sgdemo:
```

- **Objekte in einem bestimmten Bucket auflisten:**

```
rclone ls remote:bucket
```

```
# Rclone ls sgdemo:test01
```

```
    65536 TestObject.0
    65536 TestObject.1
    65536 TestObject.10
    65536 TestObject.12
    65536 TestObject.13
    65536 TestObject.14
    65536 TestObject.15
    65536 TestObject.16
    65536 TestObject.17
    65536 TestObject.18
    65536 TestObject.2
    65536 TestObject.3
    65536 TestObject.5
    65536 TestObject.6
    65536 TestObject.7
    65536 TestObject.8
    65536 TestObject.9
  33554432 bigobj
      102 key.json
       47 locked01.txt
4294967296 sequential-read.0.0
       15 test.txt
      116 version.txt
```

- **Ein Eimer löschen:**

```
rclone rmdir remote:bucket
```

```
# Rclone rmdir sgdemo:test02
```

- **Legen Sie ein Objekt:**

```
rclone copy filename remote:bucket
```

```
# Rclone copy ~/Test/testfile.txt sgdemo:test01
```

- **Holen Sie sich ein Objekt:**

```
rclone copy remote:bucket/objectname filename
```

```
# Rclone copy sgdemo:test01/testfile.txt ~/Test/testfileS3.txt
```

- **Ein Objekt löschen:**

```
rclone delete remote:bucket/objectname
```

```
# Rclone delete sgdemo:test01/testfile.txt
```

- **Objekte in einen Bucket migrieren**

```
rclone sync source:bucket destination:bucket --progress

rclone sync source_directory destination:bucket --progress
```

```
# Rclone Sync sgdemo:test01 sgdemo:clone01 --progress

Transferred:        4.032 GiB / 4.032 GiB, 100%, 95.484 KiB/s, ETA
0s
Transferred:           22 / 22, 100%
Elapsed time:       1m4.2s
```

Verwenden Sie --progress oder -P, um den Fortschritt der Aufgabe anzuzeigen. Andernfalls gibt es keine Ausgabe.

- **Löschen eines Buckets und aller Objektinhalte**

```
rclone purge remote:bucket --progress
```

Rclone purge sgdemo:test01 --progress

```
Transferred:              0 B / 0 B, -, 0 B/s, ETA -
Checks:                46 / 46, 100%
Deleted:               23 (files), 1 (dirs)
Elapsed time:        10.2s
```

Rclone ls sgdemo:test01

```
2023/04/14 09:40:51 Failed to ls: directory not found
```

StorageGRID Best Practices für die Implementierung mit Veeam Backup and Replication

Von Oliver Haensel und Aron Klein

Dieser Leitfaden konzentriert sich auf die Konfiguration von NetApp StorageGRID und teilweise Veeam Backup and Replication. Dieses Dokument richtet sich an Storage- und Netzwerkadministratoren, die mit Linux-Systemen vertraut sind und mit der Wartung oder Implementierung eines NetApp StorageGRID-Systems in Kombination mit Veeam Backup and Replication betraut sind.

Überblick

Speicheradministratoren möchten das Wachstum ihrer Daten mit Lösungen managen, die die Anforderungen an Verfügbarkeit, schnelle Wiederherstellung erfüllen, an ihre Bedürfnisse anpassen und ihre Richtlinien für die langfristige Aufbewahrung von Daten automatisieren. Diese Lösungen sollten auch Schutz vor Verlust oder böswilligen Angriffen bieten. Veeam und NetApp haben gemeinsam eine Datensicherungslösung entwickelt, die Veeam Backup & Recovery mit NetApp StorageGRID kombiniert und damit Objekt-Storage vor Ort ermöglicht.

Veeam und NetApp StorageGRID bieten eine benutzerfreundliche Lösung, die zusammen die Anforderungen eines schnellen Datenwachstums und die zunehmenden Vorschriften weltweit erfüllt. Cloud-basierter Objekt-Storage ist für seine Ausfallsicherheit, Skalierbarkeit, betriebliche Effizienz und Kosteneffizienz bekannt, die ihn zur ersten Wahl für Ihre Backups machen. Dieses Dokument enthält Anleitungen und Empfehlungen für die Konfiguration Ihrer Veeam Backup-Lösung und des StorageGRID Systems.

Der Objekt-Workload von Veeam erstellt eine große Anzahl von gleichzeitigen PUT-, DELETE- und LISTENVORGÄNGEN für kleine Objekte. Durch die Unveränderlichkeit wird die Anzahl der Anfragen an den Objektspeicher zur Festlegung von Aufbewahrungs- und Listenversionen weiter addiert. Der Prozess eines Backup-Jobs umfasst das Schreiben von Objekten für die tägliche Änderung. Nach Abschluss der neuen Schreibvorgänge löscht der Job alle Objekte, die auf der Aufbewahrungsrichtlinie des Backups basieren. Die Planung von Backup-Jobs wird sich fast immer überschneiden. Diese Überschneidung führt zu einem großen Teil des Backup-Fensters, das aus 50/50 PUT/DELETE Workloads auf dem Objektspeicher besteht. Anpassungen an die Anzahl gleichzeitiger Vorgänge mit der Einstellung für den Task-Slot vornehmen und die Objektgröße dadurch erhöhen, dass die Blockgröße für den Backup-Job erhöht wird, die Anzahl der Objekte in den Anforderungen zum Löschen mehrerer Objekte reduziert wird, und wenn Sie das maximale Zeitfenster für die Fertigstellung der Jobs auswählen, wird die Lösung hinsichtlich Performance und Kosten optimiert.

Lesen Sie unbedingt die Produktdokumentation für "Veeam Backup und Replication" Und "StorageGRID" bevor Sie beginnen. Veeam bietet Rechner zum Verständnis der Dimensionierung der Veeam-Infrastruktur und der Kapazitätsanforderungen, die vor der Dimensionierung Ihrer StorageGRID Lösung verwendet werden sollten. Bitte überprüfen Sie immer die Veeam- NetApp validierten Konfigurationen auf der Veeam Ready Program Website für "Veeam Ready Objekt, Unveränderlichkeit von Objekten und Repository" .

Veeam Konfiguration

Empfohlene Version

Es wird empfohlen, immer auf dem neuesten Stand zu bleiben und die neuesten Hotfixes für Ihr Veeam Backup & Replication 12- oder 12.1-System anzuwenden. Derzeit wird empfohlen, mindestens Veeam 12 Patch P20230718 zu installieren.

S3-Repository-Konfiguration

Ein Scale-out-Backup-Repository (SOBR) ist die Kapazitäts-Tier des S3-Objekt-Storage. Die Kapazitäts-Tier ist eine Erweiterung des primären Repositorys mit längeren Aufbewahrungszeiträumen und einer kostengünstigeren Storage-Lösung. Veeam ermöglicht Unveränderlichkeit über die S3 Object Lock API. Veeam 12 kann mehrere Buckets in einem Scale-out-Repository verwenden. StorageGRID hat keine Obergrenze für die Anzahl der Objekte oder Kapazität in einem einzelnen Bucket. Die Verwendung mehrerer Buckets verbessert möglicherweise die Performance beim Backup von sehr großen Datensätzen, bei denen die Backup-Daten in Objekten bis in den Petabyte-Bereich skaliert werden können.

Je nach Dimensionierung Ihrer spezifischen Lösung und den Anforderungen können Sie gleichzeitige Tasks beschränken. In den Standardeinstellungen wird für jeden CPU-Kern ein Repository-Tasksteckplatz und für jeden Task-Steckplatz ein Limit von 64 gleichzeitig ausgeführten Tasksteckplätzen festgelegt. Wenn Ihr Server beispielsweise 2 CPU-Kerne hat, werden insgesamt 128 gleichzeitige Threads für den Objektspeicher verwendet. Dies beinhaltet PUT, GET und Batch Delete. Es wird empfohlen, einen konservativen Grenzwert für die Taskslots auszuwählen, um mit zu beginnen und diesen Wert einzustellen, sobald Veeam-Backups einen stabilen Zustand von neuen Backups und auslaufenden Backupdaten erreicht haben. Arbeiten Sie mit Ihrem NetApp Account Team zusammen, um die Größe des StorageGRID Systems entsprechend anzupassen, damit die gewünschten Zeitfenster und Leistungen eingehalten werden. Um die optimale Lösung zu bieten, müssen Sie die Anzahl der Aufgabenplätze und die Anzahl der Aufgaben pro Steckplatz anpassen.

Konfiguration des Backupjobs

Veeam Backup-Jobs können mit anderen Blockgrößen konfiguriert werden, die besonders sorgfältig geprüft werden sollten. Die standardmäßige Blockgröße beträgt 1 MB und mit der Speichereffizienz, die Veeam mit Komprimierung und Deduplizierung bietet, erzeugt Objektgrößen von ca. 500 KB für das erste vollständige Backup und 100-200-KB-Objekte für die inkrementellen Jobs. Wir können die Performance des Objektspeichers deutlich steigern und die Anforderungen reduzieren, indem wir eine größere Blockgröße für Backups auswählen. Obwohl die größere Blockgröße zu großen Verbesserungen der Objektspeicher-Performance führt, geht dies zu Kosten, da potenziell höhere Anforderungen an die Kapazität des primären Storage aufgrund niedrigerer Storage-Effizienz-Performance entstehen. Es wird empfohlen, die Backup-Jobs mit einer Blockgröße von 4 MB zu konfigurieren, die ca. 2 MB Objekte für die vollständigen Backups und 700kB-1MB Objektgrößen für inkrementelle Backups erzeugt. Kunden ziehen möglicherweise sogar die Konfiguration von Backup-Jobs mit einer Blockgröße von 8 MB in Betracht, die mithilfe des Veeam Supports aktiviert werden kann.

Bei der Implementierung von unveränderlichen Backups wird auf S3 Object Lock im Objektspeicher gesetzt. Die Option „Unveränderlichkeit“ generiert eine größere Anzahl von Anfragen an den Objektspeicher zur Auflistung und Aktualisierung der Aufbewahrung der Objekte.

Wenn Backup-Retentions ablaufen, verarbeiten die Backup-Jobs das Löschen von Objekten. Veeam sendet die Löschanforderungen je Anforderung in 1000 Objekten an den Objektspeicher. Bei kleinen Lösungen muss diese ggf. angepasst werden, um die Anzahl der Objekte pro Anfrage zu verringern. Eine Senkung dieses Werts hat den zusätzlichen Vorteil, dass die Löschanforderungen gleichmäßig auf die Knoten im StorageGRID-System verteilt werden. Es wird empfohlen, die Werte in der folgenden Tabelle als Ausgangspunkt für die Konfiguration der Grenze für das Löschen mehrerer Objekte zu verwenden. Multiplizieren Sie den Wert in der Tabelle mit der Anzahl der Knoten für den ausgewählten Gerätetyp, um den Wert für die Einstellung in Veeam zu erhalten. Wenn dieser Wert gleich oder größer als 1000 ist, muss der Standardwert nicht angepasst werden. Wenn dieser Wert angepasst werden muss, wenden Sie sich an den Veeam-Support, um die Änderung vorzunehmen.

Appliance-Modell	S3MultiObjectDeleteLimit pro Knoten
SG5712	34
SG5760	75
SG6060	200

Wenden Sie sich an Ihr NetApp Account Team, um die empfohlene Konfiguration basierend auf Ihren spezifischen Anforderungen zu erhalten. Die Empfehlungen für die Veeam-Konfigurationseinstellungen umfassen:

- Blockgröße des Backupjobs = 4 MB
- SOBR-Task-Slot-Limit= 2-16
- Limit Für Mehrere Objekte Löschen = 34-1000

StorageGRID-Konfiguration

Empfohlene Version

NetApp StorageGRID 11.9 oder 12.0 mit dem neuesten Hotfix sind die empfohlenen Versionen für Veeam-Bereitstellungen. Es wird immer empfohlen, auf dem neuesten Stand zu bleiben und die neuesten Hotfixes für Ihr StorageGRID System anzuwenden.

Load Balancer und S3-Endpunktkonfiguration

Für Veeam muss der Endpunkt nur über HTTPS verbunden sein. Eine nicht verschlüsselte Verbindung wird von Veeam nicht unterstützt. Das SSL-Zertifikat kann ein selbstsigniertes Zertifikat, eine private vertrauenswürdige Zertifizierungsstelle oder eine öffentliche vertrauenswürdige Zertifizierungsstelle sein. Um den kontinuierlichen Zugriff auf das S3-Repository zu gewährleisten, wird die Verwendung von mindestens zwei Load Balancern in einer HA-Konfiguration empfohlen. Beim Lastausgleich kann es sich um einen von StorageGRID bereitgestellten integrierten Load Balancer handeln, der sich auf jedem Administrator-Node und Gateway-Node oder bei Lösungen von Drittanbietern wie F5, Kemp, HAProxy, Loadbalancer.org usw. befindet Mithilfe eines StorageGRID Load Balancer kann man Traffic-Klassifikatoren (QoS-Regeln) festlegen, die den Veeam Workload priorisieren können oder Veeam auf Workloads mit höherer Priorität im StorageGRID System beschränken.

S3-Bucket

StorageGRID ist ein sicheres Multi-Tenant-Speichersystem. Es wird empfohlen, einen dedizierten Mandanten für die Veeam-Workload zu erstellen. Optional kann ein Speicherkontingent zugewiesen werden. Aktivieren Sie als Best Practice „Eigene Identitätsquelle verwenden“. Sichern Sie den Stammverwaltungsbenutzer des

Mandanten mit einem entsprechenden Kennwort. Veeam Backup 12 erfordert eine starke Konsistenz für S3-Buckets. StorageGRID bietet mehrere Konsistenzoptionen, die auf Bucket-Ebene konfiguriert werden. Wählen Sie für Bereitstellungen an mehreren Standorten, bei denen Veeam von mehreren Standorten auf die Daten zugreift, „strong-global“ aus. Wenn Veeam-Backups und -Wiederherstellungen nur an einem einzigen Standort erfolgen, sollte die Konsistenzebene auf „starker Standort“ eingestellt werden. Weitere Informationen zu den Eimerkonsistenzstufen finden Sie in der "Dokumentation" . Um StorageGRID für Veeam-Unveränderlichkeitssicherungen zu verwenden, muss S3 Object Lock global aktiviert und während der Bucket-Erstellung im Bucket konfiguriert werden.

Lifecycle Management

StorageGRID unterstützt Replizierung und Erasure Coding für eine Sicherung auf Objektebene über StorageGRID Nodes und Standorte hinweg. Erasure Coding erfordert mindestens eine Objektgröße von 200 kB. Die standardmäßige Blockgröße für Veeam von 1 MB erzeugt Objektgrößen, die oft unter dieser empfohlenen Mindestgröße von 200 KB liegen können, nachdem Veeam die Storage-Effizienz erreicht hat. Für die Performance der Lösung wird empfohlen, kein Erasure Coding-Profil für mehrere Standorte zu verwenden, es sei denn, die Verbindung zwischen den Standorten reicht aus, um keine Latenz hinzuzufügen oder die Bandbreite des StorageGRID-Systems zu beschränken. Bei einem StorageGRID System mit mehreren Standorten kann die ILM-Regel so konfiguriert werden, dass eine einzige Kopie an jedem Standort gespeichert wird. Um die ultimative Aufbewahrungszeit zu gewährleisten, kann eine Regel für die Speicherung einer Kopie, die nach dem Verfahren zur Fehlerkorrektur codiert wurde, an jedem Standort konfiguriert werden. Die am besten empfohlene Implementierung für diesen Workload ist der lokale Einsatz von zwei Kopien auf den Veeam Backup Servern.

Leistung löschen

Veeam ermöglicht die Optimierung der Löschanforderungsrate und die Planung des Sicherungslöschvorgangs. Um die Löschleistung weiter zu optimieren, können Sie synchrone Löschvorgänge deaktivieren und das endgültige Löschen von Objekten dem ILM-Scanner überlassen.

Schritte zum Deaktivieren synchroner Löschungen

1. Öffnen Sie den StorageGRID Grid Manager.
2. Wählen Sie in der oberen rechten Ecke das Fragezeichen und dann API-Dokumentation aus.
3. Klicken Sie oben rechts auf den Link zur Seite „Private API-Dokumentation“.
4. Erweitern Sie ilm-advanced.
5. Wählen Sie GET ilm-advanced.
6. Wählen Sie „Ausprobieren“ und dann „Ausführen“.
7. Überprüfen Sie das Antwortergebnis.

    a. Wenn die Werte null sind, bedeutet dies, dass die standardmäßigen ILM-Advanced-Werte verwendet werden.

    b. Wenn die Werte nicht null sind, bedeutet dies, dass benutzerdefinierte erweiterte ILM-Werte verwendet werden. Kopieren Sie die gesamte Ausgabe nach „data“:, beginnend mit { bis zum vorletzten }.

        i. Speichern Sie es in einem Texteditor.

        Beispielantwort:

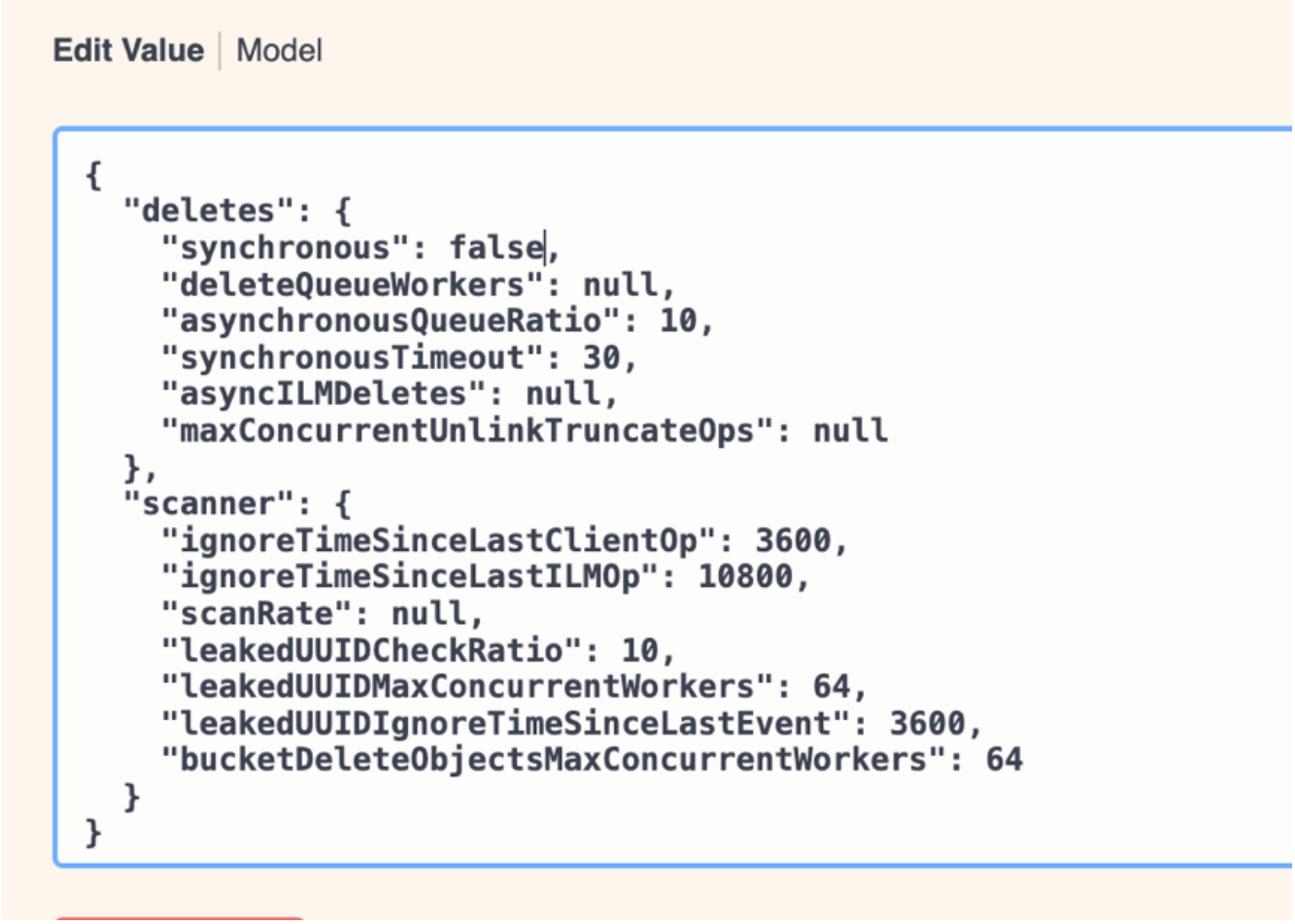
Response body


```
{
  "responseTime": "2025-09-19T15:01:28.142Z",
  "status": "success",
  "apiVersion": "4.2",
  "data": {
    "deletes": {
      "synchronous": null,
      "deleteQueueWorkers": null,
      "asynchronousQueueRatio": null,
      "synchronousTimeout": null,
      "asyncILMDeletes": null,
      "maxConcurrentUnlinkTruncateOps": null
    },
    "scanner": {
      "ignoreTimeSinceLastClientOp": null,
      "ignoreTimeSinceLastILMOp": null,
      "scanRate": null,
      "leakedUUIDCheckRatio": null,
      "leakedUUIDMaxConcurrentWorkers": null,
      "leakedUUIDIgnoreTimeSinceLastEvent": null,
      "bucketDeleteObjectsMaxConcurrentWorkers": null
    }
  }
}
```


8. Wählen Sie PUT ilm-advanced.
9. Wählen Sie „Ausprobieren“ aus, um mit der Bearbeitung des API-Texts zu beginnen.
    a. Standardmäßig enthält der API-Text Standardwerte und keine zuvor konfigurierten benutzerdefinierten Werte. Aus diesem Grund ist es SEHR wichtig, die Schritte 5 bis 7 auszuführen.
10. Wenn in den Schritten 5–7 nicht standardmäßige Werte gefunden werden, ersetzen Sie den API-Text durch die in Schritt 7 gespeicherte Ausgabe. . Andernfalls, wenn die Werte in den Schritten 5–7 null waren, lassen Sie den API-Text unverändert.
11. Passen Sie die folgenden Parameter im API-Body-Feld an:

    a. Setzen Sie den synchronen Wert auf „false“.

    Beispiel für API-Textkörper:

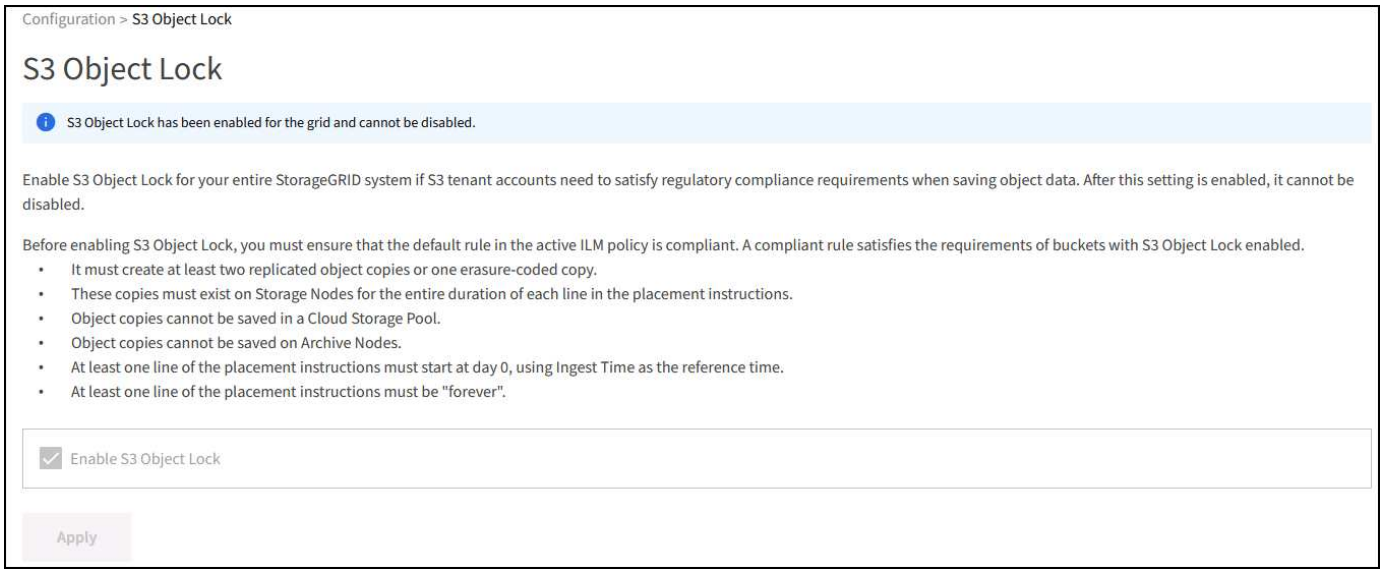


12. Wenn Sie fertig sind, wählen Sie Ausführen

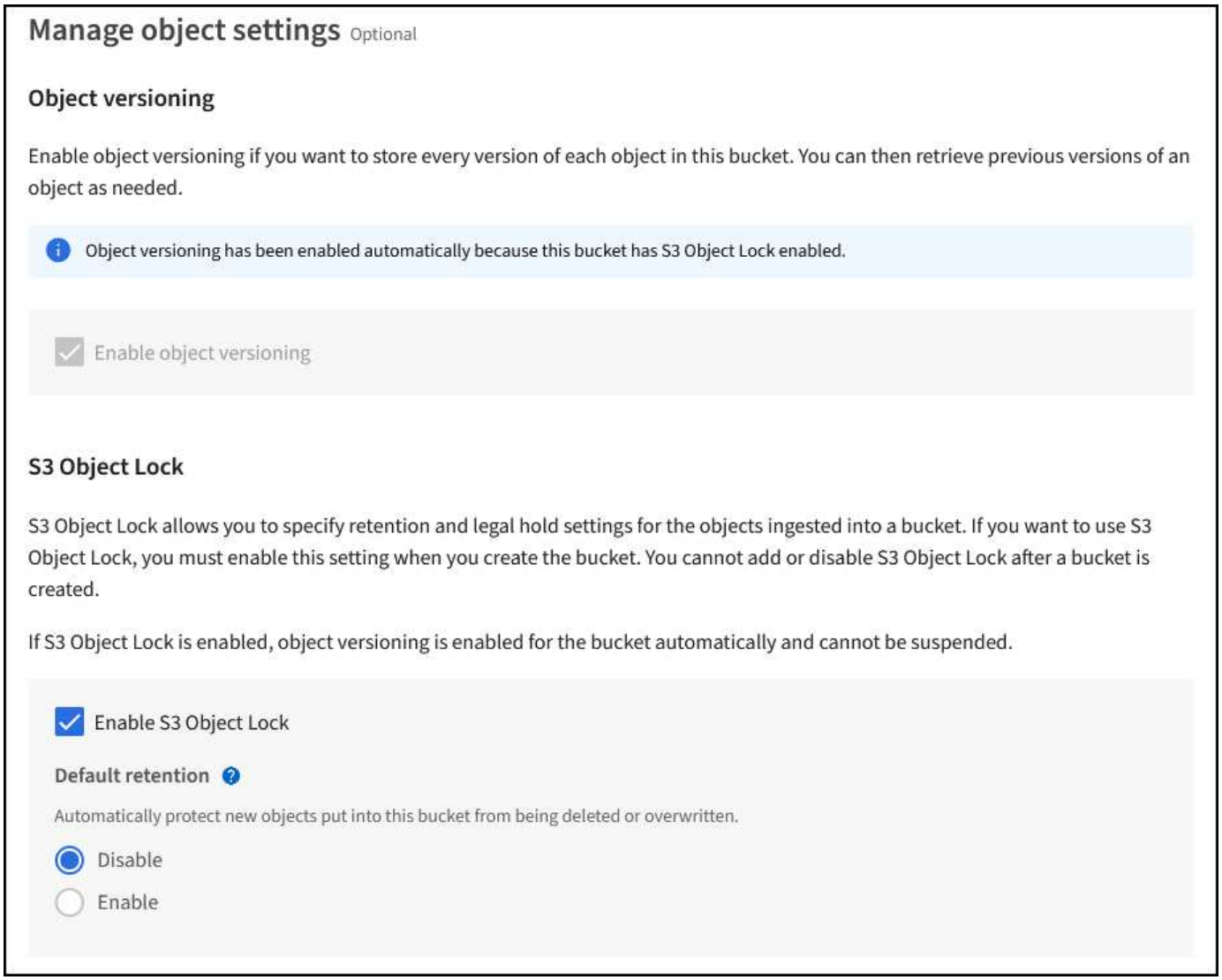
Zentrale Punkte bei der Implementierung

StorageGRID

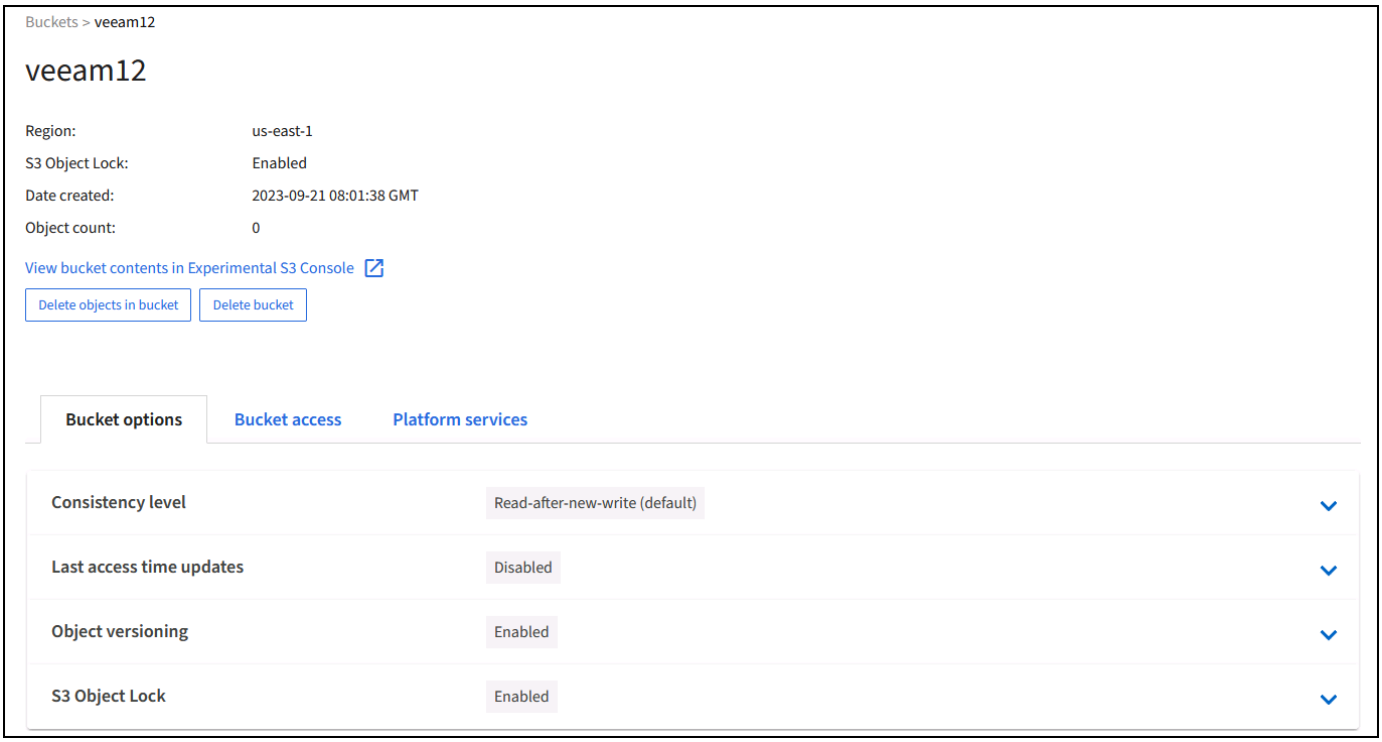
Stellen Sie sicher, dass die Objektsperre auf dem StorageGRID System aktiviert ist, falls eine Unveränderlichkeit erforderlich ist. Suchen Sie die Option in der Management-UI unter Configuration/S3 Object Lock.



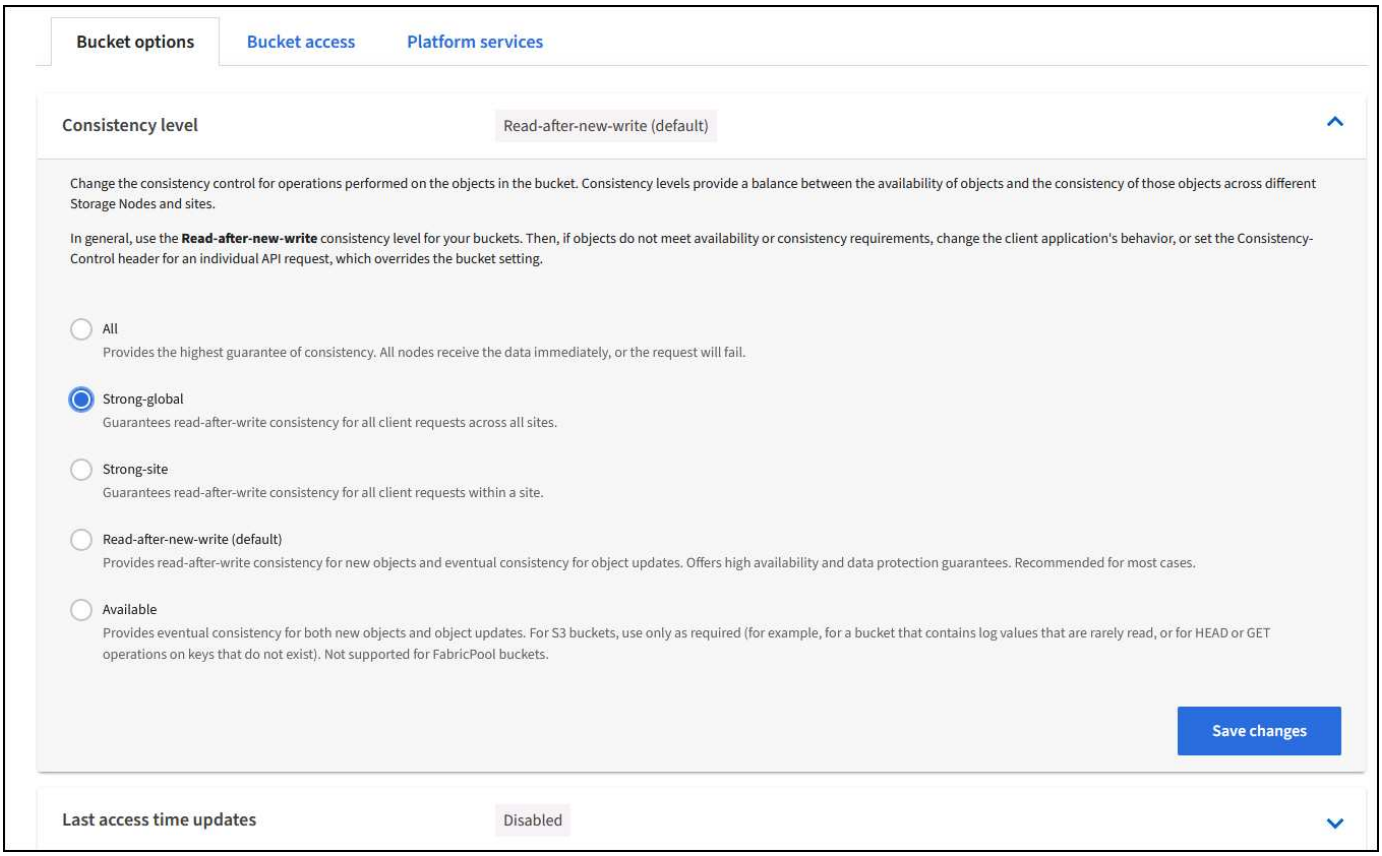
Wählen Sie bei der Erstellung des Buckets die Option „S3 Object Lock aktivieren“ aus, wenn dieser Bucket zur Unveränderlichkeit von Backups verwendet werden soll. Dadurch wird die Bucket-Versionierung automatisch aktiviert. Die Standardaufbewahrung bleibt deaktiviert, da Veeam die Objektaufbewahrung explizit festlegt. Versionierung und S3 Object Lock sollten nicht ausgewählt werden, wenn Veeam keine unveränderlichen Backups erstellt.



Sobald der Bucket erstellt wurde, gehen Sie zur Detailseite des erstellten Buckets. Wählen Sie die Konsistenzstufe aus.



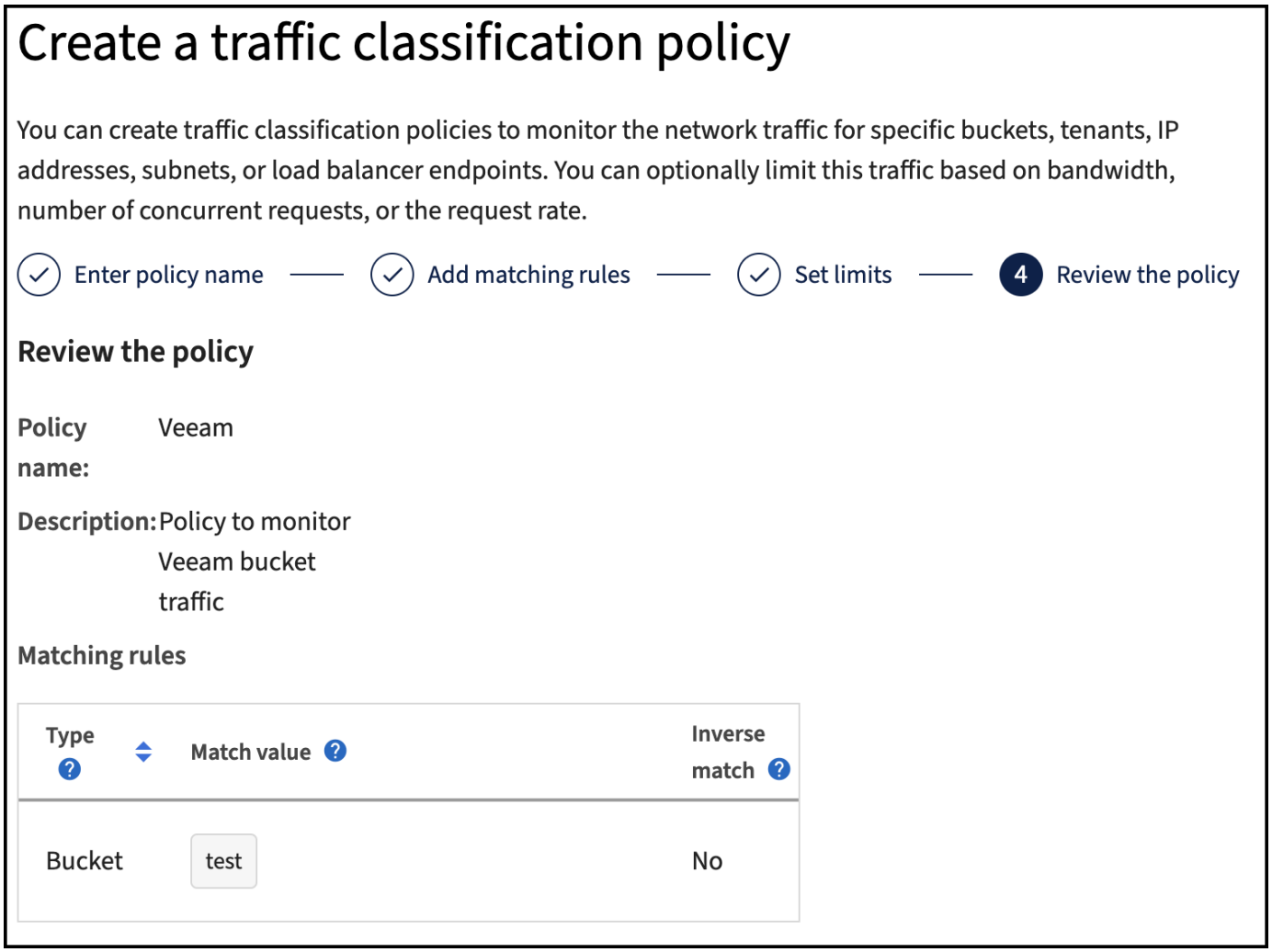
Veeam erfordert eine hohe Konsistenz für S3-Buckets. Wenn also Implementierungen an mehreren Standorten implementiert werden, bei denen Veeam von diversen Standorten auf die Daten zugreifen kann, wählen Sie „Strong Global“. Wenn Veeam-Backups und -Restores nur an einem einzigen Standort durchgeführt werden, sollte das Konsistenzniveau auf „Strong-Site“ gesetzt werden. Speichern Sie die Änderungen.



StorageGRID bietet einen integrierten Load Balancer auf jedem Admin-Node und dedizierten Gateway-Nodes.

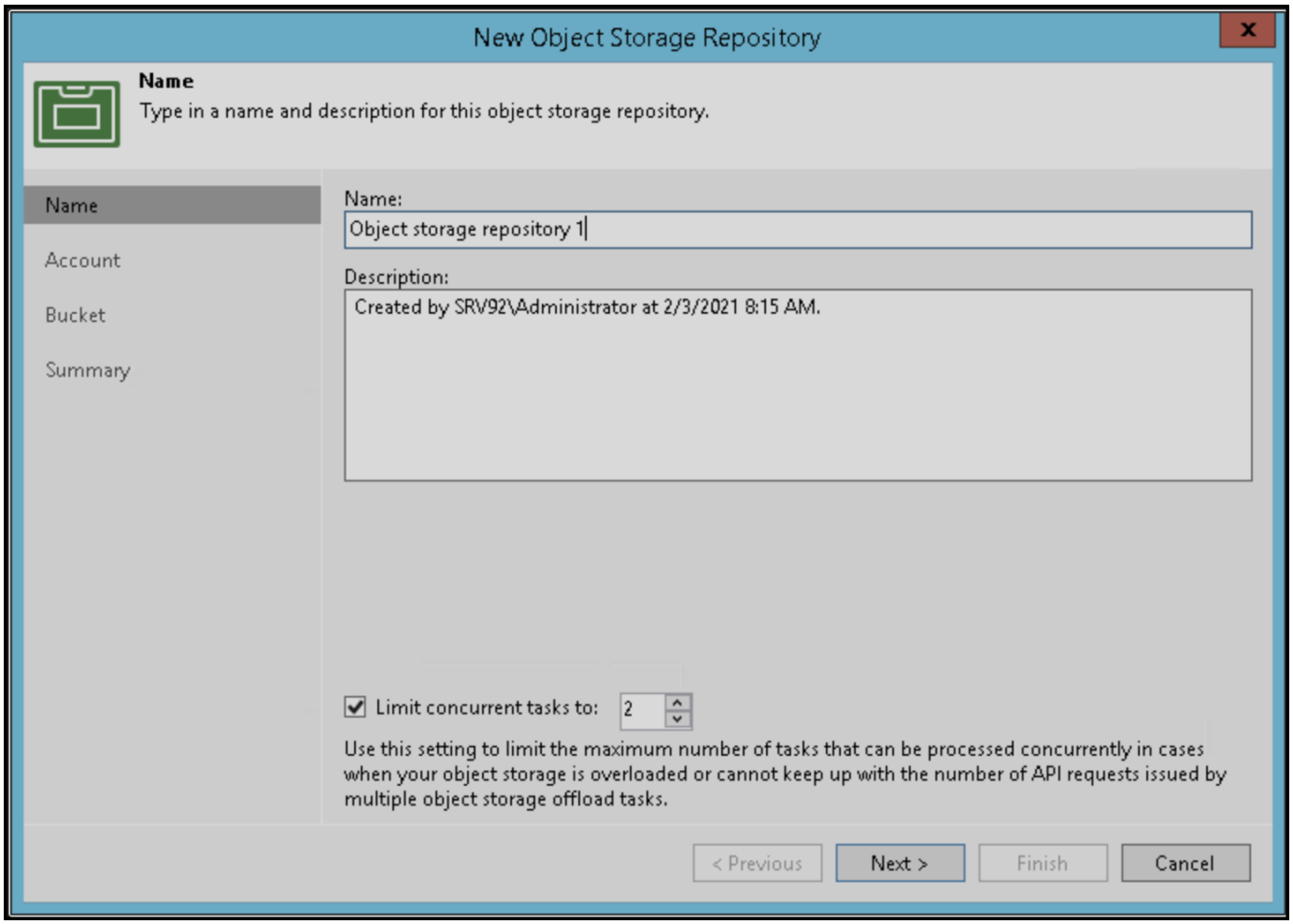
Einer der vielen Vorteile dieser Load Balancer ist die Möglichkeit zur Konfiguration von Richtlinien zur Traffic-Klassifizierung (QoS). Diese dienen hauptsächlich der Beschränkung der Auswirkungen von Applikationen auf andere Client-Workloads oder der Priorisierung von Workloads gegenüber anderen. Sie bieten jedoch auch einen Bonus bei der Erfassung zusätzlicher Metriken zur Unterstützung des Monitorings.

Wählen Sie auf der Registerkarte „Konfiguration“ die Option „Traffic Classification“ aus, und erstellen Sie eine neue Richtlinie. Benennen Sie die Regel, und wählen Sie entweder den/die Bucket(s) oder den Mandanten als Typ aus. Geben Sie die Namen der Bucket(s) oder Tenant ein. Falls QoS erforderlich ist, legen Sie eine Grenze fest. Bei den meisten Implementierungen jedoch möchten wir nur die Monitoring-Vorteile hinzufügen, damit Sie keine Obergrenze festlegen können.

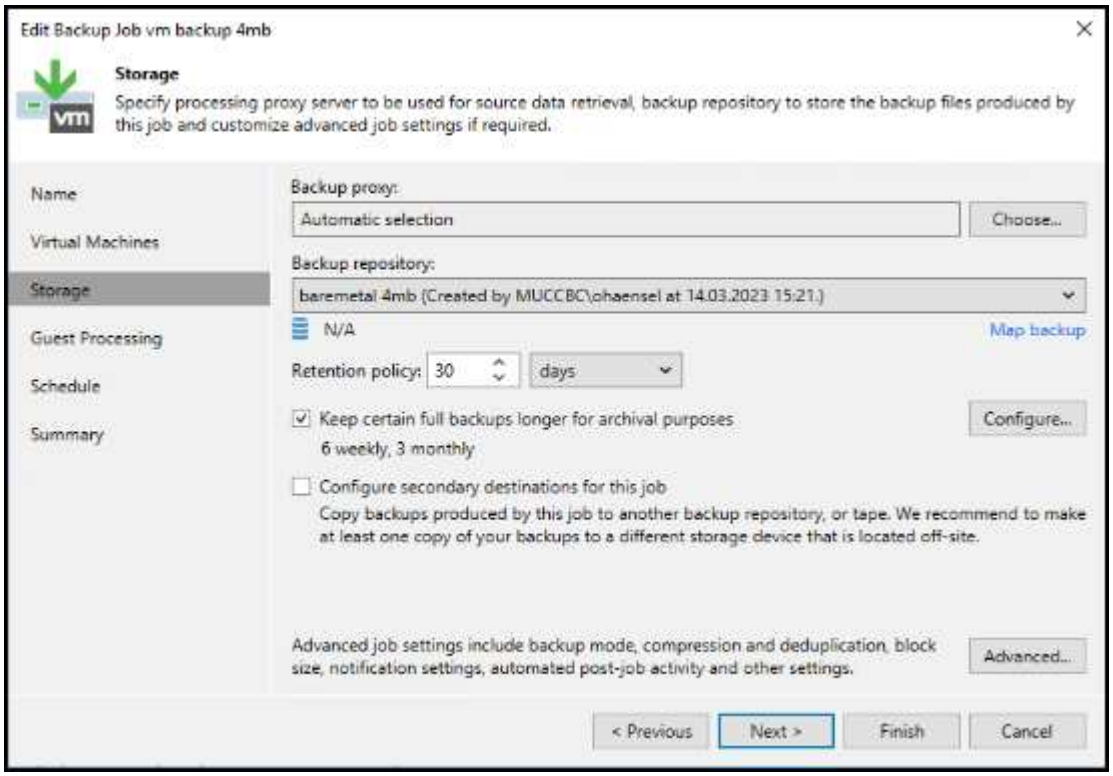


Veeam

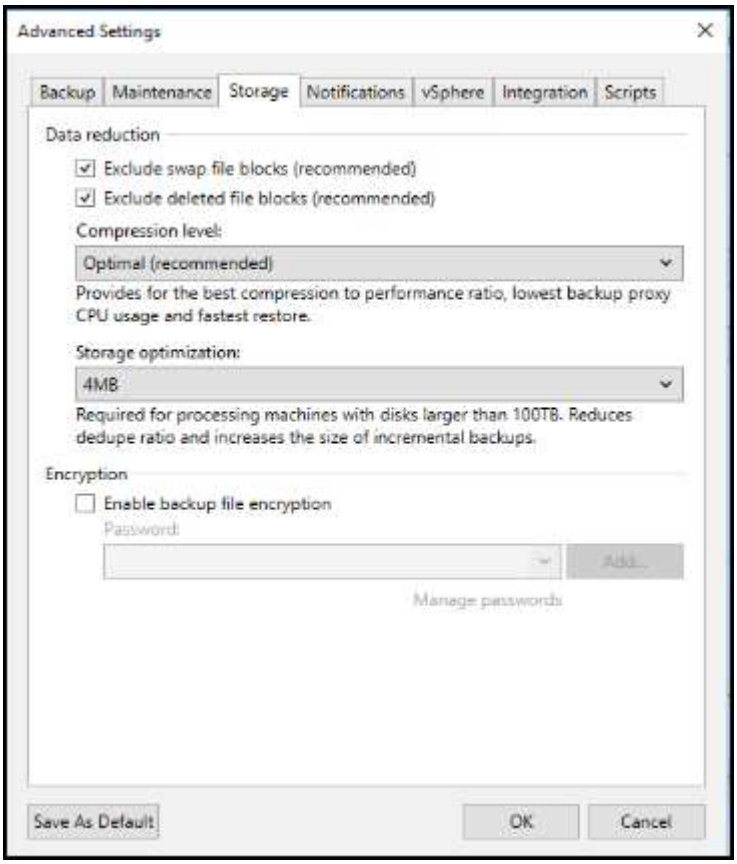
Je nach Modell und Anzahl der StorageGRID Appliances kann es erforderlich sein, eine Begrenzung der Anzahl gleichzeitiger Operationen auf dem Bucket auszuwählen und zu konfigurieren.



Folgen Sie der Veeam Dokumentation zur Konfiguration des Backup-Jobs in der Veeam Konsole, um den Assistenten zu starten. Wählen Sie nach dem Hinzufügen von VMs das SOBR-Repository aus.



Klicken Sie auf Erweiterte Einstellungen, und ändern Sie die Einstellungen für die Speicheroptimierung auf 4 MB oder mehr. Komprimierung und Deduplizierung sollen aktiviert werden. Ändern Sie die Gasteinstellungen entsprechend Ihren Anforderungen und konfigurieren Sie den Zeitplan für den Backupjob.



Monitoring von StorageGRID

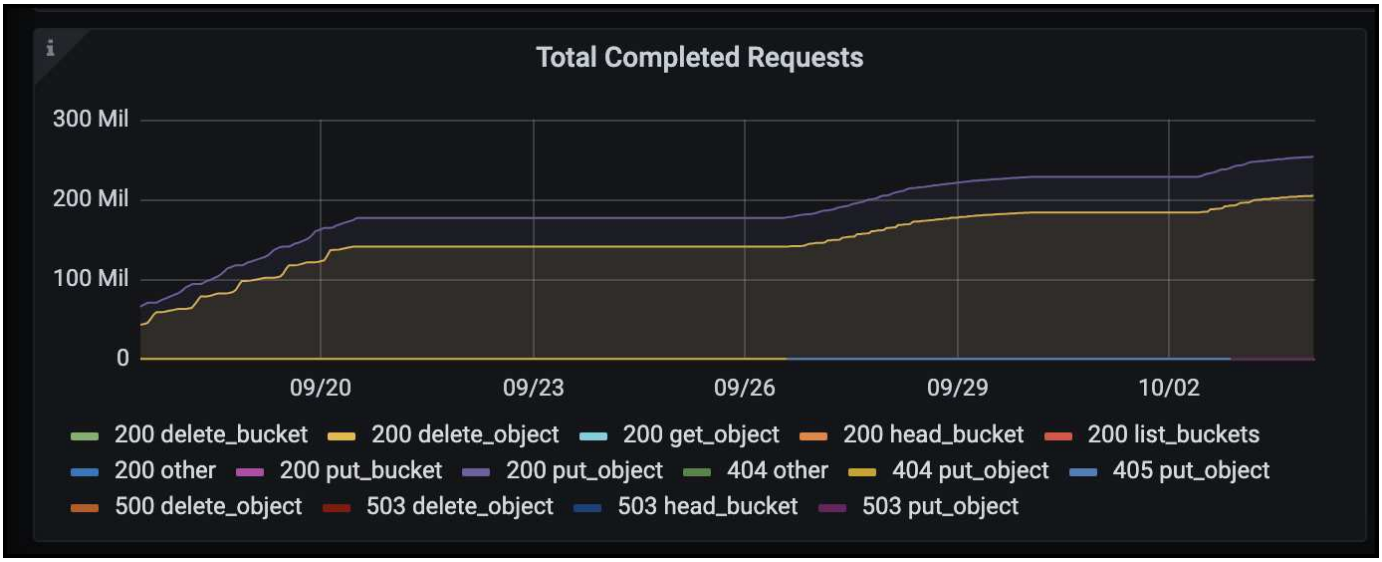
Um sich ein vollständiges Bild davon zu machen, wie Veeam und StorageGRID zusammenarbeiten, müssen Sie warten, bis die Aufbewahrungszeit der ersten Backups abgelaufen ist. Bis zu diesem Zeitpunkt besteht der Veeam-Workload in erster Linie aus PUT-Vorgängen und es sind keine Löschungen aufgetreten. Sobald Sicherungsdaten ablaufen und Clean-ups durchgeführt werden, können Sie jetzt die vollständige konsistente Nutzung im Objektspeicher sehen und die Einstellungen in Veeam bei Bedarf anpassen.

StorageGRID bietet bequeme Diagramme zur Überwachung des Betriebs des Systems auf der Registerkarte „Support“ auf der Seite „Kennzahlen“. Sie sehen sich primär die S3 Übersicht, ILM und die Richtlinie zur Klassifizierung von Datenverkehr an, wenn eine Richtlinie erstellt wurde. Im S3-Übersichts-Dashboard erhalten Sie Informationen zu den S3-Betriebsraten, Latenzen und Anfragenreaktionen.

Bei Blick auf die S3-Raten und aktiven Anfragen sehen Sie, wie viel von der Last die einzelnen Nodes verarbeiten, und wie viele Anfragen insgesamt nach Typ verarbeitet werden.

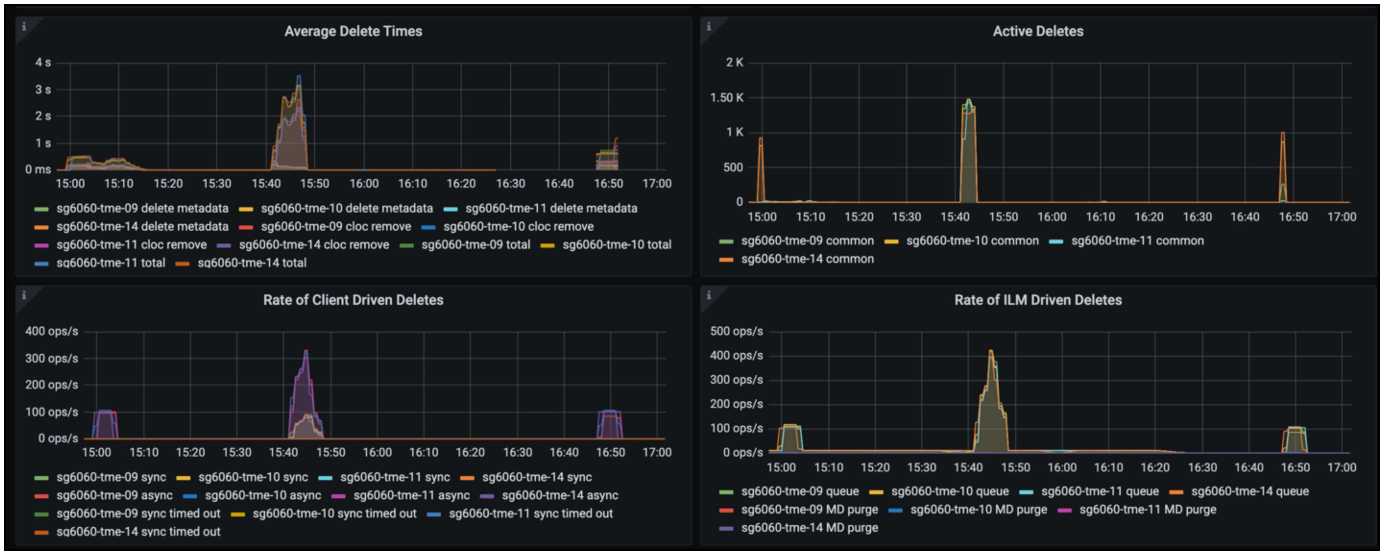
Im Diagramm „Durchschnittliche Dauer“ wird die durchschnittliche Zeit angezeigt, die jeder Knoten für jeden Anforderungstyp einnimmt. Dies ist die durchschnittliche Latenz der Anfrage und kann ein guter Indikator dafür sein, dass möglicherweise zusätzliche Anpassungen erforderlich sind, oder dass das StorageGRID-System mehr Last aufnehmen kann.

Im Diagramm „abgeschlossene Anforderungen gesamt“ werden die Anforderungen nach Typ und Antwortcodes angezeigt. Wenn Sie andere Antworten als 200 (OK) für die Antworten sehen, kann dies auf ein Problem hinweisen, wie das StorageGRID-System wird stark geladen Senden 503 (Slow Down) Antworten und einige zusätzliche Tuning erforderlich sein, oder die Zeit ist gekommen, um das System für die erhöhte Last zu erweitern.



Im ILM Dashboard können Sie die Performance beim Löschen des StorageGRID Systems überwachen.

StorageGRID verwendet eine Kombination aus synchronen und asynchronen Löschungen auf jedem Node, um die Gesamtleistung für alle Anforderungen zu optimieren.



Mithilfe einer Richtlinie zur Traffic-Klassifizierung können wir Kennzahlen zum Load Balancer Anforderungsdurchsatz, zu Raten, zur Dauer sowie zu den Objektgrößen anzeigen, die Veeam sendet und empfängt.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- "NetApp StorageGRID -Produktdokumentation"
- "Veeam Backup und Replication"

Dremio Datenquelle mit StorageGRID konfigurieren

Von Angela Cheng

Dremio unterstützt eine Vielzahl von Datenquellen, einschließlich Cloud-basiertem oder lokalem Objektspeicher. Sie können Dremio so konfigurieren, dass StorageGRID als Objektspeicher-Datenquelle verwendet wird.

Dremio-Datenquelle konfigurieren

Voraussetzungen

- Eine StorageGRID S3-Endpunkt-URL, eine s3-Zugriffsschlüssel-ID des Mandanten und ein geheimer Zugriffsschlüssel.
- StorageGRID-Konfigurationsempfehlung: Deaktivieren Sie die Komprimierung (standardmäßig deaktiviert).

  Dremio verwendet Byte-Bereich GET, um während der Abfrage verschiedene Byte-Bereiche aus demselben Objekt gleichzeitig abzurufen. Die typische Größe für Anforderungen im Byte-Bereich beträgt 1 MB. Komprimiertes Objekt beeinträchtigt die GET-Performance im Byte-Bereich.

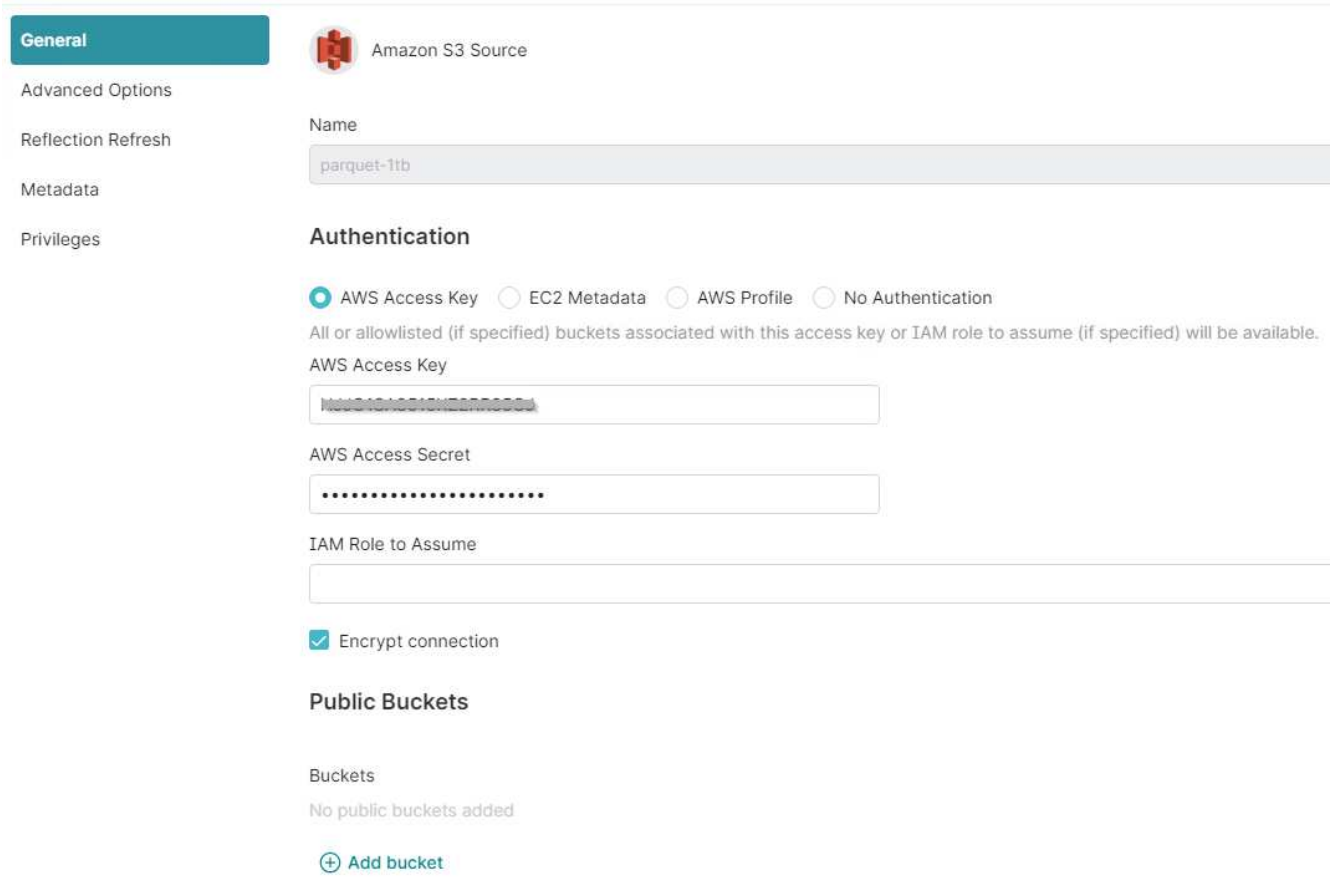
Dremio-Führer

"Connecting to Amazon S3 - Configuring S3-Compatible Storage".

Anweisung

1. Klicken Sie auf der Seite Dremio Datasets auf + signieren, um eine Quelle hinzuzufügen, und wählen Sie „Amazon S3“.
2. Geben Sie einen Namen für diese neue Datenquelle ein: StorageGRID S3-Mandanten-Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel.
3. Aktivieren Sie das Kontrollkästchen „Verbindung verschlüsseln“, wenn HTTPS für die Verbindung zum

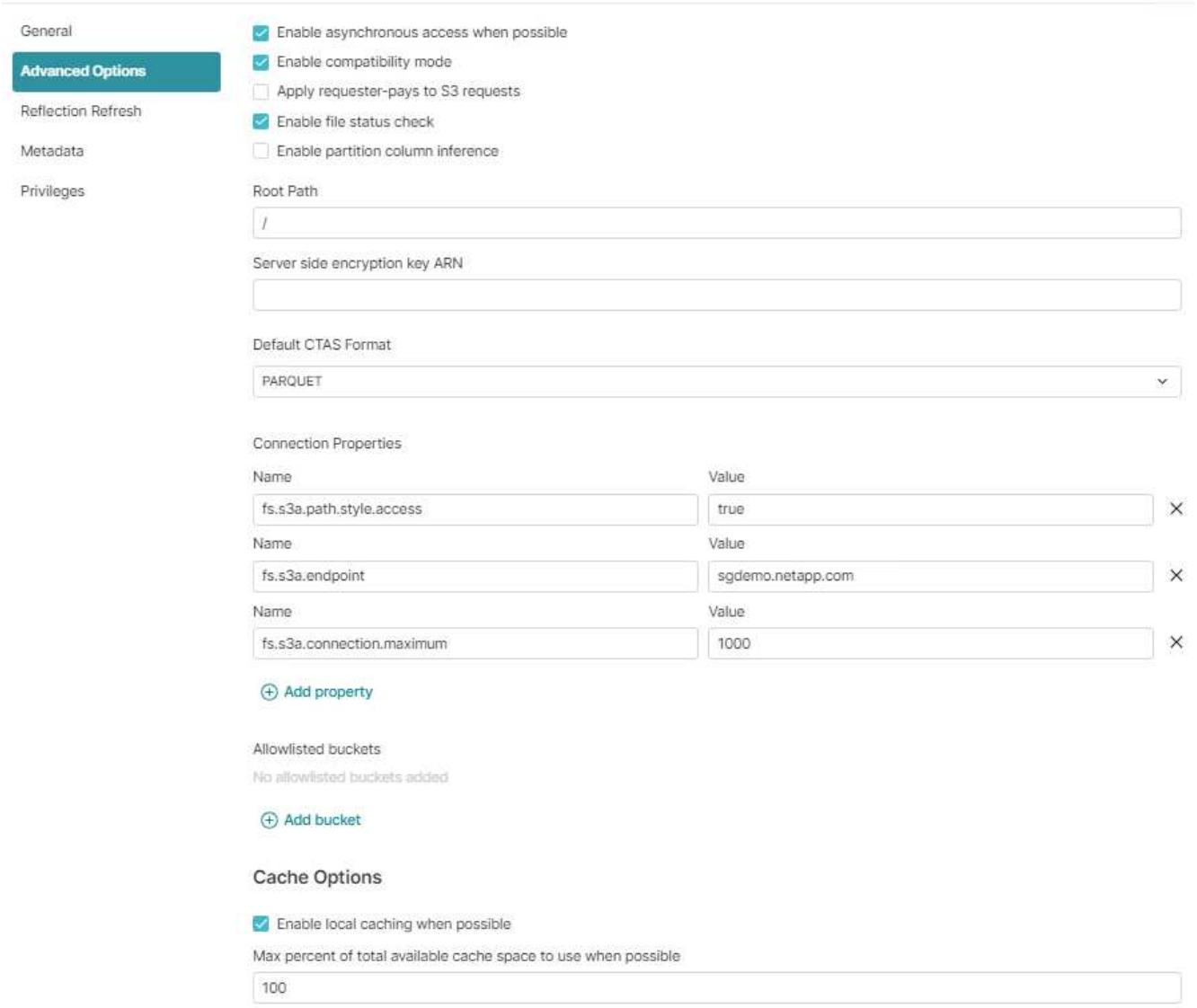
StorageGRID S3-Endpunkt verwendet wird.
Wenn Sie ein selbstsigniertes CA-Zertifikat für diesen s3-Endpunkt verwenden, folgen Sie der Dremio-Anleitung, um dieses CA-Zertifikat in den <JAVA_HOME>/jre/lib/Security + des Dremio-Servers hinzuzufügen
Beispiel Screenshot



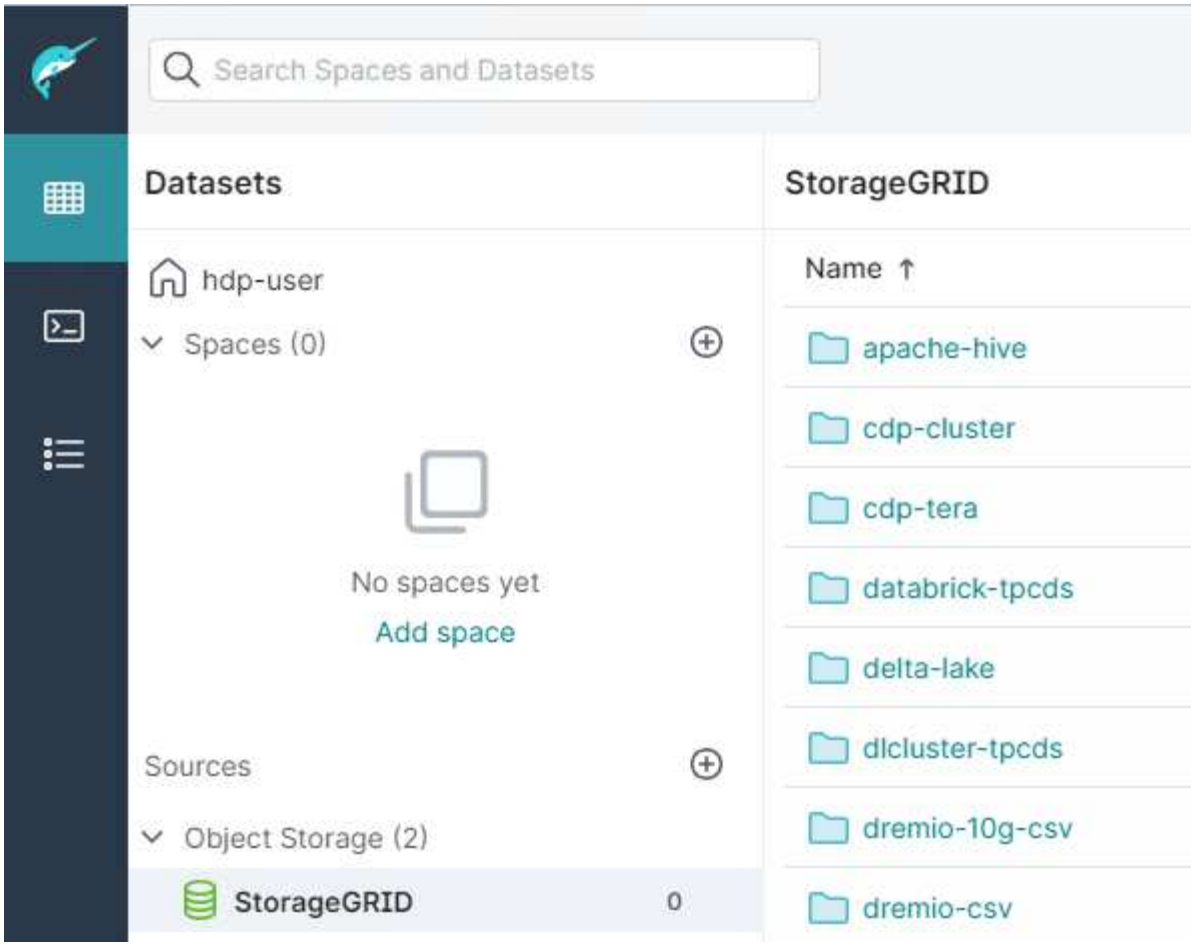
4. Klicken Sie auf „Erweiterte Optionen“, und aktivieren Sie „Kompatibilitätsmodus aktivieren“.
5. Klicken Sie unter Verbindungseigenschaften auf + Eigenschaften hinzufügen, und fügen Sie diese s3a-Eigenschaften hinzu.
6. fs.s3a.Connection.die Standardeinstellung ist 100. Wenn Ihre s3-Datensätze große Parkett-Dateien mit 100 oder mehr Spalten enthalten, muss ein Wert größer als 100 eingegeben werden. Diese Einstellung finden Sie im Dremio-Handbuch.

Name	Wert
fs.s3a.Endpunkt	*<StorageGRID S3 Endpunkt:Port>*
fs.s3a.path.style.Access	Richtig
fs.s3a.Verbindung.Maximum	*<ein Wert größer als 100>*

Beispiel Screenshot



7. Konfigurieren Sie andere Dremio-Optionen gemäß Ihren Unternehmens- oder Anwendungsanforderungen.
8. Klicken Sie auf die Schaltfläche Speichern, um diese neue Datenquelle zu erstellen.
9. Sobald die StorageGRID-Datenquelle erfolgreich hinzugefügt wurde, wird im linken Bereich eine Liste der Buckets angezeigt.
   Beispiel Screenshot



NetApp StorageGRID mit GitLab

Von Angela Cheng

NetApp hat StorageGRID mit GitLab getestet. Siehe Beispielkonfiguration für GitLab unten. Siehe "Gitlab Leitfaden zur Konfiguration von Objektspeicher" Entsprechende Details.

Beispiel für eine Objekt-Storage-Verbindung

Für Linux Package-Installationen ist dies ein Beispiel für das `connection` Einstellung im konsolidierten Formular. Bearbeiten `/etc/gitlab/gitlab.rb` Und fügen Sie die folgenden Zeilen hinzu, um die gewünschten Werte zu ersetzen:

```
# Consolidated object storage configuration
gitlab_rails['object_store']['enabled'] = true
gitlab_rails['object_store']['proxy_download'] = true
gitlab_rails['object_store']['connection'] = {
  'provider' => 'AWS',
  'region' => 'us-east-1',
  'endpoint' => 'https://<storagegrid-s3-endpoint:port>',
  'path_stype' => 'true',
  'aws_access_key_id' => '<AWS_ACCESS_KEY_ID>',
  'aws_secret_access_key' => '<AWS_SECRET_ACCESS_KEY>'
}
# OPTIONAL: The following lines are only needed if server side encryption
is required
gitlab_rails['object_store']['storage_options'] = {
  'server_side_encryption' => 'AES256'
}
gitlab_rails['object_store']['objects']['artifacts']['bucket'] = 'gitlab-
artifacts'
gitlab_rails['object_store']['objects']['external_diffs']['bucket'] =
'gitlab-mr-diffs'
gitlab_rails['object_store']['objects']['lfs']['bucket'] = 'gitlab-lfs'
gitlab_rails['object_store']['objects']['uploads']['bucket'] = 'gitlab-
uploads'
gitlab_rails['object_store']['objects']['packages']['bucket'] = 'gitlab-
packages'
gitlab_rails['object_store']['objects']['dependency_proxy']['bucket'] =
'gitlab-dependency-proxy'
gitlab_rails['object_store']['objects']['terraform_state']['bucket'] =
'gitlab-terraform-state'
gitlab_rails['object_store']['objects']['pages']['bucket'] = 'gitlab-
pages'
```

Beispiele für Verfahren und APIs

Testen und Demonstrieren der S3 Verschlüsselungsoptionen auf StorageGRID

Von Aron Klein

StorageGRID und die S3-API bieten verschiedene Methoden zur Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter "Prüfen Sie die StorageGRID Verschlüsselungsmethoden".

In diesem Leitfaden werden die S3-API-Verschlüsselungsmethoden demonstriert.

Serverseitige Verschlüsselung (SSE)

Mit SSE kann der Client ein Objekt speichern und mit einem eindeutigen Schlüssel verschlüsseln, der von StorageGRID verwaltet wird. Wenn das Objekt angefordert wird, wird das Objekt durch den in StorageGRID gespeicherten Schlüssel entschlüsselt.

Beispiel: SSE

- SETZEN Sie ein Objekt mit SSE

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- LEITEN Sie das Objekt, um die Verschlüsselung zu überprüfen

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- GET das Objekt

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)

Mit SSE kann der Client ein Objekt speichern und mit einem eindeutigen Schlüssel verschlüsseln, der vom Client mit dem Objekt bereitgestellt wird. Wenn das Objekt angefordert wird, muss derselbe Schlüssel bereitgestellt werden, um das Objekt zu entschlüsseln und zurückzugeben.

Beispiel SSE-C

- Sie können zu Test- oder Demonstrationszwecken einen Schlüssel erstellen
  - Erstellen eines Verschlüsselungsschlüssels

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- Legen Sie ein Objekt mit dem generierten Schlüssel

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- Das Objekt in den Kopf stellen

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:20:02+00:00",
    "ContentLength": 47,
    "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
    "ContentType": "binary/octet-stream",
    "Metadata": {},
    "SSECustomerAlgorithm": "AES256",
    "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
}
```

Wenn Sie den Verschlüsselungsschlüssel nicht angeben, erhalten Sie einen Fehler „ein Fehler ist aufgetreten (404), wenn Sie den HeadObject-Vorgang aufrufen: Nicht gefunden“.

- Get das Objekt

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

Wenn Sie den Verschlüsselungsschlüssel nicht bereitstellen, erhalten Sie beim Aufruf des GetObject-Vorgangs einen Fehler „aufgetreten (InvalidRequest): Das Objekt wurde mit einer Form von serverseitiger Verschlüsselung gespeichert. Zum Abrufen des Objekts müssen die richtigen Parameter angegeben werden.“

Bucket-serverseitige Verschlüsselung (SSE-S3)

Mit SSE-S3 kann der Client ein Standardverschlüsselungsverhalten für alle in einem Bucket gespeicherten Objekte definieren. Die Objekte werden mit einem eindeutigen Schlüssel verschlüsselt, der von StorageGRID gemanagt wird. Wenn das Objekt angefordert wird, wird das Objekt von dem in StorageGRID gespeicherten Schlüssel entschlüsselt.

Beispiel für Bucket SSE-S3

- Erstellen eines neuen Buckets und Festlegen einer Standardverschlüsselungsrichtlinie
  - Erstellen eines neuen Buckets

    ```
    aws s3api create-bucket --bucket <bucket> --region us-east-1
    --endpoint-url https://s3.example.com
    ```

  - Put Bucket-Verschlüsselung

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- Legen Sie ein Objekt in den Bucket

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- Das Objekt in den Kopf stellen

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- GET das Objekt

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

S3-Objektsperre auf StorageGRID testen und demonstrieren

Von Aron Klein

Object Lock bietet ein WORM-Modell, um das Löschen oder Überschreiben von Objekten zu verhindern. Die StorageGRID Implementierung von Objektsperrung wird auf Cohasset überprüft, um gesetzliche Vorgaben einzuhalten, den gesetzlichen Aufbewahrungs- und Compliance-Modus für Objektspeicherung zu unterstützen und standardmäßige Bucket-Aufbewahrungsrichtlinien einzuhalten.

In diesem Handbuch wird die S3-Objekt-Lock-API demonstriert.

Gesetzliche Aufbewahrungspflichten

- Object Lock Legal Hold ist ein einfacher ein-/Ausschaltstatus, der auf ein Objekt angewendet wird.

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- Überprüfen Sie es mit EINEM GET-Vorgang.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- Deaktivieren Sie die gesetzliche Aufbewahrungspflichten

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- Überprüfen Sie es mit EINEM GET-Vorgang.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Compliance-Modus

- Die Objektspeicherung erfolgt mit einer Aufbewahrung bis zum Zeitstempel.

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- Überprüfen Sie den Aufbewahrungsstatus

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

Standardaufbewahrung

- Legen Sie den Aufbewahrungszeitraum in Tagen und Jahren als Aufbewahrungsdatum fest, das mit der API pro Objekt definiert wurde.

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- Überprüfen Sie den Aufbewahrungsstatus

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- Legen Sie ein Objekt in den Bucket

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- Die auf dem Bucket festgelegte Aufbewahrungsdauer wird in einen Aufbewahrungszeitstempel des Objekts konvertiert.

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Testen Löschen eines Objekts mit einer definierten Aufbewahrung

Objekt Lock basiert auf der Versionierung. Die Aufbewahrung ist für eine Version des Objekts definiert. Wenn versucht wird, ein Objekt mit einer definierten Aufbewahrung zu löschen, und keine Version angegeben wird, wird als aktuelle Version des Objekts eine Löschmarkierung erstellt.

- Löschen Sie das Objekt mit definierter Aufbewahrung

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- Listen Sie die Objekte im Bucket auf

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

  - Beachten Sie, dass das Objekt nicht aufgeführt ist.
- Listen Sie Versionen auf, um die Löschen-Markierung und die ursprüngliche gesperrte Version anzuzeigen

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- Löschen Sie die gesperrte Version des Objekts

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

Richtlinien und Berechtigungen in StorageGRID

Hier sind Beispielrichtlinien und Berechtigungen in StorageGRID S3.

Die Struktur einer Richtlinie

In StorageGRID sind die Gruppenrichtlinien mit den S3 Service-Richtlinien für AWS Benutzer (IAM) identisch.

Gruppenrichtlinien sind in StorageGRID erforderlich. Ein Benutzer mit S3-Zugriffsschlüsseln, aber keiner Benutzergruppe zugewiesen oder einer Gruppe ohne Richtlinie zugewiesen, die einige Berechtigungen erteilt, kann auf keine Daten zugreifen.

Bucket- und Gruppenrichtlinien verwenden die meisten Elemente gemeinsam. Richtlinien werden im json-Format erstellt und können mit dem erstellt werden "AWS-Richtliniengenerator"

Alle Richtlinien definieren den Effekt, die Aktion(en) und die Ressource(en). In Bucket-Richtlinien wird auch ein Principal definiert.

Der **Effekt** wird entweder sein, die Anfrage zuzulassen oder abzulehnen.

Der * Principal*

- Gilt nur für Bucket-Richtlinien.
- Der Hauptbenutzer ist der/die Konto(e)/Benutzer, dem/den die Berechtigungen gewährt oder verweigert werden.
- Kann definiert werden als:
  - Ein Platzhalter „+*“

    ```
    "Principal":"*"
    ```

    ```
    "Principal":{"AWS":"*"}
    ```

  - Eine Mandanten-ID für alle Benutzer in einem Mandanten (entspricht AWS-Konto)

```
"Principal": { "AWS": "27233906934684427525" }
```

- Ein Benutzer (lokal oder föderiert aus dem Mandanten, der sich im Bucket befindet, oder ein anderer Mandant im Grid)

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:user/tenant1user1" }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/tenant2user1" }
```

- Eine Gruppe (lokal oder föderiert aus dem Mandanten, der sich im Bucket befindet, oder ein anderer Mandant im Grid).

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:group/DevOps"  }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

Die **Aktion** ist der Satz von S3-Operationen, die dem/den Benutzer(n) gewährt oder verweigert werden.

> Für Gruppenrichtlinien ist die zulässige Aktion s3:ListBucket erforderlich, damit Benutzer alle S3-Aktionen ausführen können.

Die **Ressource** ist der Eimer oder Eimer, dem die Principals die Fähigkeit zur Ausführung der Aktionen gewährt oder verweigert werden. Optional kann es eine **Bedingung** geben, wenn die Richtlinienaktion gültig ist.

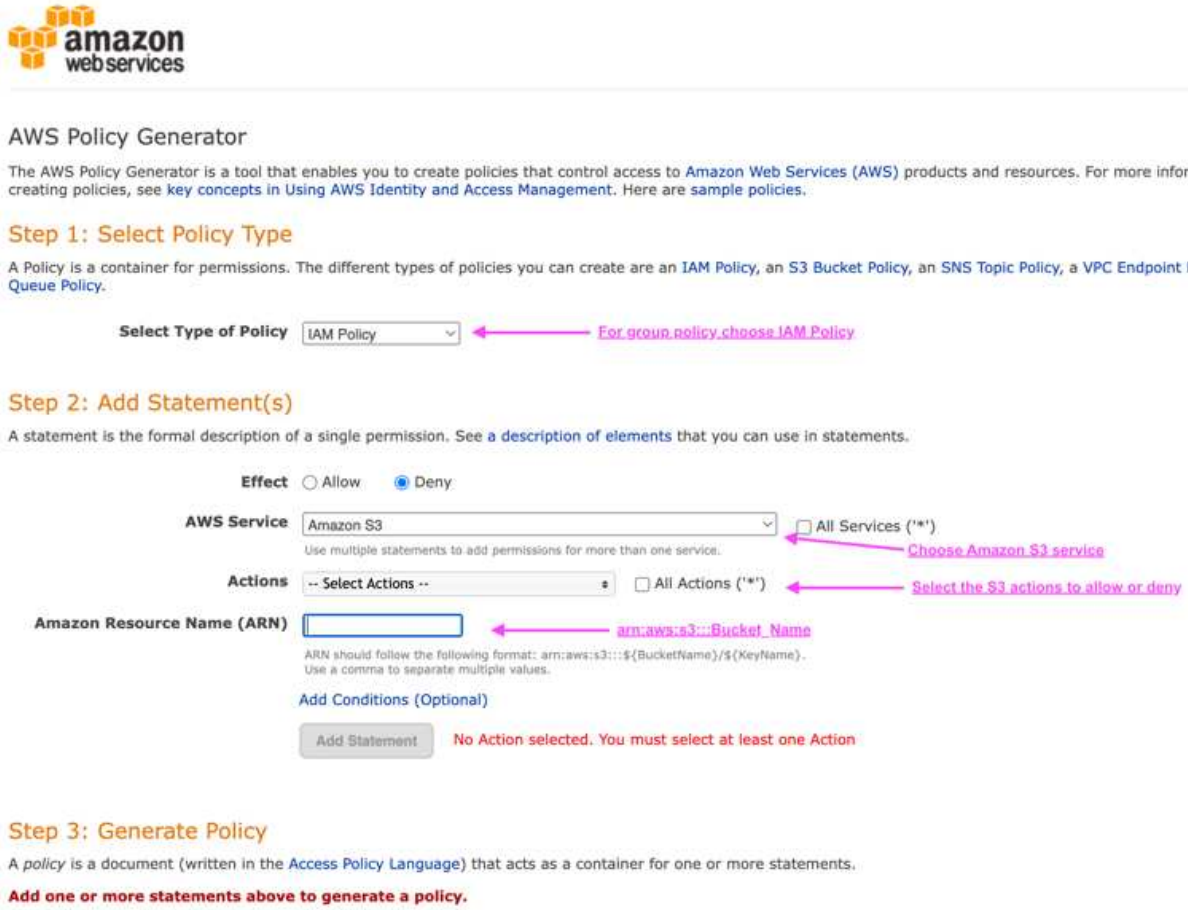
Das Format der JSON-Richtlinie sieht wie folgt aus:

```
{
  "Statement": [
    {
      "Sid": "Custom name for this permission",
      "Effect": "Allow or Deny",
      "Principal": {
        "AWS": [
          "arn:aws:iam::tenant_ID::user/User_Name",
          "arn:aws:iam::tenant_ID::federated-user/User_Name",
          "arn:aws:iam::tenant_ID:group/Group_Name",
          "arn:aws:iam::tenant_ID:federated-group/Group_Name",
          "tenant_ID"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:Other_Action"
      ],
      "Resource": [
        "arn:aws:s3:::Example_Bucket",
        "arn:aws:s3:::Example_Bucket/*"
      ],
    }
  ]
}
```

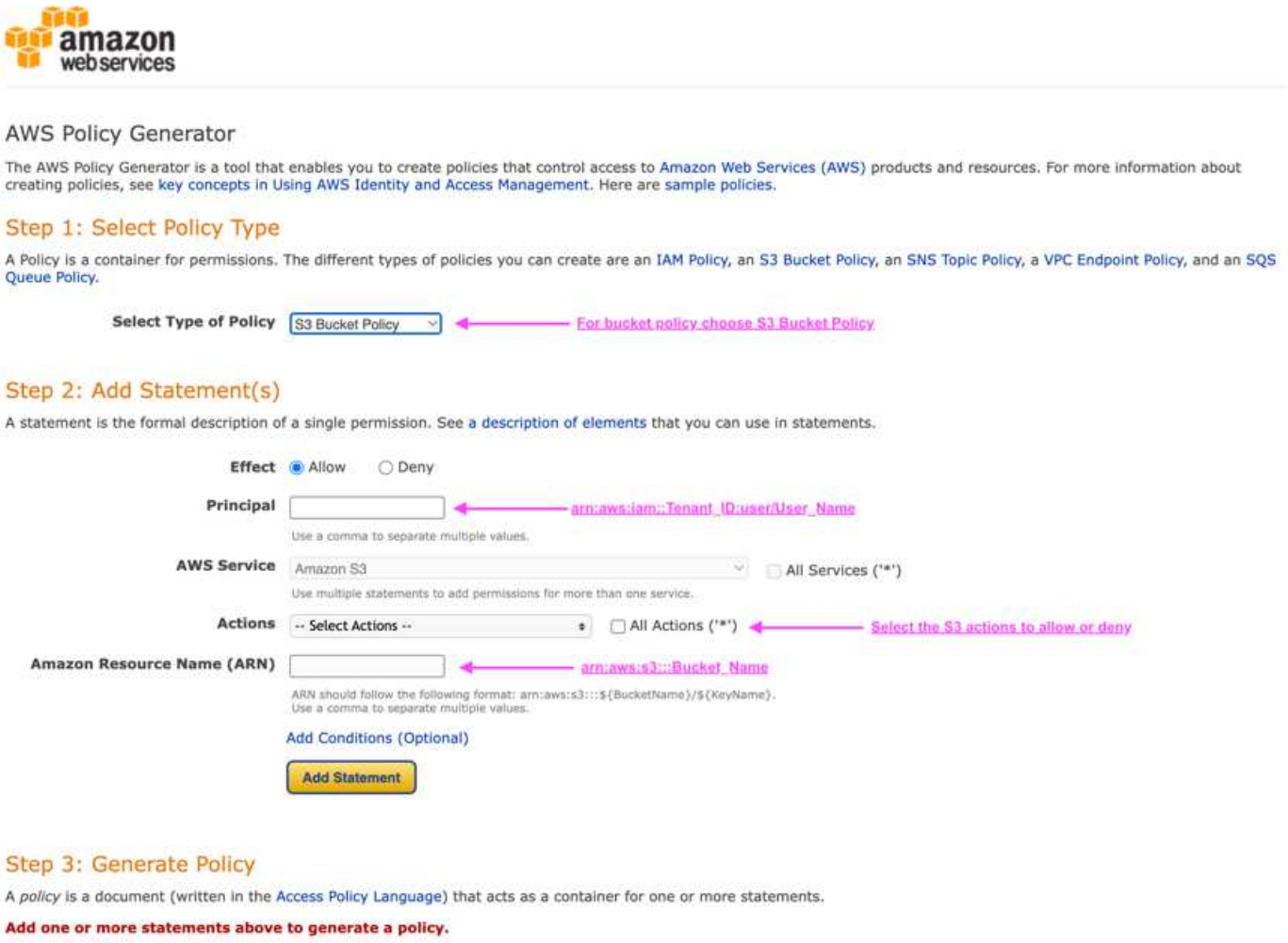
Verwenden des AWS-Richtliniengenerators

Der AWS Richtlinien-Generator ist ein großartiges Werkzeug, um den json-Code mit dem richtigen Format und den Informationen zu erhalten, die Sie zu implementieren versuchen.

So generieren Sie die Berechtigungen für eine StorageGRID-Gruppenrichtlinie: * Wählen Sie die IAM-Richtlinie für den Typ der Richtlinie aus. * Wählen Sie die Schaltfläche für den gewünschten Effekt - Zulassen oder verweigern. Es empfiehlt sich, Ihre Richtlinien mit den Deny-Berechtigungen zu starten und dann die Allow-Berechtigungen * in das Dropdown-Menü Actions hinzuzufügen. Klicken Sie auf das Feld neben so vielen S3-Aktionen, die Sie in diese Berechtigung oder das Feld „All Actions“ aufnehmen möchten. * Geben Sie die Bucket-Pfade in das Feld Amazon Resource Name (ARN) ein. Fügen Sie vor dem Bucket-Namen „arn:aws:s3:::“ ein. Beispiel: „arn:aws:s3::example_bucket“

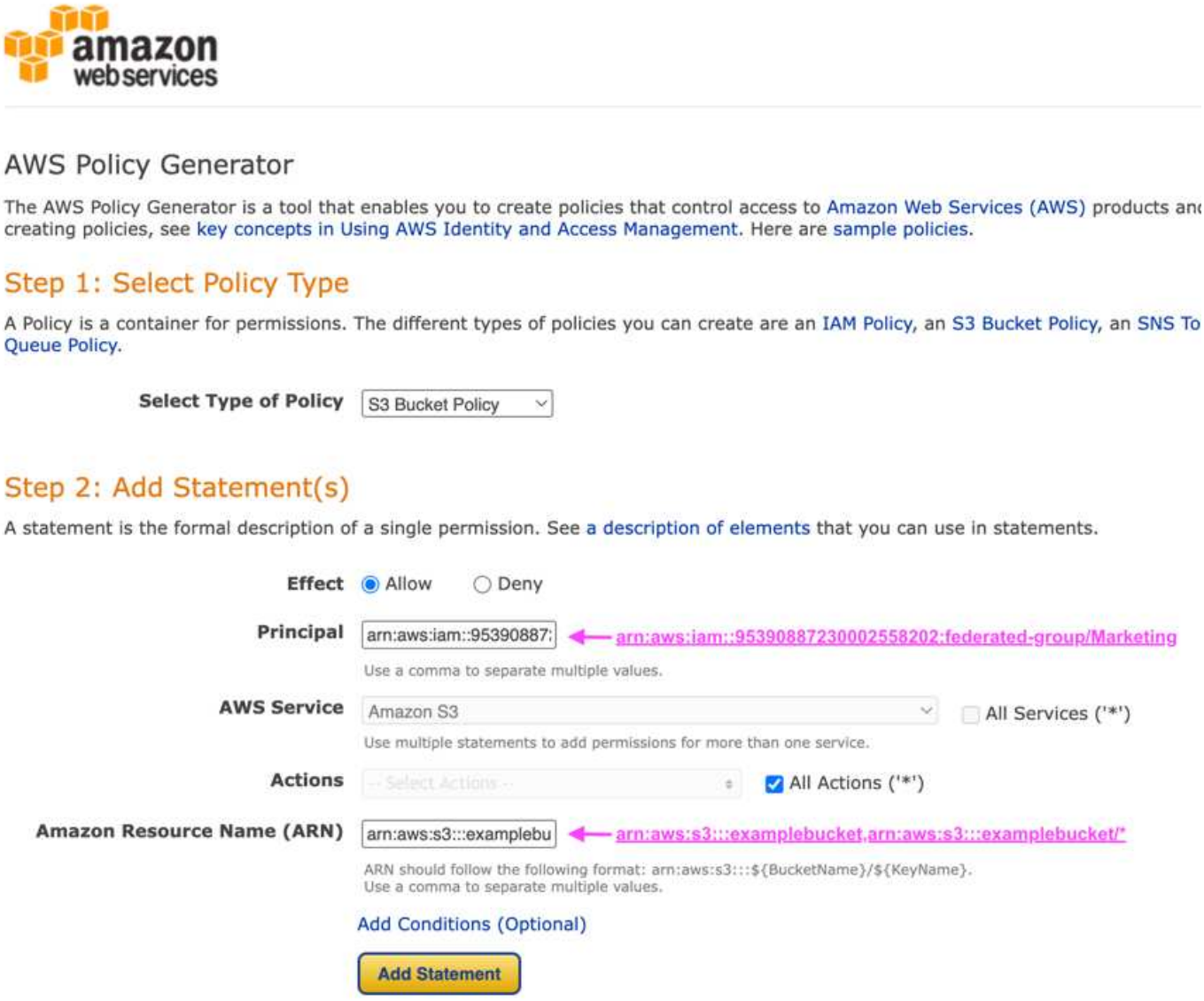


So generieren Sie die Berechtigungen für eine Bucket-Richtlinie: * Wählen Sie die S3-Bucket-Richtlinie für den Typ der Richtlinie aus. * Wählen Sie die Schaltfläche für den gewünschten Effekt - Zulassen oder verweigern. Es empfiehlt sich, Ihre Richtlinien mit den Berechtigungen „verweigern“ zu starten und anschließend den Typ „Berechtigungen zulassen“ * in die Benutzer- oder Gruppeninformationen für den Prinzipal einzufügen. * Klicken Sie in der Dropdown-Liste Aktionen auf das Feld neben so vielen S3-Aktionen, die Sie in diese Berechtigung oder das Feld "Alle Aktionen" aufnehmen möchten. * Geben Sie die Bucket-Pfade in das Feld Amazon Resource Name (ARN) ein. Fügen Sie vor dem Bucket-Namen „arn:aws:s3:::“ ein. Beispiel: „arn:aws:s3::example_bucket“



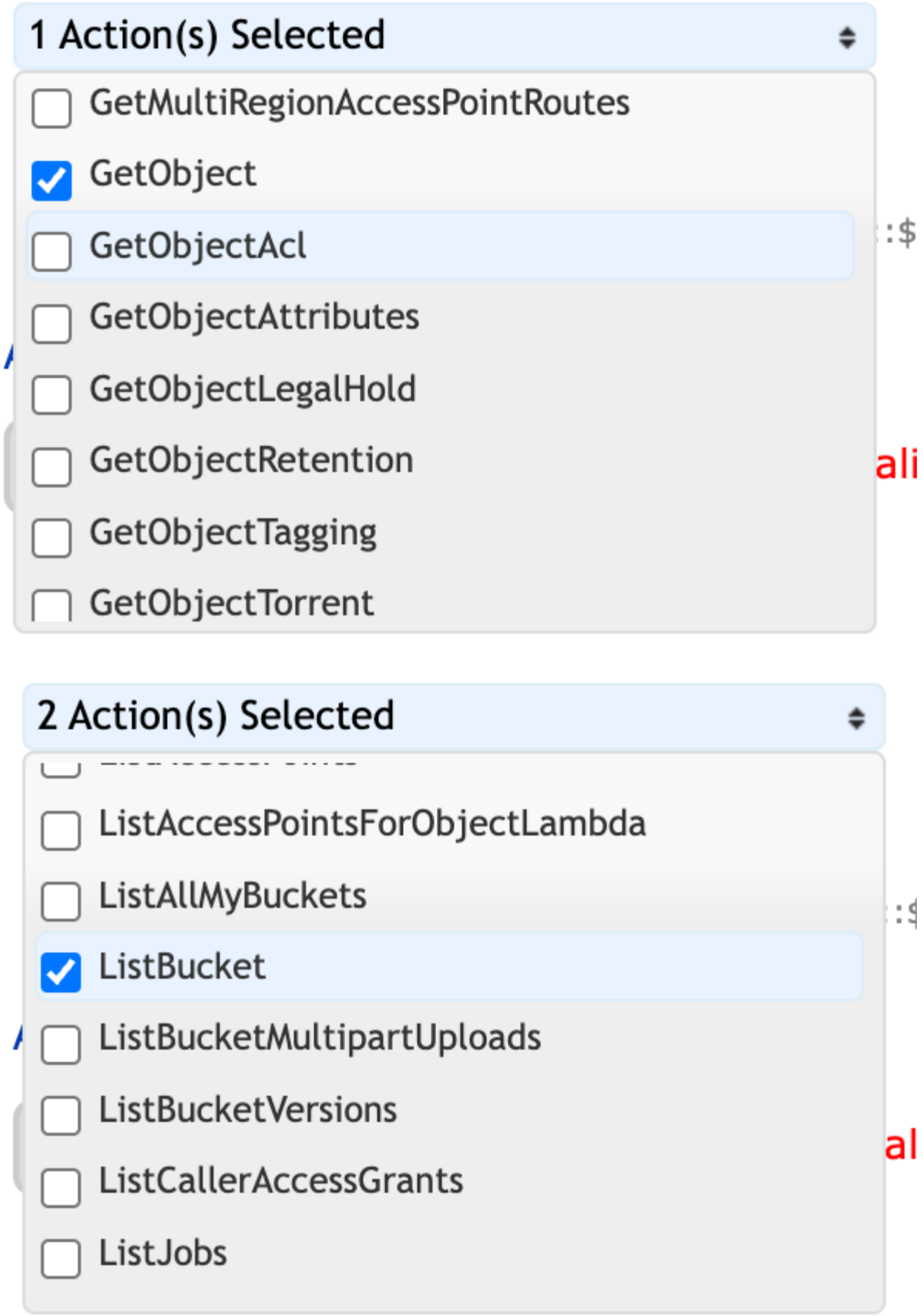
Wenn Sie beispielsweise eine Bucket-Richtlinie erstellen möchten, die allen Benutzern die Ausführung von GetObject-Operationen für alle Objekte im Bucket ermöglicht, während nur Benutzern, die der Gruppe „Marketing“ im angegebenen Konto angehören, Vollzugriff gewährt wird.

- Wählen Sie als Richtlinientyp S3-Bucket-Richtlinie aus.
- Wählen Sie den Zulassen-Effekt
- Geben Sie die Informationen der Marketinggruppe ein - arn:aws:iam::95390887230002558202:Federated-Group/Marketing
- Klicken Sie auf das Feld für „Alle Aktionen“.
- Geben Sie die Bucket-Informationen ein - arn:aws:s3:::example_bucket,arn:aws:s3:::example_bucket/*

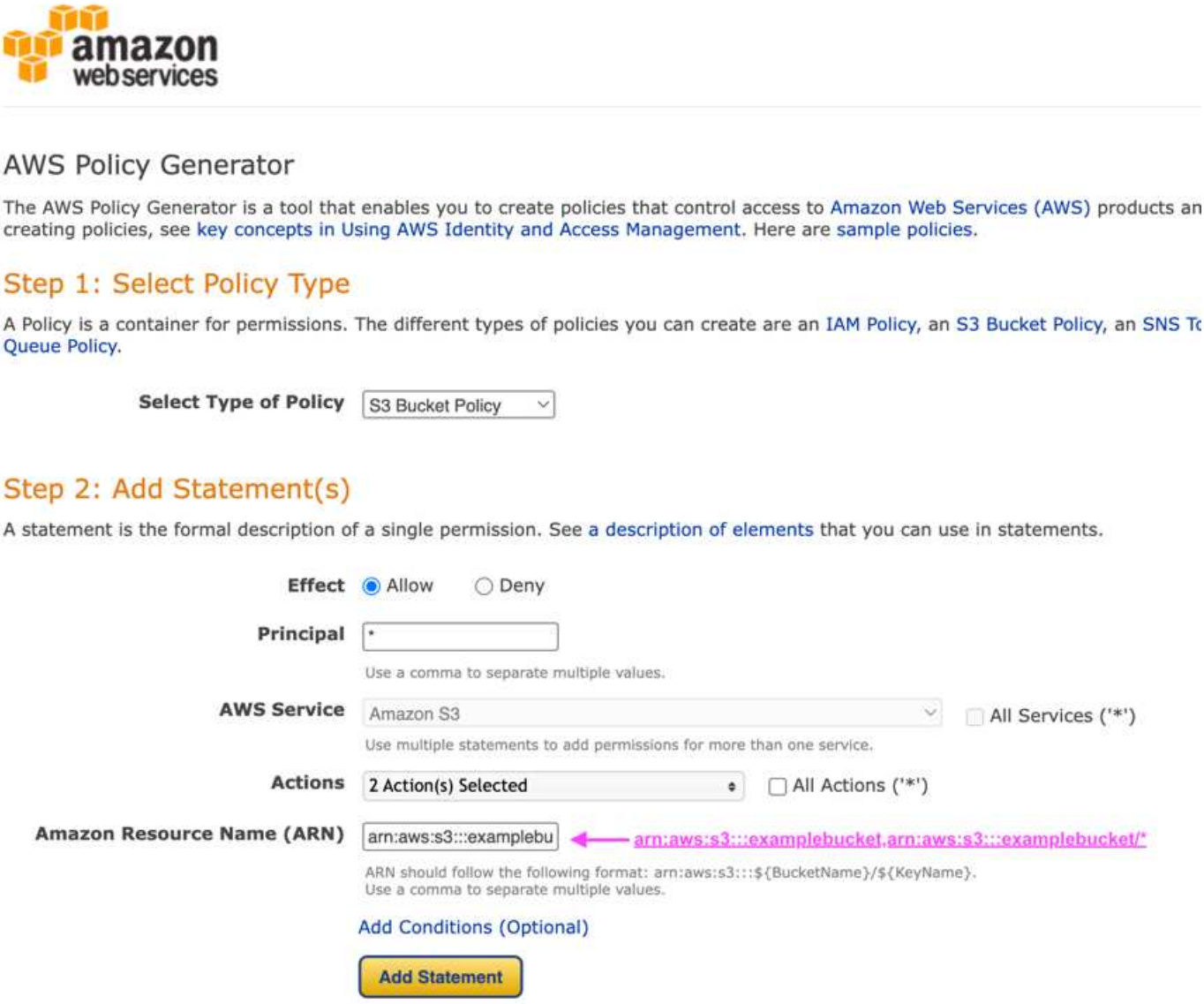


- Klicken Sie auf die Schaltfläche „Anweisung hinzufügen“

- Wählen Sie den Zulassen-Effekt
- Geben Sie das Sternchen +* für alle ein
- Klicken Sie auf das Feld neben GetObject und ListBucket Actions“

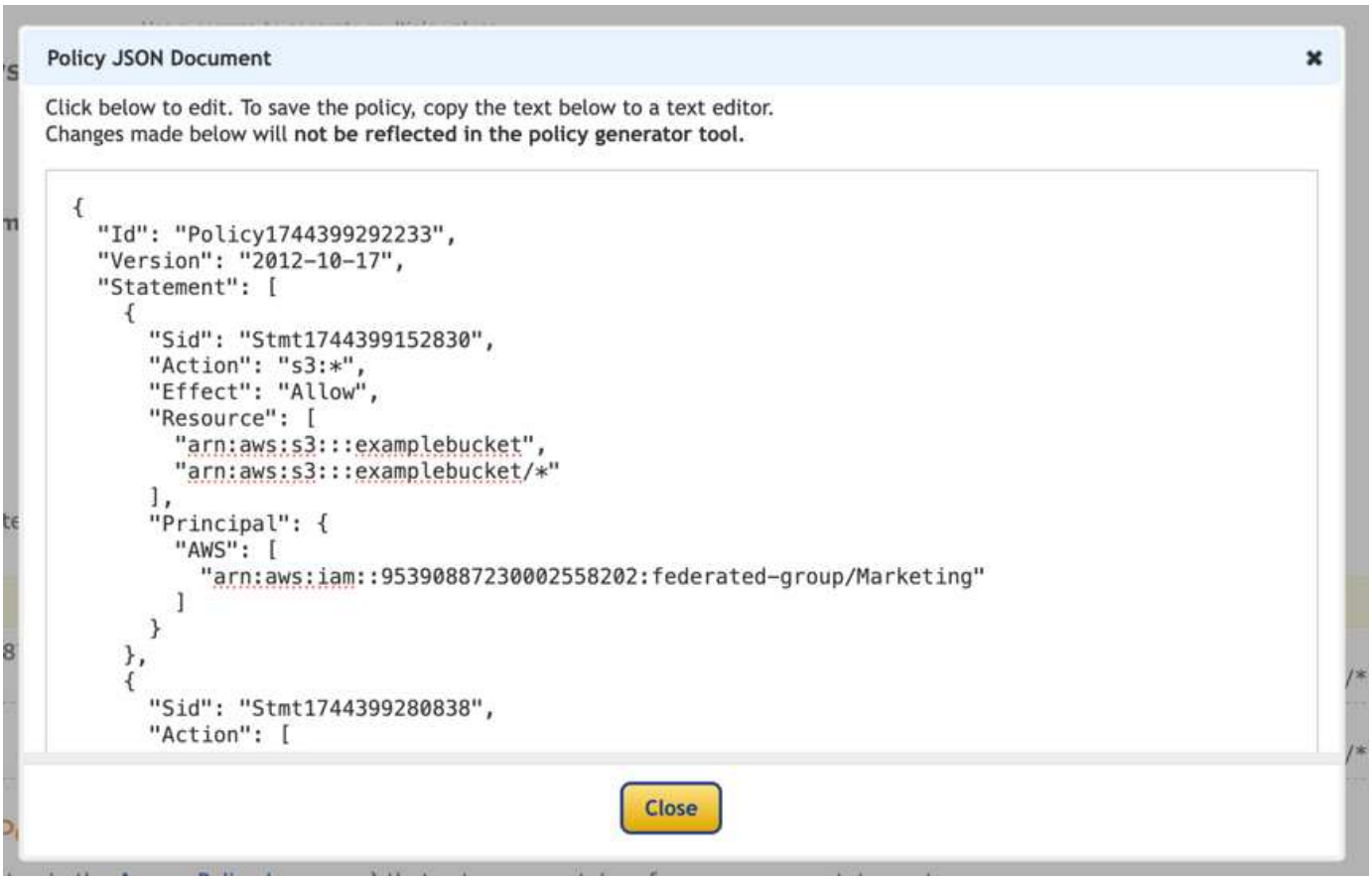


- Geben Sie die Bucket-Informationen ein - arn:aws:s3:::example_bucket,arn:aws:s3:::example_bucket/*



- Klicken Sie auf die Schaltfläche „Anweisung hinzufügen“

- Klicken Sie auf die Schaltfläche „Richtlinie generieren“. Daraufhin wird ein Popup-Fenster mit der erstellten Richtlinie angezeigt.



- Kopieren Sie den vollständigen json-Text, der wie folgt aussehen sollte:

```
{
  "Id": "Policy1744399292233",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1744399152830",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "Stmt1744399280838",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

Dieser json kann wie sie ist verwendet werden, oder Sie können die ID- und Versionszeilen über der Zeile "Anweisung" entfernen und Sie können die Sid für jede Berechtigung mit einem aussagekräftigeren Titel für jede Berechtigung anpassen oder diese können auch entfernt werden.

Beispiel:

```
{
  "Statement": [
    {
      "Sid": "MarketingAllowFull",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "EveryoneReadOnly",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

Gruppenrichtlinien (IAM)

Bucket-Zugriff im Home Directory-Stil

Diese Gruppenrichtlinie erlaubt Benutzern nur den Zugriff auf Objekte im Bucket mit dem Namen „username“.

```
{
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

Erstellung von Bucket-Objektsperrung verweigern

Diese Gruppenrichtlinie schränkt Benutzer am Erstellen eines Buckets ein, für den die Objektsperre für den Bucket aktiviert ist.

> Diese Richtlinie wird in der StorageGRID-Benutzeroberfläche nicht durchgesetzt, sie wird nur durch die S3-API durchgesetzt.

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Aufbewahrungslimit für Objektsperre

Diese Bucket-Richtlinie beschränkt die Aufbewahrungsdauer der Objektsperre auf maximal 10 Tage

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

Benutzer daran hindern, Objekte mit VersionID zu löschen

Diese Gruppenrichtlinie schränkt Benutzer davon ab, versionierte Objekte nach VersionID zu löschen

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Beschränken Sie eine Gruppe auf ein einzelnes Unterverzeichnis (Präfix) mit Lesezugriff

Diese Richtlinie ermöglicht Mitgliedern der Gruppe schreibgeschützten Zugriff auf ein Unterverzeichnis (Präfix) innerhalb eines Buckets. Der Bucket-Name lautet „Study“ und das Unterverzeichnis lautet „study01“.

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3::: study"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```

Bucket-Richtlinien

Bucket auf einzelnen Benutzer mit schreibgeschütztem Zugriff beschränken

Diese Richtlinie erlaubt einem einzelnen Benutzer, schreibgeschützten Zugriff auf einen Bucket zu haben und explizit allen anderen Benutzern den zugriff zu verweigert. Die Gruppierung der Ablehenserklärungen an der Spitze der Richtlinie ist eine gute Methode für eine schnellere Bewertung.

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

Beschränken Sie einen Bucket auf einige Benutzer mit schreibgeschütztem Zugriff.

```
{
    "Statement": [
      {
        "Sid": "Deny all S3 actions to employees 002-005",
        "Effect": "deny",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": "*",
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      },
      {
        "Sid": "Allow read-only access for employees 002-005",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion"
        ],
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      }
    ]
}
```

Beschränken Sie das Löschen versionierter Objekte in einem Bucket

Diese Bucket-Richtlinie beschränkt das Löschen versionierter Objekte durch einen Benutzer (identifiziert durch Benutzer-ID „56622399308951294926“) nach VersionID

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

Bucket-Lebenszyklus in StorageGRID

Sie können eine S3-Lebenszyklukonfiguration erstellen, um zu steuern, wann bestimmte Objekte aus dem StorageGRID System gelöscht werden.

Was ist eine Lebenszykluskonfiguration?

Eine Lifecycle-Konfiguration ist ein Satz von Regeln, die auf die Objekte in bestimmten S3-Buckets angewendet werden. Jede Regel gibt an, welche Objekte betroffen sind und wann diese Objekte ablaufen (an einem bestimmten Datum oder nach einigen Tagen).

Jedes Objekt folgt den Aufbewahrungseinstellungen eines S3 Bucket-Lebenszyklus oder einer ILM-Richtlinie. Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Lifecycle-Ablaufaktionen die ILM-Richtlinie für Objekte, die mit dem Bucket-Lifecycle-Filter übereinstimmen. Objekte, die nicht mit dem Bucket-Lebenszyklusfilter übereinstimmen, verwenden die Aufbewahrungseinstellungen der ILM-Richtlinie. Wenn ein

Objekt mit einem Bucket-Lebenszyklusfilter übereinstimmt und keine Ablaufaktionen explizit angegeben werden, werden die Aufbewahrungseinstellungen der ILM-Richtlinie nicht verwendet, und es wird impliziert, dass Objektversionen für immer aufbewahrt werden.

Aus diesem Grund kann ein Objekt aus dem Grid entfernt werden, obwohl die Speicheranweisungen in einer ILM-Regel noch auf das Objekt gelten. Oder ein Objekt kann auf dem Raster verbleiben, selbst wenn alle ILM-Platzierungsanweisungen für das Objekt abgelaufen sind.

StorageGRID unterstützt in einer Lebenszykluskonfiguration bis zu 1,000 Lebenszyklusregeln. Jede Regel kann die folgenden XML-Elemente enthalten:

- Ablauf: Löschen eines Objekts, wenn ein bestimmtes Datum erreicht wird oder wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend mit dem Zeitpunkt der Aufnahme des Objekts.
- NoncurrentVersionExpiration: Löschen Sie ein Objekt, wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend ab dem Zeitpunkt, an dem das Objekt nicht mehr aktuell wurde.
- Filter (Präfix, Tag)
- Status *ID

StorageGRID unterstützt den Einsatz der folgenden Bucket-Operationen zum Management der Lebenszykluskonfigurationen:

- DeleteBucketLifecycle
- GetBucketLifecycleKonfiguration
- PutBucketLifecycleKonfiguration

Aufbau einer Lifecycle-Policy

Als erster Schritt beim Erstellen einer Lebenszykluskonfiguration erstellen Sie eine JSON-Datei mit einem oder mehreren Regeln. Diese JSON-Datei enthält beispielsweise drei Regeln:

1. **Regel 1** gilt nur für Objekte, die dem Präfix „category1/“ entsprechen und den Wert „key2“ von „tag2“ haben. Der Parameter „Expiration“ gibt an, dass Objekte, die dem Filter entsprechen, am 22. August 2020 um Mitternacht ablaufen.
2. **Regel 2** gilt nur für Objekte, die dem Präfix „category2/“ entsprechen. Der Parameter „Expiration“ gibt an, dass Objekte, die dem Filter entsprechen, 100 Tage nach ihrer Aufnahme ablaufen.

   > Regeln, die eine Anzahl von Tagen angeben, sind relativ zu dem Zeitpunkt, an dem das Objekt aufgenommen wurde. Wenn das aktuelle Datum das Aufnahmedatum plus die Anzahl der Tage überschreitet, werden einige Objekte möglicherweise aus dem Bucket entfernt, sobald die Lebenszykluskonfiguration angewendet wird.

3. **Regel 3** gilt nur für Objekte mit dem Präfix „category3/“. Der Parameter „Expiration“ gibt an, dass alle nicht aktuellen Versionen übereinstimmender Objekte 50 Tage nach ihrer Nicht-Aktualisierung ablaufen.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Lifecycle-Konfiguration auf Bucket anwenden

Nachdem Sie die Lebenszykluskonfigurationsdatei erstellt haben, wenden Sie sie auf einen Bucket an, indem Sie eine Anforderung von PutkBucketLifecycleConfiguration ausgeben.

Diese Anforderung wendet die Lebenszykluskonfiguration in der Beispieldatei auf Objekte in einem Bucket mit dem Namen `testbucket`an.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Um zu überprüfen, ob eine Lebenszykluskonfiguration erfolgreich auf den Bucket angewendet wurde, geben Sie eine GetBucketLifecycleConfiguration-Anforderung aus. Beispiel:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Beispiel-Lebenszyklusrichtlinien für Standard-Buckets (ohne Versionsangabe)

Objekte nach 90 Tagen löschen

Anwendungsfall: Diese Richtlinie eignet sich ideal für die Verwaltung zeitlich begrenzt relevanter Daten, wie z. B. temporäre Dateien, Protokolle oder Zwischenverarbeitungsdaten. Vorteil: Reduzieren Sie die Speicherkosten und sorgen Sie für einen übersichtlichen Bucket.

```
{
    "Rules": [
      {
        "ID": "Delete after 90 day rule",
        "Filter": {},
        "Status": "Enabled",
          "Expiration": {
              "Days": 90
        }
      }
    ]
}
```

Beispiel-Lebenszyklusrichtlinien für versionierte Buckets

Nicht aktuelle Versionen nach 10 Tagen löschen

Anwendungsfall: Diese Richtlinie hilft bei der Verwaltung der Speicherung veralteter Versionsobjekte, die sich im Laufe der Zeit ansammeln und viel Speicherplatz beanspruchen können. Vorteil: Optimieren Sie die

Speichernutzung, indem Sie nur die neueste Version speichern.

```
{
    "Rules": [
            {
        "ID": "NoncurrentVersionExpiration 10 day rule",
        "Filter": {},
        "Status": "Enabled",
          "NoncurrentVersionExpiration": {
              "NoncurrentDays": 10
        }
    }
    ]
}
```

Behalten Sie 5 nicht aktuelle Versionen

Anwendungsfall: Nützlich, wenn Sie eine begrenzte Anzahl früherer Versionen zu Wiederherstellungs- oder Prüfzwecken behalten möchten. Vorteil: Behalten Sie genügend nicht aktuelle Versionen, um ausreichend Verlauf und Wiederherstellungspunkte sicherzustellen.

```
{
    "Rules": [
      {
        "ID": "NewerNoncurrentVersions 5 version rule",
        "Filter": {},
        "Status": "Enabled",
        "NoncurrentVersionExpiration": {
            "NewerNoncurrentVersions": 5
        }
    }
    ]
}
```

Löschmarkierungen entfernen, wenn keine anderen Versionen vorhanden sind

Anwendungsfall: Diese Richtlinie hilft bei der Verwaltung der Löschmarkierungen, die nach dem Entfernen aller nicht aktuellen Versionen übrig bleiben und sich im Laufe der Zeit ansammeln können. Vorteil: Reduzierung unnötiger Unordnung.

```
{
    "Rules": [
    {
        "ID": "Delete marker cleanup rule",
        "Filter": {},
        "Status": "Enabled",
        "Expiration": {
        "ExpiredObjectDeleteMarker": true
        }
    }
    ]
}
```

Löschen Sie aktuelle Versionen nach 30 Tagen, löschen Sie nicht aktuelle Versionen nach 60 Tagen und entfernen Sie die Löschmarkierungen, die durch das Löschen der aktuellen Version erstellt wurden, sobald keine anderen Versionen mehr vorhanden sind.

Anwendungsfall: Bereitstellung eines vollständigen Lebenszyklus für aktuelle und nicht aktuelle Versionen inklusive Löschmarkierungen. Vorteil: Reduzieren Sie die Speicherkosten und sorgen Sie für einen übersichtlichen Bucket, während ausreichend Wiederherstellungspunkte und Verlauf erhalten bleiben.

```
{
  "Rules": [
    {
      "ID": "Delete current version",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "Days": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 60
      }
    },
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    }
  ]
}
```

Entfernen Sie Löschmarkierungen, die keine anderen Versionen haben. Behalten Sie 4 nicht aktuelle Versionen und mindestens 30 Tage Verlauf für Objekte mit dem Präfix „accounts_“ und behalten Sie 2 Versionen und mindestens 10 Tage Verlauf für alle anderen Objektversionen.

Anwendungsfall: Definieren Sie eindeutige Regeln für bestimmte Objekte neben anderen Objekten, um den gesamten Lebenszyklus aktueller und nicht aktueller Versionen inklusive Löschmarkierungen zu verwalten. Vorteil: Reduzieren Sie die Speicherkosten und sorgen Sie für einen übersichtlichen Bucket. Gleichzeitig bleiben ausreichend Wiederherstellungspunkte und Verlaufsdaten erhalten, um verschiedene Kundenanforderungen zu erfüllen.

```
{
  "Rules": [
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    },
    {
      "ID": "accounts version retention",
      "Filter": {"Prefix":"account_"},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 4,
        "NoncurrentDays": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 2,
        "NoncurrentDays": 10
      }
    }
  ]
}
```

Schlussfolgerung

- Überprüfen und aktualisieren Sie Lebenszyklusrichtlinien regelmäßig und richten Sie sie an den ILM- und Datenverwaltungszielen aus.
- Testen Sie Richtlinien in einer Nicht-Produktionsumgebung oder einem Bucket, bevor Sie sie allgemein anwenden, um sicherzustellen, dass sie wie vorgesehen funktionieren.
- Verwenden Sie beschreibende IDs für Regeln, um sie intuitiver zu gestalten, da die logische Struktur komplex werden kann
- Überwachen Sie die Auswirkungen dieser Bucket-Lebenszyklusrichtlinien auf die Speichernutzung und Leistung, um die erforderlichen Anpassungen vorzunehmen.

Technische Berichte

Einführung in technische Berichte von StorageGRID

NetApp StorageGRID ist eine Suite für softwaredefinierten Objekt-Storage, die eine Vielzahl von Anwendungsfällen in Public-, Private- und Hybrid-Multi-Cloud-Umgebungen unterstützt. StorageGRID bietet nicht nur nativen Support für die Amazon S3-API, sondern auch branchenführende Innovationen wie automatisiertes Lifecycle Management. Damit können Sie unstrukturierte Daten kostengünstig über längere Zeiträume hinweg speichern, sichern, schützen und aufbewahren.

StorageGRID enthält eine Dokumentation, in der Best Practices und Empfehlungen für verschiedene Funktionen und Integrationen von StorageGRID behandelt werden.

NetApp StorageGRID und Big Data Analytics

Anwendungsfälle für NetApp StorageGRID

Die NetApp StorageGRID Objekt-Storage-Lösung bietet Skalierbarkeit, Datenverfügbarkeit, Sicherheit und hohe Performance. Unternehmen jeder Größe und Branche nutzen StorageGRID S3 für zahlreiche Anwendungsfälle. Sehen wir uns einige typische Szenarien an:

Big Data Analytics: StorageGRID S3 wird häufig als Data Lake verwendet, wo Unternehmen mit Tools wie Apache Spark, Splunk SmartStore und Dremio große Mengen an strukturierten und unstrukturierten Daten für Analysen speichern.

Daten-Tiering: NetApp Kunden nutzen die FabricPool Funktion von ONTAP, um Daten automatisch zwischen einem hochperformanten lokalen Tier zu StorageGRID zu verschieben. Durch Tiering wird teurer Flash-Storage für häufig abgerufene Daten frei. Kalte Daten werden auf kostengünstigem Objekt-Storage bereitgehalten. Dadurch werden Performance und Einsparungen maximiert.

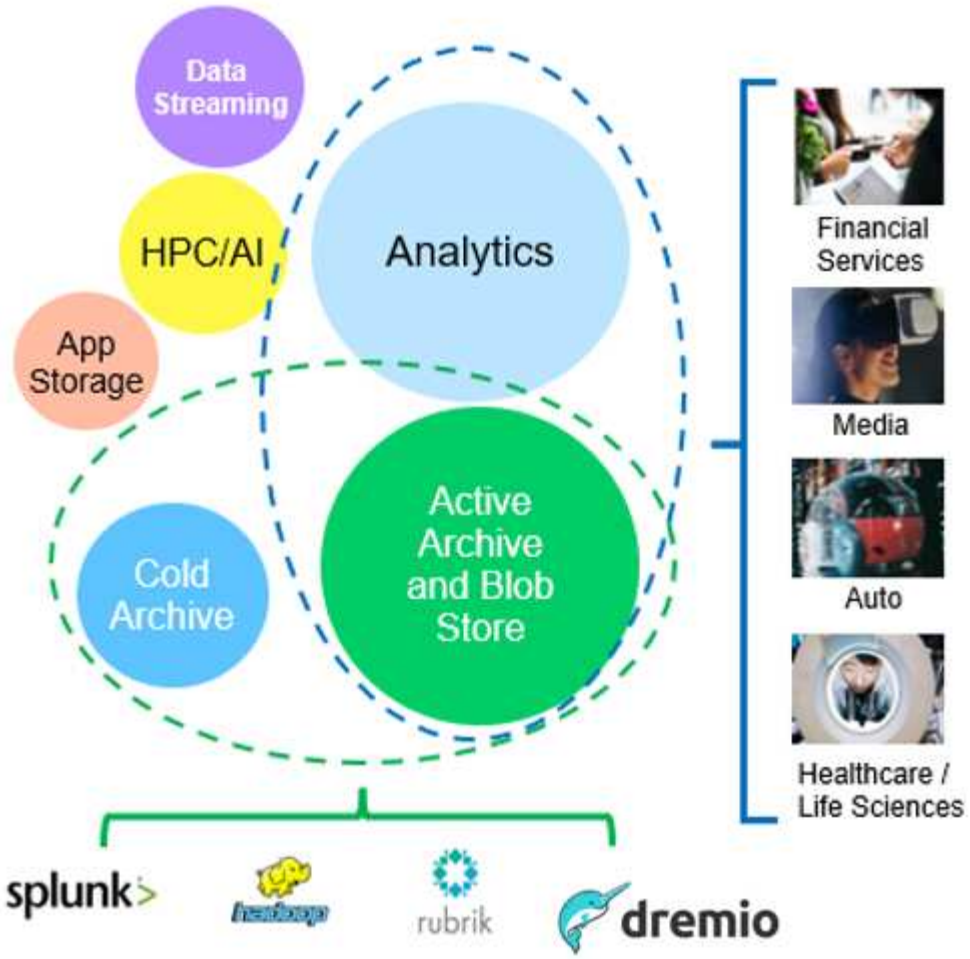
Daten-Backup und Disaster Recovery: Unternehmen können StorageGRID S3 als zuverlässige und kostengünstige Lösung für Backup und Recovery kritischer Daten im Notfall einsetzen.

Datenspeicher für Anwendungen: StorageGRID S3 kann als Speicher-Backend für Anwendungen verwendet werden, so dass Entwickler Dateien, Bilder, Videos und andere Arten von Daten einfach speichern und abrufen können.

Inhaltsbereitstellung: StorageGRID S3 kann verwendet werden, um statische Website-Inhalte, Mediendateien und Software-Downloads für Benutzer auf der ganzen Welt zu speichern und bereitzustellen. Dabei wird die geografische Distribution und der globale Namespace von StorageGRID für eine schnelle und zuverlässige Content-Bereitstellung genutzt.

Datenarchiv: StorageGRID bietet verschiedene Speichertypen und unterstützt Tiering zu öffentlichen, langfristigen und kostengünstigen Speicheroptionen. Damit ist es eine ideale Lösung für die Archivierung und langfristige Aufbewahrung von Daten, die für Compliance- oder historische Zwecke aufbewahrt werden müssen.

Anwendungsfälle für Objekt-Storage

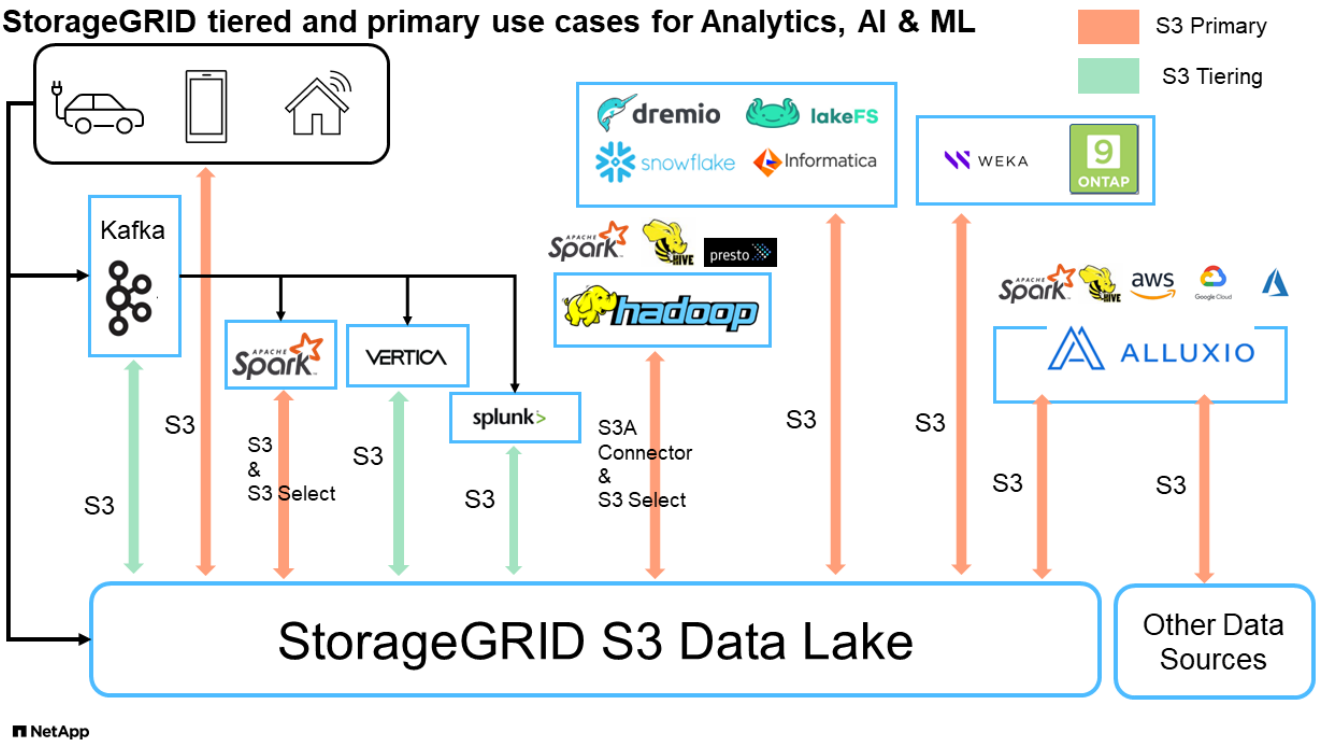


Zu den oben genannten Fällen gehört Big-Data-Analysen zu den häufigsten Nutzungsfällen und die Nutzung dieser Daten ist mit einem Aufwärtstrend verbunden.

Warum StorageGRID für Data Lakes?

- Verstärkte Zusammenarbeit: Enorme, gemeinsam genutzte Mandantenfähigkeit mit branchenüblicher API-Zugriff
- Niedrigere Betriebskosten: Einfacher Betrieb in einer einzelnen, automatisierten Scale-out-Architektur mit Selbstreparatur
- Skalierbarkeit – im Gegensatz zu herkömmlichen Hadoop- und Data-Warehouse-Lösungen entkoppelt der StorageGRID S3 Objekt-Storage den Storage von Computing und Daten. So können Unternehmen ihre Storage-Anforderungen mit wachsendem Bedarf skalieren.
- Langlebigkeit und Zuverlässigkeit: StorageGRID bietet eine Lebensdauer von 99.999999999 %, was bedeutet, dass die gespeicherten Daten sehr resistent gegen Datenverlust sind. Darüber hinaus ist Hochverfügbarkeit gewährleistet, sodass die Daten jederzeit abrufbar sind.
- Sicherheit – StorageGRID bietet verschiedene Sicherheitsfunktionen, darunter Verschlüsselung, Zugriffssteuerungsrichtlinien, Daten-Lifecycle-Management, Objektsperre und Versionierung zum Schutz der in S3 Buckets gespeicherten Daten

StorageGRID S3 Data Lakes



Benchmarking von Data Warehouses und Lakehouses mit S3 Object Storage: Eine vergleichende Studie

Dieser Artikel stellt eine umfassende Benchmark verschiedener Data Warehouse- und Lakehouse-Ökosysteme vor, die NetApp StorageGRID verwenden. Ziel ist es zu ermitteln, welches System mit S3 Objekt-Storage am besten funktioniert. In diesem Abschnitt "Apache Iceberg: Der Endgültige Führer"erfahren Sie mehr über Datawarehous/Lakehouse-Architekturen und Tischformate (Parkett und Iceberg).

- Benchmark-Tool - TPC-DS - https://www.tpc.org/tpcds/
- Big-Data-Ecosysteme
  - Cluster von VMs mit jeweils 128 GB RAM und 24 vCPUs, SSD-Storage für Systemfestplatte
  - Hadoop 3.3.5 mit Hive 3.1.3 (1 Name Node + 4 Daten-Nodes)
  - Delta Lake mit Spark 3.2.0 (1 Master + 4 Workers) und Hadoop 3.3.5
  - Dremio v25.2 (1 Koordinator + 5 Ausführende)
  - Trino v438 (1 Koordinator + 5 Mitarbeiter)
  - Starburst v453 (1 Koordinator + 5 Mitarbeiter)
- Objekt-Storage
  - NetApp® StorageGRID® 11.8 mit 3 SG6060 + 1 SG1000 Load Balancer
  - Objektschutz – 2 Kopien (Ergebnis ist ähnlich wie EC 2+1)
- Datenbankgröße 1.000 GB
- Cache wurde in allen Ökosystemen für jeden Abfragetest mit dem Parkettformat deaktiviert. Für das Iceberg-Format haben wir die Anzahl der S3-GET-Anforderungen und die gesamte Abfragezeit zwischen Cache-deaktivierten und Cache-fähigen Szenarien verglichen.

TPC-DS umfasst 99 komplexe SQL-Abfragen, die für das Benchmarking entwickelt wurden. Wir haben die

Gesamtdauer für die Ausführung aller 99 Abfragen gemessen. Für eine detaillierte Analyse haben wir die Art und Anzahl der S3-Anfragen untersucht. Unsere Tests verglichen die Effizienz zweier beliebter Tischformate: Parkett und Iceberg.

TPC-DS Abfrageergebnis mit Parkett-Tabellenformat

Ecosystem	Hive	Delta Lake	Dremio	Trino	Starburst
TPCDS 99 Abfragen Minuten gesamt	1084 [1]	55	36	32	28
S3 Anfragen – Aufschlüsselung	GET	1,117,184	2,074,610	3.939.690	1.504.212
1.495.039	Beobachtung: Alle Reichweite ERHALTEN	80% Bereich von 2 KB bis 2 MB von 32 MB Objekten, 50 - 100 Anfragen/Sek.	73% Bereich unter 100 KB von 32-MB-Objekten, 1000 - 1400 Anforderungen/Sek.	90 % 1 MB-Bereich von Objekten mit 256 MB, 2500 bis 3000 Anforderungen/Sek.	Bereich GET size: 50% unter 100KB, 16% um 1MB, 27% 2MB-9MB, 3500 - 4000 Anfragen/sec
Bereich GET size: 50% unter 100KB, 16% um 1MB, 27% 2MB-9MB, 4000 - 5000 Anfrage/sec	Objekte auflisten	312,053	24,158	120	509
512	KOPF (Nicht vorhandenes Objekt)	156,027	12,103	96	0
0	KOPF (Vorhandenes Objekt)	982,126	922,732	0	0
0	Gesamtanforderungen	2,567,390	3,033,603	3.939,906	1.504.721

[1] Hive konnte die Abfragenummer 72 nicht abschließen

TPC-DS Abfrageergebnis mit Iceberg-Tabellenformat

Ecosystem	Dremio	Trino	Starburst
TPCDS 99 Abfragen + Summe Minuten (Cache deaktiviert)	22	28	22
TPCDS 99 Abfragen + Gesamtzahl Minuten [2] (Cache aktiviert)	16	28	21,5
S3 Anfragen – Aufschlüsselung	ABRUFEN (Cache deaktiviert)	1.985.922	938.639
931.582	GET (Cache aktiviert)	611.347	30.158
3.281	Beobachtung: Alle Reichweite ERHALTEN	Bereich GET size: 67% 1 MB, 15% 100 KB, 10% 500 KB, 3500 - 4500 Anfragen/sec	Bereich GET size: 42% unter 100KB, 17% um 1MB, 33% 2MB-9MB, 3500 - 4000 Anfragen/sec
Bereich GET size: 43% unter 100KB, 17% um 1MB, 33% 2MB-9MB, 4000 - 5000 Anfragen/sec	Objekte auflisten	1465	0
0	KOPF (Nicht vorhandenes Objekt)	1464	0
0	KOPF (Vorhandenes Objekt)	3.702	509
509	Anfragen gesamt (Cache deaktiviert)	1.992.553	939.148

[2] die Performance von Trino/Starburst wird durch Computing-Ressourcen in Engpässe gebracht. Durch Hinzufügen von zusätzlichem RAM zum Cluster wird die gesamte Abfragezeit verringert.

Wie in der ersten Tabelle gezeigt, ist Hive deutlich langsamer als andere moderne Data-Lakehouse-Ökosysteme. Wir beobachteten, dass Hive eine große Anzahl von S3-Listenobjektanfragen gesendet hat, die in der Regel auf allen Objekt-Storage-Plattformen langsam sind, insbesondere bei Buckets, die zahlreiche Objekte enthalten. Dadurch erhöht sich die gesamte Abfragedauer deutlich. Zusätzlich können moderne Lakehouse-Ökosysteme eine hohe Anzahl von GET-Anfragen parallel senden, die von 2,000 bis 5,000 Anfragen pro Sekunde reichen, verglichen mit Hive's 50 bis 100 Anfragen pro Sekunde. Die Standard-Filesystem-Mimikry von Hive und Hadoop S3A trägt zur Langsamkeit von Hive bei der Interaktion mit S3-Objektspeicher bei.

Bei der Nutzung von Hadoop (entweder auf HDFS oder S3 Objekt-Storage) mit Hive oder Spark sind umfassende Kenntnisse sowohl zu Hadoop als auch zu Hive/Spark erforderlich. Außerdem müssen Sie sich mit den Einstellungen der einzelnen Services vertraut machen. Zusammen haben sie über 1,000 Einstellungen, von denen viele miteinander verknüpft sind und nicht unabhängig voneinander geändert werden können. Die optimale Kombination von Einstellungen und Werten zu finden, erfordert viel Zeit und Aufwand.

Wenn wir die Ergebnisse von Parkett und Iceberg vergleichen, stellen wir fest, dass das Tabellenformat ein wichtiger Leistungsfaktor ist. Das Iceberg-Tabellenformat ist hinsichtlich der Anzahl der S3-Anfragen effizienter

als das Parkett, mit 35% bis 50% weniger Anfragen im Vergleich zum Parkett-Format.

Die Leistung von Dremio, Trino oder Starburst wird in erster Linie durch die Rechenleistung des Clusters angetrieben. Alle drei verwenden zwar den S3A-Connector für die S3-Objektspeicher-Verbindung, benötigen jedoch kein Hadoop. Die meisten der fs.s3a-Einstellungen von Hadoop werden von diesen Systemen nicht verwendet. Dies vereinfacht das Performance-Tuning und macht das Erlernen und Testen verschiedener Hadoop S3A Einstellungen überflüssig.

Aus diesem Benchmark-Ergebnis können wir schließen, dass Big-Data-Analysesysteme für S3-basierte Workloads zu einem wesentlichen Performance-Faktor werden. Moderne Lakehouses optimieren die Abfrageausführung, nutzen Metadaten effizient und ermöglichen nahtlosen Zugriff auf S3-Daten. Dies ermöglicht eine bessere Performance als Hive bei der Arbeit mit S3 Storage.

Hier "Seite" können Sie die Dremio S3-Datenquelle mit StorageGRID konfigurieren.

Unter den folgenden Links erfahren Sie mehr darüber, wie StorageGRID und Dremio gemeinsam eine moderne und effiziente Data-Lake-Infrastruktur bereitstellen und wie NetApp von Hive + HDFS auf Dremio + StorageGRID migrierte, um die Analyseeffizienz von Big Data drastisch zu steigern.

- "Mehr Performance für Big Data mit NetApp StorageGRID"
- "Moderne, leistungsstarke und effiziente Data-Lake-Infrastruktur mit StorageGRID und Dremio"
- "Wie NetApp die Kundenerfahrung mit Produktanalysen neu definiert"

Hadoop S3A-Tuning

Von Angela Cheng

Der Hadoop S3A Connector ermöglicht die nahtlose Interaktion zwischen Hadoop-basierten Applikationen und S3 Objektspeicher. Um die Performance bei der Arbeit mit S3-Objektspeicher zu optimieren, ist die Anpassung des Hadoop S3A Connector unerlässlich. Bevor wir uns mit der Feinabstimmung befassen, wollen wir zunächst ein grundlegendes Verständnis von Hadoop und seinen Komponenten haben.

Was ist Hadoop?

Hadoop ist ein leistungsfähiges Open-Source-Framework, das für die Verarbeitung und Speicherung großer Datenmengen entwickelt wurde. Sie ermöglicht verteilte Speicherung und parallele Verarbeitung über Cluster von Computern hinweg.

Die drei Kernkomponenten von Hadoop sind:

- **Hadoop HDFS (Hadoop Distributed File System)**: Dies verarbeitet Speicherung, teilt Daten in Blöcke auf und verteilt sie über Knoten.
- **Hadoop MapReduce**: Verantwortlich für die Verarbeitung der Daten durch Aufteilen von Aufgaben in kleinere Blöcke und deren parallele Ausführung.
- **Hadoop YARN (noch ein weiterer Resource Negotiator):** "Managt Ressourcen und plant Aufgaben effizient"

Hadoop HDFS- und S3A-Steckverbinder

HDFS ist eine wichtige Komponente des Hadoop Ecosystems und spielt eine entscheidende Rolle bei der effizienten Verarbeitung von Big Data. HDFS ermöglicht zuverlässige Speicherung und Verwaltung. Sie ermöglicht die parallele Verarbeitung und optimiert den Datenspeicher, was zu schnellerem Datenzugriff und

schnelleren Analysen führt.

Bei der Big Data-Verarbeitung überzeugt HDFS durch fehlertoleranten Storage für große Datensätze. Es erreicht dies durch Datenreplikation. Die IT kann große Mengen strukturierter und unstrukturierter Daten in einer Data Warehouse-Umgebung speichern und managen. Darüber hinaus lässt sich die Software nahtlos in führende Big Data Processing Frameworks wie Apache Spark, Hive, Pig und Flink integrieren und ermöglicht so eine skalierbare und effiziente Datenverarbeitung. Er ist mit Unix-basierten (Linux) Betriebssystemen kompatibel und somit eine ideale Wahl für Unternehmen, die Linux-basierte Umgebungen für ihre Big-Data-Verarbeitung bevorzugen.

Mit der Zeit wuchs das Datenvolumen. Daher ist es ineffizient, dem Hadoop Cluster neue Maschinen mit eigenen Computing- und Storage-Ressourcen hinzuzufügen. Lineare Skalierung führt zu Herausforderungen bei der effizienten Nutzung von Ressourcen und dem Management der Infrastruktur.

Als Antwort auf diese Herausforderungen bietet der Hadoop S3A Connector hochperformante I/O für S3 Objekt-Storage. Durch die Implementierung eines Hadoop Workflows mit S3A können Sie Objekt-Storage als Daten-Repository nutzen und Computing- und Storage-Ressourcen separat voneinander skalieren. Dadurch wiederum können Sie Computing- und Storage-Ressourcen unabhängig voneinander skalieren. Die Abkopplung von Computing und Storage erlaubt es Ihnen auch, die richtige Menge an Ressourcen für Ihre Compute-Jobs bereitzustellen und die Kapazität abhängig von der Größe des Datensatzes bereitzustellen. Somit lassen sich die Gesamtbetriebskosten für Hadoop Workflows verringern.

Hadoop S3A Connector Tuning

S3 verhält sich anders als HDFS, und einige Versuche, das Aussehen eines Filesystems beizubehalten, sind aggressiv suboptimal. Um die S3-Ressourcen möglichst effizient zu nutzen, sind sorgfältiges Tuning/Testen/Experimentieren erforderlich.

Die Hadoop Optionen in diesem Dokument basieren auf Hadoop 3.3.5, siehe "Hadoop 3.3.5 core-site.xml" Für alle verfügbaren Optionen.

Hinweis – einige Hadoop fs.s3a Einstellungen sind in den jeweiligen Hadoop Versionen unterschiedlich. Überprüfen Sie unbedingt den Standardwert Ihrer aktuellen Hadoop Version. Werden diese Einstellungen nicht in Hadoop core-site.xml angegeben, so wird als Standardwert verwendet. Sie können den Wert zur Laufzeit mithilfe der Konfigurationsoptionen Spark oder Hive überschreiben.

Sie müssen zu diesem gehen "Apache Hadoop Seite aufrufen" Um die einzelnen Optionen von fs.s3a zu verstehen. Testen Sie diese nach Möglichkeit im nicht produktiven Hadoop Cluster, um die optimalen Werte zu ermitteln.

Sie sollten lesen "Maximale Leistung bei der Arbeit mit dem S3A-Steckverbinder" Für weitere Optimierungsempfehlungen.

Sehen wir uns einige wichtige Überlegungen an:

1. Datenkomprimierung

Aktivieren Sie die StorageGRID-Komprimierung nicht. Die meisten Big-Data-Systeme verwenden Byte-Bereich get, anstatt das gesamte Objekt abzurufen. Die Verwendung von Byte Range Get mit komprimierten Objekten beeinträchtigt die GET-Performance erheblich.

2. S3A Committer

Generell wird Magic s3a Committer empfohlen. Weitere Informationen finden Sie hier "Allgemeine Seite mit den Optionen für den S3A-Committer" Um ein besseres Verständnis von Magic Committer und den damit

verbundenen s3a-Einstellungen zu bekommen.

Magic Committer:

Der Magic Committer setzt speziell auf S3Guard, um konsistente Verzeichnisauflistungen im S3-Objektspeicher zu bieten.

Mit konsistenten S3 (was jetzt der Fall ist), kann der Magic Committer sicher mit jedem S3-Bucket verwendet werden.

Auswahl und Experimentieren:

Je nach Anwendungsfall können Sie zwischen dem Staging Committer (der auf einem Cluster HDFS-Dateisystem basiert) und dem Magic Committer wählen.

Experimentieren Sie mit beiden, um zu ermitteln, welche Lösung am besten zu Ihrem Workload und Ihren Anforderungen passt.

Zusammenfassend stellen die S3A Committers eine Lösung für die grundlegende Herausforderung dar, die ein konsistentes, leistungsstarkes und zuverlässiges Leistungsengagement für S3 darstellt. Das interne Design gewährleistet einen effizienten Datentransfer bei gleichzeitiger Wahrung der Datenintegrität.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable “magic committer” support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

3. Thread, Größe des Verbindungspools und Blockgröße

- Jeder **S3A**-Client, der mit einem einzelnen Bucket interagiert, hat einen eigenen dedizierten Pool von offenen HTTP 1.1-Verbindungen und Threads für Upload- und Kopiervorgänge.
- "Sie können diese Poolgrößen so anpassen, dass ein ausgewogenes Verhältnis zwischen Leistung und Speicher-/Thread-Nutzung erzielt wird".
- Beim Hochladen von Daten in S3 werden sie in Blöcke unterteilt. Die standardmäßige Blockgröße beträgt 32 MB. Sie können diesen Wert anpassen, indem Sie die Eigenschaft fs.s3a.Block.size festlegen.
- Größere Blockgrößen verbessern die Performance beim Hochladen großer Daten, da sich der Managementaufwand für mehrteilige Teile während des Uploads verringert. Der empfohlene Wert ist 256

MB oder höher für große Datensätze.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

4. Mehrteiliges Hochladen

s3a-Committer **Always** Verwenden Sie MPU (mehrteilige Uploads) zum Hochladen von Daten in s3-Buckets. Dies ist erforderlich, um Folgendes zu ermöglichen: Task Failure, spekulative Ausführung von Aufgaben und Job Abbrüche vor Commit. Hier sind einige wichtige Spezifikationen für mehrteilige Uploads:

- Maximale Objektgröße: 5 tib (Terabyte).
- Maximale Anzahl von Teilen pro Upload: 10,000.
- Teilenummern: Von 1 bis 10,000 (inklusive).
- Größe des Teils: Zwischen 5 MiB und 5 gib. Insbesondere gibt es keine Mindestgröße für den letzten Teil Ihres mehrteiligen Uploads.

Die Verwendung kleinerer Teilgröße für S3-Multipart-Uploads hat sowohl vor- als auch Nachteile.

Vorteile:

- Schnelle Wiederherstellung von Netzwerkproblemen: Wenn Sie kleinere Teile hochladen, werden die Auswirkungen des Neustarts eines fehlgeschlagenen Uploads aufgrund eines Netzwerkfehlers minimiert.

Wenn ein Teil fehlschlägt, müssen Sie nur dieses Teil neu hochladen, nicht das gesamte Objekt.

- Bessere Parallelisierung: Mehr Teile können parallel hochgeladen werden, wobei Multi-Threading oder gleichzeitige Verbindungen genutzt werden können. Diese Parallelisierung verbessert die Performance, insbesondere bei der Verarbeitung großer Dateien.

Nachteil:

- Netzwerk-Overhead: Kleinere Teilegröße bedeutet, dass mehr Teile hochgeladen werden müssen, jedes Teil benötigt eine eigene HTTP-Anforderung. Mehr HTTP-Anfragen erhöhen den Overhead beim Initiieren und Abschließen einzelner Anfragen. Die Verwaltung einer großen Anzahl von Kleinteilen kann die Leistung beeinträchtigen.
- Komplexität: Die Verwaltung der Bestellung, die Nachverfolgung von Teilen und die Sicherstellung erfolgreicher Uploads können umständlich sein. Wenn der Upload abgebrochen werden muss, müssen alle bereits hochgeladenen Teile nachverfolgt und gelöscht werden.

Für Hadoop wird eine Teilegröße von 256 MB oder höher für fs.s3a.Multipart.size empfohlen. Stellen Sie immer den Wert fs.s3a.mutlipart.threshold auf 2 x fs.s3a.multipart.size ein. Beispiel: Fs.s3a.multipart.size = 256M, fs.s3a.mutlipart.threshold sollte 512M sein.

Größere Teilegröße für großen Datensatz verwenden Es ist wichtig, eine Teilegröße zu wählen, die diese Faktoren auf der Grundlage Ihres spezifischen Anwendungsfalls und der Netzwerkbedingungen ausgleicht.

Ein mehrteiliges Hochladen ist ein "Prozess in drei Schritten":

1. Der Upload wird gestartet, StorageGRID gibt eine Upload-ID zurück.
2. Die Objektteile werden mit der Upload-ID hochgeladen.
3. Sobald alle Objektteile hochgeladen sind, sendet die komplette mehrteilige Upload-Anfrage mit Upload-ID. StorageGRID erstellt das Objekt aus den hochgeladenen Teilen, und der Client kann auf das Objekt zugreifen.

Wenn die Anfrage zum vollständigen Hochladen mehrerer Teile nicht erfolgreich gesendet wird, bleiben die Teile in StorageGRID und erstellen kein Objekt. Dies geschieht, wenn Jobs unterbrochen, fehlgeschlagen oder abgebrochen werden. Die Teile verbleiben im Raster, bis der Upload mehrerer Teile abgeschlossen ist oder abgebrochen wird oder StorageGRID diese Teile löscht, wenn 15 Tage nach dem Upload vergangen sind. Wenn sich viele (einige Hunderttausend bis Millionen) mehrteilige Uploads in einem Bucket befinden und Hadoop ‘list-Multipart-Uploads’ sendet (diese Anfrage filtert nicht nach Upload-id), kann die Bearbeitung der Anfrage sehr viel Zeit in Anspruch nehmen oder eventuell eine bestimmte Zeit in Anspruch nehmen. Sie können die Einstellung fs.s3a.mutlipart.purge mit dem entsprechenden Wert fs.s3a.Multipart.purge.age (z. B. 5 bis 7 Tage, verwenden Sie den Standardwert 86400, d. h. 1 Tag) auf true setzen. Oder wenden Sie sich an den NetApp Support, um die Situation zu untersuchen.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

5. Pufferschreibdaten im Speicher

Zur Verbesserung der Performance können Sie Schreibdaten vor dem Hochladen in S3 zwischenspeichern. Dies kann die Anzahl kleiner Schreibvorgänge reduzieren und die Effizienz verbessern.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

S3 und HDFS funktionieren jedoch auf unterschiedliche Weise. Um die S3-Ressourcen optimal zu nutzen, sind

sorgfältiges Tuning/Test/Experiment nötig.

TR-4871: Konfiguration von StorageGRID für Backup und Recovery mit CommVault

Backup und Recovery von Daten mit StorageGRID und CommVault

CommVault und NetApp haben gemeinsam eine gemeinsame Datensicherungslösung entwickelt, die CommVault Complete Backup and Recovery for NetApp Software mit der NetApp StorageGRID Software für Cloud-Storage kombiniert. CommVault Complete Backup and Recovery und NetApp StorageGRID bieten einzigartige, benutzerfreundliche Lösungen, die Sie dabei unterstützen, die Anforderungen eines schnellen Datenwachstums und die zunehmenden Vorschriften weltweit zu erfüllen.

Viele Unternehmen möchten ihren Storage in die Cloud migrieren, ihre Systeme skalieren und ihre Richtlinien zur langfristigen Aufbewahrung von Daten automatisieren. Cloud-basierter Objekt-Storage ist für seine Ausfallsicherheit, Skalierbarkeit und betriebliche und Kosteneffizienz bekannt, die es zur ersten Wahl für Ihr Backup machen. CommVault und NetApp haben ihre kombinierte Lösung 2014 gemeinsam zertifiziert und bieten seitdem eine engere Integration der beiden Lösungen an. Kunden aller Branchen weltweit haben die kombinierte Lösung CommVault Complete Backup and Recovery sowie StorageGRID eingeführt.

CommVault und StorageGRID

Die Software CommVault Complete Backup and Recovery ist eine integrierte Daten- und Informationsmanagement-Lösung der Enterprise-Klasse, die von Grund auf auf auf einer einzigen Plattform und mit einer einheitlichen Code-Basis aufgebaut wurde. Alle Funktionen sind mit Back-End-Technologien ausgestattet und bieten so die unvergleichlichen Vorteile und Vorteile eines vollständig integrierten Ansatzes zum Schutz, Management und Zugriff auf Ihre Daten. Die Software enthält Module zum Schützen, Archivieren, Analysieren, Replizieren und Durchsuchen Ihrer Daten. Die Module verfügen über gemeinsame Back-End-Services und erweiterte Funktionen, die nahtlos miteinander interagieren. Die Lösung deckt alle Aspekte des Datenmanagements in Ihrem Unternehmen ab und sorgt gleichzeitig für grenzenlose Skalierbarkeit und beispiellose Kontrolle über Daten und Informationen.

NetApp StorageGRID als Cloud-Tier von CommVault ist eine Objekt-Storage-Lösung für die Hybrid Cloud der Enterprise-Klasse. Sie kann an mehreren Standorten eingesetzt werden, entweder auf einer speziell entwickelten Appliance oder als softwaredefinierte Implementierung. Mit StorageGRID können Kunden Richtlinien für das Datenmanagement festlegen, die festlegen, wie Daten gespeichert und gesichert werden. StorageGRID erfasst die Informationen, die Sie für die Entwicklung und Durchsetzung von Richtlinien benötigen. Untersucht werden eine Vielzahl von Merkmalen und Anforderungen, darunter Performance, Langlebigkeit, Verfügbarkeit, geografischer Standort Langlebigkeit und Kosten. Daten werden während der Verschiebung zwischen Standorten und mit zunehmendem Alter vollständig gepflegt und geschützt.

Die intelligente Richtlinien-Engine von StorageGRID bietet Ihnen eine der folgenden Optionen:

- Mit Erasure Coding können Sie Daten aus Resilience-heraus über mehrere Standorte hinweg sichern.
- Um Objekte an Remote-Standorte zu kopieren und so die WAN-Latenz und die Kosten zu minimieren.

Wenn ein Objekt von StorageGRID gespeichert wird, greifen Sie als ein Objekt auf es zu, unabhängig davon, wo es sich befindet oder wie viele Kopien vorhanden sind. Dieses Verhalten ist bei der Disaster Recovery von entscheidender Bedeutung, da StorageGRID Ihre Daten selbst dann wiederherstellen kann, wenn eine Sicherungskopie der Daten beschädigt ist.

Die Aufbewahrung von Backup-Daten in Ihrem Primärspeicher kann kostspielig werden. Wenn Sie NetApp StorageGRID verwenden, geben Sie Speicherplatz auf Ihrem primären Storage frei, indem Sie inaktive Backup-Daten in StorageGRID migrieren und gleichzeitig von den zahlreichen Funktionen von StorageGRID profitieren. Der Wert von Backup-Daten ändert sich im Laufe der Zeit, genauso wie die Kosten für deren Speicherung. StorageGRID kann die Kosten für primären Storage minimieren und die Langlebigkeit der Daten verbessern.

Wichtige Funktionen

Zu den wichtigsten Funktionen der CommVault Softwareplattform gehören:

- Eine umfassende Datensicherungslösung, die alle wichtigen Betriebssysteme, Applikationen und Datenbanken auf virtuellen und physischen Servern, NAS-Systemen, Cloud-basierten Infrastrukturen und Mobilgeräten unterstützt
- Vereinfachtes Management über eine einzige Konsole: Sie können alle Funktionen sowie alle Daten und Informationen im gesamten Unternehmen anzeigen, managen und darauf zugreifen.
- Verschiedene Sicherungsmethoden wie Daten-Backup und -Archivierung, Snapshot-Management, Datenreplizierung und Content-Indizierung für E-Discovery
- Effizientes Storage-Management mit Deduplizierung für Festplatten- und Cloud-Storage
- Integration in NetApp Storage-Arrays wie AFF, FAS, NetApp HCI und E-Series Arrays sowie^ horizontal skalierbare NetApp SolidFire^ Storage-Systeme Auch in die NetApp Cloud Volumes ONTAP Software integrierbar, um die Erstellung indizierter, applikationsgerechter NetApp Snapshot™ Kopien im gesamten NetApp Storage-Portfolio zu automatisieren.
- Umfassendes Management virtueller Infrastrukturen, das führende lokale virtuelle Hypervisoren und Hyperscaler-Plattformen für Public Clouds unterstützt
- Erweiterte Sicherheitsfunktionen zur Einschränkung des Zugriffs auf kritische Daten, zur Bereitstellung granularer Verwaltungsfunktionen und zur Bereitstellung von Single-Sign-on-Zugriff für Active Directory-Benutzer.
- Richtlinienbasiertes Datenmanagement, mit dem Daten je nach Geschäftsanforderungen und nicht nach physischem Standort gemanagt werden können
- Eine hochmoderne End-User-Erfahrung, mit der Ihre Anwender ihre Daten selbst schützen, finden und wiederherstellen können.
- API-gestützte Automatisierung, sodass Sie zum Management Ihrer Datensicherungs- und Recovery-Vorgänge Tools von Drittanbietern wie vRealize Automation oder Service Now verwenden können.

Weitere Informationen zu unterstützten Workloads finden Sie unter "Die unterstützten Technologien von CommVault".

Backup-Optionen

Die Implementierung der CommVault Complete Backup and Recovery-Software mit Cloud-Storage bietet zwei Backup-Optionen:

- Es wird ein Backup auf ein primäres Festplattenziel erstellt und außerdem eine zusätzliche Kopie in einem Cloud-Storage gesichert.
- Backup auf Cloud-Storage als primäres Ziel,

In der Vergangenheit wurde Cloud- oder Objekt-Storage als zu leistungsschwach für das primäre Backup angesehen. Durch die Verwendung eines primären Festplattenziels konnten Kunden schnellere Backup- und Restore-Prozesse durchführen und eine zusätzliche Kopie als Cold Backup in der Cloud aufbewahren.

StorageGRID ist die Objekt-Storage-Generation der nächsten Generation. StorageGRID bietet neben hoher Performance und enormem Durchsatz auch Performance und Flexibilität eine im Vergleich zu anderen Objekt-Storage-Anbietern hervorragende Leistung.

In der folgenden Tabelle sind die Vorteile der einzelnen Backup-Optionen mit StorageGRID aufgeführt:

	Primäres Backup-to-Disk und eine zusätzliche Kopie an StorageGRID	**Primäres Backup auf StorageGRID**
Leistung	Schnellste Recovery-Zeit mithilfe von Live-Mounten oder Live-Recovery: Ideal für Tier 0/Tier 1-Workloads.	Kann nicht für Live-Mount- oder Live-Recovery-Vorgänge verwendet werden. Ideal für Streaming-Wiederherstellungsvorgänge und für langfristige Aufbewahrung.
Implementierungsarchitektur	Verwendet rein Flash-basierten oder rotierenden Festplatten als erste Backup-Landing Tier. StorageGRID wird als sekundäre Ebene verwendet.	Vereinfacht die Implementierung durch die Verwendung von StorageGRID als umfassendes Backup-Ziel.
Erweiterte Funktionen (Live-Wiederherstellung)	Unterstützt	Nicht unterstützt

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- StorageGRID 11.9 Dokumentationszentrum + https://docs.netapp.com/us-en/storagegrid-119/
- NetApp Produktdokumentation
  https://docs.netapp.com
- CommVault Dokumentation
  https://documentation.commvault.com/2024/essential/index.html

Übersicht über die getestete Lösung

Die getestete Lösung kombiniert CommVault und NetApp Lösungen in einer leistungsstarken gemeinsamen Lösung.

Lösungseinrichtung

Die StorageGRID-Umgebung bestand in der Lab-Einrichtung aus vier NetApp StorageGRID SG5712 Appliances, einem virtuellen primären Administrator-Node und einem virtuellen Gateway Node. Die SG5712 Appliance ist eine Entry-Level-Option – eine Basiskonfiguration. Durch die Auswahl von Optionen für Appliances mit höherer Performance, wie z. B. NetApp StorageGRID SG5760 oder SG6060, können deutliche Performance-Vorteile erzielt werden. Wenden Sie sich an Ihren NetApp StorageGRID Solution Architect, um Hilfe bei der Dimensionierung zu erhalten.

Die StorageGRID Richtlinie für Datensicherung verwendet für das Management und die Sicherung von Daten eine Richtlinie für integriertes Lifecycle Management (ILM). ILM-Regeln werden in einer Richtlinie von oben nach unten bewertet. Die in der folgenden Tabelle dargestellte ILM-Richtlinie wurde implementiert:

ILM-Regel	Kriterien	Aufnahmeverhalten
Erasure Coding 2+1	Objekte über 200 KB	Ausgeglichen
2 Kopien	Alle Objekte	Doppelte Provisionierung

Die Standardregel für ILM 2 Kopien ist. Für diesen Test wurde die Regel Erasure Coding 2+1 auf jedes Objekt mit mindestens 200 KB angewendet. Die Standardregel wurde auf Objekte angewendet, die kleiner als 200 KB sind. Die Anwendung der Regeln auf diese Weise ist eine StorageGRID Best Practice.

Technische Details zu dieser Testumgebung finden Sie im Abschnitt Solution Design and Best Practices in der "NetApp Scale-out-Datensicherung mit CommVault" Technischer Bericht.

Hardware-Spezifikationen für StorageGRID

Die folgende Tabelle beschreibt die bei diesen Tests verwendete NetApp StorageGRID-Hardware. Die StorageGRID SG5712 Appliance mit 10 Gbit/s-Netzwerkbetrieb ist die Einstiegsoption und stellt eine Basiskonfiguration dar. Optional kann die SG5712 für 25-Gbit/s-Netzwerke konfiguriert werden.

Trennt	Menge	Festplatte	Nutzbare Kapazität	Netzwerk
StorageGRID SG5712 Appliances	4	48 x 4 TB (Nearline SAS-HDD)	136 TB	10 Gbit/s

Durch die Auswahl von Appliance-Optionen mit höherer Performance, wie z. B. NetApp StorageGRID SG5760, SG6060 oder All-Flash SGF6112 Appliances, können deutliche Performance-Vorteile erzielt werden. Wenden Sie sich an Ihren NetApp StorageGRID Solution Architect, um Hilfe bei der Dimensionierung zu erhalten.

Softwareanforderungen von CommVault und StorageGRID

In den folgenden Tabellen sind die Software-Anforderungen für die auf der Software von VMware installierte CommVault und NetApp StorageGRID für unsere Tests aufgeführt. Vier MediaAgent Datenübertragungsmanager und ein CommServe-Server wurden installiert. In den Tests wurden 10-Gbit-s-Networking für die VMware Infrastruktur implementiert. Der folgenden Tabelle zu entnehmen

In der folgenden Tabelle sind die Gesamtsystemanforderungen der CommVault Software aufgeführt:

Komponente	Menge	Datenspeicher	Größe	Gesamt	Gesamte erforderliche IOPS
CommServe Server	1	BETRIEBSSYSTEM	500 GB	500 GB	1. A.
		SQL SERVER GESCHULT SIND	500 GB	500 GB	1. A.

Komponente	Menge	Datenspeicher	Größe	Gesamt	Gesamte erforderliche IOPS
MediaAgent	4	Virtuelle CPU (vCPU)	16	64	1. A.
		RAM	128 GB	512	1. A.
		BETRIEBSSYSTEM	500 GB	2 TB	1. A.
		Index-Cache	2 TB	8 TB	200+
		DDB	2 TB	8 TB	200–80.000 K

In der Testumgebung wurden ein primärer virtueller Administrator-Node und ein virtueller Gateway-Node auf VMware auf einem NetApp E-Series E2812 Storage-Array implementiert. Jeder Knoten befand sich auf einem separaten Server mit den in der folgenden Tabelle beschriebenen Mindestanforderungen an die Produktionsumgebung:

Die folgende Tabelle listet die Anforderungen für virtuelle StorageGRID-Admin-Nodes und Gateway-Nodes auf:

Node-Typ	Menge	VCPU	RAM	Storage
Gateway-Node	1	8	24 GB	100 GB LUN für das OS
Administrator-Node	1	8	24 GB	100 GB LUN für das OS 200-GB-LUN für Administrator-Node-Tabellen 200 GB-LUN für das Admin-Node-Revisionsprotokoll

Leitfaden zur StorageGRID Dimensionierung

Wenden Sie sich an Ihre NetApp Datenschutzexperten, um Informationen zur spezifischen Dimensionierung für Ihre Umgebung zu erhalten. NetApp-Spezialisten können mit dem CommVault Total Backup Storage Calculator die Anforderungen an die Backup-Infrastruktur einschätzen. Für das Tool ist der Zugriff auf das CommVault Partner Portal erforderlich. Melden Sie sich bei Bedarf an, um darauf zuzugreifen.

Eingaben zur CommVault-Größenbestimmung

Die folgenden Aufgaben können zur Durchführung einer Bestandsaufnahme für die Dimensionierung der Datensicherheitslösung verwendet werden:

- Identifizieren Sie die System- oder Applikations-/Datenbank-Workloads und die entsprechende Front-End-Kapazität (in Terabyte [TB]), die geschützt werden muss.
- Identifizieren Sie den VM-/Datei-Workload und ähnliche Front-End-Kapazität (TB), die geschützt werden muss.
- Identifizieren Sie Anforderungen für die kurzfristige und langfristige Datenaufbewahrung.
- Ermittlung der täglichen prozentualen Änderungsrate für die ermittelten Datensätze/Workloads
- Ermittlung des prognostizierten Datenwachstums in den nächsten 12, 24 und 36 Monaten
- Definieren Sie RTO und RPO für Datensicherung/Recovery entsprechend den geschäftlichen Anforderungen.

Wenn diese Informationen verfügbar sind, kann die Dimensionierung der Backup-Infrastruktur vorgenommen werden, was zu einer Aufschlüsselung der benötigten Speicherkapazitäten führt.

Leitfaden zur StorageGRID Dimensionierung

Bevor Sie die NetApp StorageGRID Dimensionierung durchführen, sollten Sie die folgenden Aspekte für Ihre Workloads berücksichtigen:

- Nutzbare Kapazität
- Worm-Modus
- Durchschnittliche Objektgröße
- Performance-Anforderungen erfüllt
- ILM-Richtlinie angewendet

Die nutzbare Kapazität muss der Größe des Backup-Workloads entsprechen, den Sie in StorageGRID gestaffelt haben, sowie dem Aufbewahrungszeitplan.

Wird der WORM-Modus aktiviert oder nicht? Wenn WORM in CommVault aktiviert ist, wird dadurch die Objektsperre auf StorageGRID konfiguriert. Dadurch wird die erforderliche Objektspeicher-Kapazität erhöht. Die erforderliche Kapazität variiert basierend auf der Aufbewahrungsdauer und der Anzahl der Objektänderungen bei jedem Backup.

Die durchschnittliche Objektgröße ist ein Eingabeparameter, der bei der Dimensionierung für die Performance in einer StorageGRID Umgebung hilft. Die durchschnittliche Objektgröße, die für einen CommVault-Workload verwendet wird, hängt vom Backup-Typ ab.

In der folgenden Tabelle sind die durchschnittlichen Objektgrößen nach Backup-Typ aufgeführt und die Lesevorgänge aus dem Objektspeicher werden durch den Wiederherstellungsprozess beschrieben:

Backup-Typ	Durchschnittliche Objektgröße	Wiederherstellungsverhalten
Erstellen Sie eine Zusatzkopie in StorageGRID	32 MB	Vollständiger Lesezugriff auf ein 32-MB-Objekt

Backup-Typ	Durchschnittliche Objektgröße	Wiederherstellungsverhalten
Leiten des Backups auf StorageGRID (Deduplizierung aktiviert)	8 MB	1 MB zufälliger Lesebereich
Leiten Sie das Backup auf StorageGRID (Deduplizierung deaktiviert)	32 MB	Vollständiger Lesezugriff auf ein 32-MB-Objekt

Darüber hinaus sind Sie über die Performance-Anforderungen für vollständige Backups und inkrementelle Backups in der Lage, die Dimensionierung für die StorageGRID Storage-Nodes zu bestimmen. StorageGRID Richtlinie für Information Lifecycle Management (ILM) Datensicherungsmethoden bestimmen die zur Speicherung von CommVault Backups benötigte Kapazität und wirken sich auf die Grid-Größe aus.

StorageGRID ILM-Replizierung ist einer von zwei Mechanismen, die StorageGRID zum Speichern von Objektdaten verwendet. Wenn StorageGRID einer ILM-Regel Objekte zuweist, die Daten repliziert, erstellt das System exakte Kopien der Objektdaten und speichert die Kopien auf Storage-Nodes.

Das Verfahren zur Einhaltung von Datenkonsistenz ist die zweite Methode, die von StorageGRID zum Speichern von Objektdaten verwendet wird. Wenn StorageGRID einer ILM-Regel Objekte zuweist, die für die Erstellung von Kopien, die nach Erasure codiert wurden, konfiguriert wird, werden Objektdaten in Datenfragmente unterteilt. Danach werden zusätzliche Paritätsfragmente berechnet und jedes Fragment auf einem anderen Storage Node gespeichert. Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Datenfragment oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zur Fehlerkorrektur ein neues Fragment unter Verwendung einer Untergruppe der verbleibenden Daten- und Paritätsfragmente erstellen.

Die beiden Mechanismen erfordern unterschiedliche Mengen an Storage, wie die folgenden Beispiele zeigen:

- Wenn Sie zwei replizierte Kopien speichern, verdoppelt sich Ihr Storage-Overhead.
- Wenn Sie eine 2 Kopie, die nach der Datenlöschung codiert wurde, speichern, erhöht sich Ihr Storage-Overhead um das 1.5-Fache.

Für die getestete Lösung wurde eine Entry-Level StorageGRID Implementierung an einem einzelnen Standort genutzt:

- Admin-Node: VMware Virtual Machine (VM)
- Load Balancer: VMware VM
- Storage-Nodes: 4 x SG5712 mit 4-TB-Laufwerken
- Primärer Admin-Node und Gateway-Node: VMware VMs mit den Mindestanforderungen für Produktions-Workloads

StorageGRID unterstützt auch Load Balancer von Drittanbietern.

StorageGRID wird in der Regel an zwei oder mehr Standorten mit Datensicherungsrichtlinien implementiert, die Daten replizieren, um vor Ausfällen auf Node- und Site-Ebene zu schützen. Wenn Sie Ihre Daten in StorageGRID sichern, sind Ihre Daten durch mehrere Kopien oder durch Erasure Coding geschützt, durch das Daten zuverlässig durch einen Algorithmus getrennt und neu zusammengestellt werden.

Sie können das Sizing-Tool verwenden "Fusion" Zur Größenbeaufstellung des Rasters.

Skalierbarkeit

Ein NetApp StorageGRID System lässt sich mit weiteren Storage-Nodes erweitern, einem vorhandenen Standort neue Grid-Nodes hinzufügen oder ein neues Datacenter hinzufügen. Eine Erweiterung kann vorgenommen werden, ohne den Betrieb des aktuellen Systems zu unterbrechen.
StorageGRID skaliert die Performance mithilfe von Nodes mit höherer Performance für die Storage-Nodes oder der physischen Appliance mit dem Load Balancer und den Admin-Nodes oder durch einfaches Hinzufügen weiterer Nodes.

Weitere Informationen zur Erweiterung des StorageGRID-Systems finden Sie unter "StorageGRID 11.9 Erweiterungsleitfaden".

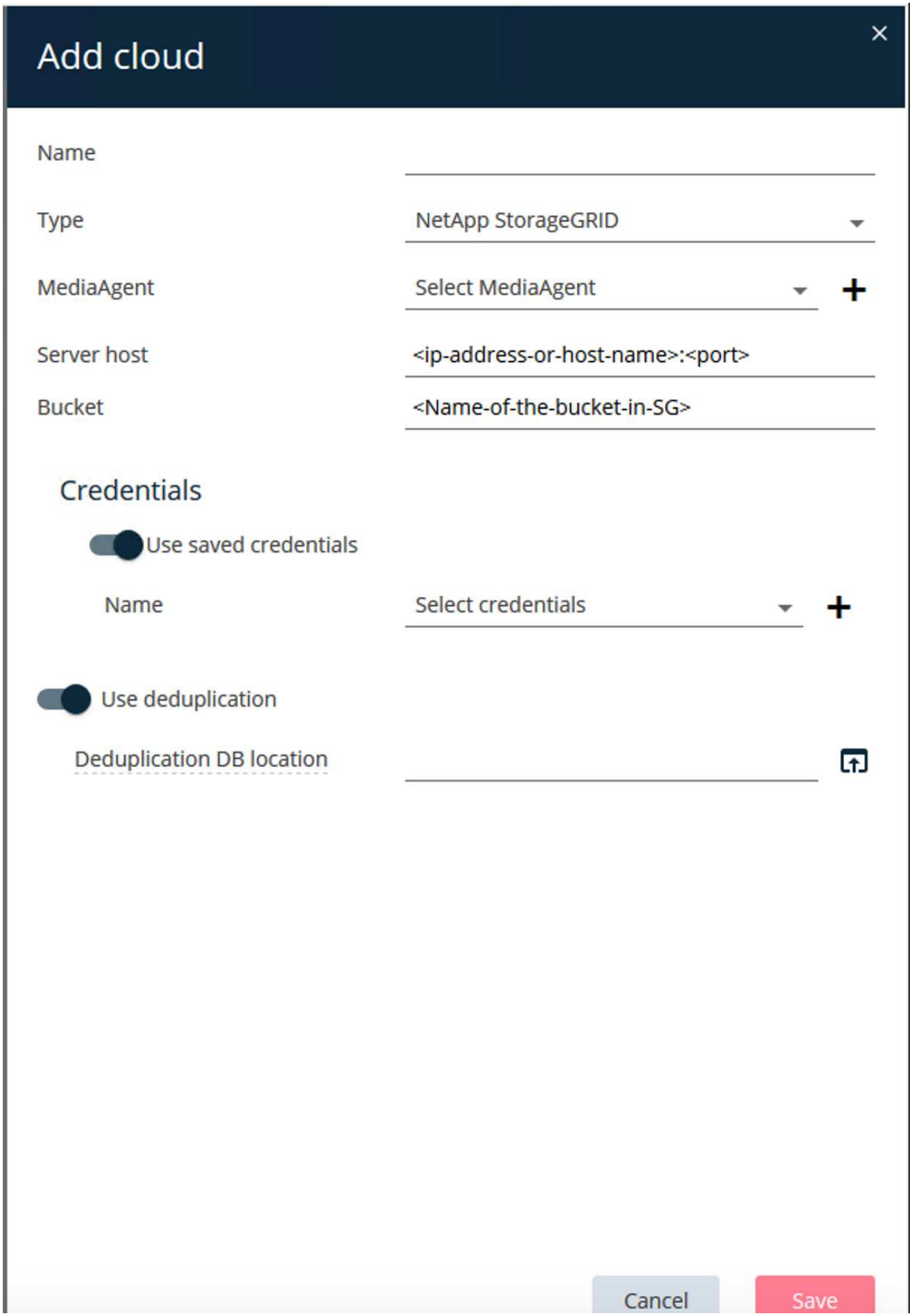
Einen Datensicherungsauftrag ausführen

Zur Konfiguration von StorageGRID mit CommVault Complete Backup and Recovery for NetApp wurden folgende Schritte durchgeführt, um StorageGRID als Cloud-Bibliothek innerhalb der CommVault Software hinzuzufügen.

Schritt: CommVault mit StorageGRID konfigurieren

Schritte

1. Melden Sie sich beim CommVault Command Center an. Klicken Sie im linken Fensterbereich auf Storage > Cloud > Add, um das Dialogfeld Add Cloud anzuzeigen und darauf zu antworten:


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. Wählen Sie für Typ die Option NetApp StorageGRID aus.
3. Wählen Sie für MediaAgent alle mit der Cloud-Bibliothek verknüpften Optionen aus.
4. Geben Sie unter Serverhost die IP-Adresse oder den Hostnamen des StorageGRID-Endpunkts und die Portnummer ein.

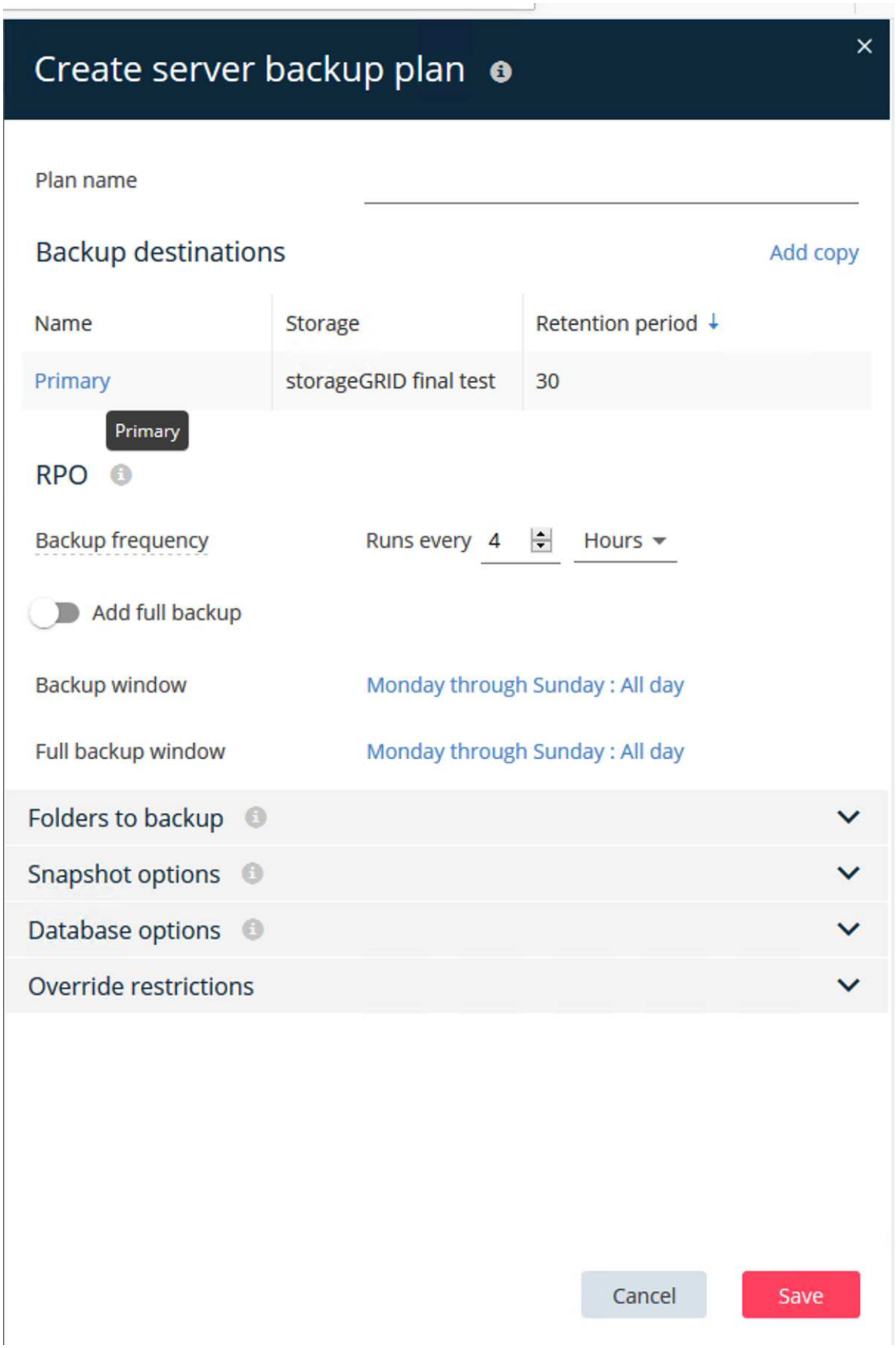
   Folgen Sie den Schritten in der StorageGRID-Dokumentation auf "So konfigurieren Sie einen Load Balancer-Endpunkt (Port)". Stellen Sie sicher, dass Sie über einen HTTPS-Port mit einem selbstsignierten Zertifikat und der IP-Adresse oder dem Domänennamen des StorageGRID-Endpunkts verfügen.

5. Wenn Sie Deduplizierung verwenden möchten, aktivieren Sie diese Option und geben den Pfad zum Speicherort der Deduplizierungsdatenbank an.
6. Klicken Sie auf Speichern .

Schritt 2: Erstellen eines Backup-Plans mit StorageGRID als primäres Ziel

Schritte

1. Wählen Sie im linken Fensterbereich Verwalten > Pläne aus, um das Dialogfeld Serverbackup-Plan erstellen anzuzeigen und darauf zu antworten.

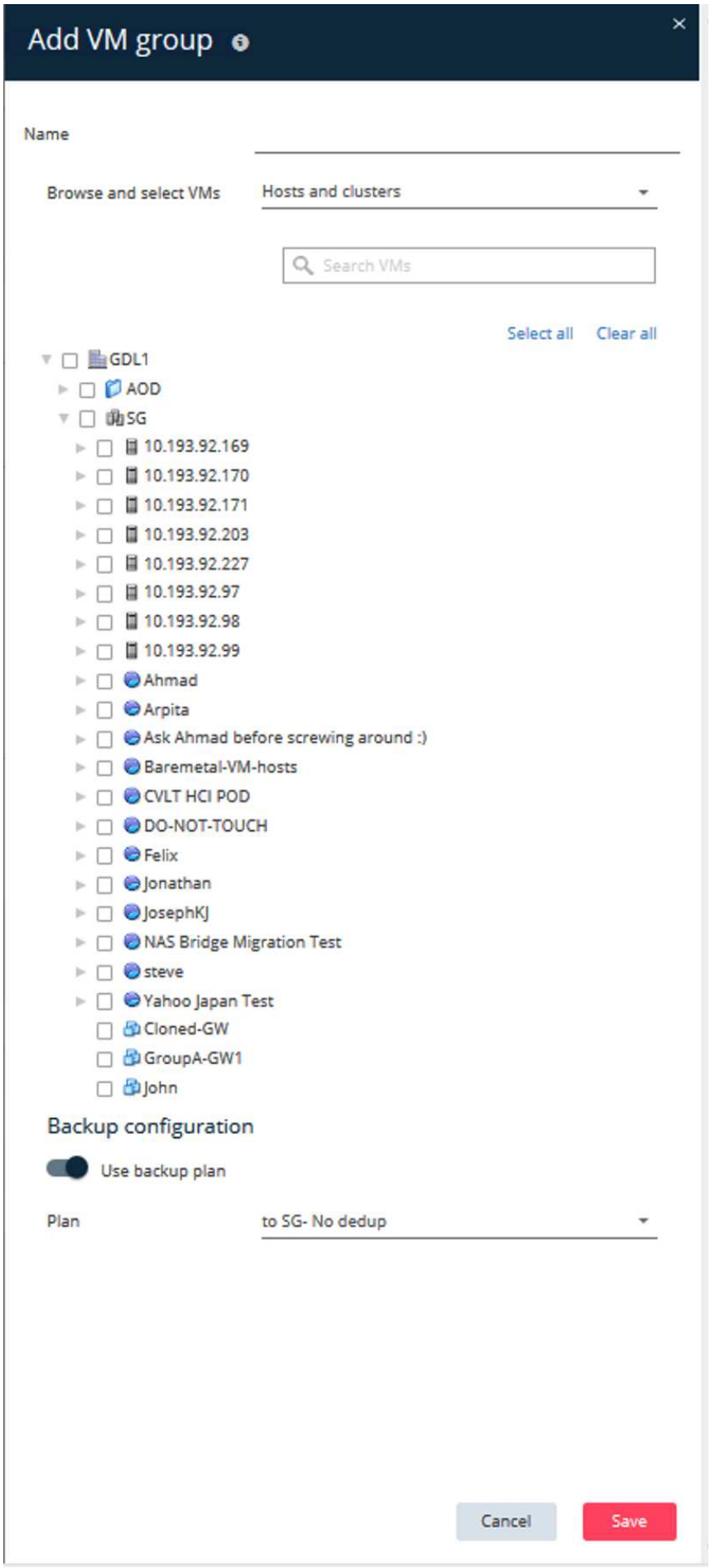

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. Geben Sie einen Plannamen ein.
3. Wählen Sie das zuvor erstellte Backup-Ziel für den StorageGRID Simple Storage Service (S3) Storage aus.
4. Geben Sie die gewünschte Backup-Aufbewahrungsfrist und das Recovery Point Objective (RPO) ein.
5. Klicken Sie auf Speichern .

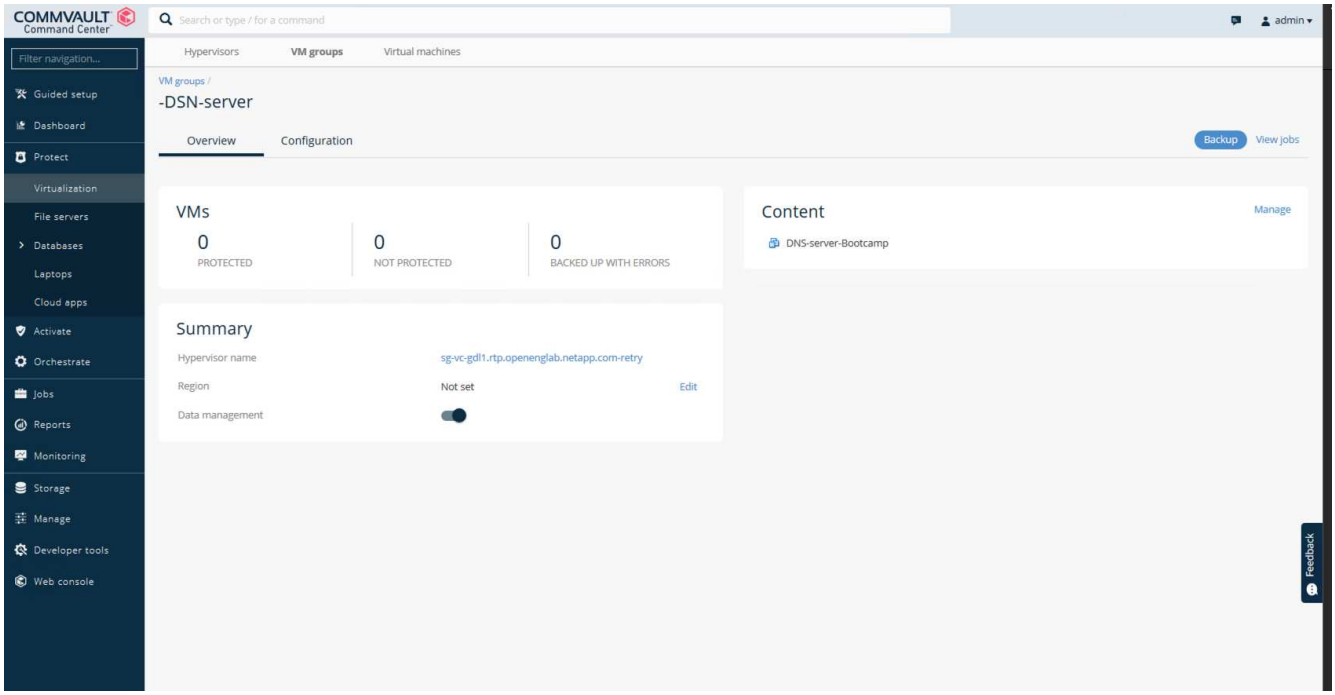
Schritt 3: Starten Sie einen Backup-Job zum Schutz Ihrer Workloads

Schritte

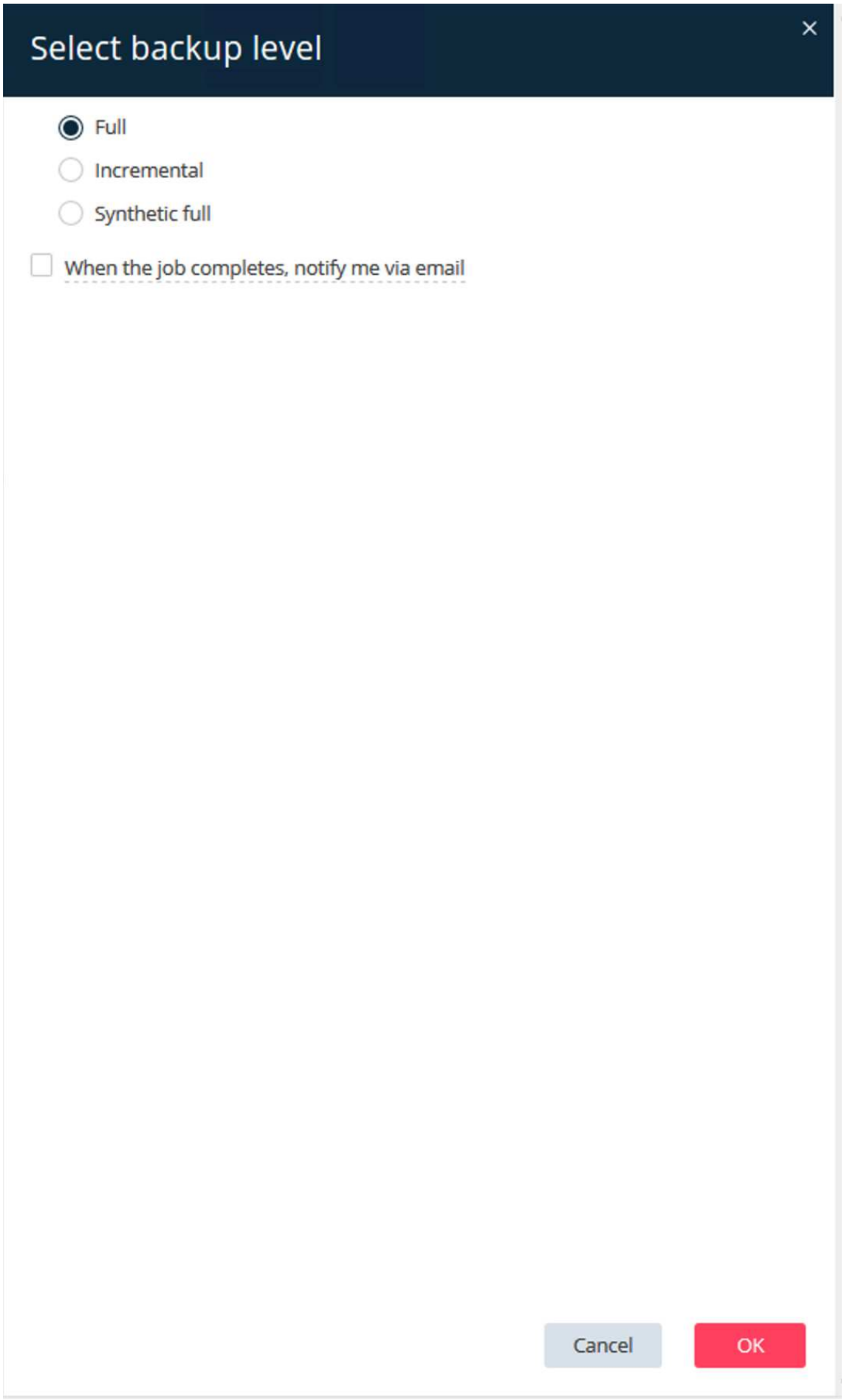
1. Navigieren Sie im CommVault Command Center zu Protect > Virtualization.
2. Fügen Sie einen VMware vCenter Server-Hypervisor hinzu.
3. Klicken Sie auf den Hypervisor, den Sie gerade hinzugefügt haben.
4. Klicken Sie auf VM-Gruppe hinzufügen, um auf das Dialogfeld VM-Gruppe hinzufügen zu antworten, damit Sie die vCenter-Umgebung sehen können, die Sie schützen möchten.


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

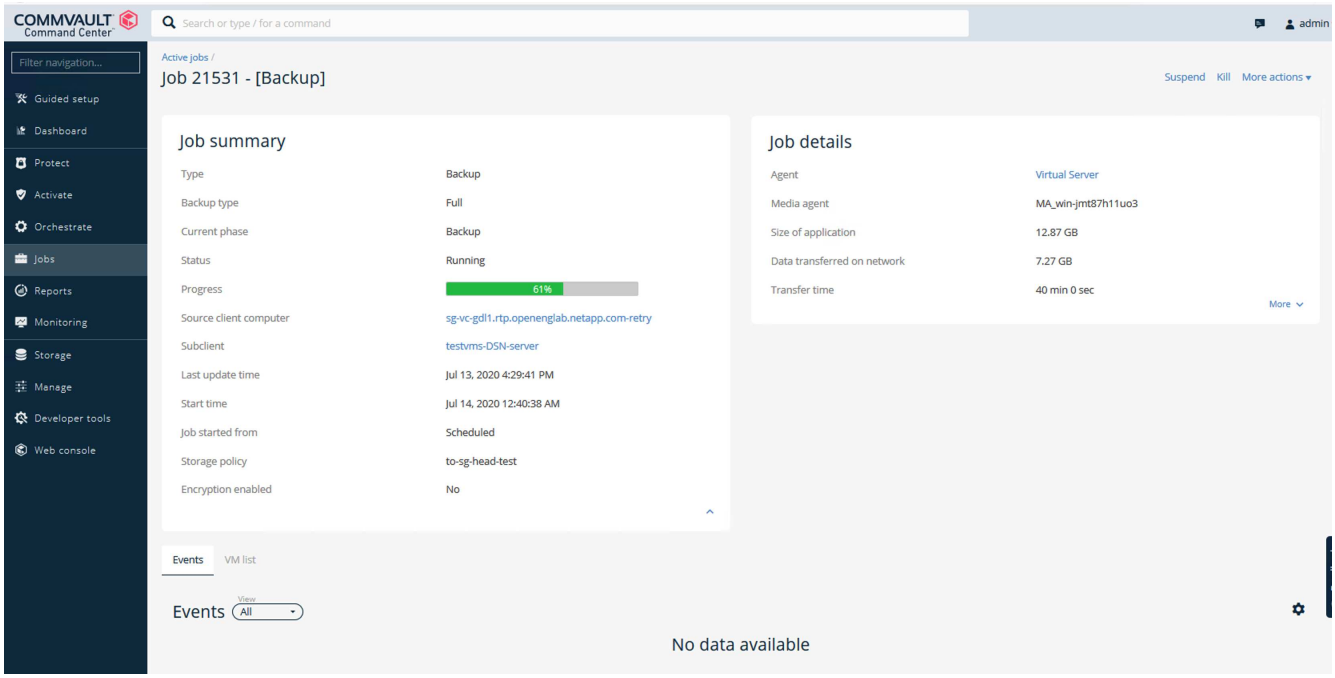
5. Wählen Sie einen Datenspeicher, eine VM oder eine Sammlung von VMs aus und geben Sie einen Namen dafür ein.
6. Wählen Sie den Backup-Plan aus, den Sie in der vorherigen Aufgabe erstellt haben.
7. Klicken Sie auf Speichern, um die erstellte VM-Gruppe anzuzeigen.
8. Wählen Sie oben rechts im VM-Gruppenfenster die Option Backup:



9. Wählen Sie als Sicherungsebene die Option voll aus, fordern Sie (optional) eine E-Mail an, wenn die Sicherung abgeschlossen ist, und klicken Sie dann auf OK, um den Sicherungsauftrag zu starten:


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. Navigieren Sie zur Seite mit der Jobzusammenfassung, um die Jobmetriken anzuzeigen:



Performance-Tests der Baseline prüfen

Beim Aux-Kopiervorgang haben vier CommVault MediaAgents Daten auf einem NetApp AFF A300-System gesichert und eine zusätzliche Kopie auf NetApp StorageGRID erstellt. Details zur Test-Setup-Umgebung finden Sie im Abschnitt Solution Design and Best Practices im "NetApp Scale-out-Datensicherung mit CommVault" technischen Bericht.

Die Tests wurden mit 100 VMs und 1000 VMs durchgeführt, wobei beide Tests mit einer Kombination aus Windows und CentOS VMs 50/50 durchgeführt wurden. Die folgende Tabelle enthält die Ergebnisse unserer grundlegenden Performance-Tests:

Betrieb	Backup-Geschwindigkeit	Wiederherstellungsgeschwindigkeit
Aux-Kopie	2 TB/Stunde	1.27 TB/Stunde
Direkt zum und vom Objekt (Deduplizierung ein)	2.2 TB/Stunde	1.22 TB/Stunde

Um eine Performance-Steigerung zu testen, wurden 2.5 Millionen Objekte gelöscht. Wie in den Abbildungen 2 und 3 dargestellt, wurde die Löschung in weniger als 3 Stunden abgeschlossen und mehr als 80 TB an Speicherplatz freigegeben. Der Löschvorgang begann um 10:30 UHR.

Abbildung 1: Löschung von 2.5 Millionen (80 TB) Objekten in weniger als 3 Stunden

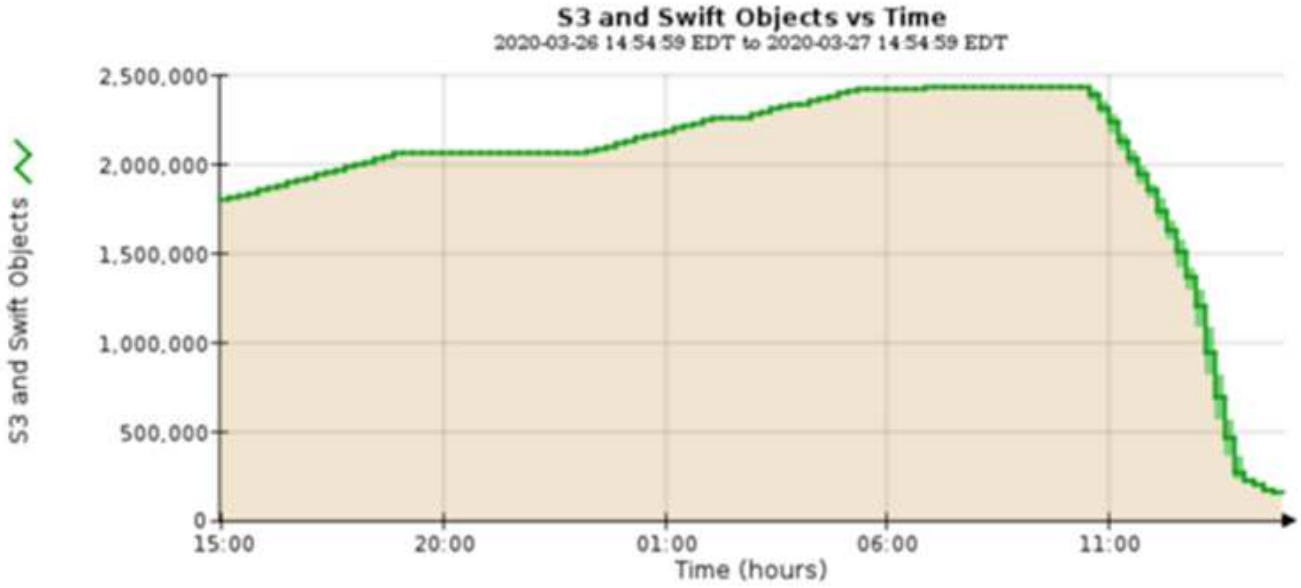
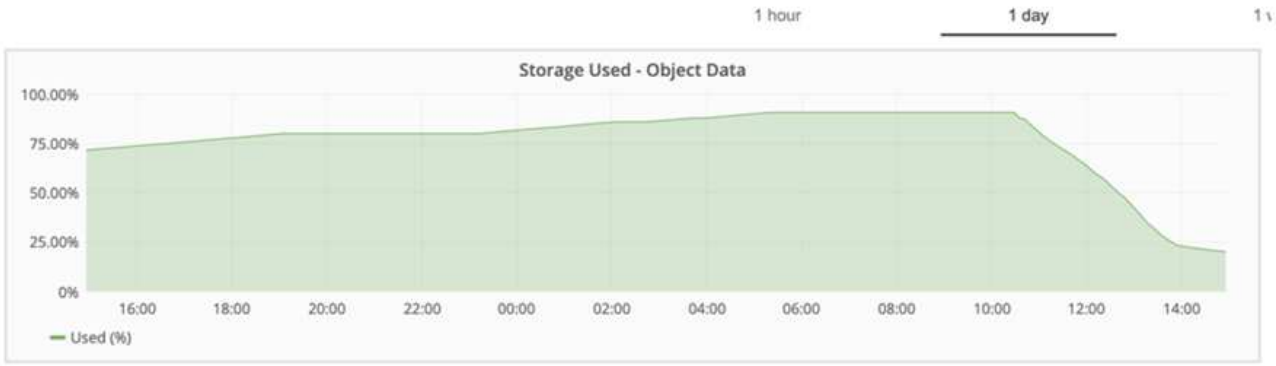


Abbildung 2: Freigabe von bis zu 80 TB Storage in weniger als 3 Stunden



Empfehlung für die Bucket-Konsistenzstufe

Mit NetApp StorageGRID kann der Endbenutzer die Konsistenzstufe für Vorgänge auswählen, die für Objekte in S3-Buckets (Simple Storage Service) durchgeführt werden.

CommVault MediaAgents sind die Data Mover in einer CommVault-Umgebung. In den meisten Fällen werden MediaAgents so konfiguriert, dass sie lokal in einen primären StorageGRID-Standort schreiben. Aus diesem Grund wird eine hohe Konsistenz innerhalb eines lokalen primären Standorts empfohlen. Beachten Sie die folgenden Richtlinien, wenn Sie die Konsistenzstufe für CommVault Buckets festlegen, die in StorageGRID erstellt wurden.

Wenn Sie eine CommVault-Version vor 11.0.0 - Service Pack 16 haben, sollten Sie ein Upgrade von CommVault auf die neueste Version in Betracht ziehen. Wenn dies keine Option ist, beachten Sie bitte die Richtlinien für Ihre Version.

- CommVault-Versionen vor 11.0.0 - Service Pack 16.* in Versionen vor 11.0.0 - Service Pack 16 führt CommVault S3 HEAD und GET-Operationen an nicht vorhandenen Objekten als Teil des Wiederherstellungs- und Beschneidungsprozesses durch. Wenn Sie die Konsistenzstufe für Bucket auf starke Standorte festlegen, wird die optimale Konsistenzstufe für CommVault Backups auf StorageGRID erreicht.

- CommVault-Versionen 11.0.0 - Service Pack 16 und höher.* in Version 11.0.0 - Service Pack 16 und höher wird die Anzahl der S3-HEAD- und GET-Vorgänge für nicht vorhandene Objekte minimiert. Setzen Sie die Standard-Bucket-Konsistenzstufe auf „Read-after-New-write“, um eine hohe Konsistenzstufe in der CommVault- und StorageGRID-Umgebung zu gewährleisten.

TR-4626: Load Balancer

Verwenden Sie Load Balancer von Drittanbietern mit StorageGRID

Erfahren Sie mehr über die Rolle eines Drittanbieters und globaler Load Balancer in einem Objektspeicher-System wie StorageGRID.

Allgemeine Hinweise für die Implementierung von NetApp® StorageGRID® mit Load Balancern von Drittanbietern.

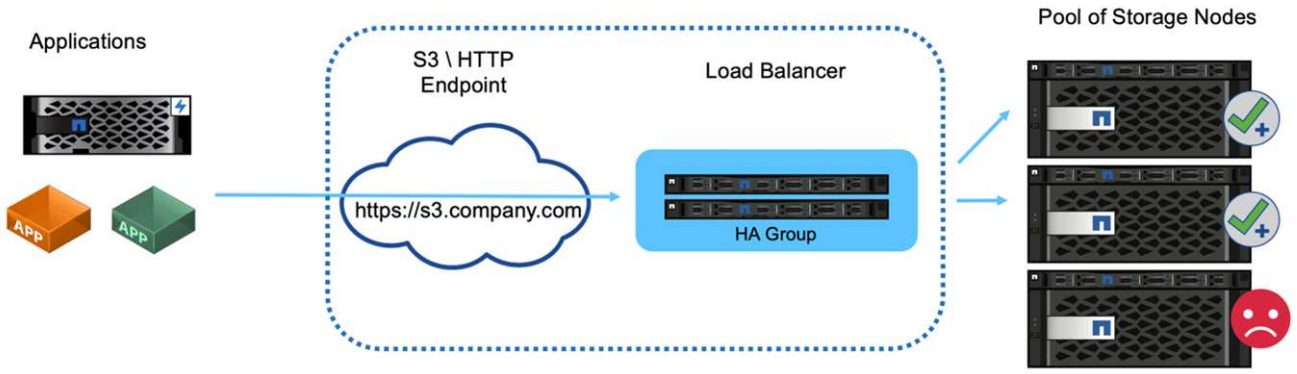
Objekt-Storage ist gleichbedeutend mit dem Begriff Cloud-Storage. Wie Sie erwarten würden, adressieren Applikationen, die Cloud-Storage nutzen, diesen Storage über eine URL. Unter dieser einfachen URL StorageGRID lässt sich die Kapazität, Performance und Langlebigkeit auf einen einzelnen Standort oder über geografisch verteilte Standorte skalieren. Die Komponente, die diese Einfachheit ermöglicht, ist ein Load Balancer.

Dieses Dokument dient dazu, StorageGRID Kunden über Load Balancer-Optionen zu informieren und allgemeine Hinweise zur Konfiguration von Load Balancern anderer Anbieter zu geben.

Grundlagen der Lastverteilung

Load Balancer sind eine wesentliche Komponente von Objekt-Storage-Systemen der Enterprise-Klasse wie StorageGRID. StorageGRID besteht aus mehreren Storage-Nodes, von denen jeder den gesamten S3-Namensraum (Simple Storage Service) für eine bestimmte StorageGRID Instanz darstellen kann. Load Balancer erzeugen einen hochverfügbaren Endpunkt, hinter dem StorageGRID Nodes platziert werden können. StorageGRID ist einzigartig unter S3-kompatiblen Objektspeichersystemen, da es einen eigenen Load Balancer anbietet, aber auch Load Balancer von Drittanbietern oder Mehrzweck-Systemen wie F5, Citrix NetScaler, HA Proxy, NGINX usw. unterstützt.

In der folgenden Abbildung wird der Beispiel-URL/ Fully Qualified Domain Name (FQDN) „s3.company.com” verwendet. Der Load Balancer erstellt eine virtuelle IP (VIP), die über DNS in den FQDN aufgelöst wird und leitet dann alle Anforderungen von Anwendungen an einen Pool von StorageGRID-Knoten weiter. Der Load Balancer führt eine Integritätsprüfung für jeden Node durch und stellt nur Verbindungen zu funktionstüchtigen Nodes her.



Die Abbildung zeigt den von StorageGRID bereitgestellten Load Balancer, das Konzept ist jedoch dasselbe bei

Load Balancern von Drittanbietern. Anwendungen richten eine HTTP-Sitzung mithilfe der VIP auf dem Load Balancer ein und der Datenverkehr wird über den Load Balancer zu den Speicher-Nodes geleitet. Standardmäßig wird der gesamte Datenverkehr von der Anwendung zum Load Balancer und vom Load Balancer zum Speicher-Node über HTTPS verschlüsselt. HTTP ist eine unterstützte Option.

Lokale und globale Load Balancer

Es gibt zwei Arten von Load Balancern:

- * Local Traffic Manager (LTM)*. Verteilt Verbindungen über einen Node-Pool an einem einzelnen Standort.
- **Global Service Load Balancer (GSLB)**. Verteilt Verbindungen über mehrere Standorte und sorgt so für einen effektiven Lastenausgleich bei LTM-Load-Balancern. Stellen Sie sich ein GSLB als intelligenten DNS-Server vor. Wenn ein Client eine StorageGRID-Endpunkt-URL anfordert, löst die GSLB sie auf Grundlage der Verfügbarkeit oder anderer Faktoren in die VIP eines LTM auf (z. B. welche Website kann eine niedrigere Latenz für die Anwendung bereitstellen). Es ist zwar immer ein LTM erforderlich, abhängig von der Anzahl der StorageGRID-Standorte und Ihren Applikationsanforderungen ist jedoch ein GSLB optional.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID Dokumentationscenterhttps://docs.netapp.com/us-en/storagegrid/[]
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- Überlegungen zum Design der StorageGRID f5 Load Balancer https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load NetApp StorageGRID ausgleichen https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp – Load Balancing NetApp StorageGRID https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Verwenden Sie StorageGRID Load Balancer

Erfahren Sie mehr über die Rolle eines StorageGRID Gateway Node-Load Balancers.

Allgemeine Anleitung zur Implementierung von NetApp® StorageGRID® Gateway Nodes.

Load Balancer für StorageGRID-Gateway-Nodes im Vergleich zum Load Balancer eines Drittanbieters

StorageGRID ist einzigartig unter S3-kompatiblen Objekt-Storage-Anbietern und bietet einen nativen Load Balancer als speziell entwickelte Appliance, VM oder Container. Der von StorageGRID bereitgestellte Load Balancer wird auch als Gateway-Node bezeichnet.

Für Kunden, die noch keinen Load Balancer wie F5, Citrix usw. besitzen, kann die Implementierung eines Load Balancers eines Drittanbieters sehr komplex sein. Der StorageGRID Load Balancer vereinfacht den Load Balancer erheblich.

Der Gateway Node ist ein hochverfügbarer und hochperformanter Load Balancer der Enterprise-Klasse. Kunden können den Gateway Node, den Load Balancer eines Drittanbieters oder sogar beide in einem Grid implementieren. Der Gateway Node ist ein lokaler Traffic-Manager und kein GSLB.

Der StorageGRID Load Balancer bietet folgende Vorteile:

- **Einfachheit**. Automatische Konfiguration von Ressourcen-Pools, Zustandsprüfungen, Patching und Wartung, alle gemanagt durch StorageGRID.
- **Leistung**. Der StorageGRID Load Balancer ist speziell für StorageGRID vorgesehen, kann Hochleistungs-Caching bereitstellen und Sie konkurrieren nicht mit anderen Anwendungen um Bandbreite.
- **Kosten**. Die Versionen für Virtual Machines (VM) und Container werden ohne zusätzliche Kosten bereitgestellt.
- **Verkehrsklassifizierungen**. Die Funktion zur erweiterten Traffic-Klassifizierung ermöglicht für StorageGRID spezifische QoS-Regeln sowie Workload-Analysen.
- **Zukünftige StorageGRID-spezifische Funktionen**. StorageGRID wird den Load Balancer in künftigen Versionen weiter optimieren und um innovative Funktionen erweitern.

Als integrierter Knoten von StorageGRID kann der lokale Verkehrsmanager erweiterte Integritätsprüfungen durchführen, um Anfragen basierend auf der Integrität, Auslastung und Ressourcenverfügbarkeit des Speicherknotens zu verteilen. Darüber hinaus besteht die Möglichkeit, die Last auf mehrere Standorte zu verteilen, wenn die StorageGRID Verbindungskosten zwischen den Standorten auf „0“ gesetzt sind. Falls die Speicherknoten nicht verfügbar sind, der Gateway-Knoten an einem Standort jedoch verfügbar ist, wird die Last automatisch an einen anderen Standort im Netz umgeleitet.

Die Load Balancer-Caching-Funktion des Gateway-Knotens soll eine erhebliche Leistungsverbesserung für bestimmte Workloads (wie z. B. KI-Training) bieten, bei denen ein Datensatz im Rahmen der Verarbeitung dieser Daten mehrmals erneut gelesen wird. Caching-Gateway-Knoten können auch physisch vom Rest des Grids entfernt bereitgestellt werden, was bei einigen Workloads eine bessere Leistung und eine geringere WAN-Netzwerkauslastung ermöglicht. Der Cache arbeitet in einem Rücklesemodus, in dem Schreibvorgänge nicht zwischengespeichert werden und den Zustand des Caches nicht ändern. Jeder Caching-Gateway-Knoten arbeitet unabhängig von allen anderen Caching-Gateway-Knoten.

Weitere Informationen zum Bereitstellen des StorageGRID Gateway Node finden Sie im "StorageGRID-Dokumentation" .

Erfahren Sie, wie Sie SSL-Zertifikate für HTTPS in StorageGRID implementieren

Verstehen Sie die Wichtigkeit und die Schritte zur Implementierung von SSL-Zertifikaten in StorageGRID.

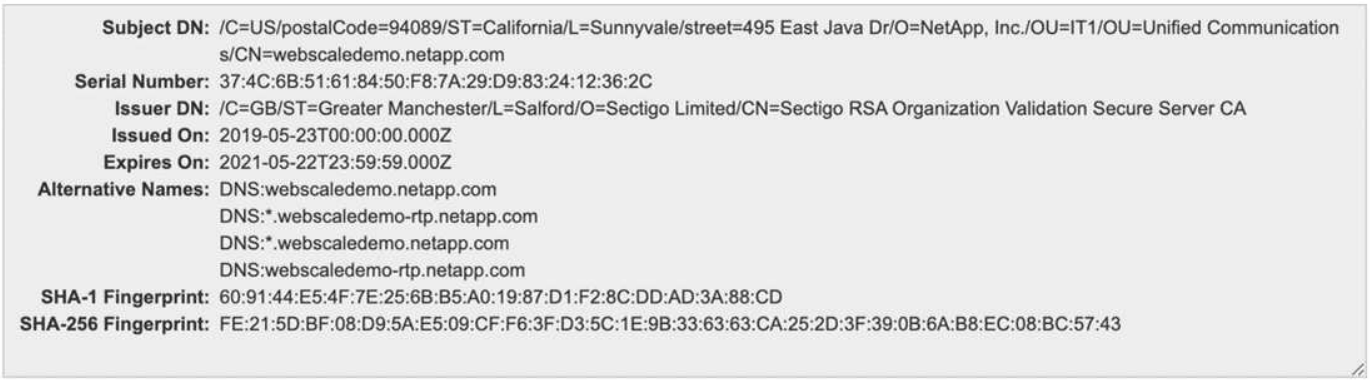
Wenn Sie HTTPS verwenden, müssen Sie über ein SSL-Zertifikat (Secure Sockets Layer) verfügen. Das SSL-Protokoll identifiziert die Clients und Endpunkte und validiert sie als vertrauenswürdig. SSL bietet auch die Verschlüsselung des Datenverkehrs. Das SSL-Zertifikat muss von den Clients vertrauenswürdig sein. Dazu kann das SSL-Zertifikat von einer global vertrauenswürdigen Zertifizierungsstelle (CA) wie DigiCert, einer privaten Zertifizierungsstelle, die in Ihrer Infrastruktur ausgeführt wird, oder einem vom Host generierten selbstsignierten Zertifikat stammen.

Die Verwendung eines global vertrauenswürdigen Zertifizierungsstellenzertifikats ist die bevorzugte Methode, da keine zusätzlichen clientseitigen Aktionen erforderlich sind. Das Zertifikat wird in den Load Balancer oder StorageGRID geladen, und die Clients vertrauen dem Endpunkt und stellen eine Verbindung her.

Für die Verwendung einer privaten Zertifizierungsstelle muss der Stammverzeichnis und alle untergeordneten Zertifikate zum Client hinzugefügt werden. Der Prozess zum Vertrauen auf ein privates CA-Zertifikat kann je nach Client-Betriebssystem und -Anwendungen variieren. Beispielsweise müssen Sie in ONTAP für FabricPool jedes Zertifikat in der Kette einzeln (Stammzertifikat, untergeordnetes Zertifikat, Endpunktzertifikat) auf das ONTAP-Cluster hochladen.

Bei Verwendung eines selbstsignierten Zertifikats muss der Client dem bereitgestellten Zertifikat vertrauen, ohne dass eine Zertifizierungsstelle die Authentizität überprüft. Einige Anwendungen akzeptieren möglicherweise keine selbstsignierten Zertifikate und können die Überprüfung nicht ignorieren.

Die Platzierung des SSL-Zertifikats im StorageGRID-Pfad des Client Load Balancer hängt davon ab, wo Sie die SSL-Terminierung benötigen. Sie können einen Load Balancer als Abschlussendpunkt für den Client konfigurieren und dann erneut verschlüsseln oder mit einem neuen SSL-Zertifikat für den Load Balancer zur StorageGRID-Verbindung verschlüsseln. Sie können auch den Datenverkehr passieren und StorageGRID als Endpunkt für die SSL-Terminierung verwenden. Wenn der Load Balancer der SSL-Abschlussendpunkt ist, wird das Zertifikat auf dem Load Balancer installiert und enthält den Betreffnamen für den DNS-Namen/die DNS-URL sowie alle alternativen URL-/DNS-Namen, für die ein Client für die Verbindung mit dem StorageGRID-Ziel über den Load Balancer konfiguriert ist. einschließlich aller Platzhalternamen. Wenn der Load Balancer für Passthrough konfiguriert ist, muss das SSL-Zertifikat in StorageGRID installiert werden. Auch hier muss das Zertifikat den Subject-Namen für den DNS-Namen/die URL sowie alle alternativen URL-/DNS-Namen enthalten, für die ein Client konfiguriert ist, um über den Load Balancer eine Verbindung zum StorageGRID-Ziel herzustellen, einschließlich aller Platzhalternamen. Einzelne Storage-Node-Namen müssen nicht im Zertifikat enthalten sein, sondern nur die Endpunkt-URLs.



Konfigurieren Sie den Load Balancer eines vertrauenswürdigen Drittanbieters in StorageGRID

Erfahren Sie, wie Sie einen vertrauenswürdigen Drittanbieter-Load Balancer in StorageGRID konfigurieren.

Wenn Sie einen oder mehrere externe Layer-7-Load-Balancer und IP-basierte S3-Bucket oder Gruppenrichtlinien verwenden, muss StorageGRID die IP-Adresse des tatsächlichen Absenders ermitteln. Dies geschieht durch einen Blick auf den X-Forwarded-for (XFF) Header, der vom Load Balancer in die Anfrage eingefügt wird. Da der XFF-Header einfach in Anfragen gespoooofing werden kann, die direkt an die Speicherknoten gesendet werden, muss StorageGRID bestätigen, dass jede Anforderung von einem vertrauenswürdigen Layer 7-Load-Balancer weitergeleitet wird. Wenn StorageGRID der Quelle der Anforderung nicht vertrauen kann, ignoriert er den XFF-Header. Es gibt eine Grid-Management-API, über die eine Liste vertrauenswürdiger externer Load Balancer der Ebene 7 konfiguriert werden kann. Diese neue API ist privat und kann sich bei zukünftigen StorageGRID Versionen ändern. Die aktuellsten Informationen finden Sie im KB-Artikel, "So konfigurieren Sie StorageGRID für die Verwendung mit Layer-7-Load-Balancern von Drittanbietern".

Informieren Sie sich über Load Balancer für lokale Traffic Manager

Informieren Sie sich über die Richtlinien für den Lastenausgleich von lokalen Traffic-Managern und ermitteln Sie die optimale Konfiguration.

Die folgenden Informationen werden als allgemeine Anleitung für die Konfiguration von Load Balancern von Drittanbietern dargestellt. Ermitteln Sie zusammen mit dem Load Balancer-Administrator die optimale Konfiguration für Ihre Umgebung.

Erstellen Sie eine Ressourcengruppe von Storage-Nodes

Gruppieren Sie StorageGRID-Speicherknoten in einen Ressourcen-Pool oder eine Dienstgruppe (die Terminologie kann sich von bestimmten Load Balancern unterscheiden). StorageGRID-Storage-Nodes stellen die S3-API auf den folgenden Ports zur Verfügung:

- S3 HTTPS: 18082
- S3 HTTP: 18084

Die meisten Kunden entscheiden sich dafür, die APIs auf dem virtuellen Server über die standardmäßigen HTTPS- und HTTP-Ports (443 und 80) bereitzustellen.

> Für jeden StorageGRID-Standort sind standardmäßig drei Storage-Nodes erforderlich, von denen zwei ordnungsgemäß sein müssen.

Zustandsprüfung

Load Balancer von Drittanbietern erfordern eine Methode, um den Zustand der einzelnen Nodes und ihre Eignung für den Empfang von Traffic zu bestimmen. NetApp empfiehlt zur Durchführung der Integritätsprüfung die HTTP- `OPTIONS` Methode. Der Load Balancer sendet HTTP- `OPTIONS` Anforderungen an jeden einzelnen Speicher-Node und erwartet eine `200` Statusantwort.

Wenn ein Speicher-Node keine Antwort bereitstellt, kann dieser Node keine `200` Speicheranforderungen bearbeiten. Ihre Anwendungs- und Geschäftsanforderungen sollten das Zeitlimit für diese Prüfungen und die Maßnahmen bestimmen, die Ihr Load Balancer ergreift.

Wenn beispielsweise drei von vier Storage-Nodes in Datacenter 1 ausgefallen sind, können Sie den gesamten Datenverkehr an Datacenter 2 leiten.

Das empfohlene Abfrageintervall beträgt einmal pro Sekunde und markiert den Knoten nach drei fehlgeschlagenen Überprüfungen offline.

Beispiel für S3-Integritätsprüfung

Im folgenden Beispiel senden wir `OPTIONS` und überprüfen nach `200 OK`. Wir verwenden `OPTIONS` , da Amazon S3) nicht autorisierte Anfragen unterstützt.

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

Zustandsprüfungen für Dateien oder Inhalte

Im Allgemeinen werden von NetApp keine dateibasierten Zustandsprüfungen empfohlen. In der Regel wird eine kleine Datei —`healthcheck.htm`z. B. in einem Bucket mit einer schreibgeschützten Richtlinie erstellt. Diese Datei wird dann vom Load Balancer abgerufen und ausgewertet. Dieser Ansatz hat mehrere Nachteile:

- **Abhängig von einem einzigen Konto.** Wenn das Konto, dem die Datei gehört, deaktiviert ist, schlägt die Integritätsprüfung fehl und es werden keine Speicheranforderungen verarbeitet.
- **Datenschutzregeln.** Das standardmäßige Datensicherungsschema hat einen Ansatz mit zwei Kopien. Wenn in diesem Szenario die beiden Speicherknoten, auf denen die Zustandspeckdatei gehostet wird, nicht verfügbar sind, schlägt die Integritätsprüfung fehl, und Speicheranforderungen werden nicht an funktionstüchtige Speicherknoten gesendet, wodurch das Grid offline geschaltet wird.
- **Audit Log Bloat.** Der Load Balancer ruft die Datei alle X Minuten von jedem Storage-Node ab und erstellt so viele Audit-Log-Einträge.
- **Ressourcenintensiv.** Das Abrufen der Zustandspeckdatei von jedem Node alle paar Sekunden verbraucht Grid- und Netzwerkressourcen.

Wenn eine inhaltsbasierte Zustandsprüfung erforderlich ist, verwenden Sie einen dedizierten Mandanten mit einem dedizierten S3-Bucket.

Persistenz der Sitzung

Sitzungspersistence oder Stickiness bezieht sich auf den Zeitpunkt, zu dem eine bestimmte HTTP-Sitzung bestehen darf. Standardmäßig werden Sitzungen von Storage-Nodes nach 10 Minuten getrennt. Längere Persistenz kann zu besserer Performance führen, da die Applikationen nicht für jede Aktion neu Sitzungen erstellen müssen. Offen zu halten, verbraucht jedoch Ressourcen. Wenn Sie feststellen, dass Ihr Workload von Vorteil ist, können Sie die Persistenz der Sitzung bei einem Load Balancer eines Drittanbieters verringern.

Virtuelle Hosted-Style-Adressierung

Virtual Hosted-Style ist jetzt die Standardmethode für AWS S3. Während StorageGRID und viele Applikationen weiterhin Pfadstil unterstützen, empfiehlt es sich, Unterstützung im Virtual Hosted-Stil zu implementieren. Virtuelle Anforderungen im gehosteten Stil enthalten den Bucket als Teil des Host-Namens.

Gehen Sie wie folgt vor, um Virtual Hosted-Style zu unterstützen:

- Unterstützung von Wildcard-DNS-Suchvorgängen: *.s3.company.com
- Verwenden Sie ein SSL-Zertifikat mit Subject alt-Namen, um Wildcard zu unterstützen: *.s3.company.com einige Kunden haben Sicherheitsbedenken bezüglich der Verwendung von Wildcard-Zertifikaten geäußert. StorageGRID unterstützt wie wichtige Applikationen wie FabricPool weiterhin den Zugriff auf Pfadstil. Allerdings schlagen bestimmte S3-API-Aufrufe fehl oder verhalten sich ohne virtuelle gehostete Unterstützung nicht ordnungsgemäß.

SSL-Terminierung

Die SSL-Terminierung bei Load Balancern von Drittanbietern bietet Sicherheitsvorteile. Wenn der Load Balancer beschädigt ist, wird das Grid unterteilt.

Es gibt drei unterstützte Konfigurationen:

- **SSL-Passthrough.** Das SSL-Zertifikat wird auf StorageGRID als benutzerdefiniertes Serverzertifikat installiert.
- **SSL-Terminierung und Re-Verschlüsselung (empfohlen).** Dies könnte von Vorteil sein, wenn Sie bereits die SSL-Zertifikatsverwaltung auf dem Load Balancer ausführen, anstatt das SSL-Zertifikat auf StorageGRID zu installieren. Diese Konfiguration bietet den zusätzlichen Sicherheitsvorteil, wenn die Angriffsfläche auf den Load Balancer begrenzt wird.
- **SSL-Terminierung mit HTTP.** In dieser Konfiguration wird SSL auf dem Load Balancer des Drittanbieters beendet und die Kommunikation vom Load Balancer zu StorageGRID ist unverschlüsselt, um die Vorteile von SSL-Off-Load zu nutzen (bei SSL-Bibliotheken, die in moderne Prozessoren integriert sind, ist dies nur ein begrenzter Vorteil).

Konfiguration durchlaufen

Wenn Sie den Load Balancer für Passthrough konfigurieren möchten, müssen Sie das Zertifikat auf StorageGRID installieren. Gehen Sie zum Menü:Konfiguration[Serverzertifikate > Object Storage API Service Endpoints Server Certificate].

IP-Sichtbarkeit des Quell-Clients

Mit StorageGRID 11.4 wurde das Konzept eines vertrauenswürdigen Load Balancers eines Drittanbieters eingeführt. Um die Client-Anwendungs-IP an StorageGRID weiterzuleiten, müssen Sie diese Funktion konfigurieren. Weitere Informationen finden Sie unter "So konfigurieren Sie StorageGRID für die Verwendung mit Layer-7-Load-Balancern von Drittanbietern."

So aktivieren Sie den XFF-Header, um die IP-Adresse der Client-Anwendung anzuzeigen:

Schritte

1. Notieren Sie die Client-IP im Überwachungsprotokoll.
2. Verwendung von `aws:SourceIp` S3-Bucket oder Gruppenrichtlinien

Strategien für die Lastverteilung

Die meisten Lastausgleichslösungen bieten mehrere Strategien für den Lastausgleich. Es folgen gängige Strategien:

- * Rundrobin.* Universelle Passform, jedoch mit wenigen Knoten und großen Transfers, die einzelne Knoten verstopfen
- **Geringste Verbindung.** Eignet sich für kleine und gemischte Objekt-Workloads, sodass die Verbindungen auf alle Nodes gleichmäßig verteilt werden.

Die Auswahl des Algorithmus wird mit einer wachsenden Anzahl von Storage-Nodes weniger wichtig.

Datenpfad

Alle Daten fließen über den Lastenausgleich des lokalen Traffic Managers. StorageGRID unterstützt kein direktes Server-Routing (DSR).

Überprüfen der Verteilung der Verbindungen

Um zu überprüfen, ob Ihre Methode die Last gleichmäßig auf die Storage-Nodes verteilt, überprüfen Sie die festgelegten Sitzungen auf jedem Node an einem bestimmten Standort:

- **UI-Methode.** Gehen Sie zum Menü:Support[Kennzahlen > S3-Übersicht > LDR HTTP-Sitzungen]
- **Metrics API.** Verwenden `storagegrid_http_sessions_incoming_currently_established`

Lernen Sie einige Anwendungsfälle für StorageGRID Konfigurationen kennen

Sehen Sie sich einige Anwendungsfälle für StorageGRID-Konfigurationen an, die von Kunden und NetApp IT implementiert wurden.

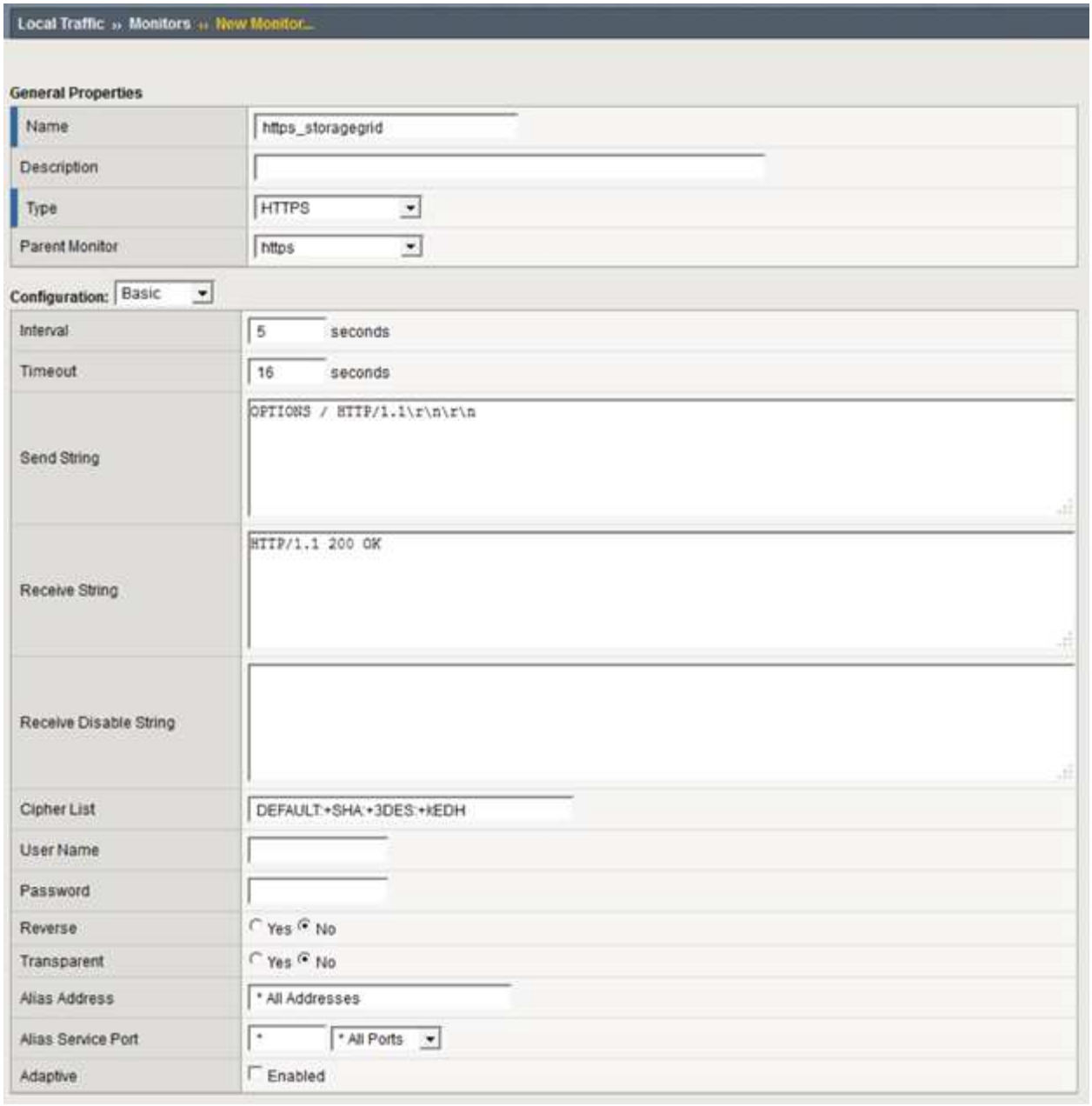
Die folgenden Beispiele veranschaulichen die Konfigurationen, die von StorageGRID Kunden, einschließlich NetApp IT, implementiert wurden.

Systemzustandsüberwachung von F5 BIG-IP Local Traffic Manager für S3 Bucket

Gehen Sie wie folgt vor, um die Integritätsprüfung für den F5 BIG-IP Local Traffic Manager zu konfigurieren:

Schritte

1. Erstellen Sie einen neuen Monitor.
   a. Geben Sie im Feld Typ `HTTPS`.
   b. Konfigurieren Sie das Intervall und die Zeitüberschreitung nach Bedarf.
   c. Geben Sie im Feld Send String \r\n sind Wagenrückläufe ein `OPTIONS / HTTP/1.1\r\n\r\n.` ; verschiedene Versionen der BIG-IP-Software erfordern Null, einen oder zwei Sätze von \r\n Sequenzen. Weitere Informationen finden Sie unter https://support.f5.com/csp/article/K10655.
   d. Geben Sie im Feld Empfangszeichenfolge Folgendes ein: `HTTP/1.1 200 OK`.



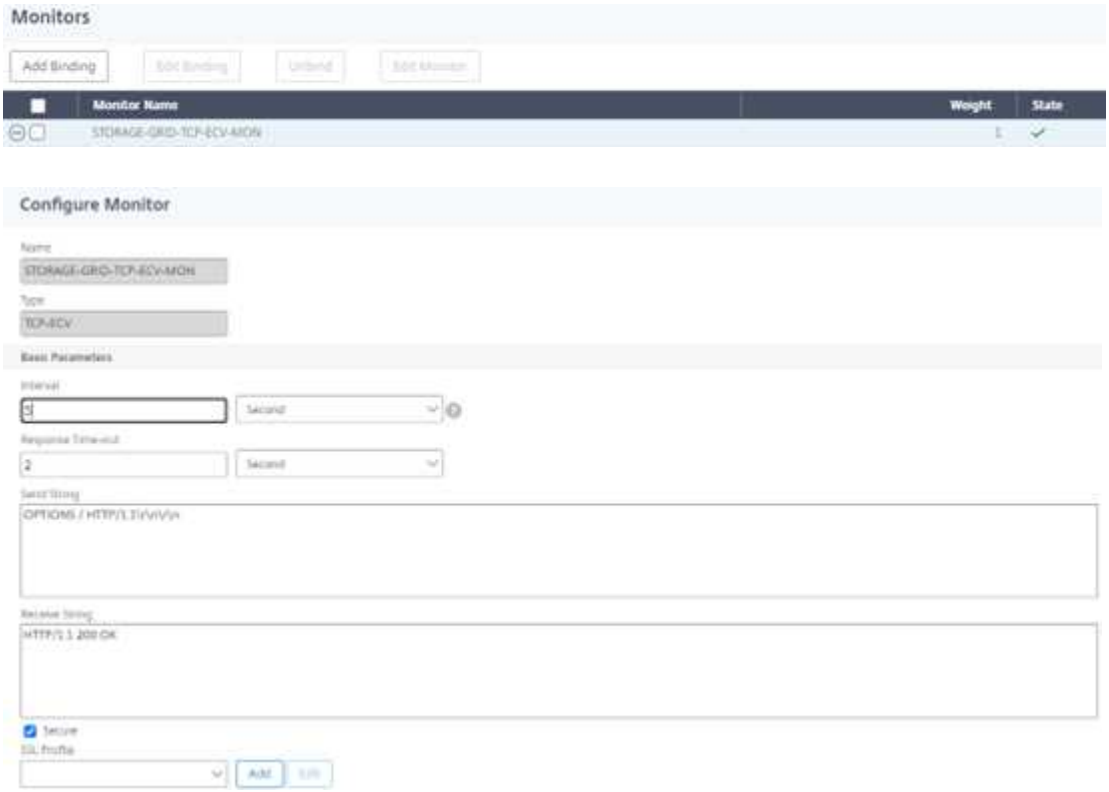
2. Erstellen Sie in Create Pool für jeden erforderlichen Port einen Pool.
   a. Weisen Sie die im vorherigen Schritt erstellte Systemzustandsüberwachung zu.
   b. Wählen Sie eine Lastausgleichsmethode aus.
   c. Wählen Sie Service Port: 18082 (S3).
   d. Nodes hinzufügen.

Citrix NetScaler

Citrix NetScaler erstellt einen virtuellen Server für den Speicherendpunkt und verweist auf StorageGRID-Speicherknoten als Anwendungsserver, die dann in Dienste gruppiert werden.

Verwenden Sie die HTTPS-ECV-Integritätsprüfung, um einen benutzerdefinierten Monitor zu erstellen, der die empfohlene Integritätsprüfung mithilfe der OPTIONSANFRAGE und des Empfangs durchführt `200`. HTTP-ECV ist mit einem Sendestring konfiguriert und validiert eine Empfangszeichenfolge.

Weitere Informationen finden Sie in der Citrix-Dokumentation, "Beispielkonfiguration für HTTP-ECV-Integritätsprüfung".



Loadbalancer.org

Loadbalancer.org hat eigene Integrationstests mit StorageGRID durchgeführt und hat einen umfassenden Konfigurationsleitfaden: https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp hat eigene Integrationstests mit StorageGRID durchgeführt und verfügt über einen umfassenden Konfigurationsleitfaden: https://kemptechnologies.com/solutions/netapp/.

HAProxy

Konfigurieren Sie HAProxy so, dass die OPTIONS-Anfrage verwendet wird, und prüfen Sie auf eine 200-Statusantwort für die Integritätsprüfung in haproxy.cfg. Sie können den Bind-Port am Front-End in einen anderen Port ändern, z. B. 443.

Im Folgenden finden Sie ein Beispiel für die SSL-Terminierung auf HAProxy:

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

Im Folgenden ein Beispiel für SSL-Passthrough:

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

Vollständige Beispiele für Konfigurationen für StorageGRID finden Sie unter "Beispiele für die HAProxy-Konfiguration" auf GitHub.

SSL-Verbindung in StorageGRID validieren

Erfahren Sie, wie Sie die SSL-Verbindung in StorageGRID validieren.

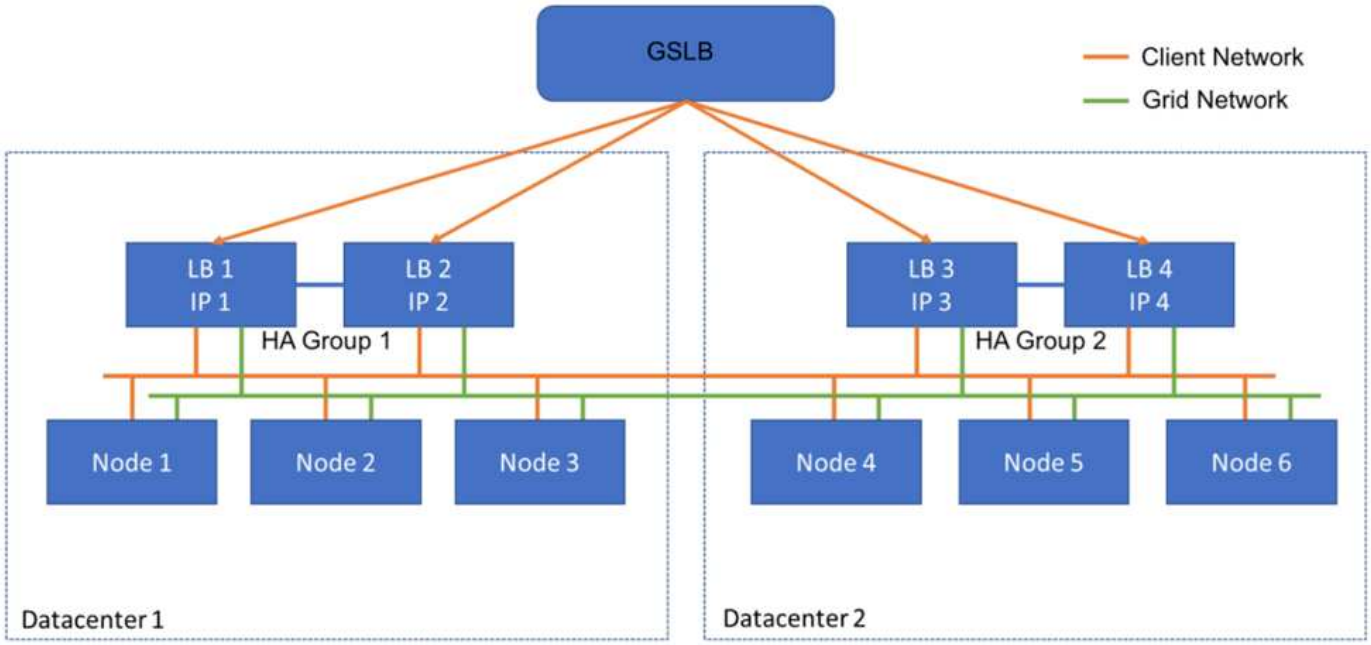
Nachdem der Load Balancer konfiguriert ist, sollten Sie die Verbindung mit Tools wie OpenSSL und der AWS CLI validieren. Andere Anwendungen, wie beispielsweise S3 Browser, ignorieren möglicherweise eine fehlerhafte SSL-Konfiguration.

Informationen zu den globalen Lastausgleichsanforderungen für StorageGRID

Informieren Sie sich über die Designüberlegungen und Anforderungen für den globalen Lastausgleich in StorageGRID.

Globaler Lastausgleich erfordert die Integration in DNS, um intelligentes Routing über mehrere StorageGRID-Standorte hinweg zu ermöglichen. Diese Funktion fällt nicht in die StorageGRID-Domäne und muss von einer Drittanbieterlösung bereitgestellt werden, z. B. den bereits erläuterten Load Balancer-Produkten und/oder einer DNS-Lösung zur Traffic-Kontrolle wie Infoblox. Dieser Lastenausgleich der obersten Ebene bietet intelligentes

Routing zum nächsten Zielstandort im Namespace sowie Ausfallerkennung und Umleitung zum nächsten Standort im Namespace. Eine typische GSLB-Implementierung besteht aus dem GSLB der obersten Ebene mit Standortpools mit standortlokalen Load Balancern. Die Standortlastverteiler enthalten Pools der lokalen Speicher-Nodes am Standort. Dies kann eine Kombination aus Load Balancern von Drittanbietern für GSLB-Funktionen und StorageGRID für den lokalen Lastausgleich oder eine Kombination aus Drittanbietern sein. Oder viele der zuvor besprochenen Drittanbieter bieten sowohl GSLB als auch einen standortweiten lokalen Lastausgleich.



TR-4645: Sicherheitsfunktionen

Sichern von StorageGRID-Daten und -Metadaten in einem Objektspeicher

Entdecken Sie die integrierten Sicherheitsfunktionen der StorageGRID Objekt-Storage-Lösung.

Dies ist eine Übersicht über die zahlreichen Sicherheitsfunktionen in NetApp® StorageGRID®, die Datenzugriff, Objekte und Metadaten, Administratorzugriff und Plattformsicherheit abdecken. Es wurde aktualisiert, um die neuesten Funktionen zu enthalten, die mit StorageGRID 12.0 veröffentlicht wurden.

Sicherheit ist ein integraler Bestandteil der NetApp StorageGRID Objekt-Storage-Lösung. Die Sicherheit ist besonders wichtig, da viele Arten von umfangreichen Datenmengen, die gut für Objekt-Storage geeignet sind, ebenfalls sehr sensibel sind und gesetzlichen Vorschriften und Compliance unterliegen. Während sich die Funktionen von StorageGRID weiterentwickeln, stellt die Software viele Sicherheitsfunktionen zur Verfügung, die von unschätzbarem Wert sind, um die Sicherheit eines Unternehmens zu schützen und dem Unternehmen dabei zu helfen, die Best Practices der Branche einzuhalten.

Dieses Dokument bietet einen Überblick über die zahlreichen Sicherheitsfunktionen in StorageGRID 12.0, unterteilt in fünf Kategorien:

- Sicherheitsfunktionen für den Datenzugriff
- Sicherheitsfunktionen für Objekte und Metadaten
- Sicherheitsfunktionen für die Administration

- Plattformsicherheitsfunktionen
- Cloud-Integration

Dieses Dokument ist als Sicherheitsdatenblatt gedacht. Es enthält keine detaillierten Informationen zur Konfiguration des Systems, um die darin aufgeführten Sicherheitsfunktionen zu unterstützen, die nicht standardmäßig konfiguriert sind. Der "Leitfaden zum StorageGRID Hardening" ist auf der offiziellen "StorageGRID-Dokumentation" Seite.

Zusätzlich zu den in diesem Bericht beschriebenen Funktionen folgt StorageGRID den "NetApp Richtlinie zur Reaktion auf und Benachrichtigung bei Produktsicherheitsschwachstellen". Gemeldete Schwachstellen werden überprüft und entsprechend dem Reaktionsprozess für Produktsicherheitsvorfälle reagiert.

NetApp StorageGRID bietet erweiterte Sicherheitsfunktionen für äußerst anspruchsvolle Enterprise-Objekt-Storage-Anwendungsfälle.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID: Bewertung DER Compliance-Anforderungen gemäß SEC 17a-4(f), FINRA 4511(c) und CFTC 1.31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- NetApp StorageGRID NIST FIPS 140-3 Kernel Crypto-Zertifizierung https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- NetApp StorageGRID NIST SP 800-90B Entropie-Zertifizierung https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- NetApp StorageGRID Canadian Centre for Cyber Security Common Criteria Zertifizierung https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- StorageGRID -Dokumentationsseitehttps://docs.netapp.com/us-en/storagegrid/[]
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Begriffe und Akronyme

Dieser Abschnitt enthält Definitionen für die im Dokument verwendete Terminologie.

Begriff oder Akronym	Definition
S3	Simple Storage Service.
Client	Eine Applikation, die eine Schnittstelle zu StorageGRID entweder über das S3-Protokoll für den Datenzugriff oder das HTTP-Protokoll für das Management bietet.
Mandantenadministrator	Der Administrator des StorageGRID-Mandantenkontos
Mandantenbenutzer	Ein Benutzer in einem StorageGRID-Mandantenkonto
TLS	Sicherheit In Transportschicht
ILM	Information Lifecycle Management
LAN	Lokales Netzwerk
Grid-Administrator	Der Administrator des StorageGRID-Systems

Begriff oder Akronym	Definition
Raster	Dem StorageGRID-System
Eimer	Ein Container für in S3 gespeicherte Objekte
LDAP	Lightweight Directory Access Protocol
SEK.	Securities and Exchange Commission; regelt Börsenmitglieder, Makler oder Händler
FINRA	Aufsichtsbehörde für die Finanzindustrie; entspricht den Format- und Medienanforderungen der SEC Rule 17a-4(f)
CFTC	Commodities Futures Trading Commissions; regelt den Handel mit Rohstoffttermingeschäften
NIST	National Institute of Standards and Technology

Sicherheitsfunktionen für den Datenzugriff

Erfahren Sie mehr über die Sicherheitsfunktionen für den Datenzugriff in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Konfigurierbare TLS (Transport Layer Security)	TLS erstellt ein Handshake-Protokoll für die Kommunikation zwischen einem Client und einem StorageGRID-Gateway-Node, Speicher-Node oder Load Balancer-Endpunkt. StorageGRID unterstützt die folgenden Verschlüsselungssuites für TLS: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 TLS v1.2 und 1.3 unterstützt. SSLv3, TLS v1.1 und früher werden nicht unterstützt.	Ein Client und ein StorageGRID können sich gegenseitig identifizieren und authentifizieren und mit Vertraulichkeit und Datenintegrität kommunizieren. Stellt die Verwendung einer aktuellen TLS-Version sicher. Die Chiffren können jetzt unter den Konfigurations-/Sicherheitseinstellungen konfiguriert werden	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Konfigurierbares Serverzertifikat (Load Balancer Endpoint)	Grid-Administratoren können Load-Balancer-Endpunkte konfigurieren, um ein Serverzertifikat zu erstellen oder zu verwenden.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle (CA) signiert wurden, um Objekt-API-Vorgänge zwischen Grid und Client pro Load Balancer-Endpunkt zu authentifizieren.	—
Konfigurierbares Serverzertifikat (API-Endpunkt)	Grid-Administratoren können alle StorageGRID-API-Endpunkte zentral so konfigurieren, dass ein von der vertrauenswürdigen CA ihres Unternehmens signiertes Serverzertifikat verwendet wird.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle signiert wurden, um Objekt-API-Vorgänge zwischen einem Client und dem Grid zu authentifizieren.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Mandantenfähigkeit	StorageGRID unterstützt mehrere Mandanten pro Grid, wobei jeder Mandant einen eigenen Namespace besitzt. Ein Mandant stellt ein S3-Protokoll bereit. Standardmäßig ist der Zugriff auf Buckets/Container und Objekte auf Benutzer in dem Konto beschränkt. Mandanten können einen Benutzer (z. B. eine Unternehmensimplementierung , bei der jeder Benutzer ein eigenes Konto hat) oder mehrere Benutzer (z. B. eine Service-Provider-Implementierung, bei der jedes Konto ein Unternehmen und ein Kunde des Service-Providers ist) aufweisen. Benutzer können lokal oder föderiert sein; föderierte Benutzer werden durch Active Directory oder Lightweight Directory Access Protocol (LDAP) definiert. StorageGRID bietet ein mandantenfähiges Dashboard, in dem sich Benutzer mit ihren lokalen oder föderierten Kontoinformationen anmelden können. Benutzer können auf visualisierte Berichte zur Mandantennutzung anhand des vom Grid-Administrator zugewiesenen Kontingents zugreifen, einschließlich Nutzungsinformationen in Daten und Objekten, die von Buckets gespeichert sind. Benutzer mit Administratorrechten können Systemadministrationsaufgaben auf Mandantenebene durchführen, wie zum Beispiel Benutzer und Gruppen und Zugriffsschlüssel managen.	StorageGRID-Administratoren können Daten von mehreren Mandanten hosten, dabei den Mandantenzugriff isolieren und die Benutzeridentität festlegen, indem Benutzer mit einem externen Identitätsanbieter wie Active Directory oder LDAP verknüpft werden.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Nichtabstreitbarkeit der Zugangsdaten	Jeder S3-Vorgang wird mit einem eindeutigen Mandantenkonto, einem eindeutigen Benutzer und einem Zugriffsschlüssel identifiziert und protokolliert.	Ermöglicht Grid-Administratoren festzulegen, welche API-Aktionen von welchen Personen ausgeführt werden.	—
Anonymer Zugriff deaktiviert	Standardmäßig ist der anonyme Zugriff für S3-Konten deaktiviert. Ein Anforderer muss über gültige Zugangsdaten für einen gültigen Benutzer im Mandantenkonto verfügen, um auf Buckets, Container oder Objekte innerhalb des Kontos zugreifen zu können. Anonymer Zugriff auf S3-Buckets oder -Objekte kann mit einer expliziten IAM-Richtlinie aktiviert werden.	Ermöglicht Grid-Administratoren, den anonymen Zugriff auf Buckets/Container und Objekte zu deaktivieren oder zu steuern.	—
Compliance-WORM	Entwickelt, um die Anforderungen der SEC Rule 17a-4(f) zu erfüllen und von Cohasset validiert. Kunden können Compliance auf Bucket-Ebene aktivieren. Die Aufbewahrung kann erweitert, aber nie reduziert werden. Regeln für Information Lifecycle Management (ILM) setzen minimale Datensicherungsstufen fest.	Mandanten mit gesetzlichen Datenaufbewahrungsanforderungen ermöglichen WORM-Schutz bei gespeicherten Objekten und Objektmetadaten.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
WORM	Grid-Administratoren können den WORM für das gesamte Grid aktivieren, indem sie die Option Client-Änderung deaktivieren aktivieren, die verhindert, dass Clients Objekte oder Objektmetadaten in allen Mandantenkonten überschreiben oder löschen. S3-Mandantenadministratoren können WORM auch nach Mandant, Bucket oder Objektpräfix durch Angabe der IAM-Richtlinie aktivieren, die die benutzerdefinierte S3: PutOverwriteObject-Berechtigung für Objekt- und Metadatenüberschreibungen umfasst.	Grid-Administratoren und Mandantenadministratoren können die WORM-Sicherung von gespeicherten Objekten und Objektmetadaten steuern.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
KMS-Host-Server-Verschlüsselungsschlüsselverwaltung	Grid-Administratoren können einen oder mehrere externe KMS (Key Management Server) im Grid Manager konfigurieren, um Verschlüsselungen für StorageGRID Services und Storage Appliances bereitzustellen. Jeder KMS-Hostserver oder KMS-Hostserver-Cluster verwendet das Key Management Interoperability Protocol (KMIP), um einen Verschlüsselungsschlüssel für die Appliance-Nodes am zugehörigen StorageGRID-Standort bereitzustellen.	Die Verschlüsselung ruhender Daten wird erreicht. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS-Hostserver kommunizieren kann.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Automatisiertes Failover	StorageGRID bietet integrierte Redundanz und automatisiertes Failover. Der Zugriff auf Mandantenkonten, Buckets und Objekte kann auch bei diversen Ausfällen – von Festplatten oder Nodes bis hin zu ganzen Standorten – fortgesetzt werden. StorageGRID erkennt Ressourcen und leitet Anfragen automatisch an verfügbare Nodes und Datenspeicherorte um. StorageGRID Standorte können sogar im Inselmodus betrieben werden. Wenn ein WAN-Ausfall die Verbindung eines Standorts zum restlichen System trennt, können Lese- und Schreibvorgänge mit den lokalen Ressourcen fortgesetzt werden, und die Replizierung wird automatisch wieder aufgenommen, sobald das WAN wiederhergestellt ist.	Ermöglicht Grid-Administratoren, Uptime, SLA und andere vertragliche Verpflichtungen zu erfüllen und Business-Continuity-Pläne zu implementieren.	—
S3-spezifische Datenzugriffssicherheitsfunktionen	AWS Signature Version 2 und Version 4	Das Signieren von API-Anforderungen bietet eine Authentifizierung für S3-API-Vorgänge. Amazon unterstützt zwei Versionen von Signature Version 2 und Version 4. Beim Signaturprozess wird die Identität des Anforderers überprüft, die Daten während der Übertragung geschützt und vor potenziellen Replay-Angriffen geschützt.	Entspricht der AWS-Empfehlung für Signature Version 4 und ermöglicht Abwärtskompatibilität mit älteren Anwendungen mit Signature Version 2.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	S3-Objektsperre	Die S3-Objektsperrfunktion in StorageGRID ist eine Objektschutzlösung, die S3-Objektsperrung in Amazon S3 entspricht.	Ermöglicht Mandanten, Buckets mit aktivierter S3 Object Lock zu erstellen, um Vorschriften zu erfüllen, für die bestimmte Objekte für einen festgelegten Zeitraum oder auf unbestimmte Zeit aufbewahrt werden müssen.
SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)	Sichere Speicherung der S3 Zugangsdaten	S3-Zugriffsschlüssel werden in einem Format gespeichert, das durch eine Passwort-Hashing-Funktion (SHA-2) geschützt ist.	Ermöglicht die sichere Speicherung von Zugriffsschlüsseln durch eine Kombination aus Schlüssellänge (10^{31} zufällig generierte Nummer) und einem Passwort-Hashing-Algorithmus.
—	Zeitgebundene S3-Zugriffsschlüssel	Beim Erstellen eines S3 Zugriffsschlüssels für einen Benutzer können Kunden ein Ablaufdatum und eine Uhrzeit für den Zugriffsschlüssel festlegen.	Bietet Grid-Administratoren die Möglichkeit, temporäre S3-Zugriffsschlüssel bereitzustellen.
—	Mehrere Zugriffsschlüssel pro Benutzerkonto	Mit StorageGRID können mehrere Zugriffsschlüssel erstellt und gleichzeitig für ein Benutzerkonto aktiv werden. Da jede API-Aktion mit einem Mandanten-Benutzerkonto und einem Zugriffsschlüssel protokolliert wird, bleibt die Nichtabstreitbarkeit erhalten, obwohl mehrere Schlüssel aktiv sind.	Ermöglicht Clients das unterbrechungsfreie Drehen von Zugriffsschlüsseln und ermöglicht jedem Client einen eigenen Schlüssel, wodurch die gemeinsame Nutzung von Schlüsseln über Clients hinweg vermieden wird.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	S3 IAM-Zugriffsrichtlinie	StorageGRID unterstützt S3 IAM-Richtlinien, sodass Grid-Administratoren granulare Zugriffssteuerung nach Mandanten, Bucket oder Objektpräfix angeben können. StorageGRID unterstützt außerdem IAM-Richtlinienbedingungen und -Variablen, wodurch dynamischere Zugriffssteuerungsrichtlinien ermöglicht werden.	Ermöglicht Grid-Administratoren, die Zugriffssteuerung nach Benutzergruppen für den gesamten Mandanten festzulegen; ermöglicht es den Mandantenbenutzern auch, die Zugriffssteuerung für ihre eigenen Buckets und Objekte festzulegen.
—	S3 Security Token Service API AssumeRole	StorageGRID unterstützt die S3 STS API AssumeRole, um temporäre Sicherheitsanmeldeinformationen (Zugriffsschlüssel-ID, geheimer Zugriffsschlüssel, Sitzungstoken) mit eingeschränkten Berechtigungen und begrenzter Dauer bereitzustellen. Inline-Sitzungsrichtlinien zur weiteren Einschränkung von Berechtigungen während der Sitzung werden als Teil der AssumeRole-API unterstützt.	Ermöglicht Mandantenadministratoren, sicheren temporären Zugriff auf Objektdaten bereitzustellen.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	Einfacher Benachrichtigungsdienst	StorageGRID unterstützt das Senden von Benachrichtigungen beim Objektzugriff. Die folgenden Ereignistypen werden unterstützt: • s3:Objekt erstellt: • s3:ObjektErstellt:Put • s3:ObjektErstellt:Post • s3:ObjektErstellt:Kopie • s3:Objekterstellt:MehrteiligerUpload abgeschlossen • s3:Objekt entfernt: • s3:Objekt entfernt:Löschen • s3:Objekt entfernt:DeleteMarker erstellt • s3:ObjectRestore:Post	Ermöglicht Mandantenadministratoren die Überwachung des Zugriffs auf Objekte
—	Serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln (SSE)	StorageGRID unterstützt SSE und ermöglicht mandantenfähigen Schutz von Daten im Ruhezustand mit von StorageGRID gemanagten Verschlüsselungen.	Ermöglicht Mandanten die Verschlüsselung von Objekten. Zum Schreiben und Abrufen dieser Objekte ist ein Verschlüsselungsschlüssel erforderlich.
SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)	Serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)	StorageGRID unterstützt SSE-C und ermöglicht damit mandantenfähigen Schutz von Daten im Ruhezustand mit vom Client gemanagten Verschlüsselungsschlüsseln. Obwohl StorageGRID alle Objektverschlüsselung und -Entschlüsselung managt, muss der Client bei SSE-C die Schlüssel selbst managen.	Ermöglicht Clients die Verschlüsselung von Objekten mit den Schlüsseln, die sie steuern. Zum Schreiben und Abrufen dieser Objekte ist ein Verschlüsselungsschlüssel erforderlich.

Sicherheit von Objekten und Metadaten

Entdecken Sie die Sicherheitsfunktionen für Objekte und Metadaten in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Advanced Encryption Standard (AES) Server-seitige Objektverschlüsselung	StorageGRID bietet serverseitige Objektverschlüsselung nach AES 128 und AES 256. Grid-Administratoren können die Verschlüsselung als globale Standardeinstellung aktivieren. StorageGRID unterstützt außerdem den S3 x-amz-Server-seitigen Verschlüsselungsheader, um die Verschlüsselung für einzelne Objekte zu aktivieren oder zu deaktivieren. Wenn diese Option aktiviert ist, werden die Objekte bei der Speicherung bzw. Übertragung zwischen den Grid-Nodes verschlüsselt.	Unterstützt die sichere Speicherung und Übertragung von Objekten, unabhängig von der zugrunde liegenden Storage-Hardware.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Integriertes Verschlüsselungsmanagement	Bei aktivierter Verschlüsselung wird jedes Objekt mit einem zufällig generierten eindeutigen symmetrischen Schlüssel verschlüsselt, der ohne externen Zugriff in StorageGRID gespeichert wird.	Ermöglicht die Verschlüsselung von Objekten ohne externes Verschlüsselungsmanagement	
FIPS 140-2-2-konforme Verschlüsselungsfestplatten (Federal Information Processing Standard	Die StorageGRID Appliances SG5812, SG5860, SG6160 und SGF6024 bieten die Möglichkeit, FIPS 140-2-2-konforme Verschlüsselungsfestplatten anzubieten. Die Schlüssel für die Festplatten können optional von einem externen KMIP-Server gemanagt werden.	Ermöglicht sichere Speicherung von Systemdaten, Metadaten und Objekten StorageGRID bietet außerdem softwarebasierte Objektverschlüsselung, die die Storage und die Übertragung von Objekten sichert.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Federal Information Processing Standard (FIPS) 140-3-konforme Verschlüsselung für Knoten	Die StorageGRID -Geräte SG5812, SG5860, SG6160, SGF6112, SG1100 und SG110 bieten die Option einer FIPS 140-3-konformen Knotenverschlüsselung. Die Verschlüsselungsschlüssel für die Knoten werden von einem externen KMIP-Server verwaltet.	Ermöglicht sichere Speicherung von Systemdaten, Metadaten und Objekten StorageGRID bietet außerdem softwarebasierte Objektverschlüsselung, die die Storage und die Übertragung von Objekten sichert.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Hintergrundintegrität sprüfung und Selbstheilung	StorageGRID nutzt einen Verriegelungsmechanismus aus Hashes, Prüfsummen und zyklischen Redundanzprüfungen (Cyclic Redundancy Checks, CRCs) auf Objekt- und Unterobjektebene, um sich sowohl im Storage- als auch auf der Übertragungsstrecke vor Dateninkonsistenz, Manipulation oder Änderung zu schützen. StorageGRID erkennt beschädigte und manipulierte Objekte automatisch und ersetzt sie. Gleichzeitig werden die geänderten Daten in Quarantäne verschoben und der Administrator benachrichtigt.	Grid-Administratoren können SLAs, Vorschriften und andere Verpflichtungen hinsichtlich der Datenaufbewahrung erfüllen. Unterstützt Kunden dabei, Ransomware oder Viren zu erkennen, die versuchen, Daten zu verschlüsseln, zu manipulieren oder zu ändern.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Richtlinienbasierte Objektplatzierung und -Aufbewahrung	Mit StorageGRID können Grid-Administratoren ILM-Regeln konfigurieren, die die Objektaufbewahrung, -Platzierung, -Sicherung, -Übertragung und -Verfallsdaten festlegen. Grid-Administratoren können StorageGRID konfigurieren, um Objekte nach Metadaten zu filtern und Regeln auf verschiedenen Granularitätsebenen anzuwenden, einschließlich Grid-weiter, Mandant, Bucket, Schlüsselpräfix, und benutzerdefinierte Metadaten-Schlüssel-Wert-Paare. StorageGRID hilft sicherzustellen, dass Objekte während ihrer gesamten Lebenszyklen gemäß den ILM-Regeln gespeichert werden, es sei denn, sie werden vom Client ausdrücklich gelöscht.	Hilft bei der Durchsetzung von Datenablage, Datensicherheit und Datenhaltung. Unterstützt Kunden bei der Einhaltung von SLAs für Langlebigkeit, Verfügbarkeit und Performance.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Metadaten werden im Hintergrund gescannt	StorageGRID scannt regelmäßig Objektmetadaten im Hintergrund, um Änderungen an der Platzierung oder Sicherung von Objektdaten gemäß ILM anzuwenden.	Hilft bei der Erkennung beschädigter Objekte.	
Abstimmbare Konsistenz	Mandanten können Konsistenzstufen auf Bucket-Ebene auswählen, um sicherzustellen, dass Ressourcen wie standortübergreifende Konnektivität verfügbar sind.	Bietet die Möglichkeit, Schreibvorgänge nur dann in das Grid zu übertragen, wenn eine erforderliche Anzahl von Standorten oder Ressourcen verfügbar ist.	

Sicherheitsfunktionen für die Administration

Entdecken Sie die Sicherheitsfunktionen für die Administration in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Serverzertifikat (Grid-Managementoberfläche)	Grid-Administratoren können die Grid-Managementoberfläche so konfigurieren, dass ein von der vertrauenswürdigen CA ihres Unternehmens signiertes Serverzertifikat verwendet wird.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle signiert sind, um die Management-UI und den API-Zugriff zwischen einem Management-Client und dem Grid zu authentifizieren.	—
Administrative Benutzerauthentifizierung	Administratorbenutzer werden mit Benutzername und Passwort authentifiziert. Administrative Benutzer und Gruppen können lokal oder föderiert sein und aus dem Active Directory oder LDAP des Kunden importiert werden. Lokale Kontokennwörter werden in einem durch bcrypt geschützten Format gespeichert; Kommandozeilen-Passwörter werden in einem durch SHA-2 geschützten Format gespeichert.	Authentifiziert den administrativen Zugriff auf die Management-UI und -APIs.	—
SAML Support	StorageGRID unterstützt Single Sign-On (SSO) unter Verwendung des SAML 2.0-Standards (Security Assertion Markup Language 2.0). Wenn SSO aktiviert ist, müssen alle Benutzer von einem externen Identitäts-Provider authentifiziert werden, bevor sie auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.	Zusätzliche Sicherheitsstufen für Grid- und Mandantenadministratoren wie SSO und Multi-Faktor-Authentifizierung (MFA)	NIST SP800-63

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Granulare Berechtigungskontrolle	Grid-Administratoren können Rollen Berechtigungen zuweisen und administrativen Benutzergruppen Rollen zuweisen. Dadurch werden die Aufgaben erzwungen, die administrative Clients sowohl über die Management-UI als auch über APIs ausführen dürfen.	Ermöglicht Grid-Administratoren das Management der Zugriffssteuerung für Admin-Benutzer und -Gruppen.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Verteilte Audit-Protokollierung	StorageGRID bietet eine integrierte, verteilte Audit-Protokollierungs-Infrastruktur, die auf Hunderte Nodes an bis zu 16 Standorten skalierbar ist. Die StorageGRID-Software-Knoten erzeugen Audit-Meldungen, die über ein redundantes Audit-Relay-System übertragen und schließlich in einem oder mehreren Audit-Log-Repositorys erfasst werden. Audit-Meldungen erfassen Ereignisse auf Objektebene, z. B. Client-initiierte S3-API-Operationen, Objekt-Lebenszyklus-Ereignisse durch ILM, Zustandsprüfungen von Objekten im Hintergrund sowie Konfigurationsänderungen, die über die Management-UI oder -APIs vorgenommen werden. Prüfprotokolle können per Syslog exportiert werden, sodass Prüfmeldungen von Tools wie Splunk und ELK ausgewertet werden können. Es gibt vier Arten von Prüfmeldungen: • Systemaudits Meldungen • Audit-Meldungen zu Objekt-Storage • HTTP-Protokollauditmeldungen • Meldungen von Management-Audits Prüfprotokolle können zur langfristigen Aufbewahrung und für den Anwendungszugriff in einem S3-Bucket gespeichert werden.	Bietet Grid-Administratoren einen bewährten und skalierbaren Audit-Service und ermöglicht es ihnen, Audit-Daten für verschiedene Ziele zu extrahieren. Zu diesen Zielen gehören Fehlerbehebung, Revision der SLA-Performance, Client-Datenzugriffs-API-Operationen und Änderungen der Managementkonfiguration.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Systemprüfung	Systemauditmeldungen erfassen systembezogene Ereignisse, wie Grid-Node-Status, Erkennung beschädigter Objekte, Objekte, die per ILM-Regel an allen angegebenen Standorten festgelegt wurden, und den Fortschritt systemweiter Wartungsaufgaben (Grid-Aufgaben).	Unterstützt Kunden bei der Behebung von Systemproblemen und liefert den Nachweis, dass Objekte gemäß SLA gespeichert werden. SLAs werden durch StorageGRID ILM-Regeln implementiert und sind integritätsgeschützt.	—
Objekt-Storage-Prüfung	Objekt-Storage-Audit-Nachrichten erfassen Objekt-API-Transaktionen und Lifecycle-bezogene Ereignisse. Zu diesen Ereignissen gehören Objekt-Storage und -Abruf, Grid-Node zu Grid-Node-Transfers und Überprüfungen.	Unterstützt Kunden bei der Prüfung des Fortschritts der Daten über das System und bei der Bereitstellung von SLAs mit dem Namen StorageGRID ILM.	—
HTTP-Protokollaudit	HTTP-Protokollauditmeldungen erfassen HTTP-Protokollinteraktionen im Zusammenhang mit Client-Anwendungen und StorageGRID-Knoten. Darüber hinaus können Kunden bestimmte HTTP-Anforderungsheader (z. B. X-Forwarded-for und Benutzer-Metadaten [x-amz-meta-*]) in einem Audit erfassen.	Unterstützt Kunden beim Prüfen von API-Operationen für den Datenzugriff zwischen Clients und StorageGRID und bei der Nachverfolgung einer Aktion auf ein einzelnes Benutzerkonto und einen Zugriffsschlüssel. Kunden können zudem Benutzermetadaten bei einem Audit protokollieren und mithilfe von Tools für das Mining wie Splunk oder ELK nach Objekt-Metadaten suchen.	—
Management-Prüfung	Management Audit-Nachrichten protokollieren Benutzeranforderungen von Administratoren an die Management-UI (Grid Management Interface) oder APIs. Jede Anfrage, die keine GET- oder HEAD-Anforderung an die API ist, protokolliert eine Antwort mit dem Benutzernamen, der IP und der Art der Anfrage an die API.	Hilft Grid-Administratoren, eine Aufzeichnung der Änderungen an der Systemkonfiguration zu erstellen, die von welchem Benutzer von welcher Quell-IP und welcher Ziel-IP zu welchem Zeitpunkt vorgenommen wurden.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
TLS 1.3-Unterstützung für Management UI- und API-Zugriff	TLS erstellt ein Handshake-Protokoll für die Kommunikation zwischen einem Admin-Client und einem StorageGRID-Admin-Node.	Ein administrativer Client und ein StorageGRID können sich gegenseitig identifizieren und authentifizieren und kommunizieren mit Vertraulichkeit und Datenintegrität.	—
SNMPv3 für StorageGRID-Überwachung	SNMPv3 bietet Sicherheit durch eine starke Authentifizierung und Datenverschlüsselung zum Schutz der Privatsphäre. Mit v3 werden die Protokolldateneinheiten verschlüsselt, wobei CBC-DES für das Verschlüsselungsprotokoll verwendet wird. Die Benutzerauthentifizierung, wer die Protokolldateneinheit gesendet hat, wird entweder über das HMAC-SHA- oder das HMAC-MD5-Authentifizierungsprotokoll bereitgestellt. SNMPv2 und v1 werden weiterhin unterstützt.	Unterstützt Grid-Administratoren bei der Überwachung des StorageGRID-Systems durch Aktivieren eines SNMP-Agenten auf dem Admin-Knoten.	—
Client-Zertifikate für Prometheus Kennzahlenexport	Grid-Administratoren können Client-Zertifikate hochladen oder generieren, die für einen sicheren, authentifizierten Zugriff auf die StorageGRID Prometheus-Datenbank verwendet werden können.	Grid-Administratoren können StorageGRID mithilfe von Client-Zertifikaten extern mit Applikationen wie Grafana überwachen.	—

Plattformsicherheitsfunktionen

Erfahren Sie mehr über die Plattformsicherheitsfunktionen in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Interne Public-Key-Infrastruktur (PKI), Node-Zertifikate und TLS	StorageGRID verwendet interne PKI- und Node-Zertifikate zur Authentifizierung und Verschlüsselung der Kommunikation zwischen den Knoten. Die Kommunikation zwischen den Knoten ist durch TLS gesichert.	Unterstützt den sicheren Systemdatenverkehr über LAN oder WAN, insbesondere bei standortübergreifenden Bereitstellungen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Knoten-Firewall	StorageGRID konfiguriert automatisch IP-Tabellen und Firewallregeln zur Steuerung von eingehendem und ausgehendem Netzwerk-Traffic sowie zum Schließen nicht verwendeter Ports.	Der Schutz von StorageGRID-Systemen, Daten und Metadaten vor unaufgefordertem Netzwerkverkehr	—
OS-Sicherung	Das Basis-Betriebssystem der physischen Appliances und virtuellen Nodes von StorageGRID ist gehärtet; zugehörige Softwarepakete werden entfernt.	Minimiert mögliche Angriffsflächen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Regelmäßige Plattform- und Software-Updates	StorageGRID veröffentlicht regelmäßige Software-Versionen, die das Betriebssystem, Binärdateien von Applikationen und Software Updates enthalten.	Hilft dabei, das StorageGRID System mit aktueller Software und Binärdateien zu aktualisieren.	—
Root-Anmeldung über Secure Shell (SSH) deaktiviert	Die Root-Anmeldung über SSH ist auf allen StorageGRID Nodes deaktiviert. SSH-Zugriff verwendet Zertifikatauthentifizierung.	Hilft Kunden, sich vor einem möglichen Remote-Passwort-Cracking der Root-Anmeldung zu schützen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Automatisierte Zeitsynchronisierung	StorageGRID synchronisiert Systemuhren jedes Node automatisch mit mehreren externen NTP-Servern (Time Network Time Protocol). Mindestens vier NTP-Server von Stratum 3 oder höher sind erforderlich.	Stellt die gleiche Zeitreferenz für alle Knoten sicher.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Getrennte Netzwerke für Client-, Admin- und internen Grid-Traffic	StorageGRID Software Nodes und Hardware Appliances unterstützen mehrere virtuelle und physische Netzwerkschnittstellen, sodass die Kunden den Client-, Administrations- und internen Grid-Traffic über verschiedene Netzwerke trennen können.	Grid-Administratoren können internen und externen Netzwerkverkehr trennen und Datenverkehr über Netzwerke mit unterschiedlichen SLAs bereitstellen.	—
Mehrere virtuelle LAN-Schnittstellen (VLAN)	StorageGRID unterstützt die Konfiguration von VLAN-Schnittstellen auf Ihren StorageGRID-Client- und Grid-Netzwerken.	Grid-Administratoren können den Datenverkehr von Applikationen partitionieren und isolieren, um so Sicherheit, Flexibilität und Performance zu gewährleisten.	
Nicht Vertrauenswürdiges Client-Netzwerk	Die nicht vertrauenswürdige Client-Netzwerkschnittstelle akzeptiert eingehende Verbindungen nur an Ports, die explizit als Load-Balancer-Endpunkte konfiguriert wurden.	Stellt sicher, dass Schnittstellen geschützt sind, die nicht vertrauenswürdigen Netzwerken zugänglich sind.	—
Konfigurierbare Firewall	Verwaltung offener und geschlossener Ports für Admin-, Grid- und Client-Netzwerke.	Ermöglichen Sie Grid-Administratoren, den Zugriff auf Ports zu steuern und den genehmigten Gerätezugriff auf die Ports zu verwalten.	
Erweitertes SSH-Verhalten	Deaktivieren Sie SSH standardmäßig vor der Installation. Im Standardzustand ist der SSH-Zugriff nur auf die Adresse der Link-Local-Verwaltungsports aktiviert. Die Passwörter für die Benutzer „Admin“ und „Root“ sind auf die Seriennummer des Compute Controllers des Geräts eingestellt. Die Anmeldung ist nur auf der seriellen Konsole und der grafischen Konsole (BMC KVM) zulässig. SSH ist auf allen Netzwerkports deaktiviert.	Verbessert den Netzwerkzugriffsschutz.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Node-Verschlüsselung	Als Teil der neuen KMS-Host-Server-Verschlüsselungsfunktion wird dem StorageGRID-Appliance-Installationsprogramm eine neue Einstellung für die Knotenverschlüsselung hinzugefügt.	Diese Einstellung muss während der Hardwarekonfigurationsphase der Appliance-Installation aktiviert werden.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Cloud-Integration

Integration von StorageGRID in Cloud-Services

Funktion	Funktion	Auswirkungen
Benachrichtigungs-basierte Virus-Scan	Die StorageGRID Plattform-Services unterstützen Ereignisbenachrichtigungen. Ereignisbenachrichtigungen können mit externen Cloud Computing Services verwendet werden, um Workflows zur Virenprüfung der Daten zu starten.	Mandantenadministratoren können einen Virus-Scan von Daten mithilfe von externen Cloud-Computing-Services auslösen.

TR-4921: Ransomware-Verteidigung

StorageGRID S3 Objekte vor Ransomware schützen

Informieren Sie sich über Ransomware-Angriffe und den Schutz von Daten mit StorageGRID Sicherheits-Best Practices.

Ransomware-Angriffe sind auf dem Vormarsch. Dieses Dokument enthält einige Empfehlungen zum Schutz Ihrer Objektdaten auf StorageGRID.

Ransomware heute ist die allgegenwärtige Gefahr im Datacenter. Ransomware wurde entwickelt, um Daten zu verschlüsseln und sie für Benutzer und Applikationen, die darauf angewiesen sind, nicht nutzbar zu machen. Der Schutz beginnt mit den üblichen Schutzmaßnahmen für gehärtete Netzwerke und solide Benutzersicherheitspraktiken, und wir müssen die Sicherheitsverfahren für den Datenzugriff befolgen.

Ransomware ist eine der größten Sicherheitsbedrohungen von heute. Das NetApp StorageGRID Team arbeitet mit unseren Kunden zusammen, um diesen Bedrohungen einen Schritt voraus zu sein. Mit der Verwendung von Objektsperre und Versionierung können Sie sich vor unerwünschten Änderungen schützen und sich vor böswilligen Angriffen erholen. Datensicherheit ist ein Multi-Layer-Unternehmen, dessen Objekt-Storage nur ein Teil in Ihrem Datacenter ist.

Best Practices von StorageGRID

Für StorageGRID sollten Sicherheits-Best-Practices die Verwendung von HTTPS mit signierten Zertifikaten für Management und Objektzugriff umfassen. Erstellen Sie dedizierte Benutzerkonten für Anwendungen und Personen und verwenden Sie die Mandanten-Root-Konten nicht für den Zugriff auf Anwendungen oder Benutzerdaten. Mit anderen Worten, folgen Sie dem Prinzip der geringsten Privilegien. Verwenden Sie Sicherheitsgruppen mit definierten IAM-Richtlinien (Identity and Access Management) zur Steuerung von Benutzerrechten und Zugriffskonten für spezifische Anwendungen und Benutzer. Mit diesen Maßnahmen müssen Sie dennoch sicherstellen, dass Ihre Daten geschützt sind. Bei Simple Storage Service (S3) wird bei Änderungen von Objekten zur Verschlüsselung das ursprüngliche Objekt überschrieben.

Verteidigungsmethoden

Der primäre Mechanismus zum Schutz vor Ransomware in der S3-API ist die Implementierung von Objektsperrung. Nicht alle Anwendungen sind mit Objektsperre kompatibel, daher gibt es zwei weitere Optionen zum Schutz Ihrer Objekte, die in diesem Bericht beschrieben werden: Replikation in einen anderen Bucket mit aktivierter Versionierung und Versionierung mit IAM-Richtlinien.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

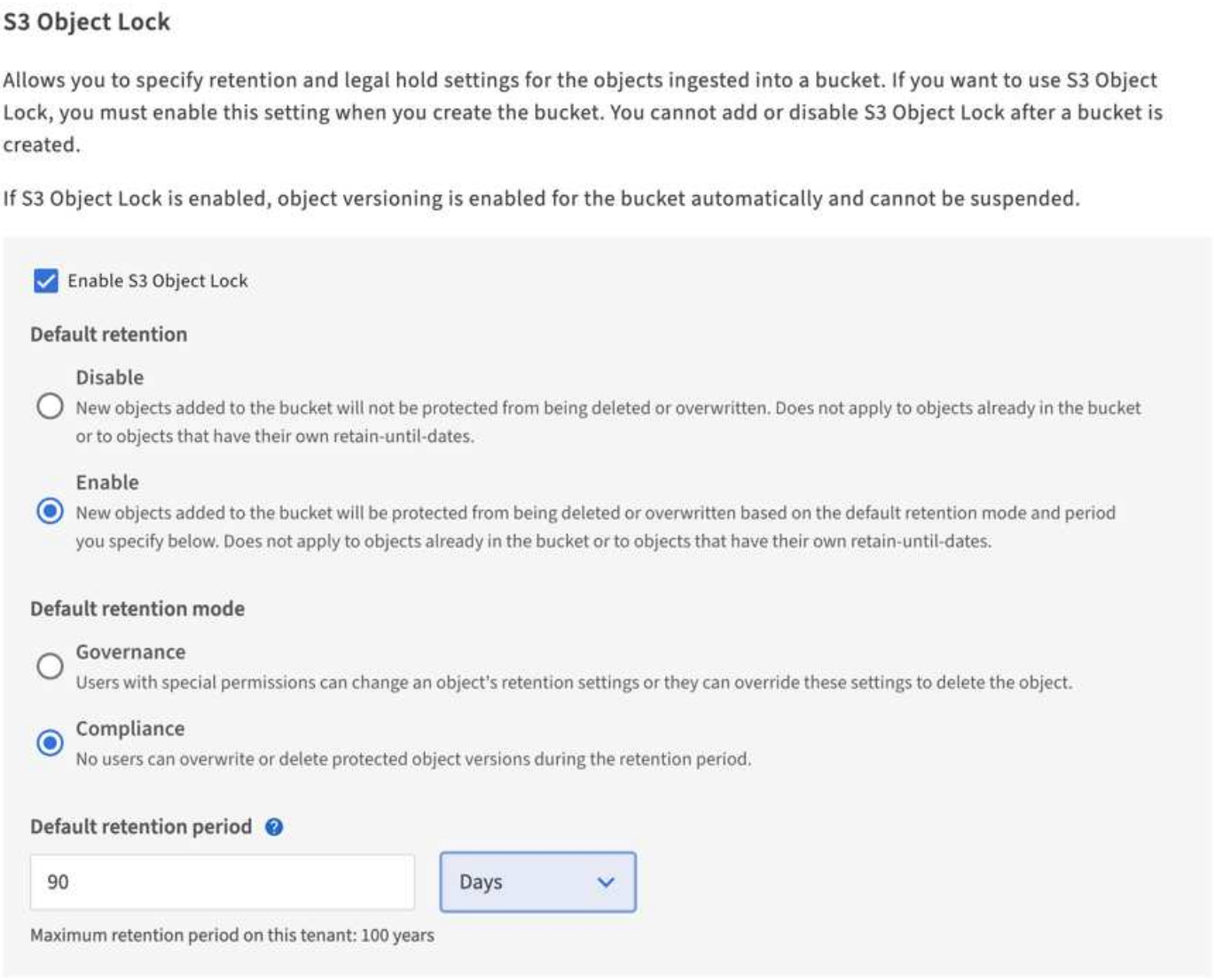
- NetApp StorageGRID Dokumentationscenterhttps://docs.netapp.com/us-en/storagegrid/[]
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Ransomware-Verteidigung mit Objektsperre

Entdecken Sie, wie die Objektsperre in StorageGRID ein WORM-Modell bietet, das das Löschen oder Überschreiben von Daten verhindert, und wie es die gesetzlichen Vorgaben erfüllt.

Die Objektsperrung verfügt über ein WORM-Modell, mit dem verhindert wird, dass Objekte gelöscht oder überschrieben werden. Die StorageGRID-Implementierung von Objektsperrung "Cohasset bewertet" unterstützt die Einhaltung gesetzlicher Vorgaben; sie unterstützt die gesetzliche Aufbewahrungspflichten, den Compliance-Modus und den Governance-Modus für die Objektaufbewahrung sowie die standardmäßigen Bucket-Aufbewahrungsrichtlinien. Sie müssen die Objektsperre als Teil der Bucket-Erstellung und -Versionierung aktivieren. Eine bestimmte Version eines Objekts ist gesperrt, und wenn keine Versions-ID definiert ist, wird die Aufbewahrung auf die aktuelle Version des Objekts platziert. Wenn für die aktuelle Version die Aufbewahrung konfiguriert ist und versucht wird, das Objekt zu löschen, zu ändern oder zu überschreiben, wird eine neue Version mit einer Löschmarkierung oder der neuen Revision des Objekts als aktuelle Version erstellt. und die gesperrte Version wird als nicht aktuelle Version beibehalten. Für Applikationen, die noch nicht kompatibel sind, können Sie möglicherweise noch Objektsperre und eine Standardkonfiguration für die Aufbewahrung auf dem Bucket nutzen. Nach der Definition der Konfiguration wird dabei eine Objektaufbewahrung auf jedes neue Objekt angewendet, das in den Bucket aufgenommen wird. Dies funktioniert, solange die Anwendung so konfiguriert ist, dass die Objekte nicht vor Ablauf der Aufbewahrungszeit gelöscht oder überschrieben werden.

Wenn Sie in der Benutzeroberfläche der Mandantenverwaltung einen Bucket erstellen, können Sie die Objektsperre aktivieren und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer konfigurieren. Wenn dies konfiguriert ist, wird für jedes Objekt, das in diesen Bucket aufgenommen wird, eine Mindestaufbewahrungsdauer für die Objektsperre festgelegt.



Hier sind einige Beispiele für die Verwendung der Objektsperre API:

Objektsperre Legal Hold ist ein einfacher ein/aus-Status, der auf ein Objekt angewendet wird.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

Wenn Sie den Legal Hold-Status festlegen, wird bei Erfolg kein Wert zurückgegeben, sodass er mit einer GET-Operation überprüft werden kann.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

Um die Legal Hold-Taste zu deaktivieren, wenden Sie den AUS-Status an.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Die Objektaufbewahrung wird mit einem Zeitstempel bis beibehalten.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

Auch hier gibt es keinen zurückgegebenen Wert auf Erfolg, so dass Sie den Status der Aufbewahrung ähnlich mit einem get Call überprüfen können.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

Wenn für einen Bucket mit aktivierter Objektsperre eine Standardaufbewahrung eingerichtet wird, wird eine Aufbewahrungsfrist in Tagen und Jahren verwendet.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

Wie bei den meisten dieser Operationen wird bei Erfolg keine Antwort zurückgegeben. Daher können wir ein GET durchführen, damit die Konfiguration überprüft werden kann.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

Als Nächstes können Sie ein Objekt mit der angewandten Aufbewahrungskonfiguration in den Bucket legen.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

Der PUT-Vorgang gibt eine Antwort zurück.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

Für das Aufbewahrungs-Objekt wird die Aufbewahrungsdauer, die im vorhergehenden Beispiel auf dem Bucket festgelegt wurde, in einen Aufbewahrungszeitstempel für das Objekt konvertiert.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Ransomware-Verteidigung durch replizierten Bucket mit Versionierung

Erfahren Sie, wie Sie Objekte mit StorageGRID CloudMirror in einen sekundären Bucket replizieren.

Nicht alle Applikationen und Workloads werden mit Objektsperre kompatibel sein. Eine weitere Option besteht darin, die Objekte auf einen sekundären Bucket zu replizieren, entweder im selben Grid (vorzugsweise ein anderer Mandant mit eingeschränktem Zugriff) oder auf einen anderen S3-Endpunkt mit dem StorageGRID-Plattformservice CloudMirror.

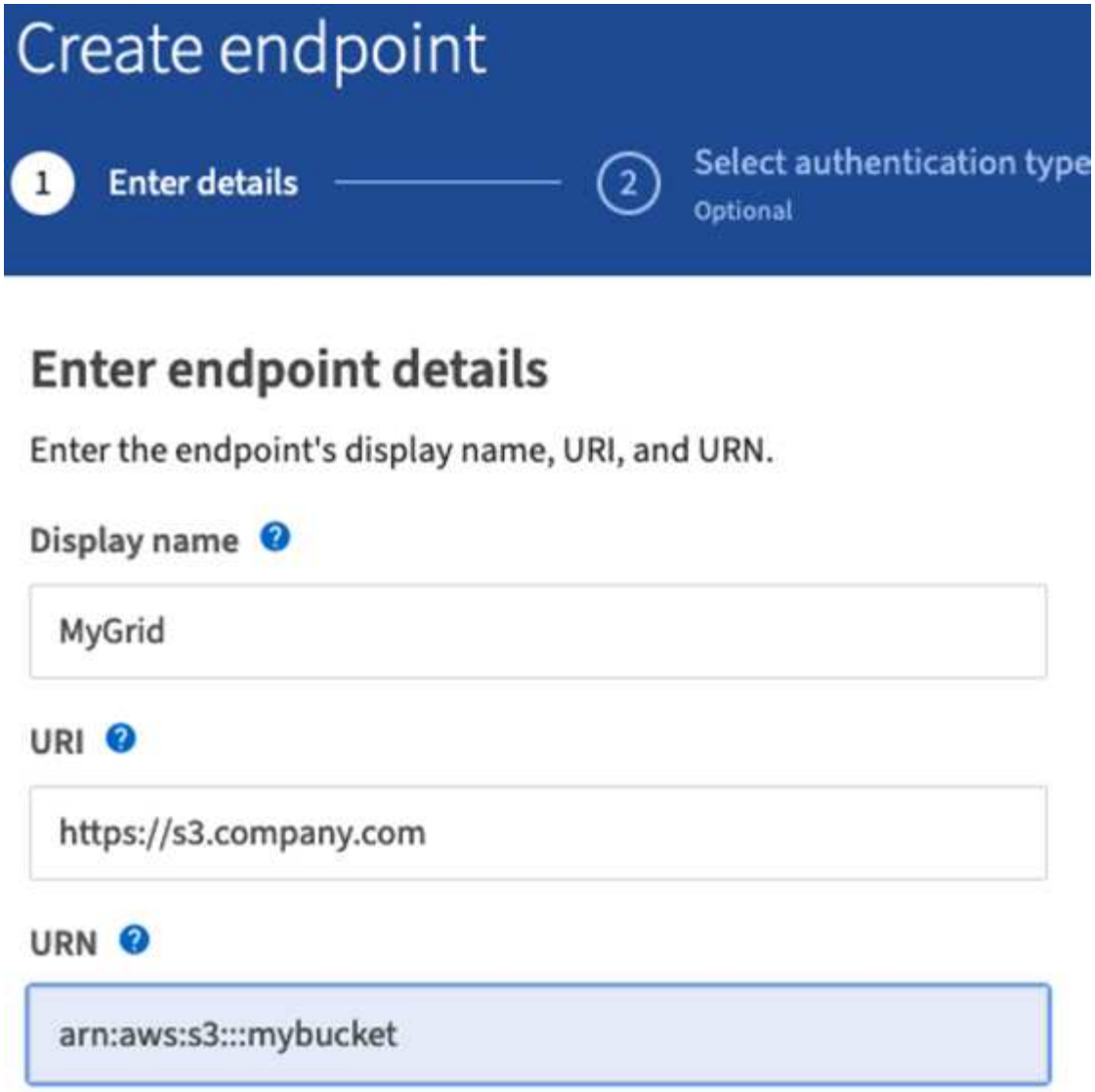
StorageGRID CloudMirror ist eine Komponente von StorageGRID, die so konfiguriert werden kann, dass Objekte eines Buckets auf ein definiertes Ziel repliziert werden, da sie in den Quell-Bucket aufgenommen werden und Löschungen nicht repliziert werden. Da CloudMirror eine integrierte Komponente von StorageGRID ist, kann sie nicht durch einen S3-API-basierten Angriff deaktiviert oder manipuliert werden. Sie können diesen replizierten Bucket mit aktivierter Versionierung konfigurieren. In diesem Szenario benötigen Sie eine automatisierte Bereinigung der alten Versionen des replizierten Buckets, die sicher zu verwerfen sind. Dazu können Sie die StorageGRID ILM-Richtlinien-Engine verwenden. Erstellen Sie Regeln, um die Objektplatzierung auf Basis der nicht aktuellen Zeit für mehrere Tage zu verwalten, die ausreichend sind, um einen Angriff identifiziert und wiederhergestellt zu haben.

Ein Nachteil dieses Ansatzes besteht darin, dass mehr Storage verbraucht wird. Dazu ist eine vollständige zweite Kopie des Buckets und mehrere Versionen der Objekte verfügbar, die einige Zeit aufbewahrt werden. Darüber hinaus müssen die Objekte, die absichtlich aus dem primären Bucket gelöscht wurden, manuell aus dem replizierten Bucket entfernt werden. Außerhalb des Produkts gibt es weitere Replizierungsoptionen, wie z. B. NetApp CloudSync, mit denen Löschvorgänge für eine ähnliche Lösung repliziert werden können. Ein weiterer Nachteil für den sekundären Bucket, bei dem die Versionierung aktiviert und nicht die Objektsperre aktiviert ist, besteht darin, dass eine Reihe privilegierter Konten vorhanden ist, die verwendet werden könnten, um Schäden am sekundären Standort zu verursachen. Der Vorteil ist, dass es sich um ein eindeutiges Konto für diesen Endpunkt oder Mandanten-Bucket handeln sollte, und der Kompromiss wahrscheinlich keinen Zugriff auf Konten am primären Standort oder umgekehrt umfasst.

Nachdem die Quell- und Ziel-Buckets erstellt und das Ziel mit Versionierung konfiguriert wurde, können Sie die Replikation wie folgt konfigurieren und aktivieren:

Schritte

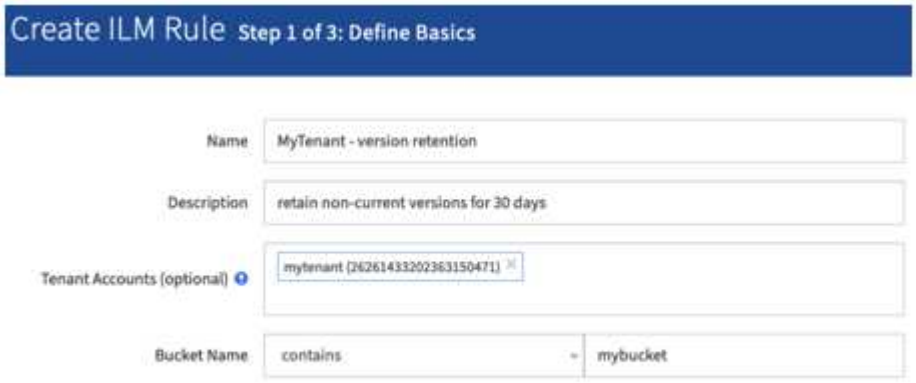
1. Erstellen Sie zum Konfigurieren von CloudMirror einen Plattformservices-Endpunkt für das S3-Ziel.

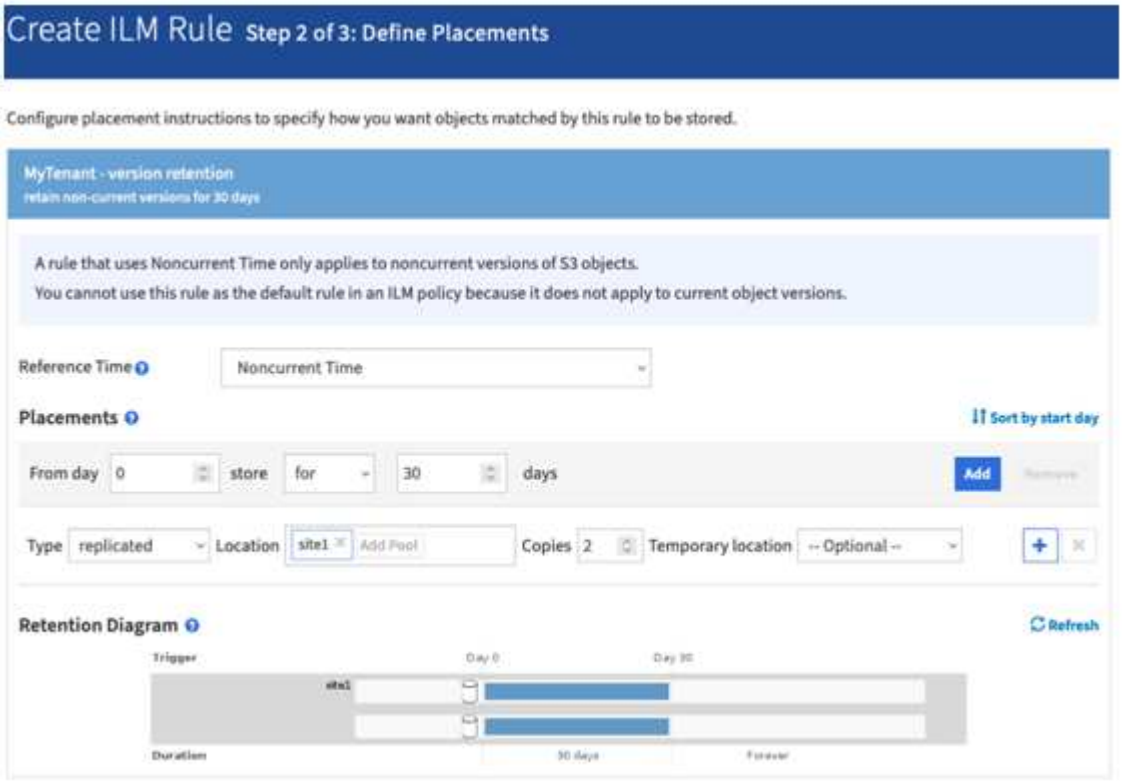


2. Konfigurieren Sie auf dem Quell-Bucket die Replikation zur Verwendung des konfigurierten Endpunkts.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. Erstellen Sie ILM-Regeln, um die Storage-Platzierung und das Versionsspeicherzeitmanagement zu managen. In diesem Beispiel werden die nicht aktuellen Versionen der zu speichernden Objekte konfiguriert.





An Standort 1 sind 30 Tage lang zwei Kopien vorhanden. Sie konfigurieren außerdem die Regeln für die aktuelle Version der Objekte basierend auf der Verwendung der Aufnahmezeit als Referenzzeit in der ILM-Regel, um der Speicherdauer des Quell-Buckets anzupassen. Die Storage-Platzierung für die Objektversionen kann Erasure Coded oder repliziert werden.

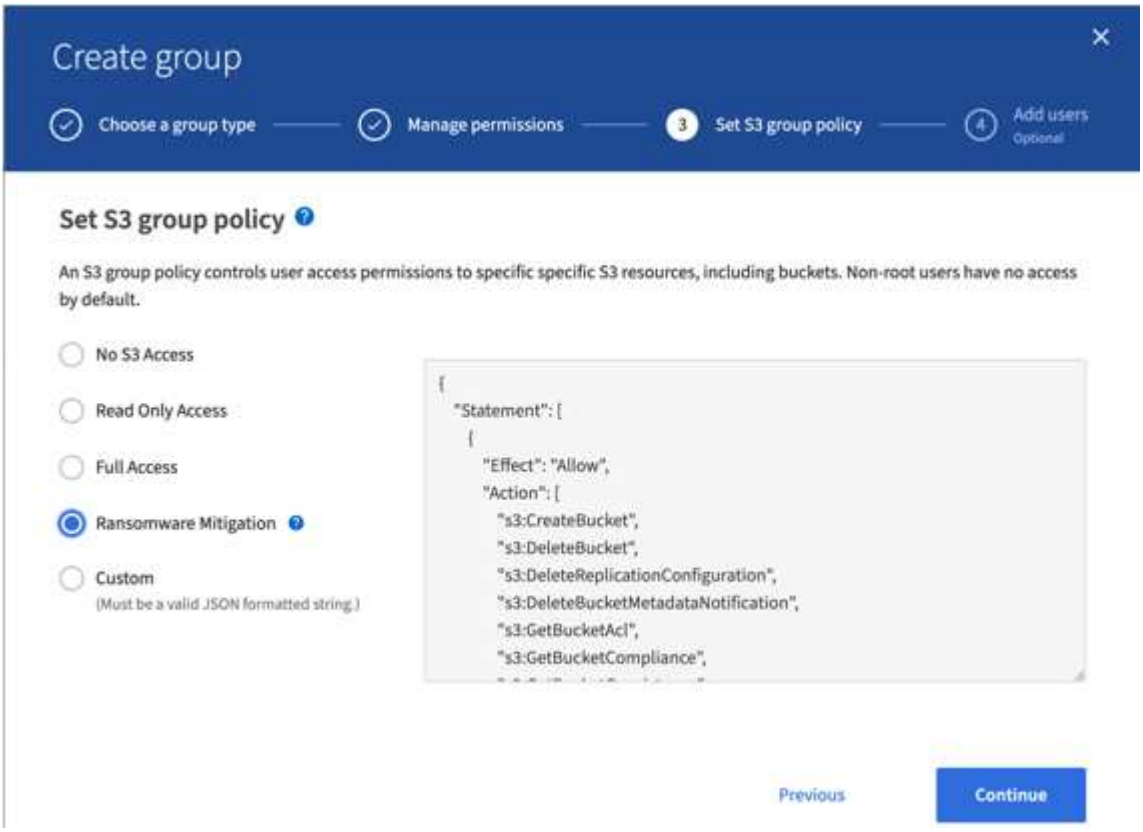
Ransomware-Verteidigung durch Versionierung mit Schutz-IAM-Richtlinie

Erfahren Sie, wie Sie Ihre Daten schützen, indem Sie die Versionierung auf dem Bucket aktivieren und IAM-Richtlinien auf Benutzersicherheitsgruppen in StorageGRID implementieren.

Eine Methode zum Schutz Ihrer Daten ohne Objektsperre oder Replikation besteht darin, die Versionierung auf dem Bucket zu aktivieren und IAM-Richtlinien auf den Benutzersicherheitsgruppen zu implementieren, um die Fähigkeit des Benutzers zu beschränken, Versionen der Objekte zu verwalten. Im Falle eines Angriffs werden neue fehlerhafte Versionen der Daten als aktuelle Version erstellt, und die neueste nicht-aktuelle Version ist die

sichere saubere Daten. Die Konten, die für den Zugriff auf die Daten kompromittiert wurden, haben keinen Zugriff auf das Löschen oder anderweitige Ändern der nicht-aktuellen Version, um sie für spätere Wiederherstellungsvorgänge zu schützen. Wie im vorherigen Szenario verwalten ILM-Regeln die Aufbewahrung der nicht aktuellen Versionen mit einer Dauer Ihrer Wahl. Der Nachteil ist, dass es immer noch die Möglichkeit von privilegierten Konten für einen schlechten Akteurangriff gibt, aber alle Anwendungsdienstkonten und Benutzer müssen mit einem restriktiveren Zugriff konfiguriert werden. Die restriktive Gruppenrichtlinie muss jede Aktion, die Benutzer oder Anwendungen ausführen sollen, ausdrücklich zulassen und alle Aktionen, die nicht ausgeführt werden sollen, ausdrücklich ablehnen. NetApp empfiehlt keine Platzhalterfunktion, da in Zukunft möglicherweise eine neue Aktion eingeführt wird. Sie sollten dann kontrollieren, ob sie erlaubt oder verweigert wird. Für diese Lösung muss die Deny-Liste DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration und PutBucketVersioning enthalten, um die Versionskonfiguration des Buckets und Objektversionen vor Benutzer- oder programmatischen Änderungen zu schützen.

In StorageGRID erleichtert die S3-Gruppenrichtlinienoption „Ransomware Mitigation“ die Implementierung dieser Lösung. Wenn Sie im Mandanten eine Benutzergruppe erstellen, können Sie nach Auswahl der Gruppenberechtigungen diese optionale Richtlinie sehen.



Im Folgenden finden Sie den Inhalt der Gruppenrichtlinie, die die meisten verfügbaren Vorgänge explizit erlaubt und das erforderliche Minimum abgelehnt enthält.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
```

```
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
```

```
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Untersuchung und Behebung von Ransomware

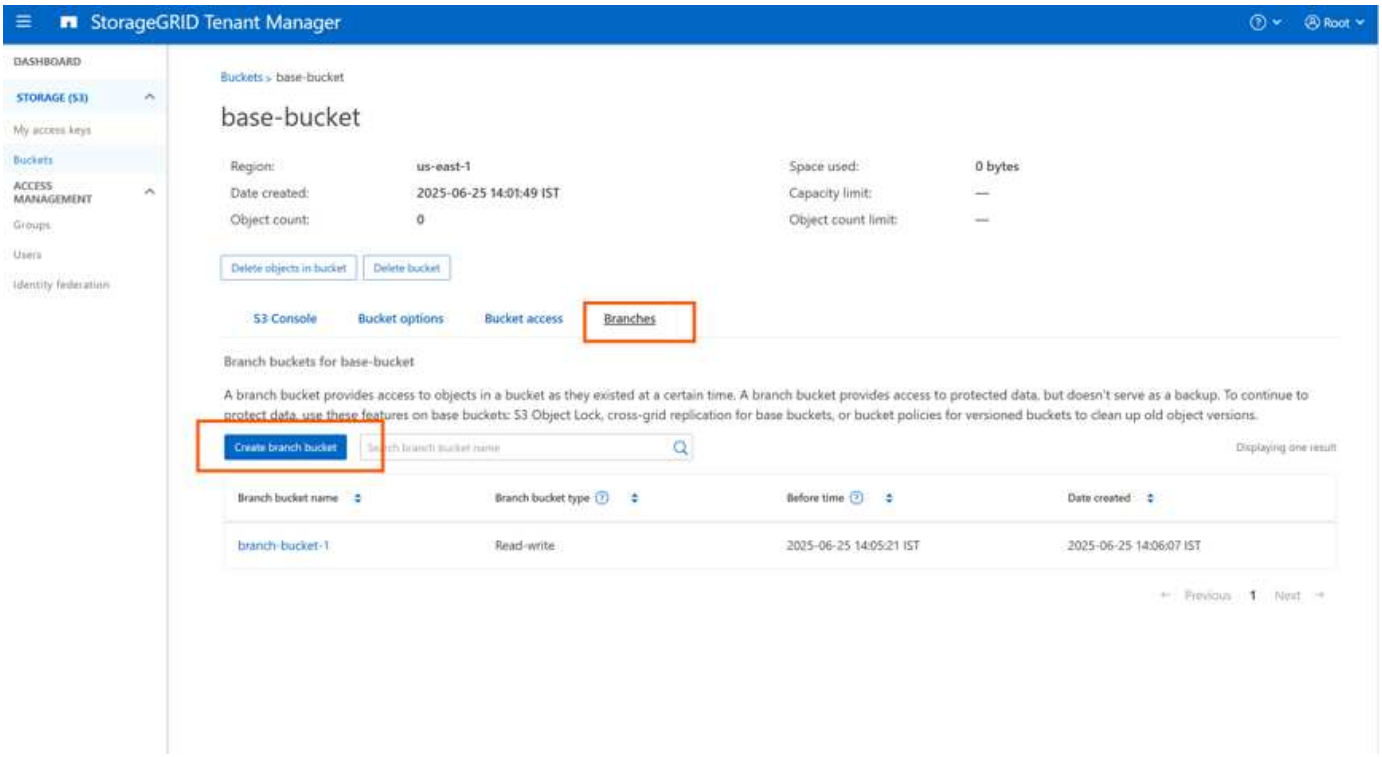
Erfahren Sie, wie Sie Buckets nach einem möglichen Ransomware-Angriff mit StorageGRID untersuchen und beheben.

In StorageGRID 12.0 wurde die neue Branch-Bucket-Funktion hinzugefügt, um die Nützlichkeit der Versionierung für die Ransomware-Abwehr zu erweitern. Ein Branch-Bucket bietet Zugriff auf Objekte in einem Bucket, wie sie zu einem bestimmten Zeitpunkt existierten, sofern sie noch im Bucket vorhanden sind. Branch-Buckets können nur für versionierungsfähige Basis-Buckets erstellt werden.

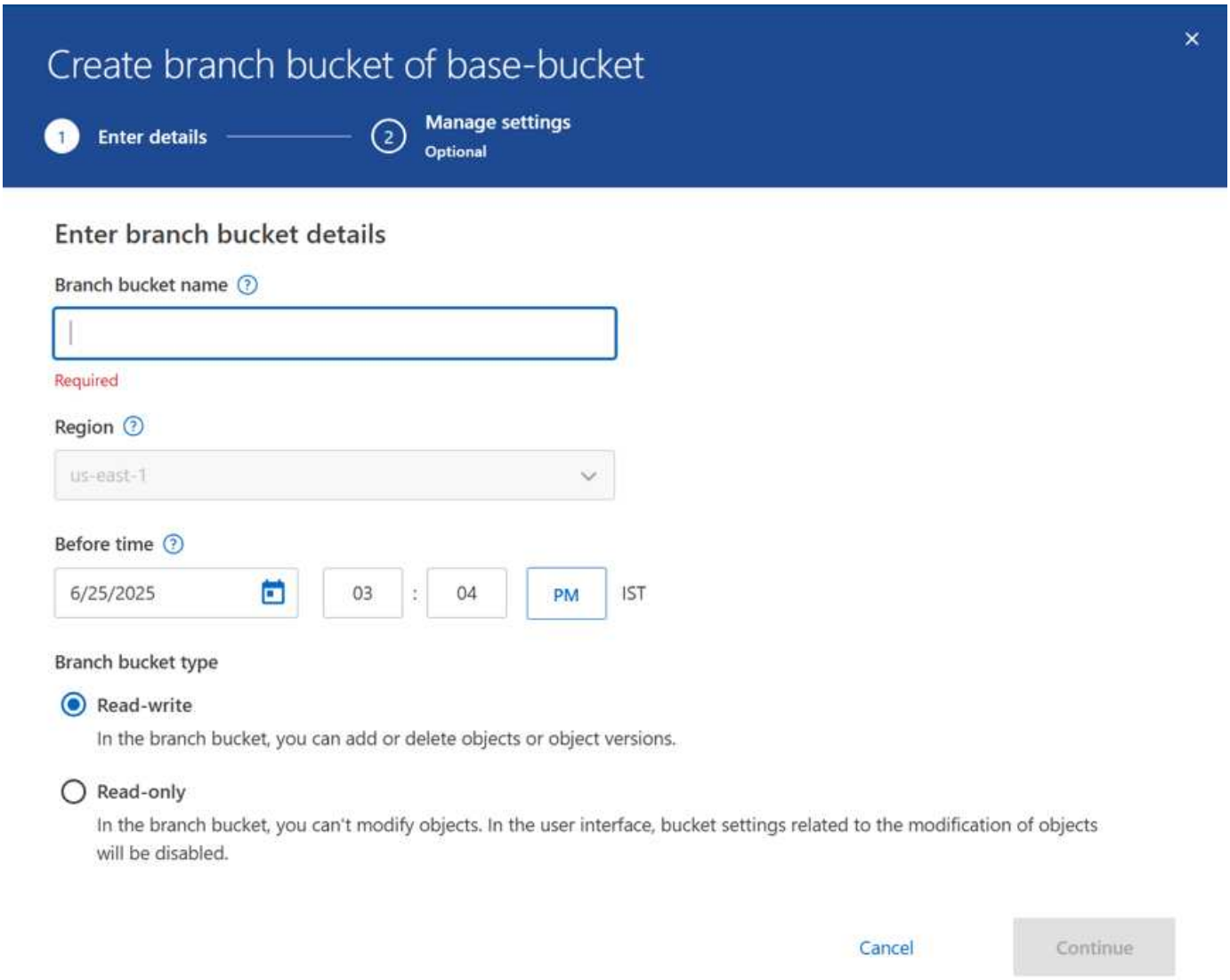
Das bedeutet, dass Sie bei Verdacht auf einen Ransomware-Angriff einen Lese-/Schreib- oder schreibgeschützten Branch-Bucket erstellen können, der alle Objekte und Versionen enthält, die vor dem ersten Angriff vorhanden waren. Sie können diesen Zweig-Bucket zum Vergleich mit dem Inhalt des Basis-Buckets verwenden, um herauszufinden, welche Objekte geändert wurden und ob die Änderung Teil des Angriffs war oder nicht. Sie können auch einen Branch-Bucket verwenden, um die Clientvorgänge mithilfe des Clean-Branch fortzusetzen, während Sie den Angriff untersuchen.

Erstellen eines Branch-Buckets

- Navigieren Sie zur Detailseite des Basis-Buckets und zur Registerkarte „Branches“, um einen Branch-Bucket zu erstellen.



- Sobald Sie auf die Schaltfläche „Zweig-Bucket erstellen“ klicken, wird ein Popup mit vorab ausgefüllten Details der mit dem Basis-Bucket verknüpften Region geöffnet.
- Geben Sie vor der Zeit den Namen des Branch-Buckets ein und wählen Sie aus, welcher Branch-Bucket-Typ erstellt werden soll.



TR-4765: Monitor StorageGRID

Einführung in das StorageGRID-Monitoring

Erfahren Sie, wie Sie Ihr StorageGRID System mit externen Applikationen wie Splunk überwachen.

Durch die effektive Überwachung des objektbasierten Storage von NetApp StorageGRID können Administratoren umgehend auf dringende Probleme reagieren und Ressourcen proaktiv hinzufügen, um wachsende Workloads zu bewältigen. Dieser Bericht bietet allgemeine Hinweise zur Überwachung wichtiger Kennzahlen und zur Nutzung externer Überwachungsanwendungen. Es soll das bestehende Handbuch zur Überwachung und Fehlerbehebung ergänzen.

Eine NetApp StorageGRID-Implementierung besteht in der Regel aus mehreren Standorten und mehreren Nodes, die ein verteiltes und fehlertolerantes Objekt-Storage-System erzeugen. In einem verteilten und robusten Storage-System wie StorageGRID existieren Fehlerbedingungen, während das Grid weiterhin normal arbeitet. Die Herausforderung für Sie als Administrator besteht darin, die Schwelle zu verstehen, bei der Fehlerbedingungen (z. B. Knoten ausgefallen) ein Problem darstellen, das sofort behoben werden sollte, und Informationen, die analysiert werden sollten. Durch die Analyse der von StorageGRID gespeicherten Daten

können Sie einen besseren Überblick über Ihren Workload haben und fundierte Entscheidungen treffen, beispielsweise wenn Sie zusätzliche Ressourcen hinzufügen möchten.

StorageGRID bietet eine exzellente Dokumentation, die tief in das Thema Monitoring eintaucht. In diesem Bericht wird vorausgesetzt, dass Sie mit StorageGRID vertraut sind und die Dokumentation darüber geprüft haben. Anstatt diese Informationen zu wiederholen, beziehen wir uns in der Produktdokumentation in diesem Handbuch. Die Produktdokumentation von StorageGRID ist online und als PDF verfügbar.

Ziel dieses Dokuments ist die Ergänzung der Produktdokumentation und die Erläuterung der Überwachung Ihres StorageGRID Systems mit externen Applikationen wie Splunk.

Datenquellen

Für die erfolgreiche Überwachung von NetApp StorageGRID ist es wichtig zu wissen, wo Daten über den Zustand und die Vorgänge Ihres StorageGRID Systems erfasst werden müssen.

- **Web UI und Dashboard.** Der StorageGRID-Grid-Manager bietet eine Ansicht der wichtigsten Informationen, die Sie als Administrator in einer logischen Präsentation anzeigen müssen. Als Administrator können Sie sich außerdem tiefer mit Service-Level-Informationen für die Fehlerbehebung und Protokollsammlung befassen.
- **Prüfprotokolle.** StorageGRID speichert granulare Prüfprotokolle von Mandantenaktionen wie PUT, GET und DELETE. Sie können auch den Lebenszyklus eines Objekts von der Aufnahme bis zur Anwendung der Datenmanagement-Regeln nachverfolgen.
- **Metrics API.** Dem StorageGRID GMI liegen offene APIs zugrunde, da die Benutzeroberfläche API-basiert ist. Dieser Ansatz ermöglicht es Ihnen, Daten mithilfe externer Überwachungs- und Analysetools zu extrahieren.

Wo Sie weitere Informationen finden

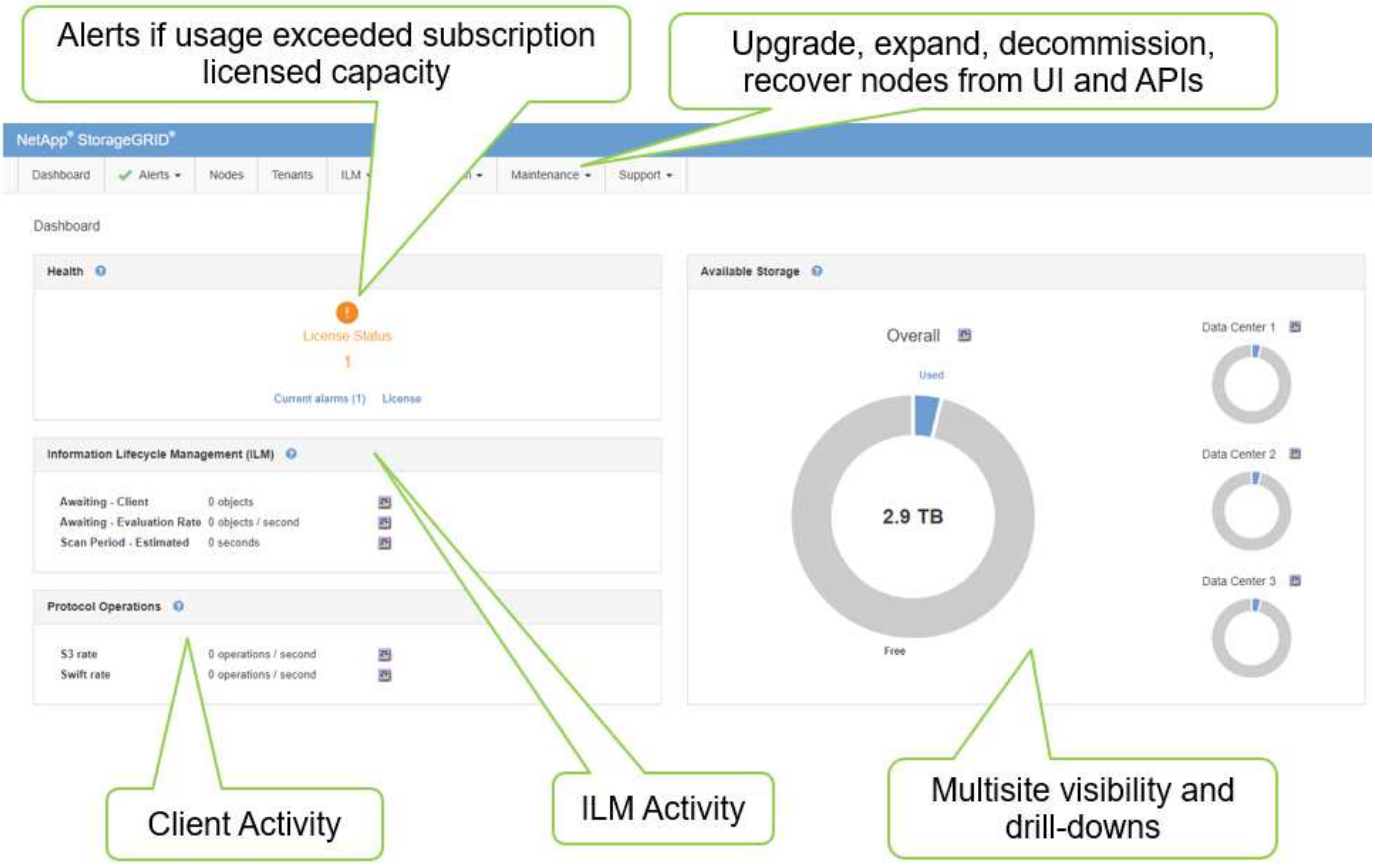
Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/
- NetApp StorageGRID App für Splunk https://splunkbase.splunk.com/app/3898/#/details

Verwenden Sie das GMI-Dashboard, um StorageGRID zu überwachen

Das StorageGRID Grid Management Interface (GMI) Dashboard bietet eine zentrale Ansicht der StorageGRID Infrastruktur. So haben Sie die Möglichkeit, den Zustand, die Performance und die Kapazität des gesamten Grids zu überwachen.

Verwenden Sie das GMI-Dashboard, um jede Kernkomponente des Rasters zu untersuchen.



Informationen, die Sie regelmäßig überwachen sollten

In einer vorherigen Version dieses technischen Berichts sind die Kennzahlen aufgeführt, die regelmäßig überprüft werden müssen, verglichen mit den Trends. Diese Informationen sind nun in der "Leitfaden zur Überwachung und Fehlerbehebung".

Überwachen Sie den Speicher

Eine vorherige Version dieses technischen Berichts war aufgeführt, wo wichtige Kennzahlen wie Objekt-Storage-Platzbedarf, Metadaten-Speicherplatz, Netzwerkressourcen usw. überwacht werden müssen. Diese Informationen sind nun in der "Leitfaden zur Überwachung und Fehlerbehebung".

Verwenden Sie Warnmeldungen, um StorageGRID zu überwachen

Erfahren Sie, wie Sie das Warnsystem in StorageGRID verwenden, um Probleme zu überwachen, benutzerdefinierte Warnmeldungen zu verwalten und Benachrichtigungen per SNMP oder E-Mail zu erweitern.

Warnmeldungen liefern wichtige Informationen, mit denen Sie die verschiedenen Ereignisse und Zustände in Ihrem StorageGRID-System überwachen können.

Das Warnmeldungssystem ist das primäre Tool für die Überwachung von Problemen, die in Ihrem StorageGRID-System auftreten können. Das Alarmsystem konzentriert sich auf umsetzbare Probleme im System und bietet eine benutzerfreundliche Oberfläche.

Wir bieten eine Reihe von Standardwarnungsregeln an, mit denen Sie Ihr System überwachen und Fehler beheben können. Sie können Warnmeldungen weiter verwalten, indem Sie benutzerdefinierte Warnmeldungen

erstellen, Standardwarnungen bearbeiten oder deaktivieren und Warnmeldungen stummschalten.

Alarme können auch über SNMP oder E-Mail-Benachrichtigungen erweitert werden.

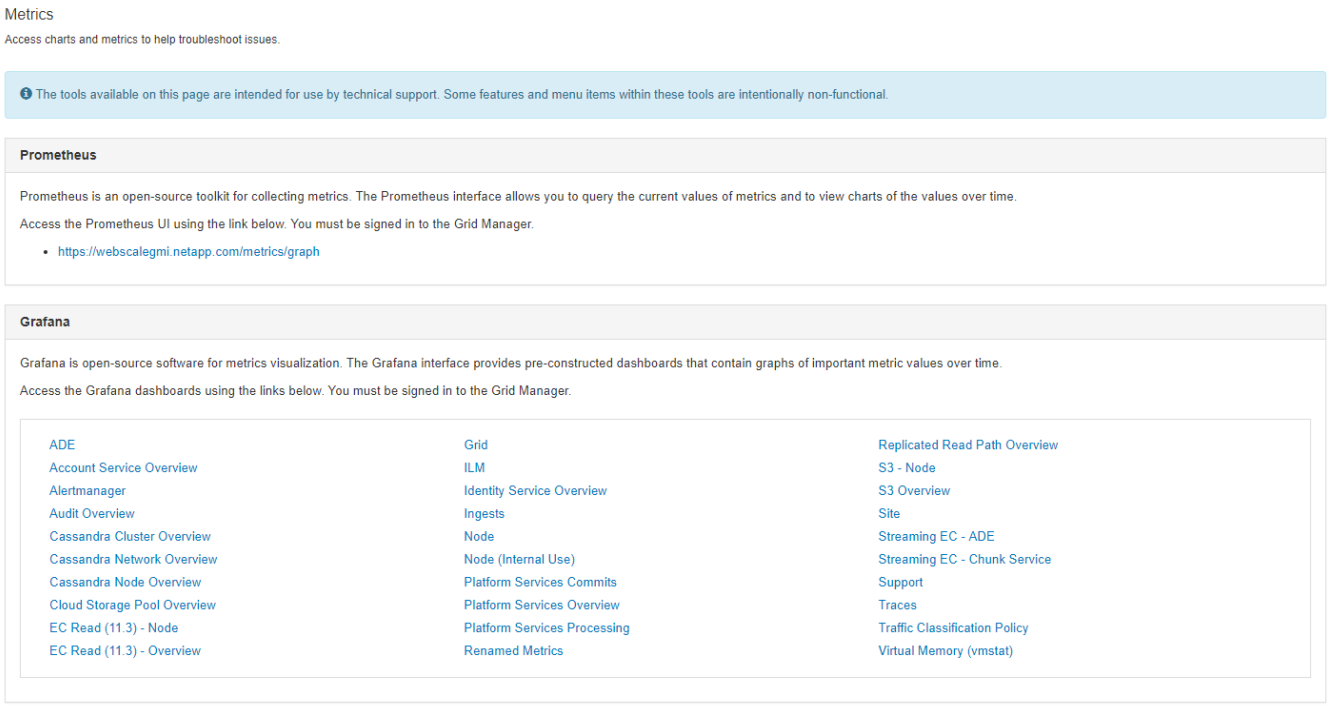
Weitere Informationen zu Warnmeldungen finden Sie im "Produktdokumentation" Online- und im PDF-Format.

Erweiterte Überwachung in StorageGRID

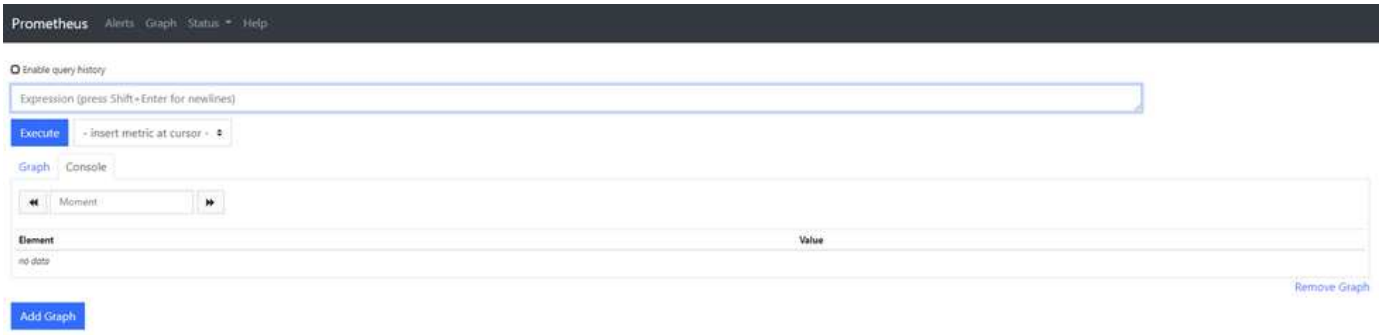
Erfahren Sie, wie Sie auf Kennzahlen zugreifen und diese exportieren, um Probleme zu beheben.

Anzeigen von Kennzahlen-API über eine Prometheus-Abfrage

Prometheus ist eine Open-Source-Software zur Erfassung von Kennzahlen. Über das GMI können Sie auf die in StorageGRID eingebetteten Prometheus zugreifen: Support[Metriken].



Alternativ können Sie direkt zu dem Link navigieren.

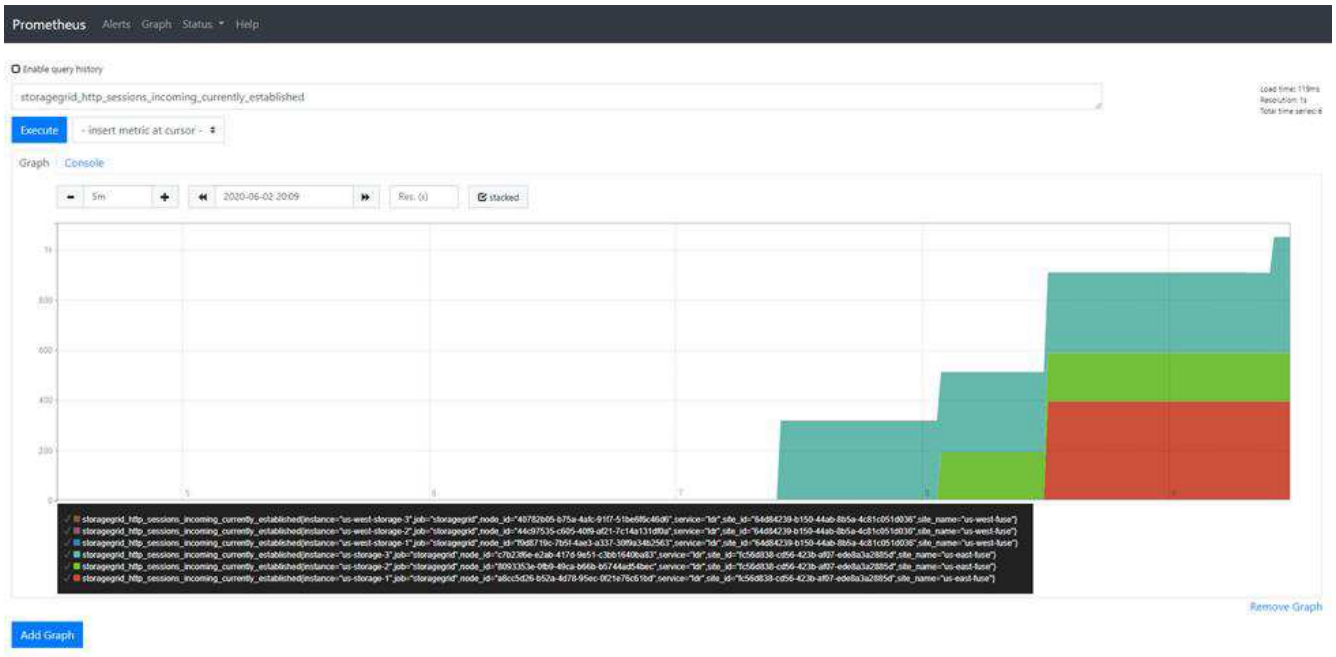


Mit dieser Ansicht können Sie auf die Prometheus-Schnittstelle zugreifen. Von dort aus können Sie die verfügbaren Metriken durchsuchen und sogar mit Abfragen experimentieren.

Gehen Sie wie folgt vor, um eine Prometheus-URL-Abfrage durchzuführen:

Schritte

1. Beginnen Sie mit der Eingabe im Textfeld für die Abfrage. Bei der Eingabe werden die Metriken aufgelistet. Für unsere Zwecke sind nur Metriken wichtig, die mit StorageGRID und Node beginnen.
2. Um die Anzahl der HTTP-Sitzungen für jeden Knoten anzuzeigen, geben Sie ein `storagegrid_http` , und wählen Sie `storagegrid_http_sessions_incoming_currently_established`. Klicken Sie auf Ausführen und zeigen Sie die Informationen in einem Diagramm- oder Konsolenformat an.



Abfragen und Diagramme, die Sie über diese URL erstellen, bleiben nicht erhalten. Komplexe Abfragen verbrauchen Ressourcen auf dem Admin-Node. NetApp empfiehlt, die verfügbaren Metriken in dieser Ansicht zu prüfen.

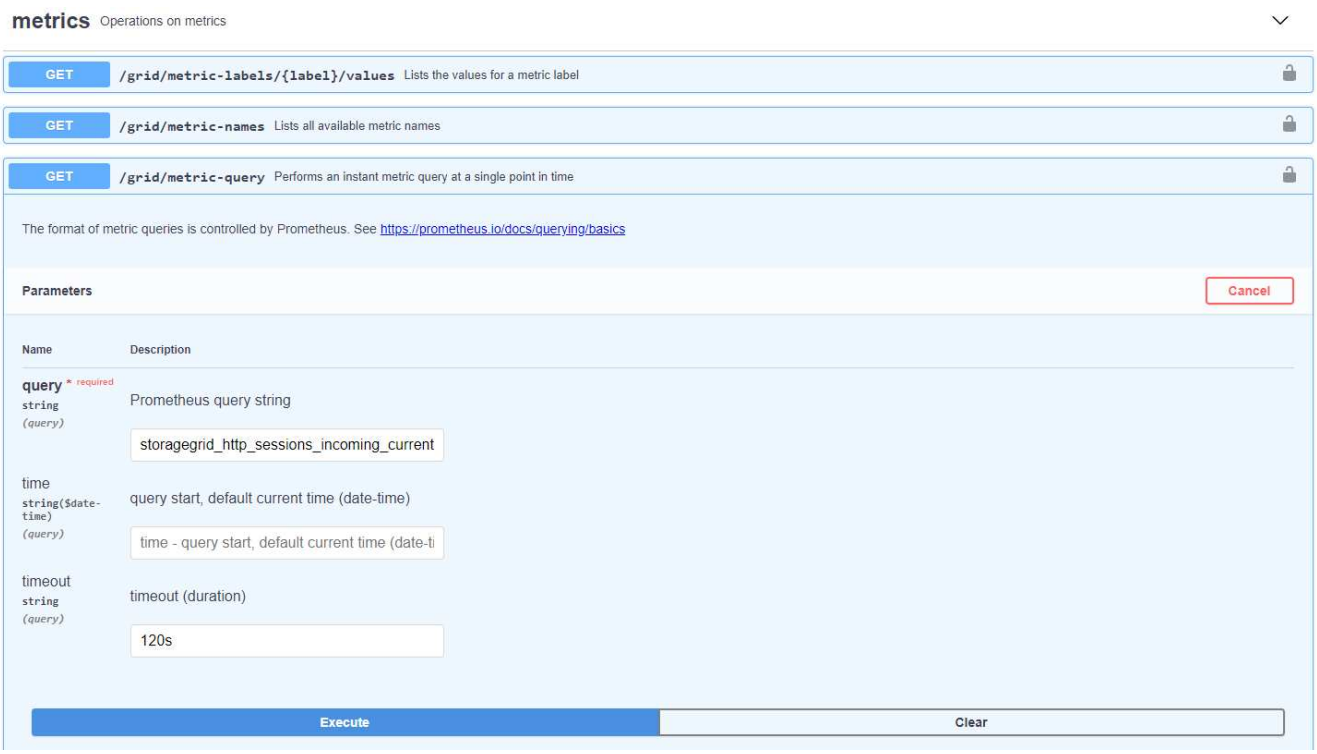
Es wird nicht empfohlen, eine direkte Schnittstelle zu unserer Prometheus Instanz zu verwenden, da hierzu zusätzliche Ports geöffnet werden müssen. Der Zugriff auf Kennzahlen über unsere API ist die empfohlene und sichere Methode.

Exportieren von Kennzahlen über die API

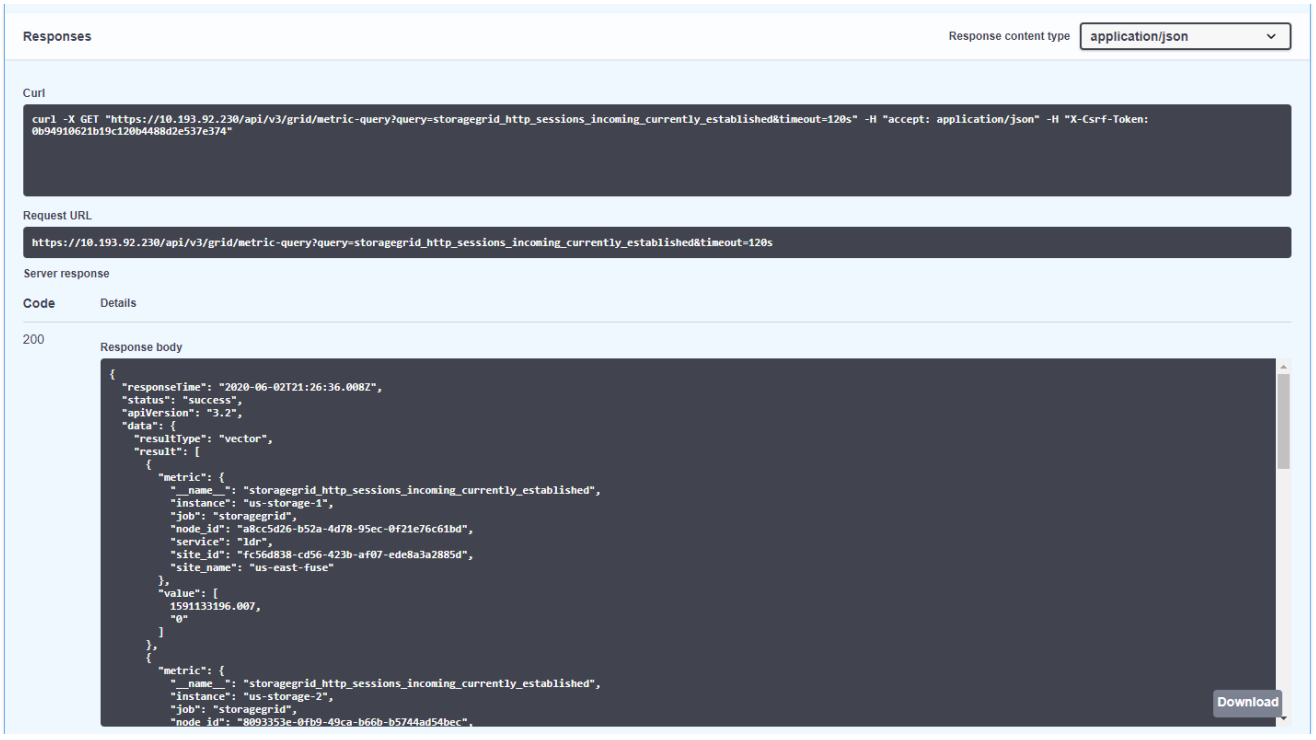
Außerdem können Sie über die StorageGRID Management-API auf dieselben Daten zugreifen.

Gehen Sie wie folgt vor, um Metriken über die API zu exportieren:

1. Wählen Sie im GMI die Option MENU:Help[API Documentation].
2. Scrollen Sie nach unten zu Metriken und wählen Sie GET /Grid/metric-query.



Die Antwort enthält dieselben Informationen, die Sie über eine Prometheus URL-Abfrage erhalten können. Sie können wieder die Anzahl der HTTP-Sitzungen anzeigen, die derzeit auf jedem Storage-Node eingerichtet sind. Sie können die Antwort zur Lesbarkeit auch im JSON-Format herunterladen. Die folgende Abbildung zeigt beispielhafte Prometheus Abfrageantworten.



Der Vorteil der Verwendung der API besteht darin, dass Sie authentifizierte Abfragen durchführen können

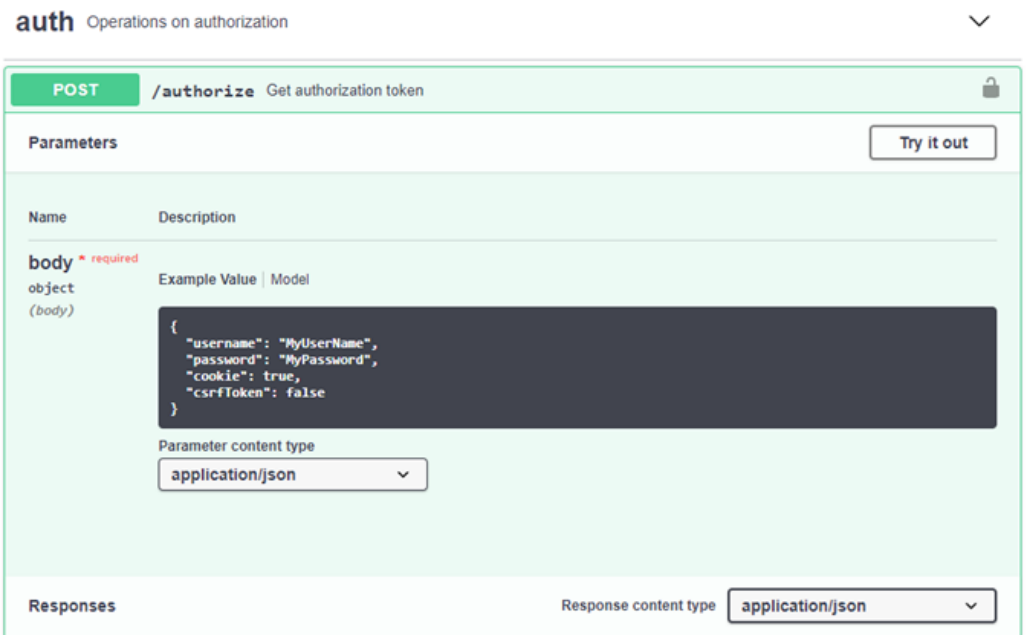
Zugriff auf Metriken mithilfe von Curl in StorageGRID

Erfahren Sie, wie Sie mithilfe von Curl über die CLI auf Metriken zugreifen.

Um diesen Vorgang auszuführen, müssen Sie zunächst ein Autorisierungs-Token anfordern. So fordern Sie ein Token an:

Schritte

1. Wählen Sie im GMI die Option MENU:Help[API Documentation].
2. Blättern Sie nach unten zu Auth, um nach Vorgängen für die Autorisierung zu suchen. Der folgende Screenshot zeigt die Parameter für die POST-Methode.



3. Klicken Sie auf Try IT Out, und bearbeiten Sie den Text mit Ihrem GMI-Benutzernamen und -Kennwort.
4. Klicken Sie Auf Ausführen.
5. Kopieren Sie den Befehl curl, der im Abschnitt curl angegeben ist, und fügen Sie ihn in ein Terminalfenster ein. Der Befehl sieht wie folgt aus:

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

> Wenn Ihr GMI-Passwort Sonderzeichen enthält, vergessen Sie nicht, \ zu verwenden, um Sonderzeichen zu umgehen. Zum Beispiel ersetzen ! Mit \!

6. Nachdem Sie den vorherigen Curl-Befehl ausgeführt haben, erhalten Sie in der Ausgabe ein Autorisierungstoken wie das folgende Beispiel:

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

Jetzt können Sie die Zeichenfolge für das Autorisierungstoken verwenden, um auf Metriken durch Curl zuzugreifen. Der Prozess für den Zugriff auf Kennzahlen ähnelt den Schritten in Abschnitt "Erweiterte Überwachung in StorageGRID". Zu Demonstrationszwecken zeigen wir jedoch ein Beispiel mit GET /GRID/metric-Labels/{Label}/values, das in der Kategorie Metrics ausgewählt wurde.

7. Beispiel: Der folgende Curl-Befehl mit dem vorangehenden Autorisierungstoken führt die Standortnamen in StorageGRID auf.

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

Der Befehl Curl erzeugt die folgende Ausgabe:

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

Anzeigen von Kennzahlen über das Grafana-Dashboard in StorageGRID

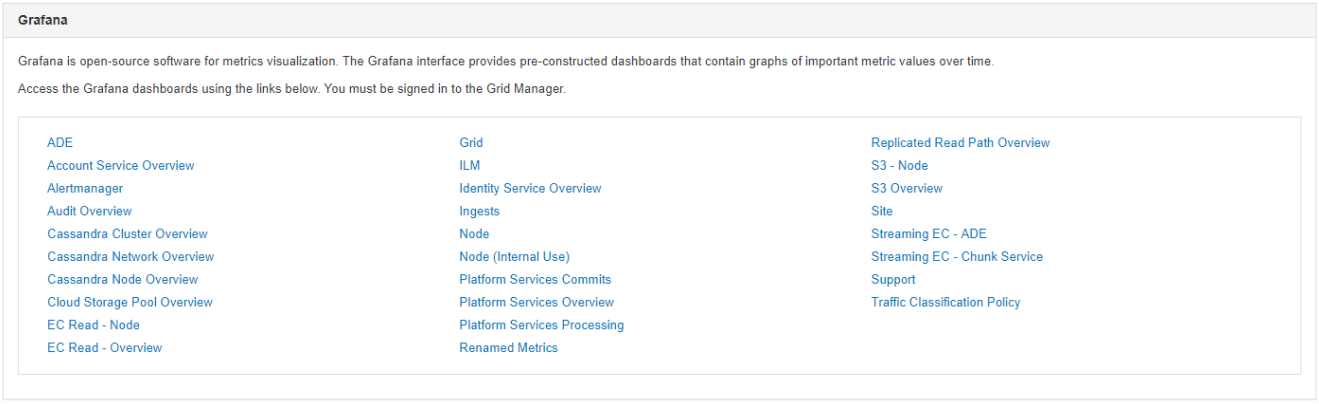
Erfahren Sie, wie Sie mit der Grafana-Schnittstelle Ihre StorageGRID-Daten visualisieren und überwachen.

Grafana ist eine Open-Source-Software für die metrische Visualisierung. Wir verfügen standardmäßig über vorgefertigte Dashboards mit nützlichen und aussagekräftigen Informationen zu Ihrem StorageGRID System.

Diese vorgefertigten Dashboards sind nicht nur für die Überwachung, sondern auch für die Fehlerbehebung bei einem Problem nützlich. Einige sind für den technischen Support bestimmt. Um z. B. die Metriken eines Storage-Nodes anzuzeigen, führen Sie die folgenden Schritte aus.

Schritte

1. Im GMI Menü:Support[Metriken].
2. Wählen Sie im Abschnitt Grafana das Knoten-Dashboard aus.



3. Legen Sie in Grafana den Host auf den Node fest, für den Sie Metriken anzeigen möchten. In diesem Fall ist ein Storage-Node ausgewählt. Es werden mehr Informationen bereitgestellt als die folgenden Screenshot-Aufnahmen.

Verwenden Sie Richtlinien zur Verkehrsklassifizierung im StorageGRID

Erfahren Sie, wie Sie Richtlinien zur Verkehrsklassifizierung einrichten und konfigurieren, um den Netzwerkverkehr in StorageGRID zu managen und zu optimieren.

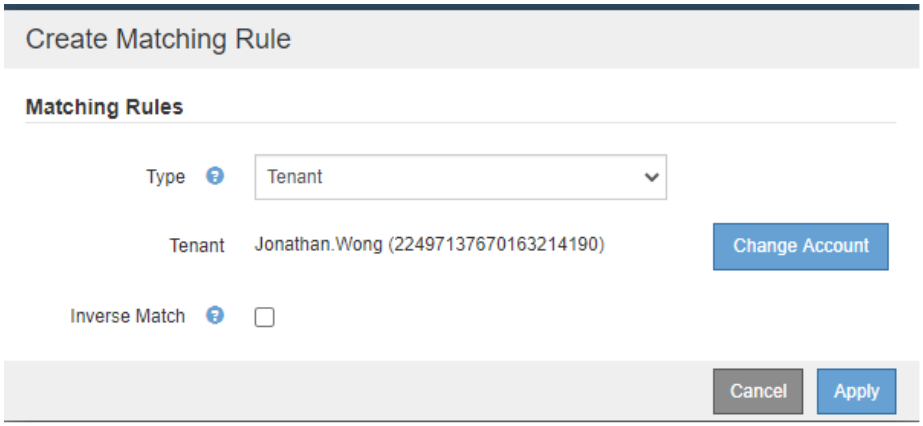
Richtlinien zur Traffic-Klassifizierung bieten eine Methode zur Überwachung und/oder Begrenzung des Datenverkehrs auf der Grundlage eines bestimmten Mandanten, Buckets, IP-Subnetzes oder Load-Balancer-Endpunkts. Netzwerkkonnektivität und Bandbreite sind besonders wichtige Kenngrößen für StorageGRID.

Gehen Sie wie folgt vor, um eine Richtlinie zur Traffic-Klassifizierung zu konfigurieren:

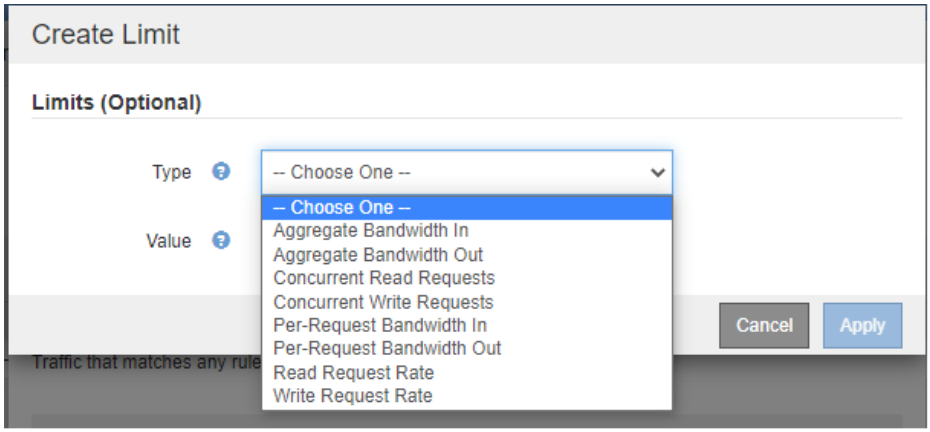
Schritte

1. Navigieren Sie im GMI zu MENU:Configuration[System Settings > Traffic Classification].
2. Klicken Sie Auf Erstellen +
3. Geben Sie einen Namen und eine Beschreibung für Ihre Richtlinie ein.

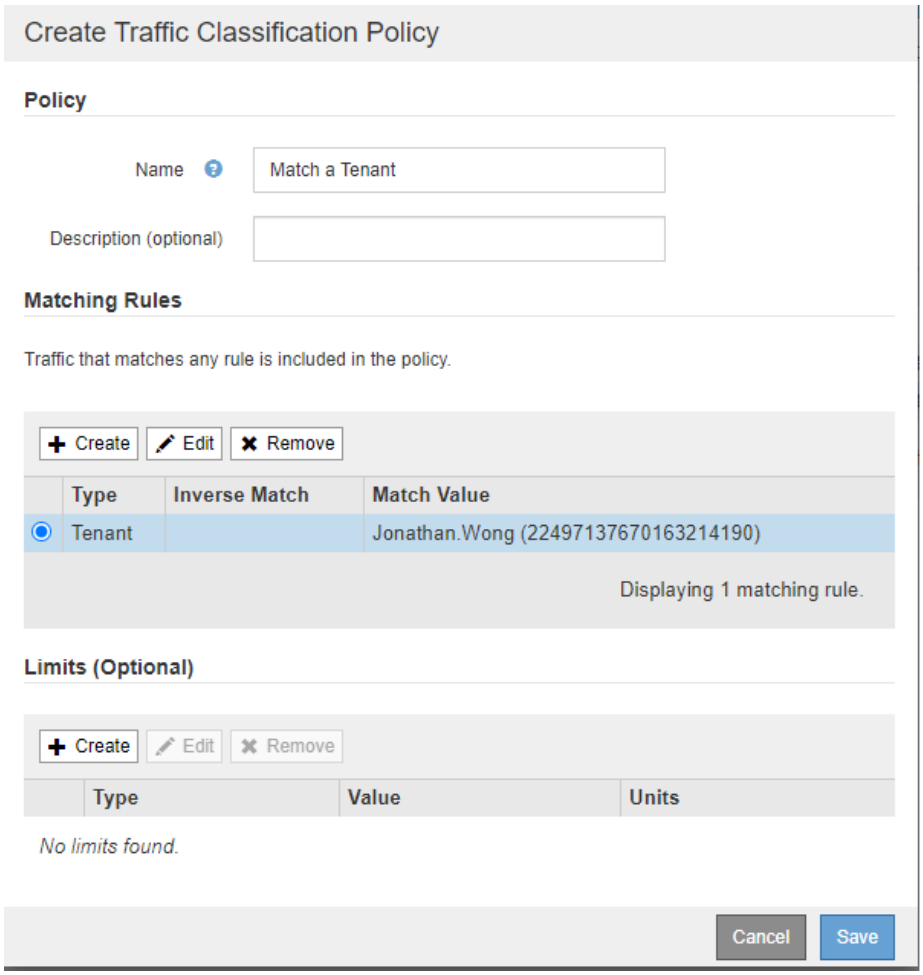
4. Erstellen Sie eine übereinstimmende Regel.



5. Legen Sie eine Grenze fest (optional).



6. Speichern Sie Ihre Richtlinie



Um die Metriken anzuzeigen, die Ihrer Richtlinie zur Traffic-Klassifizierung zugeordnet sind, wählen Sie Ihre Richtlinie aus, und klicken Sie auf Kennzahlen. Es wird ein Grafana Dashboard mit Informationen wie Load Balancer Request Traffic und Average Request Duration erstellt.

Verwenden Sie Prüfprotokolle, um StorageGRID zu überwachen

Erfahren Sie, wie Sie das StorageGRID-Revisionsprotokoll detaillierte Einblicke in Mandanten- und Grid-Aktivitäten erhalten und wie Sie Tools wie Splunk für Protokollanalysen nutzen können.

Mit dem StorageGRID Revisionsprotokoll können Sie detaillierte Informationen über Mandanten und Grid-Aktivitäten erfassen. Das Revisionsprotokoll kann zur Analyse durch NFS offengelegt werden. Ausführliche Anweisungen zum Exportieren des Überwachungsprotokolls finden Sie im Administratorhandbuch.

Nach dem Export der Prüfung können Sie Protokollanalyse-Tools wie Splunk oder Logstash + Elasticsearch verwenden, um die Mandantenaktivität zu verstehen oder detaillierte Rechnungs- und Chargeback-Berichte zu erstellen.

Details zu Audit-Meldungen sind in der StorageGRID-Dokumentation enthalten. Siehe "Audit-Meldungen".

Die StorageGRID App für Splunk

Die NetApp StorageGRID App für Splunk ermöglicht Monitoring und Analyse Ihrer StorageGRID-Umgebung innerhalb der Splunk Plattform.

Splunk ist eine Softwareplattform, die Maschinendaten importiert und indiziert, um leistungsstarke Such- und Analysefunktionen zu bieten. Die NetApp StorageGRID App ist ein Add-on für Splunk, das die aus StorageGRID verwendeten Daten importiert und anreichert.

Anweisungen zur Installation, Aktualisierung und Konfiguration des StorageGRID Add-ons finden Sie hier: https://splunkbase.splunk.com/app/3895/#/details

TR-4882: Installation eines StorageGRID Bare-Metal Grid

Einführung in die Installation von StorageGRID

Erfahren Sie, wie Sie StorageGRID auf Bare-Metal-Hosts installieren.

TR-4882 bietet eine praktische Schritt-für-Schritt-Anleitung, die zu einer funktionierenden Installation von NetApp StorageGRID führt. Die Installation kann entweder auf Bare-Metal-Systemen oder auf Virtual Machines (VMs) erfolgen, die unter Red hat Enterprise Linux (RHEL) ausgeführt werden. Der Ansatz besteht darin, eine „opinionierte“ Installation von sechs StorageGRID Container-Services auf drei physischen (oder virtuellen) Maschinen mit einer vorgegebenen Layout- und Storage-Konfiguration durchzuführen. Einige Kunden finden es unter Umständen leichter, den Implementierungsprozess zu verstehen, indem sie dem Beispiel folgen, das in diesem TR bereitgestellt wird.

Weitere Informationen zu StorageGRID und dem Installationsprozess finden Sie unter https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html [StorageGRID installieren, aktualisieren und Hotfix] in der Produktdokumentation.

Bevor Sie mit der Implementierung beginnen, sollten wir die Computing-, Storage- und Netzwerkanforderungen für NetApp StorageGRID Software untersuchen. StorageGRID wird als Container-Service in Podman oder Docker ausgeführt. Einige Anforderungen beziehen sich in diesem Modell auf das Host-Betriebssystem (das Betriebssystem, auf dem Docker gehostet wird, auf dem die StorageGRID Software ausgeführt wird). Einige Ressourcen werden direkt den Docker Containern zugewiesen, die innerhalb jedes Hosts ausgeführt werden. In dieser Implementierung implementieren wir zur Maximierung der

Hardwarenutzung zwei Services pro physischem Host. Weitere Informationen finden Sie im nächsten Abschnitt. "Voraussetzungen für die Installation von StorageGRID"

Die in dieser TR beschriebenen Schritte führen zu einer funktionierenden StorageGRID-Installation auf sechs Bare-Metal-Hosts. Sie verfügen jetzt über ein funktionierendes Grid- und Client-Netzwerk, das in den meisten Testszenarien nützlich ist.

Wo Sie weitere Informationen finden

Folgende Dokumentationsressourcen enthalten weitere Informationen zu den in diesem TR enthaltenen Informationen:

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Voraussetzungen für die Installation von StorageGRID

Informieren Sie sich über die Computing-, Storage-, Netzwerk-, Docker- und Node-Anforderungen für die Implementierung von StorageGRID.

Computing-Anforderungen

In der folgenden Tabelle sind die unterstützten Mindestanforderungen an Ressourcen für jeden Typ von StorageGRID-Knoten aufgeführt. Dies sind die Mindestressourcen, die für StorageGRID Nodes erforderlich sind.

Node-Typ	CPU-Kerne	RAM
Admin	8	24 GB
Storage	8	24 GB
Gateway	8	24 GB

Darüber hinaus sollte jedem physischen Docker Host mindestens 16 GB RAM zugewiesen sein, um den ordnungsgemäßen Betrieb zu gewährleisten. Um beispielsweise zwei der in der Tabelle beschriebenen Services gemeinsam auf einem physischen Docker Host zu hosten, führen Sie die folgende Berechnung aus:

24 + 24 +16 = 64 GB RAM und 8 + 8 = 16 Cores

Da viele moderne Server diese Anforderungen übertreffen, kombinieren wir sechs Services (StorageGRID-Container) auf drei physischen Servern.

Netzwerkanforderungen

Zu den drei Arten von StorageGRID-Datenverkehr gehören:

- **Netzverkehr (erforderlich).** Der interne StorageGRID-Datenverkehr zwischen allen Nodes im Grid.
- **Admin Traffic (optional).** Der für die Systemadministration und -Wartung verwendete Datenverkehr.
- **Client Traffic (optional).** Der Datenverkehr zwischen externen Client-Applikationen und dem Grid, einschließlich aller Objekt-Storage-Anforderungen von S3 und Swift Clients

Sie können bis zu drei Netzwerke zur Verwendung mit dem StorageGRID-System konfigurieren. Jeder Netzwerktyp muss sich in einem separaten Subnetz ohne Überschneidung befinden. Wenn sich alle Nodes im gleichen Subnetz befinden, ist keine Gateway-Adresse erforderlich.

Für diese Auswertung werden wir in zwei Netzwerken bereitstellen, die den Grid- und Client-Datenverkehr enthalten. Es ist möglich, später ein Admin-Netzwerk hinzuzufügen, um diese zusätzliche Funktion zu unterstützen.

Es ist sehr wichtig, die Netzwerke konsistent den Schnittstellen aller Hosts zuzuordnen. Wenn beispielsweise auf jedem Node zwei Schnittstellen vorhanden sind, ens192 und ens224, sollten sie alle auf allen Hosts dem gleichen Netzwerk oder VLAN zugeordnet werden. In dieser Installation ordnet das Installationsprogramm diese in den Docker Containern als eth0@if2 und eth2@if3 zu (da der Loopback if1 im Container ist), und daher ist ein konsistentes Modell sehr wichtig.

Hinweis zu Docker Networking

StorageGRID verwendet Netzwerke, die von einigen Docker Container-Implementierungen abweichen. Es wird nicht das von Docker (oder Kubernetes oder Swarm) bereitgestellte Netzwerk verwendet. Stattdessen gibt StorageGRID den Container als --net=none aus, sodass Docker für das Netzwerken des Containers nichts tut. Nachdem der Container vom StorageGRID-Dienst erstellt wurde, wird ein neues macvlan-Gerät aus der in der Node-Konfigurationsdatei definierten Schnittstelle erstellt. Dieses Gerät verfügt über eine neue MAC-Adresse und fungiert als separates Netzwerkgerät, das Pakete von der physischen Schnittstelle empfangen kann. Das macvlan-Gerät wird dann in den Container-Namespace verschoben und in eth0, eth1 oder eth2 innerhalb des Containers umbenannt. Zu diesem Zeitpunkt ist das Netzwerkgerät im Host-Betriebssystem nicht mehr sichtbar. In unserem Beispiel ist das Grid-Netzwerkgerät eth0 in den Docker Containern und das Client-Netzwerk eth2. Bei einem Admin-Netzwerk wäre das Gerät im Container eth1.

> ⓘ Die neue MAC-Adresse des Container-Netzwerkgeräts erfordert möglicherweise die Aktivierung des Promiscuous-Modus in einigen Netzwerk- und virtuellen Umgebungen. In diesem Modus kann das physische Gerät Pakete für MAC-Adressen empfangen und senden, die sich von der bekannten physischen MAC-Adresse unterscheiden. Wenn Sie in VMware vSphere ausgeführt werden, müssen Sie den Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen in den Portgruppen akzeptieren, die StorageGRID-Datenverkehr beim Ausführen von RHEL unterstützen. Ubuntu oder Debian funktioniert unter den meisten Umständen ohne diese Änderungen.

Storage-Anforderungen erfüllt

Die Nodes erfordern entweder SAN-basierte oder lokale Festplattengeräte der in der folgenden Tabelle angegebenen Größen.

> ⓘ Die Zahlen in der Tabelle gelten für jeden StorageGRID-Servicetyp und nicht für das gesamte Grid oder jeden physischen Host. Basierend auf den Bereitstellungsoptionen berechnen wir die Zahlen für jeden physischen Host in, später in "Physisches Host-Layout und Anforderungen"diesem Dokument. die mit einem Sternchen markierten Pfade oder Dateisysteme werden vom Installer selbst im StorageGRID-Container erstellt. Der Administrator benötigt keine manuelle Konfiguration oder Dateisystemerstellung, aber die Hosts benötigen Blockgeräte, um diese Anforderungen zu erfüllen. Mit anderen Worten: Das Blockgerät sollte mit dem Befehl angezeigt `lsblk` werden, jedoch nicht innerhalb des Host-Betriebssystems formatiert oder gemountet sein.

Node-Typ	Zweck der LUN	Anzahl LUNs	Minimale Größe der LUN	Manuelles Dateisystem erforderlich	Vorgeschlagener Node-Konfigurationseintrag
Alle	Admin-Node-Systemspeicherplatz `/var/local` (SSD hier hilfreich)	Einer für jeden Admin-Node	90GB	Nein	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`
Alle Nodes	Docker Storage-Pool in `/var/lib/docker for container pool`	Einer für jeden Host (physisch oder VM)	100 GB pro Container	Ja – etx4	NA – Formatieren und Mounten als Host-Dateisystem (nicht im Container zugeordnet)
Admin	Audit-Protokolle für Admin-Node (Systemdaten im Admin-Container) `/var/local/audit/export`	Einer für jeden Admin-Node	200GB	Nein	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
Admin	Admin-Node-Tabellen (Systemdaten im Admin-Container) `/var/local/mysql_ibdata`	Einer für jeden Admin-Node	200GB	Nein	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
Storage-Nodes	Objekt-Storage (Block-Geräte) `/var/local/rangedb0` (SSD hier hilfreich) `/var/local/rangedb1` `/var/local/rangedb2`	Drei für jeden Lagerbehälter	4000GB	Nein	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

In diesem Beispiel sind die in der folgenden Tabelle gezeigten Festplattengrößen pro Containertyp erforderlich. Die Anforderungen pro physischem Host werden in beschrieben, später in "Physisches Host-Layout und Anforderungen"diesem Dokument.

Festplattengrößen pro Containertyp

Admin-Container

Name	Größe (gib)
Docker-Store	100 (pro Container)

Name	Größe (gib)
ADM-OS	90
Adm-Audit	200
ADM-MySQL	200

Storage-Container

Name	Größe (gib)
Docker-Store	100 (pro Container)
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

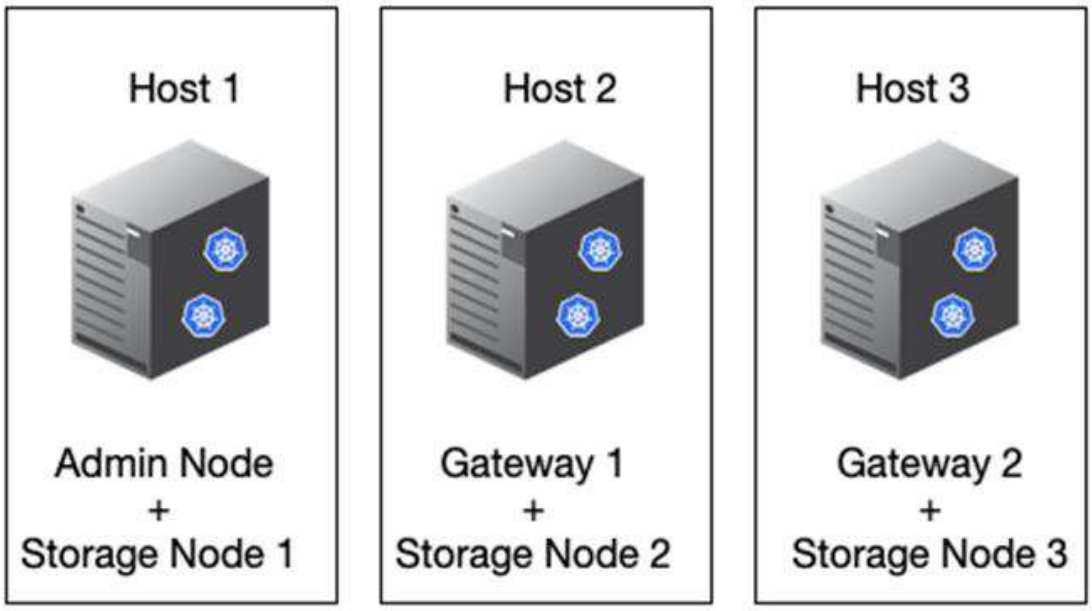
Gateway-Container

Name	Größe (gib)
Docker-Store	100 (pro Container)
/Var/local	90

Physisches Host-Layout und Anforderungen

Wenn Sie die in der obigen Tabelle aufgeführten Computing- und Netzwerkanforderungen kombinieren, erhalten Sie einen grundlegenden Hardware-Satz, der für diese Installation erforderlich ist: Drei physische (oder virtuelle) Server mit 16 Kernen, 64 GB RAM und zwei Netzwerkschnittstellen. Wenn ein höherer Durchsatz gewünscht wird, ist es möglich, zwei oder mehr Schnittstellen im Grid oder Client-Netzwerk zu verbinden und eine VLAN-getaggte Schnittstelle wie bond0.520 in der Node-Konfigurationsdatei zu verwenden. Wenn Sie mit intensiveren Workloads rechnen, ist mehr Speicher sowohl für den Host als auch für die Container besser.

Wie in der folgenden Abbildung dargestellt, hosten diese Server sechs Docker Container, zwei pro Host. Der RAM wird mithilfe von 24 GB pro Container und 16 GB für das Host-Betriebssystem selbst berechnet.



Der gesamte pro physischem Host (oder VM) erforderliche RAM beträgt 24 x 2 + 16 = 64 GB. In der folgenden Tabelle ist der erforderliche Festplattenspeicher für die Hosts 1, 2 und 3 aufgeführt.

Host 1	**Größe (gib)**
Docker Store	`/var/lib/docker` (Dateisystem)
200 (100 x 2)	**Admin-Container**
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
Lagercontainer	SN-OS `/var/local` (Gerät)
90	Rangedb-0 (Gerät)
4096	Rangedb-1 (Gerät)
4096	Rangedb-2 (Gerät)

Host 2	**Größe (gib)**
Docker Store	`/var/lib/docker` (Freigegeben)
200 (100 x 2)	**Gateway-Container**
GW-OS */`var/local`	100

Host 2	Größe (gib)
Lagercontainer	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Host 3	Größe (gib)
Docker Store	/var/lib/docker (Freigegeben)
200 (100 x 2)	**Gateway-Container**
*/var/local	100
Lagercontainer	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Der Docker Store wurde berechnet, indem 100 GB je /var/local (pro Container) x zwei Container = 200 GB zugelassen wurden.

Vorbereiten der Knoten

Um die Erstinstallation von StorageGRID vorzubereiten, installieren Sie zunächst RHEL Version 9.2 und aktivieren Sie SSH. Richten Sie Netzwerkschnittstellen, das Network Time Protocol (NTP), DNS und den Host-Namen gemäß den Best Practices ein. Sie benötigen mindestens eine aktivierte Netzwerkschnittstelle im Grid-Netzwerk und eine weitere für das Client-Netzwerk. Wenn Sie eine VLAN-getaggte Schnittstelle verwenden, konfigurieren Sie sie wie in den folgenden Beispielen. Andernfalls genügt eine einfache Konfiguration der Standard-Netzwerkschnittstelle.

Wenn Sie ein VLAN-Tag auf der Grid-Netzwerkschnittstelle verwenden müssen, sollte Ihre Konfiguration zwei Dateien im folgenden Format haben /etc/sysconfig/network-scripts/ :

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

In diesem Beispiel wird davon ausgegangen, dass Ihr physisches Netzwerkgerät für das Grid-Netzwerk enp67s0 ist. Es könnte auch ein gebundenes Gerät wie bond0 sein. Unabhängig davon, ob Sie Bonding oder eine Standard-Netzwerkschnittstelle verwenden, müssen Sie die VLAN-getaggte Schnittstelle in Ihrer Node-Konfigurationsdatei verwenden, wenn Ihr Netzwerkport kein Standard-VLAN hat oder wenn das Standard-VLAN nicht mit dem Grid-Netzwerk verknüpft ist. Der StorageGRID-Container selbst entkennzeichnet keine Ethernet-Frames, daher muss er vom übergeordneten Betriebssystem verarbeitet werden.

Optionale Speichereinrichtung mit iSCSI

Wenn Sie keinen iSCSI-Speicher verwenden, müssen Sie sicherstellen, dass host1, host2 und host3 Blockgeräte von ausreichender Größe enthalten, um ihre Anforderungen zu erfüllen. Informationen zu den Speicheranforderungen für host1, host2 und host3 finden Sie unter "Festplattengrößen pro Containertyp" .

Gehen Sie wie folgt vor, um Speicher mit iSCSI einzurichten:

Schritte

1. Wenn Sie externen iSCSI-Speicher wie NetApp E-Serie oder NetApp ONTAP® Datenmanagement-Software verwenden, installieren Sie die folgenden Pakete:

   ```
   sudo yum install iscsi-initiator-utils
   sudo yum install device-mapper-multipath
   ```

2. Suchen Sie auf jedem Host nach der Initiator-ID.

   ```
   # cat /etc/iscsi/initiatorname.iscsi
   InitiatorName=iqn.2006-04.com.example.node1
   ```

3. Ordnen Sie unter Verwendung des Initiatornamens aus Schritt 2 den einzelnen Storage-Nodes LUNs auf Ihrem Speichergerät (der in der Tabelle angegebenen Anzahl und Größe "Storage-Anforderungen erfüllt") zu.

4. Ermitteln Sie die neu erstellten LUNs mit `iscsiadm` und melden Sie sich bei ihnen an.

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

Weitere Informationen finden Sie "Erstellen eines iSCSI-Initiators" im Red hat Customer Portal.

5. Führen Sie den folgenden Befehl aus, um die Multipath-Geräte und ihre zugehörigen LUN-WWIDs anzuzeigen:

```
# multipath -ll
```

Wenn Sie iSCSI nicht mit Multipath-Geräten verwenden, mounten Sie Ihr Gerät einfach mit einem eindeutigen Pfadnamen, der Änderungen am Gerät und Neustarts beibehalten wird.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

Die einfache Verwendung von `/dev/sdx` Gerätenamen kann später Probleme verursachen, wenn Geräte entfernt oder hinzugefügt werden. Wenn Sie Multipath-Geräte verwenden, ändern Sie die `/etc/multipath.conf` Datei wie folgt, um Aliase zu verwenden.

Diese Geräte sind je nach Layout möglicherweise auf allen Knoten vorhanden oder nicht.

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

Bevor Sie Docker in Ihrem Host-Betriebssystem installieren, formatieren Sie die LUN oder die Festplatten-Backups, und mounten `/var/lib/docker`Sie sie. Die anderen LUNs sind in der Node-Konfigurationsdatei definiert und werden direkt von den StorageGRID Containern verwendet. Das heißt, sie werden nicht im Host-Betriebssystem angezeigt; sie erscheinen in den Containern selbst, und diese Dateisysteme werden vom Installer verwaltet.

Wenn Sie eine iSCSI-gestützte LUN verwenden, platzieren Sie etwas Ähnliches wie die folgende Zeile in Ihrer

fstab-Datei. Wie bereits erwähnt, müssen die anderen LUNs nicht im Host-Betriebssystem gemountet werden, sondern müssen als verfügbare Blockgeräte angezeigt werden.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Vorbereiten der Docker-Installation

Gehen Sie wie folgt vor, um die Installation von Docker vorzubereiten:

Schritte

1. Erstellen Sie auf allen drei Hosts ein Filesystem auf dem Docker Storage-Volume.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   Wenn Sie iSCSI-Geräte mit Multipath verwenden, verwenden Sie `/dev/mapper/Docker-Store`.

2. Bereitstellungspunkt für das Docker Storage-Volume erstellen:

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. Fügen Sie einen ähnlichen Eintrag für das Docker-Storage-Volume-device zu hinzu `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   Die folgende `_netdev` Option wird nur empfohlen, wenn Sie ein iSCSI-Gerät verwenden. Wenn Sie ein lokales Blockgerät verwenden `_netdev` , ist dies nicht erforderlich und `defaults` wird empfohlen.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. Mounten Sie das neue Dateisystem und zeigen Sie die Festplattennutzung an.

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. Schalten Sie den Swap aus und deaktivieren Sie ihn aus Leistungsgründen.

   ```
   $ sudo swapoff --all
   ```

6. Um die Einstellungen beizubehalten, entfernen Sie alle Swap-Einträge aus /etc/fstab, z. B.:

```
/dev/mapper/rhel-swap swap defaults 0 0
```

> Wenn Sie den Auslagerungsaustausch nicht vollständig deaktivieren, kann die Leistung erheblich gesenkt werden.

7. Führen Sie einen Testneustart des Node durch, um sicherzustellen, dass das `/var/lib/docker` Volume persistent ist und alle Festplattengeräte wieder verfügbar sind.

Installieren Sie Docker für StorageGRID

Erfahren Sie, wie Sie Docker für StorageGRID installieren.

Gehen Sie wie folgt vor, um Docker zu installieren:

Schritte

1. Konfigurieren Sie den yum repo für Docker.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. Installieren Sie die benötigten Pakete.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Starten Sie Docker.

```
sudo systemctl start docker
```

4. Docker Testen.

```
sudo docker run hello-world
```

5. Stellen Sie sicher, dass Docker beim Systemstart ausgeführt wird.

```
sudo systemctl enable docker
```

Vorbereiten der Node-Konfigurationsdateien für StorageGRID

Erfahren Sie, wie Sie die Node-Konfigurationsdateien für StorageGRID vorbereiten.

Die Node-Konfiguration umfasst im allgemeinen die folgenden Schritte:

Schritte

1. Erstellen Sie das `/etc/storagegrid/nodes` Verzeichnis auf allen Hosts.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. Erstellen Sie die erforderlichen Dateien pro physischem Host, um sie dem Layout von Container/Node-Typ anzupassen. In diesem Beispiel haben wir zwei Dateien pro physischem Host auf jedem Hostcomputer erstellt.

> Der Name der Datei definiert den tatsächlichen Node-Namen für die Installation. Wird zum Beispiel `dc1-adm1.conf` zu einem Knoten mit dem Namen `dc1-adm1`.

— Host1:
`dc1-adm1.conf`
`dc1-sn1.conf`

— Host2:
`dc1-gw1.conf`
`dc1-sn2.conf`

— Host3:
`dc1-gw2.conf`
`dc1-sn3.conf`

Vorbereiten der Node-Konfigurationsdateien

Die folgenden Beispiele verwenden das `/dev/disk/by-path` Format. Sie können die korrekten Pfade überprüfen, indem Sie die folgenden Befehle ausführen:

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

Und diese Befehle:

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

Beispiel für primären Admin-Node

Beispiel für einen Dateinamen:

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

Inhalt der Beispieldatei:

> Festplattenpfade können den folgenden Beispielen folgen oder Stilnamen verwenden `/dev/mapper/alias` . Verwenden Sie keine Blockgerätnamen, z. B. `/dev/sdb` weil sie sich beim Neustart ändern können und das Raster beschädigen können.

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Beispiel für einen Storage-Node

Beispiel für einen Dateinamen:

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

Inhalt der Beispieldatei:

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

Beispiel für Gateway Node

Beispiel für einen Dateinamen:

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

Inhalt der Beispieldatei:

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Installieren von StorageGRID-Abhängigkeiten und -Paketen

Erfahren Sie, wie Sie StorageGRID-Abhängigkeiten und -Pakete installieren.

Um die StorageGRID-Abhängigkeiten und -Pakete zu installieren, führen Sie die folgenden Befehle aus:

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

Validieren Sie die StorageGRID-Konfigurationsdateien

Erfahren Sie, wie Sie den Inhalt der Konfigurationsdateien für StorageGRID validieren.

Nachdem Sie die Konfigurationsdateien in für jeden Ihrer StorageGRID Nodes erstellt `/etc/storagegrid/nodes` haben, müssen Sie den Inhalt dieser Dateien validieren.

Um den Inhalt der Konfigurationsdateien zu validieren, führen Sie folgenden Befehl auf jedem Host aus:

```
sudo storagegrid node validate all
```

Wenn die Dateien korrekt sind, wird in der Ausgabe für jede Konfigurationsdatei ÜBERGEBEN angezeigt:

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Wenn die Konfigurationsdateien nicht korrekt sind, werden die Probleme als WARNUNG und FEHLER angezeigt. Wenn Konfigurationsfehler gefunden werden, müssen Sie sie korrigieren, bevor Sie mit der Installation fortfahren.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Starten Sie den StorageGRID Host Service

Erfahren Sie, wie Sie den StorageGRID Host Service starten.

Um die StorageGRID-Nodes zu starten und sicherzustellen, dass sie nach einem Neustart des Hosts neu gestartet werden, müssen Sie den StorageGRID-Hostdienst aktivieren und starten.

Führen Sie zum Starten des StorageGRID Host Service die folgenden Schritte aus.

Schritte

1. Führen Sie auf jedem Host folgende Befehle aus:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

   Der Startvorgang kann bei der ersten Ausführung einige Zeit in Anspruch nehmen.

2. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Bereitstellung fortgesetzt wird:

```
sudo storagegrid node status node-name
```

3. Führen Sie für jeden Knoten, der den Status oder zurückgibt `Not-Running` `Stopped`, den folgenden Befehl aus:

```
sudo storagegrid node start node-name
```

   Beispielsweise würden Sie angesichts der folgenden Ausgabe den Node starten `dc1-adm1` :

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. Wenn Sie den StorageGRID-Host-Service bereits aktiviert und gestartet haben (oder wenn Sie nicht sicher sind, ob der Service aktiviert und gestartet wurde), führen Sie auch den folgenden Befehl aus:

```
sudo systemctl reload-or-restart storagegrid
```

Konfigurieren Sie den Grid-Manager in StorageGRID

Erfahren Sie, wie Sie den Grid-Manager in StorageGRID auf dem primären Admin-Node konfigurieren.

Schließen Sie die Installation ab, indem Sie das StorageGRID-System über die Grid Manager-Benutzeroberfläche auf dem primären Admin-Node konfigurieren.

Allgemeine Schritte

Das Konfigurieren des Grids und das Abschließen der Installation umfassen die folgenden Aufgaben:

Schritte

1. Navigieren Sie zu Grid Manager
2. "Geben Sie die StorageGRID Lizenzinformationen an"
3. "Fügen Sie Sites zu StorageGRID hinzu"
4. "Subnetze für das Grid-Netzwerk angeben"
5. "Ausstehende Grid-Nodes genehmigen"
6. "Geben Sie die NTP-Serverinformationen an"
7. "Geben Sie die Serverinformationen des DNS-Systems an"
8. "Geben Sie die Passwörter für das StorageGRID-System an"
9. "Überprüfung der Konfiguration und vollständige Installation"

Navigieren Sie zu Grid Manager

Definieren Sie mit dem Grid Manager alle Informationen, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Bevor Sie beginnen, muss der primäre Admin-Node bereitgestellt und die erste Startsequenz abgeschlossen sein.

Führen Sie die folgenden Schritte aus, um mit Grid Manager Informationen zu definieren.

Schritte

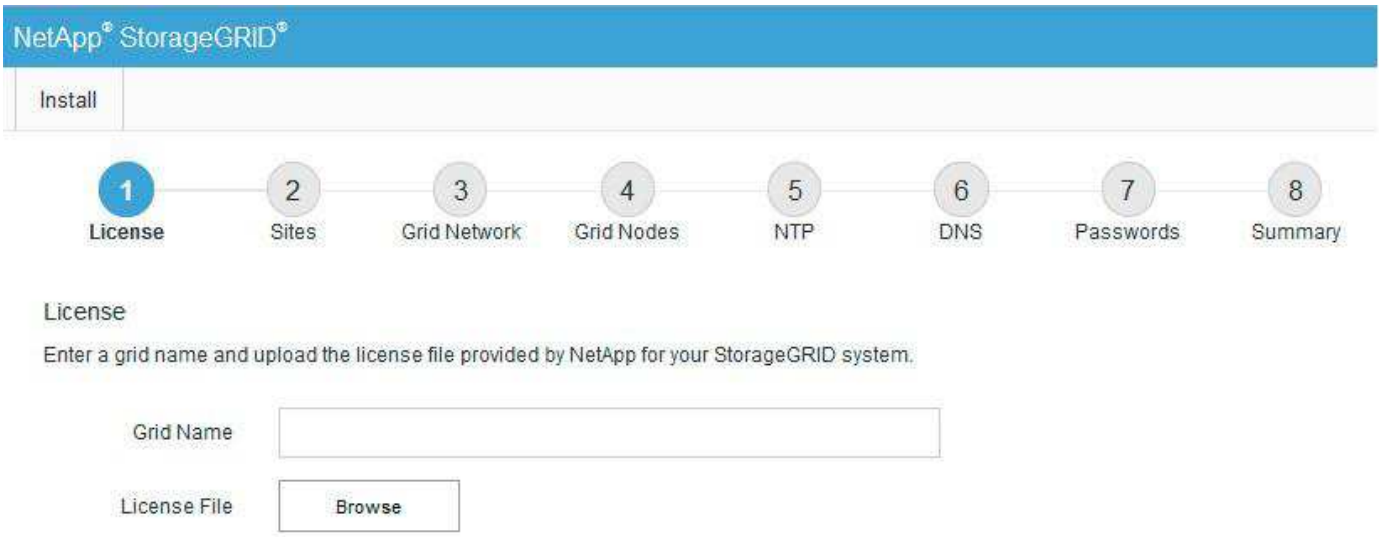
1. Greifen Sie über die folgende Adresse auf den Grid Manager zu:

   ```
   https://primary_admin_node_grid_ip
   ```

   Alternativ können Sie auf den Grid Manager auf Port 8443 zugreifen.

   ```
   https://primary_admin_node_ip:8443
   ```

2. Klicken Sie auf StorageGRID-System installieren. Die Seite, die zum Konfigurieren eines StorageGRID-Rasters verwendet wird, wird angezeigt.



Details zur StorageGRID-Lizenz hinzufügen

Erfahren Sie, wie Sie die StorageGRID Lizenzdatei hochladen.

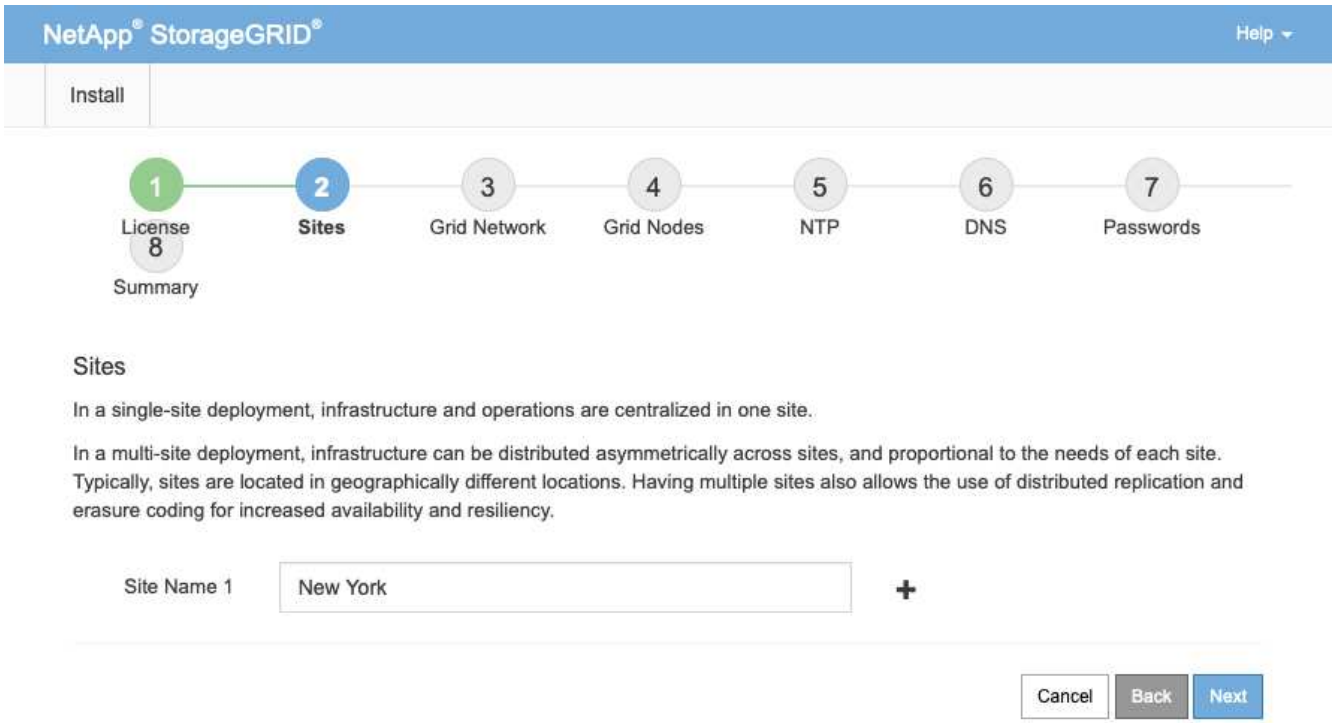
Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Gehen Sie wie folgt vor, um die StorageGRID-Lizenzinformationen anzugeben:

Schritte

1. Geben Sie auf der Lizenzseite im Feld Rastername einen Namen für Ihr StorageGRID-System ein. Nach der Installation wird der Name als oberste Ebene in der Grid-Topologiestruktur angezeigt.
2. Klicken Sie auf Durchsuchen, suchen Sie die NetApp-Lizenzdatei (`NLF-unique-id.txt`) und klicken Sie auf Öffnen. Die Lizenzdatei wird validiert, die Seriennummer und die lizenzierte Speicherkapazität werden angezeigt.

> Das StorageGRID Installationsarchiv enthält eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet. Sie können nach der Installation auf eine Lizenz aktualisieren, die Support bietet.



3. Klicken Sie Auf Weiter.

Fügen Sie Sites zu StorageGRID hinzu

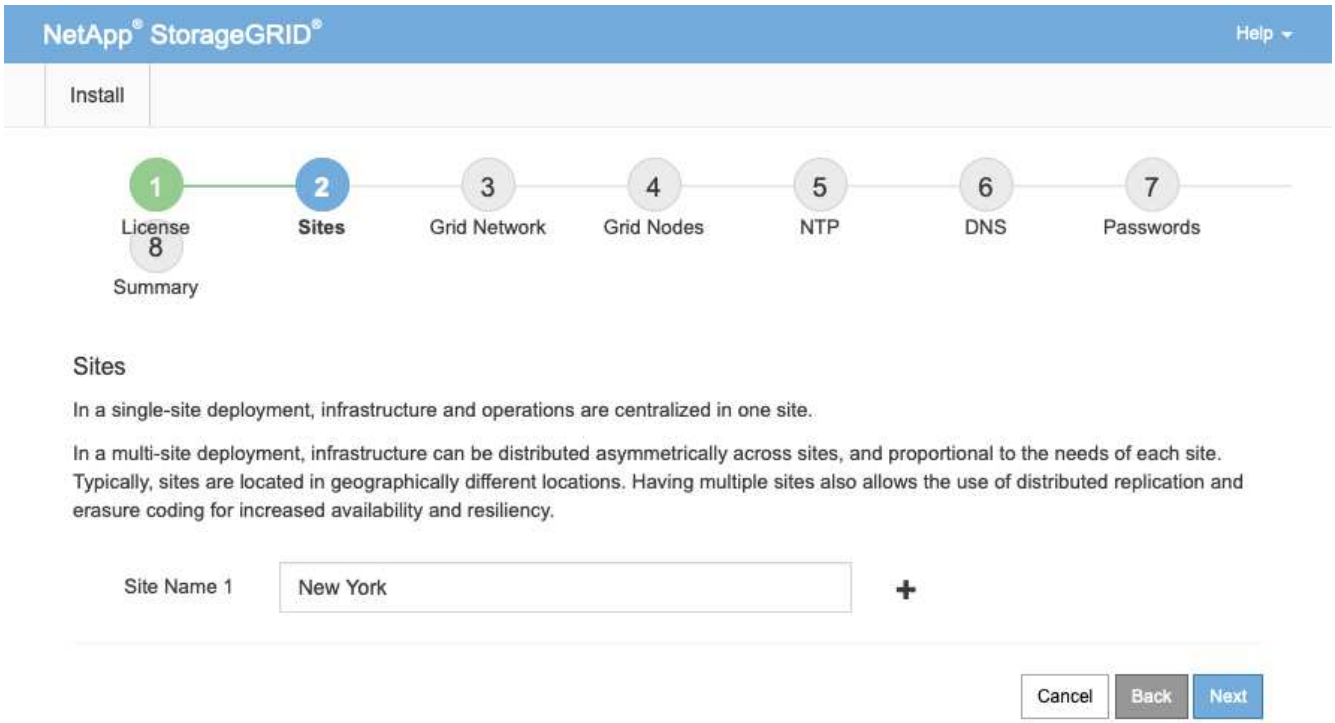
Erfahren Sie, wie Sie StorageGRID Standorte hinzufügen, um die Zuverlässigkeit und Storage-Kapazität zu verbessern.

Wenn Sie StorageGRID installieren, müssen Sie mindestens einen Standort erstellen. Sie können weitere Standorte erstellen, um die Zuverlässigkeit und Storage-Kapazität Ihres StorageGRID Systems zu erhöhen.

So fügen Sie Sites hinzu:

Schritte

1. Geben Sie auf der Seite Sites den Standortnamen ein.
2. Um weitere Sites hinzuzufügen, klicken Sie auf das Pluszeichen neben dem letzten Standorteintrag, und geben Sie den Namen in das Textfeld „Neuer Standortname“ ein. Fügen Sie so viele zusätzliche Standorte wie für Ihre Grid-Topologie hinzu. Sie können bis zu 16 Standorte hinzufügen.



3. Klicken Sie Auf Weiter.

Grid-Netzwerk-Subnetze für StorageGRID angeben

Erfahren Sie, wie Sie die Grid-Netzwerk-Subnetze für StorageGRID konfigurieren.

Sie müssen die Subnetze angeben, die im Grid-Netzwerk verwendet werden.

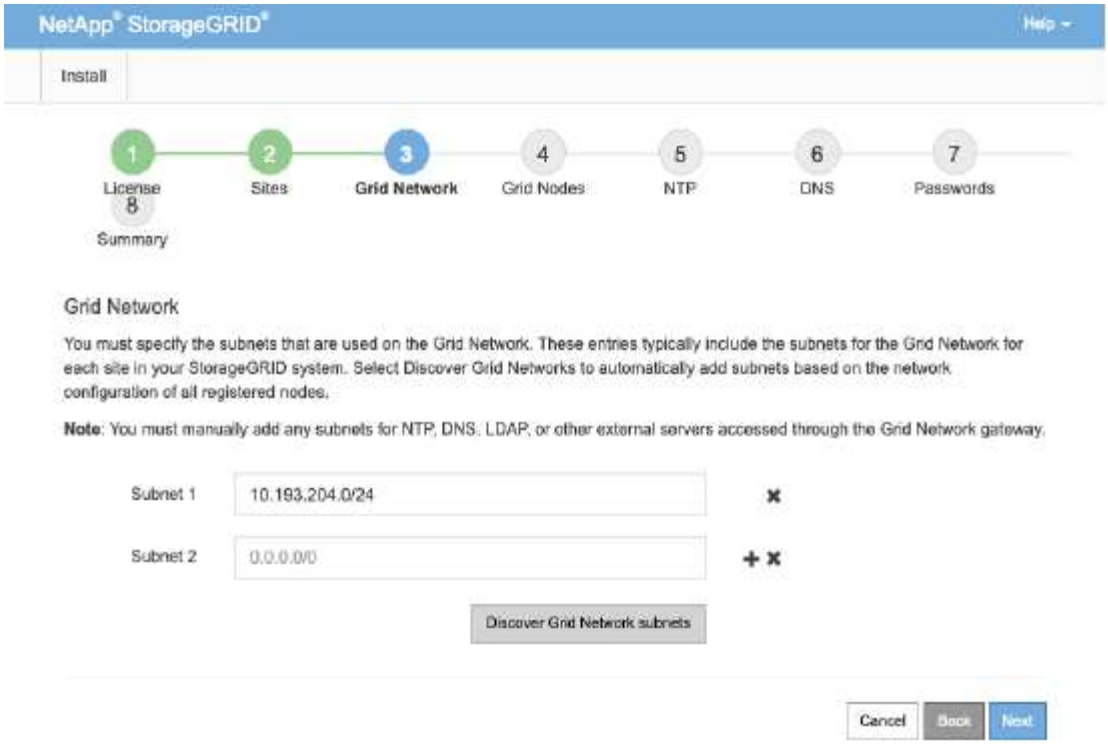
Die Subnetzeinträge umfassen die Subnetze für das Grid-Netzwerk für jeden Standort im StorageGRID-System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen (z. B. die Subnetze, auf denen Ihre NTP-Server gehostet werden).

Wenn Sie mehrere Grid-Subnetze haben, ist das Grid-Netzwerk-Gateway erforderlich. Alle angegebenen Grid-Subnetze müssen über dieses Gateway erreichbar sein.

Führen Sie die folgenden Schritte aus, um Subnetze für das Grid-Netzwerk anzugeben:

Schritte

1. Geben Sie im Textfeld Subnetz 1 die CIDR-Netzwerkadresse für mindestens ein Grid-Netzwerk an.
2. Klicken Sie auf das Pluszeichen neben dem letzten Eintrag, um einen zusätzlichen Netzwerkeintrag hinzuzufügen. Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf Subnetze von Grid Networks ermitteln, um die Subnetzliste des Grid-Netzwerks automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die bei Grid Manager registriert sind.



3. Klicken Sie Auf Weiter.

Grid-Nodes für StorageGRID genehmigen

Erfahren Sie, wie Sie ausstehende Grid-Nodes, die dem StorageGRID-System beitreten, prüfen und genehmigen.

Sie müssen jeden Grid-Node genehmigen, bevor er dem StorageGRID-System Beitritt.

Bevor Sie beginnen, müssen alle Grid-Nodes der virtuellen und StorageGRID-Appliance implementiert werden.

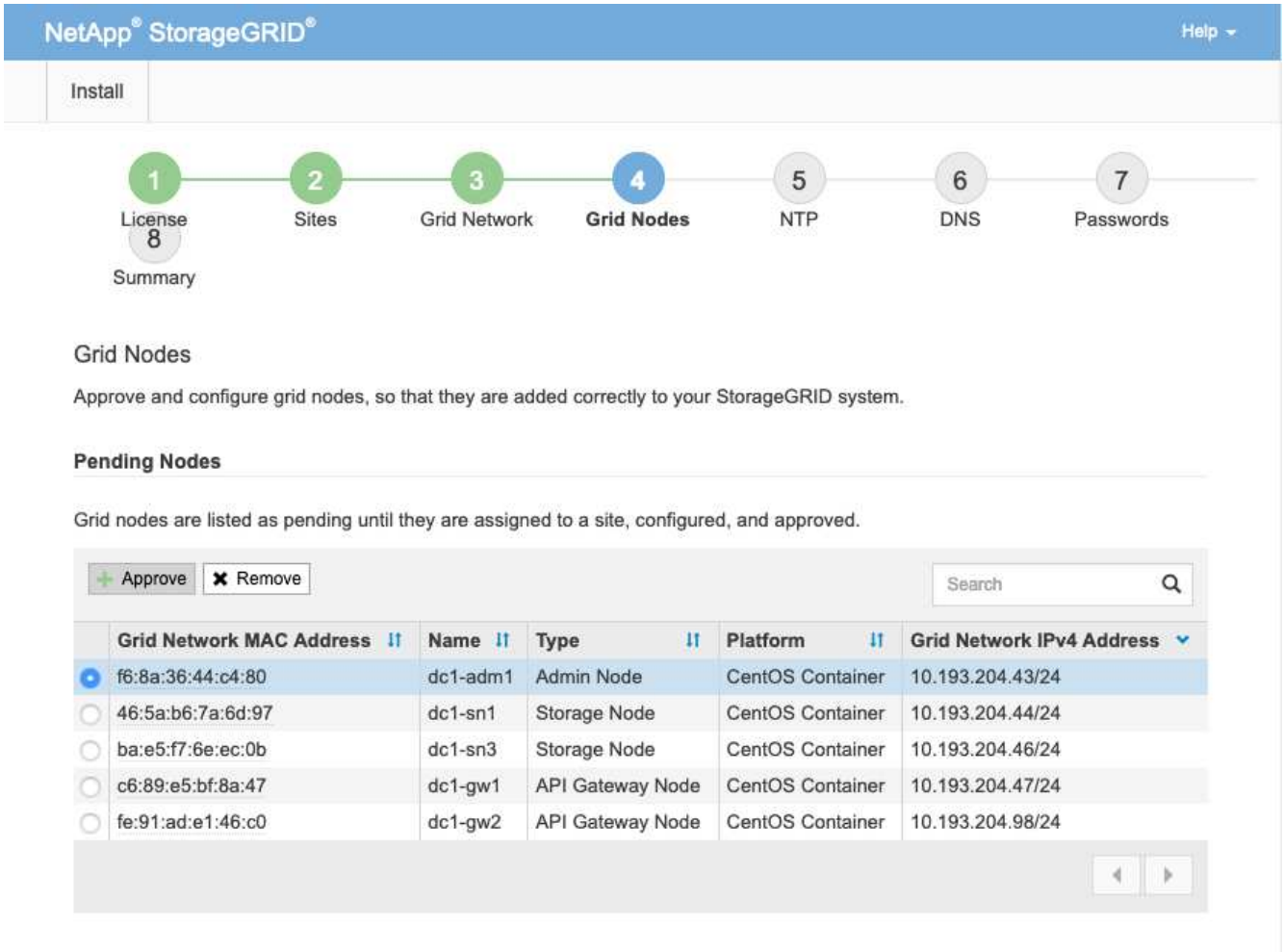
Führen Sie die folgenden Schritte aus, um ausstehende Rasterknoten zu genehmigen:

Schritte

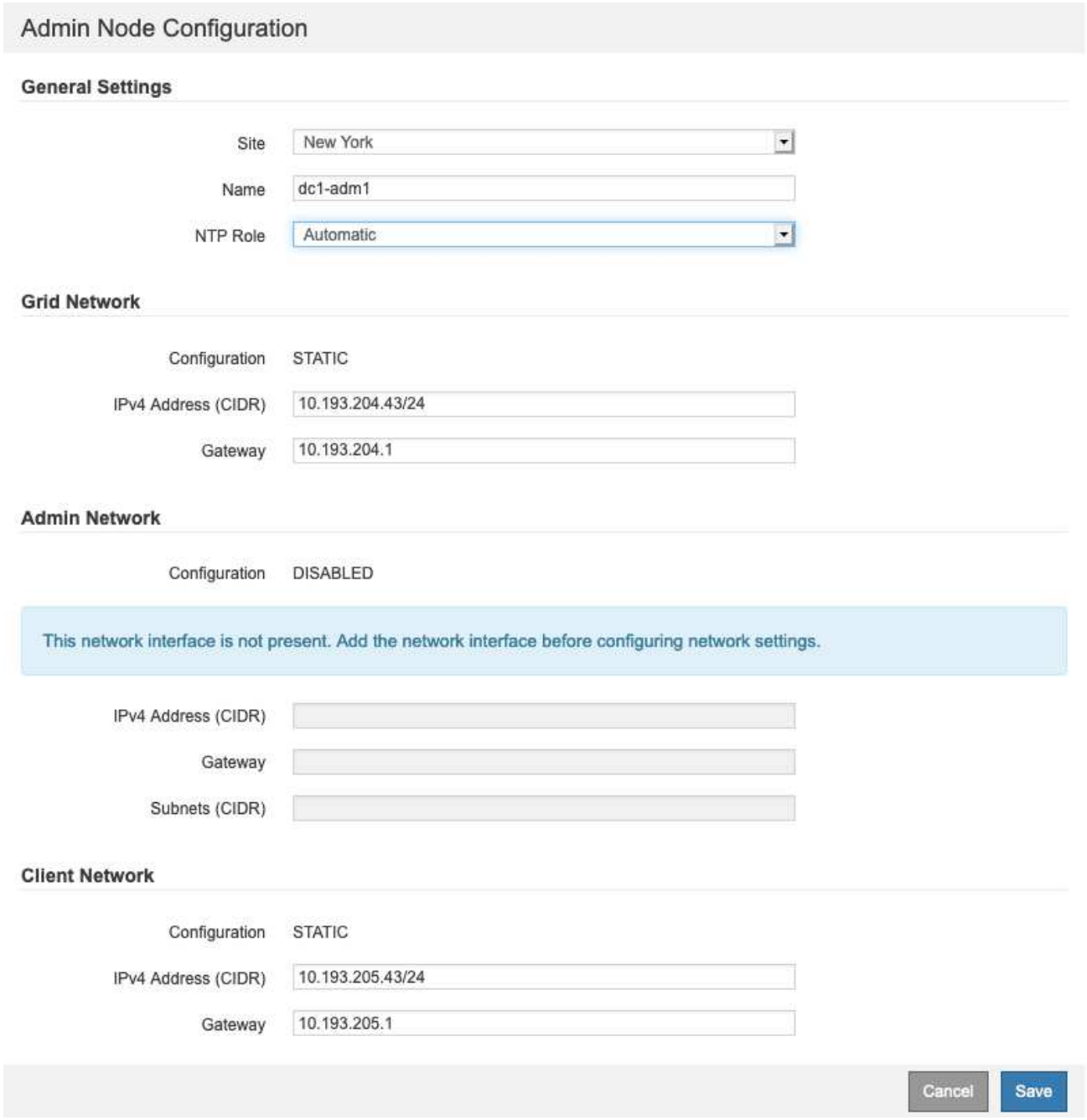
1. Überprüfen Sie die Liste Ausstehende Knoten, und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

   Wenn ein Grid-Node fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

2. Klicken Sie auf das Optionsfeld neben einem ausstehenden Knoten, den Sie genehmigen möchten.



3. Klicken Sie Auf Genehmigen.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften nach Bedarf.



— **Standort**: Der Systemname des Standorts für diesen Grid-Knoten.

— **Name**: Der Hostname, der dem Knoten zugewiesen wird, und der Name, der im Grid-Manager angezeigt wird. Der Name wird standardmäßig mit dem Namen verwendet, den Sie während der Node-Bereitstellung angegeben haben. Sie können den Namen jedoch bei Bedarf ändern.

— **NTP-Rolle**: Die NTP-Rolle des Grid-Knotens. Die Optionen lauten automatisch, Primär und Client. Durch Auswahl der Option automatisch wird die primäre Rolle den Administratorknoten, den Speicher-Nodes mit ADC-Diensten (Administrative Domain Controller), den Gateway-Nodes und allen Grid-Nodes mit nicht statischen IP-Adressen zugewiesen. Allen anderen Grid-Nodes wird die Client-Rolle zugewiesen.

Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

— **ADC-Dienst (nur Speicher-Nodes)**: Wählen Sie automatisch, damit das System bestimmen kann, ob der Knoten den ADC-Dienst benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Speicherknoten an jedem Standort müssen den ADC-Dienst enthalten. Der ADC-Dienst kann nicht einem Node hinzugefügt werden, nachdem er bereitgestellt wurde.

5. Ändern Sie in Grid Network die Einstellungen für die folgenden Eigenschaften nach Bedarf:

   — **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Netzschnittstelle (eth0 im Container). `192.168.1.234/24`Beispiel: .

   — **Gateway**: Das Grid Network Gateway. `192.168.0.1`Beispiel: .

   Wenn mehrere Grid-Subnetze vorhanden sind, ist das Gateway erforderlich.

   Wenn Sie DHCP für die Grid-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Node konfiguriert. Stellen Sie sicher, dass sich die resultierende IP-Adresse nicht in einem DHCP-Adressenpool befindet.

6. Um das Admin-Netzwerk für den Grid-Knoten zu konfigurieren, fügen Sie die Einstellungen im Abschnitt Admin-Netzwerk nach Bedarf hinzu oder aktualisieren Sie diese.

   Geben Sie die Zielsubnetze der Routen aus dieser Schnittstelle in das Textfeld Subnetze (CIDR) ein. Wenn es mehrere Admin-Subnetze gibt, ist das Admin-Gateway erforderlich.

   Wenn Sie für die Netzwerkkonfiguration für den Admin DHCP ausgewählt haben und diesen Wert hier ändern, wird der neue Wert als statische Adresse auf dem Node konfiguriert. Stellen Sie sicher, dass sich die resultierende IP-Adresse nicht in einem DHCP-Adressenpool befindet.

   Appliances: Wenn bei einer StorageGRID-Appliance das Admin-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Dialogfeld des Grid-Managers konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

   a. Starten Sie die Appliance neu: Wählen Sie im Installationsprogramm der Appliance die Option MENU:Advanced[Neustart]. Ein Neustart kann mehrere Minuten dauern.
   b. Wählen Sie MENU:Configure Networking [Link Configuration], und aktivieren Sie die entsprechenden Netzwerke.
   c. Wählen Sie MENU:Configure Networking[IP Configuration], und konfigurieren Sie die aktivierten Netzwerke.
   d. Kehren Sie zur Startseite zurück, und klicken Sie auf Installation starten.
   e. Im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.
   f. Entfernen Sie den Knoten aus der Tabelle Ausstehende Knoten.
   g. Warten Sie, bis der Knoten wieder in der Liste Ausstehende Knoten angezeigt wird.

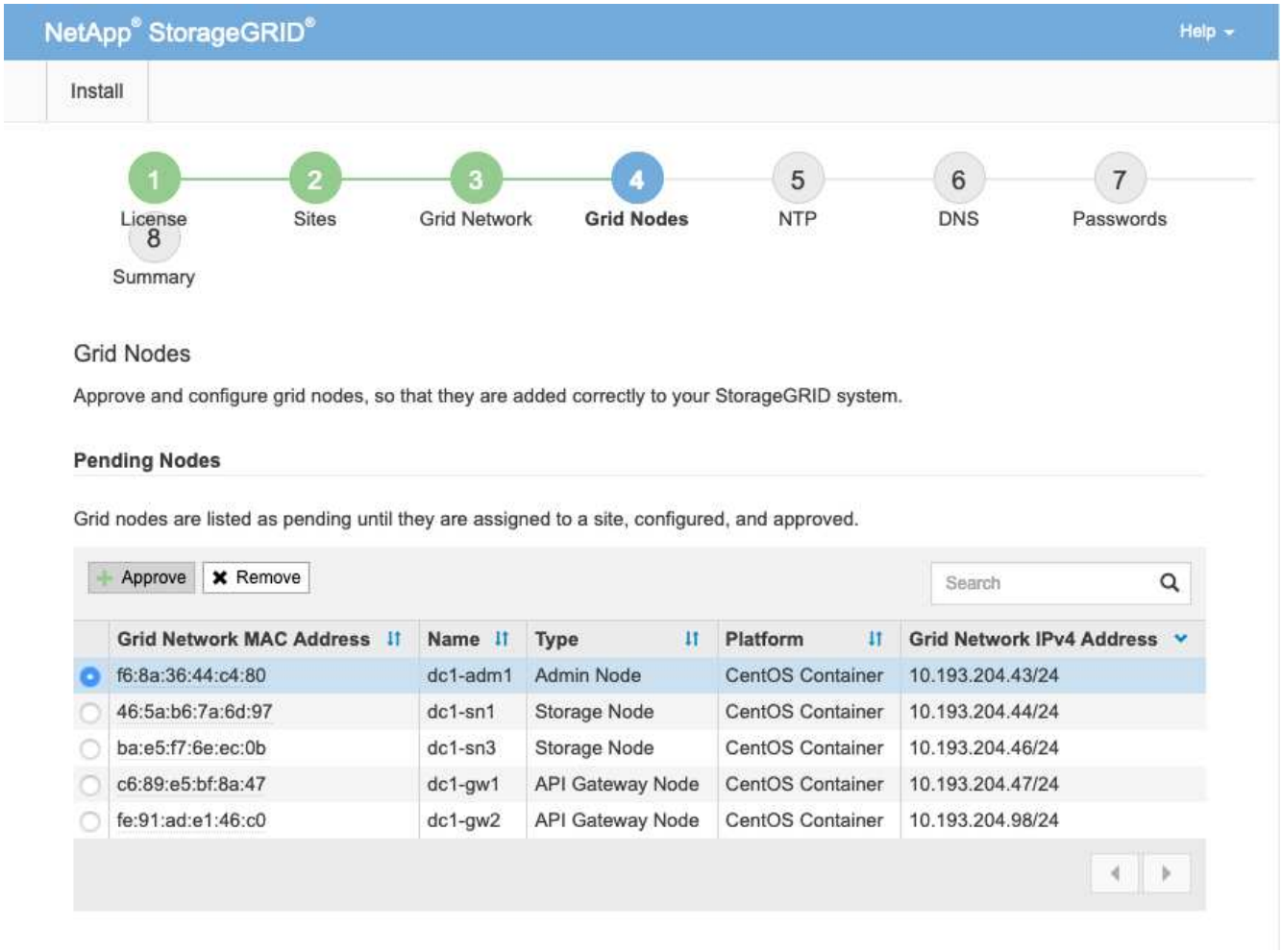
h. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration angegeben haben. Weitere Informationen finden Sie in der Installations- und Wartungsanleitung für Ihr Gerätemodell.

7. Wenn Sie das Client-Netzwerk für den Grid-Node konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt Client-Netzwerk nach Bedarf hinzu oder aktualisieren Sie sie. Wenn das Client-Netzwerk konfiguriert ist, ist das Gateway erforderlich, und es wird nach der Installation zum Standard-Gateway für den Node.

   Appliances: Wenn bei einer StorageGRID-Appliance das Clientnetzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Dialogfeld des Grid-Managers konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

   a. Starten Sie die Appliance neu: Wählen Sie im Installationsprogramm der Appliance die Option MENU:Advanced[Neustart]. Ein Neustart kann mehrere Minuten dauern.
   b. Wählen Sie MENU:Configure Networking [Link Configuration], und aktivieren Sie die entsprechenden Netzwerke.
   c. Wählen Sie MENU:Configure Networking[IP Configuration], und konfigurieren Sie die aktivierten Netzwerke.
   d. Kehren Sie zur Startseite zurück, und klicken Sie auf Installation starten.
   e. Im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.
   f. Entfernen Sie den Knoten aus der Tabelle Ausstehende Knoten.
   g. Warten Sie, bis der Knoten wieder in der Liste Ausstehende Knoten angezeigt wird.
   h. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration angegeben haben. Weitere Informationen finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

8. Klicken Sie auf Speichern . Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



9. Wiederholen Sie die Schritte 1-8 für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

   Sie müssen alle Knoten genehmigen, die Sie im Raster benötigen. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Seite Zusammenfassung auf Installieren klicken. Um die Eigenschaften eines genehmigten Gitterknotens zu ändern, klicken Sie auf das entsprechende Optionsfeld und anschließend auf Bearbeiten.

10. Wenn Sie die Genehmigung für Rasterknoten abgeschlossen haben, klicken Sie auf Weiter.

Geben Sie NTP-Serverdetails für StorageGRID an

Erfahren Sie, wie Sie NTP-Konfigurationsinformationen für Ihr StorageGRID-System angeben, damit Vorgänge auf separaten Servern synchronisiert werden können.

Um Probleme mit Zeitabweichungen zu vermeiden, müssen Sie vier externe NTP-Serverreferenzen von Stratum 3 oder höher angeben.

> Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer Windows-Version als Windows Server 2016. Der Zeitdienst in früheren Versionen von Windows ist nicht ausreichend genau und wird von Microsoft nicht für den Einsatz in anspruchsvollen Umgebungen wie StorageGRID unterstützt.

Die externen NTP-Server werden von den Nodes verwendet, denen Sie zuvor die primären NTP-Rollen

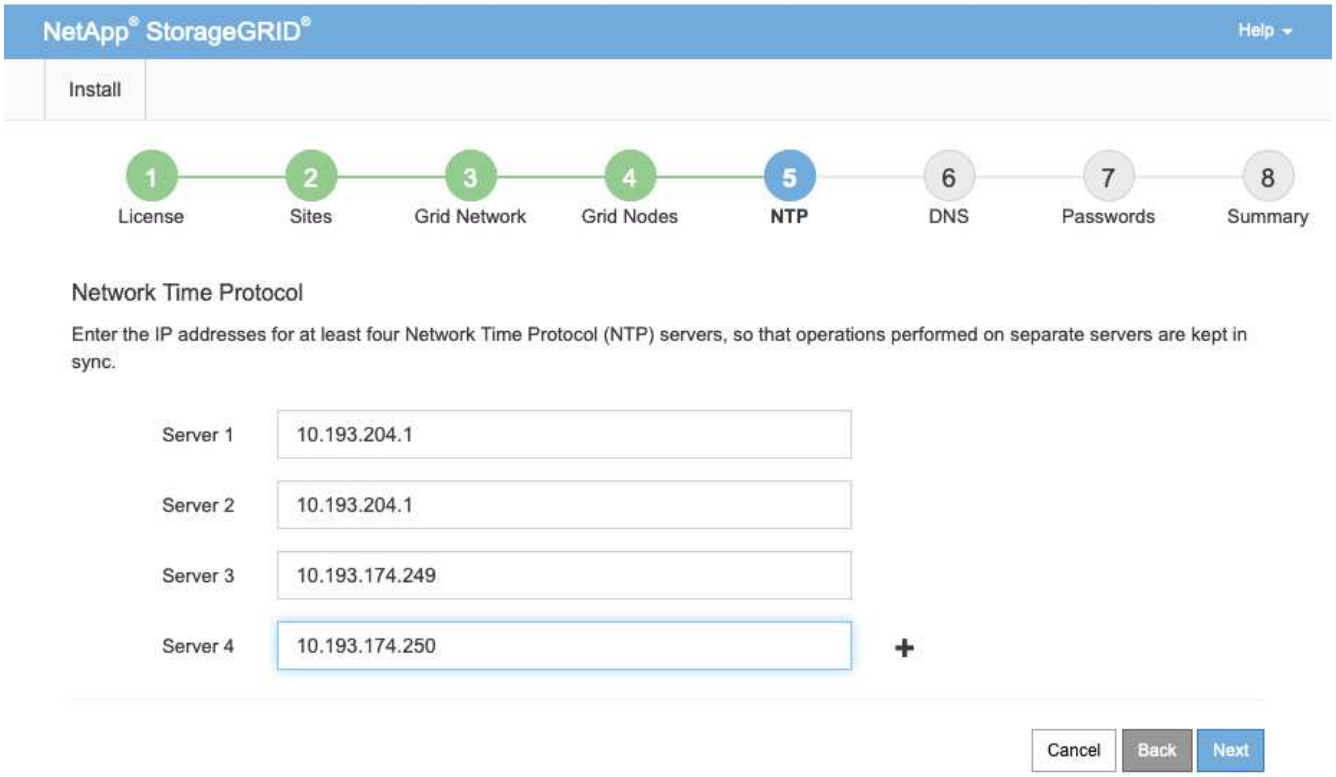
zugewiesen haben.

> Das Client-Netzwerk wird im Installationsvorgang nicht früh genug aktiviert, um die einzige Quelle für NTP-Server zu sein. Stellen Sie sicher, dass mindestens ein NTP-Server über das Grid-Netzwerk oder das Admin-Netzwerk erreicht werden kann.

Führen Sie die folgenden Schritte aus, um NTP-Serverinformationen anzugeben:

Schritte

1. Geben Sie in den Textfeldern Server 1 bis Server 4 die IP-Adressen für mindestens vier NTP-Server an.
2. Klicken Sie bei Bedarf auf das Pluszeichen neben dem letzten Eintrag, um weitere Servereinträge hinzuzufügen.



3. Klicken Sie Auf Weiter.

Geben Sie Details zum DNS-Server für StorageGRID an

Erfahren Sie, wie Sie den DNS-Server für StorageGRID konfigurieren.

Sie müssen die DNS-Informationen für Ihr StorageGRID-System angeben, damit Sie mithilfe von Hostnamen anstelle von IP-Adressen auf externe Server zugreifen können.

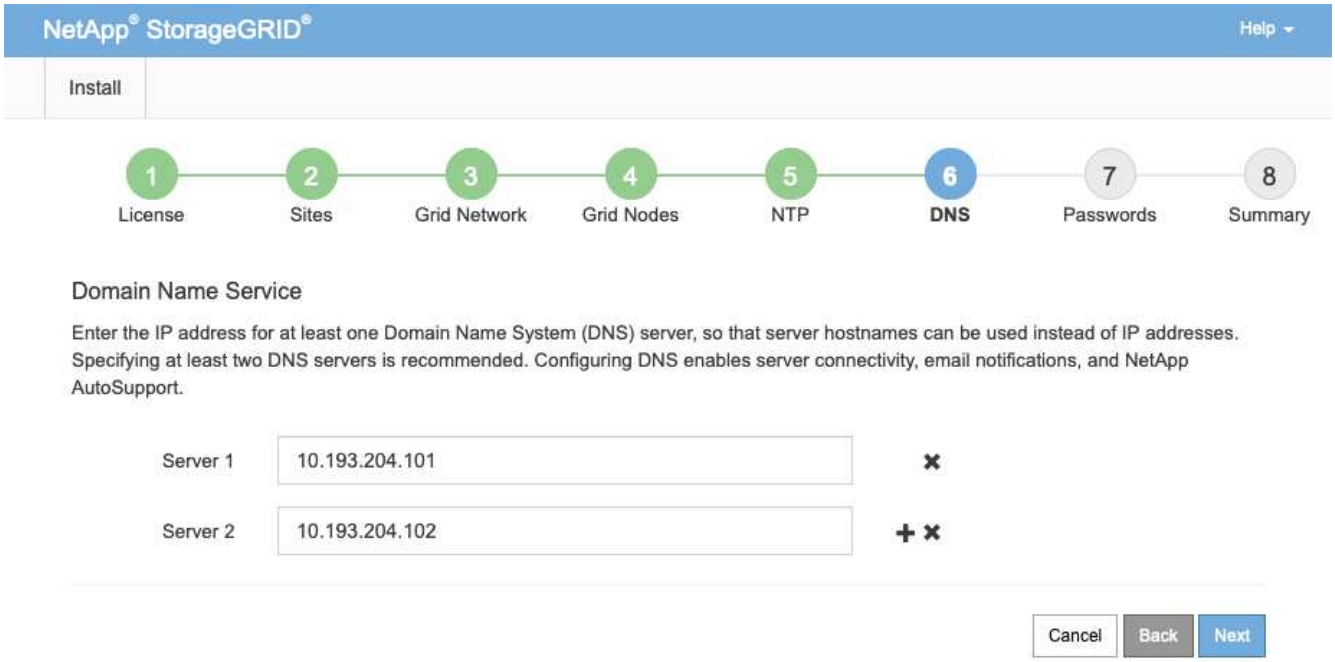
Durch die Angabe von DNS-Serverinformationen können Sie vollständig qualifizierte Domänennamen (FQDN) statt IP-Adressen für E-Mail-Benachrichtigungen und NetApp AutoSupport®-Nachrichten verwenden. NetApp empfiehlt die Angabe von mindestens zwei DNS-Servern.

Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet.

Führen Sie die folgenden Schritte aus, um DNS-Serverinformationen anzugeben:

Schritte

1. Geben Sie im Textfeld Server 1 die IP-Adresse für einen DNS-Server an.
2. Klicken Sie bei Bedarf auf das Pluszeichen neben dem letzten Eintrag, um weitere Server hinzuzufügen.



3. Klicken Sie Auf Weiter.

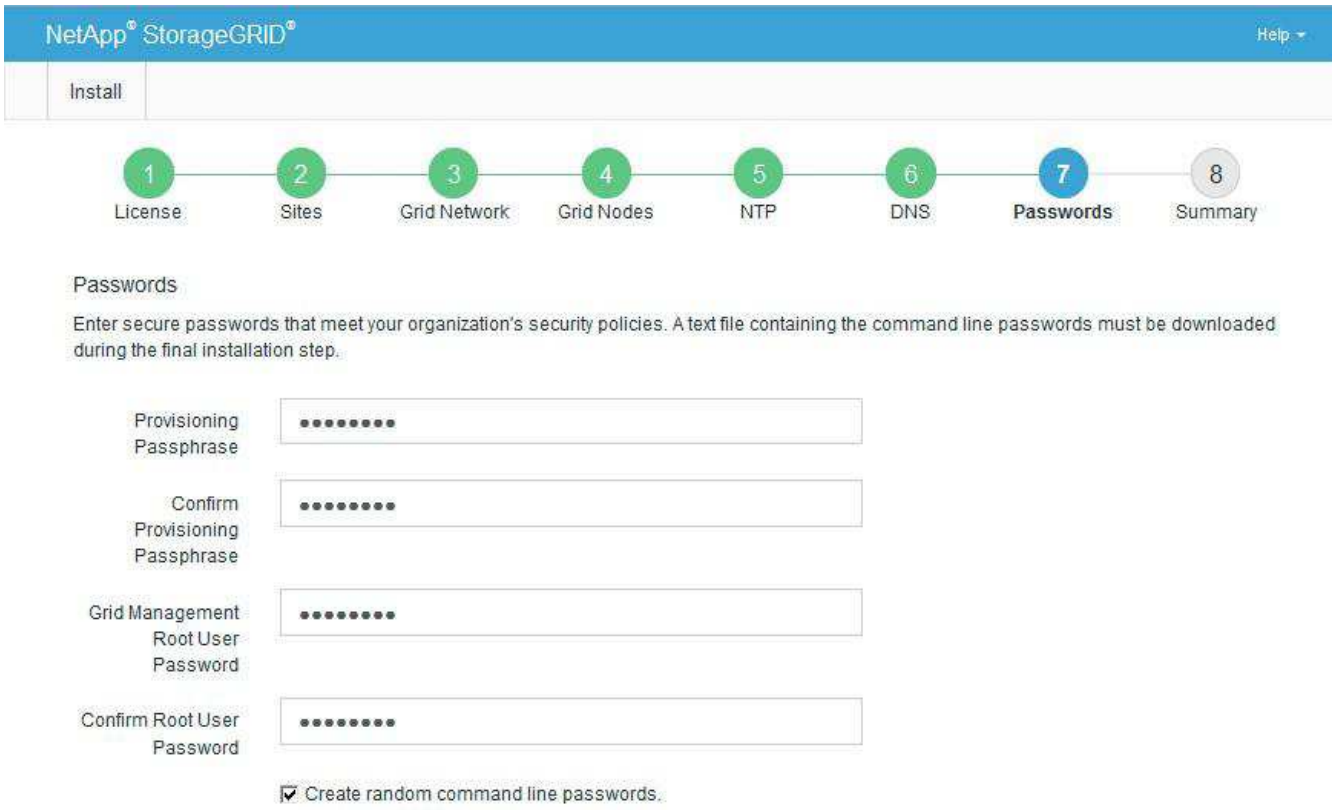
Geben Sie die Systemkennwörter für StorageGRID an

Erfahren Sie, wie Sie Ihr StorageGRID-System sichern, indem Sie die Passphrase für das Provisioning und das Root-Benutzerpasswort für das Grid-Management festlegen.

So geben Sie die Passwörter ein, die zum Schutz Ihres StorageGRID-Systems verwendet werden sollen:

Schritte

1. Geben Sie in Provisioning Passphrase die Provisionierungs-Passphrase ein, die für Änderungen an der Grid-Topologie des StorageGRID-Systems erforderlich ist. Sie sollten dieses Kennwort an einem sicheren Ort speichern.
2. Geben Sie unter Provisionierungspassphrase bestätigen die Provisionierungs-Passphrase erneut ein.
3. Geben Sie unter Grid Management Root User Password das Passwort ein, das für den Zugriff auf Grid Manager als Root-Benutzer verwendet werden soll.
4. Geben Sie unter Root-Benutzerpasswort bestätigen das Grid Manager-Kennwort erneut ein.



5. Wenn Sie ein Raster für Proof-of-Concept- oder Demo-Zwecke installieren, deaktivieren Sie die Option „Random Command Line Passwords erstellen“.

   Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Deaktivieren Sie die Option Random Command Line Passwords erstellen nur für Demo-Raster, wenn Sie Standardpasswörter verwenden möchten, um über die Befehlszeile mithilfe des Root- oder Administratorkontos auf Grid-Nodes zuzugreifen.

   Wenn Sie auf der Seite Zusammenfassung auf Installieren klicken, werden Sie aufgefordert, die Wiederherstellungspaket-Datei herunterzuladen (`sgws-recovery-packageid-revision.zip`). Sie müssen diese Datei herunterladen, um die Installation abzuschließen. Die Passwörter für den Zugriff auf das System werden in der in der Recovery Package-Datei enthaltenen Datei gespeichert `Passwords.txt` .

6. Klicken Sie Auf Weiter.

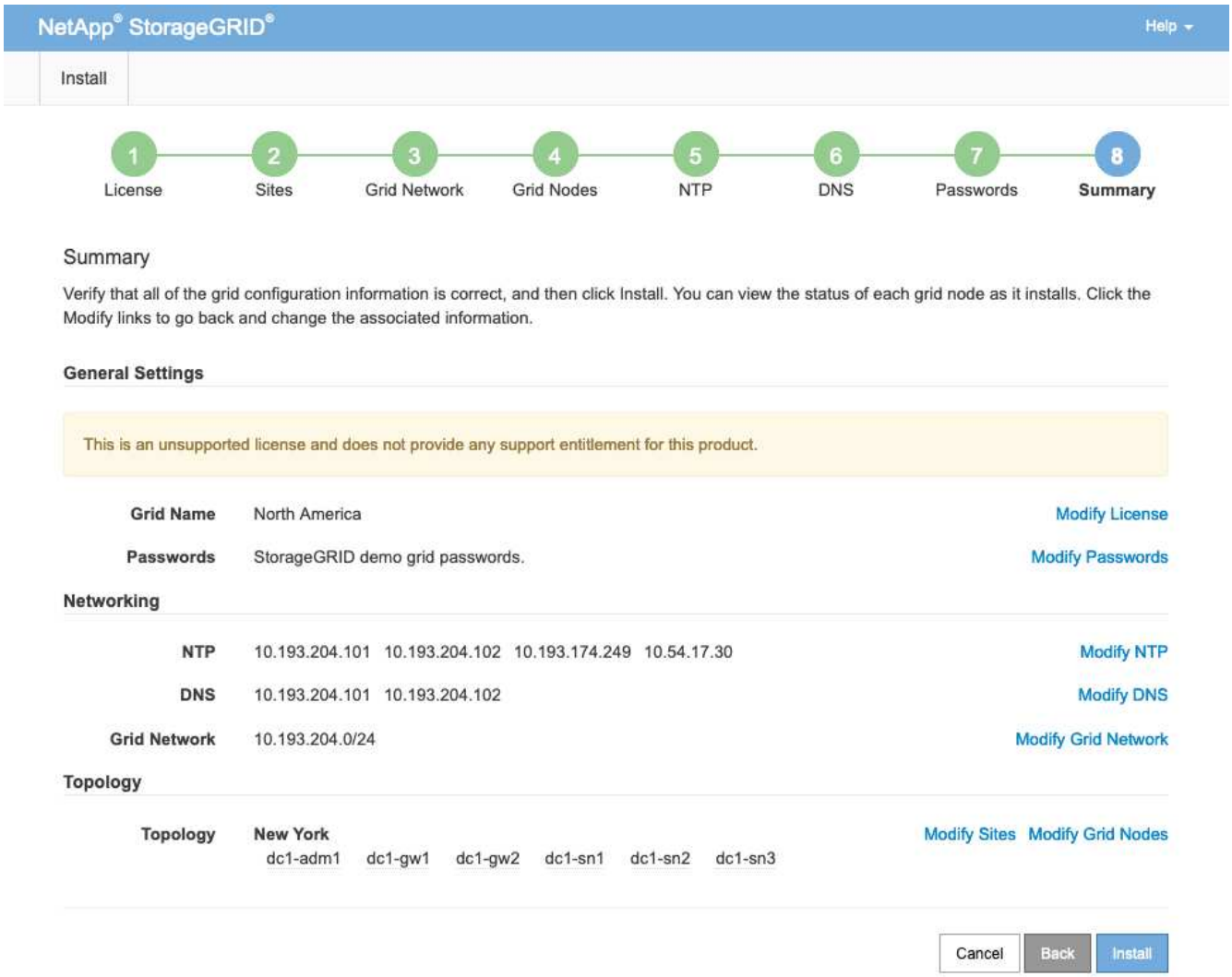
Überprüfen Sie die Konfiguration und schließen Sie die StorageGRID Installation ab

Erfahren Sie, wie Sie die Grid-Konfigurationsinformationen validieren und den StorageGRID Installationsprozess abschließen.

Um sicherzustellen, dass die Installation erfolgreich abgeschlossen wird, überprüfen Sie die von Ihnen eingegebenen Konfigurationsinformationen sorgfältig. Auszuführende Schritte:

Schritte

1. Zeigen Sie die Übersichtsseite an.



2. Vergewissern Sie sich, dass alle Informationen zur Grid-Konfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite Zusammenfassung, um zurück zu gehen und Fehler zu beheben.
3. Klicken Sie Auf Installieren.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf Installieren klicken. Wenn die Verbindung unterbrochen wird, stellen Sie sicher, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Weitere Informationen finden Sie unter „Netzwerkinstallation und -Bereitstellung“.

4. Klicken Sie Auf Wiederherstellungspaket Herunterladen.

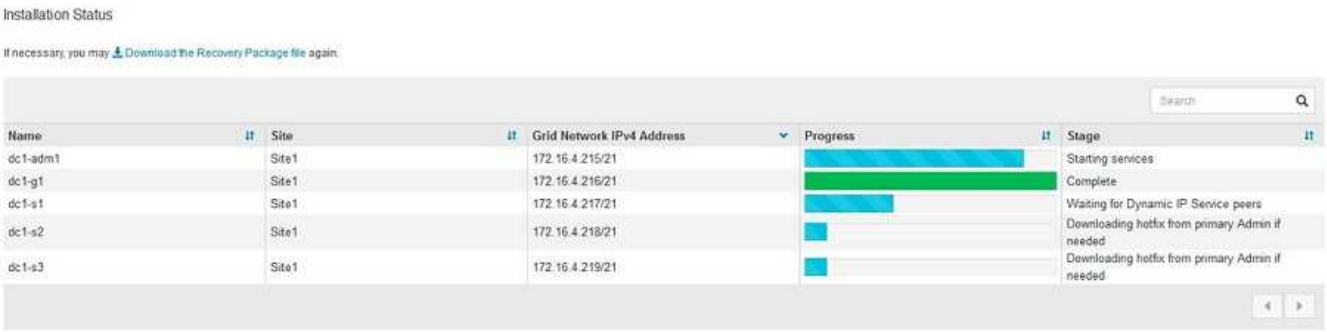
   Wenn die Installation bis zu dem Punkt fortschreitet, an dem die Rastertopologie definiert ist, werden Sie aufgefordert, die Wiederherstellungspaket-Datei herunterzuladen (`.zip`) und zu bestätigen, dass Sie auf den Inhalt dieser Datei zugreifen können. Sie müssen die Wiederherstellungspaket-Datei herunterladen, damit Sie das StorageGRID-System wiederherstellen können, falls ein oder mehrere Grid-Nodes ausfallen.

   Vergewissern Sie sich, dass Sie den Inhalt der Datei extrahieren und anschließend an zwei sicheren und separaten Speicherorten speichern können `.zip` .

Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

5. Wählen Sie die Option Ich habe die Wiederherstellungspaket-Datei erfolgreich heruntergeladen und verifiziert, und klicken Sie dann auf Weiter.

Wenn die Installation noch läuft, wird die Seite Installationsstatus geöffnet. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



Wenn die komplette Phase für alle Grid-Knoten erreicht ist, wird die Anmeldeseite für Grid Manager geöffnet.

6. Melden Sie sich beim Grid Manager als Root-Benutzer mit dem Passwort an, das Sie bei der Installation angegeben haben.

Upgrade von Bare-Metal-Nodes in StorageGRID

Erfahren Sie mehr über den Upgrade-Prozess für Bare-Metal-Nodes in StorageGRID.

Der Upgrade-Prozess für Bare-Metal-Nodes unterscheidet sich von dem für Appliances oder VMware Nodes. Bevor Sie ein Upgrade eines Bare-Metal-Knotens durchführen, müssen Sie zunächst die RPM-Dateien auf allen Hosts aktualisieren, bevor Sie das Upgrade über die GUI ausführen.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

Jetzt können Sie mit dem Software-Upgrade über die GUI fortfahren.

TR-4907: Konfigurieren Sie StorageGRID mit veritas Enterprise Vault

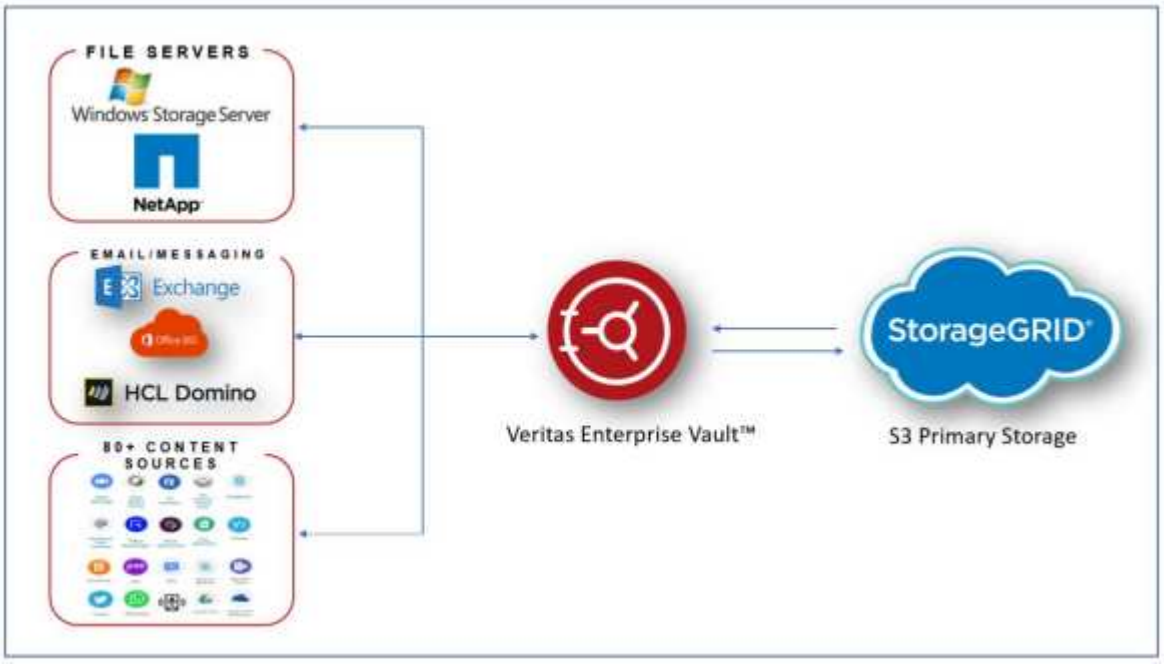
Einführung in die Konfiguration von StorageGRID für Site Failover

Erfahren Sie, wie veritas Enterprise Vault StorageGRID als primäres Storage-Ziel für Disaster Recovery verwendet.

Diese Konfigurationsanleitung enthält die Schritte zur Konfiguration von NetApp® StorageGRID® als primäres Speicherziel mit veritas Enterprise Vault. Es wird auch beschrieben, wie StorageGRID für ein Standort-Failover in einem Disaster Recovery-Szenario (DR) konfiguriert wird.

Referenzarchitektur von NetApp dar

StorageGRID bietet ein lokales, S3-kompatibles Cloud-Backup-Ziel für veritas Enterprise Vault. Die folgende Abbildung zeigt die Architektur von veritas Enterprise Vault und StorageGRID.



Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/

- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Konfigurieren Sie StorageGRID und veritas Enterprise Vault

Erfahren Sie, wie Sie grundlegende Konfigurationen für StorageGRID 11.5 oder höher und veritas Enterprise Vault 14.1 oder höher implementieren.

Dieser Konfigurationsleitfaden basiert auf StorageGRID 11.5 und Enterprise Vault 14.1. Für WORM-Modus (Write Once, Read Many) wurde Storage mit S3 Object Lock, StorageGRID 11.6 und Enterprise Vault 14.2.2 verwendet. Weitere Details zu diesen Richtlinien finden Sie auf der "StorageGRID-Dokumentation" Seite oder bei einem StorageGRID Experten.

Voraussetzungen für die Konfiguration von StorageGRID und veritas Enterprise Vault

- Bevor Sie StorageGRID mit veritas Enterprise Vault konfigurieren, überprüfen Sie die folgenden Voraussetzungen:

> Für WORM Storage (Objektsperre) ist StorageGRID 11.6 oder höher erforderlich.

- veritas Enterprise Vault 14.1 oder höher ist installiert.

> Für WORM Storage (Object Lock) ist Enterprise Vault ab Version 14.2.2 erforderlich.

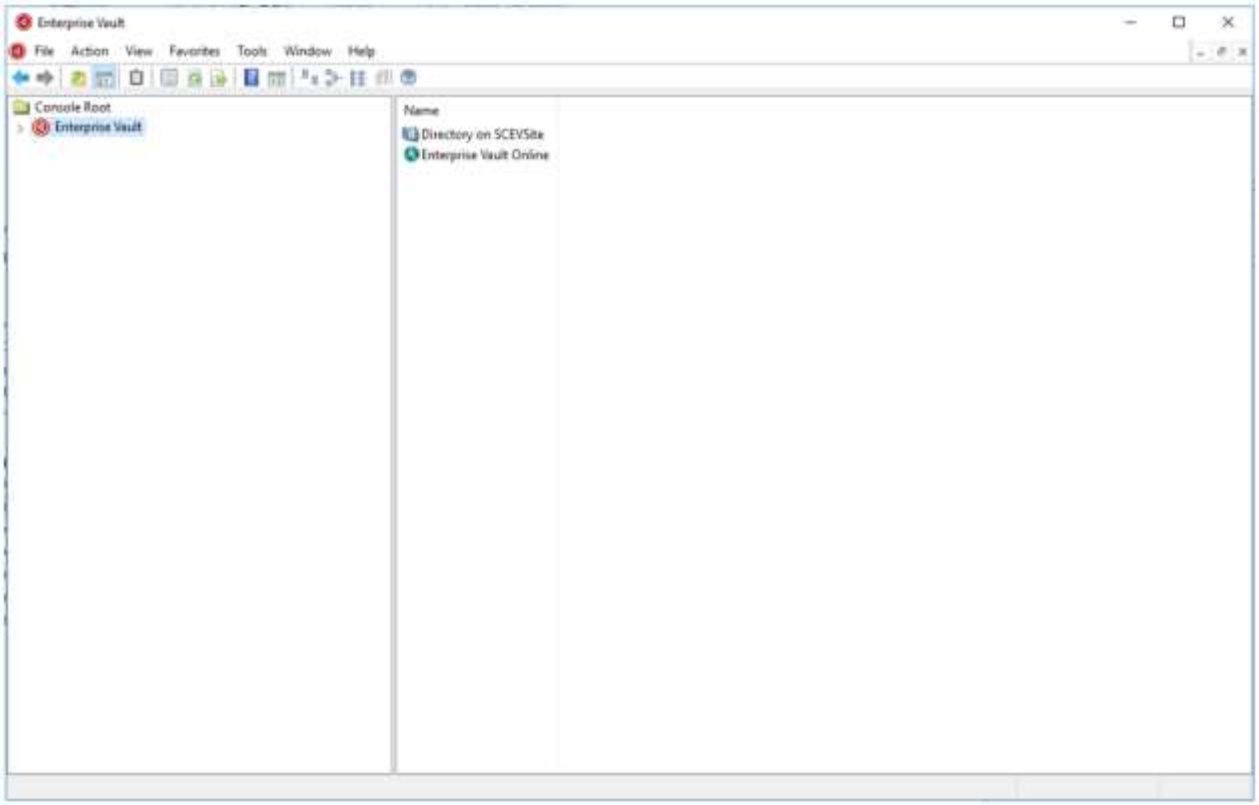
- Vault-Speichergruppen und ein Vault-Speicher wurden erstellt. Weitere Informationen finden Sie im veritas Enterprise Vault Administration Guide.
- Ein StorageGRID-Mandant, Zugriffsschlüssel, geheimer Schlüssel und Bucket wurden erstellt.
- Ein StorageGRID-Load-Balancer-Endpunkt wurde erstellt (entweder HTTP oder HTTPS).
- Wenn Sie ein selbstsigniertes Zertifikat verwenden, fügen Sie das selbstsignierte StorageGRID-CA-Zertifikat zu den Enterprise Vault-Servern hinzu. Weitere Informationen finden Sie in diesem "Artikel der veritas Knowledge Base".
- Aktualisieren Sie die aktuelle Enterprise Vault-Konfigurationsdatei, und wenden Sie sie an, um unterstützte Speicherlösungen wie NetApp StorageGRID zu ermöglichen. Weitere Informationen finden Sie in diesem "Artikel der veritas Knowledge Base".

Konfigurieren Sie StorageGRID mit veritas Enterprise Vault

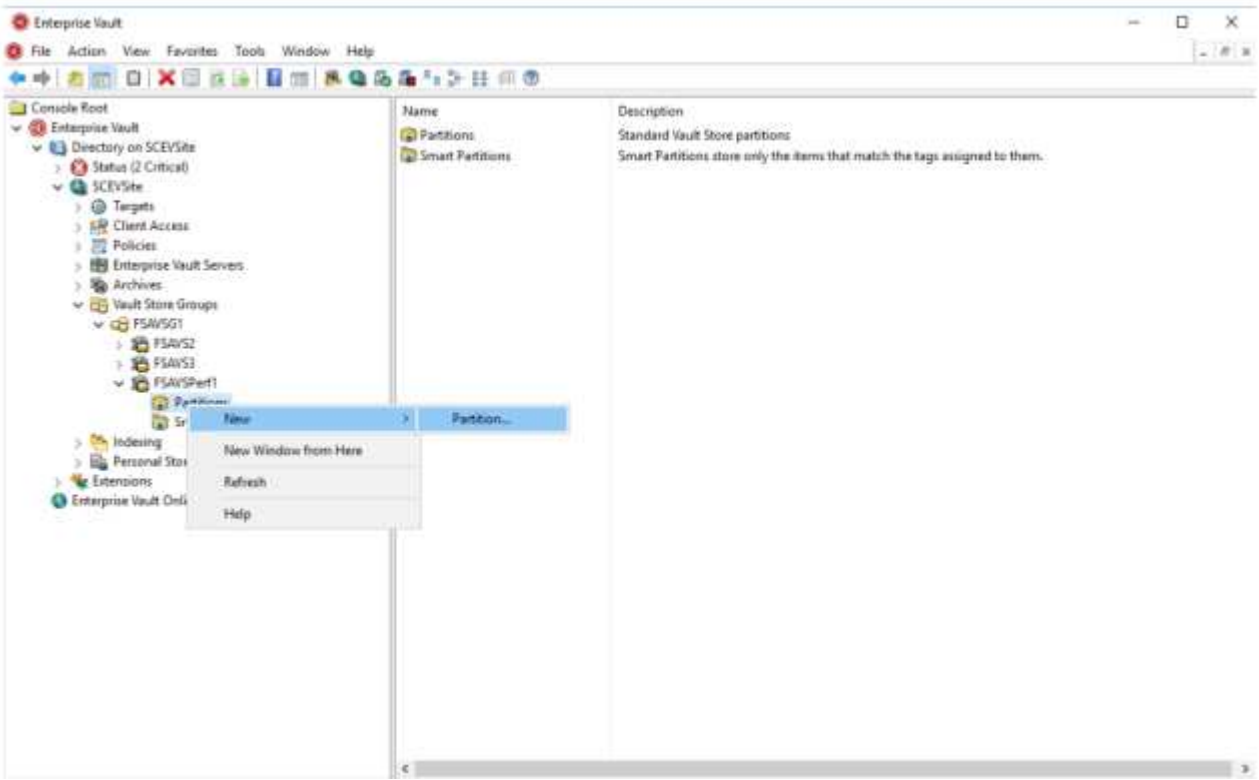
So konfigurieren Sie StorageGRID mit veritas Enterprise Vault:

Schritte

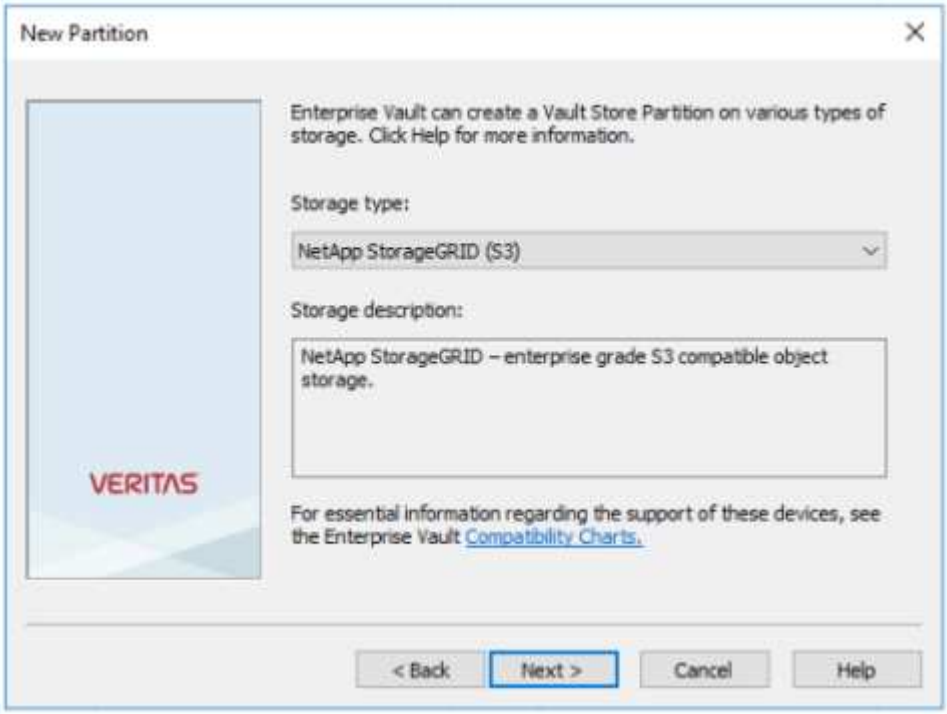
1. Starten Sie die Enterprise Vault Administration-Konsole.



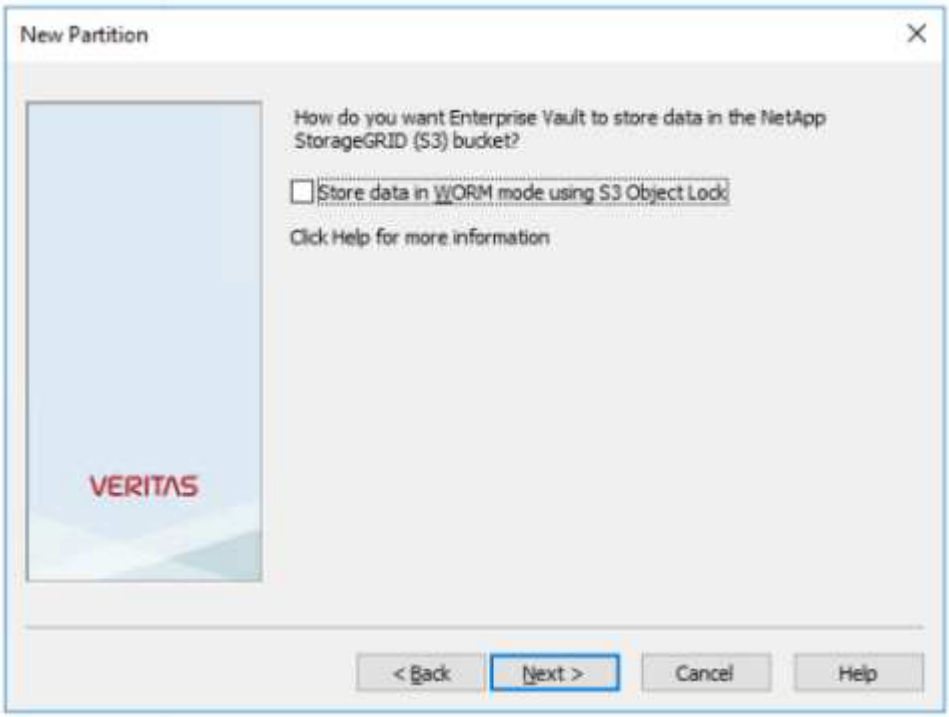
2. Erstellen Sie eine neue Vault-Speicherpartition im entsprechenden Vault-Speicher. Erweitern Sie den Ordner Vault Store Groups und anschließend den entsprechenden Vault-Speicher. Klicken Sie mit der rechten Maustaste auf Partition, und wählen Sie MENU:New[Partition].



3. Folgen Sie dem Assistenten zum Erstellen neuer Partitionen. Wählen Sie aus dem Dropdown-Menü Speichertyp die Option NetApp StorageGRID (S3) aus. Klicken Sie Auf Weiter.

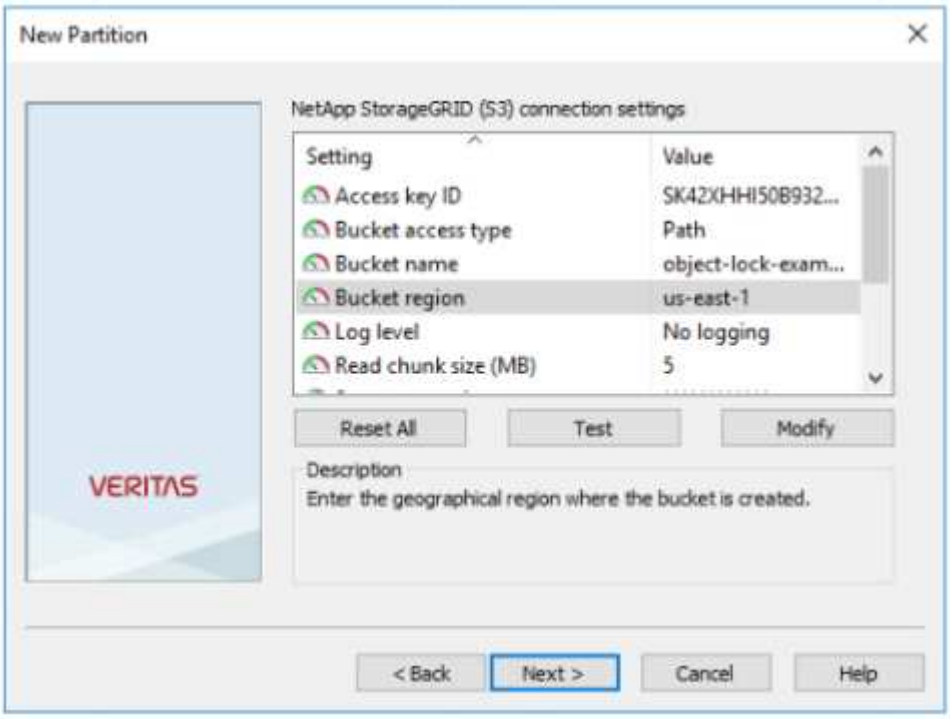


4. Lassen Sie die Option Daten im WORM-Modus mit S3 Objektsperre speichern deaktiviert. Klicken Sie Auf Weiter.

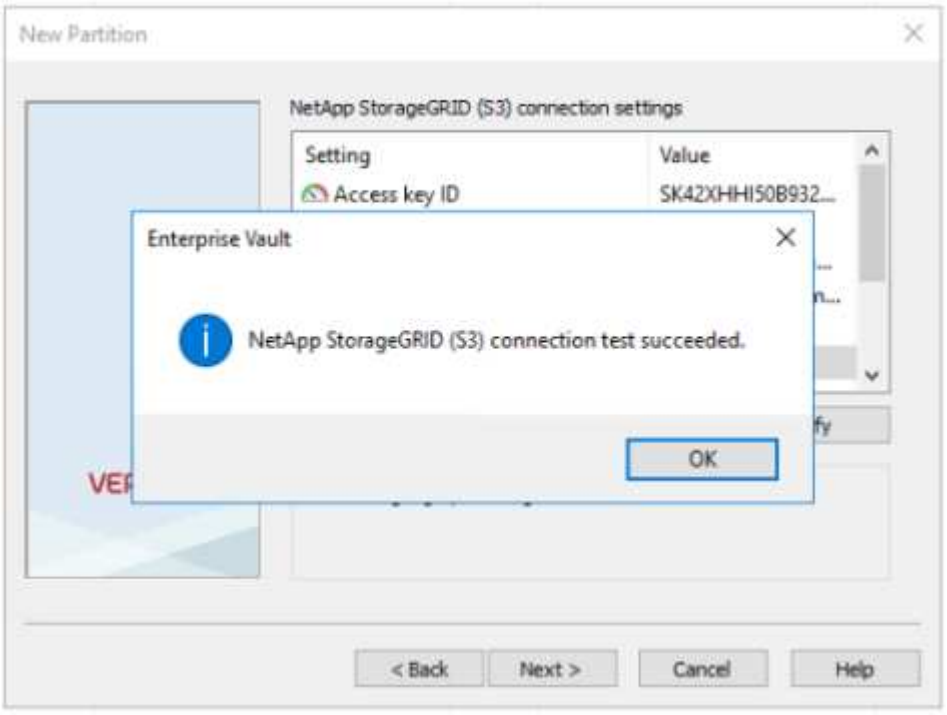


5. Geben Sie auf der Seite Verbindungseinstellungen folgende Informationen ein:
   - Zugriffsschlüssel-ID
   - Geheimer Zugriffsschlüssel
   - Service-Host-Name: Stellen Sie sicher, dass der in StorageGRID konfigurierte Load Balancer-Endpunkt (LBE)-Port (z. B. https://<hostname>:<LBE_port>) einbezogen wird.

- Bucket-Name: Name des zuvor erstellten Ziel-Buckets. veritas Enterprise Vault erstellt den Bucket nicht.
- Bucket-Region: `us-east-1` Ist der Standardwert.

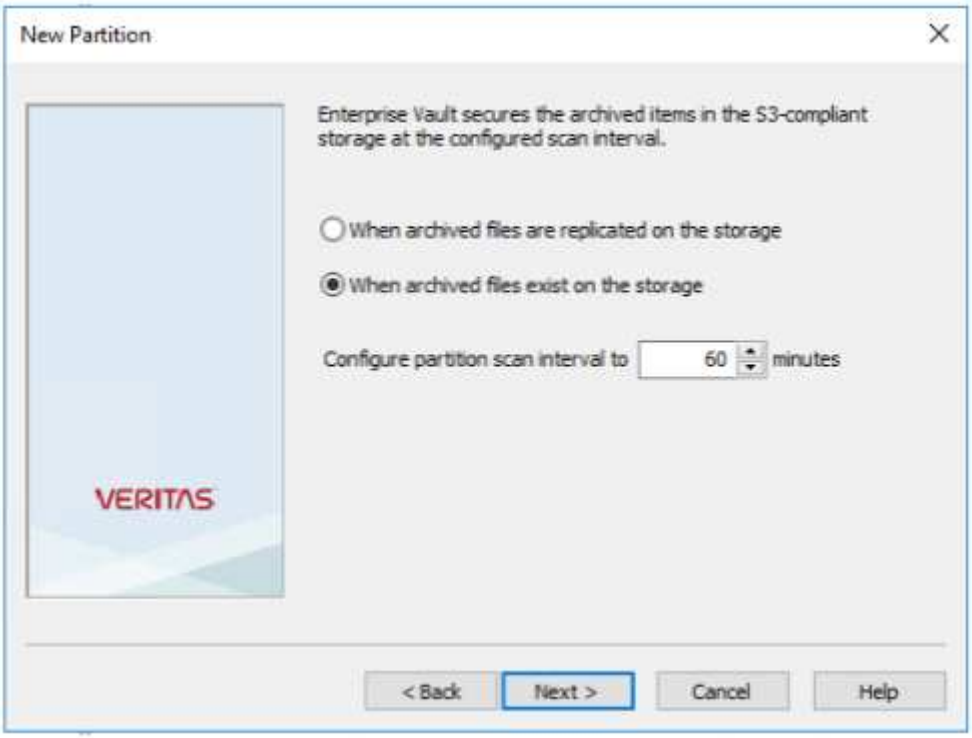


6. Um die Verbindung zum StorageGRID-Bucket zu überprüfen, klicken Sie auf Test. Überprüfen Sie, ob der Verbindungstest erfolgreich war. Klicken Sie auf OK und dann auf Weiter.

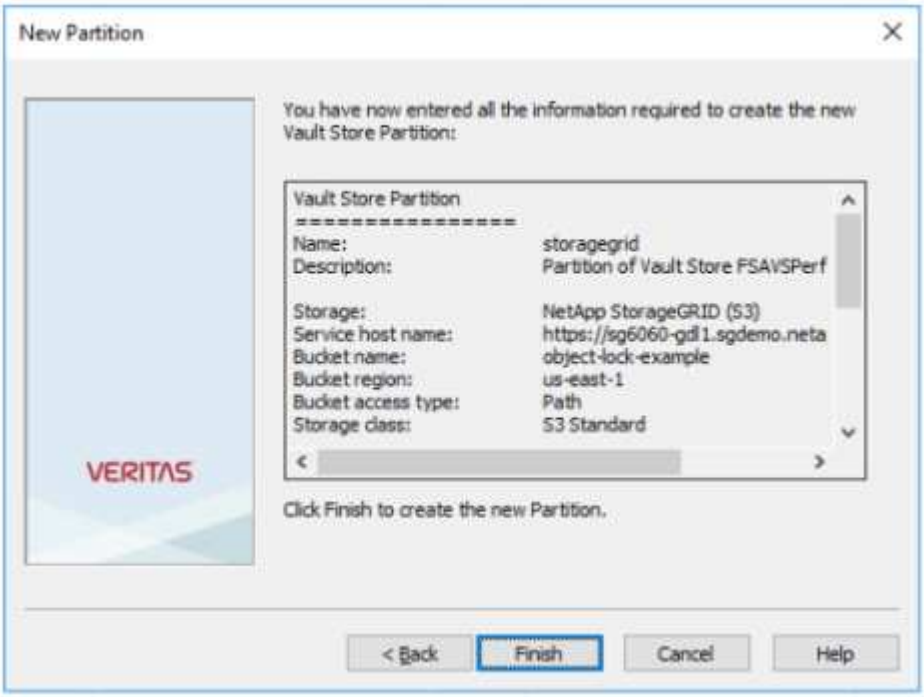


7. StorageGRID unterstützt den S3-Replizierungsparameter nicht. Zum Schutz Ihrer Objekte verwendet StorageGRID Regeln für Information Lifecycle Management (ILM), um Datensicherungsschemata festzulegen – mehrere Kopien oder Erasure Coding. Wählen Sie die Option Wenn archivierte Dateien im

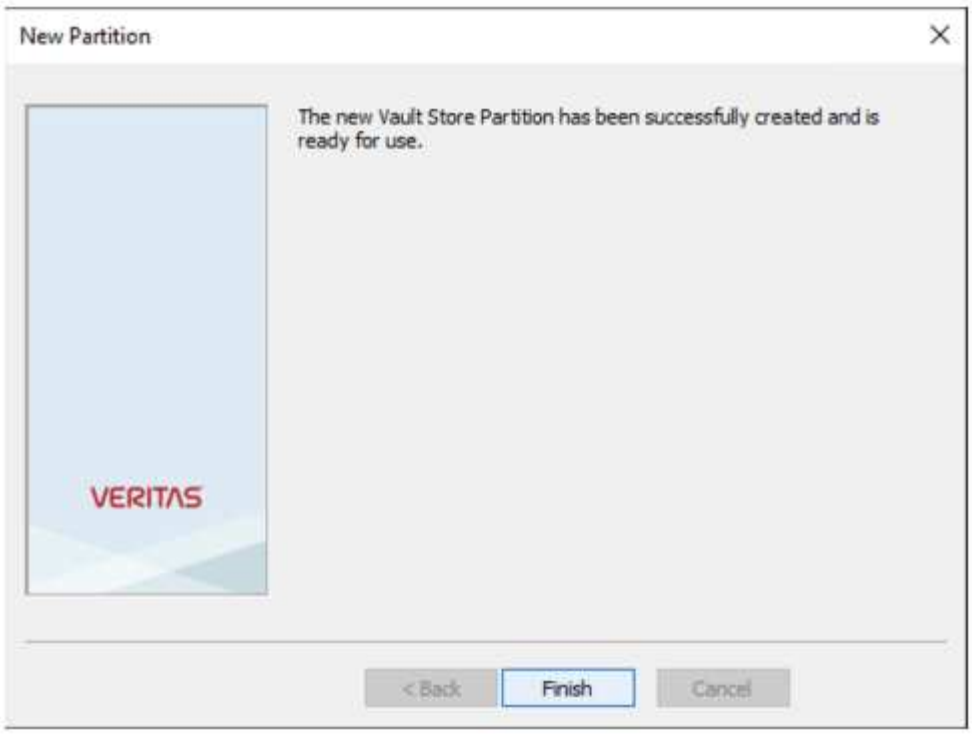
Speicher vorhanden sind aus, und klicken Sie auf Weiter.



8. Überprüfen Sie die Informationen auf der Übersichtsseite, und klicken Sie auf Fertig stellen.



9. Nachdem die neue Vault-Speicherpartition erfolgreich erstellt wurde, können Sie Daten in Enterprise Vault mit StorageGRID als primärem Speicher archivieren, wiederherstellen und suchen.



Konfigurieren Sie die StorageGRID S3 Objektsperre für WORM Storage

Erfahren Sie, wie Sie StorageGRID für WORM-Storage mit S3 Object Lock konfigurieren.

Voraussetzungen für die Konfiguration von StorageGRID für WORM Storage

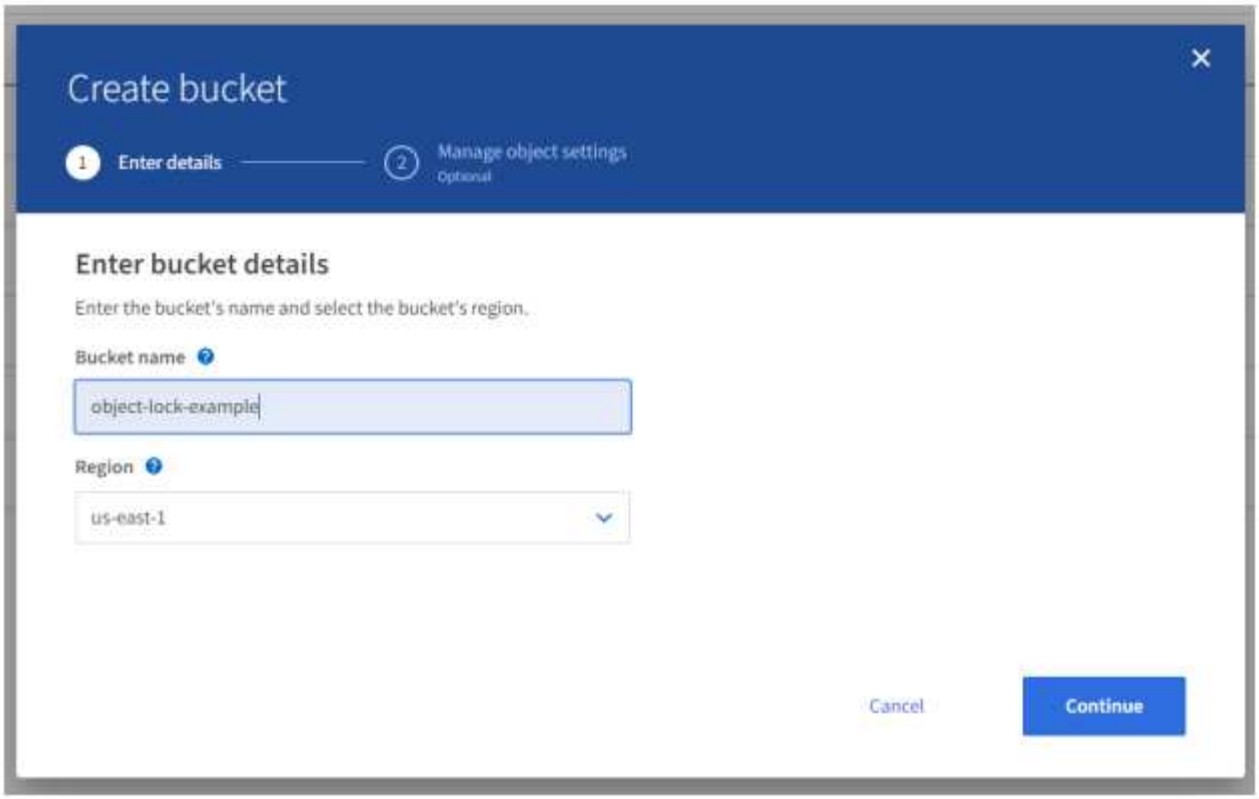
Bei WORM-Storage verwendet StorageGRID S3 Objektsperre, um Objekte zwecks Compliance aufzubewahren. Dies erfordert StorageGRID 11.6 oder höher. Dabei wurde die standardmäßige S3 Object Lock Bucket-Aufbewahrung eingeführt. Enterprise Vault erfordert außerdem Version 14.2.2 oder höher.

Konfigurieren Sie die standardmäßige Bucket-Aufbewahrung von StorageGRID S3 Object Lock

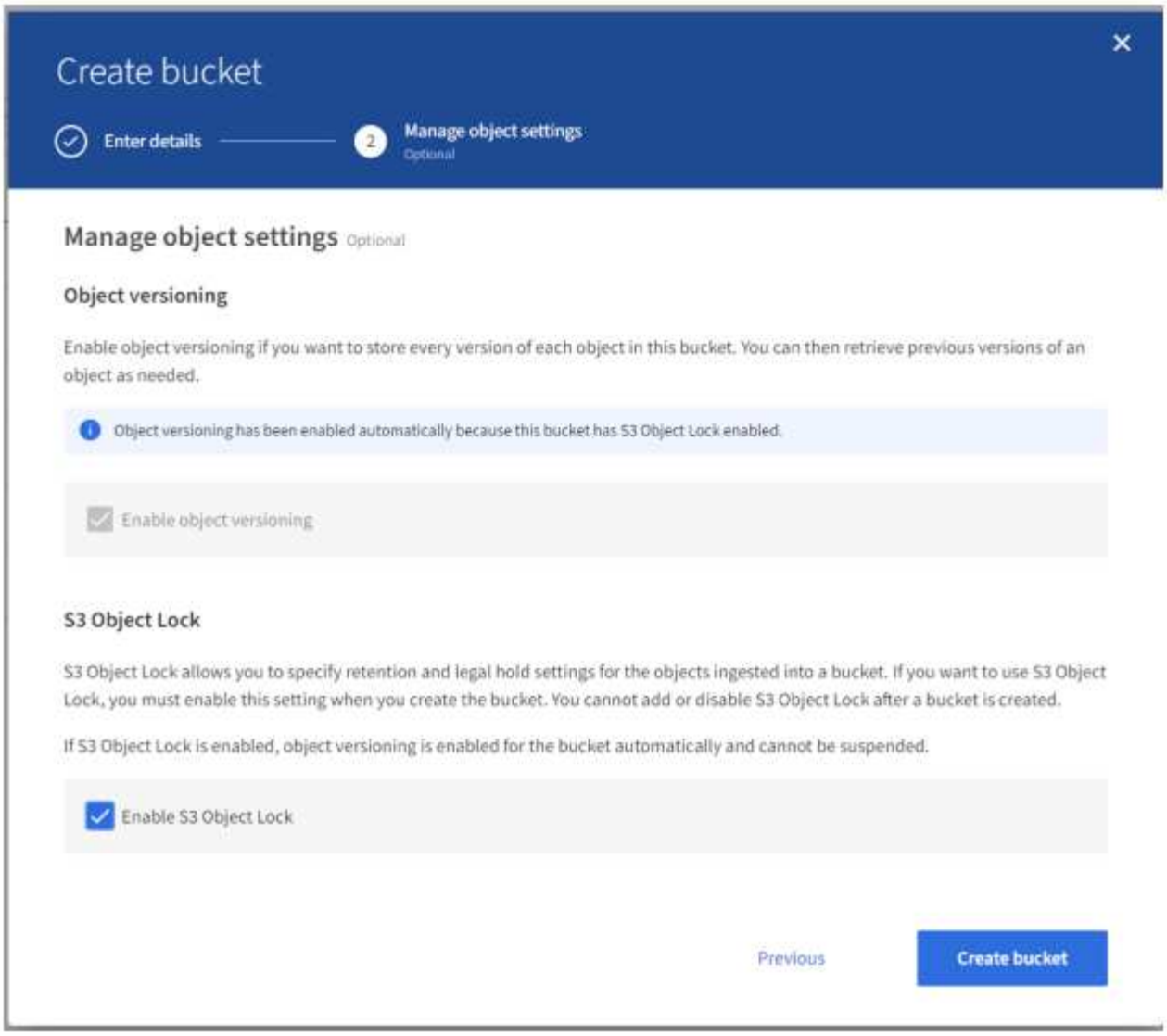
Führen Sie die folgenden Schritte aus, um die standardmäßige Bucket-Aufbewahrung von StorageGRID S3 Object Lock zu konfigurieren:

Schritte

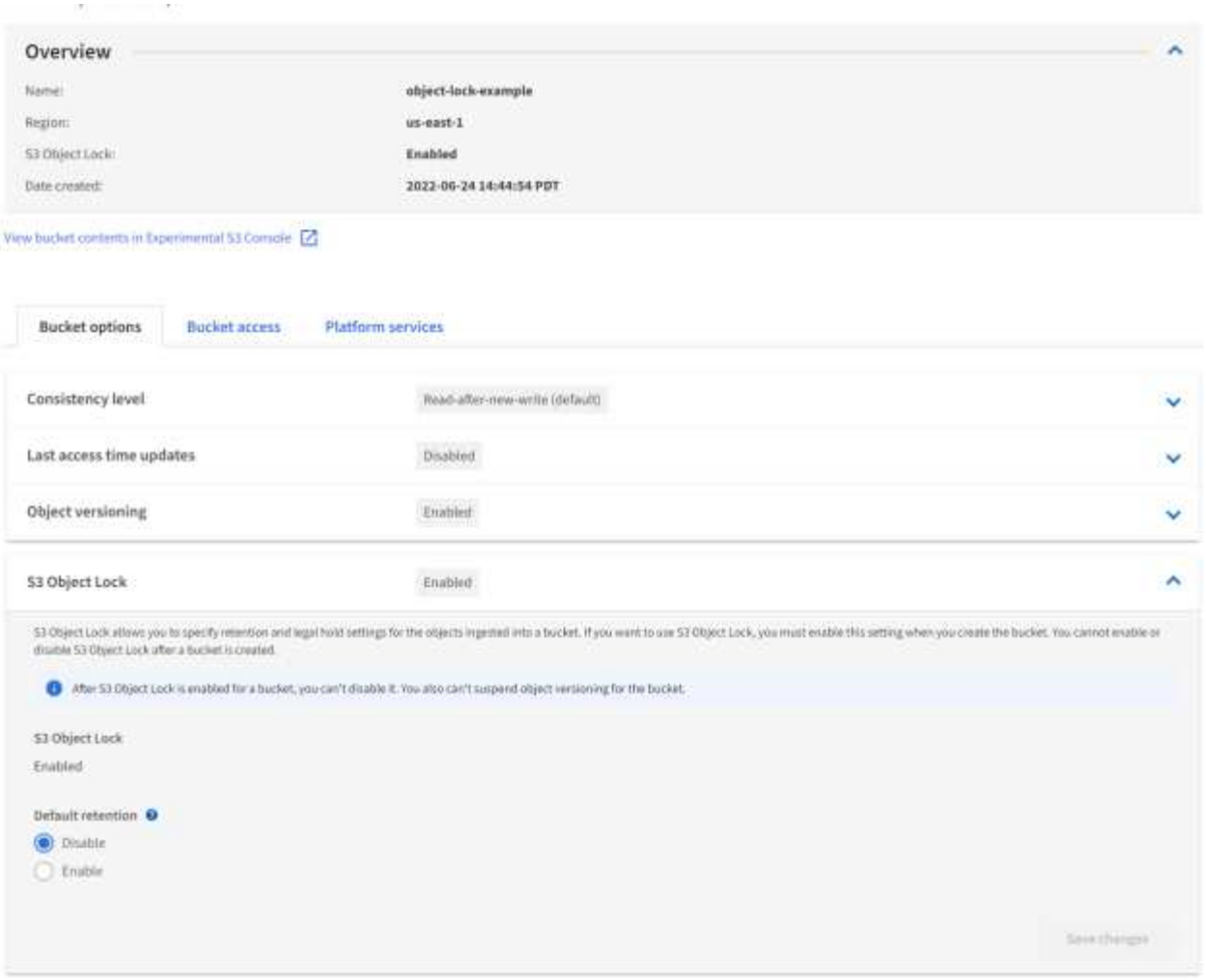
1. Erstellen Sie in StorageGRID-Mandantenmanager einen Bucket, und klicken Sie auf Fortfahren



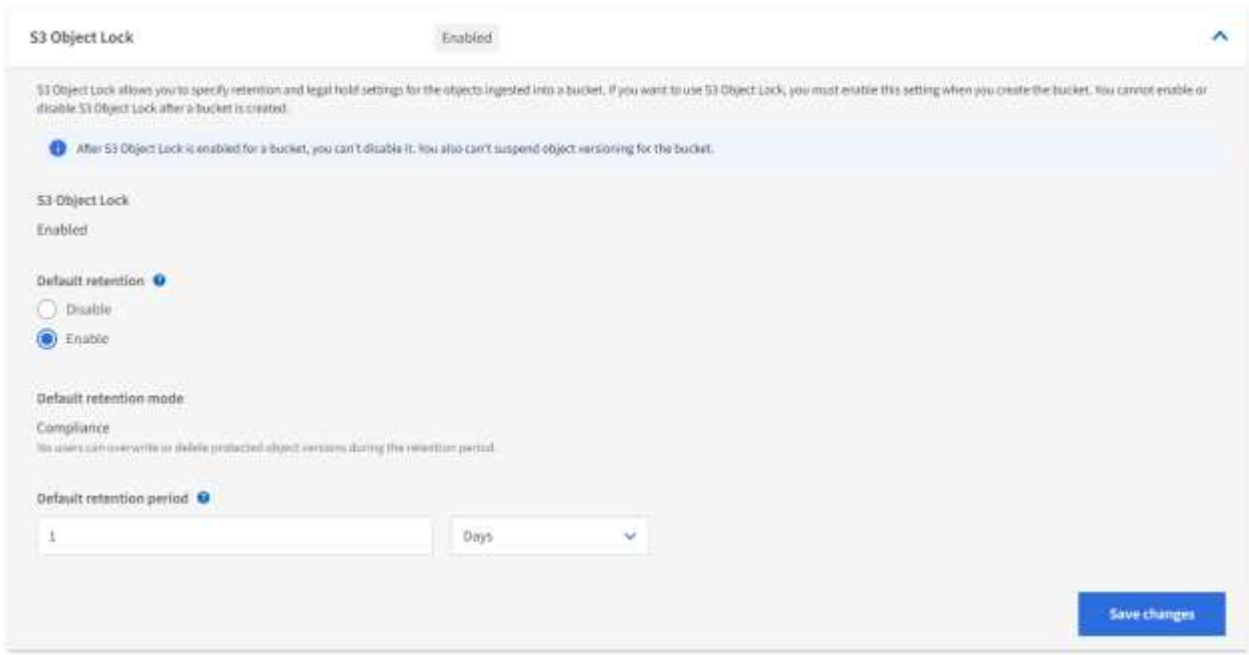
2. Wählen Sie die Option S3-Objektsperre aktivieren aus, und klicken Sie auf Bucket erstellen.



3. Nachdem der Bucket erstellt wurde, wählen Sie den Bucket aus, um die Bucket-Optionen anzuzeigen. Erweitern Sie die Dropdown-Option S3 Object Lock.



4. Wählen Sie unter Standardaufbewahrung die Option Aktivieren aus, und legen Sie eine Standardaufbewahrungsfrist von 1 Tag fest. Klicken Sie Auf Änderungen Speichern.



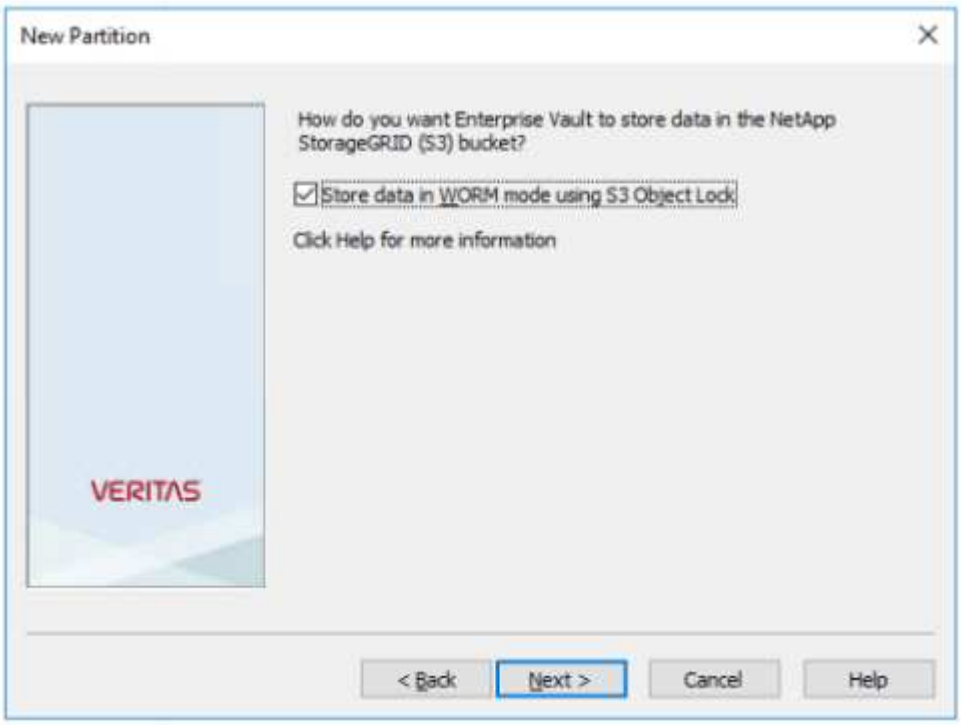
Der Bucket kann jetzt von Enterprise Vault zur Speicherung von WORM-Daten verwendet werden.

Enterprise Vault Konfigurieren

Gehen Sie wie folgt vor, um Enterprise Vault zu konfigurieren:

Schritte

1. Wiederholen Sie die Schritte 1-3 im "Basiskonfiguration" Abschnitt, wählen Sie jedoch diesmal die Option Daten im WORM-Modus mit S3 Objektsperre speichern. Klicken Sie Auf Weiter.



2. Stellen Sie bei der Eingabe der S3 Bucket-Verbindungseinstellungen sicher, dass Sie den Namen eines S3-Buckets eingeben, für den die S3 Object Lock Default Retention aktiviert ist.
3. Testen Sie die Verbindung, um die Einstellungen zu überprüfen.

Konfigurieren Sie StorageGRID-Standort-Failover für Disaster Recovery

Erfahren Sie, wie Sie ein StorageGRID-Standort-Failover in einem Disaster-Recovery-Szenario konfigurieren.

Eine Implementierung einer StorageGRID-Architektur hat gemein mehrere Standorte. Standorte können entweder aktiv/aktiv oder aktiv/Passiv für DR sein. Stellen Sie in einem DR-Szenario sicher, dass veritas Enterprise Vault die Verbindung zu seinem primären Speicher (StorageGRID) aufrechterhalten kann und bei einem Standortausfall weiterhin Daten aufnehmen und abrufen kann. Dieser Abschnitt enthält allgemeine Konfigurationsanleitungen für eine aktiv/Passiv-Bereitstellung an zwei Standorten. Detaillierte Informationen zu diesen Richtlinien finden Sie auf der "StorageGRID-Dokumentation" Seite oder bei einem StorageGRID Experten.

Voraussetzungen für die Konfiguration von StorageGRID mit veritas Enterprise Vault

Überprüfen Sie vor dem Konfigurieren des StorageGRID-Standort-Failover die folgenden Voraussetzungen:

- Es gibt eine StorageGRID-Bereitstellung an zwei Standorten, z. B. Standort 1 und STANDORT 2.
- Es wurde an jedem Standort ein Admin-Node erstellt, auf dem der Load Balancer ausgeführt wird, oder ein Gateway-Node zum Lastausgleich.
- Ein Endpunkt des StorageGRID Load Balancer wurde erstellt.

Konfigurieren Sie das StorageGRID Site Failover

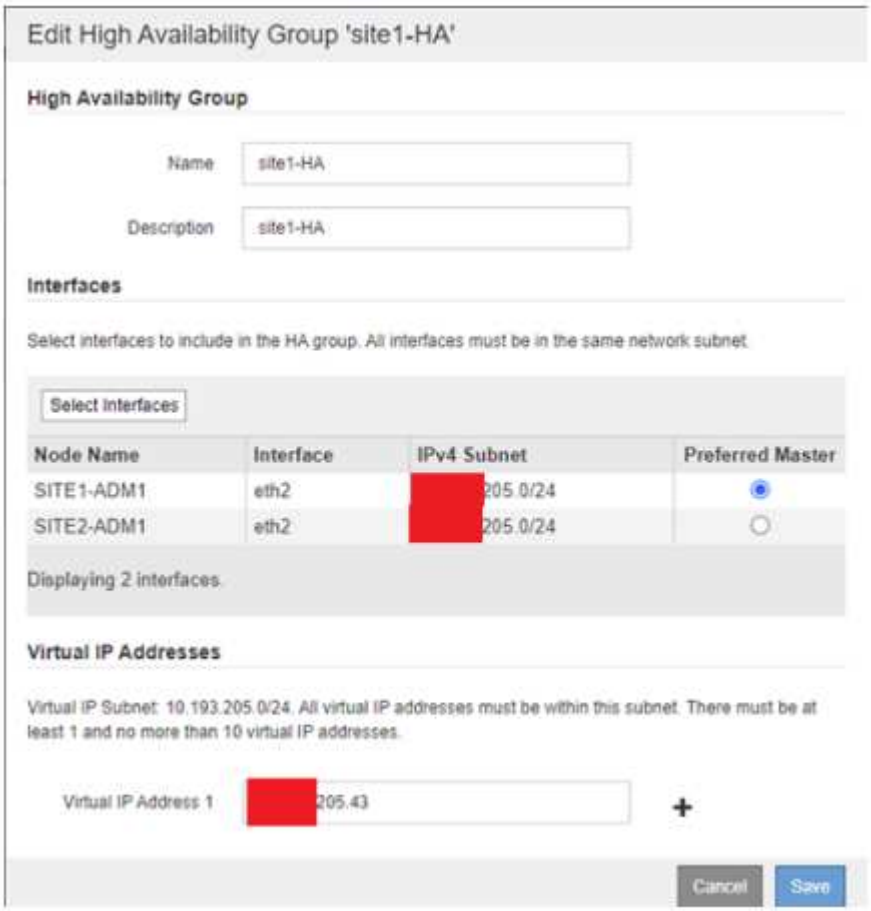
Führen Sie zum Konfigurieren des StorageGRID-Standort-Failover die folgenden Schritte aus:

Schritte

1. Konfigurieren Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit), um die Verbindung zu StorageGRID bei Standortausfällen sicherzustellen. Klicken Sie in der StorageGRID-Grid-Manager-Oberfläche (GMI) auf Konfiguration, Hochverfügbarkeitsgruppen und + Erstellen.

   [Vertias/veritas-create-High-Availability-Group]

2. Geben Sie die erforderlichen Informationen ein. Klicken Sie auf Schnittstellen auswählen und schließen Sie sowohl die Netzwerkschnittstellen von SITE 1 als auch von SITE2 ein, wobei SITE 1 (der primäre Standort) der bevorzugte Master ist. Weisen Sie eine virtuelle IP-Adresse innerhalb desselben Subnetzes zu. Klicken Sie auf Speichern .

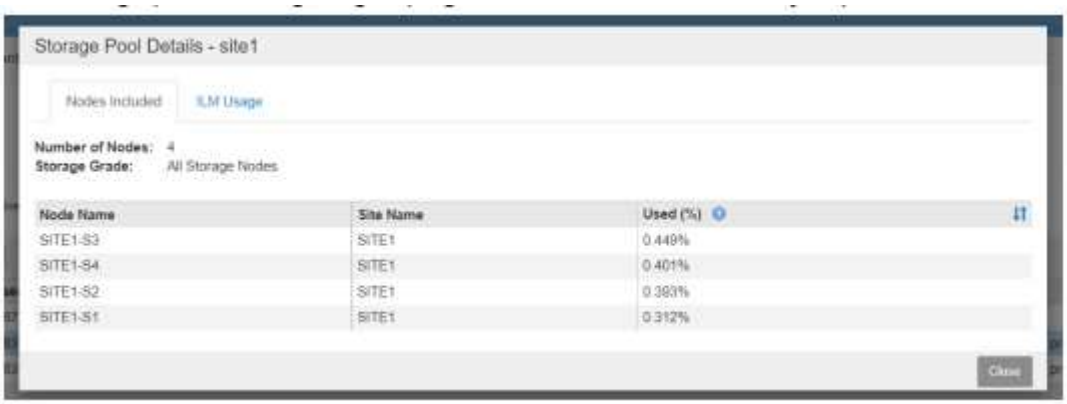


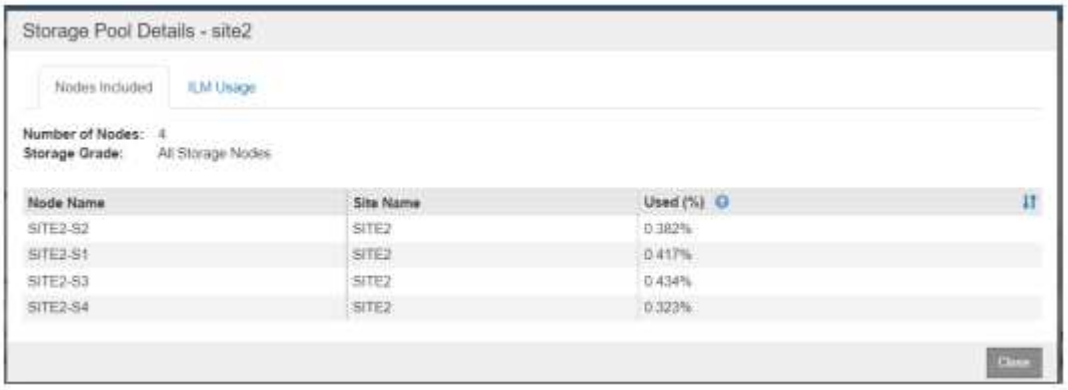
3. Diese virtuelle IP (VIP)-Adresse sollte dem S3-Hostnamen zugeordnet werden, der während der Partitionskonfiguration von veritas Enterprise Vault verwendet wird. Die VIP-Adresse löst Datenverkehr an STANDORT 1 auf. Während STANDORT 1-Fehler leitet die VIP-Adresse den Datenverkehr transparent an STANDORT 2 um.

4. Stellen Sie sicher, dass die Daten sowohl an STANDORT 1 als auch an STANDORT 2 repliziert werden. So sind die Objektdaten auch bei Ausfall von STANDORT 1 von SITE2 aus verfügbar. Dazu müssen zunächst die Speicherpools konfiguriert werden.

   Klicken Sie in StorageGRID GMI auf ILM, Speicherpools und dann auf Erstellen. Folgen Sie dem Assistenten, um zwei Speicherpools zu erstellen: Einen für STANDORT 1 und einen anderen für STANDORT 2.

   Storage-Pools sind logische Gruppen von Nodes, die zur Definition der Objektplatzierung verwendet werden





5. Klicken Sie in StorageGRID GMI auf ILM, Regeln und dann auf + Erstellen. Befolgen Sie den Assistenten, um eine ILM-Regel zu erstellen, die eine Kopie angibt, die pro Standort mit einem ausgewogenen Aufnahmeverhalten gespeichert werden soll.

6. Fügen Sie die ILM-Regel einer ILM-Richtlinie hinzu und aktivieren Sie die Richtlinie.

Diese Konfiguration hat das folgende Ergebnis:

- Eine virtuelle S3-Endpunkt-IP, wobei STANDORT 1 der primäre und STANDORT 2 der sekundäre Endpunkt ist. Wenn STANDORT 1 ausfällt, erfolgt ein Failover der VIP auf STANDORT 2.
- Wenn archivierte Daten von veritas Enterprise Vault gesendet werden, stellt StorageGRID sicher, dass eine Kopie auf SITE 1 gespeichert wird und eine andere DR-Kopie in SITE2 gespeichert wird. Wenn STANDORT 1 ausfällt, wird Enterprise Vault weiterhin von STANDORT 2 aufgenommen und abgerufen.

Beide Konfigurationen sind für veritas Enterprise Vault transparent. Der S3-Endpunkt, der Bucket-Name, die Zugriffsschlüssel usw. sind identisch. Es ist nicht notwendig, die S3-Verbindungseinstellungen auf der veritas Enterprise Vault-Partition neu zu konfigurieren.

Schritte, um auf die StorageGRID Evaluierungssoftware zuzugreifen

Diese Schulung richtet sich an NetApp Vertriebsmitarbeiter, Partner und potenzielle Kunden, die mit NetApp zusammenarbeiten.

Für ein Konto registrieren

1. Registrieren Sie sich für ein Konto auf der "NetApp Support Website" mit Ihrer geschäftlichen E-Mail-Adresse.
   a. Stellen Sie sicher, dass Sie nicht mit dem neu erstellten Konto angemeldet sind.
   b. Wenn Sie bereits über ein Konto verfügen, stellen Sie sicher, dass Sie nicht angemeldet sind, und fahren Sie mit dem nächsten Schritt fort.
2. Erstellen Sie einen nicht-technischen Support-Fall, um die Zugriffsebenen auf „Interessenten“ zu erhöhen. Klicken Sie dazu auf den ""Problem melden"Link „ in der Fußzeile der Website.
3. Wählen Sie als Feedback-Kategorie „Registrierungsproblem“ aus.
4. Schreiben Sie im Kommentarbereich: "Meine Konto-E-Mail-Adresse ist *Your-Email-Adresse*. Ich möchte potenziellen Kunden Zugang erhalten, um die StorageGRID Evaluierungssoftware herunterzuladen.“
   a. Nennen Sie den Namen der internen Person von NetApp, die den Antrag auf Zugang für einen potenziellen Kunden vorgeschlagen hat.

Laden Sie StorageGRID herunter

1. Nachdem Ihr Support-Fall geprüft und genehmigt wurde, werden Sie vom NetApp Support per E-Mail darüber informiert, dass Ihr Konto potenziellen Kunden Zugang gewährt wurde.
2. Laden Sie die herunter "StorageGRID Evaluierungssoftware".

Die Evaluierungslizenzdatei befindet sich in der ZIP-Datei. Es handelt sich um StorageGRID-Webscale-<version>, die nach der ZIP-Datei\vsphere\NLF000000.txt verwendet wurde.

Beim Herunterladen der Software handelt es sich um einen Prozess, der Maßnahmen zur Einhaltung der gesetzlichen Vorschriften beinhaltet. Um die Compliance sicherzustellen, müssen Benutzer ein Konto erstellen und einen Support-Fall eröffnen, bevor sie Zugang erhalten. Dieser Prozess hilft uns dabei, die Kontrolle und Dokumentation aufrechtzuerhalten und Interessenten die für die Produktion benötigte Software zur Verfügung zu stellen.

Wir stellen die „produktionsbereite“ Version von StorageGRID bereit, die weder eine Open Source noch eine alternative Version ist. Es ist wichtig zu beachten, dass **Support nicht zur Verfügung gestellt wird** es sei denn, der potenzielle Kunde aktualisiert auf eine Produktionslizenz.

Bitte wenden Sie sich an StorageGRID.Feedback@netapp.com, wenn Sie Probleme mit den oben genannten Schritten haben.

NetApp StorageGRID-Blogs

Hier finden Sie einige der großartigen NetApp StorageGRID Blogs:

- Februar 16 2024: "Neu: StorageGRID 11.8: Mehr Sicherheit, Einfachheit und Benutzerfreundlichkeit"
- Februar 16 2024: "Wir stellen vor: StorageGRID 11.8"
- Februar 2 2024: "Wir stellen vor: Die StorageGRID + LakeFS Lösung im Überblick"
- Dezember 12 2023: "Big Data Analytics auf StorageGRID: Dremio arbeitet 23-mal schneller als Apache Hive"
- Nov. 7 2023: "Spectra Logic On-Premises-Gletscher mit StorageGRID"
- Okt. 17 2023: "Weiter aus Hadoop: Datenanalysen modernisieren mit Dremio und StorageGRID"
- September 2023: "Mithilfe von Cloud Insights können Sie Protokolle mithilfe von Fluent Bit überwachen und erfassen"
- August 30 2023: "Bereitstellungspunkt für Amazon S3 File System ist jetzt allgemein verfügbar"
- Mai 16 2023: "Wir stellen vor: StorageGRID 11.7 und die neue All-Flash Objekt-Storage Appliance SGF6112"
- Mai 16 2023: "Neuerungen bei der StorageGRID Objekt-Storage-Produktfamilie"
- März 30 2023: "Mountpoint für Amazon S3 Alpha-Version mit StorageGRID"
- März 30 2023: "Mit BlueXP schützen Sie Epic EHR durch eine Backup-Richtlinie, die 3:2:1-konform ist"
- März 14 2023: "So sichern Sie EHR-Datenbanken von Epic Systems mit einem Befehl in einer 3:2:1-konformen Architektur"
- Februar 14 2023: "Was haben Schokolade, Skifahren, Uhren und Mainframes gemeinsam?"
- Januar 18 2023: "StorageGRID S3 Object Lock validiert für veritas NetBackup"
- Januar 16 2023: "StorageGRID erneuert die NF203- und ISO/IEC 25051-Compliance-Zertifizierung"
- Dezember 6 2022: "StorageGRID erhält die KPMG-Compliance-Zertifizierung"
- Nov. 23 2022: "Erklärbare AI mit MLOps von NetApp und Modzy"
- Nov. 7 2022: "Unterstützung von StorageGRID und ONTAP S3: Unterschiede, Gemeinsamkeiten und Integration"
- Okt. 5 2022: "NetApp Cloud Insights bietet StorageGRID Galerie-Dashboards"
- Okt. 5 2022: "Auftauen Sie Ihre Daten auf StorageGRID für Snowflake"
- September 26 2022: "NetApp StorageGRID für Service Provider"
- September 19 2022: "Unterstützung von DataLock und Ransomware-Schutz für StorageGRID"
- September 2022: "Nehmen Sie diese Metriken und graten Sie sie"
- August 23 2022: "Data-Lake-Lösung auf Basis von StorageGRID"
- August 17 2022: "Es beginnt alles mit Objekt sperren… Aufbau eines S3-Storage-Ecosystems für kritische Backup-Applikationen"
- August 16 2022: "Integration von StorageGRID in den Open-Source-ELK Stack für mehr Benutzerfreundlichkeit"
- August 5 2022: "NetApp StorageGRID erhält eine Common Criteria Security-Zertifizierung"
- Juli 26 2022: "Die wachsende Liste validierter Partnerlösungen für StorageGRID nimmt zu"

- Juni 9 2022: "Nutzen Sie Hadoop S3A-Connector von Cloudera mit StorageGRID"
- Mai 26 2022: "StorageGRID – Speichern und Managen von Backup- und Replizierungsdaten On-Premises"
- Mai 24 2022: "Modernisieren Sie Ihre Analyse-Workloads mit NetApp und Alluxio"
- Mai 10 2022: "Lab on Demand ist Ihr bestes Vertriebstool für StorageGRID"

NetApp StorageGRID-Dokumentation

Die vollständige Dokumentation zu jeder NetApp StorageGRID Version finden Sie hier:

- "StorageGRID Appliances"
- "StorageGRID Software 11.5 - 12.0"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

https://library.netapp.com/ecm/ecm_download_file/2879263

https://library.netapp.com/ecm/ecm_download_file/2881511