Tool- und Anwendungsleitfäden

StorageGRID solutions and resources

NetApp
December 10, 2025

Inhalt

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

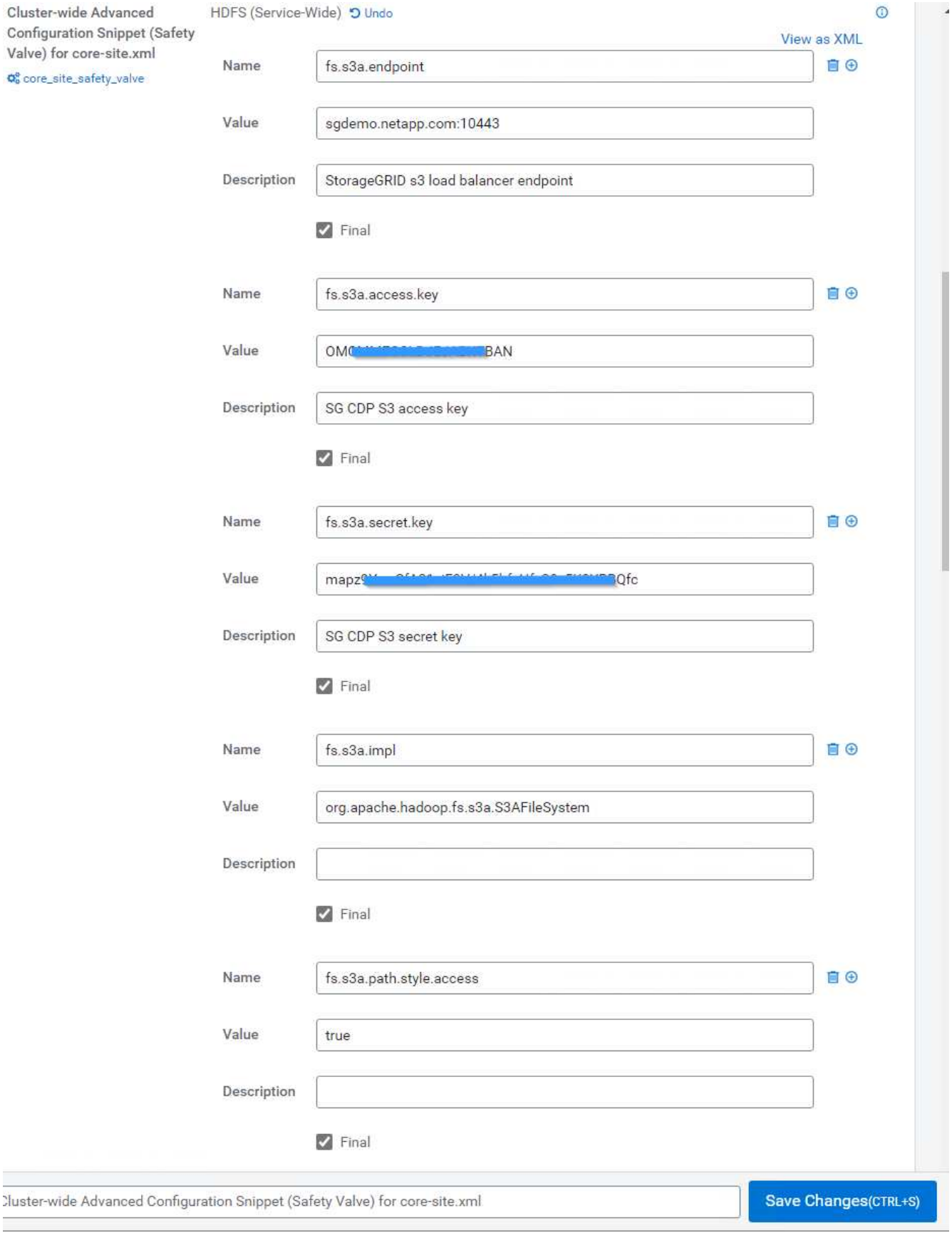
Schritte

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.

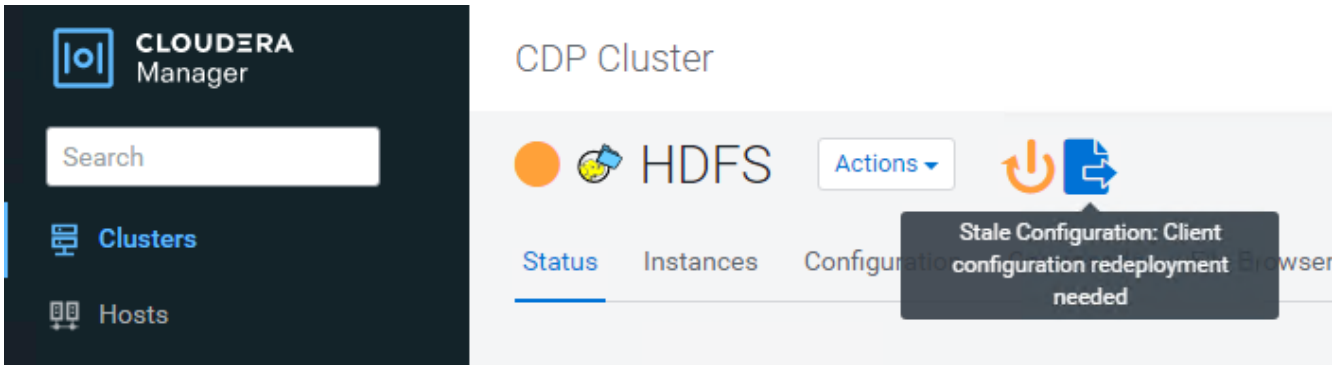
Name	Wert
fs.s3a.access.key	*<S3-Zugriffsschlüssel des Mandanten von StorageGRID>*
fs.s3a.secret.key	*<Mandant s3 geheimen Schlüssel von StorageGRID>*
fs.s3a.connection.ssl.enabled	[Wahr oder falsch] (Standardeinstellung: Https, wenn dieser Eintrag fehlt)

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.

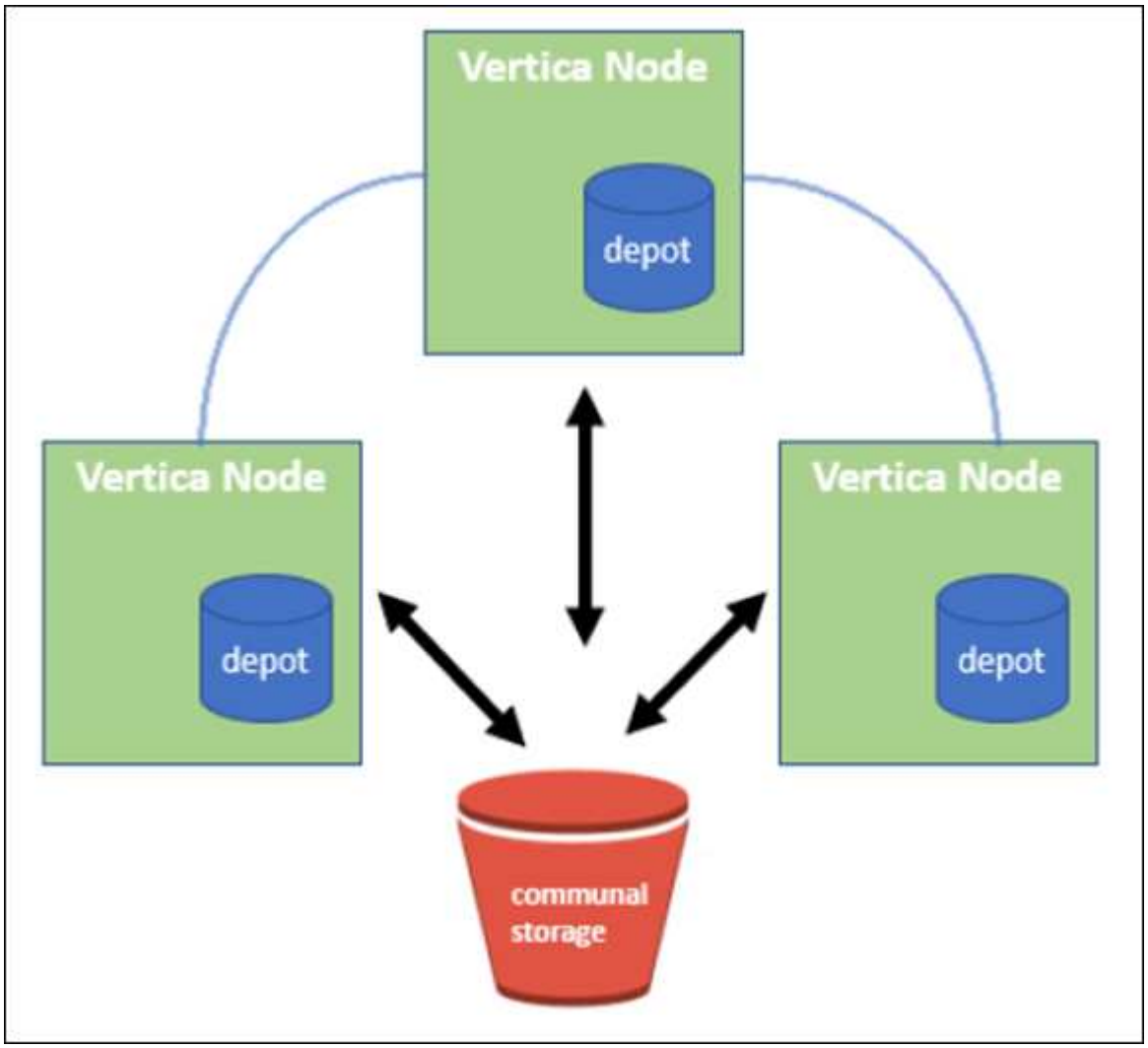
Eon- und Enterprise-Modi unterscheiden sich hauptsächlich darin, wo sie Daten speichern:

- 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

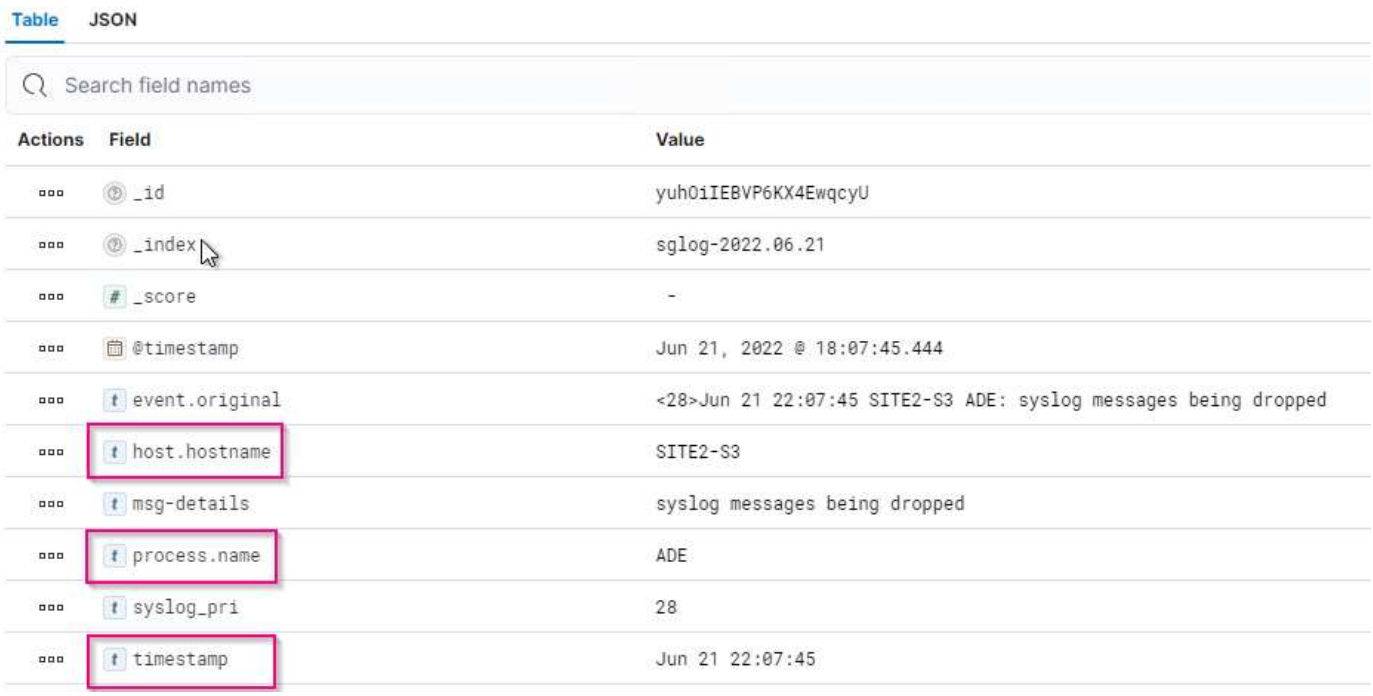
Zwei Beispielversionen werden aufgrund von Unterschieden in Namen bereitgestellt, die durch grok-Muster definiert wurden. + zum Beispiel definiert das SYSLOGBASE-grok-Muster in der Logstash config-Datei Feldnamen je nach installierter Logstash-Version unterschiedlich.

```
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
```

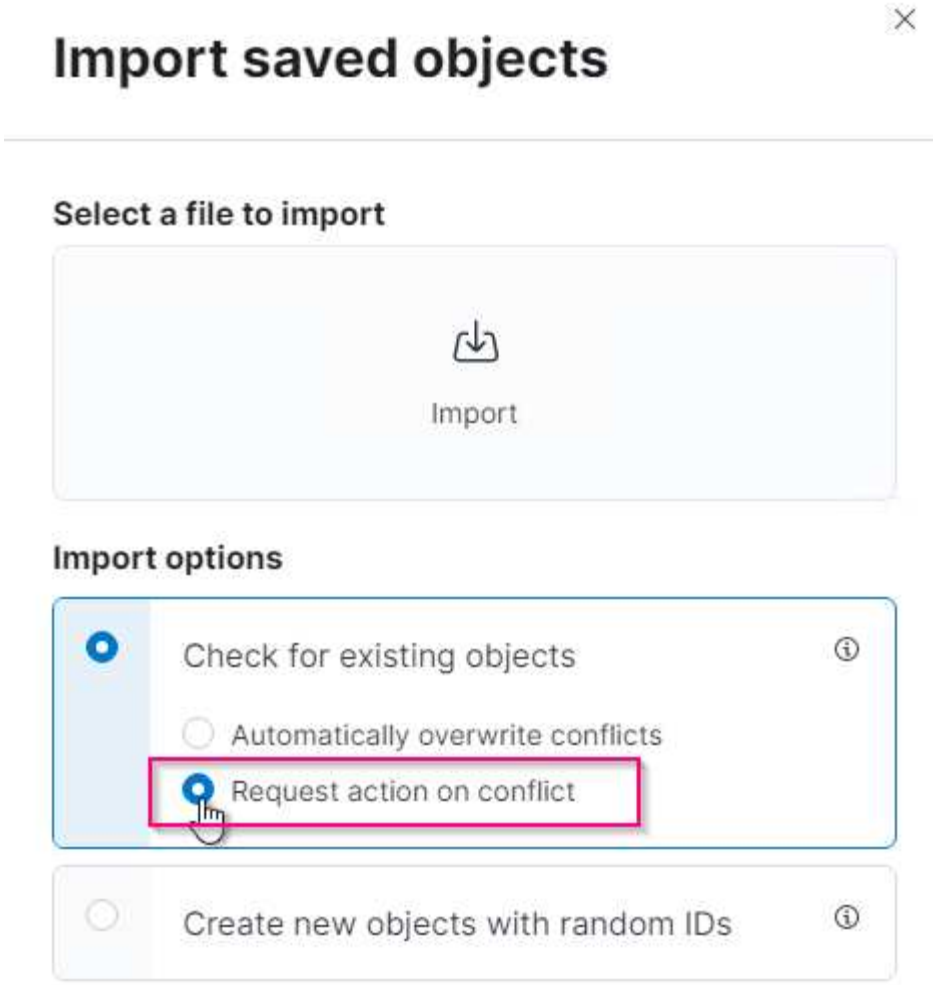
4. Prüfen Sie /var/log/logstash/logstash-plain.log und vergewissern Sie sich, dass beim Starten von Logstash mit der neuen Konfigurationsdatei keine Fehler auftreten.
5. Bestätigen Sie, dass der TCP-Port gestartet wurde und Sie zuhören. + in diesem Beispiel wird der TCP-Port 5000 verwendet.

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

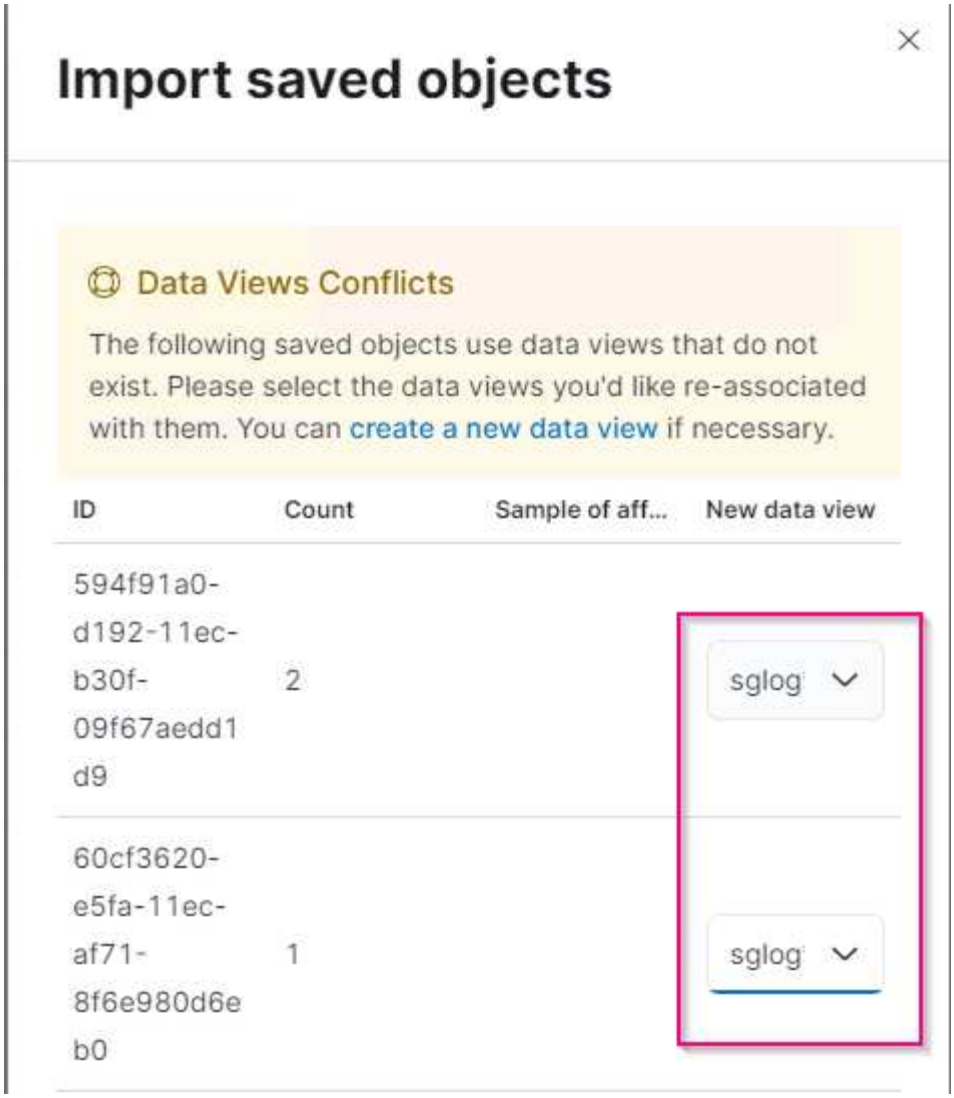
6. Konfigurieren Sie über die StorageGRID Manager-GUI einen externen Syslog-Server, um Protokollmeldungen an Logstash zu senden. Weitere Informationen finden Sie im "Demovideo" .
7. Sie müssen die Firewall auf dem Logstash-Server konfigurieren oder deaktivieren, damit StorageGRID-Knoten eine Verbindung 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

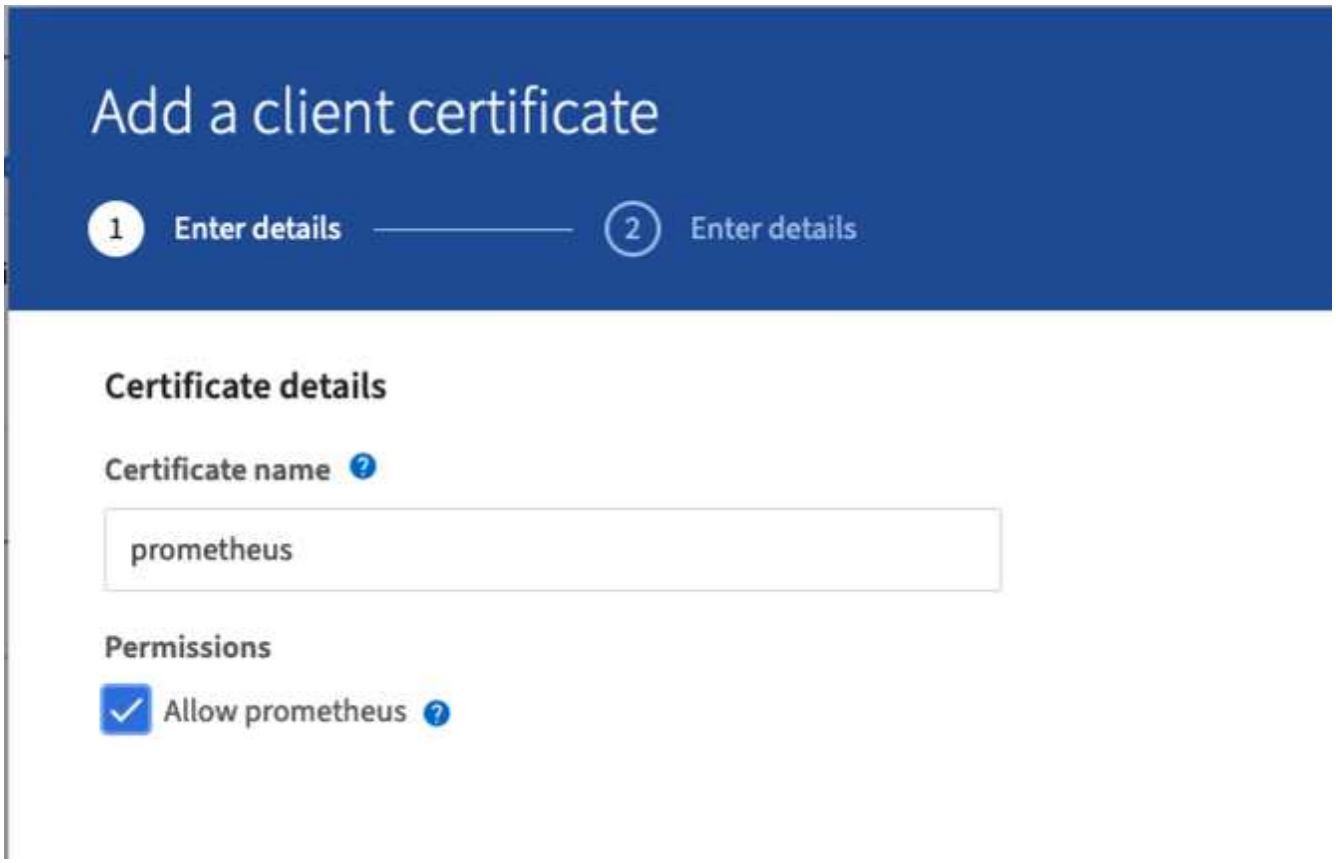
Labordetails

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.

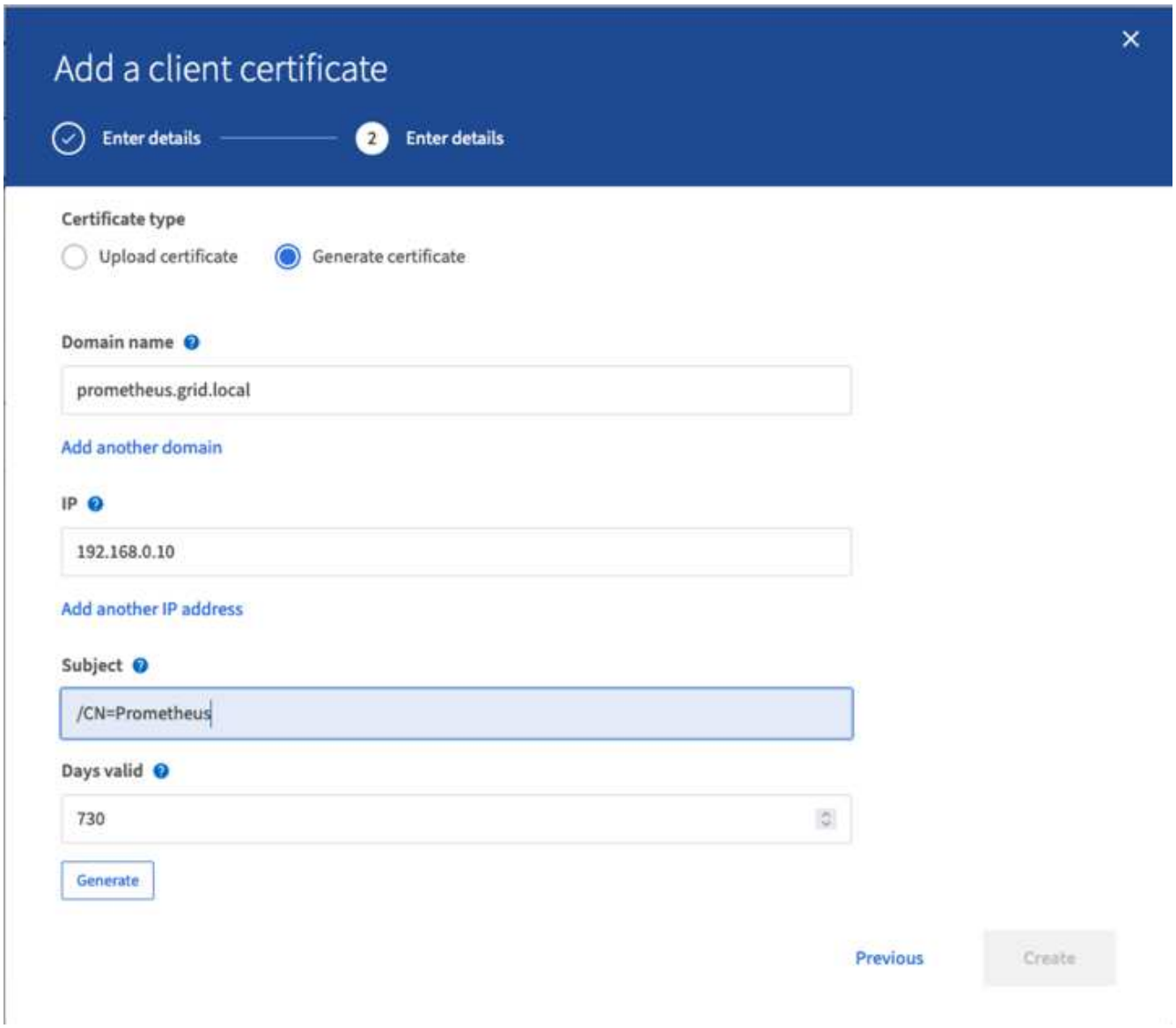
Konfigurieren Sie StorageGRID für Prometheus Client-Zugriff

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“.

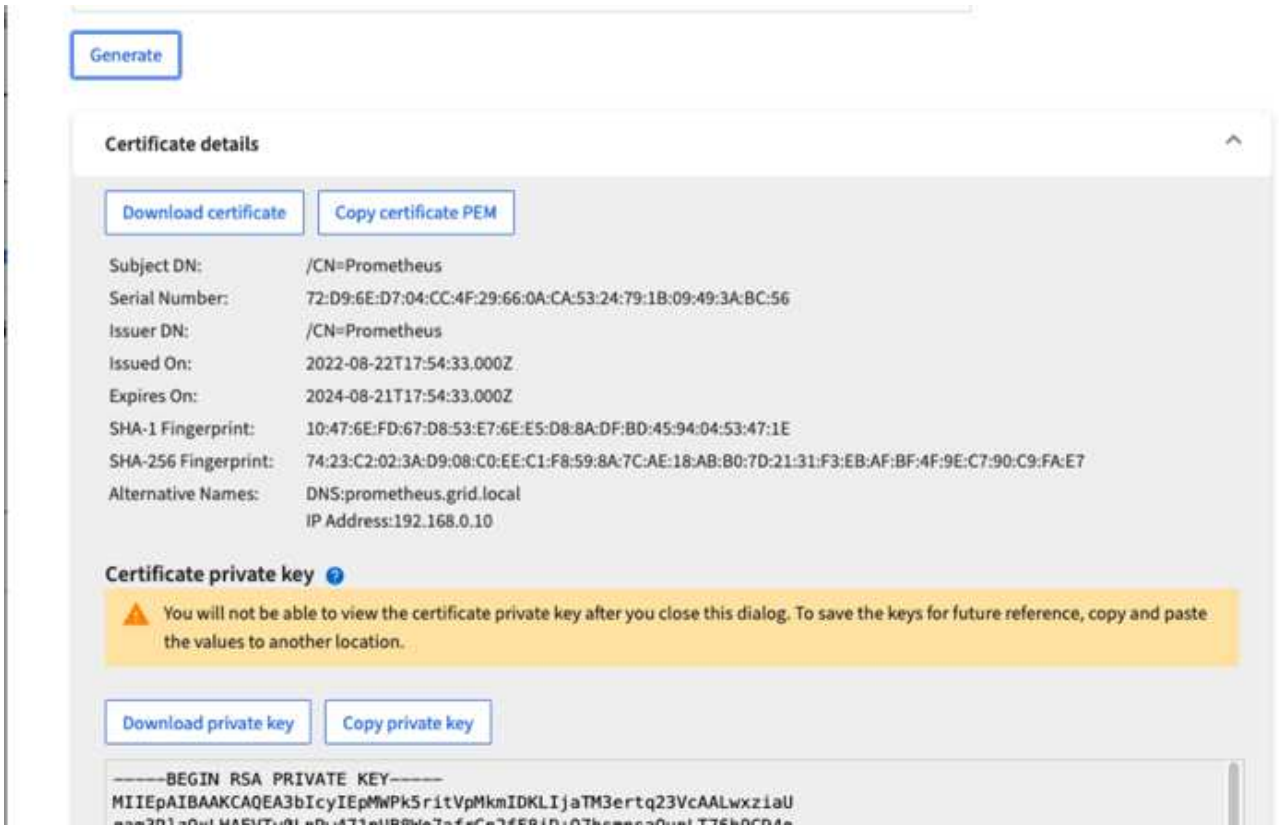


4. Wenn Sie ein CA-signiertes Zertifikat haben, können Sie das Optionsfeld für "Zertifikat hochladen" wählen, aber in unserem Fall werden wir StorageGRID das Client-Zertifikat generieren lassen, indem Sie das Optionsfeld für "Zertifikat generieren". Die Pflichtfelder werden angezeigt, in die ausgefüllt 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.

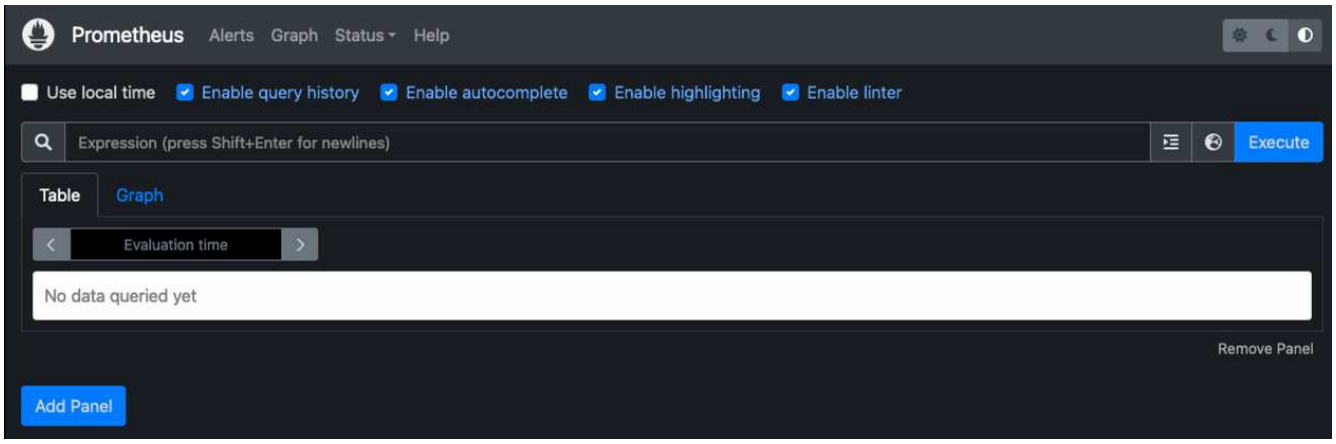
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. Überprüfen Sie, ob der Service ordnungsgemäß läuft

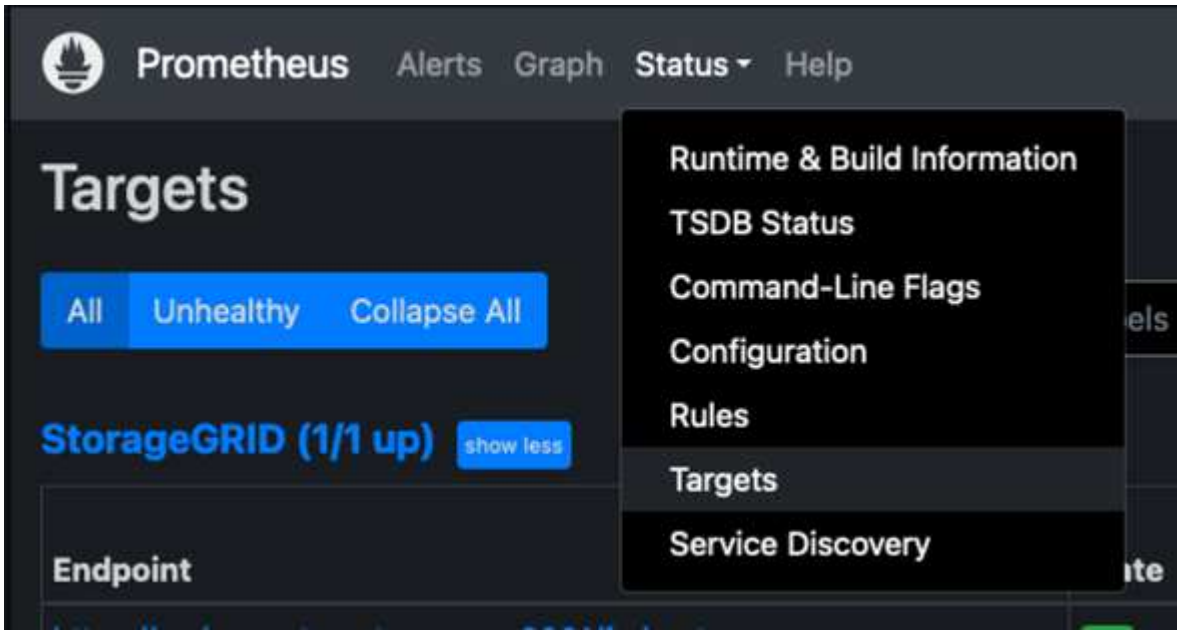
```
sudo systemctl status prometheus
```

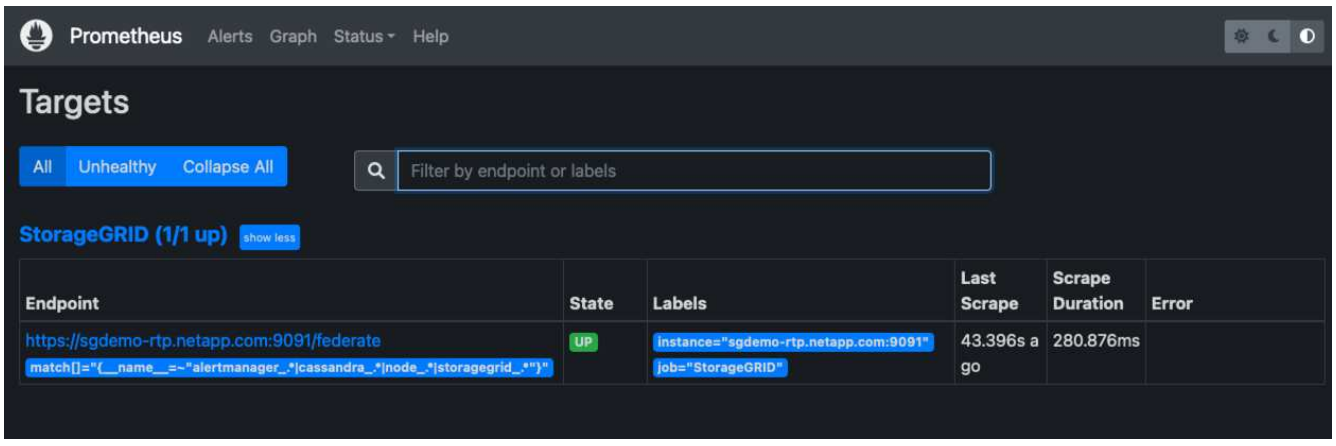
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 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

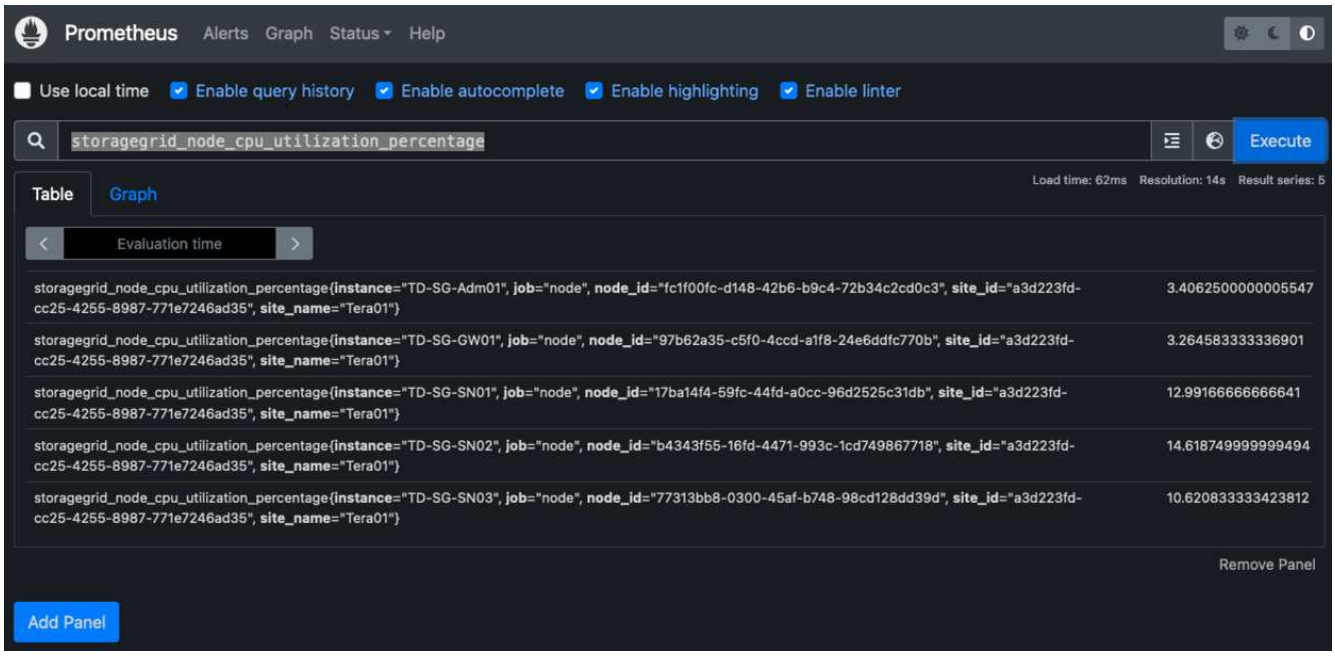


7. Unter "Status" Targets sehen Sie den Status des StorageGRID Endpunkts, den wir in prometheus.yml konfiguriert haben





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.

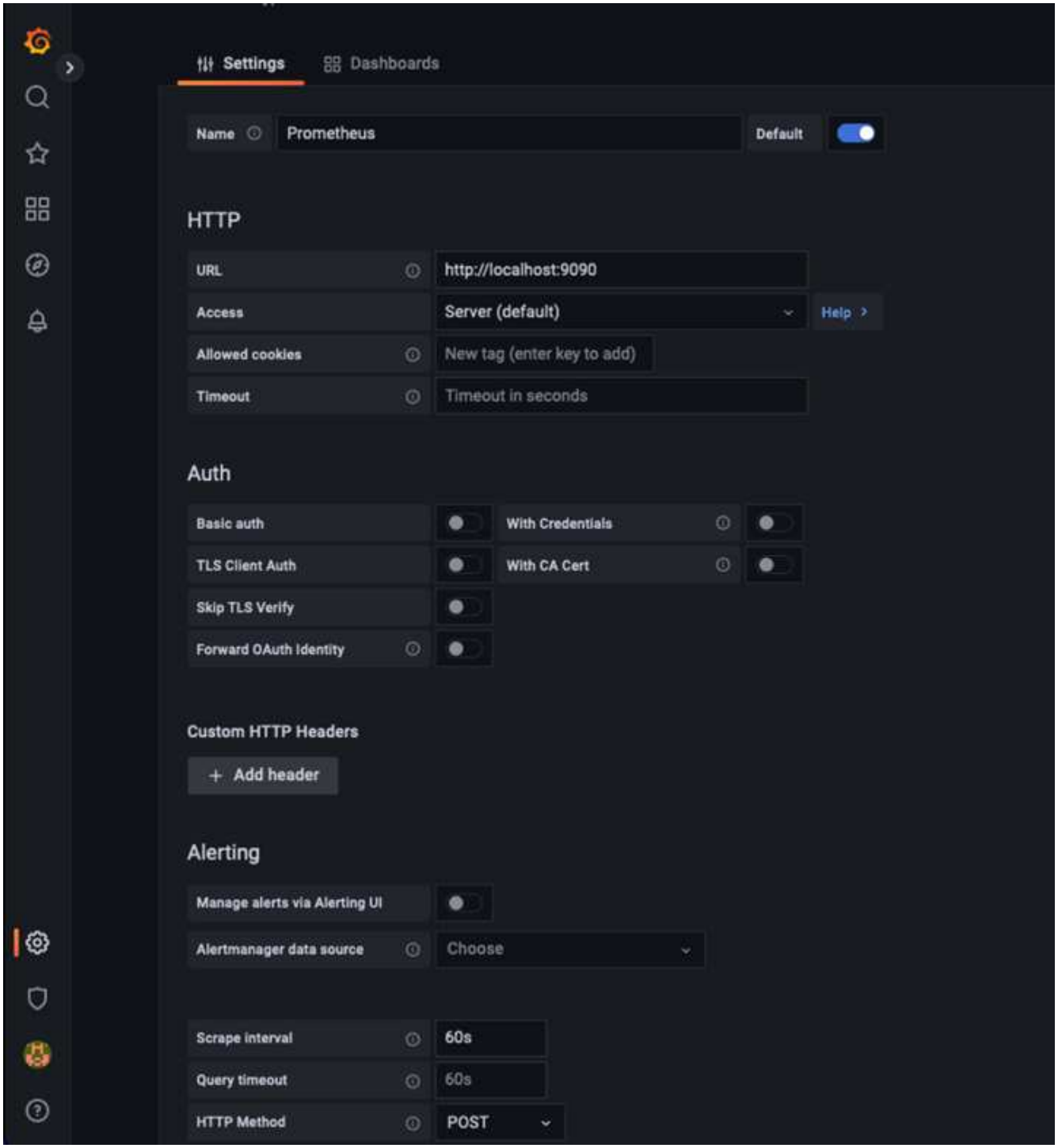
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

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.

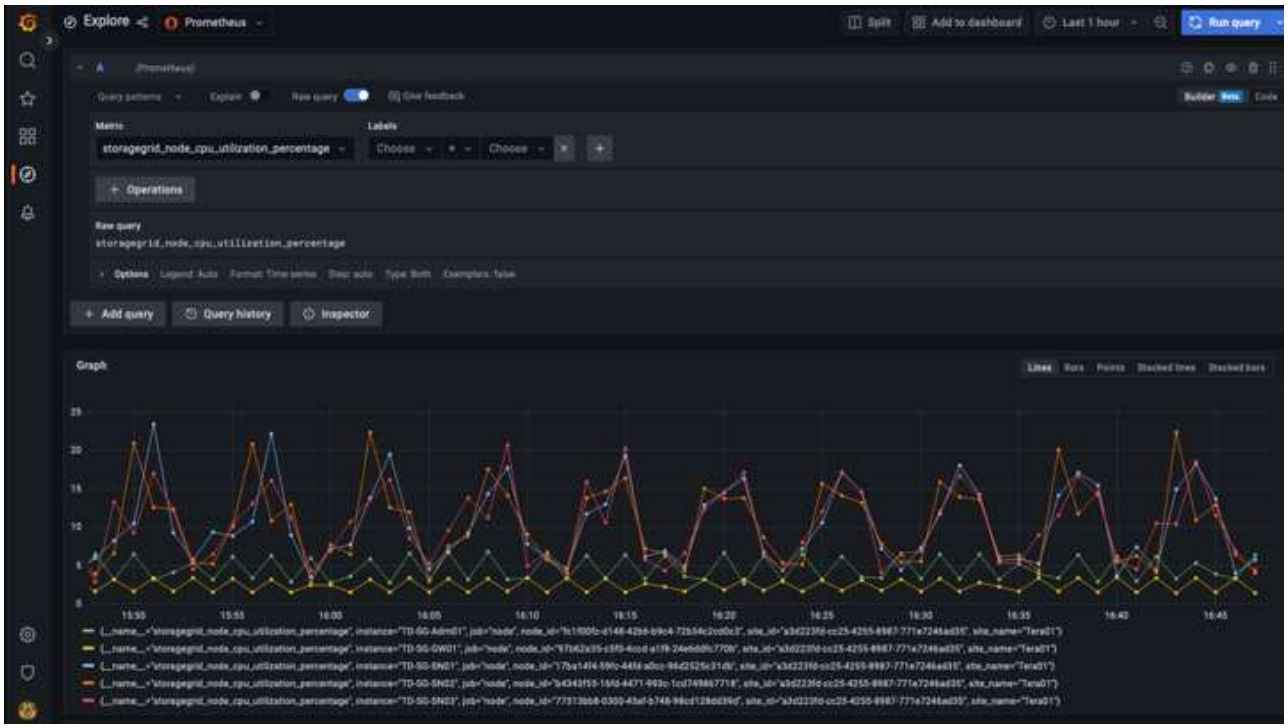
Erstellen eines Grafana Dashboards für StorageGRID

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

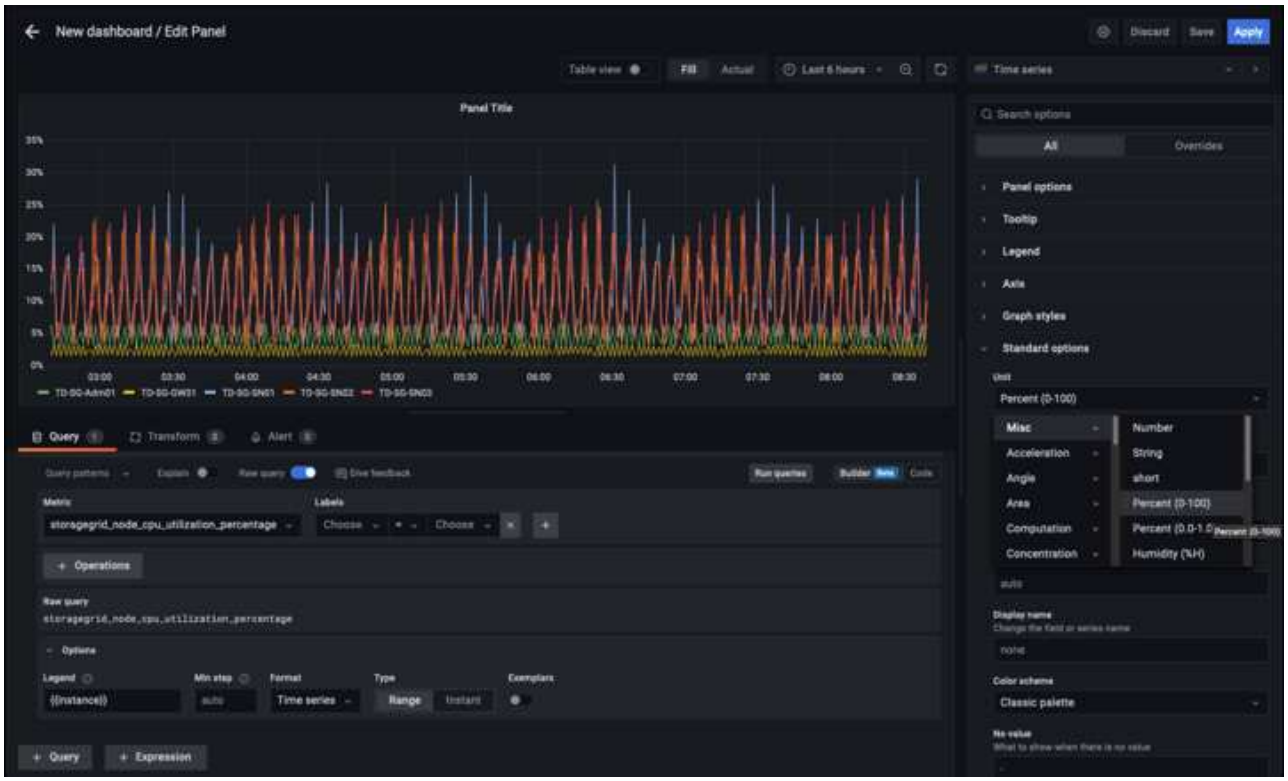
1. Erweitern Sie im linken Fensterbereich „Konfiguration“ und wählen Sie „Datenquellen“, und klicken Sie dann auf die Schaltfläche „Datenquelle hinzufügen“
2. Prometheus wird eine der wichtigsten Datenquellen zur Auswahl sein. Wenn nicht, dann verwenden Sie die Suchleiste zu finden "Prometheus"
3. Konfigurieren 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



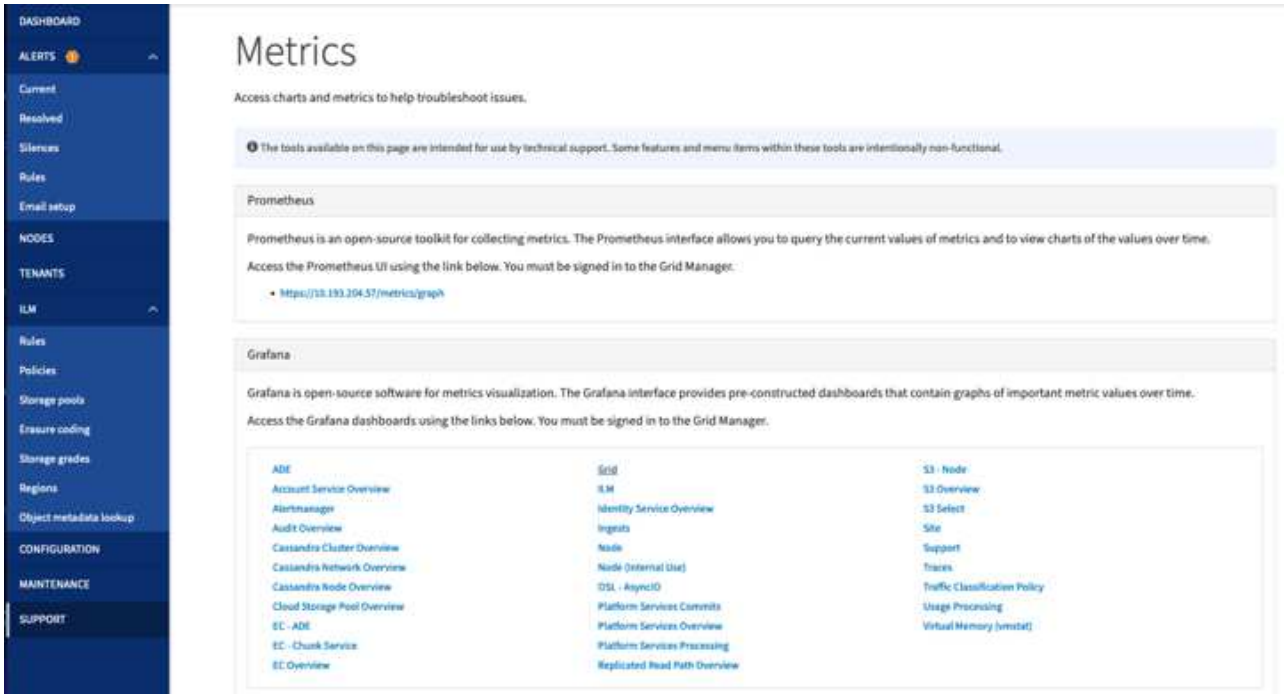
6. Nachdem die Datenquelle konfiguriert ist, können wir jetzt ein Dashboard erstellen.
   a. Erweitern Sie im linken Fensterbereich „Dashboards“ und wählen Sie „+ neues Dashboard“ aus.
   b. Wählen Sie „Neues Bedienfeld hinzufügen“ aus.
   c. Konfigurieren Sie das neue Panel durch Auswahl einer Metrik, 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.

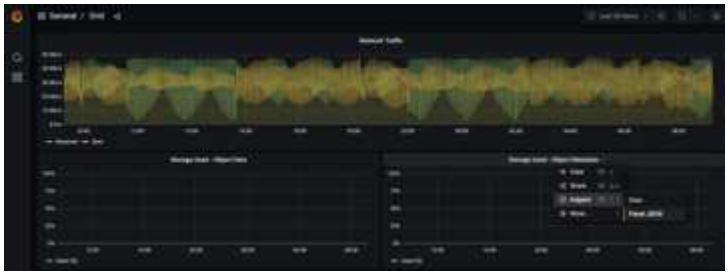
   a. Wählen Sie im linken Fensterbereich der StorageGRID-Managementoberfläche „Support“ und klicken Sie unten in der Spalte „Tools“ auf „Metriken“.

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



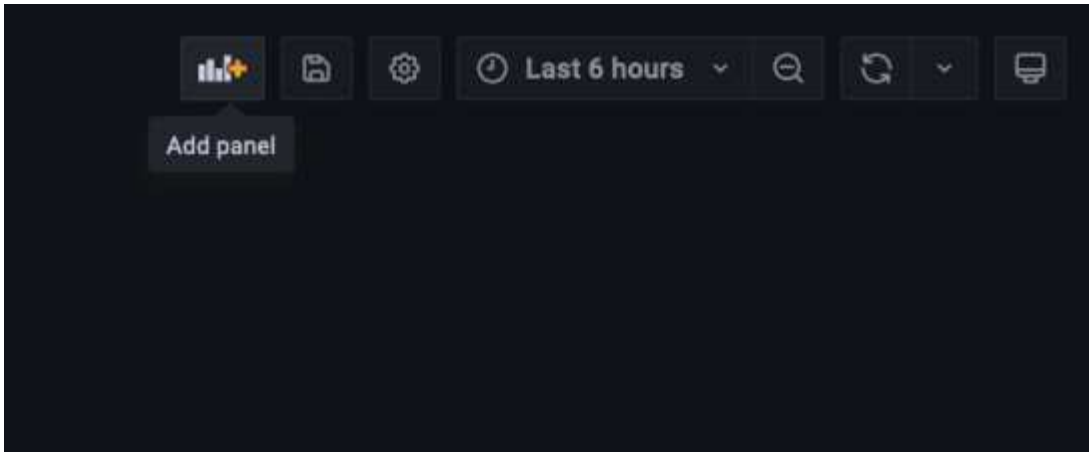
   c. Wählen Sie im Grid-Dashboard den Bereich „Storage Used - Object Metadata“ aus. Klicken Sie auf

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.



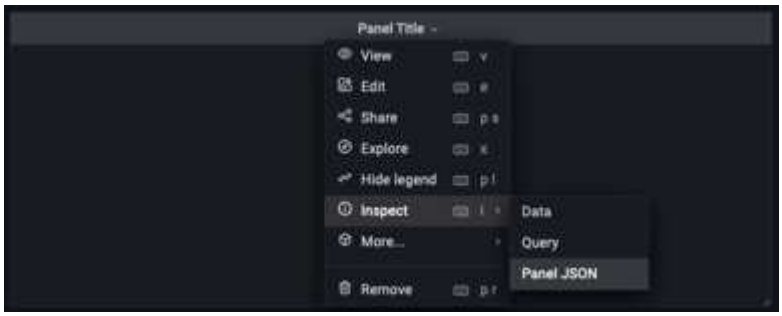
d. Kopieren Sie den JSON-Code und schließen Sie das Fenster.

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

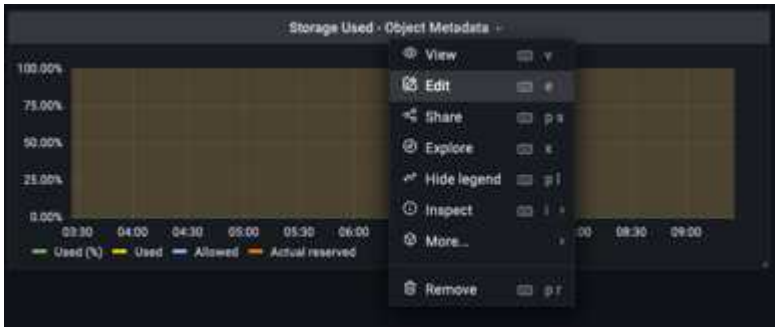


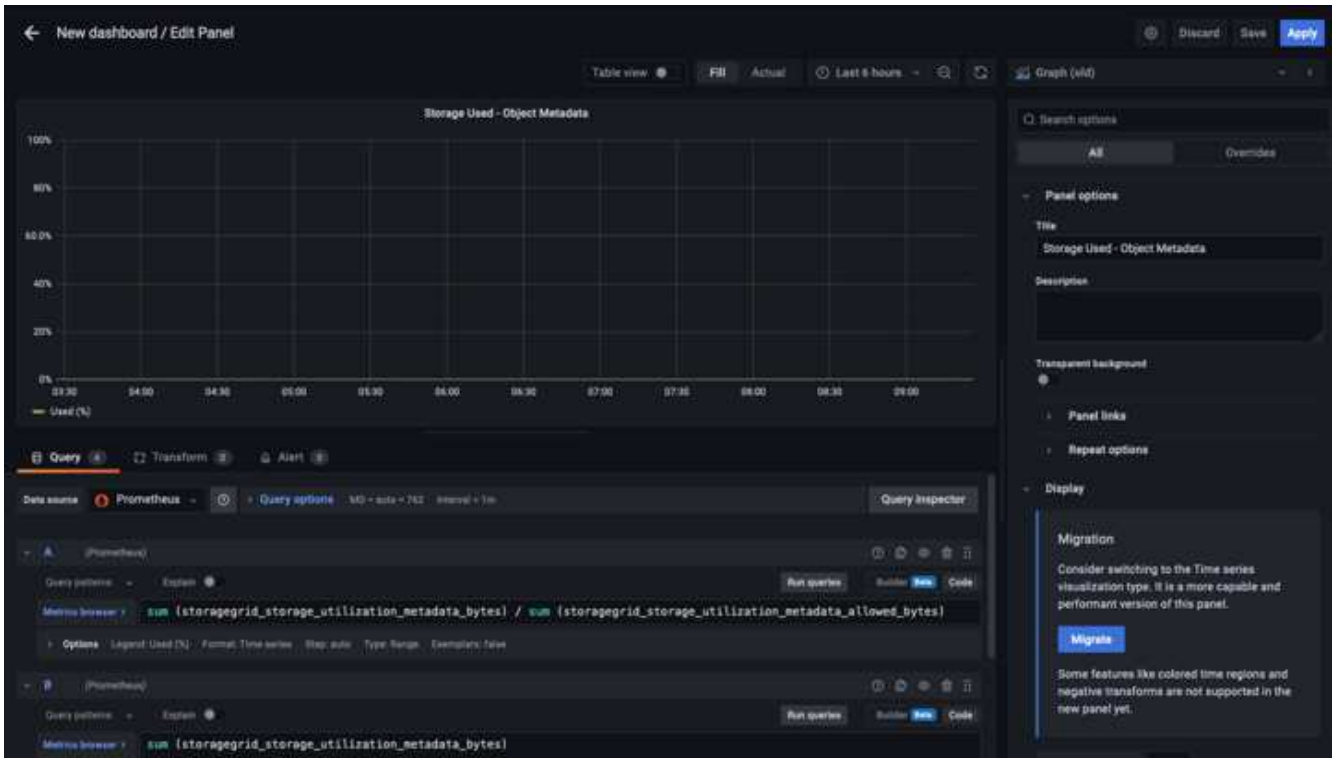
f. Wenden Sie das neue Bedienfeld an, ohne Änderungen vorzunehmen

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

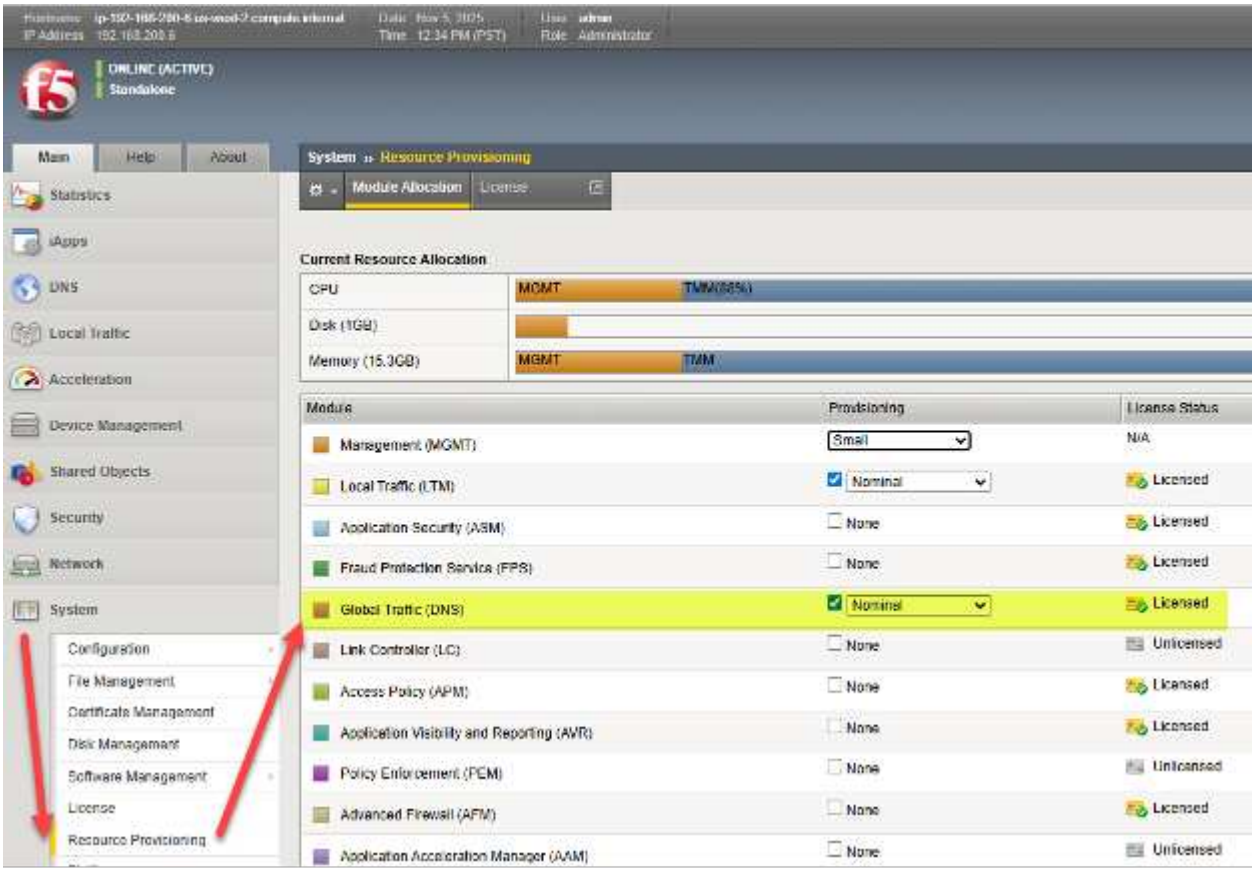
Die F5 BIG-IP DNS-Lösung, die früher BIG-IP GTM (Global Traffic Manager) und informell GSLB (Global Server Load Balancing) genannt wurde, ermöglicht einen nahtlosen Zugriff über mehrere aktive HA-Gruppen und aktive, standortübergreifende StorageGRID Lösungen hinweg.

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.

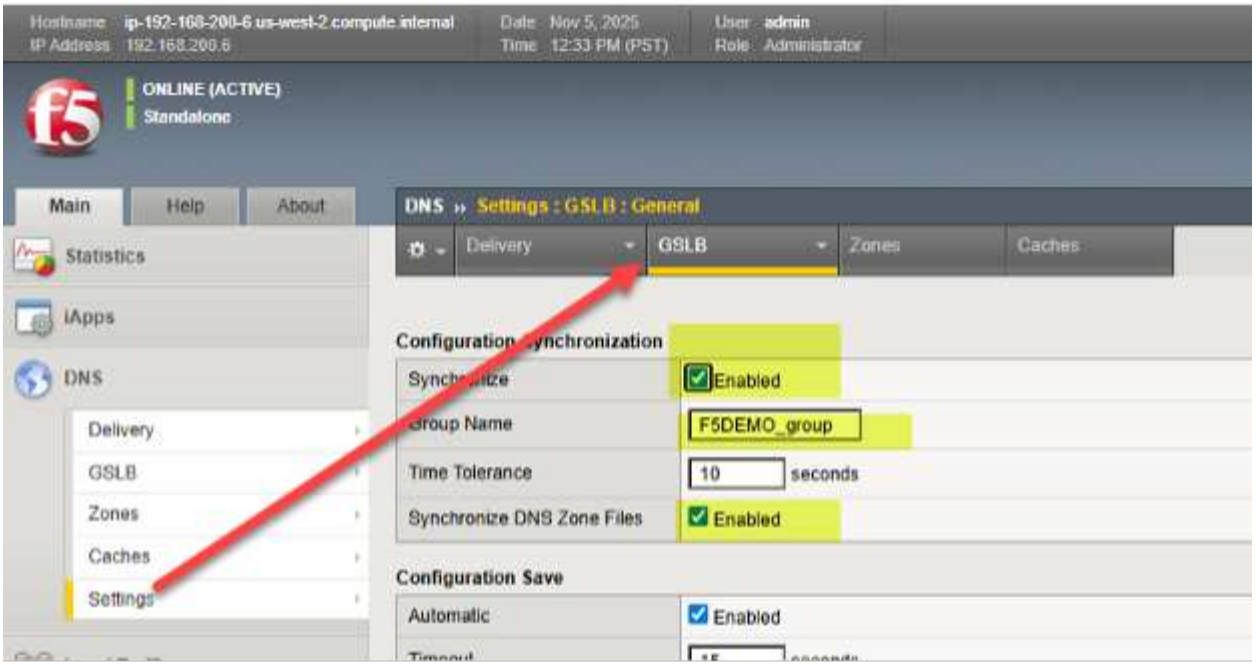
BIG-IP DNS – Erste Schritte bei der Ersteinrichtung

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.

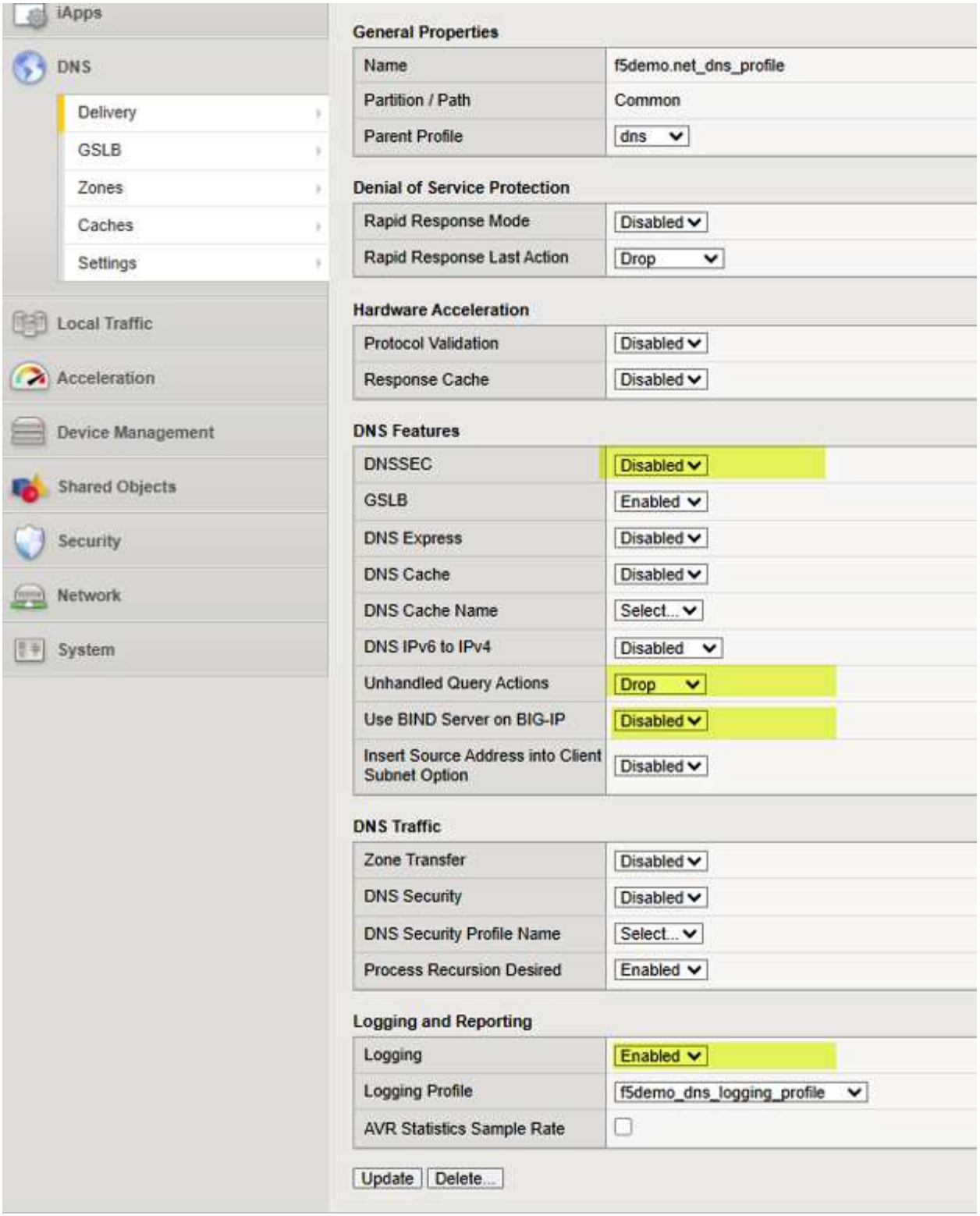


DNS-Protokoll-Grundelemente konfigurieren

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.



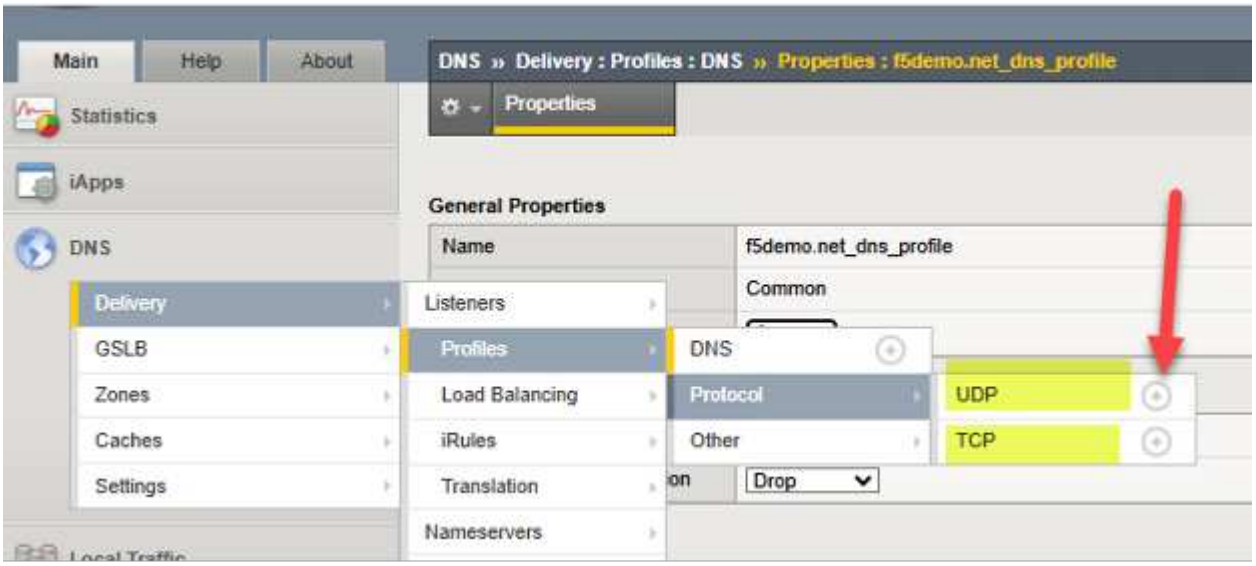
Navigieren Sie anschließend zu DNS > Zustellung > Profile > DNS: Erstellen und erstellen Sie ein Profil, das die DNS-Funktionen steuert, die Sie aktivieren oder deaktivieren möchten. Wenn Sie an der Generierung spezifischer DNS-Protokolle interessiert sind, finden Sie den vorherigen Link zum DNS-Schulungsleitfaden. 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



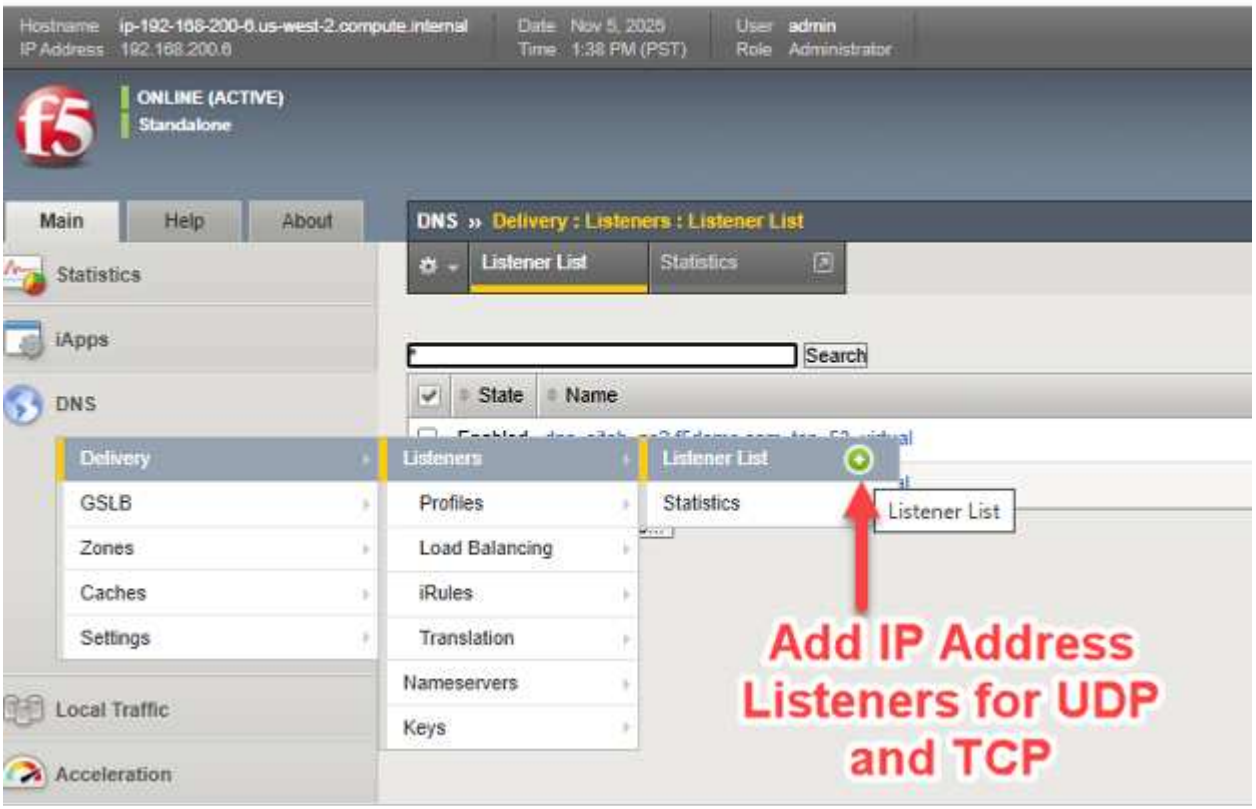
An dieser Stelle können wir die Eigenschaften der UDP- und TCP-Protokolle über erstellte „Profile“ anpassen, die beide DNS-Verkehr mit BIG-IP übertragen können. Erstellen Sie einfach ein neues Profil für UDP und TCP. Unter der Annahme, dass der DNS-Datenverkehr WAN-Verbindungen durchläuft, ist es eine 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“

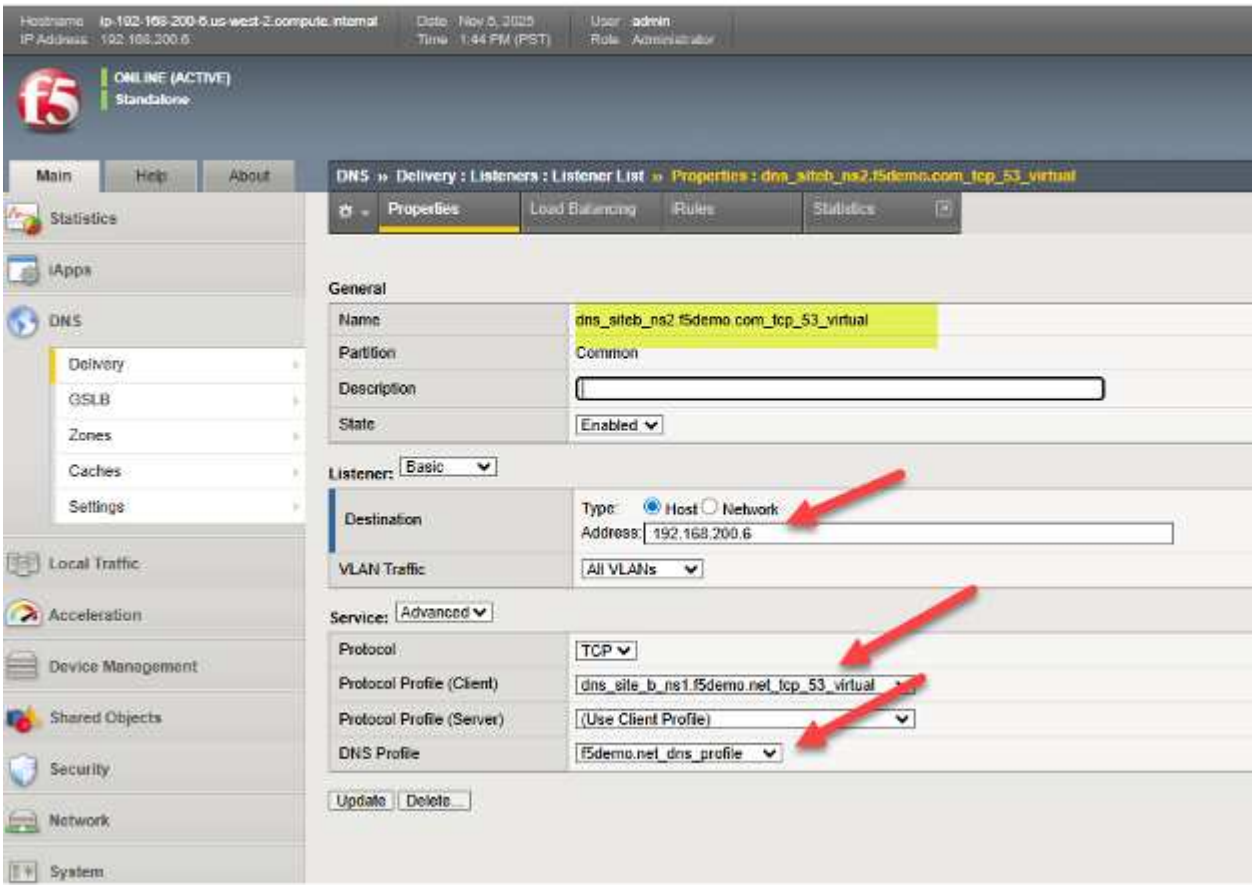


Jetzt müssen wir nur noch dem BIG-IP DNS eine IP-Adresse für den UDP- und TCP-Datenverkehr zuweisen. Für diejenigen, die mit BIG-IP LTM vertraut sind, handelt es sich im Wesentlichen um die Erstellung virtueller DNS-Server, und virtuelle Server benötigen „Listener“-IP-Adressen. Folgen Sie, wie im Screenshot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



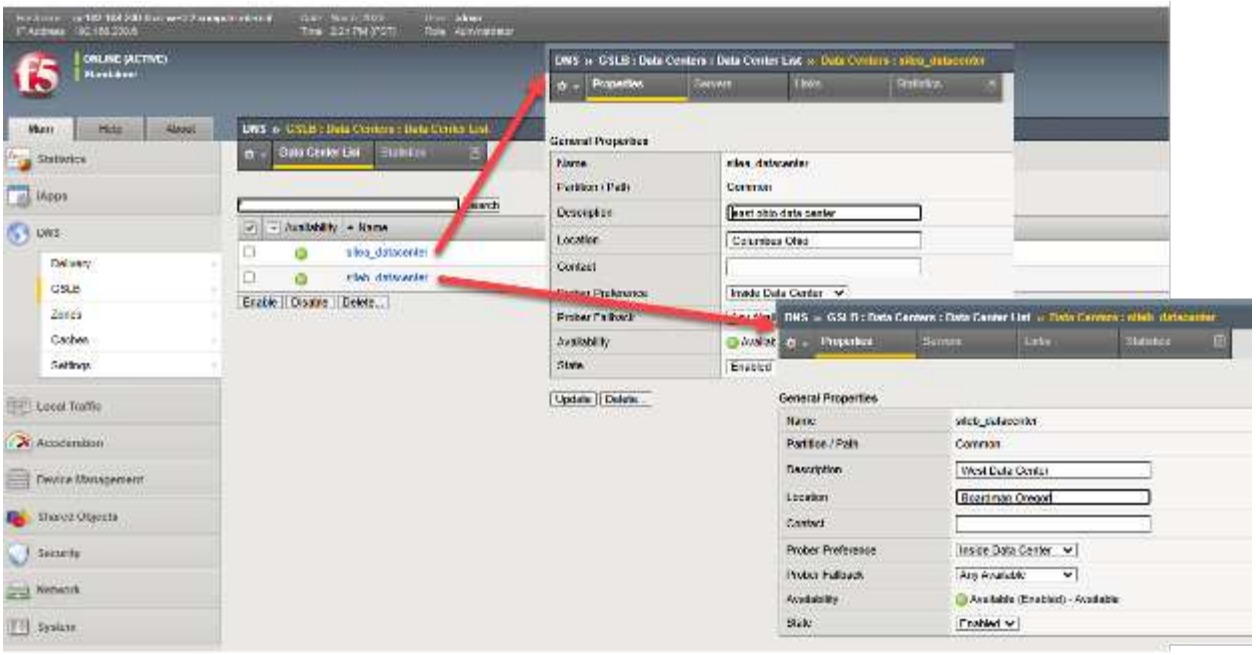
Hiermit sind die vorbereitenden, in der Regel einmaligen Einrichtungsschritte einer BIG-IP-Appliance mit aktiviertem DNS-Modul abgeschlossen. An diesem Punkt sind wir bereit, uns den Details der Einrichtung einer globalen Traffic-Management-Lösung mit unseren Appliances zuzuwenden, die selbstverständlich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

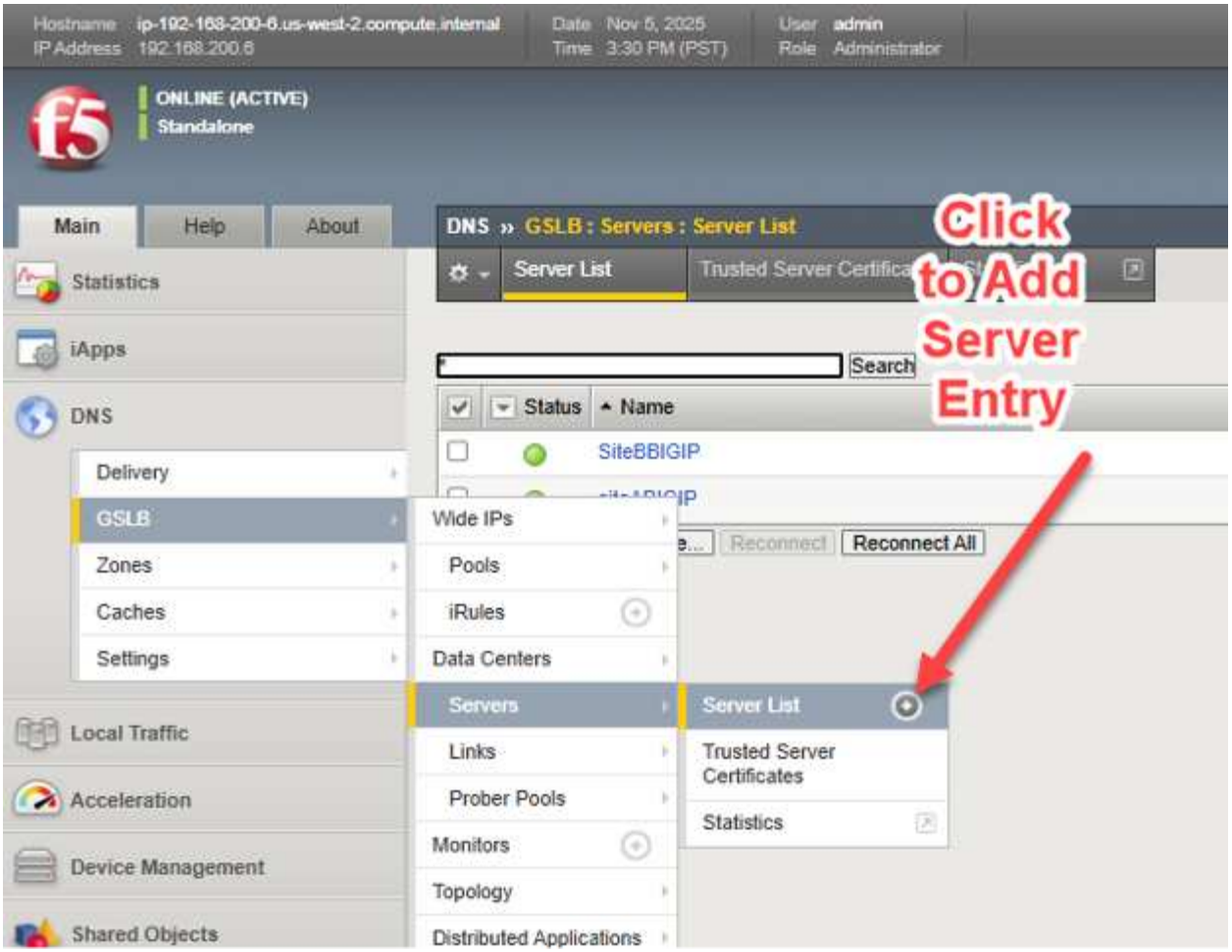
Wir sind nun bereit, die einzelnen StorageGRID Standortcluster mit der BIG-IP-DNS-Konfiguration zu verbinden. Zur Erinnerung: Die BIG-IP-Appliance an jedem Standort übernimmt den eigentlichen Lastausgleich des S3-Datenverkehrs durch die Konfiguration virtueller Server, die eine erreichbare IP-Adresse/einen 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.

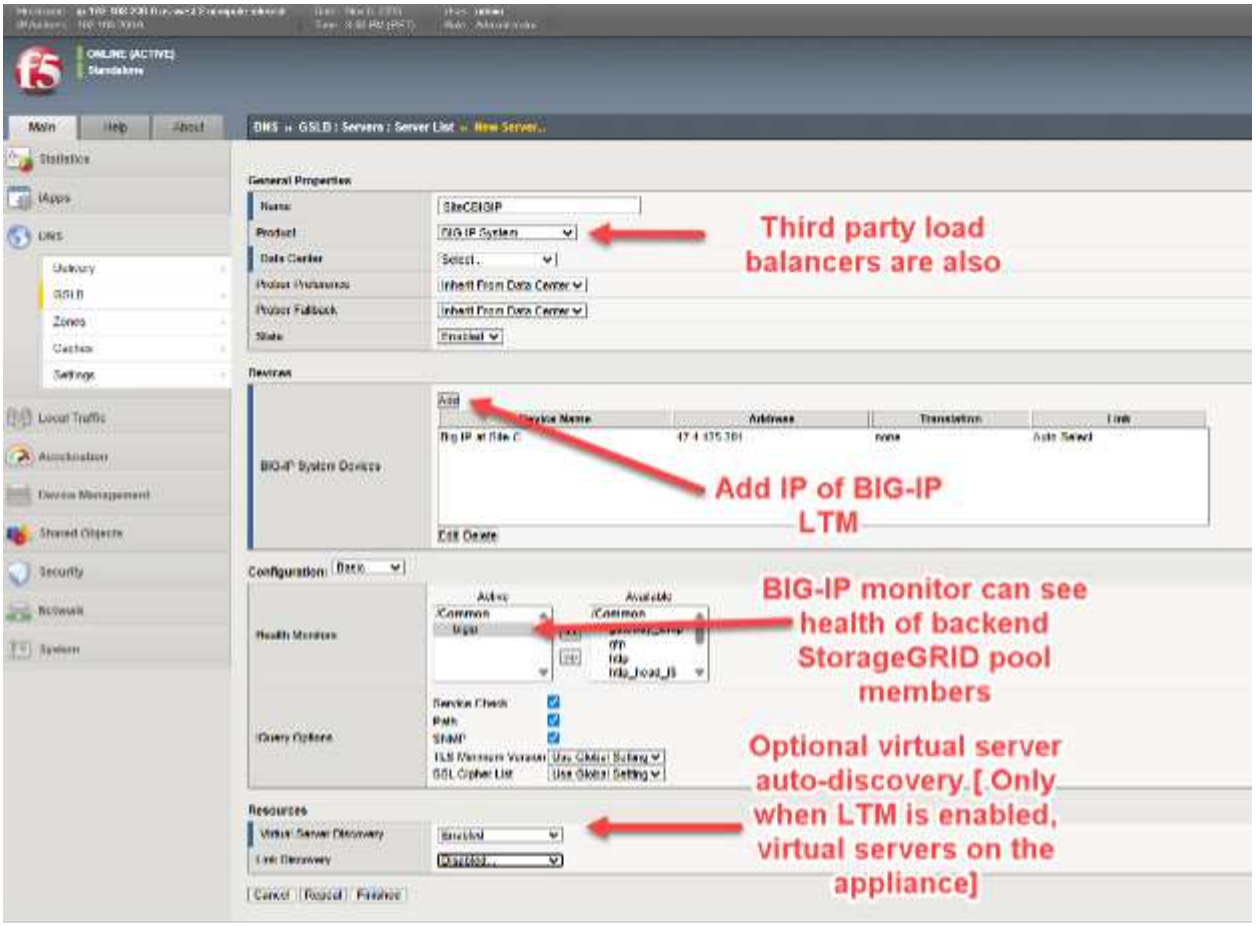
Um die StorageGrid-Sites, insbesondere die lokalen virtuellen Server, mit der BIG-IP-DNS-Konfiguration auf jedem Gerät zu verknüpfen, muss die Einrichtung nur einmal durchgeführt werden. In einem nächsten Schritt werden die Konfigurationen aller BIG-IP DNS-Geräte synchronisiert.

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.

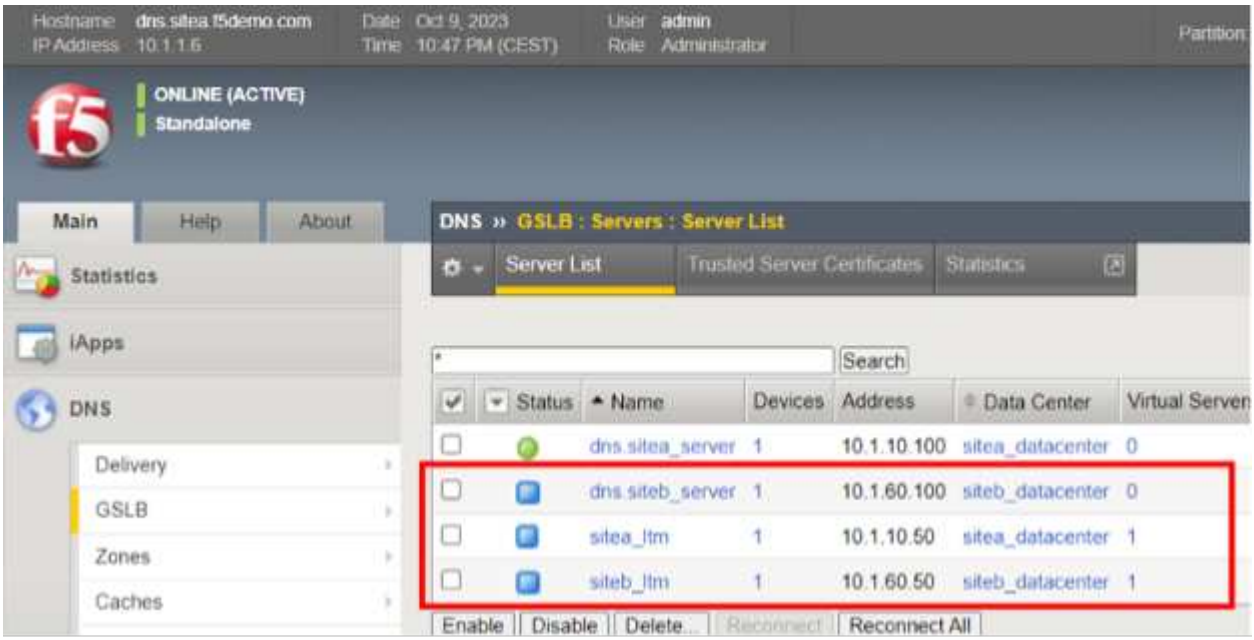


In bestimmten Situationen, wie z. B. bei vorübergehenden Netzwerkproblemen oder Firewall-ACL-Regeln zwischen Netzwerkstandorten, werden bei der Hinzufügung einer Remote-Appliance in diesem Stadium möglicherweise keine Einträge für Remote-Appliances mit konfiguriertem LTM bei der virtuellen Servererkennung 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.

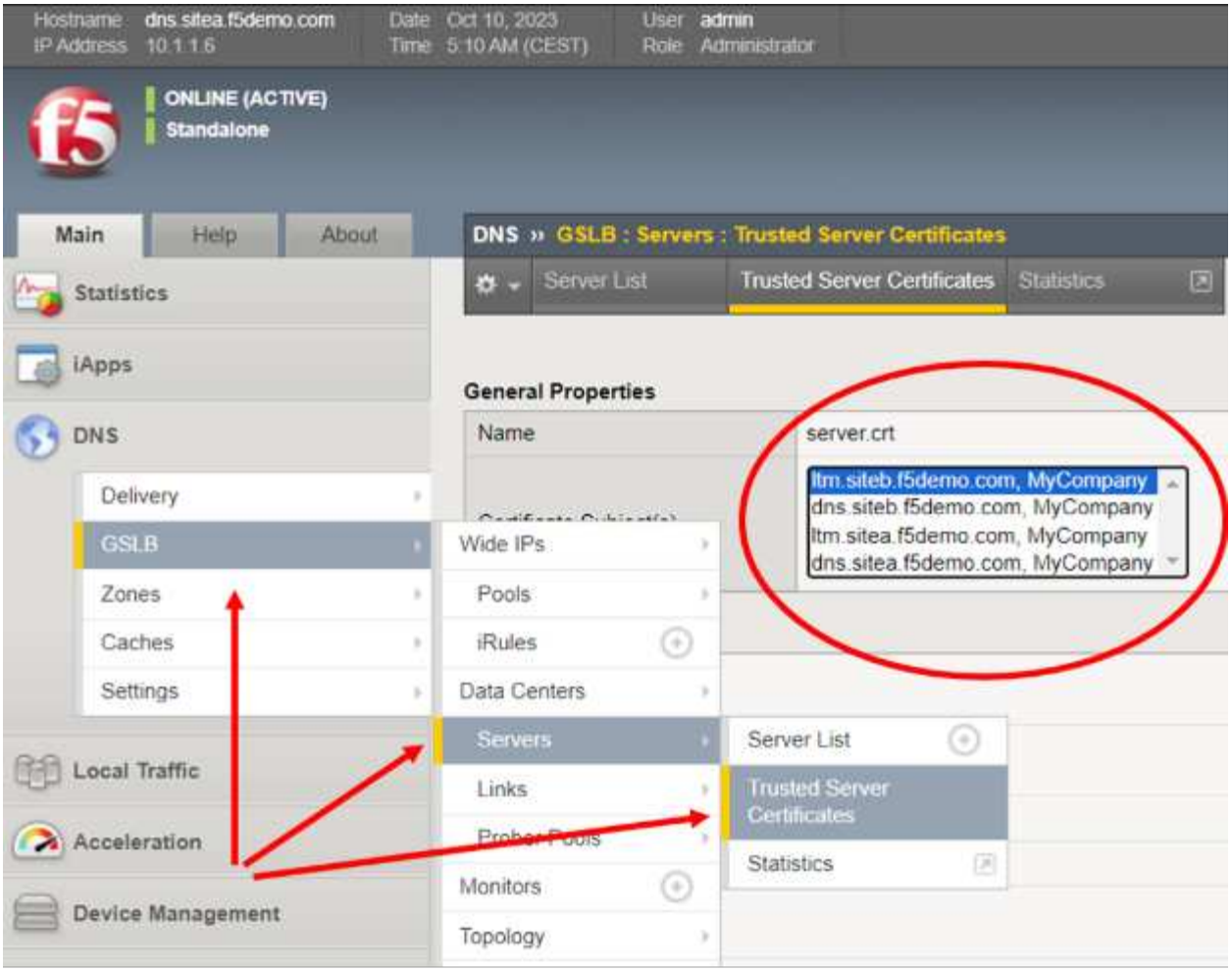
Schritt drei: Vertrauensverhältnis zwischen allen BIG-IP-Appliances herstellen

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.

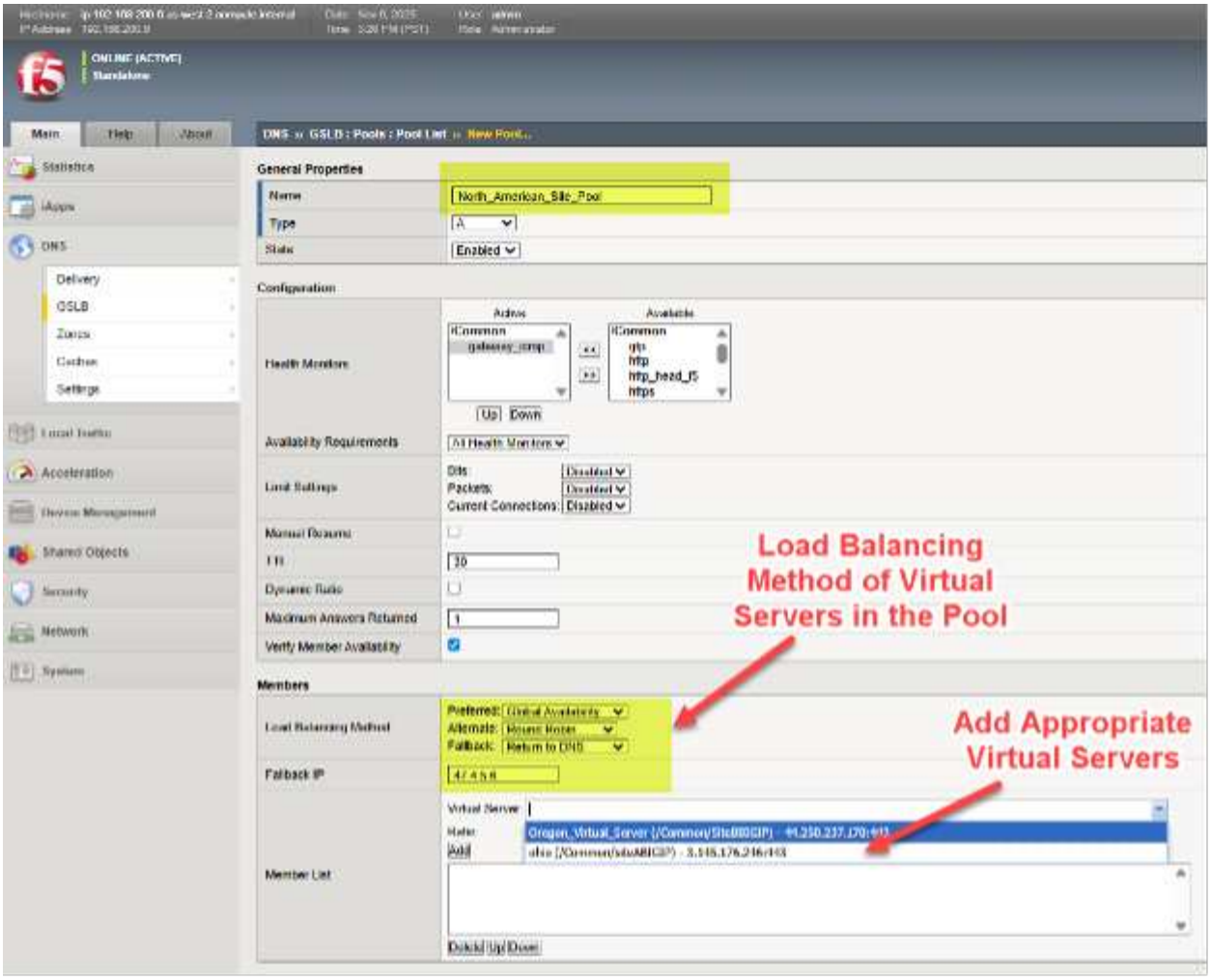
Weite IP-Adressen, Adresspools und virtuelle Server kurz erklärt

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.

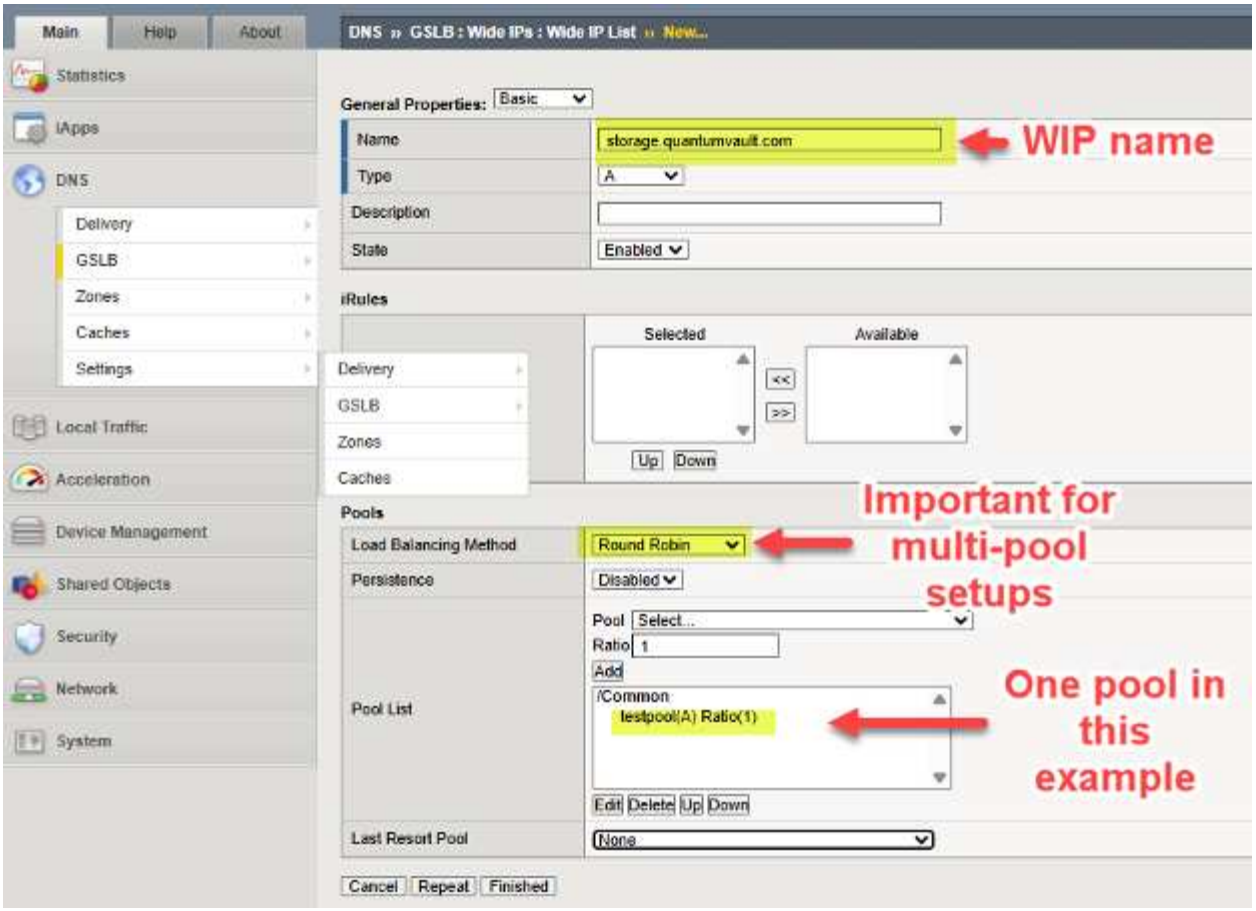
Die Auswahl des Pools könnte durch eine Reihe von politischen Entscheidungen erfolgen; vielleicht könnte ein einfaches Verhältnis von 5:1 verwendet werden, um den Großteil des Datenverkehrs auf nordamerikanische StorageGRID Standorte zu lenken. Wahrscheinlicher ist vielleicht eine topologiebasierte Wahl, 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

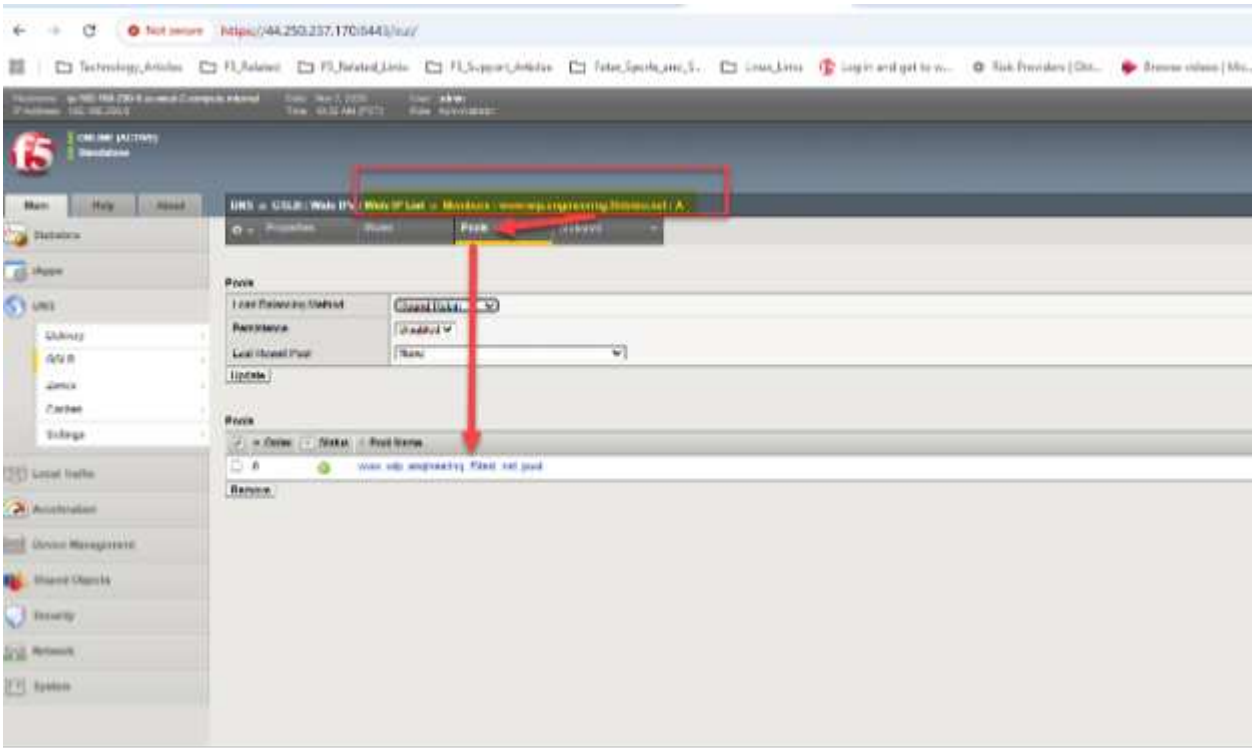
An diesem Punkt sind alle unsere zugrunde liegenden BIG-IP-Appliances bereit, GSLB (Global Server Load Balancing) durchzuführen. Wir müssen lediglich die für die S3-Datenflüsse verwendeten Namen anpassen und zuweisen, um die Lösung optimal nutzen zu können. Der allgemeine Ansatz besteht darin, einen 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.

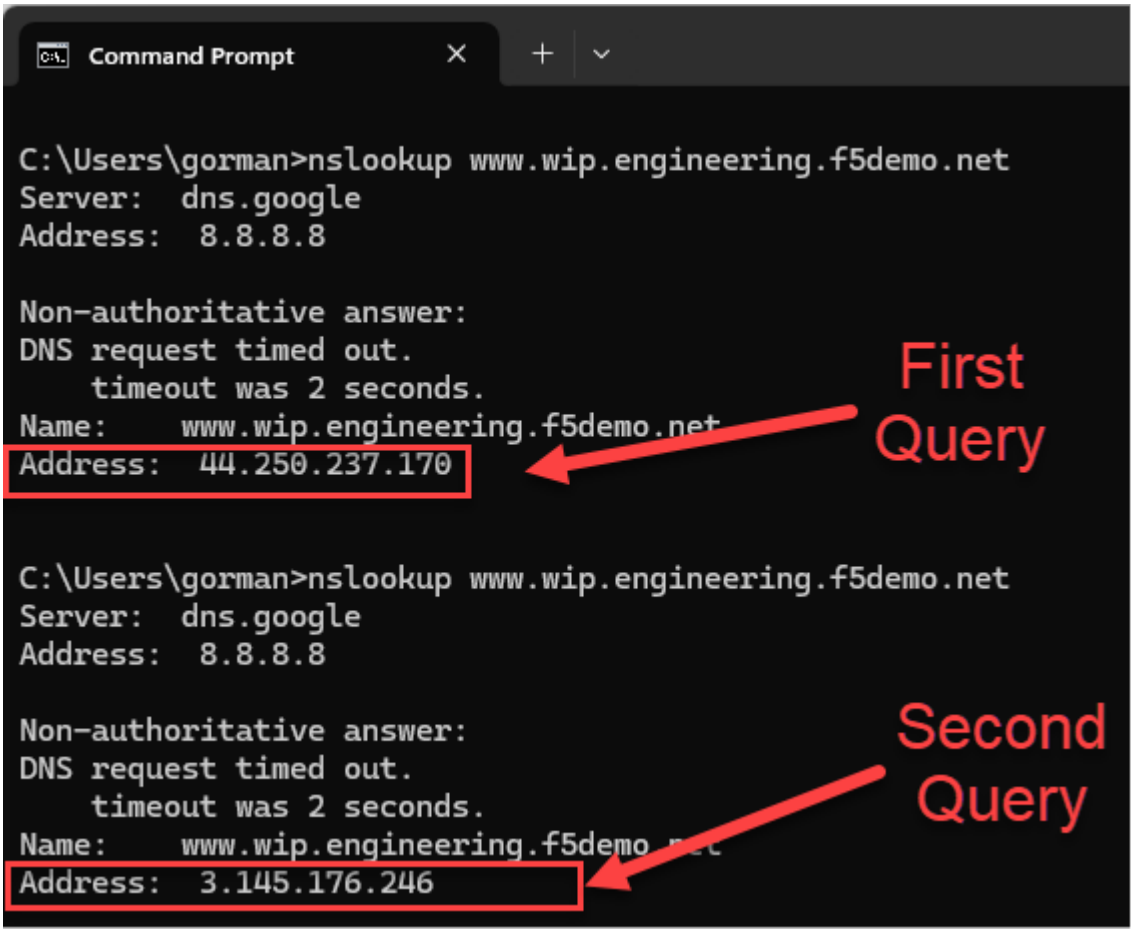
Als Beispiel richten wir nun eine Wide IP (WIP) in unserem BIG-IP DNS ein. Da DNS die Gruppensynchronisierung nutzt, müssen wir die Einstellungen nur über die GUI eines Geräts anpassen. Innerhalb der BIG-IP DNS GUI gehen Sie zu **DNS > GSLB > Wide IPs > Wide IP List (+)**. Zur Erinnerung: Bei einer herkömmlichen 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.

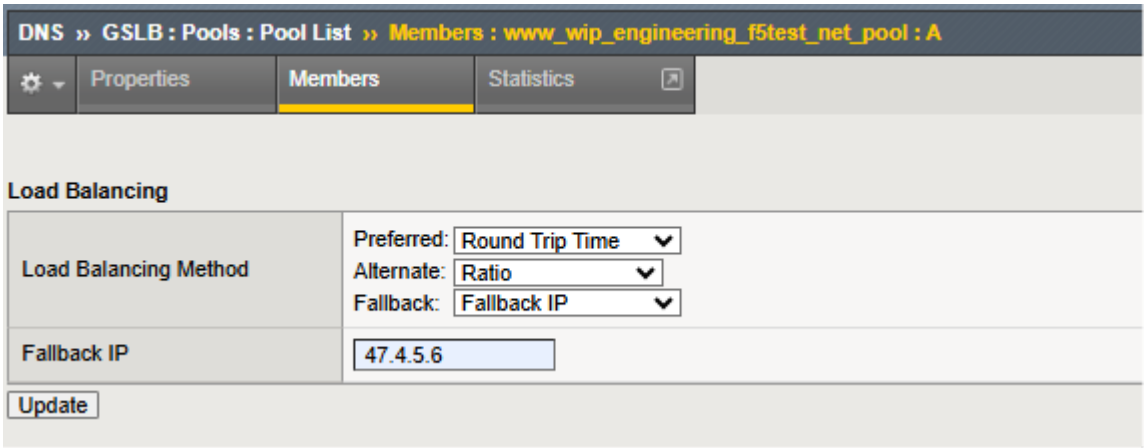


Vorschläge zur Erkundung fortgeschrittenerer Techniken

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'
```

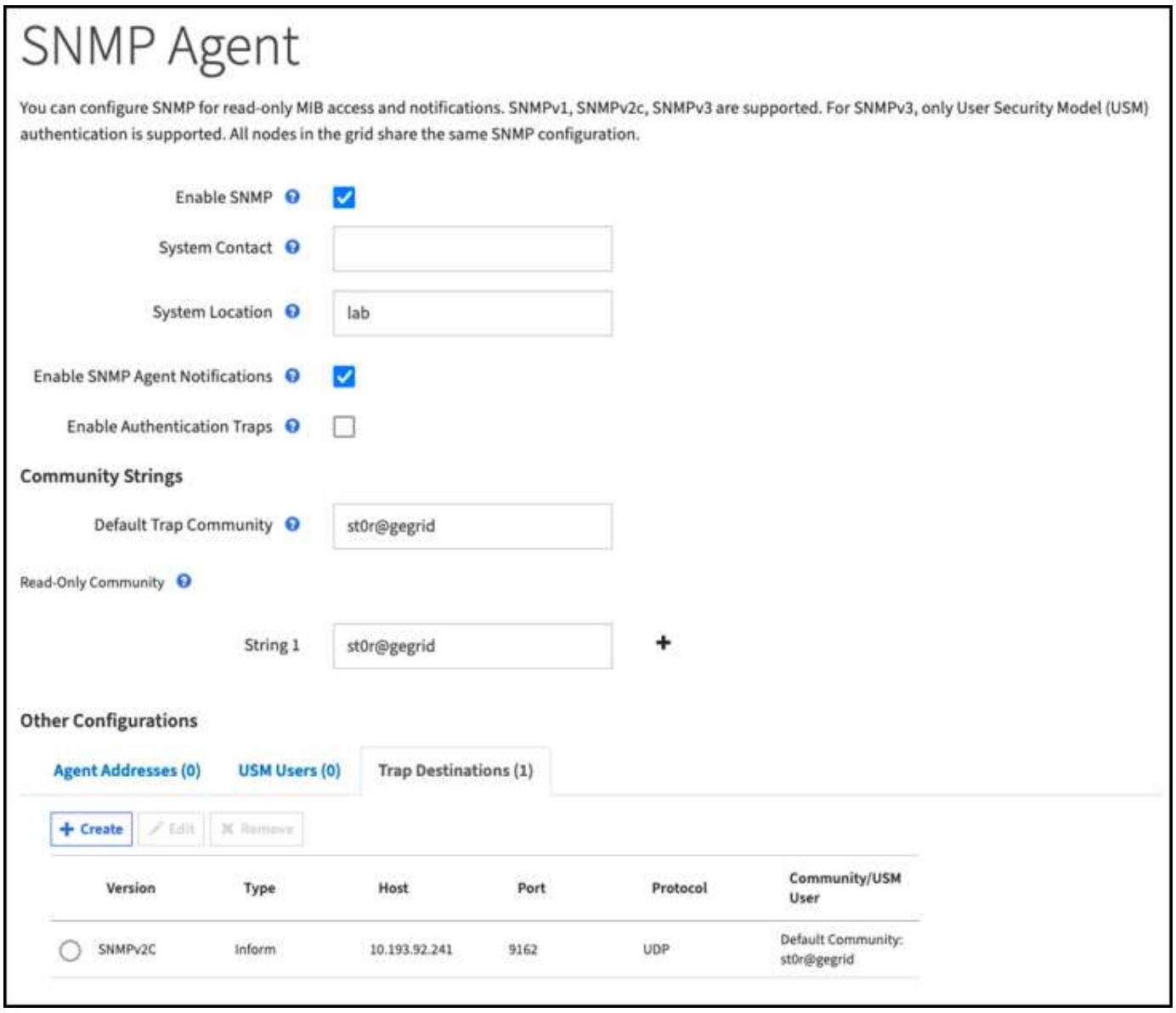
SNMP-Konfiguration für Traps

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:

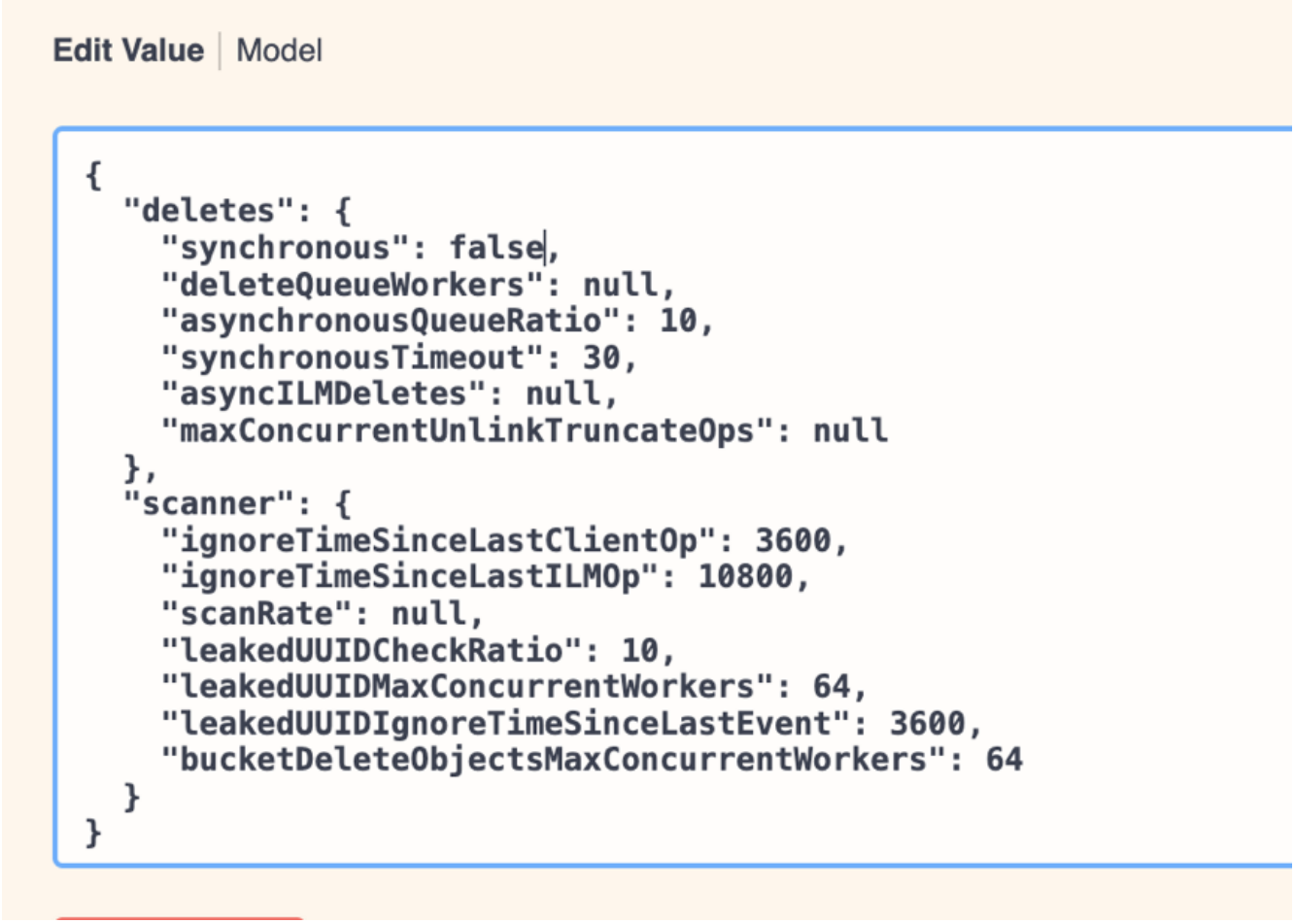
Response body


```
{
  "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:

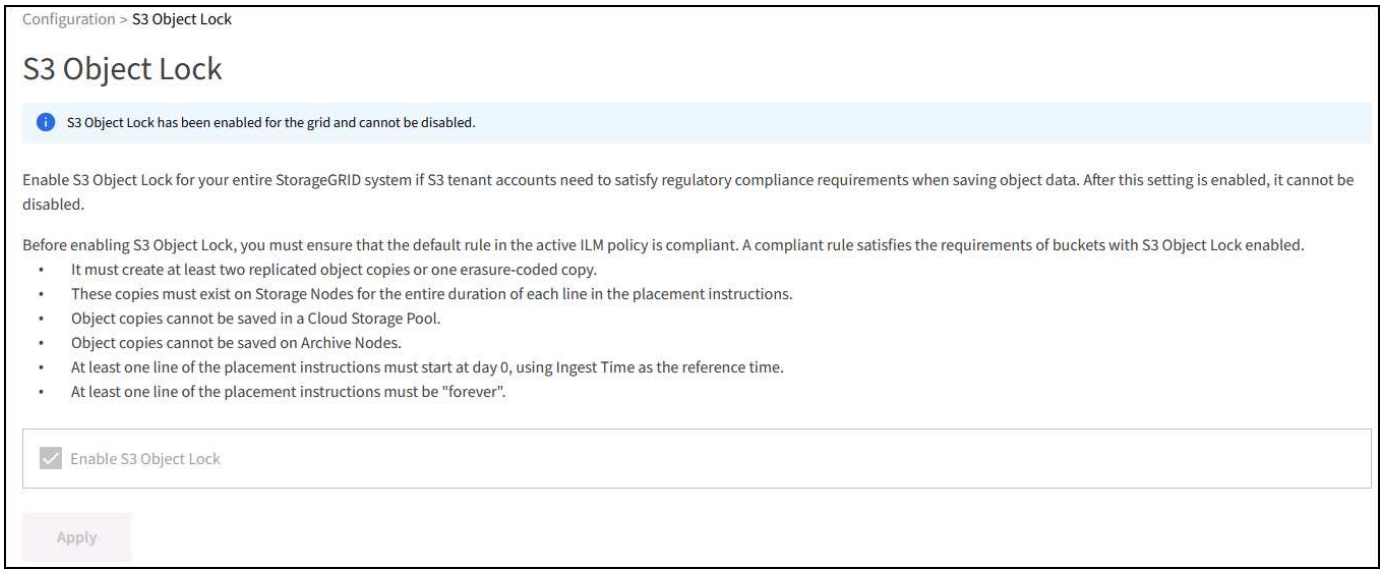


12. Wenn Sie fertig sind, wählen Sie Ausführen

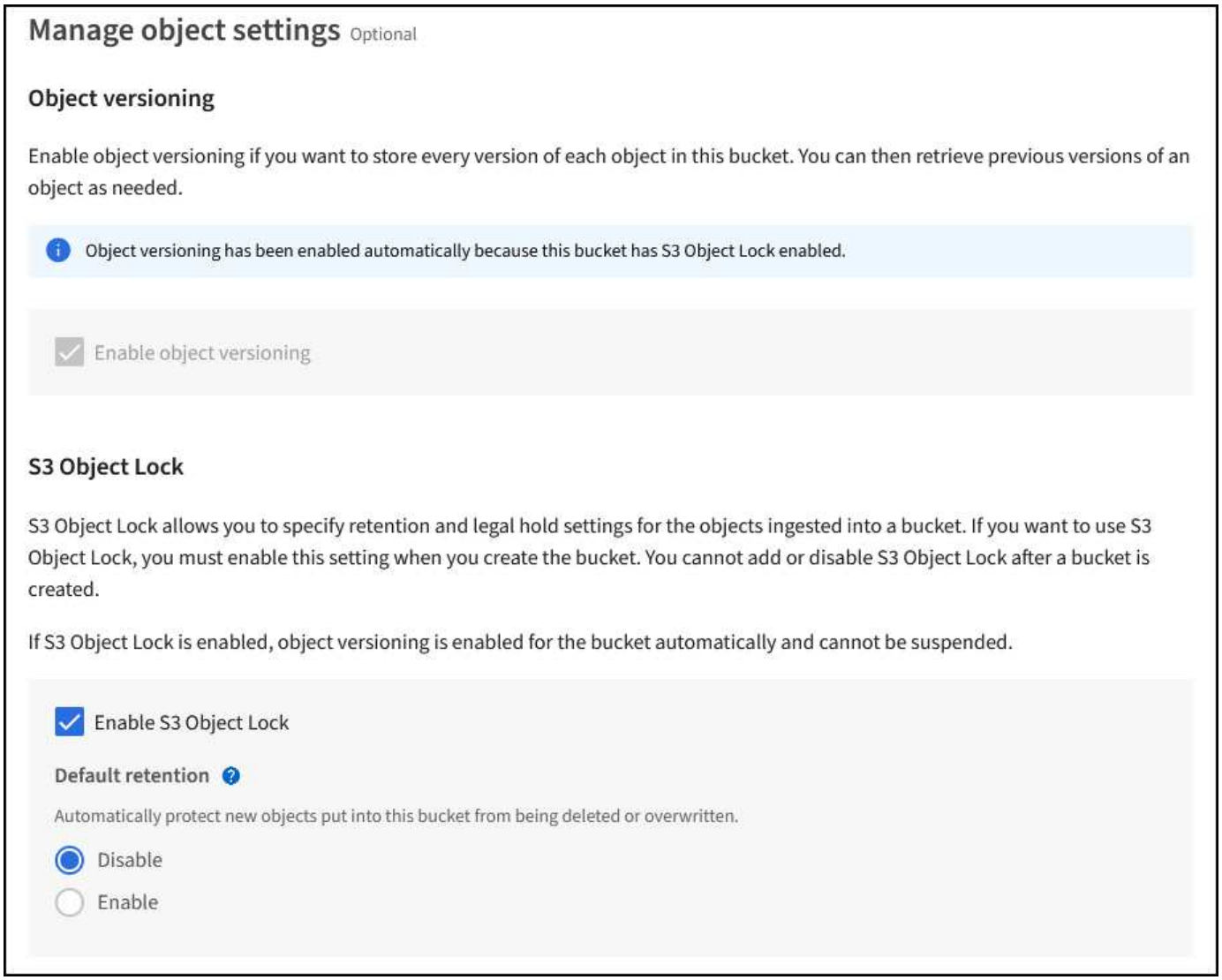
Zentrale Punkte bei der Implementierung

StorageGRID

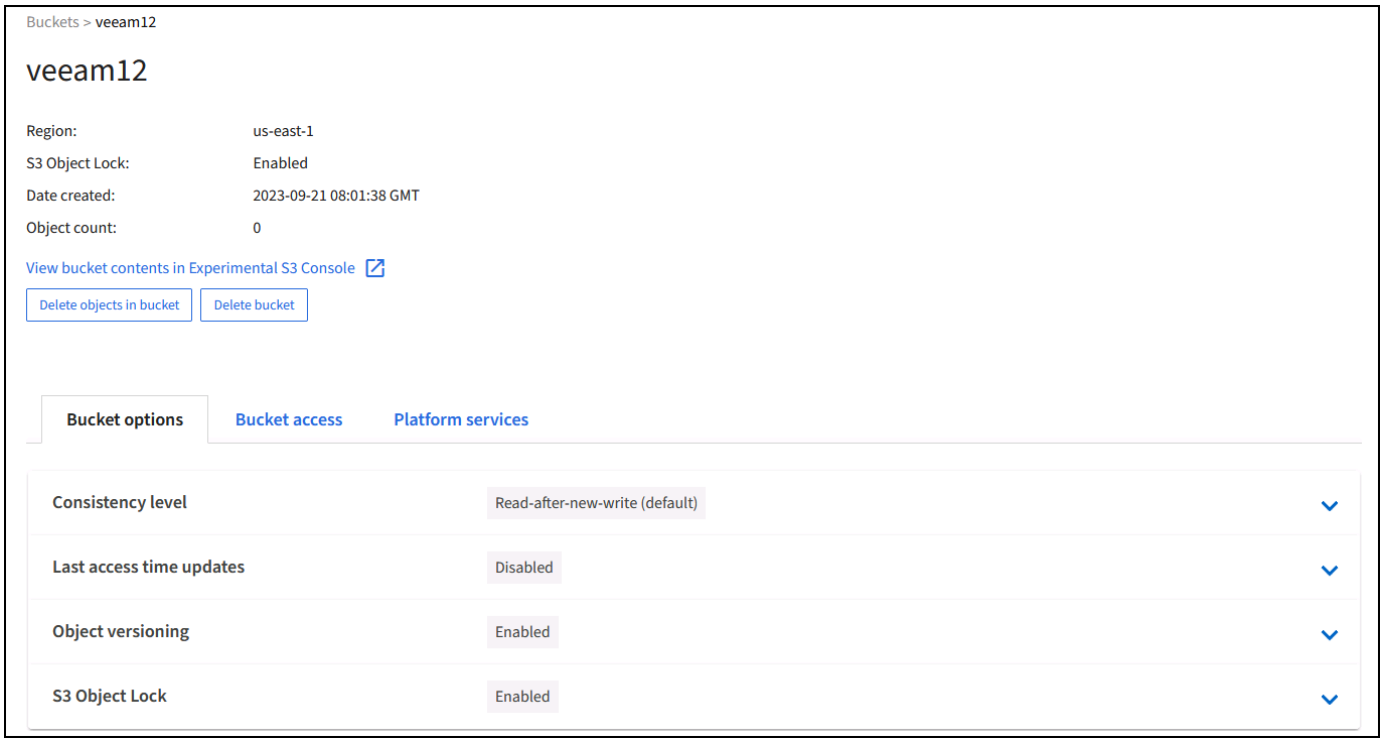
Stellen Sie sicher, dass die Objektsperre auf dem StorageGRID System aktiviert ist, falls eine Unveränderlichkeit erforderlich ist. Suchen Sie die Option in der Management-UI unter Configuration/S3 Object Lock.



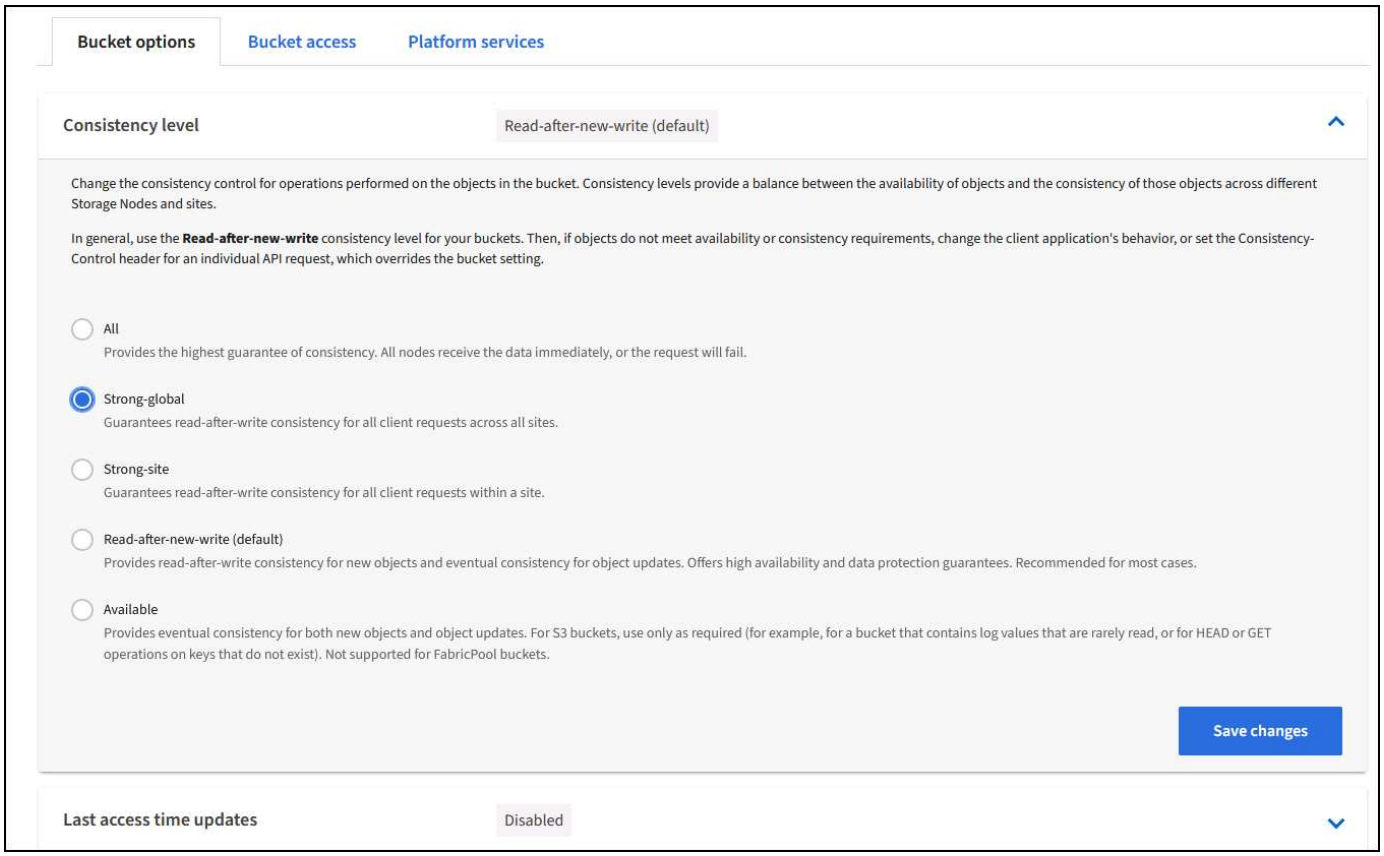
Wählen Sie bei der Erstellung des Buckets die Option „S3 Object Lock aktivieren“ aus, wenn dieser Bucket zur Unveränderlichkeit von Backups verwendet werden soll. Dadurch wird die Bucket-Versionierung automatisch aktiviert. Die Standardaufbewahrung bleibt deaktiviert, da Veeam die Objektaufbewahrung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



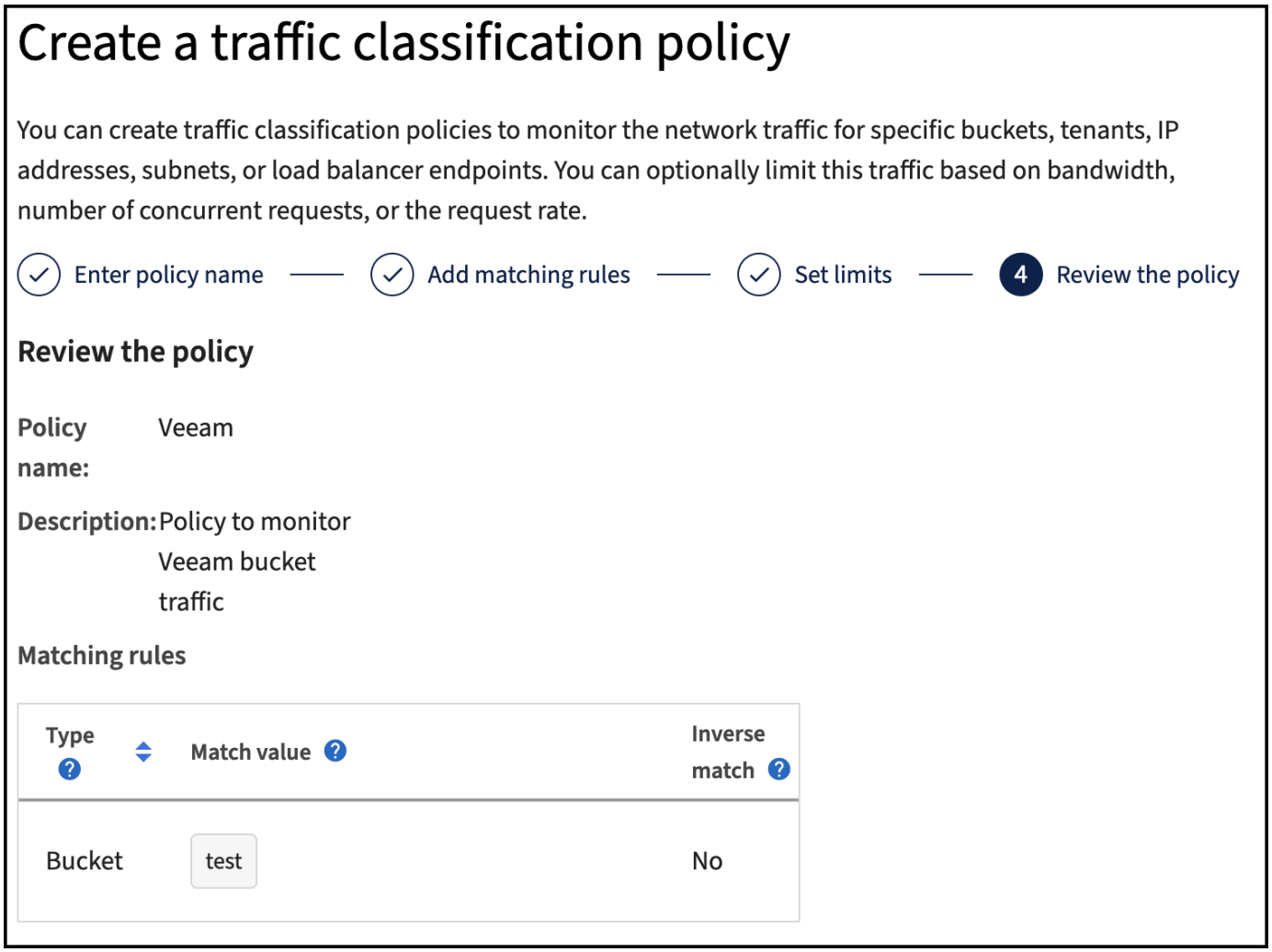
Veeam erfordert eine hohe Konsistenz für S3-Buckets. Wenn also Implementierungen an mehreren Standorten implementiert werden, bei denen Veeam von diversen Standorten auf die Daten zugreifen kann, wählen Sie „Strong Global“. Wenn Veeam-Backups und -Restores nur an einem einzigen Standort durchgeführt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

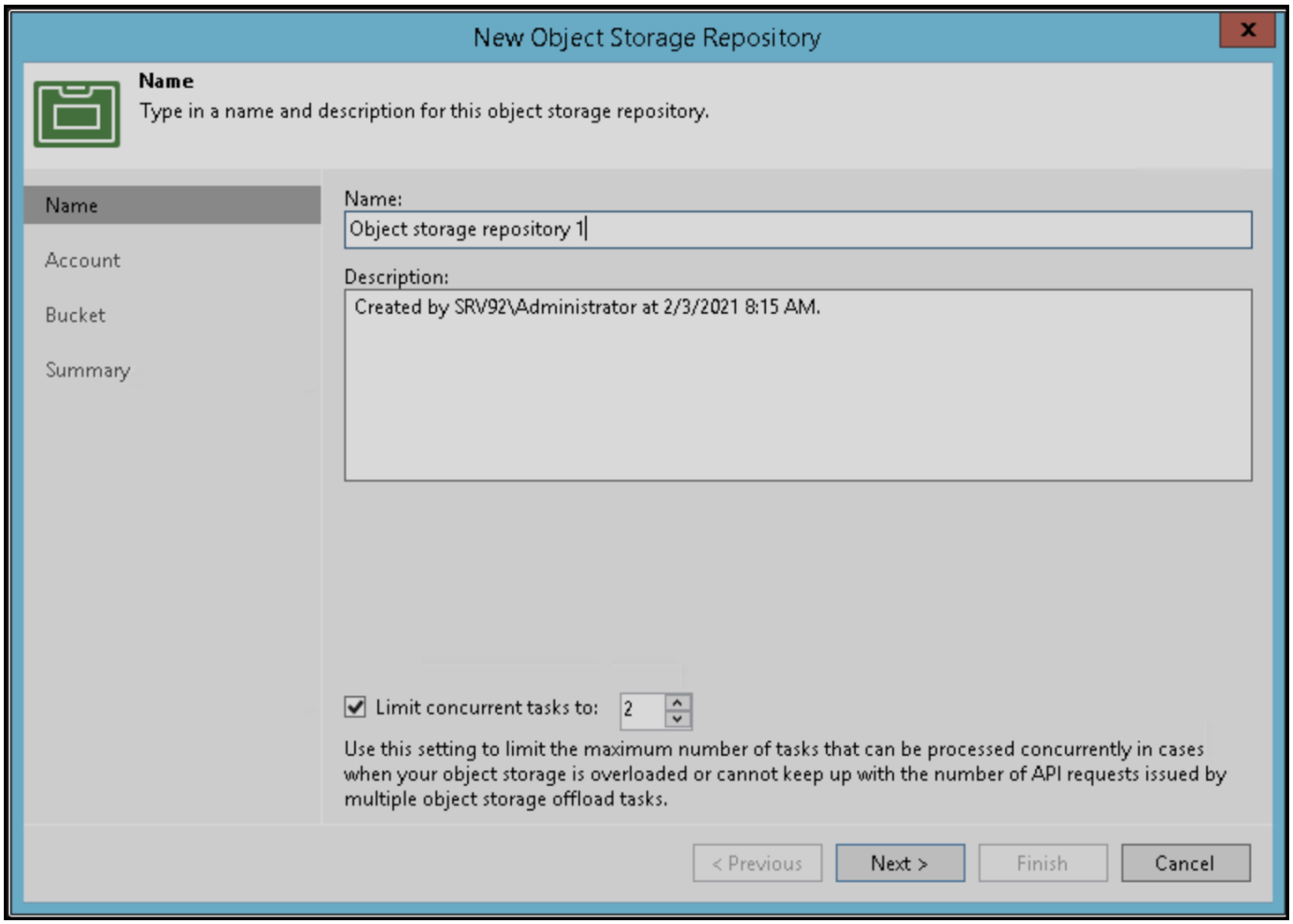
Einer der vielen Vorteile dieser Load Balancer ist die Möglichkeit zur Konfiguration von Richtlinien zur Traffic-Klassifizierung (QoS). Diese dienen hauptsächlich der Beschränkung der Auswirkungen von Applikationen auf andere Client-Workloads oder der Priorisierung von Workloads gegenüber anderen. Sie 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.

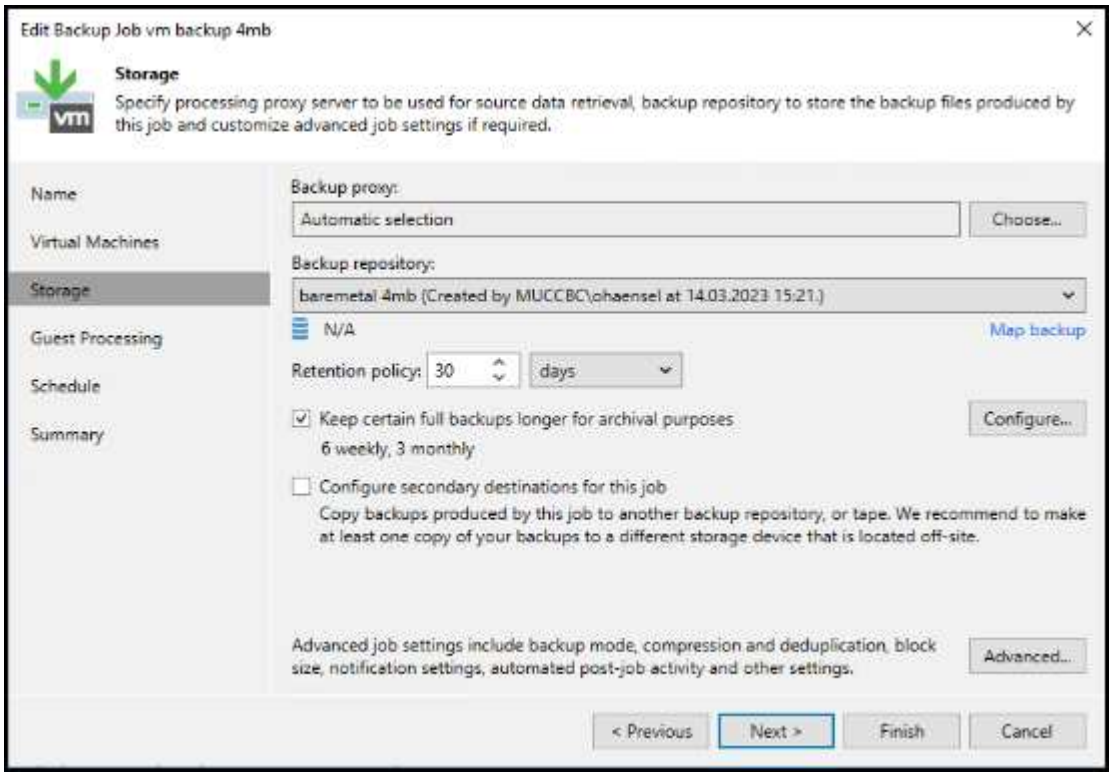


Veeam

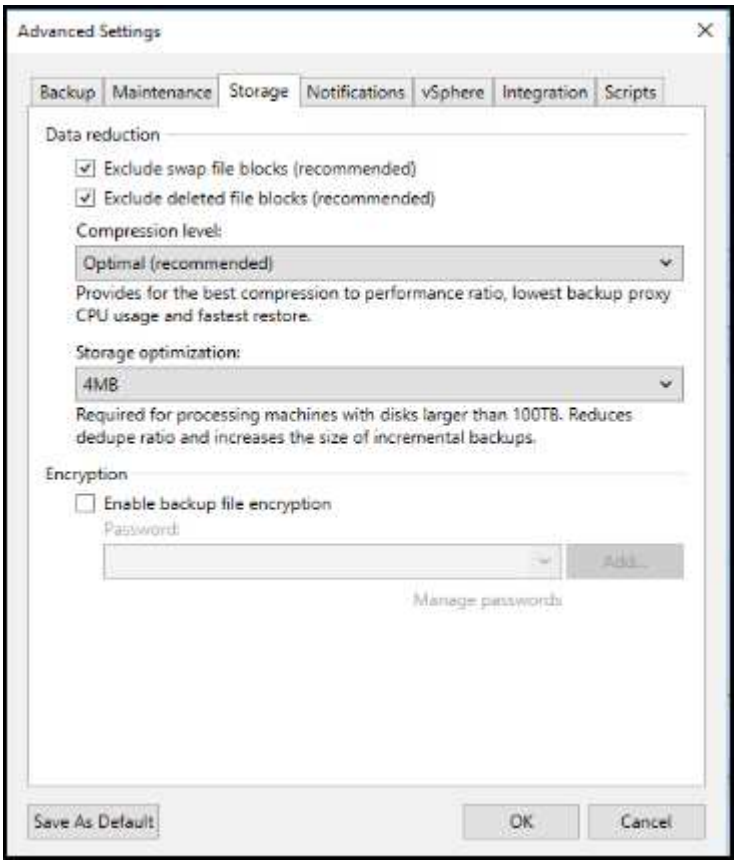
Je nach Modell und Anzahl der StorageGRID Appliances kann es erforderlich sein, eine Begrenzung der Anzahl gleichzeitiger Operationen auf dem Bucket auszuwählen und zu konfigurieren.



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

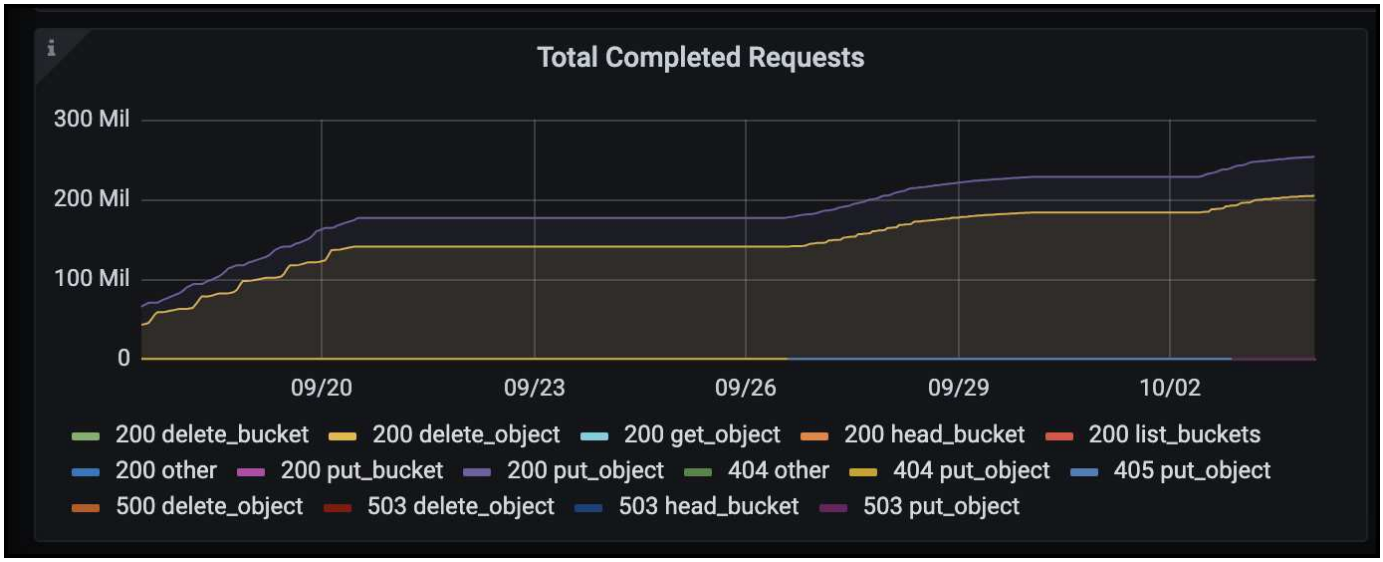
Um sich ein vollständiges Bild davon zu machen, wie Veeam und StorageGRID zusammenarbeiten, müssen Sie warten, bis die Aufbewahrungszeit der ersten Backups abgelaufen ist. Bis zu diesem Zeitpunkt besteht der Veeam-Workload in erster Linie aus PUT-Vorgängen und es sind keine Löschungen aufgetreten. Sobald 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.

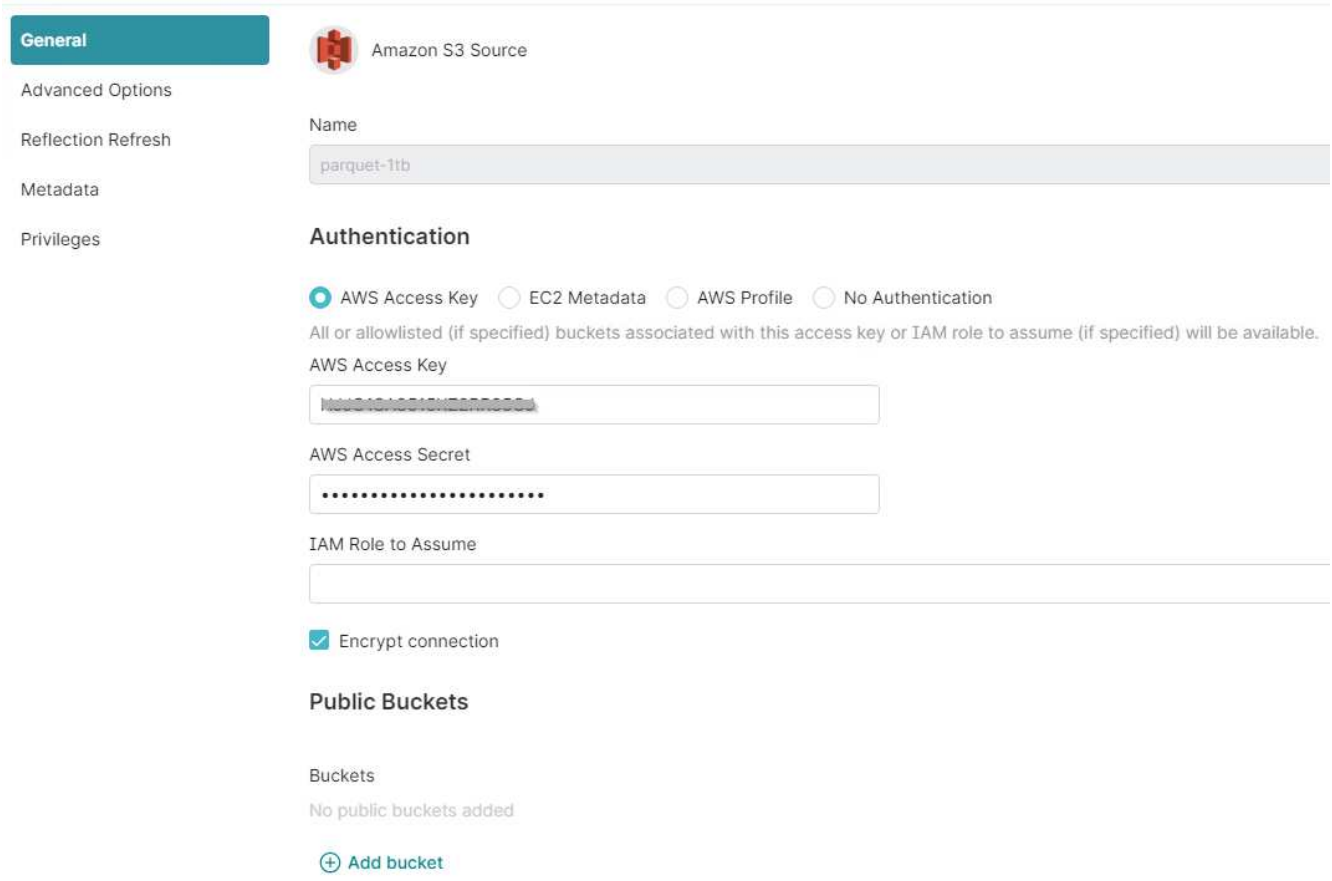
Dremio-Führer

"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

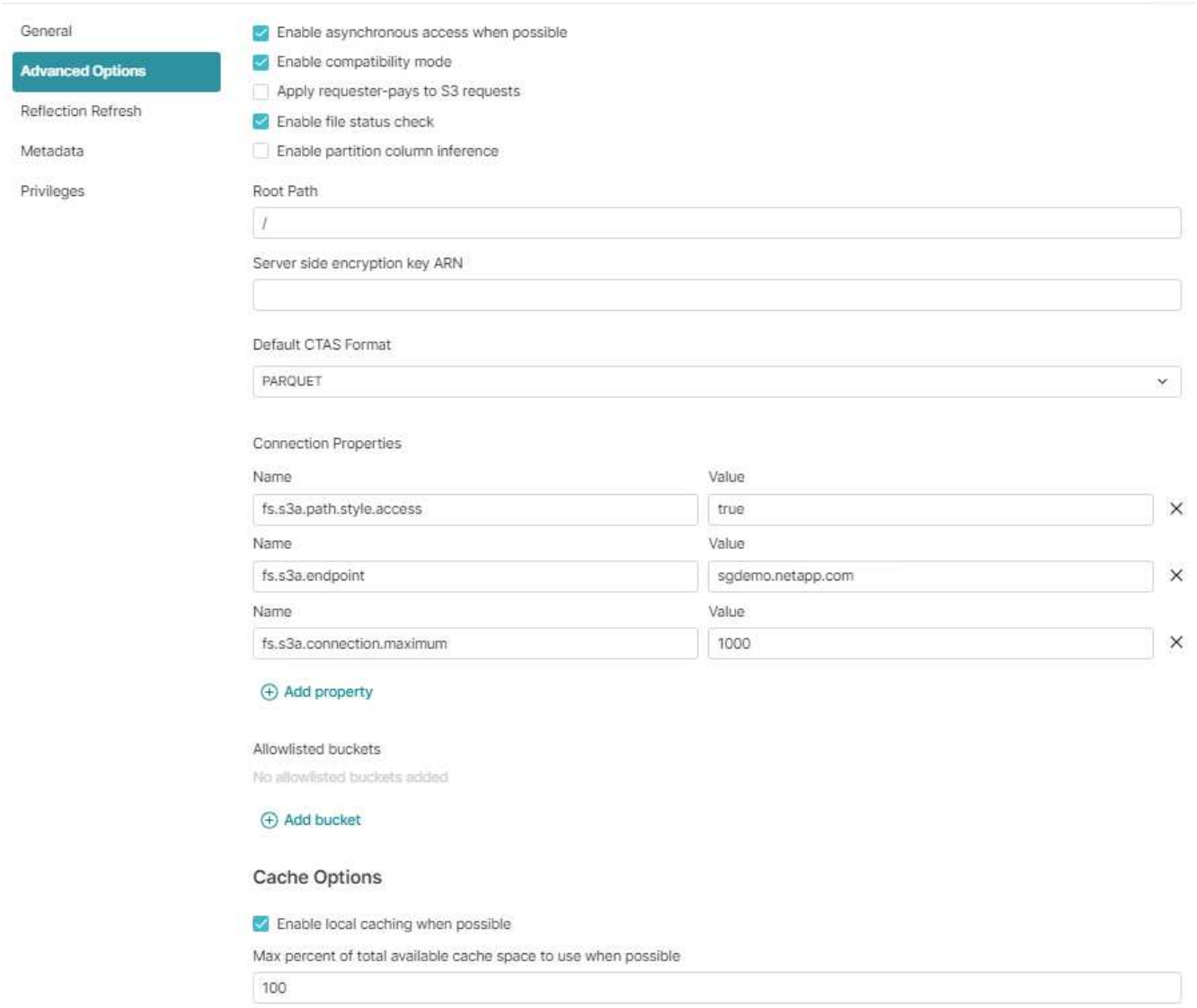
StorageGRID S3-Endpunkt verwendet wird.
Wenn Sie ein selbstsigniertes CA-Zertifikat für diesen s3-Endpunkt verwenden, folgen Sie der Dremio-Anleitung, um dieses CA-Zertifikat in den <JAVA_HOME>/jre/lib/Security + des Dremio-Servers hinzuzufügen
Beispiel Screenshot



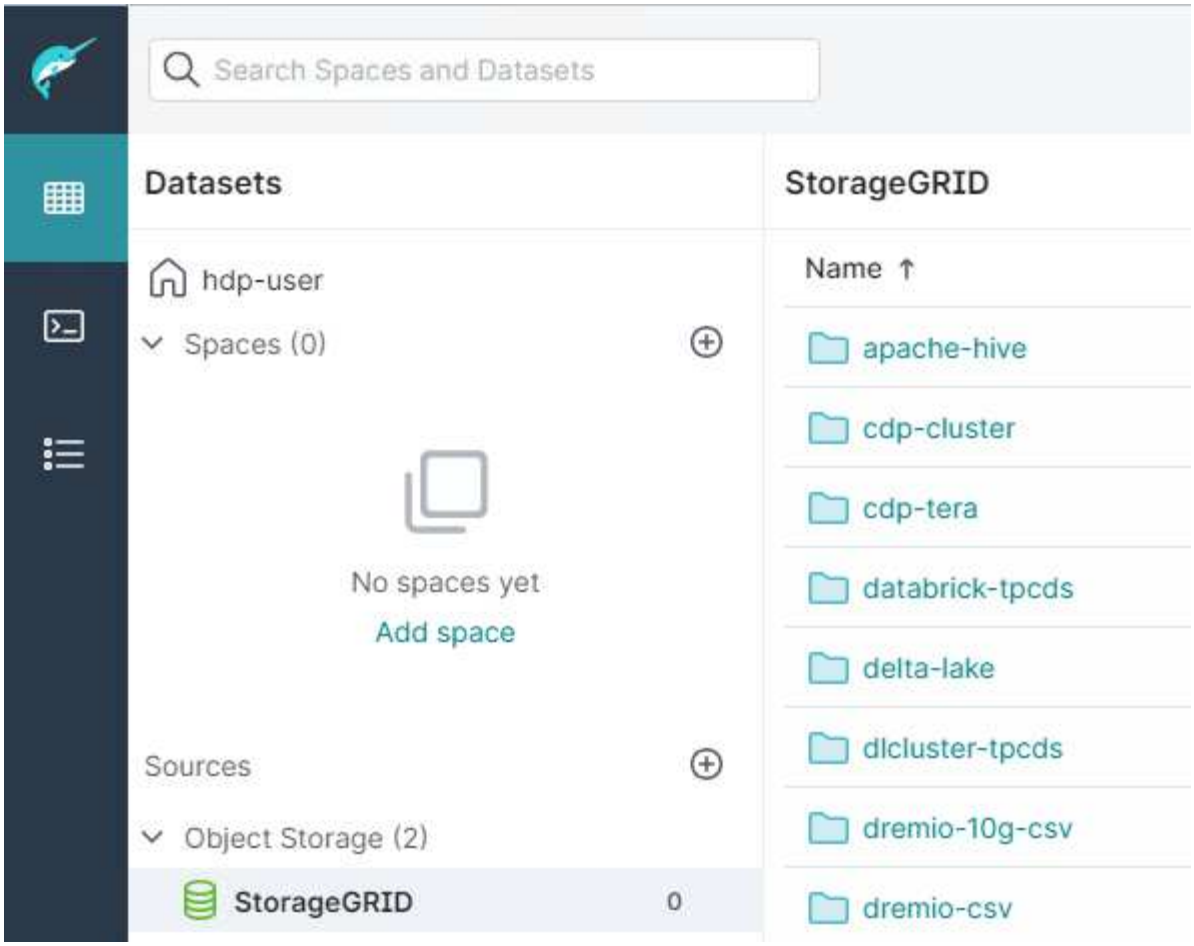
4. Klicken Sie auf „Erweiterte Optionen“, und aktivieren Sie „Kompatibilitätsmodus aktivieren“.
5. Klicken Sie unter Verbindungseigenschaften auf + Eigenschaften hinzufügen, und fügen Sie diese s3a-Eigenschaften hinzu.
6. fs.s3a.Connection.die Standardeinstellung ist 100. Wenn Ihre s3-Datensätze große 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'
```