Technische Berichte

StorageGRID solutions and resources

NetApp
December 12, 2025

Inhalt

Technische Berichte

Einführung in technische Berichte von StorageGRID

NetApp StorageGRID ist eine Suite für softwaredefinierten Objekt-Storage, die eine Vielzahl von Anwendungsfällen in Public-, Private- und Hybrid-Multi-Cloud-Umgebungen unterstützt. StorageGRID bietet nicht nur nativen Support für die Amazon S3-API, sondern auch branchenführende Innovationen wie automatisiertes Lifecycle Management. Damit können Sie unstrukturierte Daten kostengünstig über längere Zeiträume hinweg speichern, sichern, schützen und aufbewahren.

StorageGRID enthält eine Dokumentation, in der Best Practices und Empfehlungen für verschiedene Funktionen und Integrationen von StorageGRID behandelt werden.

NetApp StorageGRID und Big Data Analytics

Anwendungsfälle für NetApp StorageGRID

Die NetApp StorageGRID Objekt-Storage-Lösung bietet Skalierbarkeit, Datenverfügbarkeit, Sicherheit und hohe Performance. Unternehmen jeder Größe und Branche nutzen StorageGRID S3 für zahlreiche Anwendungsfälle. Sehen wir uns einige typische Szenarien an:

Big Data Analytics: StorageGRID S3 wird häufig als Data Lake verwendet, wo Unternehmen mit Tools wie Apache Spark, Splunk SmartStore und Dremio große Mengen an strukturierten und unstrukturierten Daten für Analysen speichern.

Daten-Tiering: NetApp Kunden nutzen die FabricPool Funktion von ONTAP, um Daten automatisch zwischen einem hochperformanten lokalen Tier zu StorageGRID zu verschieben. Durch Tiering wird teurer Flash-Storage für häufig abgerufene Daten frei. Kalte Daten werden auf kostengünstigem Objekt-Storage bereitgehalten. Dadurch werden Performance und Einsparungen maximiert.

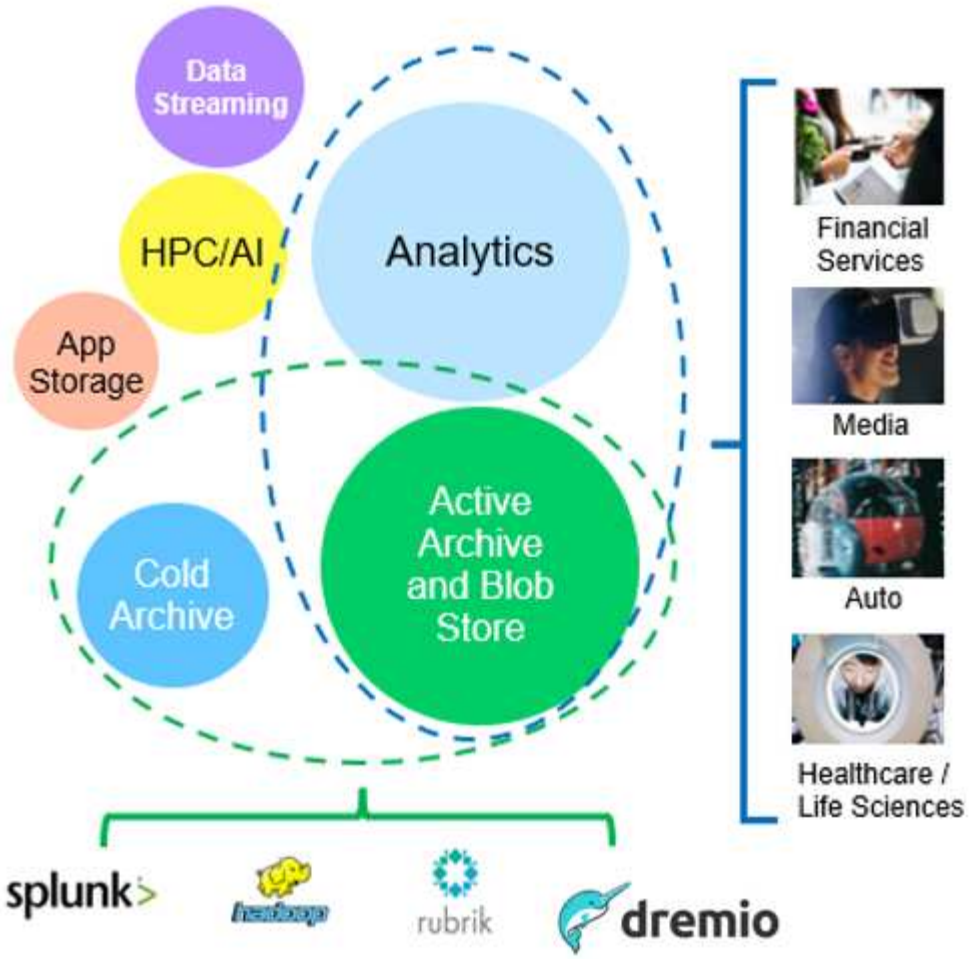
Daten-Backup und Disaster Recovery: Unternehmen können StorageGRID S3 als zuverlässige und kostengünstige Lösung für Backup und Recovery kritischer Daten im Notfall einsetzen.

Datenspeicher für Anwendungen: StorageGRID S3 kann als Speicher-Backend für Anwendungen verwendet werden, so dass Entwickler Dateien, Bilder, Videos und andere Arten von Daten einfach speichern und abrufen können.

Inhaltsbereitstellung: StorageGRID S3 kann verwendet werden, um statische Website-Inhalte, Mediendateien und Software-Downloads für Benutzer auf der ganzen Welt zu speichern und bereitzustellen. Dabei wird die geografische Distribution und der globale Namespace von StorageGRID für eine schnelle und zuverlässige Content-Bereitstellung genutzt.

Datenarchiv: StorageGRID bietet verschiedene Speichertypen und unterstützt Tiering zu öffentlichen, langfristigen und kostengünstigen Speicheroptionen. Damit ist es eine ideale Lösung für die Archivierung und langfristige Aufbewahrung von Daten, die für Compliance- oder historische Zwecke aufbewahrt werden müssen.

Anwendungsfälle für Objekt-Storage

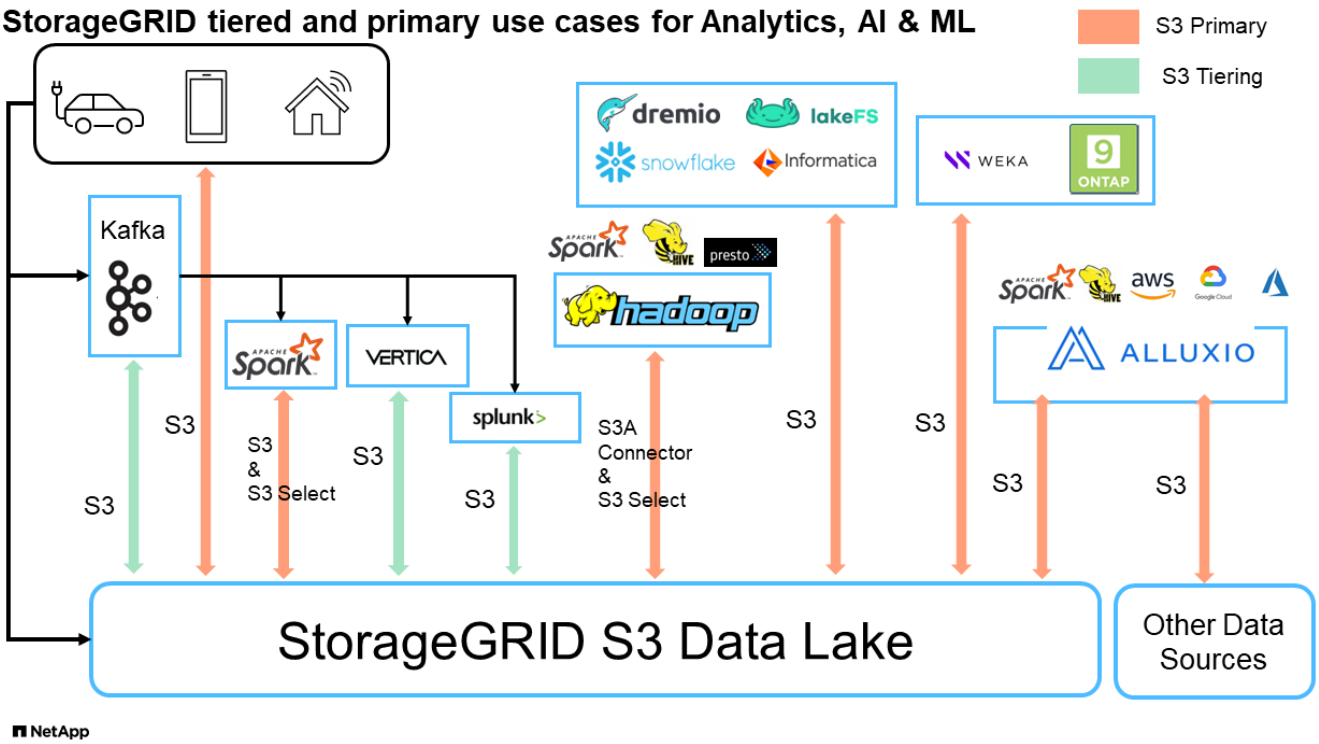


Zu den oben genannten Fällen gehört Big-Data-Analysen zu den häufigsten Nutzungsfällen und die Nutzung dieser Daten ist mit einem Aufwärtstrend verbunden.

Warum StorageGRID für Data Lakes?

- Verstärkte Zusammenarbeit: Enorme, gemeinsam genutzte Mandantenfähigkeit mit branchenüblicher API-Zugriff
- Niedrigere Betriebskosten: Einfacher Betrieb in einer einzelnen, automatisierten Scale-out-Architektur mit Selbstreparatur
- Skalierbarkeit – im Gegensatz zu herkömmlichen Hadoop- und Data-Warehouse-Lösungen entkoppelt der StorageGRID S3 Objekt-Storage den Storage von Computing und Daten. So können Unternehmen ihre Storage-Anforderungen mit wachsendem Bedarf skalieren.
- Langlebigkeit und Zuverlässigkeit: StorageGRID bietet eine Lebensdauer von 99.999999999 %, was bedeutet, dass die gespeicherten Daten sehr resistent gegen Datenverlust sind. Darüber hinaus ist Hochverfügbarkeit gewährleistet, sodass die Daten jederzeit abrufbar sind.
- Sicherheit – StorageGRID bietet verschiedene Sicherheitsfunktionen, darunter Verschlüsselung, Zugriffssteuerungsrichtlinien, Daten-Lifecycle-Management, Objektsperre und Versionierung zum Schutz der in S3 Buckets gespeicherten Daten

StorageGRID S3 Data Lakes



Benchmarking von Data Warehouses und Lakehouses mit S3 Object Storage: Eine vergleichende Studie

Dieser Artikel stellt eine umfassende Benchmark verschiedener Data Warehouse- und Lakehouse-Ökosysteme vor, die NetApp StorageGRID verwenden. Ziel ist es zu ermitteln, welches System mit S3 Objekt-Storage am besten funktioniert. In diesem Abschnitt "Apache Iceberg: Der Endgültige Führer"erfahren Sie mehr über Datawarehous/Lakehouse-Architekturen und Tischformate (Parkett und Iceberg).

- Benchmark-Tool - TPC-DS - https://www.tpc.org/tpcds/
- Big-Data-Ecosysteme
  - Cluster von VMs mit jeweils 128 GB RAM und 24 vCPUs, SSD-Storage für Systemfestplatte
  - Hadoop 3.3.5 mit Hive 3.1.3 (1 Name Node + 4 Daten-Nodes)
  - Delta Lake mit Spark 3.2.0 (1 Master + 4 Workers) und Hadoop 3.3.5
  - Dremio v25.2 (1 Koordinator + 5 Ausführende)
  - Trino v438 (1 Koordinator + 5 Mitarbeiter)
  - Starburst v453 (1 Koordinator + 5 Mitarbeiter)
- Objekt-Storage
  - NetApp® StorageGRID® 11.8 mit 3 SG6060 + 1 SG1000 Load Balancer
  - Objektschutz – 2 Kopien (Ergebnis ist ähnlich wie EC 2+1)
- Datenbankgröße 1.000 GB
- Cache wurde in allen Ökosystemen für jeden Abfragetest mit dem Parkettformat deaktiviert. Für das Iceberg-Format haben wir die Anzahl der S3-GET-Anforderungen und die gesamte Abfragezeit zwischen Cache-deaktivierten und Cache-fähigen Szenarien verglichen.

TPC-DS umfasst 99 komplexe SQL-Abfragen, die für das Benchmarking entwickelt wurden. Wir haben die

Gesamtdauer für die Ausführung aller 99 Abfragen gemessen. Für eine detaillierte Analyse haben wir die Art und Anzahl der S3-Anfragen untersucht. Unsere Tests verglichen die Effizienz zweier beliebter Tischformate: Parkett und Iceberg.

TPC-DS Abfrageergebnis mit Parkett-Tabellenformat

Ecosystem	Hive	Delta Lake	Dremio	Trino	Starburst
TPCDS 99 Abfragen Minuten gesamt	1084 [1]	55	36	32	28
S3 Anfragen – Aufschlüsselung	GET	1,117,184	2,074,610	3.939.690	1.504.212
1.495.039	Beobachtung: Alle Reichweite ERHALTEN	80% Bereich von 2 KB bis 2 MB von 32 MB Objekten, 50 - 100 Anfragen/Sek.	73% Bereich unter 100 KB von 32-MB-Objekten, 1000 - 1400 Anforderungen/Sek.	90 % 1 MB-Bereich von Objekten mit 256 MB, 2500 bis 3000 Anforderungen/Sek.	Bereich GET size: 50% unter 100KB, 16% um 1MB, 27% 2MB-9MB, 3500 - 4000 Anfragen/sec
Bereich GET size: 50% unter 100KB, 16% um 1MB, 27% 2MB-9MB, 4000 - 5000 Anfrage/sec	Objekte auflisten	312,053	24,158	120	509
512	KOPF (Nicht vorhandenes Objekt)	156,027	12,103	96	0
0	KOPF (Vorhandenes Objekt)	982,126	922,732	0	0
0	Gesamtanforderungen	2,567,390	3,033,603	3.939,906	1.504.721

[1] Hive konnte die Abfragenummer 72 nicht abschließen

TPC-DS Abfrageergebnis mit Iceberg-Tabellenformat

Ecosystem	Dremio	Trino	Starburst
TPCDS 99 Abfragen + Summe Minuten (Cache deaktiviert)	22	28	22
TPCDS 99 Abfragen + Gesamtzahl Minuten [2] (Cache aktiviert)	16	28	21,5
S3 Anfragen – Aufschlüsselung	ABRUFEN (Cache deaktiviert)	1.985.922	938.639
931.582	GET (Cache aktiviert)	611.347	30.158
3.281	Beobachtung: Alle Reichweite ERHALTEN	Bereich GET size: 67% 1 MB, 15% 100 KB, 10% 500 KB, 3500 - 4500 Anfragen/sec	Bereich GET size: 42% unter 100KB, 17% um 1MB, 33% 2MB-9MB, 3500 - 4000 Anfragen/sec
Bereich GET size: 43% unter 100KB, 17% um 1MB, 33% 2MB-9MB, 4000 - 5000 Anfragen/sec	Objekte auflisten	1465	0
0	KOPF (Nicht vorhandenes Objekt)	1464	0
0	KOPF (Vorhandenes Objekt)	3.702	509
509	Anfragen gesamt (Cache deaktiviert)	1.992.553	939.148

[2] die Performance von Trino/Starburst wird durch Computing-Ressourcen in Engpässe gebracht. Durch Hinzufügen von zusätzlichem RAM zum Cluster wird die gesamte Abfragezeit verringert.

Wie in der ersten Tabelle gezeigt, ist Hive deutlich langsamer als andere moderne Data-Lakehouse-Ökosysteme. Wir beobachteten, dass Hive eine große Anzahl von S3-Listenobjektanfragen gesendet hat, die in der Regel auf allen Objekt-Storage-Plattformen langsam sind, insbesondere bei Buckets, die zahlreiche Objekte enthalten. Dadurch erhöht sich die gesamte Abfragedauer deutlich. Zusätzlich können moderne Lakehouse-Ökosysteme eine hohe Anzahl von GET-Anfragen parallel senden, die von 2,000 bis 5,000 Anfragen pro Sekunde reichen, verglichen mit Hive's 50 bis 100 Anfragen pro Sekunde. Die Standard-Filesystem-Mimikry von Hive und Hadoop S3A trägt zur Langsamkeit von Hive bei der Interaktion mit S3-Objektspeicher bei.

Bei der Nutzung von Hadoop (entweder auf HDFS oder S3 Objekt-Storage) mit Hive oder Spark sind umfassende Kenntnisse sowohl zu Hadoop als auch zu Hive/Spark erforderlich. Außerdem müssen Sie sich mit den Einstellungen der einzelnen Services vertraut machen. Zusammen haben sie über 1,000 Einstellungen, von denen viele miteinander verknüpft sind und nicht unabhängig voneinander geändert werden können. Die optimale Kombination von Einstellungen und Werten zu finden, erfordert viel Zeit und Aufwand.

Wenn wir die Ergebnisse von Parkett und Iceberg vergleichen, stellen wir fest, dass das Tabellenformat ein wichtiger Leistungsfaktor ist. Das Iceberg-Tabellenformat ist hinsichtlich der Anzahl der S3-Anfragen effizienter

als das Parkett, mit 35% bis 50% weniger Anfragen im Vergleich zum Parkett-Format.

Die Leistung von Dremio, Trino oder Starburst wird in erster Linie durch die Rechenleistung des Clusters angetrieben. Alle drei verwenden zwar den S3A-Connector für die S3-Objektspeicher-Verbindung, benötigen jedoch kein Hadoop. Die meisten der fs.s3a-Einstellungen von Hadoop werden von diesen Systemen nicht verwendet. Dies vereinfacht das Performance-Tuning und macht das Erlernen und Testen verschiedener Hadoop S3A Einstellungen überflüssig.

Aus diesem Benchmark-Ergebnis können wir schließen, dass Big-Data-Analysesysteme für S3-basierte Workloads zu einem wesentlichen Performance-Faktor werden. Moderne Lakehouses optimieren die Abfrageausführung, nutzen Metadaten effizient und ermöglichen nahtlosen Zugriff auf S3-Daten. Dies ermöglicht eine bessere Performance als Hive bei der Arbeit mit S3 Storage.

Hier "Seite" können Sie die Dremio S3-Datenquelle mit StorageGRID konfigurieren.

Unter den folgenden Links erfahren Sie mehr darüber, wie StorageGRID und Dremio gemeinsam eine moderne und effiziente Data-Lake-Infrastruktur bereitstellen und wie NetApp von Hive + HDFS auf Dremio + StorageGRID migrierte, um die Analyseeffizienz von Big Data drastisch zu steigern.

- "Mehr Performance für Big Data mit NetApp StorageGRID"
- "Moderne, leistungsstarke und effiziente Data-Lake-Infrastruktur mit StorageGRID und Dremio"
- "Wie NetApp die Kundenerfahrung mit Produktanalysen neu definiert"

Hadoop S3A-Tuning

Von Angela Cheng

Der Hadoop S3A Connector ermöglicht die nahtlose Interaktion zwischen Hadoop-basierten Applikationen und S3 Objektspeicher. Um die Performance bei der Arbeit mit S3-Objektspeicher zu optimieren, ist die Anpassung des Hadoop S3A Connector unerlässlich. Bevor wir uns mit der Feinabstimmung befassen, wollen wir zunächst ein grundlegendes Verständnis von Hadoop und seinen Komponenten haben.

Was ist Hadoop?

Hadoop ist ein leistungsfähiges Open-Source-Framework, das für die Verarbeitung und Speicherung großer Datenmengen entwickelt wurde. Sie ermöglicht verteilte Speicherung und parallele Verarbeitung über Cluster von Computern hinweg.

Die drei Kernkomponenten von Hadoop sind:

- **Hadoop HDFS (Hadoop Distributed File System)**: Dies verarbeitet Speicherung, teilt Daten in Blöcke auf und verteilt sie über Knoten.
- **Hadoop MapReduce**: Verantwortlich für die Verarbeitung der Daten durch Aufteilen von Aufgaben in kleinere Blöcke und deren parallele Ausführung.
- **Hadoop YARN (noch ein weiterer Resource Negotiator):** "Managt Ressourcen und plant Aufgaben effizient"

Hadoop HDFS- und S3A-Steckverbinder

HDFS ist eine wichtige Komponente des Hadoop Ecosystems und spielt eine entscheidende Rolle bei der effizienten Verarbeitung von Big Data. HDFS ermöglicht zuverlässige Speicherung und Verwaltung. Sie ermöglicht die parallele Verarbeitung und optimiert den Datenspeicher, was zu schnellerem Datenzugriff und

schnelleren Analysen führt.

Bei der Big Data-Verarbeitung überzeugt HDFS durch fehlertoleranten Storage für große Datensätze. Es erreicht dies durch Datenreplikation. Die IT kann große Mengen strukturierter und unstrukturierter Daten in einer Data Warehouse-Umgebung speichern und managen. Darüber hinaus lässt sich die Software nahtlos in führende Big Data Processing Frameworks wie Apache Spark, Hive, Pig und Flink integrieren und ermöglicht so eine skalierbare und effiziente Datenverarbeitung. Er ist mit Unix-basierten (Linux) Betriebssystemen kompatibel und somit eine ideale Wahl für Unternehmen, die Linux-basierte Umgebungen für ihre Big-Data-Verarbeitung bevorzugen.

Mit der Zeit wuchs das Datenvolumen. Daher ist es ineffizient, dem Hadoop Cluster neue Maschinen mit eigenen Computing- und Storage-Ressourcen hinzuzufügen. Lineare Skalierung führt zu Herausforderungen bei der effizienten Nutzung von Ressourcen und dem Management der Infrastruktur.

Als Antwort auf diese Herausforderungen bietet der Hadoop S3A Connector hochperformante I/O für S3 Objekt-Storage. Durch die Implementierung eines Hadoop Workflows mit S3A können Sie Objekt-Storage als Daten-Repository nutzen und Computing- und Storage-Ressourcen separat voneinander skalieren. Dadurch wiederum können Sie Computing- und Storage-Ressourcen unabhängig voneinander skalieren. Die Abkopplung von Computing und Storage erlaubt es Ihnen auch, die richtige Menge an Ressourcen für Ihre Compute-Jobs bereitzustellen und die Kapazität abhängig von der Größe des Datensatzes bereitzustellen. Somit lassen sich die Gesamtbetriebskosten für Hadoop Workflows verringern.

Hadoop S3A Connector Tuning

S3 verhält sich anders als HDFS, und einige Versuche, das Aussehen eines Filesystems beizubehalten, sind aggressiv suboptimal. Um die S3-Ressourcen möglichst effizient zu nutzen, sind sorgfältiges Tuning/Testen/Experimentieren erforderlich.

Die Hadoop Optionen in diesem Dokument basieren auf Hadoop 3.3.5, siehe "Hadoop 3.3.5 core-site.xml" Für alle verfügbaren Optionen.

Hinweis – einige Hadoop fs.s3a Einstellungen sind in den jeweiligen Hadoop Versionen unterschiedlich. Überprüfen Sie unbedingt den Standardwert Ihrer aktuellen Hadoop Version. Werden diese Einstellungen nicht in Hadoop core-site.xml angegeben, so wird als Standardwert verwendet. Sie können den Wert zur Laufzeit mithilfe der Konfigurationsoptionen Spark oder Hive überschreiben.

Sie müssen zu diesem gehen "Apache Hadoop Seite aufrufen" Um die einzelnen Optionen von fs.s3a zu verstehen. Testen Sie diese nach Möglichkeit im nicht produktiven Hadoop Cluster, um die optimalen Werte zu ermitteln.

Sie sollten lesen "Maximale Leistung bei der Arbeit mit dem S3A-Steckverbinder" Für weitere Optimierungsempfehlungen.

Sehen wir uns einige wichtige Überlegungen an:

1. Datenkomprimierung

Aktivieren Sie die StorageGRID-Komprimierung nicht. Die meisten Big-Data-Systeme verwenden Byte-Bereich get, anstatt das gesamte Objekt abzurufen. Die Verwendung von Byte Range Get mit komprimierten Objekten beeinträchtigt die GET-Performance erheblich.

2. S3A Committer

Generell wird Magic s3a Committer empfohlen. Weitere Informationen finden Sie hier "Allgemeine Seite mit den Optionen für den S3A-Committer" Um ein besseres Verständnis von Magic Committer und den damit

verbundenen s3a-Einstellungen zu bekommen.

Magic Committer:

Der Magic Committer setzt speziell auf S3Guard, um konsistente Verzeichnisauflistungen im S3-Objektspeicher zu bieten.

Mit konsistenten S3 (was jetzt der Fall ist), kann der Magic Committer sicher mit jedem S3-Bucket verwendet werden.

Auswahl und Experimentieren:

Je nach Anwendungsfall können Sie zwischen dem Staging Committer (der auf einem Cluster HDFS-Dateisystem basiert) und dem Magic Committer wählen.

Experimentieren Sie mit beiden, um zu ermitteln, welche Lösung am besten zu Ihrem Workload und Ihren Anforderungen passt.

Zusammenfassend stellen die S3A Committers eine Lösung für die grundlegende Herausforderung dar, die ein konsistentes, leistungsstarkes und zuverlässiges Leistungsengagement für S3 darstellt. Das interne Design gewährleistet einen effizienten Datentransfer bei gleichzeitiger Wahrung der Datenintegrität.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable “magic committer” support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

3. Thread, Größe des Verbindungspools und Blockgröße

- Jeder **S3A**-Client, der mit einem einzelnen Bucket interagiert, hat einen eigenen dedizierten Pool von offenen HTTP 1.1-Verbindungen und Threads für Upload- und Kopiervorgänge.
- "Sie können diese Poolgrößen so anpassen, dass ein ausgewogenes Verhältnis zwischen Leistung und Speicher-/Thread-Nutzung erzielt wird".
- Beim Hochladen von Daten in S3 werden sie in Blöcke unterteilt. Die standardmäßige Blockgröße beträgt 32 MB. Sie können diesen Wert anpassen, indem Sie die Eigenschaft fs.s3a.Block.size festlegen.
- Größere Blockgrößen verbessern die Performance beim Hochladen großer Daten, da sich der Managementaufwand für mehrteilige Teile während des Uploads verringert. Der empfohlene Wert ist 256

MB oder höher für große Datensätze.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

4. Mehrteiliges Hochladen

s3a-Committer **Always** Verwenden Sie MPU (mehrteilige Uploads) zum Hochladen von Daten in s3-Buckets. Dies ist erforderlich, um Folgendes zu ermöglichen: Task Failure, spekulative Ausführung von Aufgaben und Job Abbrüche vor Commit. Hier sind einige wichtige Spezifikationen für mehrteilige Uploads:

- Maximale Objektgröße: 5 tib (Terabyte).
- Maximale Anzahl von Teilen pro Upload: 10,000.
- Teilenummern: Von 1 bis 10,000 (inklusive).
- Größe des Teils: Zwischen 5 MiB und 5 gib. Insbesondere gibt es keine Mindestgröße für den letzten Teil Ihres mehrteiligen Uploads.

Die Verwendung kleinerer Teilgröße für S3-Multipart-Uploads hat sowohl vor- als auch Nachteile.

Vorteile:

- Schnelle Wiederherstellung von Netzwerkproblemen: Wenn Sie kleinere Teile hochladen, werden die Auswirkungen des Neustarts eines fehlgeschlagenen Uploads aufgrund eines Netzwerkfehlers minimiert.

Wenn ein Teil fehlschlägt, müssen Sie nur dieses Teil neu hochladen, nicht das gesamte Objekt.

- Bessere Parallelisierung: Mehr Teile können parallel hochgeladen werden, wobei Multi-Threading oder gleichzeitige Verbindungen genutzt werden können. Diese Parallelisierung verbessert die Performance, insbesondere bei der Verarbeitung großer Dateien.

Nachteil:

- Netzwerk-Overhead: Kleinere Teilegröße bedeutet, dass mehr Teile hochgeladen werden müssen, jedes Teil benötigt eine eigene HTTP-Anforderung. Mehr HTTP-Anfragen erhöhen den Overhead beim Initiieren und Abschließen einzelner Anfragen. Die Verwaltung einer großen Anzahl von Kleinteilen kann die Leistung beeinträchtigen.
- Komplexität: Die Verwaltung der Bestellung, die Nachverfolgung von Teilen und die Sicherstellung erfolgreicher Uploads können umständlich sein. Wenn der Upload abgebrochen werden muss, müssen alle bereits hochgeladenen Teile nachverfolgt und gelöscht werden.

Für Hadoop wird eine Teilegröße von 256 MB oder höher für fs.s3a.Multipart.size empfohlen. Stellen Sie immer den Wert fs.s3a.mutlipart.threshold auf 2 x fs.s3a.multipart.size ein. Beispiel: Fs.s3a.multipart.size = 256M, fs.s3a.mutlipart.threshold sollte 512M sein.

Größere Teilegröße für großen Datensatz verwenden Es ist wichtig, eine Teilegröße zu wählen, die diese Faktoren auf der Grundlage Ihres spezifischen Anwendungsfalls und der Netzwerkbedingungen ausgleicht.

Ein mehrteiliges Hochladen ist ein "Prozess in drei Schritten":

1. Der Upload wird gestartet, StorageGRID gibt eine Upload-ID zurück.
2. Die Objektteile werden mit der Upload-ID hochgeladen.
3. Sobald alle Objektteile hochgeladen sind, sendet die komplette mehrteilige Upload-Anfrage mit Upload-ID. StorageGRID erstellt das Objekt aus den hochgeladenen Teilen, und der Client kann auf das Objekt zugreifen.

Wenn die Anfrage zum vollständigen Hochladen mehrerer Teile nicht erfolgreich gesendet wird, bleiben die Teile in StorageGRID und erstellen kein Objekt. Dies geschieht, wenn Jobs unterbrochen, fehlgeschlagen oder abgebrochen werden. Die Teile verbleiben im Raster, bis der Upload mehrerer Teile abgeschlossen ist oder abgebrochen wird oder StorageGRID diese Teile löscht, wenn 15 Tage nach dem Upload vergangen sind. Wenn sich viele (einige Hunderttausend bis Millionen) mehrteilige Uploads in einem Bucket befinden und Hadoop ‘list-Multipart-Uploads’ sendet (diese Anfrage filtert nicht nach Upload-id), kann die Bearbeitung der Anfrage sehr viel Zeit in Anspruch nehmen oder eventuell eine bestimmte Zeit in Anspruch nehmen. Sie können die Einstellung fs.s3a.mutlipart.purge mit dem entsprechenden Wert fs.s3a.Multipart.purge.age (z. B. 5 bis 7 Tage, verwenden Sie den Standardwert 86400, d. h. 1 Tag) auf true setzen. Oder wenden Sie sich an den NetApp Support, um die Situation zu untersuchen.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

5. Pufferschreibdaten im Speicher

Zur Verbesserung der Performance können Sie Schreibdaten vor dem Hochladen in S3 zwischenspeichern. Dies kann die Anzahl kleiner Schreibvorgänge reduzieren und die Effizienz verbessern.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

S3 und HDFS funktionieren jedoch auf unterschiedliche Weise. Um die S3-Ressourcen optimal zu nutzen, sind

sorgfältiges Tuning/Test/Experiment nötig.

TR-4871: Konfiguration von StorageGRID für Backup und Recovery mit CommVault

Backup und Recovery von Daten mit StorageGRID und CommVault

CommVault und NetApp haben gemeinsam eine gemeinsame Datensicherungslösung entwickelt, die CommVault Complete Backup and Recovery for NetApp Software mit der NetApp StorageGRID Software für Cloud-Storage kombiniert. CommVault Complete Backup and Recovery und NetApp StorageGRID bieten einzigartige, benutzerfreundliche Lösungen, die Sie dabei unterstützen, die Anforderungen eines schnellen Datenwachstums und die zunehmenden Vorschriften weltweit zu erfüllen.

Viele Unternehmen möchten ihren Storage in die Cloud migrieren, ihre Systeme skalieren und ihre Richtlinien zur langfristigen Aufbewahrung von Daten automatisieren. Cloud-basierter Objekt-Storage ist für seine Ausfallsicherheit, Skalierbarkeit und betriebliche und Kosteneffizienz bekannt, die es zur ersten Wahl für Ihr Backup machen. CommVault und NetApp haben ihre kombinierte Lösung 2014 gemeinsam zertifiziert und bieten seitdem eine engere Integration der beiden Lösungen an. Kunden aller Branchen weltweit haben die kombinierte Lösung CommVault Complete Backup and Recovery sowie StorageGRID eingeführt.

CommVault und StorageGRID

Die Software CommVault Complete Backup and Recovery ist eine integrierte Daten- und Informationsmanagement-Lösung der Enterprise-Klasse, die von Grund auf auf auf einer einzigen Plattform und mit einer einheitlichen Code-Basis aufgebaut wurde. Alle Funktionen sind mit Back-End-Technologien ausgestattet und bieten so die unvergleichlichen Vorteile und Vorteile eines vollständig integrierten Ansatzes zum Schutz, Management und Zugriff auf Ihre Daten. Die Software enthält Module zum Schützen, Archivieren, Analysieren, Replizieren und Durchsuchen Ihrer Daten. Die Module verfügen über gemeinsame Back-End-Services und erweiterte Funktionen, die nahtlos miteinander interagieren. Die Lösung deckt alle Aspekte des Datenmanagements in Ihrem Unternehmen ab und sorgt gleichzeitig für grenzenlose Skalierbarkeit und beispiellose Kontrolle über Daten und Informationen.

NetApp StorageGRID als Cloud-Tier von CommVault ist eine Objekt-Storage-Lösung für die Hybrid Cloud der Enterprise-Klasse. Sie kann an mehreren Standorten eingesetzt werden, entweder auf einer speziell entwickelten Appliance oder als softwaredefinierte Implementierung. Mit StorageGRID können Kunden Richtlinien für das Datenmanagement festlegen, die festlegen, wie Daten gespeichert und gesichert werden. StorageGRID erfasst die Informationen, die Sie für die Entwicklung und Durchsetzung von Richtlinien benötigen. Untersucht werden eine Vielzahl von Merkmalen und Anforderungen, darunter Performance, Langlebigkeit, Verfügbarkeit, geografischer Standort Langlebigkeit und Kosten. Daten werden während der Verschiebung zwischen Standorten und mit zunehmendem Alter vollständig gepflegt und geschützt.

Die intelligente Richtlinien-Engine von StorageGRID bietet Ihnen eine der folgenden Optionen:

- Mit Erasure Coding können Sie Daten aus Resilience-heraus über mehrere Standorte hinweg sichern.
- Um Objekte an Remote-Standorte zu kopieren und so die WAN-Latenz und die Kosten zu minimieren.

Wenn ein Objekt von StorageGRID gespeichert wird, greifen Sie als ein Objekt auf es zu, unabhängig davon, wo es sich befindet oder wie viele Kopien vorhanden sind. Dieses Verhalten ist bei der Disaster Recovery von entscheidender Bedeutung, da StorageGRID Ihre Daten selbst dann wiederherstellen kann, wenn eine Sicherungskopie der Daten beschädigt ist.

Die Aufbewahrung von Backup-Daten in Ihrem Primärspeicher kann kostspielig werden. Wenn Sie NetApp StorageGRID verwenden, geben Sie Speicherplatz auf Ihrem primären Storage frei, indem Sie inaktive Backup-Daten in StorageGRID migrieren und gleichzeitig von den zahlreichen Funktionen von StorageGRID profitieren. Der Wert von Backup-Daten ändert sich im Laufe der Zeit, genauso wie die Kosten für deren Speicherung. StorageGRID kann die Kosten für primären Storage minimieren und die Langlebigkeit der Daten verbessern.

Wichtige Funktionen

Zu den wichtigsten Funktionen der CommVault Softwareplattform gehören:

- Eine umfassende Datensicherungslösung, die alle wichtigen Betriebssysteme, Applikationen und Datenbanken auf virtuellen und physischen Servern, NAS-Systemen, Cloud-basierten Infrastrukturen und Mobilgeräten unterstützt
- Vereinfachtes Management über eine einzige Konsole: Sie können alle Funktionen sowie alle Daten und Informationen im gesamten Unternehmen anzeigen, managen und darauf zugreifen.
- Verschiedene Sicherungsmethoden wie Daten-Backup und -Archivierung, Snapshot-Management, Datenreplizierung und Content-Indizierung für E-Discovery
- Effizientes Storage-Management mit Deduplizierung für Festplatten- und Cloud-Storage
- Integration in NetApp Storage-Arrays wie AFF, FAS, NetApp HCI und E-Series Arrays sowie^ horizontal skalierbare NetApp SolidFire^ Storage-Systeme Auch in die NetApp Cloud Volumes ONTAP Software integrierbar, um die Erstellung indizierter, applikationsgerechter NetApp Snapshot™ Kopien im gesamten NetApp Storage-Portfolio zu automatisieren.
- Umfassendes Management virtueller Infrastrukturen, das führende lokale virtuelle Hypervisoren und Hyperscaler-Plattformen für Public Clouds unterstützt
- Erweiterte Sicherheitsfunktionen zur Einschränkung des Zugriffs auf kritische Daten, zur Bereitstellung granularer Verwaltungsfunktionen und zur Bereitstellung von Single-Sign-on-Zugriff für Active Directory-Benutzer.
- Richtlinienbasiertes Datenmanagement, mit dem Daten je nach Geschäftsanforderungen und nicht nach physischem Standort gemanagt werden können
- Eine hochmoderne End-User-Erfahrung, mit der Ihre Anwender ihre Daten selbst schützen, finden und wiederherstellen können.
- API-gestützte Automatisierung, sodass Sie zum Management Ihrer Datensicherungs- und Recovery-Vorgänge Tools von Drittanbietern wie vRealize Automation oder Service Now verwenden können.

Weitere Informationen zu unterstützten Workloads finden Sie unter "Die unterstützten Technologien von CommVault".

Backup-Optionen

Die Implementierung der CommVault Complete Backup and Recovery-Software mit Cloud-Storage bietet zwei Backup-Optionen:

- Es wird ein Backup auf ein primäres Festplattenziel erstellt und außerdem eine zusätzliche Kopie in einem Cloud-Storage gesichert.
- Backup auf Cloud-Storage als primäres Ziel,

In der Vergangenheit wurde Cloud- oder Objekt-Storage als zu leistungsschwach für das primäre Backup angesehen. Durch die Verwendung eines primären Festplattenziels konnten Kunden schnellere Backup- und Restore-Prozesse durchführen und eine zusätzliche Kopie als Cold Backup in der Cloud aufbewahren.

StorageGRID ist die Objekt-Storage-Generation der nächsten Generation. StorageGRID bietet neben hoher Performance und enormem Durchsatz auch Performance und Flexibilität eine im Vergleich zu anderen Objekt-Storage-Anbietern hervorragende Leistung.

In der folgenden Tabelle sind die Vorteile der einzelnen Backup-Optionen mit StorageGRID aufgeführt:

	Primäres Backup-to-Disk und eine zusätzliche Kopie an StorageGRID	**Primäres Backup auf StorageGRID**
Leistung	Schnellste Recovery-Zeit mithilfe von Live-Mounten oder Live-Recovery: Ideal für Tier 0/Tier 1-Workloads.	Kann nicht für Live-Mount- oder Live-Recovery-Vorgänge verwendet werden. Ideal für Streaming-Wiederherstellungsvorgänge und für langfristige Aufbewahrung.
Implementierungsarchitektur	Verwendet rein Flash-basierten oder rotierenden Festplatten als erste Backup-Landing Tier. StorageGRID wird als sekundäre Ebene verwendet.	Vereinfacht die Implementierung durch die Verwendung von StorageGRID als umfassendes Backup-Ziel.
Erweiterte Funktionen (Live-Wiederherstellung)	Unterstützt	Nicht unterstützt

Wo Sie weitere Informationen finden

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

- StorageGRID 11.9 Dokumentationszentrum + https://docs.netapp.com/us-en/storagegrid-119/
- NetApp Produktdokumentation
  https://docs.netapp.com
- CommVault Dokumentation
  https://documentation.commvault.com/2024/essential/index.html

Übersicht über die getestete Lösung

Die getestete Lösung kombiniert CommVault und NetApp Lösungen in einer leistungsstarken gemeinsamen Lösung.

Lösungseinrichtung

Die StorageGRID-Umgebung bestand in der Lab-Einrichtung aus vier NetApp StorageGRID SG5712 Appliances, einem virtuellen primären Administrator-Node und einem virtuellen Gateway Node. Die SG5712 Appliance ist eine Entry-Level-Option – eine Basiskonfiguration. Durch die Auswahl von Optionen für Appliances mit höherer Performance, wie z. B. NetApp StorageGRID SG5760 oder SG6060, können deutliche Performance-Vorteile erzielt werden. Wenden Sie sich an Ihren NetApp StorageGRID Solution Architect, um Hilfe bei der Dimensionierung zu erhalten.

Die StorageGRID Richtlinie für Datensicherung verwendet für das Management und die Sicherung von Daten eine Richtlinie für integriertes Lifecycle Management (ILM). ILM-Regeln werden in einer Richtlinie von oben nach unten bewertet. Die in der folgenden Tabelle dargestellte ILM-Richtlinie wurde implementiert:

ILM-Regel	Kriterien	Aufnahmeverhalten
Erasure Coding 2+1	Objekte über 200 KB	Ausgeglichen
2 Kopien	Alle Objekte	Doppelte Provisionierung

Die Standardregel für ILM 2 Kopien ist. Für diesen Test wurde die Regel Erasure Coding 2+1 auf jedes Objekt mit mindestens 200 KB angewendet. Die Standardregel wurde auf Objekte angewendet, die kleiner als 200 KB sind. Die Anwendung der Regeln auf diese Weise ist eine StorageGRID Best Practice.

Technische Details zu dieser Testumgebung finden Sie im Abschnitt Solution Design and Best Practices in der "NetApp Scale-out-Datensicherung mit CommVault" Technischer Bericht.

Hardware-Spezifikationen für StorageGRID

Die folgende Tabelle beschreibt die bei diesen Tests verwendete NetApp StorageGRID-Hardware. Die StorageGRID SG5712 Appliance mit 10 Gbit/s-Netzwerkbetrieb ist die Einstiegsoption und stellt eine Basiskonfiguration dar. Optional kann die SG5712 für 25-Gbit/s-Netzwerke konfiguriert werden.

Trennt	Menge	Festplatte	Nutzbare Kapazität	Netzwerk
StorageGRID SG5712 Appliances	4	48 x 4 TB (Nearline SAS-HDD)	136 TB	10 Gbit/s

Durch die Auswahl von Appliance-Optionen mit höherer Performance, wie z. B. NetApp StorageGRID SG5760, SG6060 oder All-Flash SGF6112 Appliances, können deutliche Performance-Vorteile erzielt werden. Wenden Sie sich an Ihren NetApp StorageGRID Solution Architect, um Hilfe bei der Dimensionierung zu erhalten.

Softwareanforderungen von CommVault und StorageGRID

In den folgenden Tabellen sind die Software-Anforderungen für die auf der Software von VMware installierte CommVault und NetApp StorageGRID für unsere Tests aufgeführt. Vier MediaAgent Datenübertragungsmanager und ein CommServe-Server wurden installiert. In den Tests wurden 10-Gbit-s-Networking für die VMware Infrastruktur implementiert. Der folgenden Tabelle zu entnehmen

In der folgenden Tabelle sind die Gesamtsystemanforderungen der CommVault Software aufgeführt:

Komponente	Menge	Datenspeicher	Größe	Gesamt	Gesamte erforderliche IOPS
CommServe Server	1	BETRIEBSSYSTEM	500 GB	500 GB	1. A.
		SQL SERVER GESCHULT SIND	500 GB	500 GB	1. A.

Komponente	Menge	Datenspeicher	Größe	Gesamt	Gesamte erforderliche IOPS
MediaAgent	4	Virtuelle CPU (vCPU)	16	64	1. A.
		RAM	128 GB	512	1. A.
		BETRIEBSSYSTEM	500 GB	2 TB	1. A.
		Index-Cache	2 TB	8 TB	200+
		DDB	2 TB	8 TB	200–80.000 K

In der Testumgebung wurden ein primärer virtueller Administrator-Node und ein virtueller Gateway-Node auf VMware auf einem NetApp E-Series E2812 Storage-Array implementiert. Jeder Knoten befand sich auf einem separaten Server mit den in der folgenden Tabelle beschriebenen Mindestanforderungen an die Produktionsumgebung:

Die folgende Tabelle listet die Anforderungen für virtuelle StorageGRID-Admin-Nodes und Gateway-Nodes auf:

Node-Typ	Menge	VCPU	RAM	Storage
Gateway-Node	1	8	24 GB	100 GB LUN für das OS
Administrator-Node	1	8	24 GB	100 GB LUN für das OS 200-GB-LUN für Administrator-Node-Tabellen 200 GB-LUN für das Admin-Node-Revisionsprotokoll

Leitfaden zur StorageGRID Dimensionierung

Wenden Sie sich an Ihre NetApp Datenschutzexperten, um Informationen zur spezifischen Dimensionierung für Ihre Umgebung zu erhalten. NetApp-Spezialisten können mit dem CommVault Total Backup Storage Calculator die Anforderungen an die Backup-Infrastruktur einschätzen. Für das Tool ist der Zugriff auf das CommVault Partner Portal erforderlich. Melden Sie sich bei Bedarf an, um darauf zuzugreifen.

Eingaben zur CommVault-Größenbestimmung

Die folgenden Aufgaben können zur Durchführung einer Bestandsaufnahme für die Dimensionierung der Datensicherheitslösung verwendet werden:

- Identifizieren Sie die System- oder Applikations-/Datenbank-Workloads und die entsprechende Front-End-Kapazität (in Terabyte [TB]), die geschützt werden muss.
- Identifizieren Sie den VM-/Datei-Workload und ähnliche Front-End-Kapazität (TB), die geschützt werden muss.
- Identifizieren Sie Anforderungen für die kurzfristige und langfristige Datenaufbewahrung.
- Ermittlung der täglichen prozentualen Änderungsrate für die ermittelten Datensätze/Workloads
- Ermittlung des prognostizierten Datenwachstums in den nächsten 12, 24 und 36 Monaten
- Definieren Sie RTO und RPO für Datensicherung/Recovery entsprechend den geschäftlichen Anforderungen.

Wenn diese Informationen verfügbar sind, kann die Dimensionierung der Backup-Infrastruktur vorgenommen werden, was zu einer Aufschlüsselung der benötigten Speicherkapazitäten führt.

Leitfaden zur StorageGRID Dimensionierung

Bevor Sie die NetApp StorageGRID Dimensionierung durchführen, sollten Sie die folgenden Aspekte für Ihre Workloads berücksichtigen:

- Nutzbare Kapazität
- Worm-Modus
- Durchschnittliche Objektgröße
- Performance-Anforderungen erfüllt
- ILM-Richtlinie angewendet

Die nutzbare Kapazität muss der Größe des Backup-Workloads entsprechen, den Sie in StorageGRID gestaffelt haben, sowie dem Aufbewahrungszeitplan.

Wird der WORM-Modus aktiviert oder nicht? Wenn WORM in CommVault aktiviert ist, wird dadurch die Objektsperre auf StorageGRID konfiguriert. Dadurch wird die erforderliche Objektspeicher-Kapazität erhöht. Die erforderliche Kapazität variiert basierend auf der Aufbewahrungsdauer und der Anzahl der Objektänderungen bei jedem Backup.

Die durchschnittliche Objektgröße ist ein Eingabeparameter, der bei der Dimensionierung für die Performance in einer StorageGRID Umgebung hilft. Die durchschnittliche Objektgröße, die für einen CommVault-Workload verwendet wird, hängt vom Backup-Typ ab.

In der folgenden Tabelle sind die durchschnittlichen Objektgrößen nach Backup-Typ aufgeführt und die Lesevorgänge aus dem Objektspeicher werden durch den Wiederherstellungsprozess beschrieben:

Backup-Typ	Durchschnittliche Objektgröße	Wiederherstellungsverhalten
Erstellen Sie eine Zusatzkopie in StorageGRID	32 MB	Vollständiger Lesezugriff auf ein 32-MB-Objekt

Backup-Typ	Durchschnittliche Objektgröße	Wiederherstellungsverhalten
Leiten des Backups auf StorageGRID (Deduplizierung aktiviert)	8 MB	1 MB zufälliger Lesebereich
Leiten Sie das Backup auf StorageGRID (Deduplizierung deaktiviert)	32 MB	Vollständiger Lesezugriff auf ein 32-MB-Objekt

Darüber hinaus sind Sie über die Performance-Anforderungen für vollständige Backups und inkrementelle Backups in der Lage, die Dimensionierung für die StorageGRID Storage-Nodes zu bestimmen. StorageGRID Richtlinie für Information Lifecycle Management (ILM) Datensicherungsmethoden bestimmen die zur Speicherung von CommVault Backups benötigte Kapazität und wirken sich auf die Grid-Größe aus.

StorageGRID ILM-Replizierung ist einer von zwei Mechanismen, die StorageGRID zum Speichern von Objektdaten verwendet. Wenn StorageGRID einer ILM-Regel Objekte zuweist, die Daten repliziert, erstellt das System exakte Kopien der Objektdaten und speichert die Kopien auf Storage-Nodes.

Das Verfahren zur Einhaltung von Datenkonsistenz ist die zweite Methode, die von StorageGRID zum Speichern von Objektdaten verwendet wird. Wenn StorageGRID einer ILM-Regel Objekte zuweist, die für die Erstellung von Kopien, die nach Erasure codiert wurden, konfiguriert wird, werden Objektdaten in Datenfragmente unterteilt. Danach werden zusätzliche Paritätsfragmente berechnet und jedes Fragment auf einem anderen Storage Node gespeichert. Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Datenfragment oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zur Fehlerkorrektur ein neues Fragment unter Verwendung einer Untergruppe der verbleibenden Daten- und Paritätsfragmente erstellen.

Die beiden Mechanismen erfordern unterschiedliche Mengen an Storage, wie die folgenden Beispiele zeigen:

- Wenn Sie zwei replizierte Kopien speichern, verdoppelt sich Ihr Storage-Overhead.
- Wenn Sie eine 2 Kopie, die nach der Datenlöschung codiert wurde, speichern, erhöht sich Ihr Storage-Overhead um das 1.5-Fache.

Für die getestete Lösung wurde eine Entry-Level StorageGRID Implementierung an einem einzelnen Standort genutzt:

- Admin-Node: VMware Virtual Machine (VM)
- Load Balancer: VMware VM
- Storage-Nodes: 4 x SG5712 mit 4-TB-Laufwerken
- Primärer Admin-Node und Gateway-Node: VMware VMs mit den Mindestanforderungen für Produktions-Workloads

StorageGRID unterstützt auch Load Balancer von Drittanbietern.

StorageGRID wird in der Regel an zwei oder mehr Standorten mit Datensicherungsrichtlinien implementiert, die Daten replizieren, um vor Ausfällen auf Node- und Site-Ebene zu schützen. Wenn Sie Ihre Daten in StorageGRID sichern, sind Ihre Daten durch mehrere Kopien oder durch Erasure Coding geschützt, durch das Daten zuverlässig durch einen Algorithmus getrennt und neu zusammengestellt werden.

Sie können das Sizing-Tool verwenden "Fusion" Zur Größenbeaufstellung des Rasters.

Skalierbarkeit

Ein NetApp StorageGRID System lässt sich mit weiteren Storage-Nodes erweitern, einem vorhandenen Standort neue Grid-Nodes hinzufügen oder ein neues Datacenter hinzufügen. Eine Erweiterung kann vorgenommen werden, ohne den Betrieb des aktuellen Systems zu unterbrechen.
StorageGRID skaliert die Performance mithilfe von Nodes mit höherer Performance für die Storage-Nodes oder der physischen Appliance mit dem Load Balancer und den Admin-Nodes oder durch einfaches Hinzufügen weiterer Nodes.

Weitere Informationen zur Erweiterung des StorageGRID-Systems finden Sie unter "StorageGRID 11.9 Erweiterungsleitfaden".

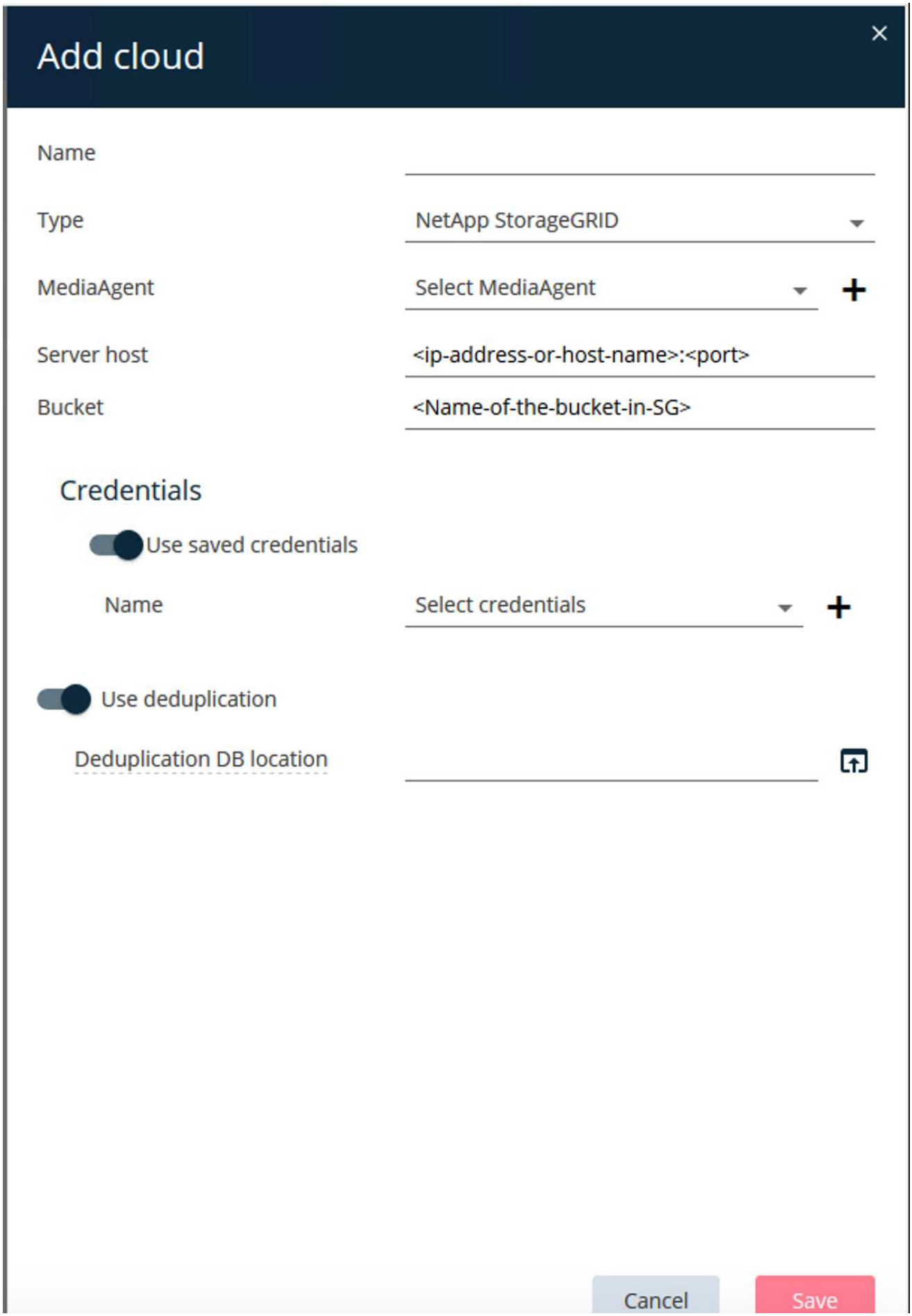
Einen Datensicherungsauftrag ausführen

Zur Konfiguration von StorageGRID mit CommVault Complete Backup and Recovery for NetApp wurden folgende Schritte durchgeführt, um StorageGRID als Cloud-Bibliothek innerhalb der CommVault Software hinzuzufügen.

Schritt: CommVault mit StorageGRID konfigurieren

Schritte

1. Melden Sie sich beim CommVault Command Center an. Klicken Sie im linken Fensterbereich auf Storage > Cloud > Add, um das Dialogfeld Add Cloud anzuzeigen und darauf zu antworten:


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. Wählen Sie für Typ die Option NetApp StorageGRID aus.
3. Wählen Sie für MediaAgent alle mit der Cloud-Bibliothek verknüpften Optionen aus.
4. Geben Sie unter Serverhost die IP-Adresse oder den Hostnamen des StorageGRID-Endpunkts und die Portnummer ein.

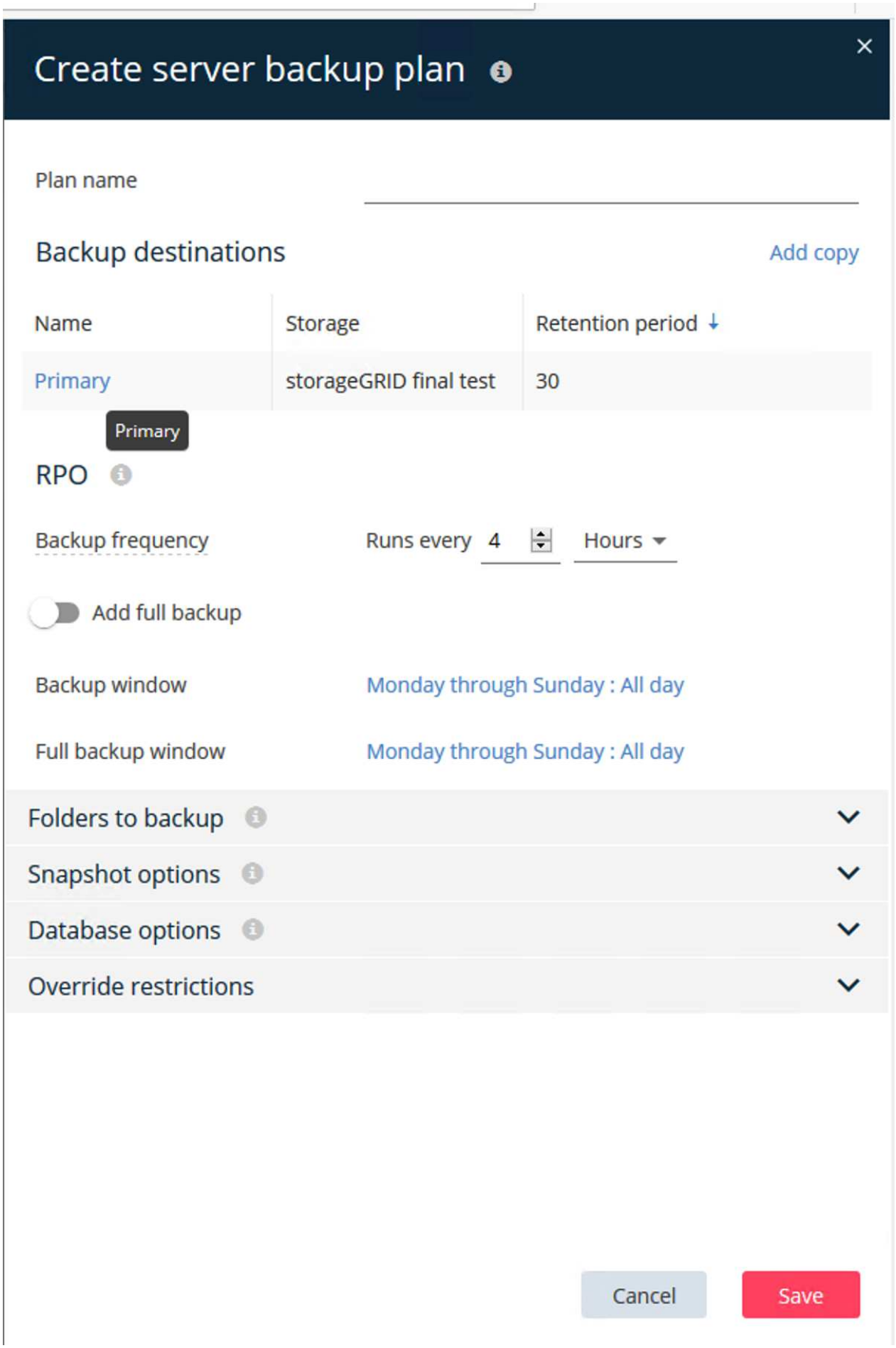
   Folgen Sie den Schritten in der StorageGRID-Dokumentation auf "So konfigurieren Sie einen Load Balancer-Endpunkt (Port)". Stellen Sie sicher, dass Sie über einen HTTPS-Port mit einem selbstsignierten Zertifikat und der IP-Adresse oder dem Domänennamen des StorageGRID-Endpunkts verfügen.

5. Wenn Sie Deduplizierung verwenden möchten, aktivieren Sie diese Option und geben den Pfad zum Speicherort der Deduplizierungsdatenbank an.
6. Klicken Sie auf Speichern .

Schritt 2: Erstellen eines Backup-Plans mit StorageGRID als primäres Ziel

Schritte

1. Wählen Sie im linken Fensterbereich Verwalten > Pläne aus, um das Dialogfeld Serverbackup-Plan erstellen anzuzeigen und darauf zu antworten.

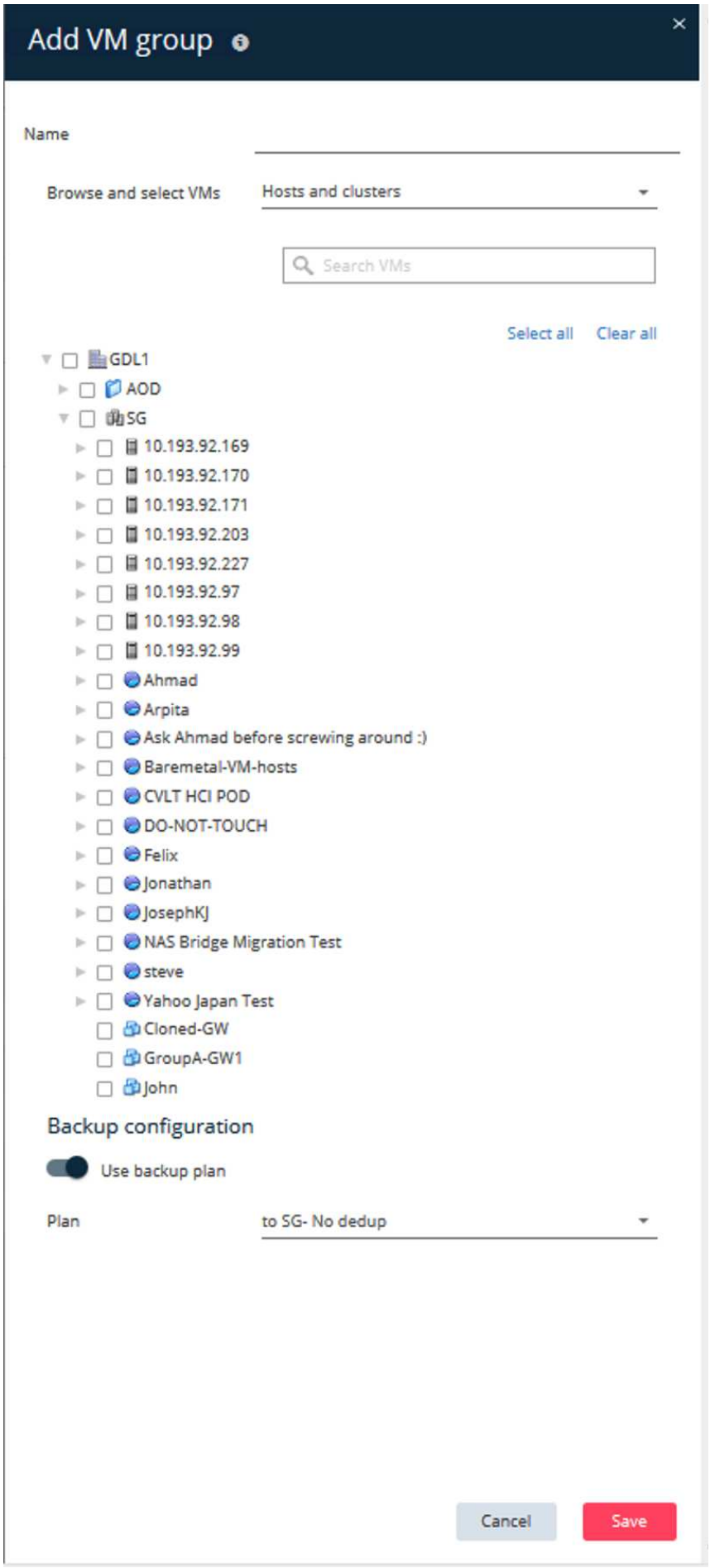

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. Geben Sie einen Plannamen ein.
3. Wählen Sie das zuvor erstellte Backup-Ziel für den StorageGRID Simple Storage Service (S3) Storage aus.
4. Geben Sie die gewünschte Backup-Aufbewahrungsfrist und das Recovery Point Objective (RPO) ein.
5. Klicken Sie auf Speichern .

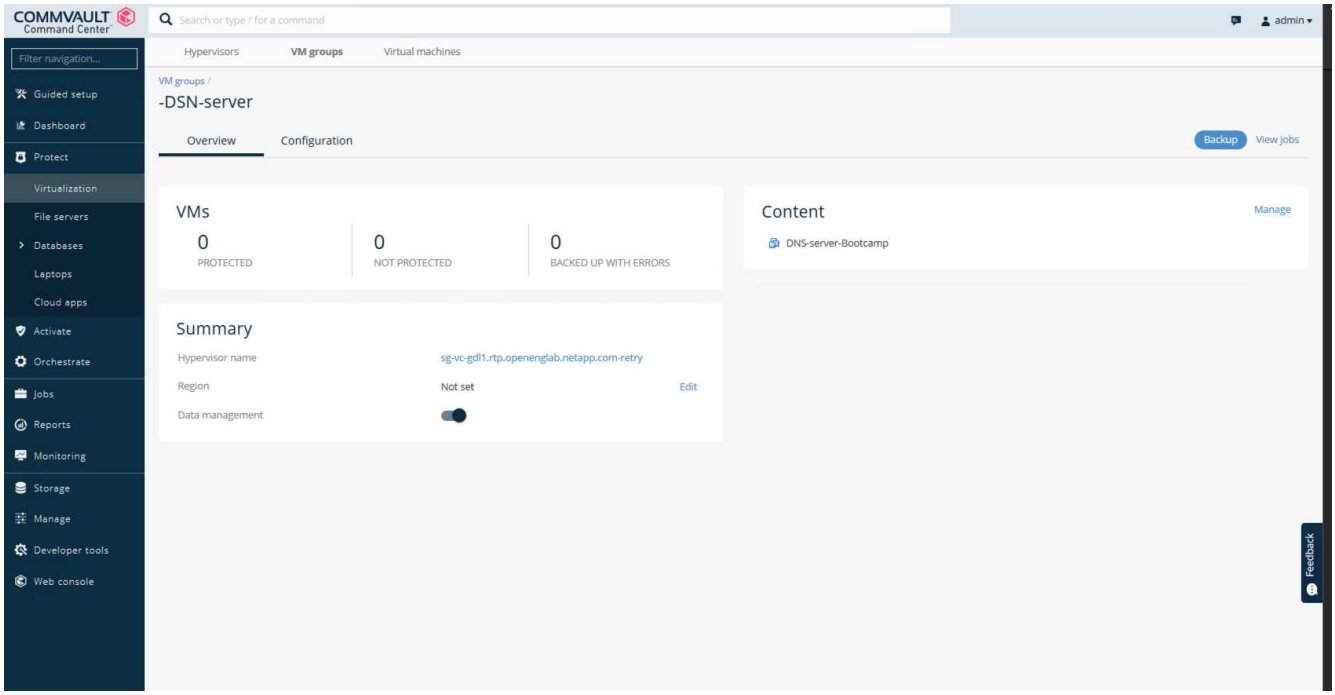
Schritt 3: Starten Sie einen Backup-Job zum Schutz Ihrer Workloads

Schritte

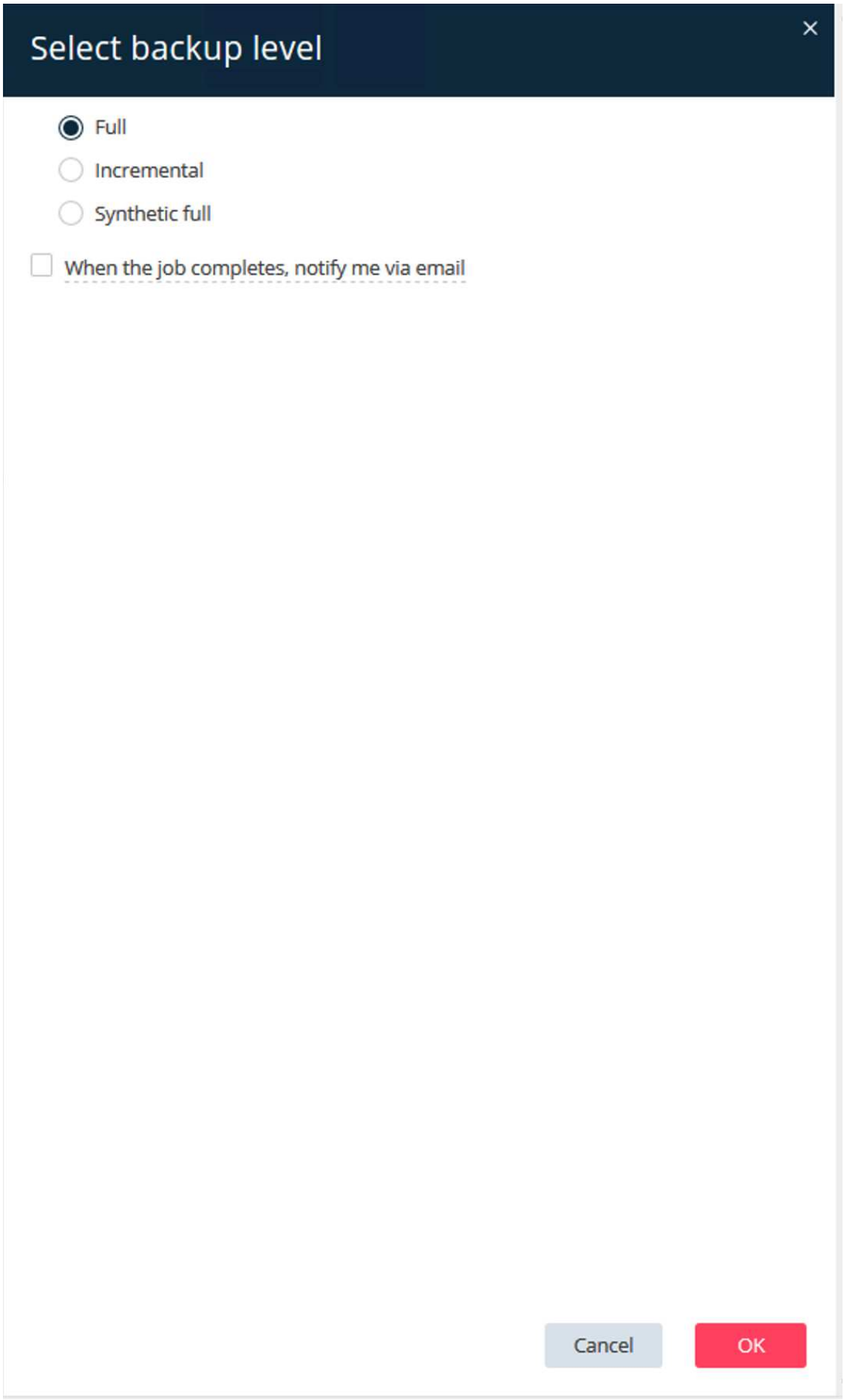
1. Navigieren Sie im CommVault Command Center zu Protect > Virtualization.
2. Fügen Sie einen VMware vCenter Server-Hypervisor hinzu.
3. Klicken Sie auf den Hypervisor, den Sie gerade hinzugefügt haben.
4. Klicken Sie auf VM-Gruppe hinzufügen, um auf das Dialogfeld VM-Gruppe hinzufügen zu antworten, damit Sie die vCenter-Umgebung sehen können, die Sie schützen möchten.


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

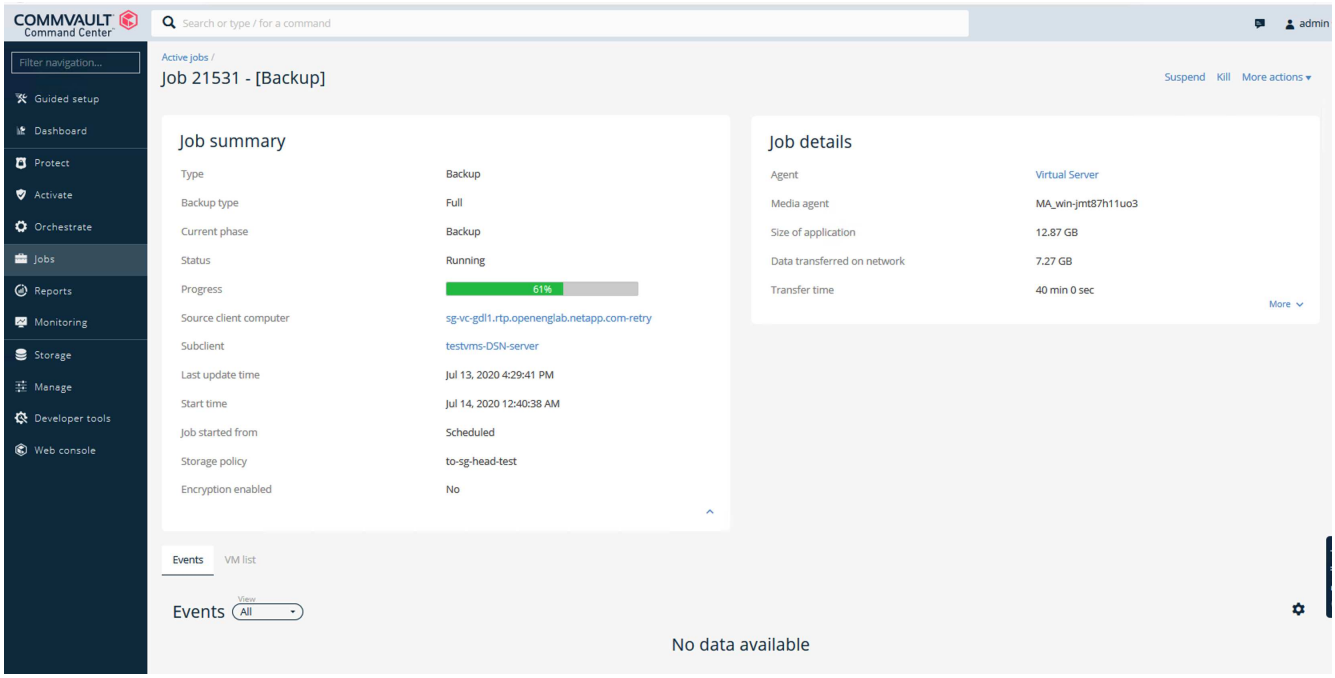
5. Wählen Sie einen Datenspeicher, eine VM oder eine Sammlung von VMs aus und geben Sie einen Namen dafür ein.
6. Wählen Sie den Backup-Plan aus, den Sie in der vorherigen Aufgabe erstellt haben.
7. Klicken Sie auf Speichern, um die erstellte VM-Gruppe anzuzeigen.
8. Wählen Sie oben rechts im VM-Gruppenfenster die Option Backup:



9. Wählen Sie als Sicherungsebene die Option voll aus, fordern Sie (optional) eine E-Mail an, wenn die Sicherung abgeschlossen ist, und klicken Sie dann auf OK, um den Sicherungsauftrag zu starten:


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. Navigieren Sie zur Seite mit der Jobzusammenfassung, um die Jobmetriken anzuzeigen:



Performance-Tests der Baseline prüfen

Beim Aux-Kopiervorgang haben vier CommVault MediaAgents Daten auf einem NetApp AFF A300-System gesichert und eine zusätzliche Kopie auf NetApp StorageGRID erstellt. Details zur Test-Setup-Umgebung finden Sie im Abschnitt Solution Design and Best Practices im "NetApp Scale-out-Datensicherung mit CommVault" technischen Bericht.

Die Tests wurden mit 100 VMs und 1000 VMs durchgeführt, wobei beide Tests mit einer Kombination aus Windows und CentOS VMs 50/50 durchgeführt wurden. Die folgende Tabelle enthält die Ergebnisse unserer grundlegenden Performance-Tests:

Betrieb	Backup-Geschwindigkeit	Wiederherstellungsgeschwindigkeit
Aux-Kopie	2 TB/Stunde	1.27 TB/Stunde
Direkt zum und vom Objekt (Deduplizierung ein)	2.2 TB/Stunde	1.22 TB/Stunde

Um eine Performance-Steigerung zu testen, wurden 2.5 Millionen Objekte gelöscht. Wie in den Abbildungen 2 und 3 dargestellt, wurde die Löschung in weniger als 3 Stunden abgeschlossen und mehr als 80 TB an Speicherplatz freigegeben. Der Löschvorgang begann um 10:30 UHR.

Abbildung 1: Löschung von 2.5 Millionen (80 TB) Objekten in weniger als 3 Stunden

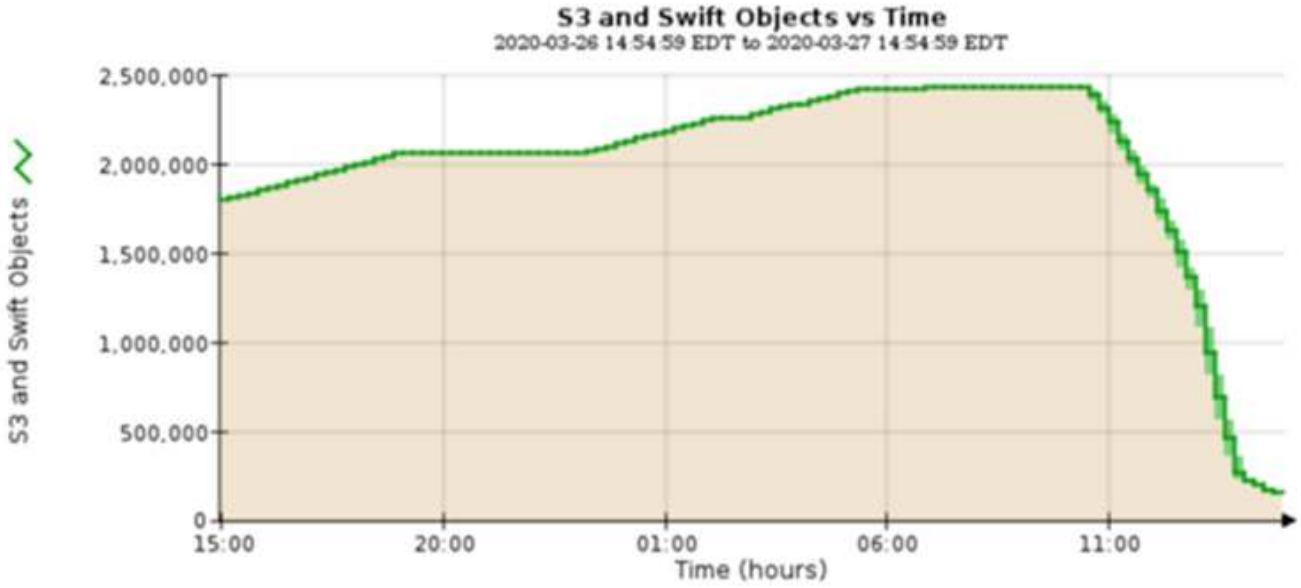
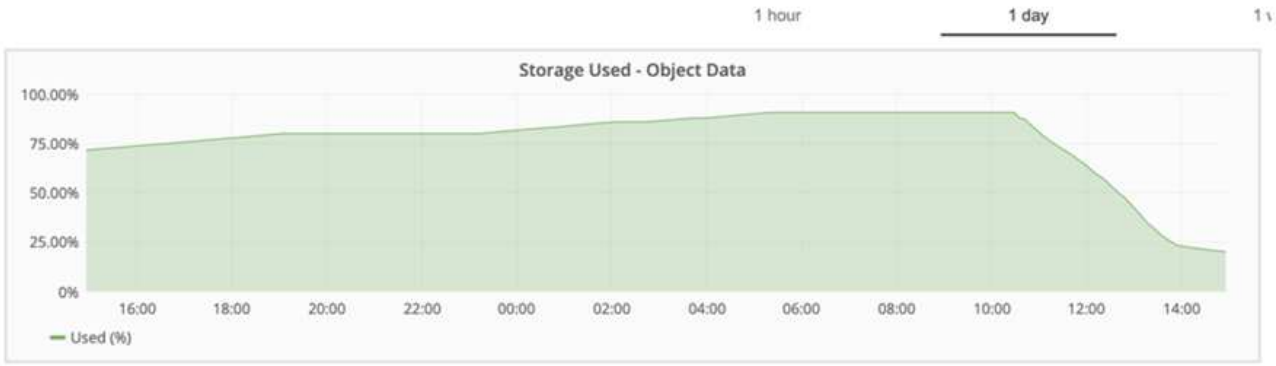


Abbildung 2: Freigabe von bis zu 80 TB Storage in weniger als 3 Stunden



Empfehlung für die Bucket-Konsistenzstufe

Mit NetApp StorageGRID kann der Endbenutzer die Konsistenzstufe für Vorgänge auswählen, die für Objekte in S3-Buckets (Simple Storage Service) durchgeführt werden.

CommVault MediaAgents sind die Data Mover in einer CommVault-Umgebung. In den meisten Fällen werden MediaAgents so konfiguriert, dass sie lokal in einen primären StorageGRID-Standort schreiben. Aus diesem Grund wird eine hohe Konsistenz innerhalb eines lokalen primären Standorts empfohlen. Beachten Sie die folgenden Richtlinien, wenn Sie die Konsistenzstufe für CommVault Buckets festlegen, die in StorageGRID erstellt wurden.

Wenn Sie eine CommVault-Version vor 11.0.0 - Service Pack 16 haben, sollten Sie ein Upgrade von CommVault auf die neueste Version in Betracht ziehen. Wenn dies keine Option ist, beachten Sie bitte die Richtlinien für Ihre Version.

- CommVault-Versionen vor 11.0.0 - Service Pack 16.* in Versionen vor 11.0.0 - Service Pack 16 führt CommVault S3 HEAD und GET-Operationen an nicht vorhandenen Objekten als Teil des Wiederherstellungs- und Beschneidungsprozesses durch. Wenn Sie die Konsistenzstufe für Bucket auf starke Standorte festlegen, wird die optimale Konsistenzstufe für CommVault Backups auf StorageGRID erreicht.

- CommVault-Versionen 11.0.0 - Service Pack 16 und höher.* in Version 11.0.0 - Service Pack 16 und höher wird die Anzahl der S3-HEAD- und GET-Vorgänge für nicht vorhandene Objekte minimiert. Setzen Sie die Standard-Bucket-Konsistenzstufe auf „Read-after-New-write“, um eine hohe Konsistenzstufe in der CommVault- und StorageGRID-Umgebung zu gewährleisten.

TR-4626: Load Balancer

Verwenden Sie Load Balancer von Drittanbietern mit StorageGRID

Erfahren Sie mehr über die Rolle eines Drittanbieters und globaler Load Balancer in einem Objektspeicher-System wie StorageGRID.

Allgemeine Hinweise für die Implementierung von NetApp® StorageGRID® mit Load Balancern von Drittanbietern.

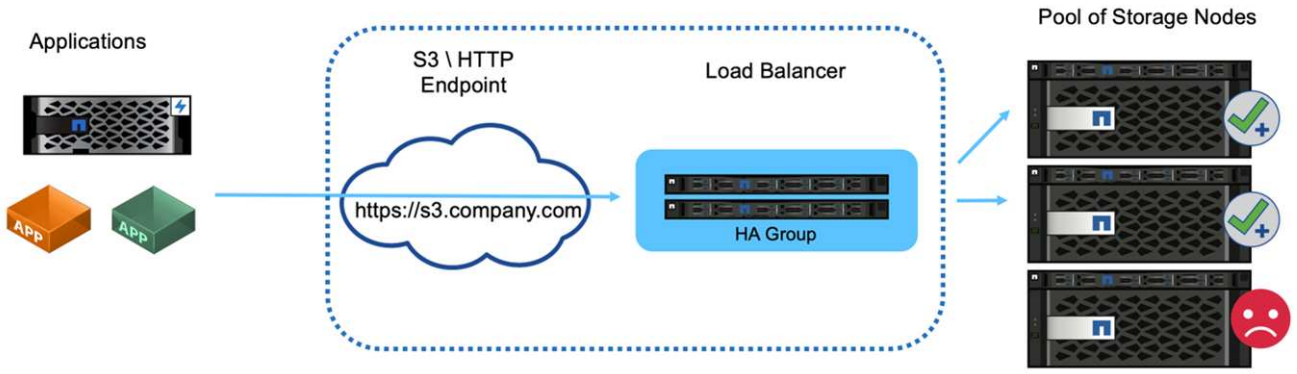
Objekt-Storage ist gleichbedeutend mit dem Begriff Cloud-Storage. Wie Sie erwarten würden, adressieren Applikationen, die Cloud-Storage nutzen, diesen Storage über eine URL. Unter dieser einfachen URL StorageGRID lässt sich die Kapazität, Performance und Langlebigkeit auf einen einzelnen Standort oder über geografisch verteilte Standorte skalieren. Die Komponente, die diese Einfachheit ermöglicht, ist ein Load Balancer.

Dieses Dokument dient dazu, StorageGRID Kunden über Load Balancer-Optionen zu informieren und allgemeine Hinweise zur Konfiguration von Load Balancern anderer Anbieter zu geben.

Grundlagen der Lastverteilung

Load Balancer sind eine wesentliche Komponente von Objekt-Storage-Systemen der Enterprise-Klasse wie StorageGRID. StorageGRID besteht aus mehreren Storage-Nodes, von denen jeder den gesamten S3-Namensraum (Simple Storage Service) für eine bestimmte StorageGRID Instanz darstellen kann. Load Balancer erzeugen einen hochverfügbaren Endpunkt, hinter dem StorageGRID Nodes platziert werden können. StorageGRID ist einzigartig unter S3-kompatiblen Objektspeichersystemen, da es einen eigenen Load Balancer anbietet, aber auch Load Balancer von Drittanbietern oder Mehrzweck-Systemen wie F5, Citrix NetScaler, HA Proxy, NGINX usw. unterstützt.

In der folgenden Abbildung wird der Beispiel-URL/ Fully Qualified Domain Name (FQDN) „s3.company.com” verwendet. Der Load Balancer erstellt eine virtuelle IP (VIP), die über DNS in den FQDN aufgelöst wird und leitet dann alle Anforderungen von Anwendungen an einen Pool von StorageGRID-Knoten weiter. Der Load Balancer führt eine Integritätsprüfung für jeden Node durch und stellt nur Verbindungen zu funktionstüchtigen Nodes her.



Die Abbildung zeigt den von StorageGRID bereitgestellten Load Balancer, das Konzept ist jedoch dasselbe bei

Load Balancern von Drittanbietern. Anwendungen richten eine HTTP-Sitzung mithilfe der VIP auf dem Load Balancer ein und der Datenverkehr wird über den Load Balancer zu den Speicher-Nodes geleitet. Standardmäßig wird der gesamte Datenverkehr von der Anwendung zum Load Balancer und vom Load Balancer zum Speicher-Node über HTTPS verschlüsselt. HTTP ist eine unterstützte Option.

Lokale und globale Load Balancer

Es gibt zwei Arten von Load Balancern:

- * Local Traffic Manager (LTM)*. Verteilt Verbindungen über einen Node-Pool an einem einzelnen Standort.
- **Global Service Load Balancer (GSLB)**. Verteilt Verbindungen über mehrere Standorte und sorgt so für einen effektiven Lastenausgleich bei LTM-Load-Balancern. Stellen Sie sich ein GSLB als intelligenten DNS-Server vor. Wenn ein Client eine StorageGRID-Endpunkt-URL anfordert, löst die GSLB sie auf Grundlage der Verfügbarkeit oder anderer Faktoren in die VIP eines LTM auf (z. B. welche Website kann eine niedrigere Latenz für die Anwendung bereitstellen). Es ist zwar immer ein LTM erforderlich, abhängig von der Anzahl der StorageGRID-Standorte und Ihren Applikationsanforderungen ist jedoch ein GSLB optional.

Wo Sie weitere Informationen finden

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

- NetApp StorageGRID Dokumentationscenterhttps://docs.netapp.com/us-en/storagegrid/[]
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- Überlegungen zum Design der StorageGRID f5 Load Balancer https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load NetApp StorageGRID ausgleichen https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp – Load Balancing NetApp StorageGRID https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Verwenden Sie StorageGRID Load Balancer

Erfahren Sie mehr über die Rolle eines StorageGRID Gateway Node-Load Balancers.

Allgemeine Anleitung zur Implementierung von NetApp® StorageGRID® Gateway Nodes.

Load Balancer für StorageGRID-Gateway-Nodes im Vergleich zum Load Balancer eines Drittanbieters

StorageGRID ist einzigartig unter S3-kompatiblen Objekt-Storage-Anbietern und bietet einen nativen Load Balancer als speziell entwickelte Appliance, VM oder Container. Der von StorageGRID bereitgestellte Load Balancer wird auch als Gateway-Node bezeichnet.

Für Kunden, die noch keinen Load Balancer wie F5, Citrix usw. besitzen, kann die Implementierung eines Load Balancers eines Drittanbieters sehr komplex sein. Der StorageGRID Load Balancer vereinfacht den Load Balancer erheblich.

Der Gateway Node ist ein hochverfügbarer und hochperformanter Load Balancer der Enterprise-Klasse. Kunden können den Gateway Node, den Load Balancer eines Drittanbieters oder sogar beide in einem Grid implementieren. Der Gateway Node ist ein lokaler Traffic-Manager und kein GSLB.

Der StorageGRID Load Balancer bietet folgende Vorteile:

- **Einfachheit**. Automatische Konfiguration von Ressourcen-Pools, Zustandsprüfungen, Patching und Wartung, alle gemanagt durch StorageGRID.
- **Leistung**. Der StorageGRID Load Balancer ist speziell für StorageGRID vorgesehen, kann Hochleistungs-Caching bereitstellen und Sie konkurrieren nicht mit anderen Anwendungen um Bandbreite.
- **Kosten**. Die Versionen für Virtual Machines (VM) und Container werden ohne zusätzliche Kosten bereitgestellt.
- **Verkehrsklassifizierungen**. Die Funktion zur erweiterten Traffic-Klassifizierung ermöglicht für StorageGRID spezifische QoS-Regeln sowie Workload-Analysen.
- **Zukünftige StorageGRID-spezifische Funktionen**. StorageGRID wird den Load Balancer in künftigen Versionen weiter optimieren und um innovative Funktionen erweitern.

Als integrierter Knoten von StorageGRID kann der lokale Verkehrsmanager erweiterte Integritätsprüfungen durchführen, um Anfragen basierend auf der Integrität, Auslastung und Ressourcenverfügbarkeit des Speicherknotens zu verteilen. Darüber hinaus besteht die Möglichkeit, die Last auf mehrere Standorte zu verteilen, wenn die StorageGRID Verbindungskosten zwischen den Standorten auf „0“ gesetzt sind. Falls die Speicherknoten nicht verfügbar sind, der Gateway-Knoten an einem Standort jedoch verfügbar ist, wird die Last automatisch an einen anderen Standort im Netz umgeleitet.

Die Load Balancer-Caching-Funktion des Gateway-Knotens soll eine erhebliche Leistungsverbesserung für bestimmte Workloads (wie z. B. KI-Training) bieten, bei denen ein Datensatz im Rahmen der Verarbeitung dieser Daten mehrmals erneut gelesen wird. Caching-Gateway-Knoten können auch physisch vom Rest des Grids entfernt bereitgestellt werden, was bei einigen Workloads eine bessere Leistung und eine geringere WAN-Netzwerkauslastung ermöglicht. Der Cache arbeitet in einem Rücklesemodus, in dem Schreibvorgänge nicht zwischengespeichert werden und den Zustand des Caches nicht ändern. Jeder Caching-Gateway-Knoten arbeitet unabhängig von allen anderen Caching-Gateway-Knoten.

Weitere Informationen zum Bereitstellen des StorageGRID Gateway Node finden Sie im "StorageGRID-Dokumentation" .

Erfahren Sie, wie Sie SSL-Zertifikate für HTTPS in StorageGRID implementieren

Verstehen Sie die Wichtigkeit und die Schritte zur Implementierung von SSL-Zertifikaten in StorageGRID.

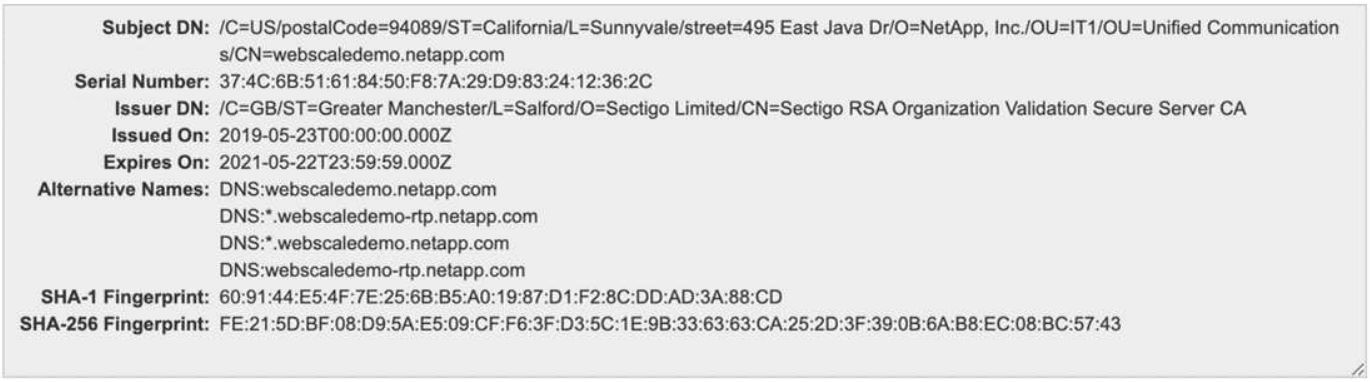
Wenn Sie HTTPS verwenden, müssen Sie über ein SSL-Zertifikat (Secure Sockets Layer) verfügen. Das SSL-Protokoll identifiziert die Clients und Endpunkte und validiert sie als vertrauenswürdig. SSL bietet auch die Verschlüsselung des Datenverkehrs. Das SSL-Zertifikat muss von den Clients vertrauenswürdig sein. Dazu kann das SSL-Zertifikat von einer global vertrauenswürdigen Zertifizierungsstelle (CA) wie DigiCert, einer privaten Zertifizierungsstelle, die in Ihrer Infrastruktur ausgeführt wird, oder einem vom Host generierten selbstsignierten Zertifikat stammen.

Die Verwendung eines global vertrauenswürdigen Zertifizierungsstellenzertifikats ist die bevorzugte Methode, da keine zusätzlichen clientseitigen Aktionen erforderlich sind. Das Zertifikat wird in den Load Balancer oder StorageGRID geladen, und die Clients vertrauen dem Endpunkt und stellen eine Verbindung her.

Für die Verwendung einer privaten Zertifizierungsstelle muss der Stammverzeichnis und alle untergeordneten Zertifikate zum Client hinzugefügt werden. Der Prozess zum Vertrauen auf ein privates CA-Zertifikat kann je nach Client-Betriebssystem und -Anwendungen variieren. Beispielsweise müssen Sie in ONTAP für FabricPool jedes Zertifikat in der Kette einzeln (Stammzertifikat, untergeordnetes Zertifikat, Endpunktzertifikat) auf das ONTAP-Cluster hochladen.

Bei Verwendung eines selbstsignierten Zertifikats muss der Client dem bereitgestellten Zertifikat vertrauen, ohne dass eine Zertifizierungsstelle die Authentizität überprüft. Einige Anwendungen akzeptieren möglicherweise keine selbstsignierten Zertifikate und können die Überprüfung nicht ignorieren.

Die Platzierung des SSL-Zertifikats im StorageGRID-Pfad des Client Load Balancer hängt davon ab, wo Sie die SSL-Terminierung benötigen. Sie können einen Load Balancer als Abschlussendpunkt für den Client konfigurieren und dann erneut verschlüsseln oder mit einem neuen SSL-Zertifikat für den Load Balancer zur StorageGRID-Verbindung verschlüsseln. Sie können auch den Datenverkehr passieren und StorageGRID als Endpunkt für die SSL-Terminierung verwenden. Wenn der Load Balancer der SSL-Abschlussendpunkt ist, wird das Zertifikat auf dem Load Balancer installiert und enthält den Betreffnamen für den DNS-Namen/die DNS-URL sowie alle alternativen URL-/DNS-Namen, für die ein Client für die Verbindung mit dem StorageGRID-Ziel über den Load Balancer konfiguriert ist. einschließlich aller Platzhalternamen. Wenn der Load Balancer für Passthrough konfiguriert ist, muss das SSL-Zertifikat in StorageGRID installiert werden. Auch hier muss das Zertifikat den Subject-Namen für den DNS-Namen/die URL sowie alle alternativen URL-/DNS-Namen enthalten, für die ein Client konfiguriert ist, um über den Load Balancer eine Verbindung zum StorageGRID-Ziel herzustellen, einschließlich aller Platzhalternamen. Einzelne Storage-Node-Namen müssen nicht im Zertifikat enthalten sein, sondern nur die Endpunkt-URLs.



Konfigurieren Sie den Load Balancer eines vertrauenswürdigen Drittanbieters in StorageGRID

Erfahren Sie, wie Sie einen vertrauenswürdigen Drittanbieter-Load Balancer in StorageGRID konfigurieren.

Wenn Sie einen oder mehrere externe Layer-7-Load-Balancer und IP-basierte S3-Bucket oder Gruppenrichtlinien verwenden, muss StorageGRID die IP-Adresse des tatsächlichen Absenders ermitteln. Dies geschieht durch einen Blick auf den X-Forwarded-for (XFF) Header, der vom Load Balancer in die Anfrage eingefügt wird. Da der XFF-Header einfach in Anfragen gespoooofing werden kann, die direkt an die Speicherknoten gesendet werden, muss StorageGRID bestätigen, dass jede Anforderung von einem vertrauenswürdigen Layer 7-Load-Balancer weitergeleitet wird. Wenn StorageGRID der Quelle der Anforderung nicht vertrauen kann, ignoriert er den XFF-Header. Es gibt eine Grid-Management-API, über die eine Liste vertrauenswürdiger externer Load Balancer der Ebene 7 konfiguriert werden kann. Diese neue API ist privat und kann sich bei zukünftigen StorageGRID Versionen ändern. Die aktuellsten Informationen finden Sie im KB-Artikel, "So konfigurieren Sie StorageGRID für die Verwendung mit Layer-7-Load-Balancern von Drittanbietern".

Informieren Sie sich über Load Balancer für lokale Traffic Manager

Informieren Sie sich über die Richtlinien für den Lastenausgleich von lokalen Traffic-Managern und ermitteln Sie die optimale Konfiguration.

Die folgenden Informationen werden als allgemeine Anleitung für die Konfiguration von Load Balancern von Drittanbietern dargestellt. Ermitteln Sie zusammen mit dem Load Balancer-Administrator die optimale Konfiguration für Ihre Umgebung.

Erstellen Sie eine Ressourcengruppe von Storage-Nodes

Gruppieren Sie StorageGRID-Speicherknoten in einen Ressourcen-Pool oder eine Dienstgruppe (die Terminologie kann sich von bestimmten Load Balancern unterscheiden). StorageGRID-Storage-Nodes stellen die S3-API auf den folgenden Ports zur Verfügung:

- S3 HTTPS: 18082
- S3 HTTP: 18084

Die meisten Kunden entscheiden sich dafür, die APIs auf dem virtuellen Server über die standardmäßigen HTTPS- und HTTP-Ports (443 und 80) bereitzustellen.

> Für jeden StorageGRID-Standort sind standardmäßig drei Storage-Nodes erforderlich, von denen zwei ordnungsgemäß sein müssen.

Zustandsprüfung

Load Balancer von Drittanbietern erfordern eine Methode, um den Zustand der einzelnen Nodes und ihre Eignung für den Empfang von Traffic zu bestimmen. NetApp empfiehlt zur Durchführung der Integritätsprüfung die HTTP- `OPTIONS` Methode. Der Load Balancer sendet HTTP- `OPTIONS` Anforderungen an jeden einzelnen Speicher-Node und erwartet eine `200` Statusantwort.

Wenn ein Speicher-Node keine Antwort bereitstellt, kann dieser Node keine `200` Speicheranforderungen bearbeiten. Ihre Anwendungs- und Geschäftsanforderungen sollten das Zeitlimit für diese Prüfungen und die Maßnahmen bestimmen, die Ihr Load Balancer ergreift.

Wenn beispielsweise drei von vier Storage-Nodes in Datacenter 1 ausgefallen sind, können Sie den gesamten Datenverkehr an Datacenter 2 leiten.

Das empfohlene Abfrageintervall beträgt einmal pro Sekunde und markiert den Knoten nach drei fehlgeschlagenen Überprüfungen offline.

Beispiel für S3-Integritätsprüfung

Im folgenden Beispiel senden wir `OPTIONS` und überprüfen nach `200 OK`. Wir verwenden `OPTIONS` , da Amazon S3) nicht autorisierte Anfragen unterstützt.

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

Zustandsprüfungen für Dateien oder Inhalte

Im Allgemeinen werden von NetApp keine dateibasierten Zustandsprüfungen empfohlen. In der Regel wird eine kleine Datei —`healthcheck.htm`z. B. in einem Bucket mit einer schreibgeschützten Richtlinie erstellt. Diese Datei wird dann vom Load Balancer abgerufen und ausgewertet. Dieser Ansatz hat mehrere Nachteile:

- **Abhängig von einem einzigen Konto.** Wenn das Konto, dem die Datei gehört, deaktiviert ist, schlägt die Integritätsprüfung fehl und es werden keine Speicheranforderungen verarbeitet.
- **Datenschutzregeln.** Das standardmäßige Datensicherungsschema hat einen Ansatz mit zwei Kopien. Wenn in diesem Szenario die beiden Speicherknoten, auf denen die Zustandspeckdatei gehostet wird, nicht verfügbar sind, schlägt die Integritätsprüfung fehl, und Speicheranforderungen werden nicht an funktionstüchtige Speicherknoten gesendet, wodurch das Grid offline geschaltet wird.
- **Audit Log Bloat.** Der Load Balancer ruft die Datei alle X Minuten von jedem Storage-Node ab und erstellt so viele Audit-Log-Einträge.
- **Ressourcenintensiv.** Das Abrufen der Zustandspeckdatei von jedem Node alle paar Sekunden verbraucht Grid- und Netzwerkressourcen.

Wenn eine inhaltsbasierte Zustandsprüfung erforderlich ist, verwenden Sie einen dedizierten Mandanten mit einem dedizierten S3-Bucket.

Persistenz der Sitzung

Sitzungspersistence oder Stickiness bezieht sich auf den Zeitpunkt, zu dem eine bestimmte HTTP-Sitzung bestehen darf. Standardmäßig werden Sitzungen von Storage-Nodes nach 10 Minuten getrennt. Längere Persistenz kann zu besserer Performance führen, da die Applikationen nicht für jede Aktion neu Sitzungen erstellen müssen. Offen zu halten, verbraucht jedoch Ressourcen. Wenn Sie feststellen, dass Ihr Workload von Vorteil ist, können Sie die Persistenz der Sitzung bei einem Load Balancer eines Drittanbieters verringern.

Virtuelle Hosted-Style-Adressierung

Virtual Hosted-Style ist jetzt die Standardmethode für AWS S3. Während StorageGRID und viele Applikationen weiterhin Pfadstil unterstützen, empfiehlt es sich, Unterstützung im Virtual Hosted-Stil zu implementieren. Virtuelle Anforderungen im gehosteten Stil enthalten den Bucket als Teil des Host-Namens.

Gehen Sie wie folgt vor, um Virtual Hosted-Style zu unterstützen:

- Unterstützung von Wildcard-DNS-Suchvorgängen: *.s3.company.com
- Verwenden Sie ein SSL-Zertifikat mit Subject alt-Namen, um Wildcard zu unterstützen: *.s3.company.com einige Kunden haben Sicherheitsbedenken bezüglich der Verwendung von Wildcard-Zertifikaten geäußert. StorageGRID unterstützt wie wichtige Applikationen wie FabricPool weiterhin den Zugriff auf Pfadstil. Allerdings schlagen bestimmte S3-API-Aufrufe fehl oder verhalten sich ohne virtuelle gehostete Unterstützung nicht ordnungsgemäß.

SSL-Terminierung

Die SSL-Terminierung bei Load Balancern von Drittanbietern bietet Sicherheitsvorteile. Wenn der Load Balancer beschädigt ist, wird das Grid unterteilt.

Es gibt drei unterstützte Konfigurationen:

- **SSL-Passthrough.** Das SSL-Zertifikat wird auf StorageGRID als benutzerdefiniertes Serverzertifikat installiert.
- **SSL-Terminierung und Re-Verschlüsselung (empfohlen).** Dies könnte von Vorteil sein, wenn Sie bereits die SSL-Zertifikatsverwaltung auf dem Load Balancer ausführen, anstatt das SSL-Zertifikat auf StorageGRID zu installieren. Diese Konfiguration bietet den zusätzlichen Sicherheitsvorteil, wenn die Angriffsfläche auf den Load Balancer begrenzt wird.
- **SSL-Terminierung mit HTTP.** In dieser Konfiguration wird SSL auf dem Load Balancer des Drittanbieters beendet und die Kommunikation vom Load Balancer zu StorageGRID ist unverschlüsselt, um die Vorteile von SSL-Off-Load zu nutzen (bei SSL-Bibliotheken, die in moderne Prozessoren integriert sind, ist dies nur ein begrenzter Vorteil).

Konfiguration durchlaufen

Wenn Sie den Load Balancer für Passthrough konfigurieren möchten, müssen Sie das Zertifikat auf StorageGRID installieren. Gehen Sie zum Menü:Konfiguration[Serverzertifikate > Object Storage API Service Endpoints Server Certificate].

IP-Sichtbarkeit des Quell-Clients

Mit StorageGRID 11.4 wurde das Konzept eines vertrauenswürdigen Load Balancers eines Drittanbieters eingeführt. Um die Client-Anwendungs-IP an StorageGRID weiterzuleiten, müssen Sie diese Funktion konfigurieren. Weitere Informationen finden Sie unter "So konfigurieren Sie StorageGRID für die Verwendung mit Layer-7-Load-Balancern von Drittanbietern."

So aktivieren Sie den XFF-Header, um die IP-Adresse der Client-Anwendung anzuzeigen:

Schritte

1. Notieren Sie die Client-IP im Überwachungsprotokoll.
2. Verwendung von `aws:SourceIp` S3-Bucket oder Gruppenrichtlinien

Strategien für die Lastverteilung

Die meisten Lastausgleichslösungen bieten mehrere Strategien für den Lastausgleich. Es folgen gängige Strategien:

- * Rundrobin.* Universelle Passform, jedoch mit wenigen Knoten und großen Transfers, die einzelne Knoten verstopfen
- **Geringste Verbindung.** Eignet sich für kleine und gemischte Objekt-Workloads, sodass die Verbindungen auf alle Nodes gleichmäßig verteilt werden.

Die Auswahl des Algorithmus wird mit einer wachsenden Anzahl von Storage-Nodes weniger wichtig.

Datenpfad

Alle Daten fließen über den Lastenausgleich des lokalen Traffic Managers. StorageGRID unterstützt kein direktes Server-Routing (DSR).

Überprüfen der Verteilung der Verbindungen

Um zu überprüfen, ob Ihre Methode die Last gleichmäßig auf die Storage-Nodes verteilt, überprüfen Sie die festgelegten Sitzungen auf jedem Node an einem bestimmten Standort:

- **UI-Methode.** Gehen Sie zum Menü:Support[Kennzahlen > S3-Übersicht > LDR HTTP-Sitzungen]
- **Metrics API.** Verwenden `storagegrid_http_sessions_incoming_currently_established`

Lernen Sie einige Anwendungsfälle für StorageGRID Konfigurationen kennen

Sehen Sie sich einige Anwendungsfälle für StorageGRID-Konfigurationen an, die von Kunden und NetApp IT implementiert wurden.

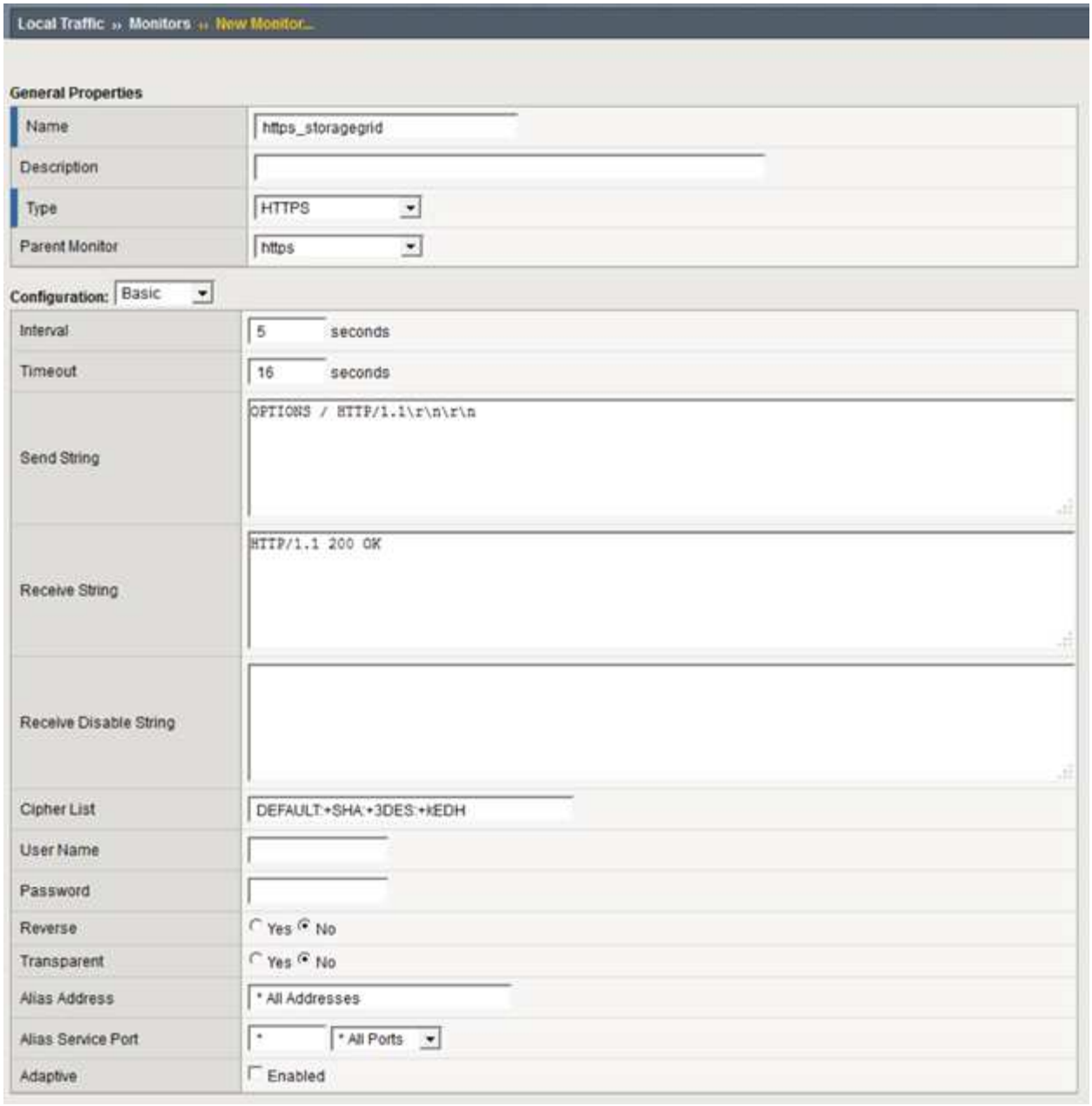
Die folgenden Beispiele veranschaulichen die Konfigurationen, die von StorageGRID Kunden, einschließlich NetApp IT, implementiert wurden.

Systemzustandsüberwachung von F5 BIG-IP Local Traffic Manager für S3 Bucket

Gehen Sie wie folgt vor, um die Integritätsprüfung für den F5 BIG-IP Local Traffic Manager zu konfigurieren:

Schritte

1. Erstellen Sie einen neuen Monitor.
   a. Geben Sie im Feld Typ `HTTPS`.
   b. Konfigurieren Sie das Intervall und die Zeitüberschreitung nach Bedarf.
   c. Geben Sie im Feld Send String \r\n sind Wagenrückläufe ein `OPTIONS / HTTP/1.1\r\n\r\n.` ; verschiedene Versionen der BIG-IP-Software erfordern Null, einen oder zwei Sätze von \r\n Sequenzen. Weitere Informationen finden Sie unter https://support.f5.com/csp/article/K10655.
   d. Geben Sie im Feld Empfangszeichenfolge Folgendes ein: `HTTP/1.1 200 OK`.



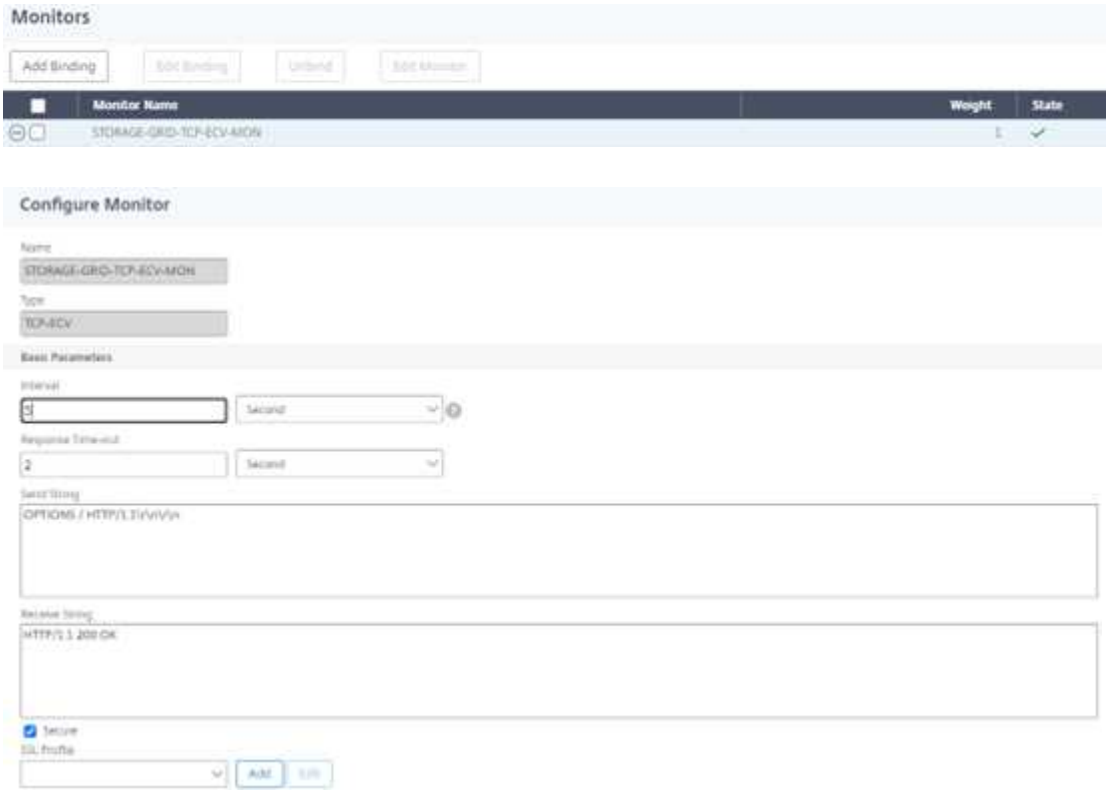
2. Erstellen Sie in Create Pool für jeden erforderlichen Port einen Pool.
   a. Weisen Sie die im vorherigen Schritt erstellte Systemzustandsüberwachung zu.
   b. Wählen Sie eine Lastausgleichsmethode aus.
   c. Wählen Sie Service Port: 18082 (S3).
   d. Nodes hinzufügen.

Citrix NetScaler

Citrix NetScaler erstellt einen virtuellen Server für den Speicherendpunkt und verweist auf StorageGRID-Speicherknoten als Anwendungsserver, die dann in Dienste gruppiert werden.

Verwenden Sie die HTTPS-ECV-Integritätsprüfung, um einen benutzerdefinierten Monitor zu erstellen, der die empfohlene Integritätsprüfung mithilfe der OPTIONSANFRAGE und des Empfangs durchführt `200`. HTTP-ECV ist mit einem Sendestring konfiguriert und validiert eine Empfangszeichenfolge.

Weitere Informationen finden Sie in der Citrix-Dokumentation, "Beispielkonfiguration für HTTP-ECV-Integritätsprüfung".



Loadbalancer.org

Loadbalancer.org hat eigene Integrationstests mit StorageGRID durchgeführt und hat einen umfassenden Konfigurationsleitfaden: https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp hat eigene Integrationstests mit StorageGRID durchgeführt und verfügt über einen umfassenden Konfigurationsleitfaden: https://kemptechnologies.com/solutions/netapp/.

HAProxy

Konfigurieren Sie HAProxy so, dass die OPTIONS-Anfrage verwendet wird, und prüfen Sie auf eine 200-Statusantwort für die Integritätsprüfung in haproxy.cfg. Sie können den Bind-Port am Front-End in einen anderen Port ändern, z. B. 443.

Im Folgenden finden Sie ein Beispiel für die SSL-Terminierung auf HAProxy:

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

Im Folgenden ein Beispiel für SSL-Passthrough:

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

Vollständige Beispiele für Konfigurationen für StorageGRID finden Sie unter "Beispiele für die HAProxy-Konfiguration" auf GitHub.

SSL-Verbindung in StorageGRID validieren

Erfahren Sie, wie Sie die SSL-Verbindung in StorageGRID validieren.

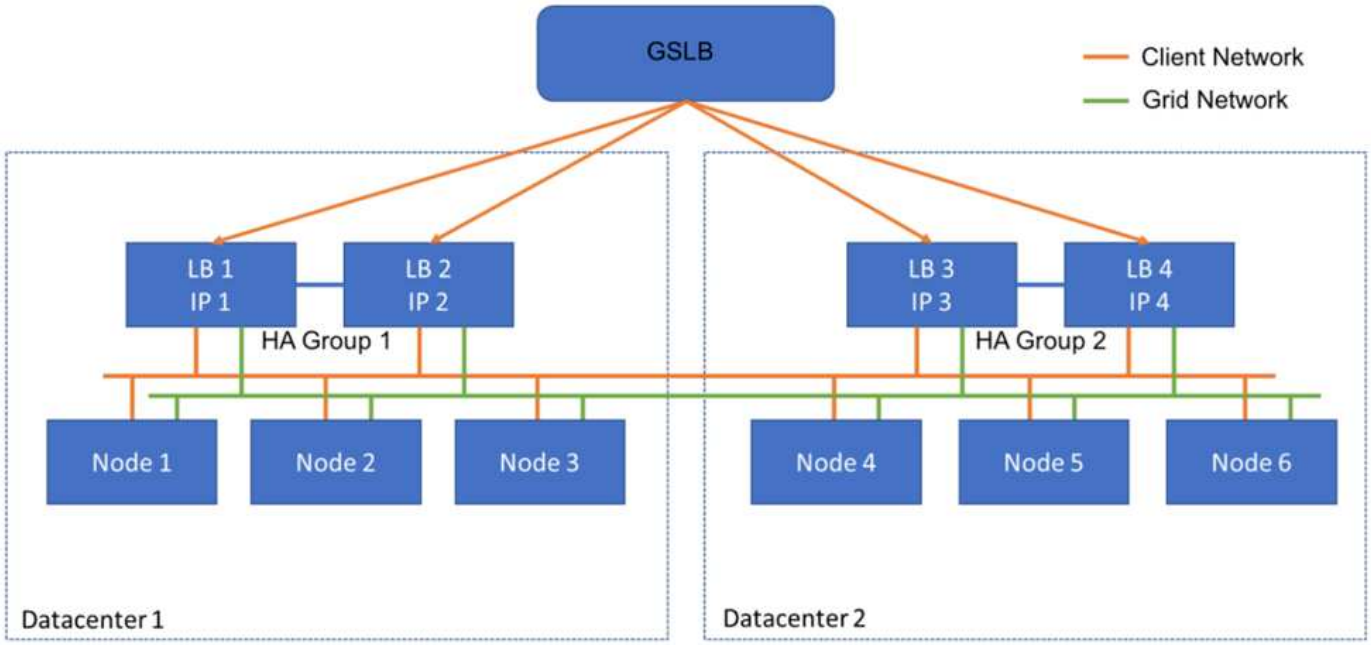
Nachdem der Load Balancer konfiguriert ist, sollten Sie die Verbindung mit Tools wie OpenSSL und der AWS CLI validieren. Andere Anwendungen, wie beispielsweise S3 Browser, ignorieren möglicherweise eine fehlerhafte SSL-Konfiguration.

Informationen zu den globalen Lastausgleichsanforderungen für StorageGRID

Informieren Sie sich über die Designüberlegungen und Anforderungen für den globalen Lastausgleich in StorageGRID.

Globaler Lastausgleich erfordert die Integration in DNS, um intelligentes Routing über mehrere StorageGRID-Standorte hinweg zu ermöglichen. Diese Funktion fällt nicht in die StorageGRID-Domäne und muss von einer Drittanbieterlösung bereitgestellt werden, z. B. den bereits erläuterten Load Balancer-Produkten und/oder einer DNS-Lösung zur Traffic-Kontrolle wie Infoblox. Dieser Lastenausgleich der obersten Ebene bietet intelligentes

Routing zum nächsten Zielstandort im Namespace sowie Ausfallerkennung und Umleitung zum nächsten Standort im Namespace. Eine typische GSLB-Implementierung besteht aus dem GSLB der obersten Ebene mit Standortpools mit standortlokalen Load Balancern. Die Standortlastverteiler enthalten Pools der lokalen Speicher-Nodes am Standort. Dies kann eine Kombination aus Load Balancern von Drittanbietern für GSLB-Funktionen und StorageGRID für den lokalen Lastausgleich oder eine Kombination aus Drittanbietern sein. Oder viele der zuvor besprochenen Drittanbieter bieten sowohl GSLB als auch einen standortweiten lokalen Lastausgleich.



TR-4645: Sicherheitsfunktionen

Sichern von StorageGRID-Daten und -Metadaten in einem Objektspeicher

Entdecken Sie die integrierten Sicherheitsfunktionen der StorageGRID Objekt-Storage-Lösung.

Dies ist eine Übersicht über die zahlreichen Sicherheitsfunktionen in NetApp® StorageGRID®, die Datenzugriff, Objekte und Metadaten, Administratorzugriff und Plattformsicherheit abdecken. Es wurde aktualisiert, um die neuesten Funktionen zu enthalten, die mit StorageGRID 12.0 veröffentlicht wurden.

Sicherheit ist ein integraler Bestandteil der NetApp StorageGRID Objekt-Storage-Lösung. Die Sicherheit ist besonders wichtig, da viele Arten von umfangreichen Datenmengen, die gut für Objekt-Storage geeignet sind, ebenfalls sehr sensibel sind und gesetzlichen Vorschriften und Compliance unterliegen. Während sich die Funktionen von StorageGRID weiterentwickeln, stellt die Software viele Sicherheitsfunktionen zur Verfügung, die von unschätzbarem Wert sind, um die Sicherheit eines Unternehmens zu schützen und dem Unternehmen dabei zu helfen, die Best Practices der Branche einzuhalten.

Dieses Dokument bietet einen Überblick über die zahlreichen Sicherheitsfunktionen in StorageGRID 12.0, unterteilt in fünf Kategorien:

- Sicherheitsfunktionen für den Datenzugriff
- Sicherheitsfunktionen für Objekte und Metadaten
- Sicherheitsfunktionen für die Administration

- Plattformsicherheitsfunktionen
- Cloud-Integration

Dieses Dokument ist als Sicherheitsdatenblatt gedacht. Es enthält keine detaillierten Informationen zur Konfiguration des Systems, um die darin aufgeführten Sicherheitsfunktionen zu unterstützen, die nicht standardmäßig konfiguriert sind. Der "Leitfaden zum StorageGRID Hardening" ist auf der offiziellen "StorageGRID-Dokumentation" Seite.

Zusätzlich zu den in diesem Bericht beschriebenen Funktionen folgt StorageGRID den "NetApp Richtlinie zur Reaktion auf und Benachrichtigung bei Produktsicherheitsschwachstellen". Gemeldete Schwachstellen werden überprüft und entsprechend dem Reaktionsprozess für Produktsicherheitsvorfälle reagiert.

NetApp StorageGRID bietet erweiterte Sicherheitsfunktionen für äußerst anspruchsvolle Enterprise-Objekt-Storage-Anwendungsfälle.

Wo Sie weitere Informationen finden

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

- NetApp StorageGRID: Bewertung DER Compliance-Anforderungen gemäß SEC 17a-4(f), FINRA 4511(c) und CFTC 1.31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- NetApp StorageGRID NIST FIPS 140-3 Kernel Crypto-Zertifizierung https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- NetApp StorageGRID NIST SP 800-90B Entropie-Zertifizierung https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- NetApp StorageGRID Canadian Centre for Cyber Security Common Criteria Zertifizierung https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- StorageGRID -Dokumentationsseitehttps://docs.netapp.com/us-en/storagegrid/[]
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Begriffe und Akronyme

Dieser Abschnitt enthält Definitionen für die im Dokument verwendete Terminologie.

Begriff oder Akronym	Definition
S3	Simple Storage Service.
Client	Eine Applikation, die eine Schnittstelle zu StorageGRID entweder über das S3-Protokoll für den Datenzugriff oder das HTTP-Protokoll für das Management bietet.
Mandantenadministrator	Der Administrator des StorageGRID-Mandantenkontos
Mandantenbenutzer	Ein Benutzer in einem StorageGRID-Mandantenkonto
TLS	Sicherheit In Transportschicht
ILM	Information Lifecycle Management
LAN	Lokales Netzwerk
Grid-Administrator	Der Administrator des StorageGRID-Systems

Begriff oder Akronym	Definition
Raster	Dem StorageGRID-System
Eimer	Ein Container für in S3 gespeicherte Objekte
LDAP	Lightweight Directory Access Protocol
SEK.	Securities and Exchange Commission; regelt Börsenmitglieder, Makler oder Händler
FINRA	Aufsichtsbehörde für die Finanzindustrie; entspricht den Format- und Medienanforderungen der SEC Rule 17a-4(f)
CFTC	Commodities Futures Trading Commissions; regelt den Handel mit Rohstoffttermingeschäften
NIST	National Institute of Standards and Technology

Sicherheitsfunktionen für den Datenzugriff

Erfahren Sie mehr über die Sicherheitsfunktionen für den Datenzugriff in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Konfigurierbare TLS (Transport Layer Security)	TLS erstellt ein Handshake-Protokoll für die Kommunikation zwischen einem Client und einem StorageGRID-Gateway-Node, Speicher-Node oder Load Balancer-Endpunkt. StorageGRID unterstützt die folgenden Verschlüsselungssuites für TLS: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 TLS v1.2 und 1.3 unterstützt. SSLv3, TLS v1.1 und früher werden nicht unterstützt.	Ein Client und ein StorageGRID können sich gegenseitig identifizieren und authentifizieren und mit Vertraulichkeit und Datenintegrität kommunizieren. Stellt die Verwendung einer aktuellen TLS-Version sicher. Die Chiffren können jetzt unter den Konfigurations-/Sicherheitseinstellungen konfiguriert werden	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Konfigurierbares Serverzertifikat (Load Balancer Endpoint)	Grid-Administratoren können Load-Balancer-Endpunkte konfigurieren, um ein Serverzertifikat zu erstellen oder zu verwenden.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle (CA) signiert wurden, um Objekt-API-Vorgänge zwischen Grid und Client pro Load Balancer-Endpunkt zu authentifizieren.	—
Konfigurierbares Serverzertifikat (API-Endpunkt)	Grid-Administratoren können alle StorageGRID-API-Endpunkte zentral so konfigurieren, dass ein von der vertrauenswürdigen CA ihres Unternehmens signiertes Serverzertifikat verwendet wird.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle signiert wurden, um Objekt-API-Vorgänge zwischen einem Client und dem Grid zu authentifizieren.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Mandantenfähigkeit	StorageGRID unterstützt mehrere Mandanten pro Grid, wobei jeder Mandant einen eigenen Namespace besitzt. Ein Mandant stellt ein S3-Protokoll bereit. Standardmäßig ist der Zugriff auf Buckets/Container und Objekte auf Benutzer in dem Konto beschränkt. Mandanten können einen Benutzer (z. B. eine Unternehmensimplementierung , bei der jeder Benutzer ein eigenes Konto hat) oder mehrere Benutzer (z. B. eine Service-Provider-Implementierung, bei der jedes Konto ein Unternehmen und ein Kunde des Service-Providers ist) aufweisen. Benutzer können lokal oder föderiert sein; föderierte Benutzer werden durch Active Directory oder Lightweight Directory Access Protocol (LDAP) definiert. StorageGRID bietet ein mandantenfähiges Dashboard, in dem sich Benutzer mit ihren lokalen oder föderierten Kontoinformationen anmelden können. Benutzer können auf visualisierte Berichte zur Mandantennutzung anhand des vom Grid-Administrator zugewiesenen Kontingents zugreifen, einschließlich Nutzungsinformationen in Daten und Objekten, die von Buckets gespeichert sind. Benutzer mit Administratorrechten können Systemadministrationsaufgaben auf Mandantenebene durchführen, wie zum Beispiel Benutzer und Gruppen und Zugriffsschlüssel managen.	StorageGRID-Administratoren können Daten von mehreren Mandanten hosten, dabei den Mandantenzugriff isolieren und die Benutzeridentität festlegen, indem Benutzer mit einem externen Identitätsanbieter wie Active Directory oder LDAP verknüpft werden.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Nichtabstreitbarkeit der Zugangsdaten	Jeder S3-Vorgang wird mit einem eindeutigen Mandantenkonto, einem eindeutigen Benutzer und einem Zugriffsschlüssel identifiziert und protokolliert.	Ermöglicht Grid-Administratoren festzulegen, welche API-Aktionen von welchen Personen ausgeführt werden.	—
Anonymer Zugriff deaktiviert	Standardmäßig ist der anonyme Zugriff für S3-Konten deaktiviert. Ein Anforderer muss über gültige Zugangsdaten für einen gültigen Benutzer im Mandantenkonto verfügen, um auf Buckets, Container oder Objekte innerhalb des Kontos zugreifen zu können. Anonymer Zugriff auf S3-Buckets oder -Objekte kann mit einer expliziten IAM-Richtlinie aktiviert werden.	Ermöglicht Grid-Administratoren, den anonymen Zugriff auf Buckets/Container und Objekte zu deaktivieren oder zu steuern.	—
Compliance-WORM	Entwickelt, um die Anforderungen der SEC Rule 17a-4(f) zu erfüllen und von Cohasset validiert. Kunden können Compliance auf Bucket-Ebene aktivieren. Die Aufbewahrung kann erweitert, aber nie reduziert werden. Regeln für Information Lifecycle Management (ILM) setzen minimale Datensicherungsstufen fest.	Mandanten mit gesetzlichen Datenaufbewahrungsanforderungen ermöglichen WORM-Schutz bei gespeicherten Objekten und Objektmetadaten.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
WORM	Grid-Administratoren können den WORM für das gesamte Grid aktivieren, indem sie die Option Client-Änderung deaktivieren aktivieren, die verhindert, dass Clients Objekte oder Objektmetadaten in allen Mandantenkonten überschreiben oder löschen. S3-Mandantenadministratoren können WORM auch nach Mandant, Bucket oder Objektpräfix durch Angabe der IAM-Richtlinie aktivieren, die die benutzerdefinierte S3: PutOverwriteObject-Berechtigung für Objekt- und Metadatenüberschreibungen umfasst.	Grid-Administratoren und Mandantenadministratoren können die WORM-Sicherung von gespeicherten Objekten und Objektmetadaten steuern.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
KMS-Host-Server-Verschlüsselungsschlüsselverwaltung	Grid-Administratoren können einen oder mehrere externe KMS (Key Management Server) im Grid Manager konfigurieren, um Verschlüsselungen für StorageGRID Services und Storage Appliances bereitzustellen. Jeder KMS-Hostserver oder KMS-Hostserver-Cluster verwendet das Key Management Interoperability Protocol (KMIP), um einen Verschlüsselungsschlüssel für die Appliance-Nodes am zugehörigen StorageGRID-Standort bereitzustellen.	Die Verschlüsselung ruhender Daten wird erreicht. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS-Hostserver kommunizieren kann.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Automatisiertes Failover	StorageGRID bietet integrierte Redundanz und automatisiertes Failover. Der Zugriff auf Mandantenkonten, Buckets und Objekte kann auch bei diversen Ausfällen – von Festplatten oder Nodes bis hin zu ganzen Standorten – fortgesetzt werden. StorageGRID erkennt Ressourcen und leitet Anfragen automatisch an verfügbare Nodes und Datenspeicherorte um. StorageGRID Standorte können sogar im Inselmodus betrieben werden. Wenn ein WAN-Ausfall die Verbindung eines Standorts zum restlichen System trennt, können Lese- und Schreibvorgänge mit den lokalen Ressourcen fortgesetzt werden, und die Replizierung wird automatisch wieder aufgenommen, sobald das WAN wiederhergestellt ist.	Ermöglicht Grid-Administratoren, Uptime, SLA und andere vertragliche Verpflichtungen zu erfüllen und Business-Continuity-Pläne zu implementieren.	—
S3-spezifische Datenzugriffssicherheitsfunktionen	AWS Signature Version 2 und Version 4	Das Signieren von API-Anforderungen bietet eine Authentifizierung für S3-API-Vorgänge. Amazon unterstützt zwei Versionen von Signature Version 2 und Version 4. Beim Signaturprozess wird die Identität des Anforderers überprüft, die Daten während der Übertragung geschützt und vor potenziellen Replay-Angriffen geschützt.	Entspricht der AWS-Empfehlung für Signature Version 4 und ermöglicht Abwärtskompatibilität mit älteren Anwendungen mit Signature Version 2.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	S3-Objektsperre	Die S3-Objektsperrfunktion in StorageGRID ist eine Objektschutzlösung, die S3-Objektsperrung in Amazon S3 entspricht.	Ermöglicht Mandanten, Buckets mit aktivierter S3 Object Lock zu erstellen, um Vorschriften zu erfüllen, für die bestimmte Objekte für einen festgelegten Zeitraum oder auf unbestimmte Zeit aufbewahrt werden müssen.
SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)	Sichere Speicherung der S3 Zugangsdaten	S3-Zugriffsschlüssel werden in einem Format gespeichert, das durch eine Passwort-Hashing-Funktion (SHA-2) geschützt ist.	Ermöglicht die sichere Speicherung von Zugriffsschlüsseln durch eine Kombination aus Schlüssellänge (10^{31} zufällig generierte Nummer) und einem Passwort-Hashing-Algorithmus.
—	Zeitgebundene S3-Zugriffsschlüssel	Beim Erstellen eines S3 Zugriffsschlüssels für einen Benutzer können Kunden ein Ablaufdatum und eine Uhrzeit für den Zugriffsschlüssel festlegen.	Bietet Grid-Administratoren die Möglichkeit, temporäre S3-Zugriffsschlüssel bereitzustellen.
—	Mehrere Zugriffsschlüssel pro Benutzerkonto	Mit StorageGRID können mehrere Zugriffsschlüssel erstellt und gleichzeitig für ein Benutzerkonto aktiv werden. Da jede API-Aktion mit einem Mandanten-Benutzerkonto und einem Zugriffsschlüssel protokolliert wird, bleibt die Nichtabstreitbarkeit erhalten, obwohl mehrere Schlüssel aktiv sind.	Ermöglicht Clients das unterbrechungsfreie Drehen von Zugriffsschlüsseln und ermöglicht jedem Client einen eigenen Schlüssel, wodurch die gemeinsame Nutzung von Schlüsseln über Clients hinweg vermieden wird.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	S3 IAM-Zugriffsrichtlinie	StorageGRID unterstützt S3 IAM-Richtlinien, sodass Grid-Administratoren granulare Zugriffssteuerung nach Mandanten, Bucket oder Objektpräfix angeben können. StorageGRID unterstützt außerdem IAM-Richtlinienbedingungen und -Variablen, wodurch dynamischere Zugriffssteuerungsrichtlinien ermöglicht werden.	Ermöglicht Grid-Administratoren, die Zugriffssteuerung nach Benutzergruppen für den gesamten Mandanten festzulegen; ermöglicht es den Mandantenbenutzern auch, die Zugriffssteuerung für ihre eigenen Buckets und Objekte festzulegen.
—	S3 Security Token Service API AssumeRole	StorageGRID unterstützt die S3 STS API AssumeRole, um temporäre Sicherheitsanmeldeinformationen (Zugriffsschlüssel-ID, geheimer Zugriffsschlüssel, Sitzungstoken) mit eingeschränkten Berechtigungen und begrenzter Dauer bereitzustellen. Inline-Sitzungsrichtlinien zur weiteren Einschränkung von Berechtigungen während der Sitzung werden als Teil der AssumeRole-API unterstützt.	Ermöglicht Mandantenadministratoren, sicheren temporären Zugriff auf Objektdaten bereitzustellen.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	Einfacher Benachrichtigungsdienst	StorageGRID unterstützt das Senden von Benachrichtigungen beim Objektzugriff. Die folgenden Ereignistypen werden unterstützt: • s3:Objekt erstellt: • s3:ObjektErstellt:Put • s3:ObjektErstellt:Post • s3:ObjektErstellt:Kopie • s3:Objekterstellt:MehrteiligerUpload abgeschlossen • s3:Objekt entfernt: • s3:Objekt entfernt:Löschen • s3:Objekt entfernt:DeleteMarker erstellt • s3:ObjectRestore:Post	Ermöglicht Mandantenadministratoren die Überwachung des Zugriffs auf Objekte
—	Serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln (SSE)	StorageGRID unterstützt SSE und ermöglicht mandantenfähigen Schutz von Daten im Ruhezustand mit von StorageGRID gemanagten Verschlüsselungen.	Ermöglicht Mandanten die Verschlüsselung von Objekten. Zum Schreiben und Abrufen dieser Objekte ist ein Verschlüsselungsschlüssel erforderlich.
SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)	Serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)	StorageGRID unterstützt SSE-C und ermöglicht damit mandantenfähigen Schutz von Daten im Ruhezustand mit vom Client gemanagten Verschlüsselungsschlüsseln. Obwohl StorageGRID alle Objektverschlüsselung und -Entschlüsselung managt, muss der Client bei SSE-C die Schlüssel selbst managen.	Ermöglicht Clients die Verschlüsselung von Objekten mit den Schlüsseln, die sie steuern. Zum Schreiben und Abrufen dieser Objekte ist ein Verschlüsselungsschlüssel erforderlich.

Sicherheit von Objekten und Metadaten

Entdecken Sie die Sicherheitsfunktionen für Objekte und Metadaten in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Advanced Encryption Standard (AES) Server-seitige Objektverschlüsselung	StorageGRID bietet serverseitige Objektverschlüsselung nach AES 128 und AES 256. Grid-Administratoren können die Verschlüsselung als globale Standardeinstellung aktivieren. StorageGRID unterstützt außerdem den S3 x-amz-Server-seitigen Verschlüsselungsheader, um die Verschlüsselung für einzelne Objekte zu aktivieren oder zu deaktivieren. Wenn diese Option aktiviert ist, werden die Objekte bei der Speicherung bzw. Übertragung zwischen den Grid-Nodes verschlüsselt.	Unterstützt die sichere Speicherung und Übertragung von Objekten, unabhängig von der zugrunde liegenden Storage-Hardware.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Integriertes Verschlüsselungsmanagement	Bei aktivierter Verschlüsselung wird jedes Objekt mit einem zufällig generierten eindeutigen symmetrischen Schlüssel verschlüsselt, der ohne externen Zugriff in StorageGRID gespeichert wird.	Ermöglicht die Verschlüsselung von Objekten ohne externes Verschlüsselungsmanagement	
FIPS 140-2-2-konforme Verschlüsselungsfestplatten (Federal Information Processing Standard	Die StorageGRID Appliances SG5812, SG5860, SG6160 und SGF6024 bieten die Möglichkeit, FIPS 140-2-2-konforme Verschlüsselungsfestplatten anzubieten. Die Schlüssel für die Festplatten können optional von einem externen KMIP-Server gemanagt werden.	Ermöglicht sichere Speicherung von Systemdaten, Metadaten und Objekten StorageGRID bietet außerdem softwarebasierte Objektverschlüsselung, die die Storage und die Übertragung von Objekten sichert.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Federal Information Processing Standard (FIPS) 140-3-konforme Verschlüsselung für Knoten	Die StorageGRID -Geräte SG5812, SG5860, SG6160, SGF6112, SG1100 und SG110 bieten die Option einer FIPS 140-3-konformen Knotenverschlüsselung. Die Verschlüsselungsschlüssel für die Knoten werden von einem externen KMIP-Server verwaltet.	Ermöglicht sichere Speicherung von Systemdaten, Metadaten und Objekten StorageGRID bietet außerdem softwarebasierte Objektverschlüsselung, die die Storage und die Übertragung von Objekten sichert.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Hintergrundintegrität sprüfung und Selbstheilung	StorageGRID nutzt einen Verriegelungsmechanismus aus Hashes, Prüfsummen und zyklischen Redundanzprüfungen (Cyclic Redundancy Checks, CRCs) auf Objekt- und Unterobjektebene, um sich sowohl im Storage- als auch auf der Übertragungsstrecke vor Dateninkonsistenz, Manipulation oder Änderung zu schützen. StorageGRID erkennt beschädigte und manipulierte Objekte automatisch und ersetzt sie. Gleichzeitig werden die geänderten Daten in Quarantäne verschoben und der Administrator benachrichtigt.	Grid-Administratoren können SLAs, Vorschriften und andere Verpflichtungen hinsichtlich der Datenaufbewahrung erfüllen. Unterstützt Kunden dabei, Ransomware oder Viren zu erkennen, die versuchen, Daten zu verschlüsseln, zu manipulieren oder zu ändern.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Richtlinienbasierte Objektplatzierung und -Aufbewahrung	Mit StorageGRID können Grid-Administratoren ILM-Regeln konfigurieren, die die Objektaufbewahrung, -Platzierung, -Sicherung, -Übertragung und -Verfallsdaten festlegen. Grid-Administratoren können StorageGRID konfigurieren, um Objekte nach Metadaten zu filtern und Regeln auf verschiedenen Granularitätsebenen anzuwenden, einschließlich Grid-weiter, Mandant, Bucket, Schlüsselpräfix, und benutzerdefinierte Metadaten-Schlüssel-Wert-Paare. StorageGRID hilft sicherzustellen, dass Objekte während ihrer gesamten Lebenszyklen gemäß den ILM-Regeln gespeichert werden, es sei denn, sie werden vom Client ausdrücklich gelöscht.	Hilft bei der Durchsetzung von Datenablage, Datensicherheit und Datenhaltung. Unterstützt Kunden bei der Einhaltung von SLAs für Langlebigkeit, Verfügbarkeit und Performance.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Metadaten werden im Hintergrund gescannt	StorageGRID scannt regelmäßig Objektmetadaten im Hintergrund, um Änderungen an der Platzierung oder Sicherung von Objektdaten gemäß ILM anzuwenden.	Hilft bei der Erkennung beschädigter Objekte.	
Abstimmbare Konsistenz	Mandanten können Konsistenzstufen auf Bucket-Ebene auswählen, um sicherzustellen, dass Ressourcen wie standortübergreifende Konnektivität verfügbar sind.	Bietet die Möglichkeit, Schreibvorgänge nur dann in das Grid zu übertragen, wenn eine erforderliche Anzahl von Standorten oder Ressourcen verfügbar ist.	

Sicherheitsfunktionen für die Administration

Entdecken Sie die Sicherheitsfunktionen für die Administration in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Serverzertifikat (Grid-Managementoberfläche)	Grid-Administratoren können die Grid-Managementoberfläche so konfigurieren, dass ein von der vertrauenswürdigen CA ihres Unternehmens signiertes Serverzertifikat verwendet wird.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle signiert sind, um die Management-UI und den API-Zugriff zwischen einem Management-Client und dem Grid zu authentifizieren.	—
Administrative Benutzerauthentifizierung	Administratorbenutzer werden mit Benutzername und Passwort authentifiziert. Administrative Benutzer und Gruppen können lokal oder föderiert sein und aus dem Active Directory oder LDAP des Kunden importiert werden. Lokale Kontokennwörter werden in einem durch bcrypt geschützten Format gespeichert; Kommandozeilen-Passwörter werden in einem durch SHA-2 geschützten Format gespeichert.	Authentifiziert den administrativen Zugriff auf die Management-UI und -APIs.	—
SAML Support	StorageGRID unterstützt Single Sign-On (SSO) unter Verwendung des SAML 2.0-Standards (Security Assertion Markup Language 2.0). Wenn SSO aktiviert ist, müssen alle Benutzer von einem externen Identitäts-Provider authentifiziert werden, bevor sie auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.	Zusätzliche Sicherheitsstufen für Grid- und Mandantenadministratoren wie SSO und Multi-Faktor-Authentifizierung (MFA)	NIST SP800-63

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Granulare Berechtigungskontrolle	Grid-Administratoren können Rollen Berechtigungen zuweisen und administrativen Benutzergruppen Rollen zuweisen. Dadurch werden die Aufgaben erzwungen, die administrative Clients sowohl über die Management-UI als auch über APIs ausführen dürfen.	Ermöglicht Grid-Administratoren das Management der Zugriffssteuerung für Admin-Benutzer und -Gruppen.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Verteilte Audit-Protokollierung	StorageGRID bietet eine integrierte, verteilte Audit-Protokollierungs-Infrastruktur, die auf Hunderte Nodes an bis zu 16 Standorten skalierbar ist. Die StorageGRID-Software-Knoten erzeugen Audit-Meldungen, die über ein redundantes Audit-Relay-System übertragen und schließlich in einem oder mehreren Audit-Log-Repositorys erfasst werden. Audit-Meldungen erfassen Ereignisse auf Objektebene, z. B. Client-initiierte S3-API-Operationen, Objekt-Lebenszyklus-Ereignisse durch ILM, Zustandsprüfungen von Objekten im Hintergrund sowie Konfigurationsänderungen, die über die Management-UI oder -APIs vorgenommen werden. Prüfprotokolle können per Syslog exportiert werden, sodass Prüfmeldungen von Tools wie Splunk und ELK ausgewertet werden können. Es gibt vier Arten von Prüfmeldungen: • Systemaudits Meldungen • Audit-Meldungen zu Objekt-Storage • HTTP-Protokollauditmeldungen • Meldungen von Management-Audits Prüfprotokolle können zur langfristigen Aufbewahrung und für den Anwendungszugriff in einem S3-Bucket gespeichert werden.	Bietet Grid-Administratoren einen bewährten und skalierbaren Audit-Service und ermöglicht es ihnen, Audit-Daten für verschiedene Ziele zu extrahieren. Zu diesen Zielen gehören Fehlerbehebung, Revision der SLA-Performance, Client-Datenzugriffs-API-Operationen und Änderungen der Managementkonfiguration.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Systemprüfung	Systemauditmeldungen erfassen systembezogene Ereignisse, wie Grid-Node-Status, Erkennung beschädigter Objekte, Objekte, die per ILM-Regel an allen angegebenen Standorten festgelegt wurden, und den Fortschritt systemweiter Wartungsaufgaben (Grid-Aufgaben).	Unterstützt Kunden bei der Behebung von Systemproblemen und liefert den Nachweis, dass Objekte gemäß SLA gespeichert werden. SLAs werden durch StorageGRID ILM-Regeln implementiert und sind integritätsgeschützt.	—
Objekt-Storage-Prüfung	Objekt-Storage-Audit-Nachrichten erfassen Objekt-API-Transaktionen und Lifecycle-bezogene Ereignisse. Zu diesen Ereignissen gehören Objekt-Storage und -Abruf, Grid-Node zu Grid-Node-Transfers und Überprüfungen.	Unterstützt Kunden bei der Prüfung des Fortschritts der Daten über das System und bei der Bereitstellung von SLAs mit dem Namen StorageGRID ILM.	—
HTTP-Protokollaudit	HTTP-Protokollauditmeldungen erfassen HTTP-Protokollinteraktionen im Zusammenhang mit Client-Anwendungen und StorageGRID-Knoten. Darüber hinaus können Kunden bestimmte HTTP-Anforderungsheader (z. B. X-Forwarded-for und Benutzer-Metadaten [x-amz-meta-*]) in einem Audit erfassen.	Unterstützt Kunden beim Prüfen von API-Operationen für den Datenzugriff zwischen Clients und StorageGRID und bei der Nachverfolgung einer Aktion auf ein einzelnes Benutzerkonto und einen Zugriffsschlüssel. Kunden können zudem Benutzermetadaten bei einem Audit protokollieren und mithilfe von Tools für das Mining wie Splunk oder ELK nach Objekt-Metadaten suchen.	—
Management-Prüfung	Management Audit-Nachrichten protokollieren Benutzeranforderungen von Administratoren an die Management-UI (Grid Management Interface) oder APIs. Jede Anfrage, die keine GET- oder HEAD-Anforderung an die API ist, protokolliert eine Antwort mit dem Benutzernamen, der IP und der Art der Anfrage an die API.	Hilft Grid-Administratoren, eine Aufzeichnung der Änderungen an der Systemkonfiguration zu erstellen, die von welchem Benutzer von welcher Quell-IP und welcher Ziel-IP zu welchem Zeitpunkt vorgenommen wurden.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
TLS 1.3-Unterstützung für Management UI- und API-Zugriff	TLS erstellt ein Handshake-Protokoll für die Kommunikation zwischen einem Admin-Client und einem StorageGRID-Admin-Node.	Ein administrativer Client und ein StorageGRID können sich gegenseitig identifizieren und authentifizieren und kommunizieren mit Vertraulichkeit und Datenintegrität.	—
SNMPv3 für StorageGRID-Überwachung	SNMPv3 bietet Sicherheit durch eine starke Authentifizierung und Datenverschlüsselung zum Schutz der Privatsphäre. Mit v3 werden die Protokolldateneinheiten verschlüsselt, wobei CBC-DES für das Verschlüsselungsprotokoll verwendet wird. Die Benutzerauthentifizierung, wer die Protokolldateneinheit gesendet hat, wird entweder über das HMAC-SHA- oder das HMAC-MD5-Authentifizierungsprotokoll bereitgestellt. SNMPv2 und v1 werden weiterhin unterstützt.	Unterstützt Grid-Administratoren bei der Überwachung des StorageGRID-Systems durch Aktivieren eines SNMP-Agenten auf dem Admin-Knoten.	—
Client-Zertifikate für Prometheus Kennzahlenexport	Grid-Administratoren können Client-Zertifikate hochladen oder generieren, die für einen sicheren, authentifizierten Zugriff auf die StorageGRID Prometheus-Datenbank verwendet werden können.	Grid-Administratoren können StorageGRID mithilfe von Client-Zertifikaten extern mit Applikationen wie Grafana überwachen.	—

Plattformsicherheitsfunktionen

Erfahren Sie mehr über die Plattformsicherheitsfunktionen in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Interne Public-Key-Infrastruktur (PKI), Node-Zertifikate und TLS	StorageGRID verwendet interne PKI- und Node-Zertifikate zur Authentifizierung und Verschlüsselung der Kommunikation zwischen den Knoten. Die Kommunikation zwischen den Knoten ist durch TLS gesichert.	Unterstützt den sicheren Systemdatenverkehr über LAN oder WAN, insbesondere bei standortübergreifenden Bereitstellungen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Knoten-Firewall	StorageGRID konfiguriert automatisch IP-Tabellen und Firewallregeln zur Steuerung von eingehendem und ausgehendem Netzwerk-Traffic sowie zum Schließen nicht verwendeter Ports.	Der Schutz von StorageGRID-Systemen, Daten und Metadaten vor unaufgefordertem Netzwerkverkehr	—
OS-Sicherung	Das Basis-Betriebssystem der physischen Appliances und virtuellen Nodes von StorageGRID ist gehärtet; zugehörige Softwarepakete werden entfernt.	Minimiert mögliche Angriffsflächen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Regelmäßige Plattform- und Software-Updates	StorageGRID veröffentlicht regelmäßige Software-Versionen, die das Betriebssystem, Binärdateien von Applikationen und Software Updates enthalten.	Hilft dabei, das StorageGRID System mit aktueller Software und Binärdateien zu aktualisieren.	—
Root-Anmeldung über Secure Shell (SSH) deaktiviert	Die Root-Anmeldung über SSH ist auf allen StorageGRID Nodes deaktiviert. SSH-Zugriff verwendet Zertifikatauthentifizierung.	Hilft Kunden, sich vor einem möglichen Remote-Passwort-Cracking der Root-Anmeldung zu schützen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Automatisierte Zeitsynchronisierung	StorageGRID synchronisiert Systemuhren jedes Node automatisch mit mehreren externen NTP-Servern (Time Network Time Protocol). Mindestens vier NTP-Server von Stratum 3 oder höher sind erforderlich.	Stellt die gleiche Zeitreferenz für alle Knoten sicher.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Getrennte Netzwerke für Client-, Admin- und internen Grid-Traffic	StorageGRID Software Nodes und Hardware Appliances unterstützen mehrere virtuelle und physische Netzwerkschnittstellen, sodass die Kunden den Client-, Administrations- und internen Grid-Traffic über verschiedene Netzwerke trennen können.	Grid-Administratoren können internen und externen Netzwerkverkehr trennen und Datenverkehr über Netzwerke mit unterschiedlichen SLAs bereitstellen.	—
Mehrere virtuelle LAN-Schnittstellen (VLAN)	StorageGRID unterstützt die Konfiguration von VLAN-Schnittstellen auf Ihren StorageGRID-Client- und Grid-Netzwerken.	Grid-Administratoren können den Datenverkehr von Applikationen partitionieren und isolieren, um so Sicherheit, Flexibilität und Performance zu gewährleisten.	
Nicht Vertrauenswürdiges Client-Netzwerk	Die nicht vertrauenswürdige Client-Netzwerkschnittstelle akzeptiert eingehende Verbindungen nur an Ports, die explizit als Load-Balancer-Endpunkte konfiguriert wurden.	Stellt sicher, dass Schnittstellen geschützt sind, die nicht vertrauenswürdigen Netzwerken zugänglich sind.	—
Konfigurierbare Firewall	Verwaltung offener und geschlossener Ports für Admin-, Grid- und Client-Netzwerke.	Ermöglichen Sie Grid-Administratoren, den Zugriff auf Ports zu steuern und den genehmigten Gerätezugriff auf die Ports zu verwalten.	
Erweitertes SSH-Verhalten	Deaktivieren Sie SSH standardmäßig vor der Installation. Im Standardzustand ist der SSH-Zugriff nur auf die Adresse der Link-Local-Verwaltungsports aktiviert. Die Passwörter für die Benutzer „Admin“ und „Root“ sind auf die Seriennummer des Compute Controllers des Geräts eingestellt. Die Anmeldung ist nur auf der seriellen Konsole und der grafischen Konsole (BMC KVM) zulässig. SSH ist auf allen Netzwerkports deaktiviert.	Verbessert den Netzwerkzugriffsschutz.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Node-Verschlüsselung	Als Teil der neuen KMS-Host-Server-Verschlüsselungsfunktion wird dem StorageGRID-Appliance-Installationsprogramm eine neue Einstellung für die Knotenverschlüsselung hinzugefügt.	Diese Einstellung muss während der Hardwarekonfigurationsphase der Appliance-Installation aktiviert werden.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Cloud-Integration

Integration von StorageGRID in Cloud-Services

Funktion	Funktion	Auswirkungen
Benachrichtigungs-basierte Virus-Scan	Die StorageGRID Plattform-Services unterstützen Ereignisbenachrichtigungen. Ereignisbenachrichtigungen können mit externen Cloud Computing Services verwendet werden, um Workflows zur Virenprüfung der Daten zu starten.	Mandantenadministratoren können einen Virus-Scan von Daten mithilfe von externen Cloud-Computing-Services auslösen.

TR-4921: Ransomware-Verteidigung

StorageGRID S3 Objekte vor Ransomware schützen

Informieren Sie sich über Ransomware-Angriffe und den Schutz von Daten mit StorageGRID Sicherheits-Best Practices.

Ransomware-Angriffe sind auf dem Vormarsch. Dieses Dokument enthält einige Empfehlungen zum Schutz Ihrer Objektdaten auf StorageGRID.

Ransomware heute ist die allgegenwärtige Gefahr im Datacenter. Ransomware wurde entwickelt, um Daten zu verschlüsseln und sie für Benutzer und Applikationen, die darauf angewiesen sind, nicht nutzbar zu machen. Der Schutz beginnt mit den üblichen Schutzmaßnahmen für gehärtete Netzwerke und solide Benutzersicherheitspraktiken, und wir müssen die Sicherheitsverfahren für den Datenzugriff befolgen.

Ransomware ist eine der größten Sicherheitsbedrohungen von heute. Das NetApp StorageGRID Team arbeitet mit unseren Kunden zusammen, um diesen Bedrohungen einen Schritt voraus zu sein. Mit der Verwendung von Objektsperre und Versionierung können Sie sich vor unerwünschten Änderungen schützen und sich vor böswilligen Angriffen erholen. Datensicherheit ist ein Multi-Layer-Unternehmen, dessen Objekt-Storage nur ein Teil in Ihrem Datacenter ist.

Best Practices von StorageGRID

Für StorageGRID sollten Sicherheits-Best-Practices die Verwendung von HTTPS mit signierten Zertifikaten für Management und Objektzugriff umfassen. Erstellen Sie dedizierte Benutzerkonten für Anwendungen und Personen und verwenden Sie die Mandanten-Root-Konten nicht für den Zugriff auf Anwendungen oder Benutzerdaten. Mit anderen Worten, folgen Sie dem Prinzip der geringsten Privilegien. Verwenden Sie Sicherheitsgruppen mit definierten IAM-Richtlinien (Identity and Access Management) zur Steuerung von Benutzerrechten und Zugriffskonten für spezifische Anwendungen und Benutzer. Mit diesen Maßnahmen müssen Sie dennoch sicherstellen, dass Ihre Daten geschützt sind. Bei Simple Storage Service (S3) wird bei Änderungen von Objekten zur Verschlüsselung das ursprüngliche Objekt überschrieben.

Verteidigungsmethoden

Der primäre Mechanismus zum Schutz vor Ransomware in der S3-API ist die Implementierung von Objektsperrung. Nicht alle Anwendungen sind mit Objektsperre kompatibel, daher gibt es zwei weitere Optionen zum Schutz Ihrer Objekte, die in diesem Bericht beschrieben werden: Replikation in einen anderen Bucket mit aktivierter Versionierung und Versionierung mit IAM-Richtlinien.

Wo Sie weitere Informationen finden

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

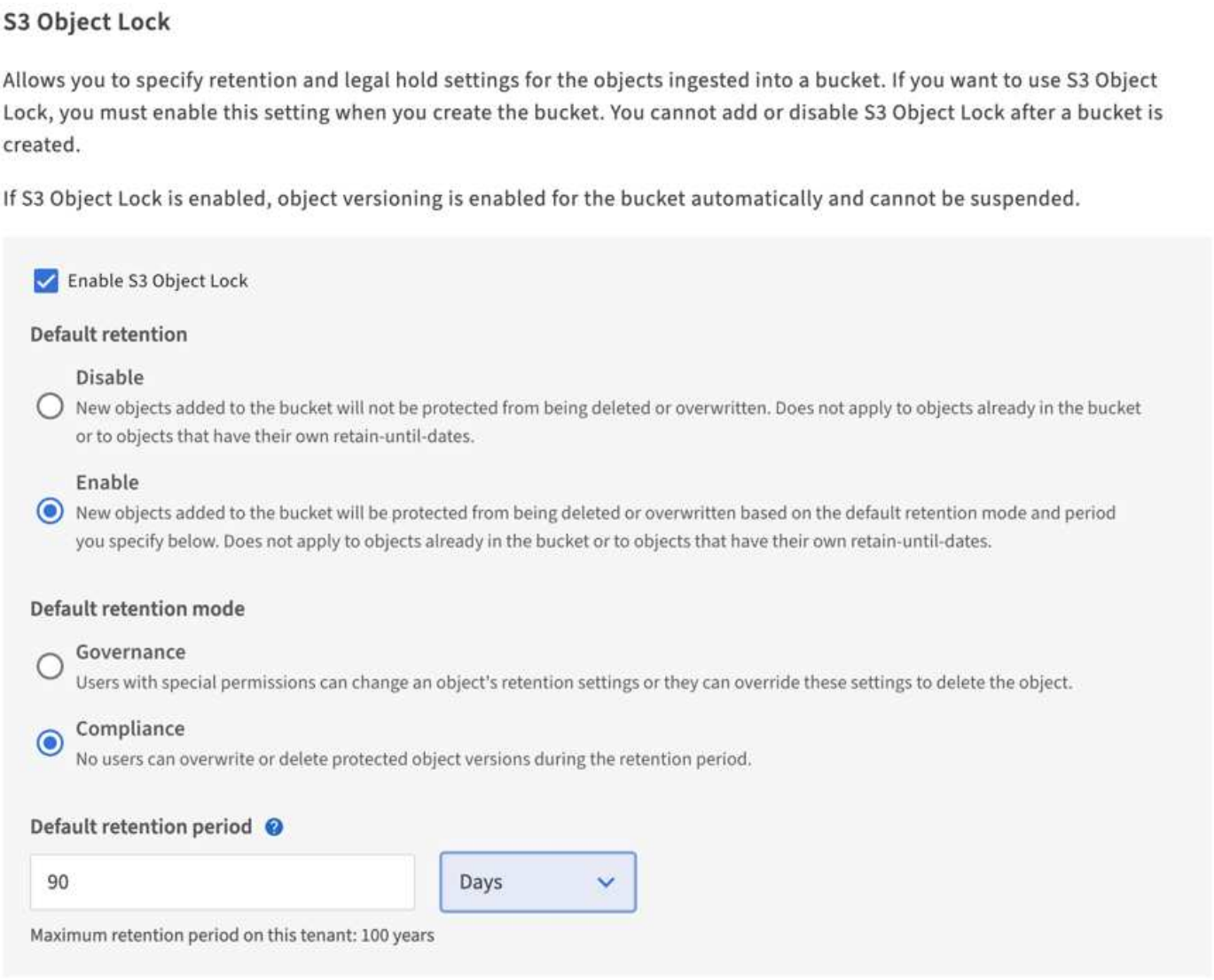
- NetApp StorageGRID Dokumentationscenterhttps://docs.netapp.com/us-en/storagegrid/[]
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Ransomware-Verteidigung mit Objektsperre

Entdecken Sie, wie die Objektsperre in StorageGRID ein WORM-Modell bietet, das das Löschen oder Überschreiben von Daten verhindert, und wie es die gesetzlichen Vorgaben erfüllt.

Die Objektsperrung verfügt über ein WORM-Modell, mit dem verhindert wird, dass Objekte gelöscht oder überschrieben werden. Die StorageGRID-Implementierung von Objektsperrung "Cohasset bewertet" unterstützt die Einhaltung gesetzlicher Vorgaben; sie unterstützt die gesetzliche Aufbewahrungspflichten, den Compliance-Modus und den Governance-Modus für die Objektaufbewahrung sowie die standardmäßigen Bucket-Aufbewahrungsrichtlinien. Sie müssen die Objektsperre als Teil der Bucket-Erstellung und -Versionierung aktivieren. Eine bestimmte Version eines Objekts ist gesperrt, und wenn keine Versions-ID definiert ist, wird die Aufbewahrung auf die aktuelle Version des Objekts platziert. Wenn für die aktuelle Version die Aufbewahrung konfiguriert ist und versucht wird, das Objekt zu löschen, zu ändern oder zu überschreiben, wird eine neue Version mit einer Löschmarkierung oder der neuen Revision des Objekts als aktuelle Version erstellt. und die gesperrte Version wird als nicht aktuelle Version beibehalten. Für Applikationen, die noch nicht kompatibel sind, können Sie möglicherweise noch Objektsperre und eine Standardkonfiguration für die Aufbewahrung auf dem Bucket nutzen. Nach der Definition der Konfiguration wird dabei eine Objektaufbewahrung auf jedes neue Objekt angewendet, das in den Bucket aufgenommen wird. Dies funktioniert, solange die Anwendung so konfiguriert ist, dass die Objekte nicht vor Ablauf der Aufbewahrungszeit gelöscht oder überschrieben werden.

Wenn Sie in der Benutzeroberfläche der Mandantenverwaltung einen Bucket erstellen, können Sie die Objektsperre aktivieren und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer konfigurieren. Wenn dies konfiguriert ist, wird für jedes Objekt, das in diesen Bucket aufgenommen wird, eine Mindestaufbewahrungsdauer für die Objektsperre festgelegt.



Hier sind einige Beispiele für die Verwendung der Objektsperre API:

Objektsperre Legal Hold ist ein einfacher ein/aus-Status, der auf ein Objekt angewendet wird.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

Wenn Sie den Legal Hold-Status festlegen, wird bei Erfolg kein Wert zurückgegeben, sodass er mit einer GET-Operation überprüft werden kann.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

Um die Legal Hold-Taste zu deaktivieren, wenden Sie den AUS-Status an.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Die Objektaufbewahrung wird mit einem Zeitstempel bis beibehalten.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

Auch hier gibt es keinen zurückgegebenen Wert auf Erfolg, so dass Sie den Status der Aufbewahrung ähnlich mit einem get Call überprüfen können.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

Wenn für einen Bucket mit aktivierter Objektsperre eine Standardaufbewahrung eingerichtet wird, wird eine Aufbewahrungsfrist in Tagen und Jahren verwendet.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

Wie bei den meisten dieser Operationen wird bei Erfolg keine Antwort zurückgegeben. Daher können wir ein GET durchführen, damit die Konfiguration überprüft werden kann.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

Als Nächstes können Sie ein Objekt mit der angewandten Aufbewahrungskonfiguration in den Bucket legen.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

Der PUT-Vorgang gibt eine Antwort zurück.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

Für das Aufbewahrungs-Objekt wird die Aufbewahrungsdauer, die im vorhergehenden Beispiel auf dem Bucket festgelegt wurde, in einen Aufbewahrungszeitstempel für das Objekt konvertiert.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Ransomware-Verteidigung durch replizierten Bucket mit Versionierung

Erfahren Sie, wie Sie Objekte mit StorageGRID CloudMirror in einen sekundären Bucket replizieren.

Nicht alle Applikationen und Workloads werden mit Objektsperre kompatibel sein. Eine weitere Option besteht darin, die Objekte auf einen sekundären Bucket zu replizieren, entweder im selben Grid (vorzugsweise ein anderer Mandant mit eingeschränktem Zugriff) oder auf einen anderen S3-Endpunkt mit dem StorageGRID-Plattformservice CloudMirror.

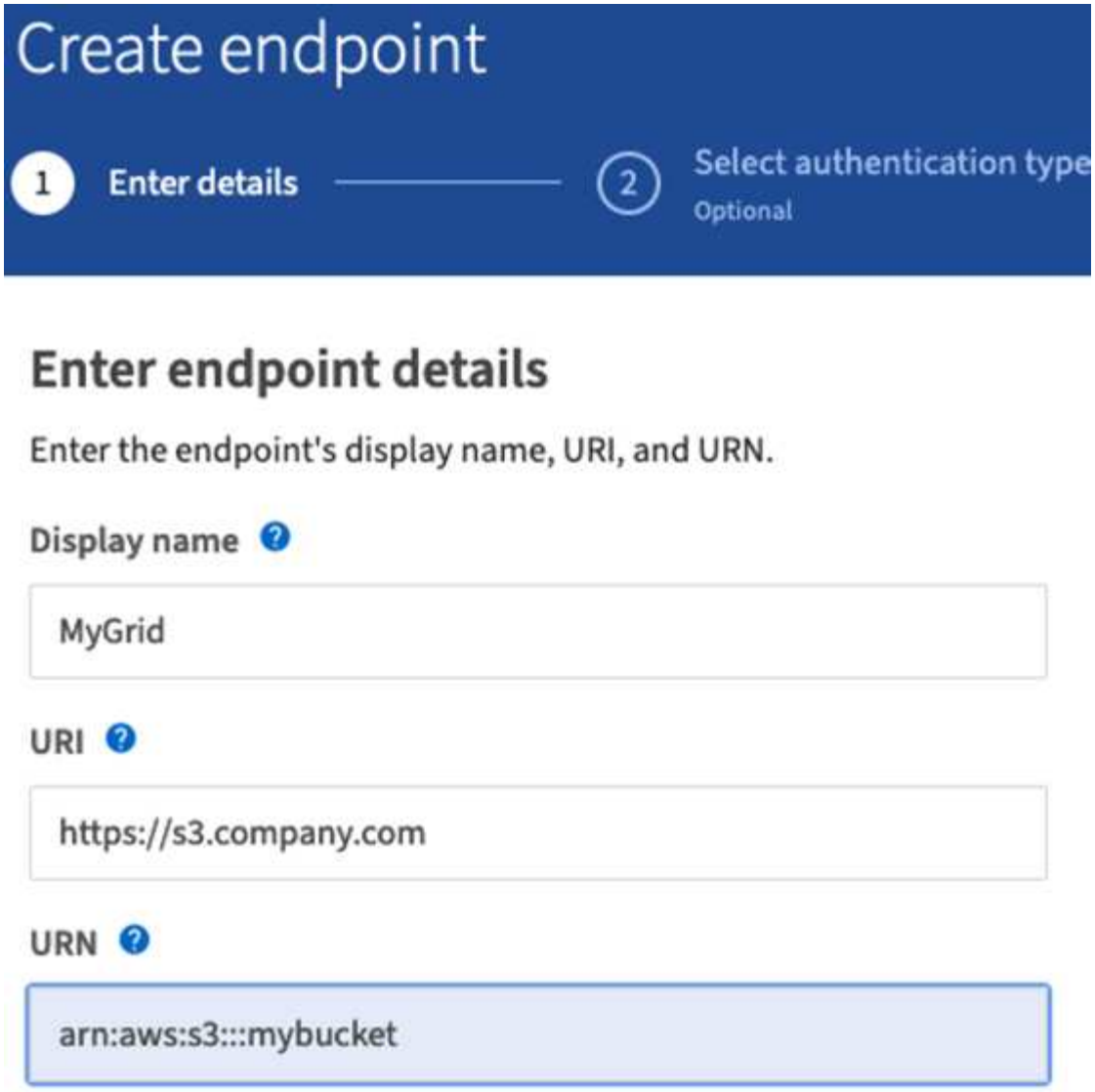
StorageGRID CloudMirror ist eine Komponente von StorageGRID, die so konfiguriert werden kann, dass Objekte eines Buckets auf ein definiertes Ziel repliziert werden, da sie in den Quell-Bucket aufgenommen werden und Löschungen nicht repliziert werden. Da CloudMirror eine integrierte Komponente von StorageGRID ist, kann sie nicht durch einen S3-API-basierten Angriff deaktiviert oder manipuliert werden. Sie können diesen replizierten Bucket mit aktivierter Versionierung konfigurieren. In diesem Szenario benötigen Sie eine automatisierte Bereinigung der alten Versionen des replizierten Buckets, die sicher zu verwerfen sind. Dazu können Sie die StorageGRID ILM-Richtlinien-Engine verwenden. Erstellen Sie Regeln, um die Objektplatzierung auf Basis der nicht aktuellen Zeit für mehrere Tage zu verwalten, die ausreichend sind, um einen Angriff identifiziert und wiederhergestellt zu haben.

Ein Nachteil dieses Ansatzes besteht darin, dass mehr Storage verbraucht wird. Dazu ist eine vollständige zweite Kopie des Buckets und mehrere Versionen der Objekte verfügbar, die einige Zeit aufbewahrt werden. Darüber hinaus müssen die Objekte, die absichtlich aus dem primären Bucket gelöscht wurden, manuell aus dem replizierten Bucket entfernt werden. Außerhalb des Produkts gibt es weitere Replizierungsoptionen, wie z. B. NetApp CloudSync, mit denen Löschvorgänge für eine ähnliche Lösung repliziert werden können. Ein weiterer Nachteil für den sekundären Bucket, bei dem die Versionierung aktiviert und nicht die Objektsperre aktiviert ist, besteht darin, dass eine Reihe privilegierter Konten vorhanden ist, die verwendet werden könnten, um Schäden am sekundären Standort zu verursachen. Der Vorteil ist, dass es sich um ein eindeutiges Konto für diesen Endpunkt oder Mandanten-Bucket handeln sollte, und der Kompromiss wahrscheinlich keinen Zugriff auf Konten am primären Standort oder umgekehrt umfasst.

Nachdem die Quell- und Ziel-Buckets erstellt und das Ziel mit Versionierung konfiguriert wurde, können Sie die Replikation wie folgt konfigurieren und aktivieren:

Schritte

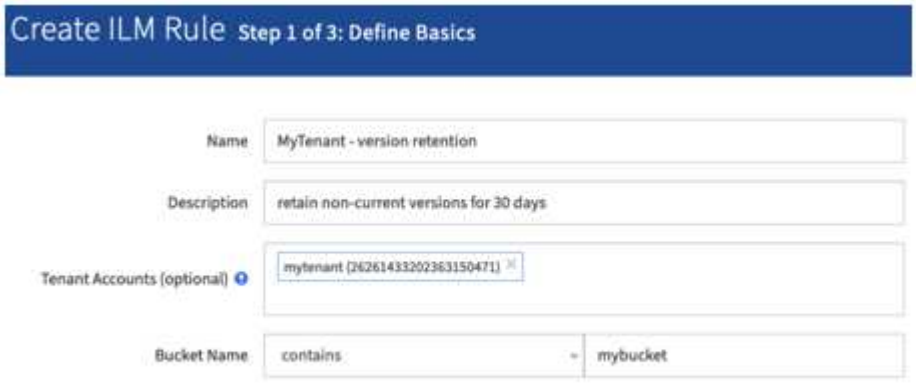
1. Erstellen Sie zum Konfigurieren von CloudMirror einen Plattformservices-Endpunkt für das S3-Ziel.

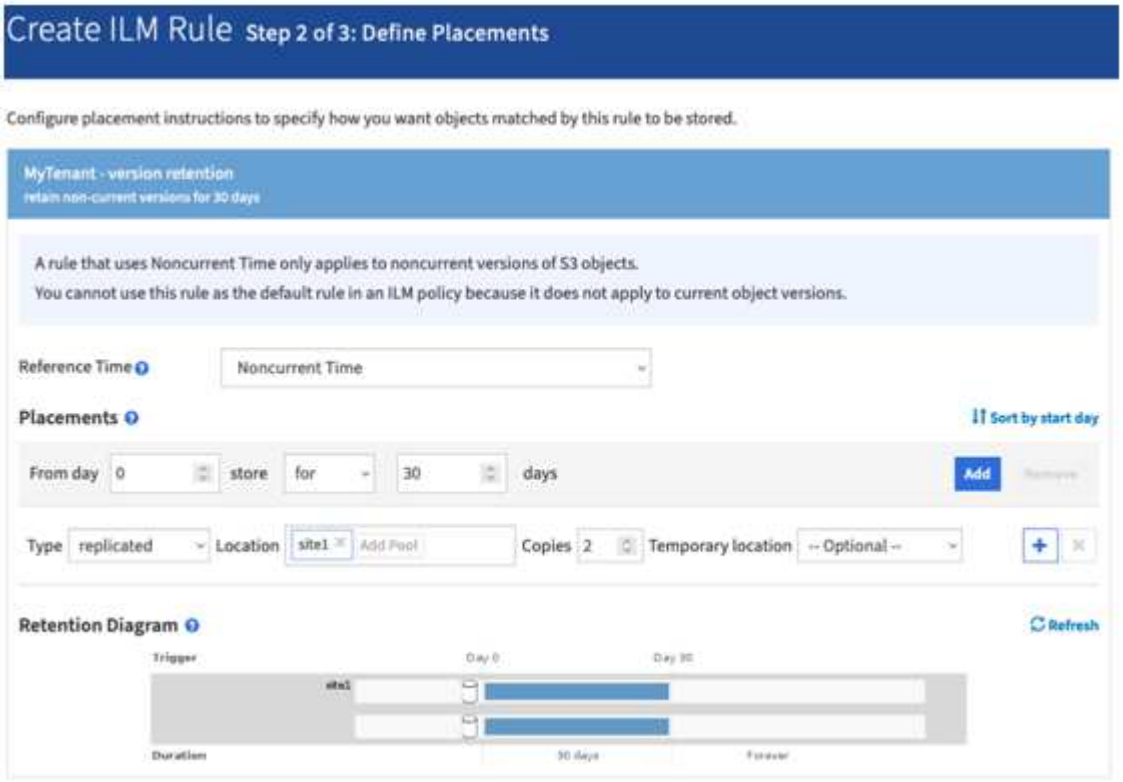


2. Konfigurieren Sie auf dem Quell-Bucket die Replikation zur Verwendung des konfigurierten Endpunkts.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. Erstellen Sie ILM-Regeln, um die Storage-Platzierung und das Versionsspeicherzeitmanagement zu managen. In diesem Beispiel werden die nicht aktuellen Versionen der zu speichernden Objekte konfiguriert.





An Standort 1 sind 30 Tage lang zwei Kopien vorhanden. Sie konfigurieren außerdem die Regeln für die aktuelle Version der Objekte basierend auf der Verwendung der Aufnahmezeit als Referenzzeit in der ILM-Regel, um der Speicherdauer des Quell-Buckets anzupassen. Die Storage-Platzierung für die Objektversionen kann Erasure Coded oder repliziert werden.

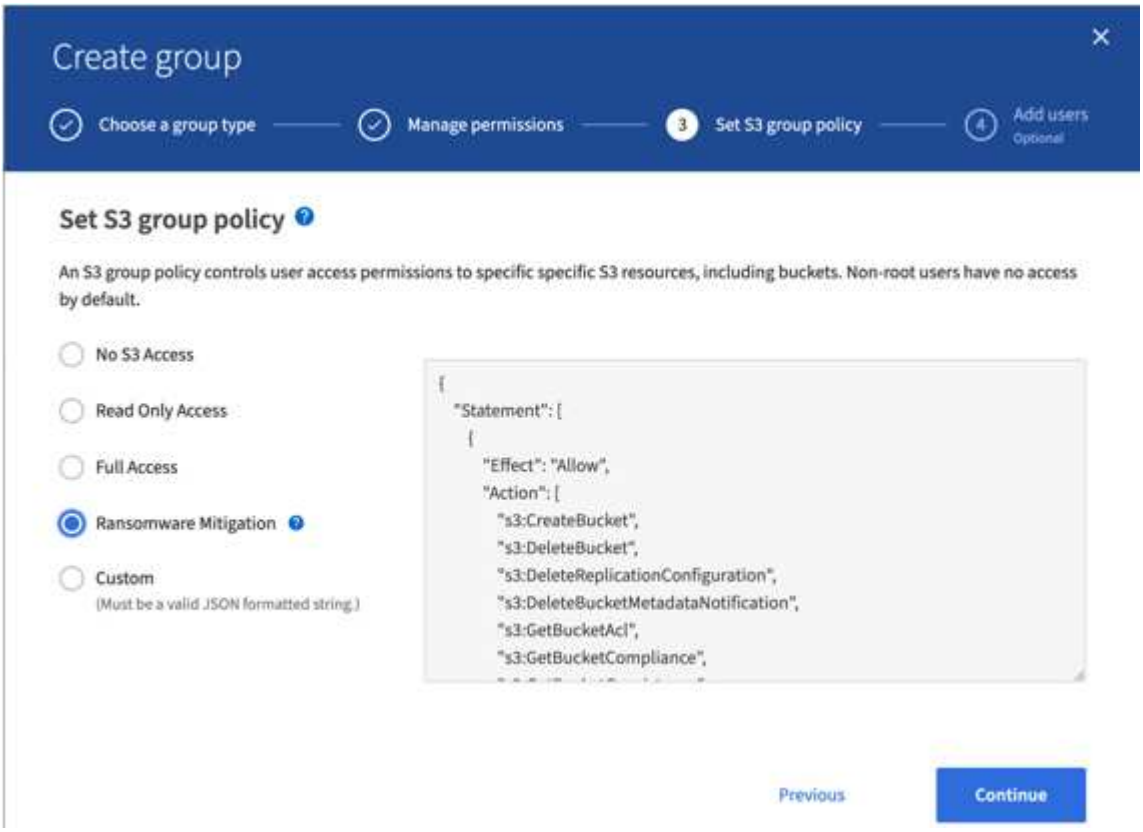
Ransomware-Verteidigung durch Versionierung mit Schutz-IAM-Richtlinie

Erfahren Sie, wie Sie Ihre Daten schützen, indem Sie die Versionierung auf dem Bucket aktivieren und IAM-Richtlinien auf Benutzersicherheitsgruppen in StorageGRID implementieren.

Eine Methode zum Schutz Ihrer Daten ohne Objektsperre oder Replikation besteht darin, die Versionierung auf dem Bucket zu aktivieren und IAM-Richtlinien auf den Benutzersicherheitsgruppen zu implementieren, um die Fähigkeit des Benutzers zu beschränken, Versionen der Objekte zu verwalten. Im Falle eines Angriffs werden neue fehlerhafte Versionen der Daten als aktuelle Version erstellt, und die neueste nicht-aktuelle Version ist die

sichere saubere Daten. Die Konten, die für den Zugriff auf die Daten kompromittiert wurden, haben keinen Zugriff auf das Löschen oder anderweitige Ändern der nicht-aktuellen Version, um sie für spätere Wiederherstellungsvorgänge zu schützen. Wie im vorherigen Szenario verwalten ILM-Regeln die Aufbewahrung der nicht aktuellen Versionen mit einer Dauer Ihrer Wahl. Der Nachteil ist, dass es immer noch die Möglichkeit von privilegierten Konten für einen schlechten Akteurangriff gibt, aber alle Anwendungsdienstkonten und Benutzer müssen mit einem restriktiveren Zugriff konfiguriert werden. Die restriktive Gruppenrichtlinie muss jede Aktion, die Benutzer oder Anwendungen ausführen sollen, ausdrücklich zulassen und alle Aktionen, die nicht ausgeführt werden sollen, ausdrücklich ablehnen. NetApp empfiehlt keine Platzhalterfunktion, da in Zukunft möglicherweise eine neue Aktion eingeführt wird. Sie sollten dann kontrollieren, ob sie erlaubt oder verweigert wird. Für diese Lösung muss die Deny-Liste DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration und PutBucketVersioning enthalten, um die Versionskonfiguration des Buckets und Objektversionen vor Benutzer- oder programmatischen Änderungen zu schützen.

In StorageGRID erleichtert die S3-Gruppenrichtlinienoption „Ransomware Mitigation“ die Implementierung dieser Lösung. Wenn Sie im Mandanten eine Benutzergruppe erstellen, können Sie nach Auswahl der Gruppenberechtigungen diese optionale Richtlinie sehen.



Im Folgenden finden Sie den Inhalt der Gruppenrichtlinie, die die meisten verfügbaren Vorgänge explizit erlaubt und das erforderliche Minimum abgelehnt enthält.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
```

```
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
```

```
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Untersuchung und Behebung von Ransomware

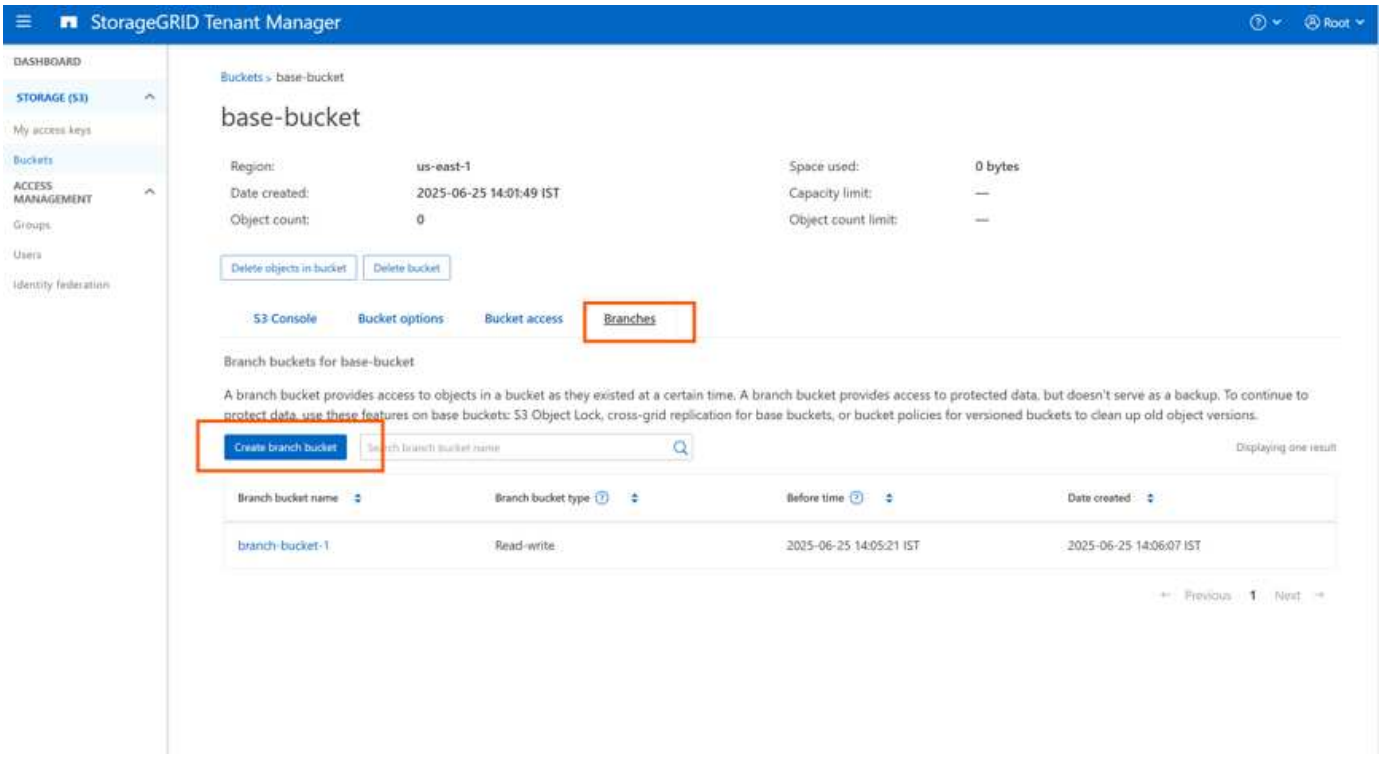
Erfahren Sie, wie Sie Buckets nach einem möglichen Ransomware-Angriff mit StorageGRID untersuchen und beheben.

In StorageGRID 12.0 wurde die neue Branch-Bucket-Funktion hinzugefügt, um die Nützlichkeit der Versionierung für die Ransomware-Abwehr zu erweitern. Ein Branch-Bucket bietet Zugriff auf Objekte in einem Bucket, wie sie zu einem bestimmten Zeitpunkt existierten, sofern sie noch im Bucket vorhanden sind. Branch-Buckets können nur für versionierungsfähige Basis-Buckets erstellt werden.

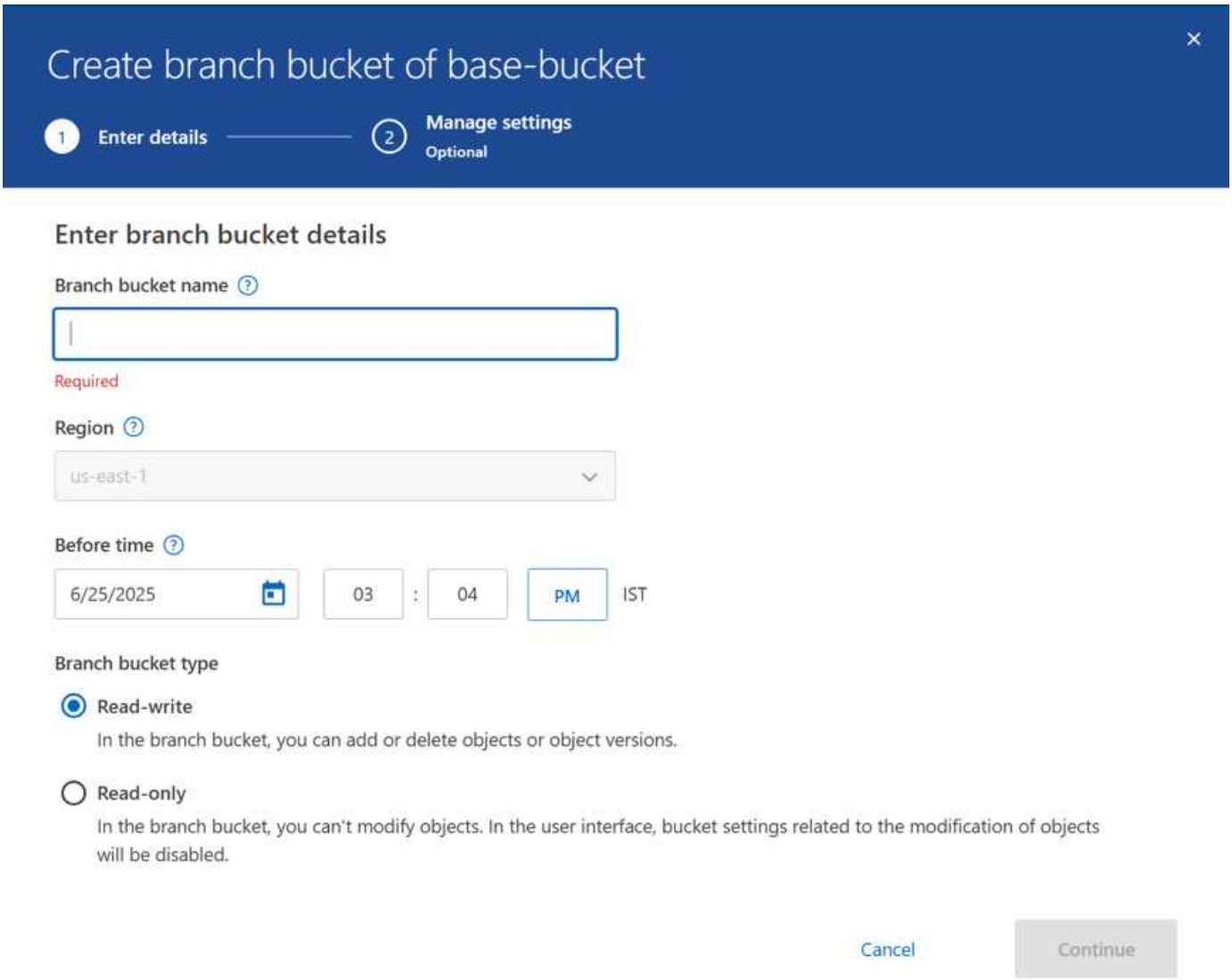
Das bedeutet, dass Sie bei Verdacht auf einen Ransomware-Angriff einen Lese-/Schreib- oder schreibgeschützten Branch-Bucket erstellen können, der alle Objekte und Versionen enthält, die vor dem ersten Angriff vorhanden waren. Sie können diesen Zweig-Bucket zum Vergleich mit dem Inhalt des Basis-Buckets verwenden, um herauszufinden, welche Objekte geändert wurden und ob die Änderung Teil des Angriffs war oder nicht. Sie können auch einen Branch-Bucket verwenden, um die Clientvorgänge mithilfe des Clean-Branch fortzusetzen, während Sie den Angriff untersuchen.

Erstellen eines Branch-Buckets

- Navigieren Sie zur Detailseite des Basis-Buckets und zur Registerkarte „Branches“, um einen Branch-Bucket zu erstellen.



- Sobald Sie auf die Schaltfläche „Zweig-Bucket erstellen“ klicken, wird ein Popup mit vorab ausgefüllten Details der mit dem Basis-Bucket verknüpften Region geöffnet.
- Geben Sie vor der Zeit den Namen des Branch-Buckets ein und wählen Sie aus, welcher Branch-Bucket-Typ erstellt werden soll.



TR-4765: Monitor StorageGRID

Einführung in das StorageGRID-Monitoring

Erfahren Sie, wie Sie Ihr StorageGRID System mit externen Applikationen wie Splunk überwachen.

Durch die effektive Überwachung des objektbasierten Storage von NetApp StorageGRID können Administratoren umgehend auf dringende Probleme reagieren und Ressourcen proaktiv hinzufügen, um wachsende Workloads zu bewältigen. Dieser Bericht bietet allgemeine Hinweise zur Überwachung wichtiger Kennzahlen und zur Nutzung externer Überwachungsanwendungen. Es soll das bestehende Handbuch zur Überwachung und Fehlerbehebung ergänzen.

Eine NetApp StorageGRID-Implementierung besteht in der Regel aus mehreren Standorten und mehreren Nodes, die ein verteiltes und fehlertolerantes Objekt-Storage-System erzeugen. In einem verteilten und robusten Storage-System wie StorageGRID existieren Fehlerbedingungen, während das Grid weiterhin normal arbeitet. Die Herausforderung für Sie als Administrator besteht darin, die Schwelle zu verstehen, bei der Fehlerbedingungen (z. B. Knoten ausgefallen) ein Problem darstellen, das sofort behoben werden sollte, und Informationen, die analysiert werden sollten. Durch die Analyse der von StorageGRID gespeicherten Daten

können Sie einen besseren Überblick über Ihren Workload haben und fundierte Entscheidungen treffen, beispielsweise wenn Sie zusätzliche Ressourcen hinzufügen möchten.

StorageGRID bietet eine exzellente Dokumentation, die tief in das Thema Monitoring eintaucht. In diesem Bericht wird vorausgesetzt, dass Sie mit StorageGRID vertraut sind und die Dokumentation darüber geprüft haben. Anstatt diese Informationen zu wiederholen, beziehen wir uns in der Produktdokumentation in diesem Handbuch. Die Produktdokumentation von StorageGRID ist online und als PDF verfügbar.

Ziel dieses Dokuments ist die Ergänzung der Produktdokumentation und die Erläuterung der Überwachung Ihres StorageGRID Systems mit externen Applikationen wie Splunk.

Datenquellen

Für die erfolgreiche Überwachung von NetApp StorageGRID ist es wichtig zu wissen, wo Daten über den Zustand und die Vorgänge Ihres StorageGRID Systems erfasst werden müssen.

- **Web UI und Dashboard.** Der StorageGRID-Grid-Manager bietet eine Ansicht der wichtigsten Informationen, die Sie als Administrator in einer logischen Präsentation anzeigen müssen. Als Administrator können Sie sich außerdem tiefer mit Service-Level-Informationen für die Fehlerbehebung und Protokollsammlung befassen.
- **Prüfprotokolle.** StorageGRID speichert granulare Prüfprotokolle von Mandantenaktionen wie PUT, GET und DELETE. Sie können auch den Lebenszyklus eines Objekts von der Aufnahme bis zur Anwendung der Datenmanagement-Regeln nachverfolgen.
- **Metrics API.** Dem StorageGRID GMI liegen offene APIs zugrunde, da die Benutzeroberfläche API-basiert ist. Dieser Ansatz ermöglicht es Ihnen, Daten mithilfe externer Überwachungs- und Analysetools zu extrahieren.

Wo Sie weitere Informationen finden

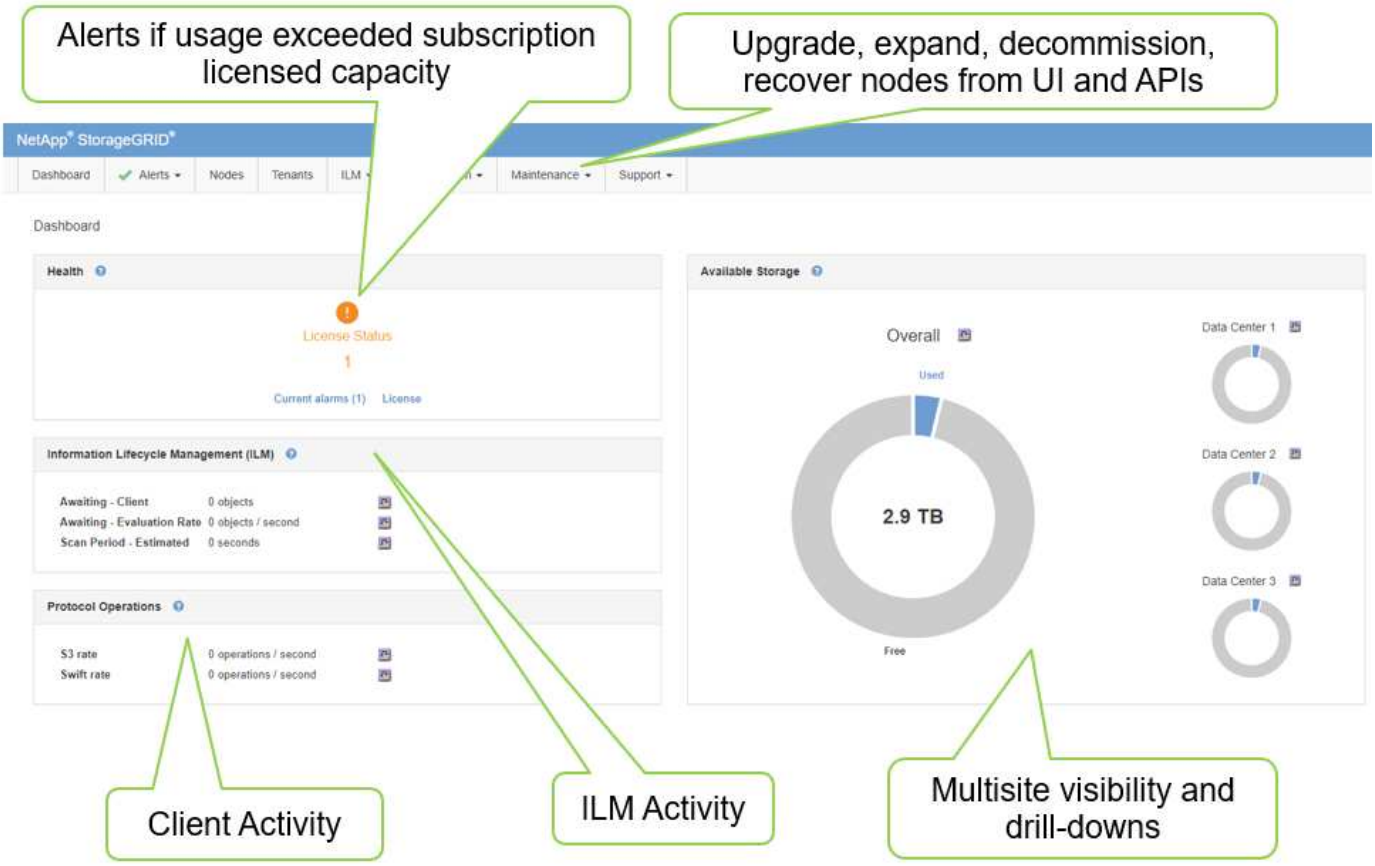
Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/
- NetApp StorageGRID App für Splunk https://splunkbase.splunk.com/app/3898/#/details

Verwenden Sie das GMI-Dashboard, um StorageGRID zu überwachen

Das StorageGRID Grid Management Interface (GMI) Dashboard bietet eine zentrale Ansicht der StorageGRID Infrastruktur. So haben Sie die Möglichkeit, den Zustand, die Performance und die Kapazität des gesamten Grids zu überwachen.

Verwenden Sie das GMI-Dashboard, um jede Kernkomponente des Rasters zu untersuchen.



Informationen, die Sie regelmäßig überwachen sollten

In einer vorherigen Version dieses technischen Berichts sind die Kennzahlen aufgeführt, die regelmäßig überprüft werden müssen, verglichen mit den Trends. Diese Informationen sind nun in der "Leitfaden zur Überwachung und Fehlerbehebung".

Überwachen Sie den Speicher

Eine vorherige Version dieses technischen Berichts war aufgeführt, wo wichtige Kennzahlen wie Objekt-Storage-Platzbedarf, Metadaten-Speicherplatz, Netzwerkressourcen usw. überwacht werden müssen. Diese Informationen sind nun in der "Leitfaden zur Überwachung und Fehlerbehebung".

Verwenden Sie Warnmeldungen, um StorageGRID zu überwachen

Erfahren Sie, wie Sie das Warnsystem in StorageGRID verwenden, um Probleme zu überwachen, benutzerdefinierte Warnmeldungen zu verwalten und Benachrichtigungen per SNMP oder E-Mail zu erweitern.

Warnmeldungen liefern wichtige Informationen, mit denen Sie die verschiedenen Ereignisse und Zustände in Ihrem StorageGRID-System überwachen können.

Das Warnmeldungssystem ist das primäre Tool für die Überwachung von Problemen, die in Ihrem StorageGRID-System auftreten können. Das Alarmsystem konzentriert sich auf umsetzbare Probleme im System und bietet eine benutzerfreundliche Oberfläche.

Wir bieten eine Reihe von Standardwarnungsregeln an, mit denen Sie Ihr System überwachen und Fehler beheben können. Sie können Warnmeldungen weiter verwalten, indem Sie benutzerdefinierte Warnmeldungen

erstellen, Standardwarnungen bearbeiten oder deaktivieren und Warnmeldungen stummschalten.

Alarme können auch über SNMP oder E-Mail-Benachrichtigungen erweitert werden.

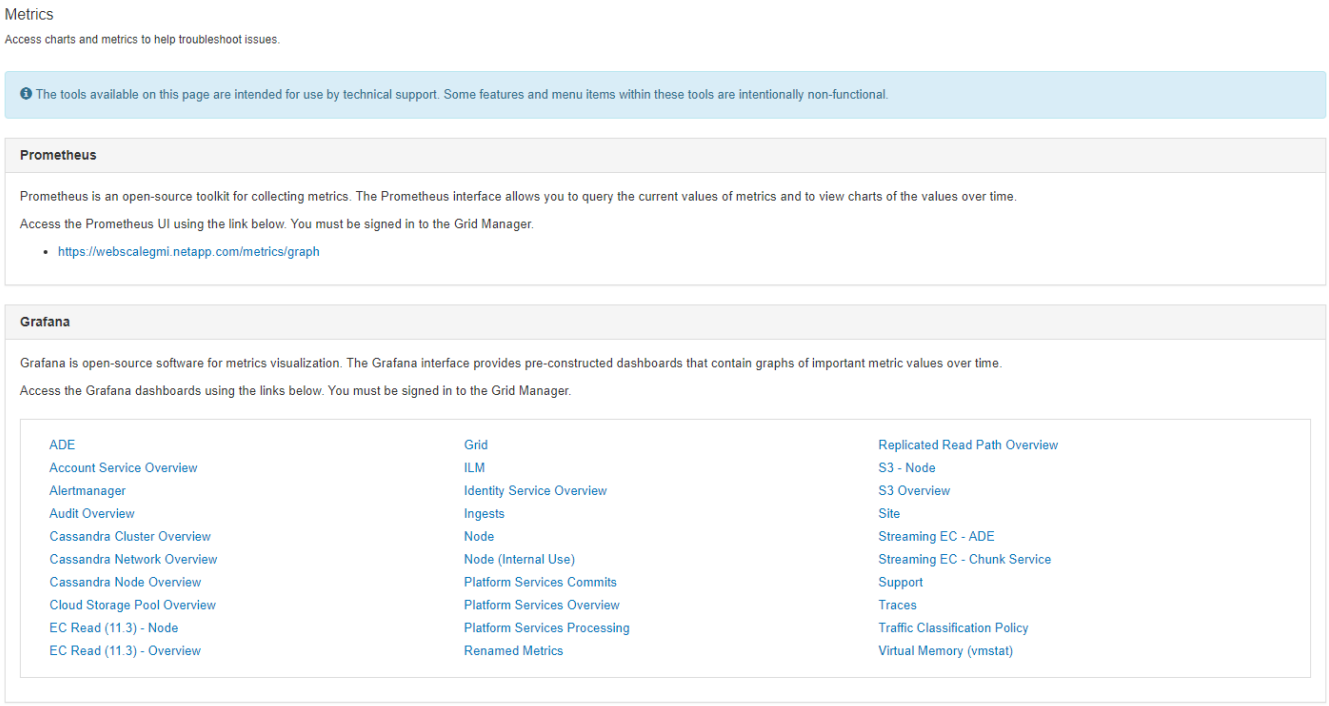
Weitere Informationen zu Warnmeldungen finden Sie im "Produktdokumentation" Online- und im PDF-Format.

Erweiterte Überwachung in StorageGRID

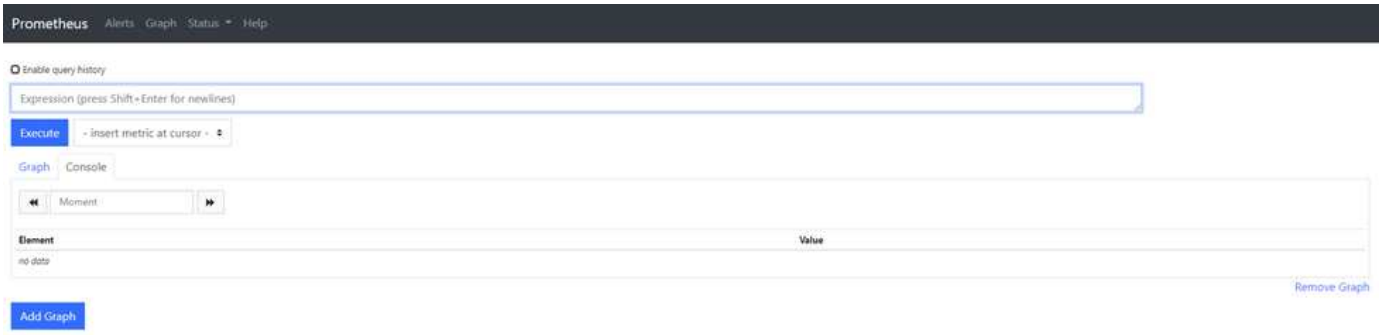
Erfahren Sie, wie Sie auf Kennzahlen zugreifen und diese exportieren, um Probleme zu beheben.

Anzeigen von Kennzahlen-API über eine Prometheus-Abfrage

Prometheus ist eine Open-Source-Software zur Erfassung von Kennzahlen. Über das GMI können Sie auf die in StorageGRID eingebetteten Prometheus zugreifen: Support[Metriken].



Alternativ können Sie direkt zu dem Link navigieren.

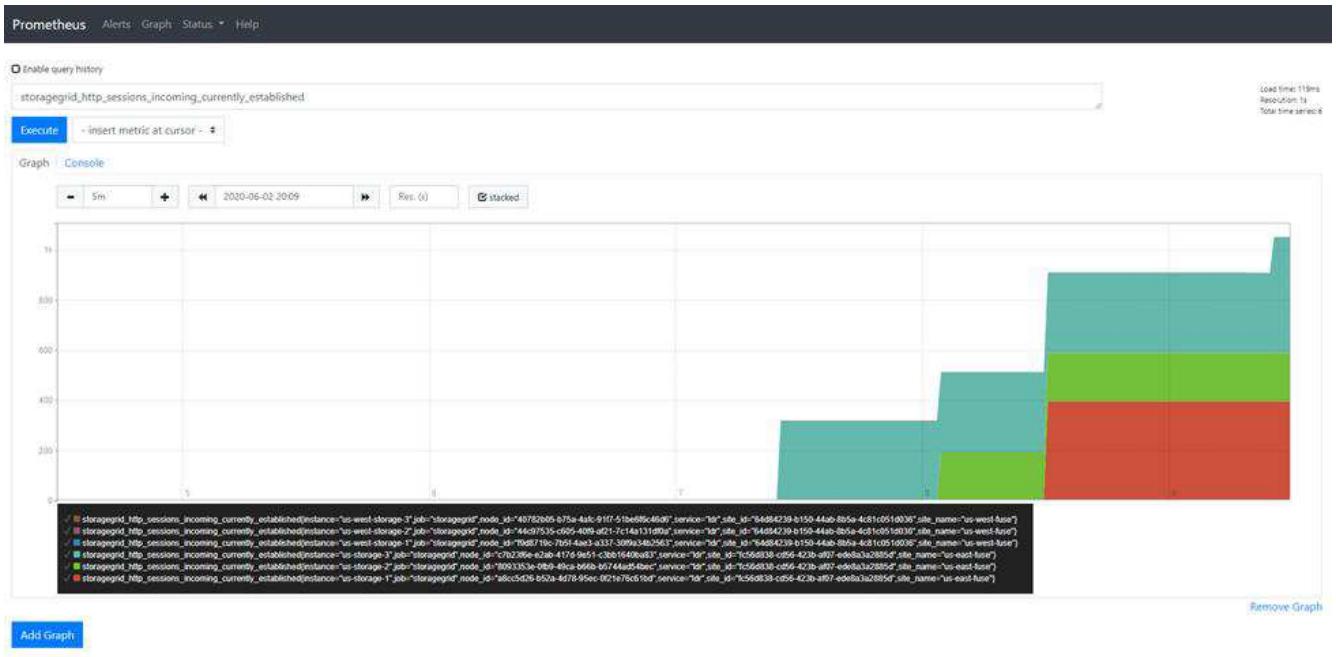


Mit dieser Ansicht können Sie auf die Prometheus-Schnittstelle zugreifen. Von dort aus können Sie die verfügbaren Metriken durchsuchen und sogar mit Abfragen experimentieren.

Gehen Sie wie folgt vor, um eine Prometheus-URL-Abfrage durchzuführen:

Schritte

1. Beginnen Sie mit der Eingabe im Textfeld für die Abfrage. Bei der Eingabe werden die Metriken aufgelistet. Für unsere Zwecke sind nur Metriken wichtig, die mit StorageGRID und Node beginnen.
2. Um die Anzahl der HTTP-Sitzungen für jeden Knoten anzuzeigen, geben Sie ein `storagegrid_http` , und wählen Sie `storagegrid_http_sessions_incoming_currently_established`. Klicken Sie auf Ausführen und zeigen Sie die Informationen in einem Diagramm- oder Konsolenformat an.



Abfragen und Diagramme, die Sie über diese URL erstellen, bleiben nicht erhalten. Komplexe Abfragen verbrauchen Ressourcen auf dem Admin-Node. NetApp empfiehlt, die verfügbaren Metriken in dieser Ansicht zu prüfen.

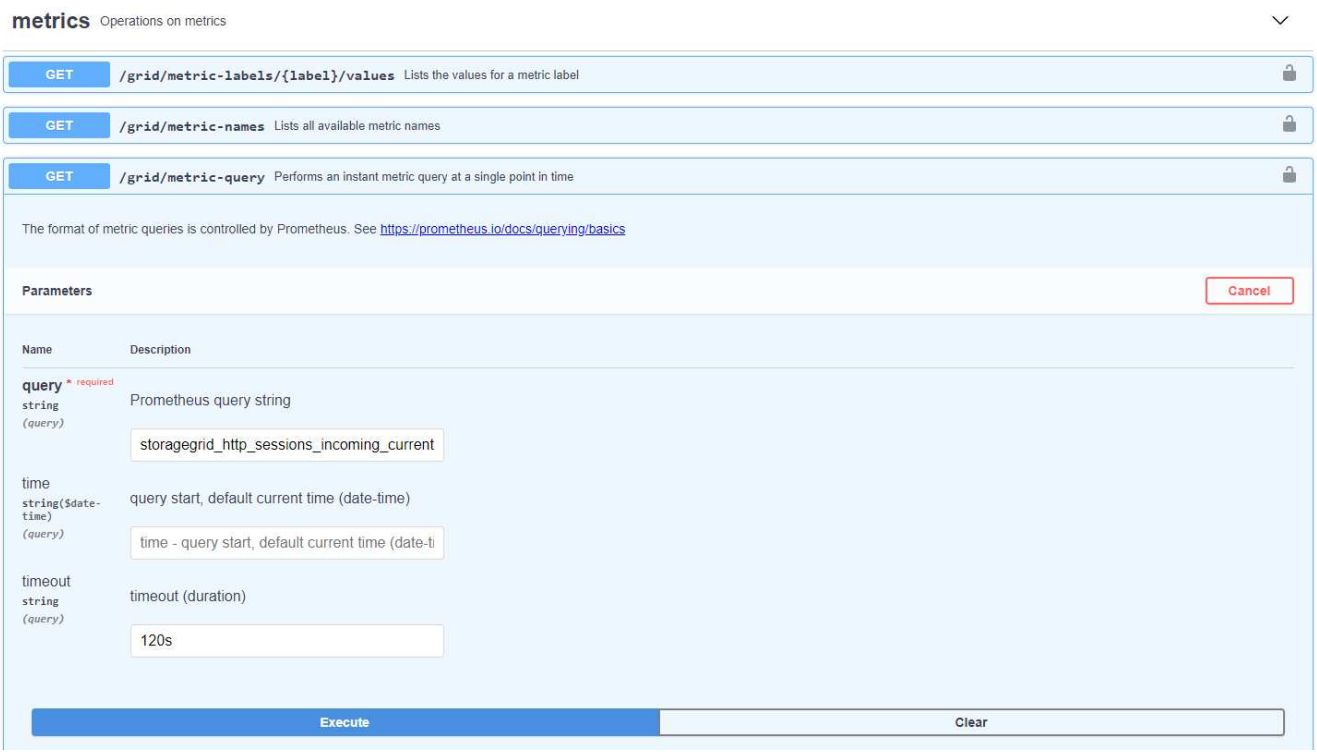
Es wird nicht empfohlen, eine direkte Schnittstelle zu unserer Prometheus Instanz zu verwenden, da hierzu zusätzliche Ports geöffnet werden müssen. Der Zugriff auf Kennzahlen über unsere API ist die empfohlene und sichere Methode.

Exportieren von Kennzahlen über die API

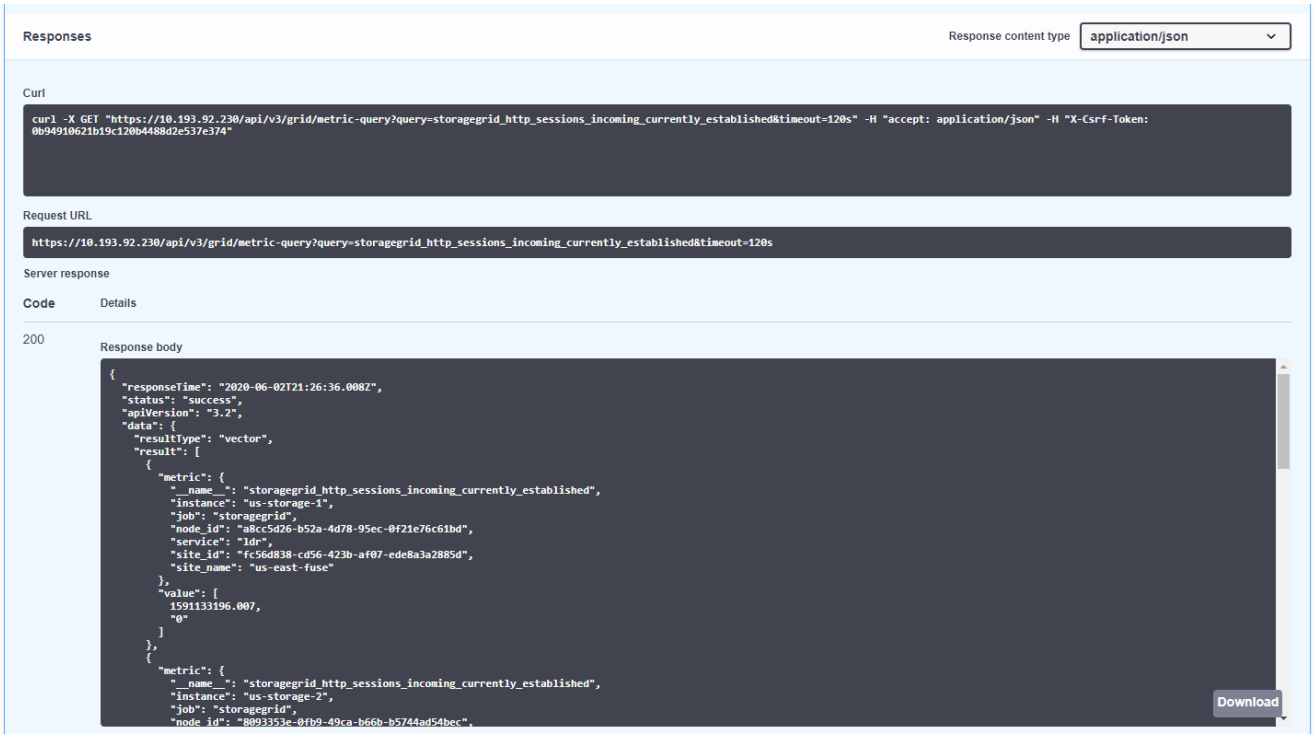
Außerdem können Sie über die StorageGRID Management-API auf dieselben Daten zugreifen.

Gehen Sie wie folgt vor, um Metriken über die API zu exportieren:

1. Wählen Sie im GMI die Option MENU:Help[API Documentation].
2. Scrollen Sie nach unten zu Metriken und wählen Sie GET /Grid/metric-query.



Die Antwort enthält dieselben Informationen, die Sie über eine Prometheus URL-Abfrage erhalten können. Sie können wieder die Anzahl der HTTP-Sitzungen anzeigen, die derzeit auf jedem Storage-Node eingerichtet sind. Sie können die Antwort zur Lesbarkeit auch im JSON-Format herunterladen. Die folgende Abbildung zeigt beispielhafte Prometheus Abfrageantworten.



Der Vorteil der Verwendung der API besteht darin, dass Sie authentifizierte Abfragen durchführen können

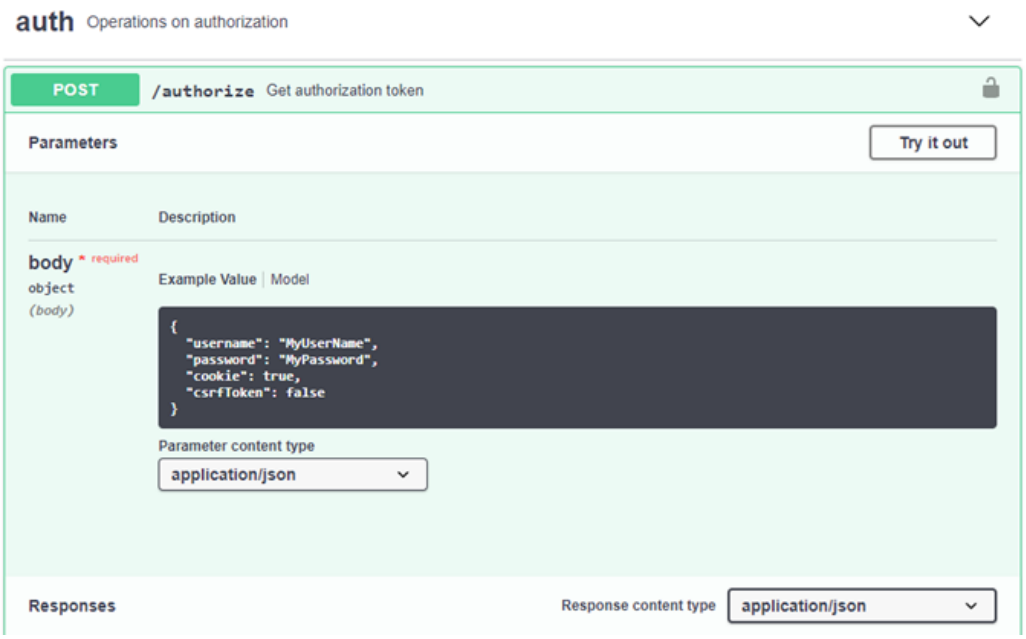
Zugriff auf Metriken mithilfe von Curl in StorageGRID

Erfahren Sie, wie Sie mithilfe von Curl über die CLI auf Metriken zugreifen.

Um diesen Vorgang auszuführen, müssen Sie zunächst ein Autorisierungs-Token anfordern. So fordern Sie ein Token an:

Schritte

1. Wählen Sie im GMI die Option MENU:Help[API Documentation].
2. Blättern Sie nach unten zu Auth, um nach Vorgängen für die Autorisierung zu suchen. Der folgende Screenshot zeigt die Parameter für die POST-Methode.



3. Klicken Sie auf Try IT Out, und bearbeiten Sie den Text mit Ihrem GMI-Benutzernamen und -Kennwort.
4. Klicken Sie Auf Ausführen.
5. Kopieren Sie den Befehl curl, der im Abschnitt curl angegeben ist, und fügen Sie ihn in ein Terminalfenster ein. Der Befehl sieht wie folgt aus:

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

> Wenn Ihr GMI-Passwort Sonderzeichen enthält, vergessen Sie nicht, \ zu verwenden, um Sonderzeichen zu umgehen. Zum Beispiel ersetzen ! Mit \!

6. Nachdem Sie den vorherigen Curl-Befehl ausgeführt haben, erhalten Sie in der Ausgabe ein Autorisierungstoken wie das folgende Beispiel:

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

Jetzt können Sie die Zeichenfolge für das Autorisierungstoken verwenden, um auf Metriken durch Curl zuzugreifen. Der Prozess für den Zugriff auf Kennzahlen ähnelt den Schritten in Abschnitt "Erweiterte Überwachung in StorageGRID". Zu Demonstrationszwecken zeigen wir jedoch ein Beispiel mit GET /GRID/metric-Labels/{Label}/values, das in der Kategorie Metrics ausgewählt wurde.

7. Beispiel: Der folgende Curl-Befehl mit dem vorangehenden Autorisierungstoken führt die Standortnamen in StorageGRID auf.

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

Der Befehl Curl erzeugt die folgende Ausgabe:

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

Anzeigen von Kennzahlen über das Grafana-Dashboard in StorageGRID

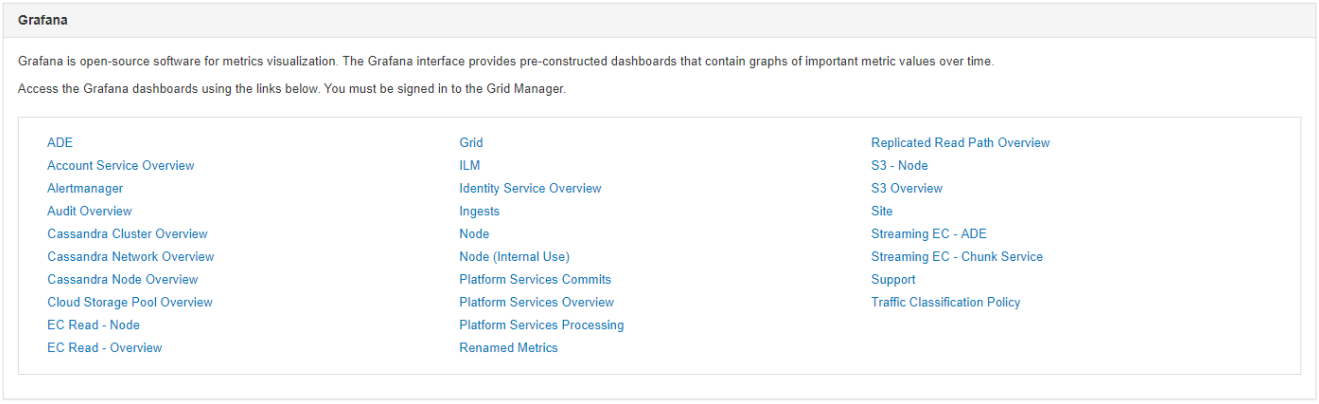
Erfahren Sie, wie Sie mit der Grafana-Schnittstelle Ihre StorageGRID-Daten visualisieren und überwachen.

Grafana ist eine Open-Source-Software für die metrische Visualisierung. Wir verfügen standardmäßig über vorgefertigte Dashboards mit nützlichen und aussagekräftigen Informationen zu Ihrem StorageGRID System.

Diese vorgefertigten Dashboards sind nicht nur für die Überwachung, sondern auch für die Fehlerbehebung bei einem Problem nützlich. Einige sind für den technischen Support bestimmt. Um z. B. die Metriken eines Storage-Nodes anzuzeigen, führen Sie die folgenden Schritte aus.

Schritte

1. Im GMI Menü:Support[Metriken].
2. Wählen Sie im Abschnitt Grafana das Knoten-Dashboard aus.



3. Legen Sie in Grafana den Host auf den Node fest, für den Sie Metriken anzeigen möchten. In diesem Fall ist ein Storage-Node ausgewählt. Es werden mehr Informationen bereitgestellt als die folgenden Screenshot-Aufnahmen.

Verwenden Sie Richtlinien zur Verkehrsklassifizierung im StorageGRID

Erfahren Sie, wie Sie Richtlinien zur Verkehrsklassifizierung einrichten und konfigurieren, um den Netzwerkverkehr in StorageGRID zu managen und zu optimieren.

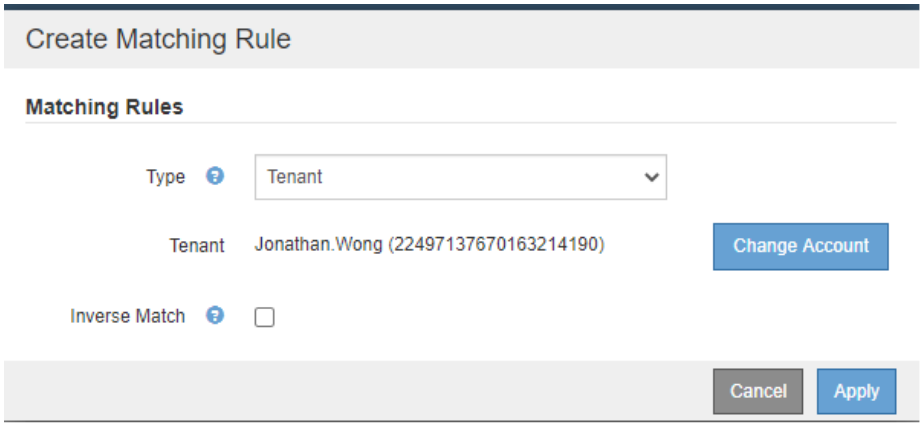
Richtlinien zur Traffic-Klassifizierung bieten eine Methode zur Überwachung und/oder Begrenzung des Datenverkehrs auf der Grundlage eines bestimmten Mandanten, Buckets, IP-Subnetzes oder Load-Balancer-Endpunkts. Netzwerkkonnektivität und Bandbreite sind besonders wichtige Kenngrößen für StorageGRID.

Gehen Sie wie folgt vor, um eine Richtlinie zur Traffic-Klassifizierung zu konfigurieren:

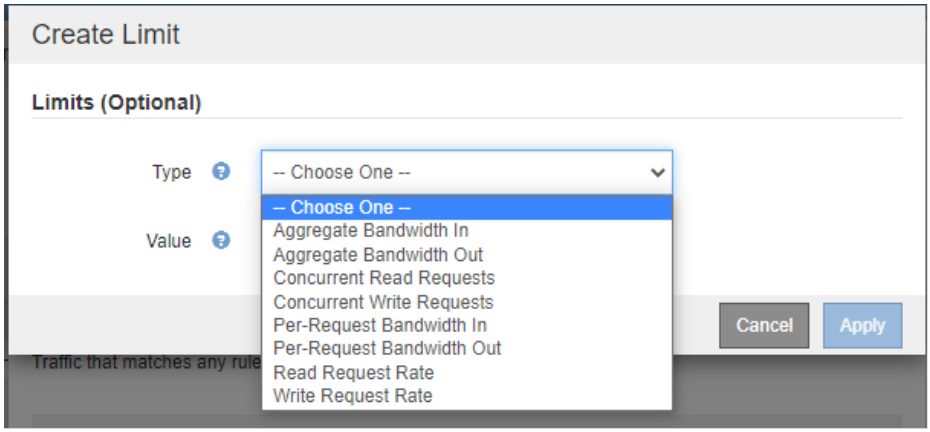
Schritte

1. Navigieren Sie im GMI zu MENU:Configuration[System Settings > Traffic Classification].
2. Klicken Sie Auf Erstellen +
3. Geben Sie einen Namen und eine Beschreibung für Ihre Richtlinie ein.

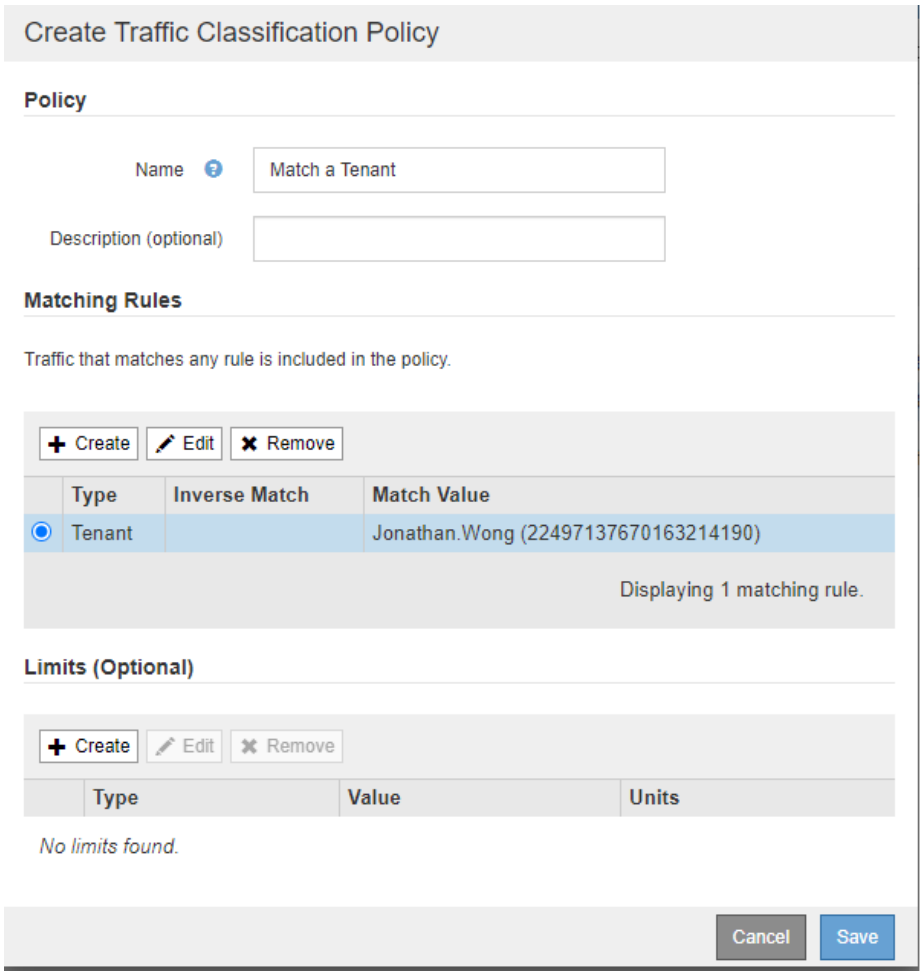
4. Erstellen Sie eine übereinstimmende Regel.



5. Legen Sie eine Grenze fest (optional).



6. Speichern Sie Ihre Richtlinie



Um die Metriken anzuzeigen, die Ihrer Richtlinie zur Traffic-Klassifizierung zugeordnet sind, wählen Sie Ihre Richtlinie aus, und klicken Sie auf Kennzahlen. Es wird ein Grafana Dashboard mit Informationen wie Load Balancer Request Traffic und Average Request Duration erstellt.

Verwenden Sie Prüfprotokolle, um StorageGRID zu überwachen

Erfahren Sie, wie Sie das StorageGRID-Revisionsprotokoll detaillierte Einblicke in Mandanten- und Grid-Aktivitäten erhalten und wie Sie Tools wie Splunk für Protokollanalysen nutzen können.

Mit dem StorageGRID Revisionsprotokoll können Sie detaillierte Informationen über Mandanten und Grid-Aktivitäten erfassen. Das Revisionsprotokoll kann zur Analyse durch NFS offengelegt werden. Ausführliche Anweisungen zum Exportieren des Überwachungsprotokolls finden Sie im Administratorhandbuch.

Nach dem Export der Prüfung können Sie Protokollanalyse-Tools wie Splunk oder Logstash + Elasticsearch verwenden, um die Mandantenaktivität zu verstehen oder detaillierte Rechnungs- und Chargeback-Berichte zu erstellen.

Details zu Audit-Meldungen sind in der StorageGRID-Dokumentation enthalten. Siehe "Audit-Meldungen".

Die StorageGRID App für Splunk

Die NetApp StorageGRID App für Splunk ermöglicht Monitoring und Analyse Ihrer StorageGRID-Umgebung innerhalb der Splunk Plattform.

Splunk ist eine Softwareplattform, die Maschinendaten importiert und indiziert, um leistungsstarke Such- und Analysefunktionen zu bieten. Die NetApp StorageGRID App ist ein Add-on für Splunk, das die aus StorageGRID verwendeten Daten importiert und anreichert.

Anweisungen zur Installation, Aktualisierung und Konfiguration des StorageGRID Add-ons finden Sie hier: https://splunkbase.splunk.com/app/3895/#/details

TR-4882: Installation eines StorageGRID Bare-Metal Grid

Einführung in die Installation von StorageGRID

Erfahren Sie, wie Sie StorageGRID auf Bare-Metal-Hosts installieren.

TR-4882 bietet eine praktische Schritt-für-Schritt-Anleitung, die zu einer funktionierenden Installation von NetApp StorageGRID führt. Die Installation kann entweder auf Bare-Metal-Systemen oder auf Virtual Machines (VMs) erfolgen, die unter Red hat Enterprise Linux (RHEL) ausgeführt werden. Der Ansatz besteht darin, eine „opinionierte“ Installation von sechs StorageGRID Container-Services auf drei physischen (oder virtuellen) Maschinen mit einer vorgegebenen Layout- und Storage-Konfiguration durchzuführen. Einige Kunden finden es unter Umständen leichter, den Implementierungsprozess zu verstehen, indem sie dem Beispiel folgen, das in diesem TR bereitgestellt wird.

Weitere Informationen zu StorageGRID und dem Installationsprozess finden Sie unter https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html [StorageGRID installieren, aktualisieren und Hotfix] in der Produktdokumentation.

Bevor Sie mit der Implementierung beginnen, sollten wir die Computing-, Storage- und Netzwerkanforderungen für NetApp StorageGRID Software untersuchen. StorageGRID wird als Container-Service in Podman oder Docker ausgeführt. Einige Anforderungen beziehen sich in diesem Modell auf das Host-Betriebssystem (das Betriebssystem, auf dem Docker gehostet wird, auf dem die StorageGRID Software ausgeführt wird). Einige Ressourcen werden direkt den Docker Containern zugewiesen, die innerhalb jedes Hosts ausgeführt werden. In dieser Implementierung implementieren wir zur Maximierung der

Hardwarenutzung zwei Services pro physischem Host. Weitere Informationen finden Sie im nächsten Abschnitt. "Voraussetzungen für die Installation von StorageGRID"

Die in dieser TR beschriebenen Schritte führen zu einer funktionierenden StorageGRID-Installation auf sechs Bare-Metal-Hosts. Sie verfügen jetzt über ein funktionierendes Grid- und Client-Netzwerk, das in den meisten Testszenarien nützlich ist.

Wo Sie weitere Informationen finden

Folgende Dokumentationsressourcen enthalten weitere Informationen zu den in diesem TR enthaltenen Informationen:

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Voraussetzungen für die Installation von StorageGRID

Informieren Sie sich über die Computing-, Storage-, Netzwerk-, Docker- und Node-Anforderungen für die Implementierung von StorageGRID.

Computing-Anforderungen

In der folgenden Tabelle sind die unterstützten Mindestanforderungen an Ressourcen für jeden Typ von StorageGRID-Knoten aufgeführt. Dies sind die Mindestressourcen, die für StorageGRID Nodes erforderlich sind.

Node-Typ	CPU-Kerne	RAM
Admin	8	24 GB
Storage	8	24 GB
Gateway	8	24 GB

Darüber hinaus sollte jedem physischen Docker Host mindestens 16 GB RAM zugewiesen sein, um den ordnungsgemäßen Betrieb zu gewährleisten. Um beispielsweise zwei der in der Tabelle beschriebenen Services gemeinsam auf einem physischen Docker Host zu hosten, führen Sie die folgende Berechnung aus:

24 + 24 +16 = 64 GB RAM und 8 + 8 = 16 Cores

Da viele moderne Server diese Anforderungen übertreffen, kombinieren wir sechs Services (StorageGRID-Container) auf drei physischen Servern.

Netzwerkanforderungen

Zu den drei Arten von StorageGRID-Datenverkehr gehören:

- **Netzverkehr (erforderlich).** Der interne StorageGRID-Datenverkehr zwischen allen Nodes im Grid.
- **Admin Traffic (optional).** Der für die Systemadministration und -Wartung verwendete Datenverkehr.
- **Client Traffic (optional).** Der Datenverkehr zwischen externen Client-Applikationen und dem Grid, einschließlich aller Objekt-Storage-Anforderungen von S3 und Swift Clients

Sie können bis zu drei Netzwerke zur Verwendung mit dem StorageGRID-System konfigurieren. Jeder Netzwerktyp muss sich in einem separaten Subnetz ohne Überschneidung befinden. Wenn sich alle Nodes im gleichen Subnetz befinden, ist keine Gateway-Adresse erforderlich.

Für diese Auswertung werden wir in zwei Netzwerken bereitstellen, die den Grid- und Client-Datenverkehr enthalten. Es ist möglich, später ein Admin-Netzwerk hinzuzufügen, um diese zusätzliche Funktion zu unterstützen.

Es ist sehr wichtig, die Netzwerke konsistent den Schnittstellen aller Hosts zuzuordnen. Wenn beispielsweise auf jedem Node zwei Schnittstellen vorhanden sind, ens192 und ens224, sollten sie alle auf allen Hosts dem gleichen Netzwerk oder VLAN zugeordnet werden. In dieser Installation ordnet das Installationsprogramm diese in den Docker Containern als eth0@if2 und eth2@if3 zu (da der Loopback if1 im Container ist), und daher ist ein konsistentes Modell sehr wichtig.

Hinweis zu Docker Networking

StorageGRID verwendet Netzwerke, die von einigen Docker Container-Implementierungen abweichen. Es wird nicht das von Docker (oder Kubernetes oder Swarm) bereitgestellte Netzwerk verwendet. Stattdessen gibt StorageGRID den Container als --net=none aus, sodass Docker für das Netzwerken des Containers nichts tut. Nachdem der Container vom StorageGRID-Dienst erstellt wurde, wird ein neues macvlan-Gerät aus der in der Node-Konfigurationsdatei definierten Schnittstelle erstellt. Dieses Gerät verfügt über eine neue MAC-Adresse und fungiert als separates Netzwerkgerät, das Pakete von der physischen Schnittstelle empfangen kann. Das macvlan-Gerät wird dann in den Container-Namespace verschoben und in eth0, eth1 oder eth2 innerhalb des Containers umbenannt. Zu diesem Zeitpunkt ist das Netzwerkgerät im Host-Betriebssystem nicht mehr sichtbar. In unserem Beispiel ist das Grid-Netzwerkgerät eth0 in den Docker Containern und das Client-Netzwerk eth2. Bei einem Admin-Netzwerk wäre das Gerät im Container eth1.

> ⓘ Die neue MAC-Adresse des Container-Netzwerkgeräts erfordert möglicherweise die Aktivierung des Promiscuous-Modus in einigen Netzwerk- und virtuellen Umgebungen. In diesem Modus kann das physische Gerät Pakete für MAC-Adressen empfangen und senden, die sich von der bekannten physischen MAC-Adresse unterscheiden. Wenn Sie in VMware vSphere ausgeführt werden, müssen Sie den Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen in den Portgruppen akzeptieren, die StorageGRID-Datenverkehr beim Ausführen von RHEL unterstützen. Ubuntu oder Debian funktioniert unter den meisten Umständen ohne diese Änderungen.

Storage-Anforderungen erfüllt

Die Nodes erfordern entweder SAN-basierte oder lokale Festplattengeräte der in der folgenden Tabelle angegebenen Größen.

> ⓘ Die Zahlen in der Tabelle gelten für jeden StorageGRID-Servicetyp und nicht für das gesamte Grid oder jeden physischen Host. Basierend auf den Bereitstellungsoptionen berechnen wir die Zahlen für jeden physischen Host in, später in "Physisches Host-Layout und Anforderungen"diesem Dokument. die mit einem Sternchen markierten Pfade oder Dateisysteme werden vom Installer selbst im StorageGRID-Container erstellt. Der Administrator benötigt keine manuelle Konfiguration oder Dateisystemerstellung, aber die Hosts benötigen Blockgeräte, um diese Anforderungen zu erfüllen. Mit anderen Worten: Das Blockgerät sollte mit dem Befehl angezeigt `lsblk` werden, jedoch nicht innerhalb des Host-Betriebssystems formatiert oder gemountet sein.

Node-Typ	Zweck der LUN	Anzahl LUNs	Minimale Größe der LUN	Manuelles Dateisystem erforderlich	Vorgeschlagener Node-Konfigurationseintrag
Alle	Admin-Node-Systemspeicherplatz `/var/local` (SSD hier hilfreich)	Einer für jeden Admin-Node	90GB	Nein	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`
Alle Nodes	Docker Storage-Pool in `/var/lib/docker for container pool`	Einer für jeden Host (physisch oder VM)	100 GB pro Container	Ja – etx4	NA – Formatieren und Mounten als Host-Dateisystem (nicht im Container zugeordnet)
Admin	Audit-Protokolle für Admin-Node (Systemdaten im Admin-Container) `/var/local/audit/export`	Einer für jeden Admin-Node	200GB	Nein	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
Admin	Admin-Node-Tabellen (Systemdaten im Admin-Container) `/var/local/mysql_ibdata`	Einer für jeden Admin-Node	200GB	Nein	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
Storage-Nodes	Objekt-Storage (Block-Geräte) `/var/local/rangedb0` (SSD hier hilfreich) `/var/local/rangedb1` `/var/local/rangedb2`	Drei für jeden Lagerbehälter	4000GB	Nein	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

In diesem Beispiel sind die in der folgenden Tabelle gezeigten Festplattengrößen pro Containertyp erforderlich. Die Anforderungen pro physischem Host werden in beschrieben, später in "Physisches Host-Layout und Anforderungen"diesem Dokument.

Festplattengrößen pro Containertyp

Admin-Container

Name	Größe (gib)
Docker-Store	100 (pro Container)

Name	Größe (gib)
ADM-OS	90
Adm-Audit	200
ADM-MySQL	200

Storage-Container

Name	Größe (gib)
Docker-Store	100 (pro Container)
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

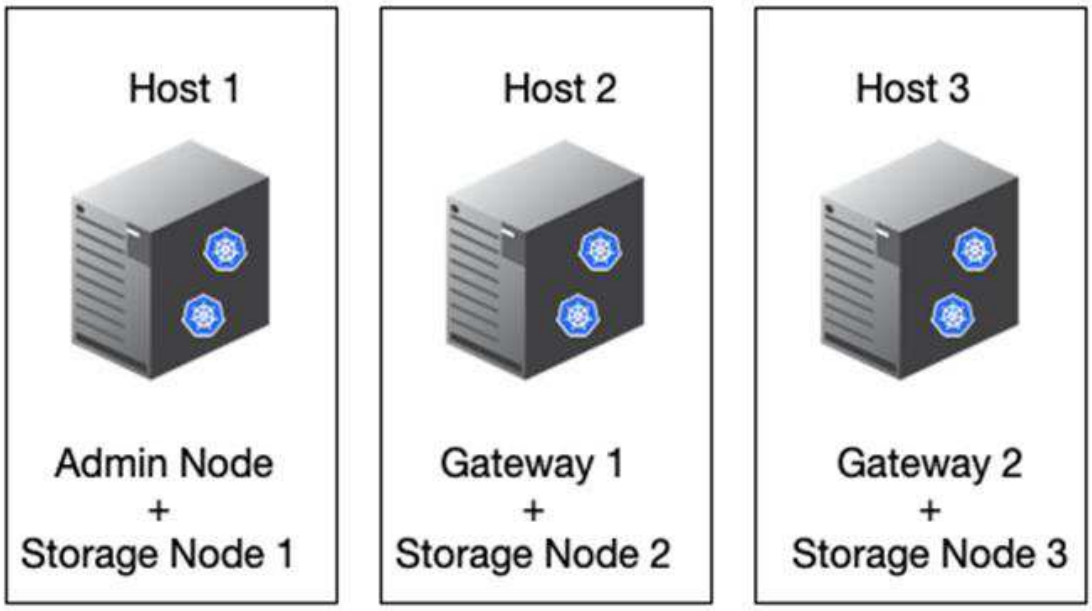
Gateway-Container

Name	Größe (gib)
Docker-Store	100 (pro Container)
/Var/local	90

Physisches Host-Layout und Anforderungen

Wenn Sie die in der obigen Tabelle aufgeführten Computing- und Netzwerkanforderungen kombinieren, erhalten Sie einen grundlegenden Hardware-Satz, der für diese Installation erforderlich ist: Drei physische (oder virtuelle) Server mit 16 Kernen, 64 GB RAM und zwei Netzwerkschnittstellen. Wenn ein höherer Durchsatz gewünscht wird, ist es möglich, zwei oder mehr Schnittstellen im Grid oder Client-Netzwerk zu verbinden und eine VLAN-getaggte Schnittstelle wie bond0.520 in der Node-Konfigurationsdatei zu verwenden. Wenn Sie mit intensiveren Workloads rechnen, ist mehr Speicher sowohl für den Host als auch für die Container besser.

Wie in der folgenden Abbildung dargestellt, hosten diese Server sechs Docker Container, zwei pro Host. Der RAM wird mithilfe von 24 GB pro Container und 16 GB für das Host-Betriebssystem selbst berechnet.



Der gesamte pro physischem Host (oder VM) erforderliche RAM beträgt 24 x 2 + 16 = 64 GB. In der folgenden Tabelle ist der erforderliche Festplattenspeicher für die Hosts 1, 2 und 3 aufgeführt.

Host 1	**Größe (gib)**
Docker Store	`/var/lib/docker` (Dateisystem)
200 (100 x 2)	**Admin-Container**
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
Lagercontainer	SN-OS `/var/local` (Gerät)
90	Rangedb-0 (Gerät)
4096	Rangedb-1 (Gerät)
4096	Rangedb-2 (Gerät)

Host 2	**Größe (gib)**
Docker Store	`/var/lib/docker` (Freigegeben)
200 (100 x 2)	**Gateway-Container**
GW-OS */`var/local`	100

Host 2	Größe (gib)
Lagercontainer	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Host 3	Größe (gib)
Docker Store	/var/lib/docker (Freigegeben)
200 (100 x 2)	**Gateway-Container**
*/var/local	100
Lagercontainer	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Der Docker Store wurde berechnet, indem 100 GB je /var/local (pro Container) x zwei Container = 200 GB zugelassen wurden.

Vorbereiten der Knoten

Um die Erstinstallation von StorageGRID vorzubereiten, installieren Sie zunächst RHEL Version 9.2 und aktivieren Sie SSH. Richten Sie Netzwerkschnittstellen, das Network Time Protocol (NTP), DNS und den Host-Namen gemäß den Best Practices ein. Sie benötigen mindestens eine aktivierte Netzwerkschnittstelle im Grid-Netzwerk und eine weitere für das Client-Netzwerk. Wenn Sie eine VLAN-getaggte Schnittstelle verwenden, konfigurieren Sie sie wie in den folgenden Beispielen. Andernfalls genügt eine einfache Konfiguration der Standard-Netzwerkschnittstelle.

Wenn Sie ein VLAN-Tag auf der Grid-Netzwerkschnittstelle verwenden müssen, sollte Ihre Konfiguration zwei Dateien im folgenden Format haben /etc/sysconfig/network-scripts/ :

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

In diesem Beispiel wird davon ausgegangen, dass Ihr physisches Netzwerkgerät für das Grid-Netzwerk enp67s0 ist. Es könnte auch ein gebundenes Gerät wie bond0 sein. Unabhängig davon, ob Sie Bonding oder eine Standard-Netzwerkschnittstelle verwenden, müssen Sie die VLAN-getaggte Schnittstelle in Ihrer Node-Konfigurationsdatei verwenden, wenn Ihr Netzwerkport kein Standard-VLAN hat oder wenn das Standard-VLAN nicht mit dem Grid-Netzwerk verknüpft ist. Der StorageGRID-Container selbst entkennzeichnet keine Ethernet-Frames, daher muss er vom übergeordneten Betriebssystem verarbeitet werden.

Optionale Speichereinrichtung mit iSCSI

Wenn Sie keinen iSCSI-Speicher verwenden, müssen Sie sicherstellen, dass host1, host2 und host3 Blockgeräte von ausreichender Größe enthalten, um ihre Anforderungen zu erfüllen. Informationen zu den Speicheranforderungen für host1, host2 und host3 finden Sie unter "Festplattengrößen pro Containertyp" .

Gehen Sie wie folgt vor, um Speicher mit iSCSI einzurichten:

Schritte

1. Wenn Sie externen iSCSI-Speicher wie NetApp E-Serie oder NetApp ONTAP® Datenmanagement-Software verwenden, installieren Sie die folgenden Pakete:

   ```
   sudo yum install iscsi-initiator-utils
   sudo yum install device-mapper-multipath
   ```

2. Suchen Sie auf jedem Host nach der Initiator-ID.

   ```
   # cat /etc/iscsi/initiatorname.iscsi
   InitiatorName=iqn.2006-04.com.example.node1
   ```

3. Ordnen Sie unter Verwendung des Initiatornamens aus Schritt 2 den einzelnen Storage-Nodes LUNs auf Ihrem Speichergerät (der in der Tabelle angegebenen Anzahl und Größe "Storage-Anforderungen erfüllt") zu.

4. Ermitteln Sie die neu erstellten LUNs mit `iscsiadm` und melden Sie sich bei ihnen an.

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

Weitere Informationen finden Sie "Erstellen eines iSCSI-Initiators" im Red hat Customer Portal.

5. Führen Sie den folgenden Befehl aus, um die Multipath-Geräte und ihre zugehörigen LUN-WWIDs anzuzeigen:

```
# multipath -ll
```

Wenn Sie iSCSI nicht mit Multipath-Geräten verwenden, mounten Sie Ihr Gerät einfach mit einem eindeutigen Pfadnamen, der Änderungen am Gerät und Neustarts beibehalten wird.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

Die einfache Verwendung von `/dev/sdx` Gerätenamen kann später Probleme verursachen, wenn Geräte entfernt oder hinzugefügt werden. Wenn Sie Multipath-Geräte verwenden, ändern Sie die `/etc/multipath.conf` Datei wie folgt, um Aliase zu verwenden.

Diese Geräte sind je nach Layout möglicherweise auf allen Knoten vorhanden oder nicht.

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

Bevor Sie Docker in Ihrem Host-Betriebssystem installieren, formatieren Sie die LUN oder die Festplatten-Backups, und mounten `/var/lib/docker`Sie sie. Die anderen LUNs sind in der Node-Konfigurationsdatei definiert und werden direkt von den StorageGRID Containern verwendet. Das heißt, sie werden nicht im Host-Betriebssystem angezeigt; sie erscheinen in den Containern selbst, und diese Dateisysteme werden vom Installer verwaltet.

Wenn Sie eine iSCSI-gestützte LUN verwenden, platzieren Sie etwas Ähnliches wie die folgende Zeile in Ihrer

fstab-Datei. Wie bereits erwähnt, müssen die anderen LUNs nicht im Host-Betriebssystem gemountet werden, sondern müssen als verfügbare Blockgeräte angezeigt werden.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Vorbereiten der Docker-Installation

Gehen Sie wie folgt vor, um die Installation von Docker vorzubereiten:

Schritte

1. Erstellen Sie auf allen drei Hosts ein Filesystem auf dem Docker Storage-Volume.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   Wenn Sie iSCSI-Geräte mit Multipath verwenden, verwenden Sie `/dev/mapper/Docker-Store`.

2. Bereitstellungspunkt für das Docker Storage-Volume erstellen:

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. Fügen Sie einen ähnlichen Eintrag für das Docker-Storage-Volume-device zu hinzu `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   Die folgende `_netdev` Option wird nur empfohlen, wenn Sie ein iSCSI-Gerät verwenden. Wenn Sie ein lokales Blockgerät verwenden `_netdev` , ist dies nicht erforderlich und `defaults` wird empfohlen.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. Mounten Sie das neue Dateisystem und zeigen Sie die Festplattennutzung an.

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. Schalten Sie den Swap aus und deaktivieren Sie ihn aus Leistungsgründen.

   ```
   $ sudo swapoff --all
   ```

6. Um die Einstellungen beizubehalten, entfernen Sie alle Swap-Einträge aus /etc/fstab, z. B.:

```
/dev/mapper/rhel-swap swap defaults 0 0
```

> Wenn Sie den Auslagerungsaustausch nicht vollständig deaktivieren, kann die Leistung erheblich gesenkt werden.

7. Führen Sie einen Testneustart des Node durch, um sicherzustellen, dass das `/var/lib/docker` Volume persistent ist und alle Festplattengeräte wieder verfügbar sind.

Installieren Sie Docker für StorageGRID

Erfahren Sie, wie Sie Docker für StorageGRID installieren.

Gehen Sie wie folgt vor, um Docker zu installieren:

Schritte

1. Konfigurieren Sie den yum repo für Docker.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. Installieren Sie die benötigten Pakete.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Starten Sie Docker.

```
sudo systemctl start docker
```

4. Docker Testen.

```
sudo docker run hello-world
```

5. Stellen Sie sicher, dass Docker beim Systemstart ausgeführt wird.

```
sudo systemctl enable docker
```

Vorbereiten der Node-Konfigurationsdateien für StorageGRID

Erfahren Sie, wie Sie die Node-Konfigurationsdateien für StorageGRID vorbereiten.

Die Node-Konfiguration umfasst im allgemeinen die folgenden Schritte:

Schritte

1. Erstellen Sie das `/etc/storagegrid/nodes` Verzeichnis auf allen Hosts.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. Erstellen Sie die erforderlichen Dateien pro physischem Host, um sie dem Layout von Container/Node-Typ anzupassen. In diesem Beispiel haben wir zwei Dateien pro physischem Host auf jedem Hostcomputer erstellt.

> Der Name der Datei definiert den tatsächlichen Node-Namen für die Installation. Wird zum Beispiel `dc1-adm1.conf` zu einem Knoten mit dem Namen `dc1-adm1`.

— Host1:
`dc1-adm1.conf`
`dc1-sn1.conf`

— Host2:
`dc1-gw1.conf`
`dc1-sn2.conf`

— Host3:
`dc1-gw2.conf`
`dc1-sn3.conf`

Vorbereiten der Node-Konfigurationsdateien

Die folgenden Beispiele verwenden das `/dev/disk/by-path` Format. Sie können die korrekten Pfade überprüfen, indem Sie die folgenden Befehle ausführen:

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

Und diese Befehle:

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

Beispiel für primären Admin-Node

Beispiel für einen Dateinamen:

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

Inhalt der Beispieldatei:

> Festplattenpfade können den folgenden Beispielen folgen oder Stilnamen verwenden `/dev/mapper/alias` . Verwenden Sie keine Blockgerätnamen, z. B. `/dev/sdb` weil sie sich beim Neustart ändern können und das Raster beschädigen können.

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Beispiel für einen Storage-Node

Beispiel für einen Dateinamen:

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

Inhalt der Beispieldatei:

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

Beispiel für Gateway Node

Beispiel für einen Dateinamen:

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

Inhalt der Beispieldatei:

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Installieren von StorageGRID-Abhängigkeiten und -Paketen

Erfahren Sie, wie Sie StorageGRID-Abhängigkeiten und -Pakete installieren.

Um die StorageGRID-Abhängigkeiten und -Pakete zu installieren, führen Sie die folgenden Befehle aus:

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

Validieren Sie die StorageGRID-Konfigurationsdateien

Erfahren Sie, wie Sie den Inhalt der Konfigurationsdateien für StorageGRID validieren.

Nachdem Sie die Konfigurationsdateien in für jeden Ihrer StorageGRID Nodes erstellt `/etc/storagegrid/nodes` haben, müssen Sie den Inhalt dieser Dateien validieren.

Um den Inhalt der Konfigurationsdateien zu validieren, führen Sie folgenden Befehl auf jedem Host aus:

```
sudo storagegrid node validate all
```

Wenn die Dateien korrekt sind, wird in der Ausgabe für jede Konfigurationsdatei ÜBERGEBEN angezeigt:

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Wenn die Konfigurationsdateien nicht korrekt sind, werden die Probleme als WARNUNG und FEHLER angezeigt. Wenn Konfigurationsfehler gefunden werden, müssen Sie sie korrigieren, bevor Sie mit der Installation fortfahren.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Starten Sie den StorageGRID Host Service

Erfahren Sie, wie Sie den StorageGRID Host Service starten.

Um die StorageGRID-Nodes zu starten und sicherzustellen, dass sie nach einem Neustart des Hosts neu gestartet werden, müssen Sie den StorageGRID-Hostdienst aktivieren und starten.

Führen Sie zum Starten des StorageGRID Host Service die folgenden Schritte aus.

Schritte

1. Führen Sie auf jedem Host folgende Befehle aus:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

   Der Startvorgang kann bei der ersten Ausführung einige Zeit in Anspruch nehmen.

2. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Bereitstellung fortgesetzt wird:

```
sudo storagegrid node status node-name
```

3. Führen Sie für jeden Knoten, der den Status oder zurückgibt `Not-Running` `Stopped`, den folgenden Befehl aus:

```
sudo storagegrid node start node-name
```

   Beispielsweise würden Sie angesichts der folgenden Ausgabe den Node starten `dc1-adm1` :

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. Wenn Sie den StorageGRID-Host-Service bereits aktiviert und gestartet haben (oder wenn Sie nicht sicher sind, ob der Service aktiviert und gestartet wurde), führen Sie auch den folgenden Befehl aus:

```
sudo systemctl reload-or-restart storagegrid
```

Konfigurieren Sie den Grid-Manager in StorageGRID

Erfahren Sie, wie Sie den Grid-Manager in StorageGRID auf dem primären Admin-Node konfigurieren.

Schließen Sie die Installation ab, indem Sie das StorageGRID-System über die Grid Manager-Benutzeroberfläche auf dem primären Admin-Node konfigurieren.

Allgemeine Schritte

Das Konfigurieren des Grids und das Abschließen der Installation umfassen die folgenden Aufgaben:

Schritte

1. Navigieren Sie zu Grid Manager
2. "Geben Sie die StorageGRID Lizenzinformationen an"
3. "Fügen Sie Sites zu StorageGRID hinzu"
4. "Subnetze für das Grid-Netzwerk angeben"
5. "Ausstehende Grid-Nodes genehmigen"
6. "Geben Sie die NTP-Serverinformationen an"
7. "Geben Sie die Serverinformationen des DNS-Systems an"
8. "Geben Sie die Passwörter für das StorageGRID-System an"
9. "Überprüfung der Konfiguration und vollständige Installation"

Navigieren Sie zu Grid Manager

Definieren Sie mit dem Grid Manager alle Informationen, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Bevor Sie beginnen, muss der primäre Admin-Node bereitgestellt und die erste Startsequenz abgeschlossen sein.

Führen Sie die folgenden Schritte aus, um mit Grid Manager Informationen zu definieren.

Schritte

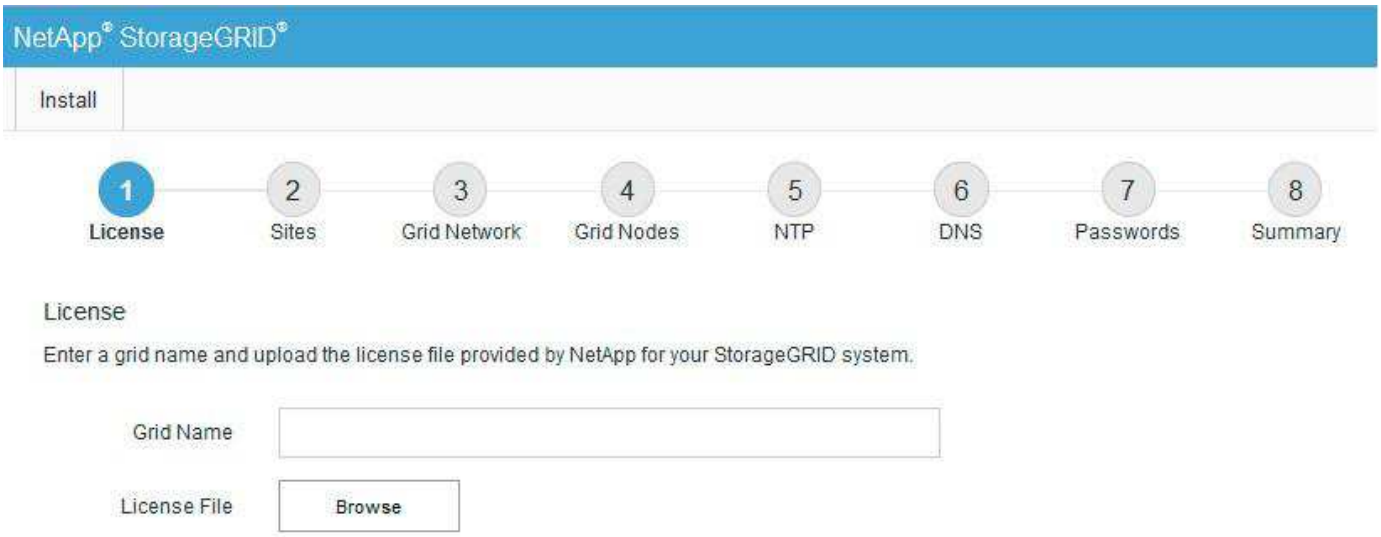
1. Greifen Sie über die folgende Adresse auf den Grid Manager zu:

   ```
   https://primary_admin_node_grid_ip
   ```

   Alternativ können Sie auf den Grid Manager auf Port 8443 zugreifen.

   ```
   https://primary_admin_node_ip:8443
   ```

2. Klicken Sie auf StorageGRID-System installieren. Die Seite, die zum Konfigurieren eines StorageGRID-Rasters verwendet wird, wird angezeigt.



Details zur StorageGRID-Lizenz hinzufügen

Erfahren Sie, wie Sie die StorageGRID Lizenzdatei hochladen.

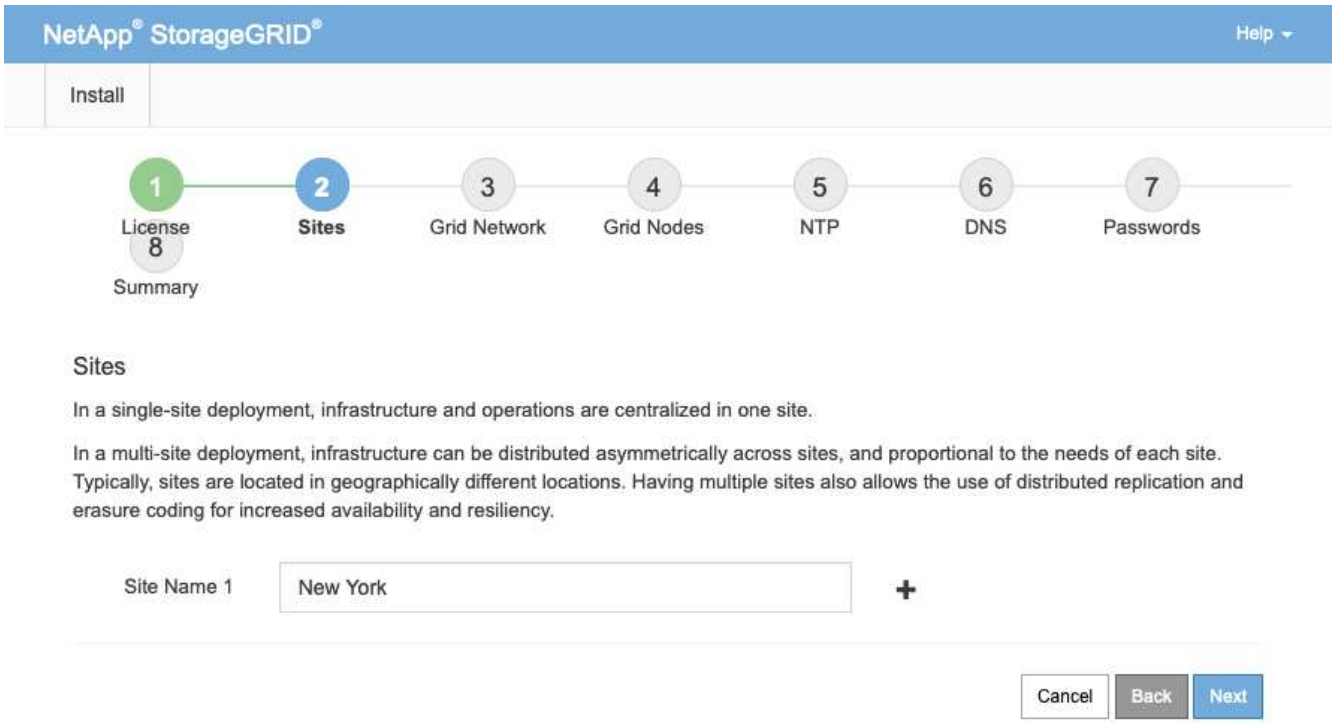
Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Gehen Sie wie folgt vor, um die StorageGRID-Lizenzinformationen anzugeben:

Schritte

1. Geben Sie auf der Lizenzseite im Feld Rastername einen Namen für Ihr StorageGRID-System ein. Nach der Installation wird der Name als oberste Ebene in der Grid-Topologiestruktur angezeigt.
2. Klicken Sie auf Durchsuchen, suchen Sie die NetApp-Lizenzdatei (`NLF-unique-id.txt`) und klicken Sie auf Öffnen. Die Lizenzdatei wird validiert, die Seriennummer und die lizenzierte Speicherkapazität werden angezeigt.

> Das StorageGRID Installationsarchiv enthält eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet. Sie können nach der Installation auf eine Lizenz aktualisieren, die Support bietet.



3. Klicken Sie Auf Weiter.

Fügen Sie Sites zu StorageGRID hinzu

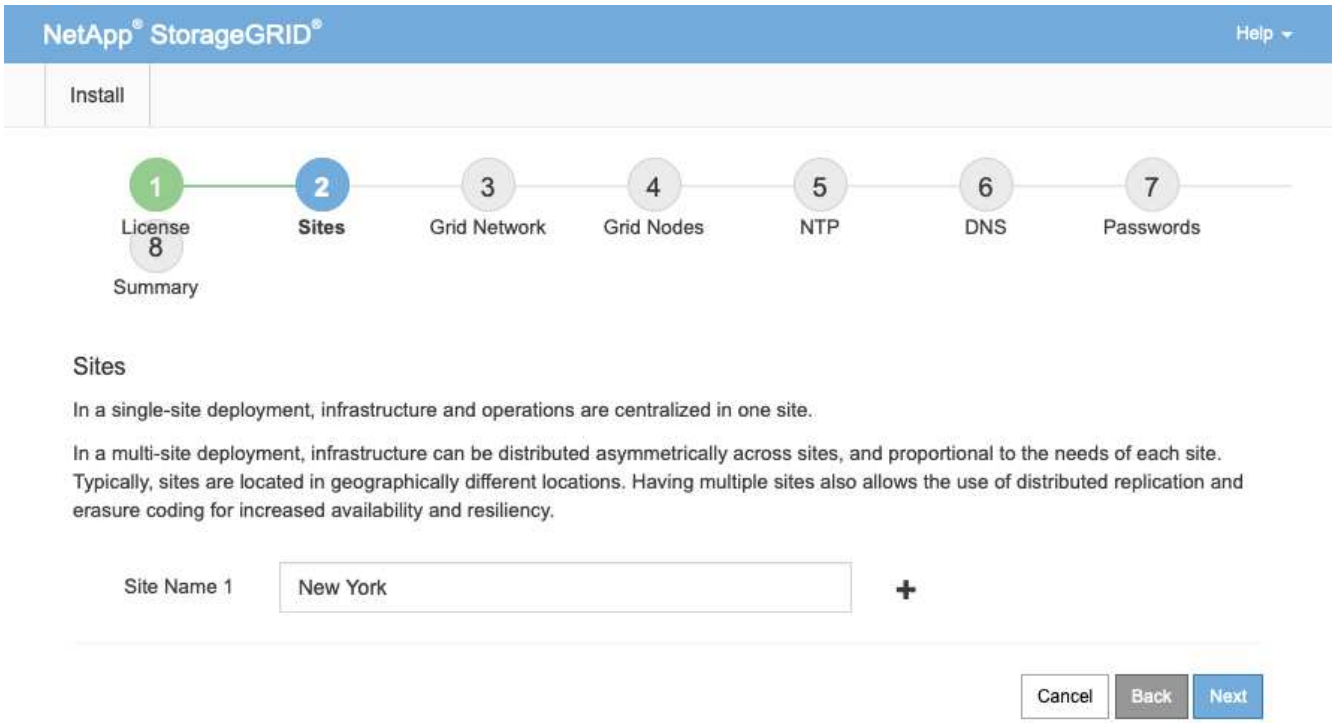
Erfahren Sie, wie Sie StorageGRID Standorte hinzufügen, um die Zuverlässigkeit und Storage-Kapazität zu verbessern.

Wenn Sie StorageGRID installieren, müssen Sie mindestens einen Standort erstellen. Sie können weitere Standorte erstellen, um die Zuverlässigkeit und Storage-Kapazität Ihres StorageGRID Systems zu erhöhen.

So fügen Sie Sites hinzu:

Schritte

1. Geben Sie auf der Seite Sites den Standortnamen ein.
2. Um weitere Sites hinzuzufügen, klicken Sie auf das Pluszeichen neben dem letzten Standorteintrag, und geben Sie den Namen in das Textfeld „Neuer Standortname“ ein. Fügen Sie so viele zusätzliche Standorte wie für Ihre Grid-Topologie hinzu. Sie können bis zu 16 Standorte hinzufügen.



3. Klicken Sie Auf Weiter.

Grid-Netzwerk-Subnetze für StorageGRID angeben

Erfahren Sie, wie Sie die Grid-Netzwerk-Subnetze für StorageGRID konfigurieren.

Sie müssen die Subnetze angeben, die im Grid-Netzwerk verwendet werden.

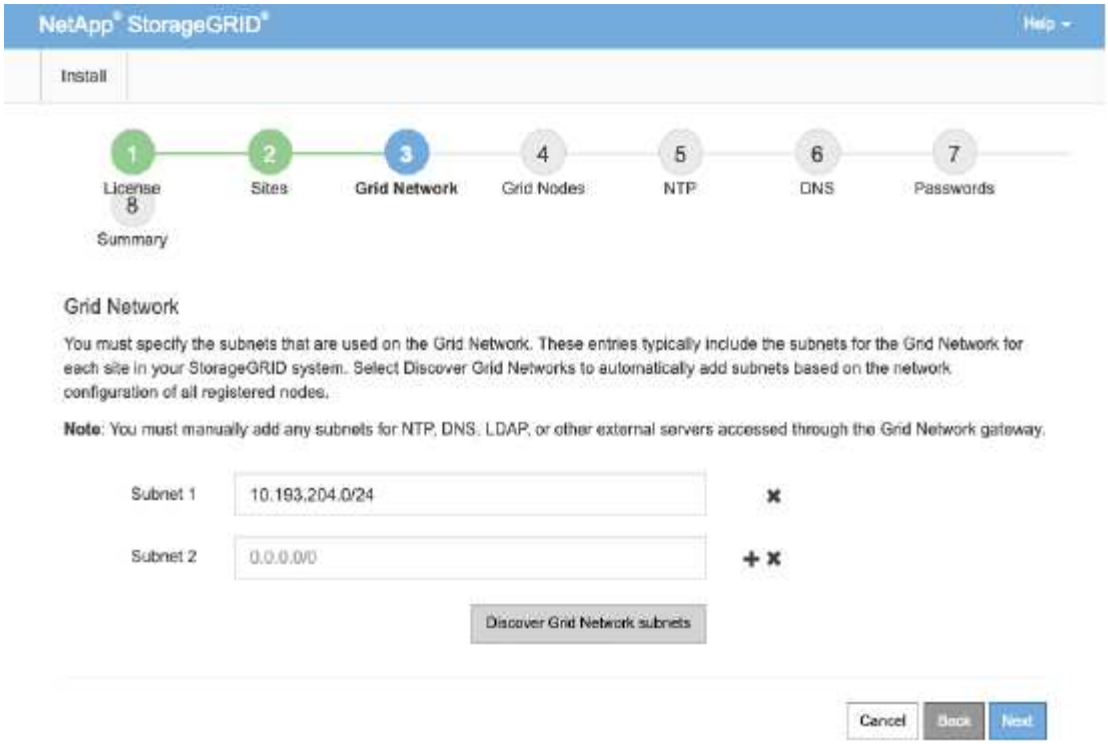
Die Subnetzeinträge umfassen die Subnetze für das Grid-Netzwerk für jeden Standort im StorageGRID-System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen (z. B. die Subnetze, auf denen Ihre NTP-Server gehostet werden).

Wenn Sie mehrere Grid-Subnetze haben, ist das Grid-Netzwerk-Gateway erforderlich. Alle angegebenen Grid-Subnetze müssen über dieses Gateway erreichbar sein.

Führen Sie die folgenden Schritte aus, um Subnetze für das Grid-Netzwerk anzugeben:

Schritte

1. Geben Sie im Textfeld Subnetz 1 die CIDR-Netzwerkadresse für mindestens ein Grid-Netzwerk an.
2. Klicken Sie auf das Pluszeichen neben dem letzten Eintrag, um einen zusätzlichen Netzwerkeintrag hinzuzufügen. Wenn Sie bereits mindestens einen Knoten bereitgestellt haben, klicken Sie auf Subnetze von Grid Networks ermitteln, um die Subnetzliste des Grid-Netzwerks automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die bei Grid Manager registriert sind.



3. Klicken Sie Auf Weiter.

Grid-Nodes für StorageGRID genehmigen

Erfahren Sie, wie Sie ausstehende Grid-Nodes, die dem StorageGRID-System beitreten, prüfen und genehmigen.

Sie müssen jeden Grid-Node genehmigen, bevor er dem StorageGRID-System Beitritt.

Bevor Sie beginnen, müssen alle Grid-Nodes der virtuellen und StorageGRID-Appliance implementiert werden.

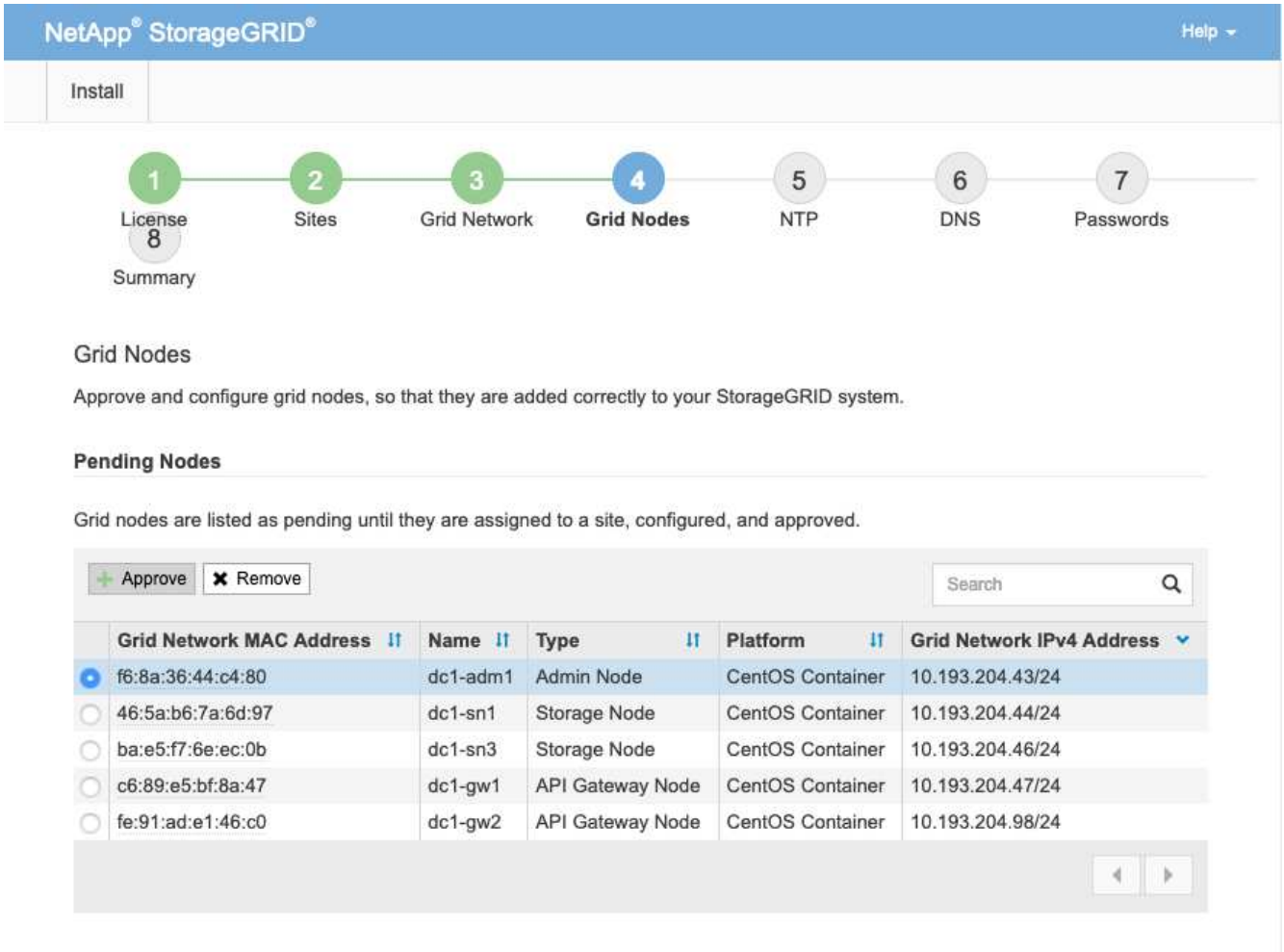
Führen Sie die folgenden Schritte aus, um ausstehende Rasterknoten zu genehmigen:

Schritte

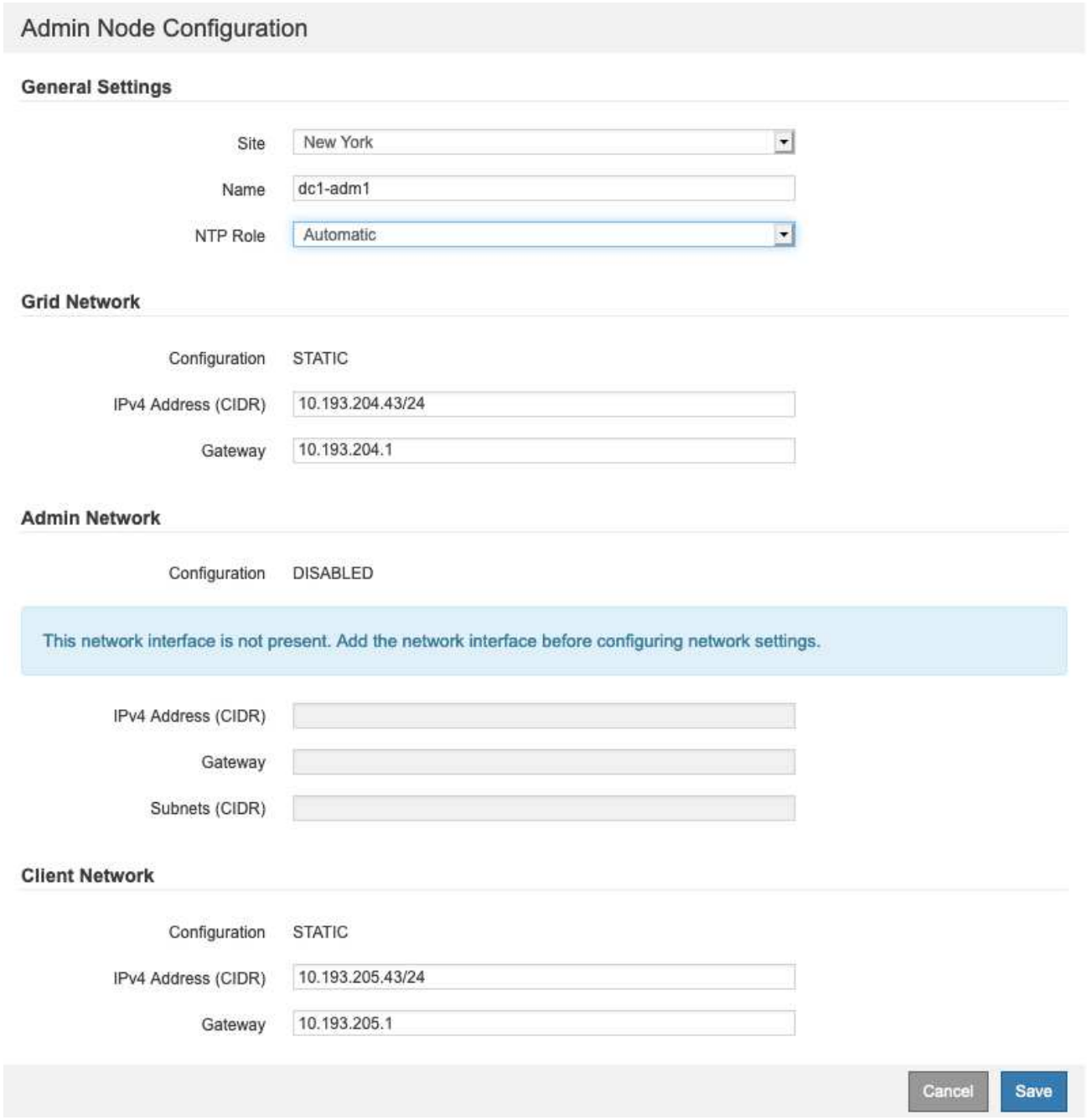
1. Überprüfen Sie die Liste Ausstehende Knoten, und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

   Wenn ein Grid-Node fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

2. Klicken Sie auf das Optionsfeld neben einem ausstehenden Knoten, den Sie genehmigen möchten.



3. Klicken Sie Auf Genehmigen.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften nach Bedarf.



— **Standort**: Der Systemname des Standorts für diesen Grid-Knoten.

— **Name**: Der Hostname, der dem Knoten zugewiesen wird, und der Name, der im Grid-Manager angezeigt wird. Der Name wird standardmäßig mit dem Namen verwendet, den Sie während der Node-Bereitstellung angegeben haben. Sie können den Namen jedoch bei Bedarf ändern.

— **NTP-Rolle**: Die NTP-Rolle des Grid-Knotens. Die Optionen lauten automatisch, Primär und Client. Durch Auswahl der Option automatisch wird die primäre Rolle den Administratorknoten, den Speicher-Nodes mit ADC-Diensten (Administrative Domain Controller), den Gateway-Nodes und allen Grid-Nodes mit nicht statischen IP-Adressen zugewiesen. Allen anderen Grid-Nodes wird die Client-Rolle zugewiesen.

Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

— **ADC-Dienst (nur Speicher-Nodes)**: Wählen Sie automatisch, damit das System bestimmen kann, ob der Knoten den ADC-Dienst benötigt. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Speicherknoten an jedem Standort müssen den ADC-Dienst enthalten. Der ADC-Dienst kann nicht einem Node hinzugefügt werden, nachdem er bereitgestellt wurde.

5. Ändern Sie in Grid Network die Einstellungen für die folgenden Eigenschaften nach Bedarf:

   — **IPv4-Adresse (CIDR)**: Die CIDR-Netzwerkadresse für die Netzschnittstelle (eth0 im Container). `192.168.1.234/24`Beispiel: .

   — **Gateway**: Das Grid Network Gateway. `192.168.0.1`Beispiel: .

   Wenn mehrere Grid-Subnetze vorhanden sind, ist das Gateway erforderlich.

   Wenn Sie DHCP für die Grid-Netzwerkkonfiguration ausgewählt haben und den Wert hier ändern, wird der neue Wert als statische Adresse auf dem Node konfiguriert. Stellen Sie sicher, dass sich die resultierende IP-Adresse nicht in einem DHCP-Adressenpool befindet.

6. Um das Admin-Netzwerk für den Grid-Knoten zu konfigurieren, fügen Sie die Einstellungen im Abschnitt Admin-Netzwerk nach Bedarf hinzu oder aktualisieren Sie diese.

   Geben Sie die Zielsubnetze der Routen aus dieser Schnittstelle in das Textfeld Subnetze (CIDR) ein. Wenn es mehrere Admin-Subnetze gibt, ist das Admin-Gateway erforderlich.

   Wenn Sie für die Netzwerkkonfiguration für den Admin DHCP ausgewählt haben und diesen Wert hier ändern, wird der neue Wert als statische Adresse auf dem Node konfiguriert. Stellen Sie sicher, dass sich die resultierende IP-Adresse nicht in einem DHCP-Adressenpool befindet.

   Appliances: Wenn bei einer StorageGRID-Appliance das Admin-Netzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Dialogfeld des Grid-Managers konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

   a. Starten Sie die Appliance neu: Wählen Sie im Installationsprogramm der Appliance die Option MENU:Advanced[Neustart]. Ein Neustart kann mehrere Minuten dauern.
   b. Wählen Sie MENU:Configure Networking [Link Configuration], und aktivieren Sie die entsprechenden Netzwerke.
   c. Wählen Sie MENU:Configure Networking[IP Configuration], und konfigurieren Sie die aktivierten Netzwerke.
   d. Kehren Sie zur Startseite zurück, und klicken Sie auf Installation starten.
   e. Im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.
   f. Entfernen Sie den Knoten aus der Tabelle Ausstehende Knoten.
   g. Warten Sie, bis der Knoten wieder in der Liste Ausstehende Knoten angezeigt wird.

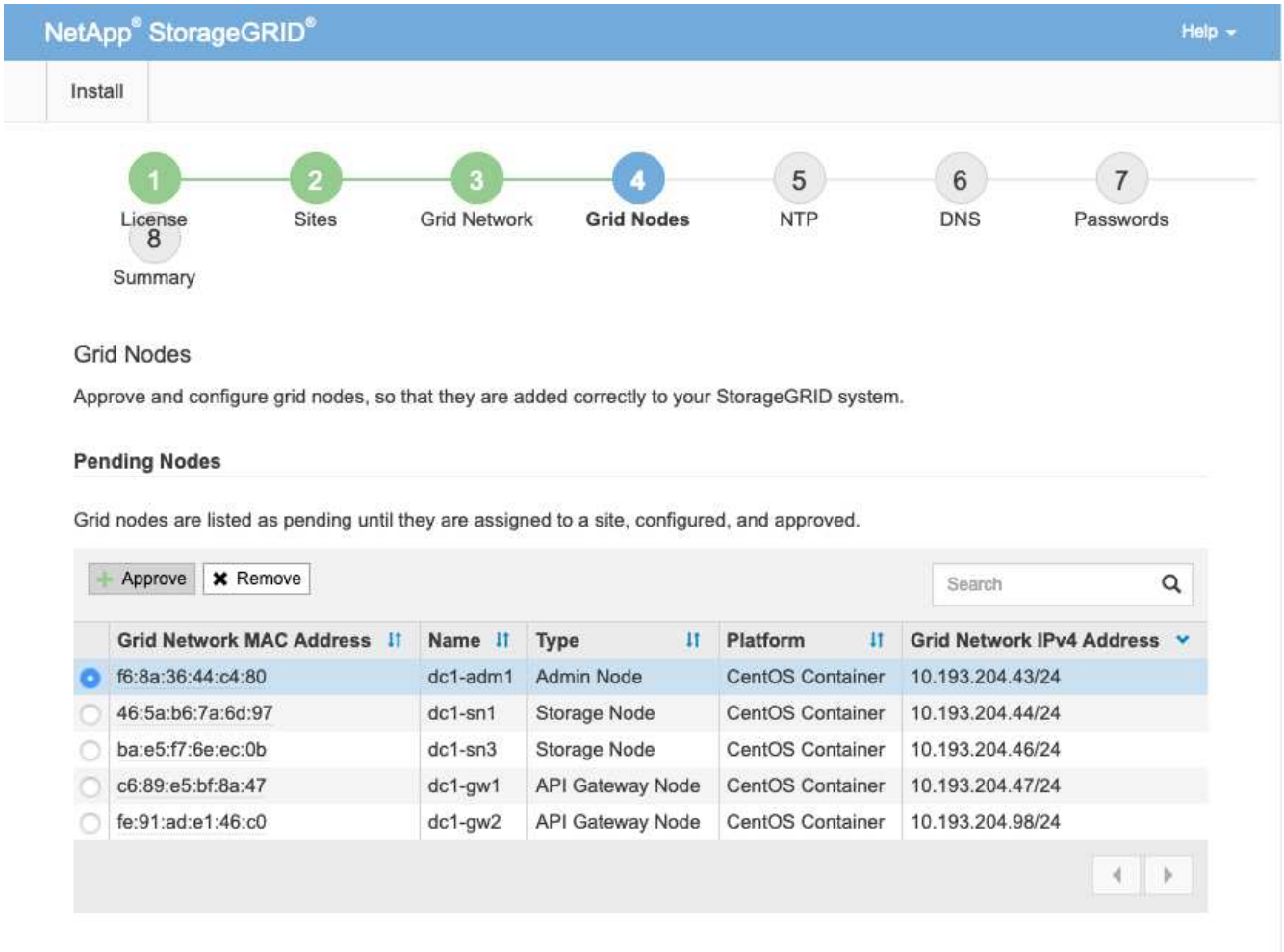
h. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration angegeben haben. Weitere Informationen finden Sie in der Installations- und Wartungsanleitung für Ihr Gerätemodell.

7. Wenn Sie das Client-Netzwerk für den Grid-Node konfigurieren möchten, fügen Sie die Einstellungen im Abschnitt Client-Netzwerk nach Bedarf hinzu oder aktualisieren Sie sie. Wenn das Client-Netzwerk konfiguriert ist, ist das Gateway erforderlich, und es wird nach der Installation zum Standard-Gateway für den Node.

   Appliances: Wenn bei einer StorageGRID-Appliance das Clientnetzwerk bei der Erstinstallation nicht mit dem StorageGRID-Gerät-Installationsprogramm konfiguriert wurde, kann es nicht in diesem Dialogfeld des Grid-Managers konfiguriert werden. Stattdessen müssen Sie folgende Schritte ausführen:

   a. Starten Sie die Appliance neu: Wählen Sie im Installationsprogramm der Appliance die Option MENU:Advanced[Neustart]. Ein Neustart kann mehrere Minuten dauern.
   b. Wählen Sie MENU:Configure Networking [Link Configuration], und aktivieren Sie die entsprechenden Netzwerke.
   c. Wählen Sie MENU:Configure Networking[IP Configuration], und konfigurieren Sie die aktivierten Netzwerke.
   d. Kehren Sie zur Startseite zurück, und klicken Sie auf Installation starten.
   e. Im Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.
   f. Entfernen Sie den Knoten aus der Tabelle Ausstehende Knoten.
   g. Warten Sie, bis der Knoten wieder in der Liste Ausstehende Knoten angezeigt wird.
   h. Vergewissern Sie sich, dass Sie die entsprechenden Netzwerke konfigurieren können. Sie sollten bereits mit den Informationen ausgefüllt werden, die Sie auf der Seite IP-Konfiguration angegeben haben. Weitere Informationen finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

8. Klicken Sie auf Speichern . Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



9. Wiederholen Sie die Schritte 1-8 für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

   Sie müssen alle Knoten genehmigen, die Sie im Raster benötigen. Sie können jedoch jederzeit zu dieser Seite zurückkehren, bevor Sie auf der Seite Zusammenfassung auf Installieren klicken. Um die Eigenschaften eines genehmigten Gitterknotens zu ändern, klicken Sie auf das entsprechende Optionsfeld und anschließend auf Bearbeiten.

10. Wenn Sie die Genehmigung für Rasterknoten abgeschlossen haben, klicken Sie auf Weiter.

Geben Sie NTP-Serverdetails für StorageGRID an

Erfahren Sie, wie Sie NTP-Konfigurationsinformationen für Ihr StorageGRID-System angeben, damit Vorgänge auf separaten Servern synchronisiert werden können.

Um Probleme mit Zeitabweichungen zu vermeiden, müssen Sie vier externe NTP-Serverreferenzen von Stratum 3 oder höher angeben.

> Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer Windows-Version als Windows Server 2016. Der Zeitdienst in früheren Versionen von Windows ist nicht ausreichend genau und wird von Microsoft nicht für den Einsatz in anspruchsvollen Umgebungen wie StorageGRID unterstützt.

Die externen NTP-Server werden von den Nodes verwendet, denen Sie zuvor die primären NTP-Rollen

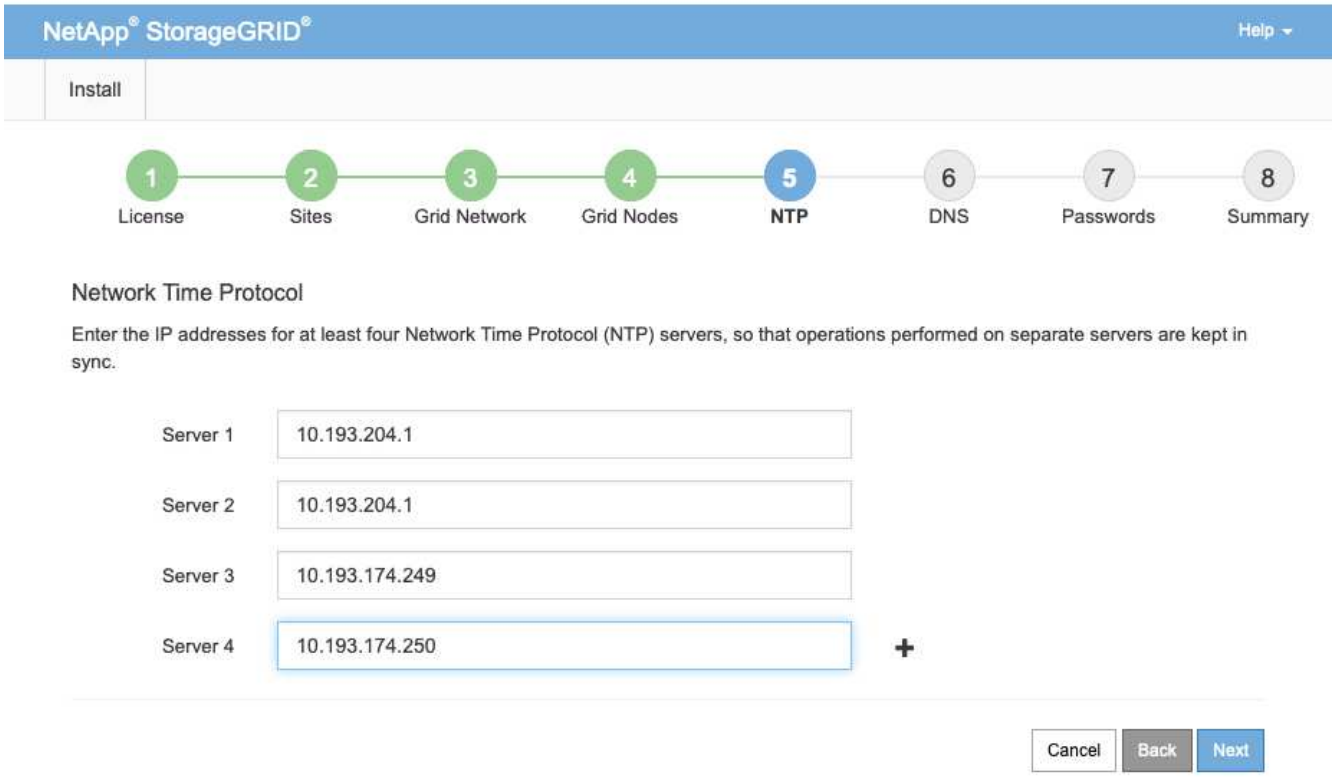
zugewiesen haben.

> Das Client-Netzwerk wird im Installationsvorgang nicht früh genug aktiviert, um die einzige Quelle für NTP-Server zu sein. Stellen Sie sicher, dass mindestens ein NTP-Server über das Grid-Netzwerk oder das Admin-Netzwerk erreicht werden kann.

Führen Sie die folgenden Schritte aus, um NTP-Serverinformationen anzugeben:

Schritte

1. Geben Sie in den Textfeldern Server 1 bis Server 4 die IP-Adressen für mindestens vier NTP-Server an.
2. Klicken Sie bei Bedarf auf das Pluszeichen neben dem letzten Eintrag, um weitere Servereinträge hinzuzufügen.



3. Klicken Sie Auf Weiter.

Geben Sie Details zum DNS-Server für StorageGRID an

Erfahren Sie, wie Sie den DNS-Server für StorageGRID konfigurieren.

Sie müssen die DNS-Informationen für Ihr StorageGRID-System angeben, damit Sie mithilfe von Hostnamen anstelle von IP-Adressen auf externe Server zugreifen können.

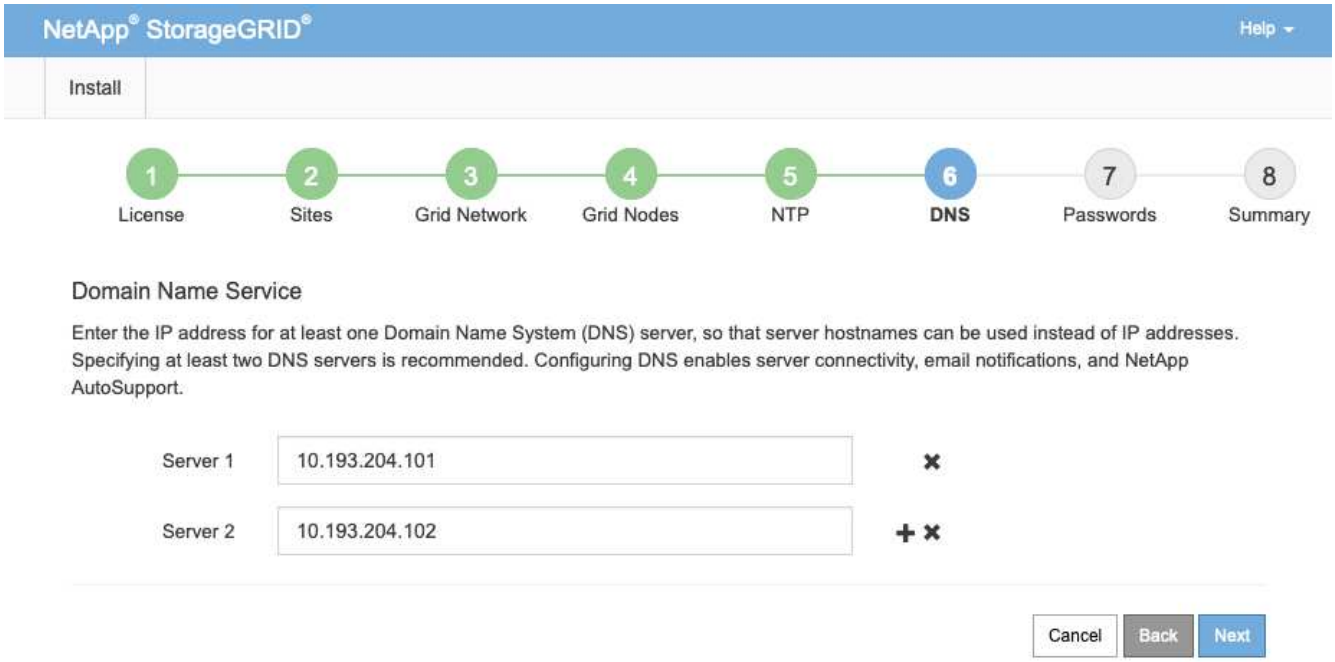
Durch die Angabe von DNS-Serverinformationen können Sie vollständig qualifizierte Domänennamen (FQDN) statt IP-Adressen für E-Mail-Benachrichtigungen und NetApp AutoSupport®-Nachrichten verwenden. NetApp empfiehlt die Angabe von mindestens zwei DNS-Servern.

Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet.

Führen Sie die folgenden Schritte aus, um DNS-Serverinformationen anzugeben:

Schritte

1. Geben Sie im Textfeld Server 1 die IP-Adresse für einen DNS-Server an.
2. Klicken Sie bei Bedarf auf das Pluszeichen neben dem letzten Eintrag, um weitere Server hinzuzufügen.



3. Klicken Sie Auf Weiter.

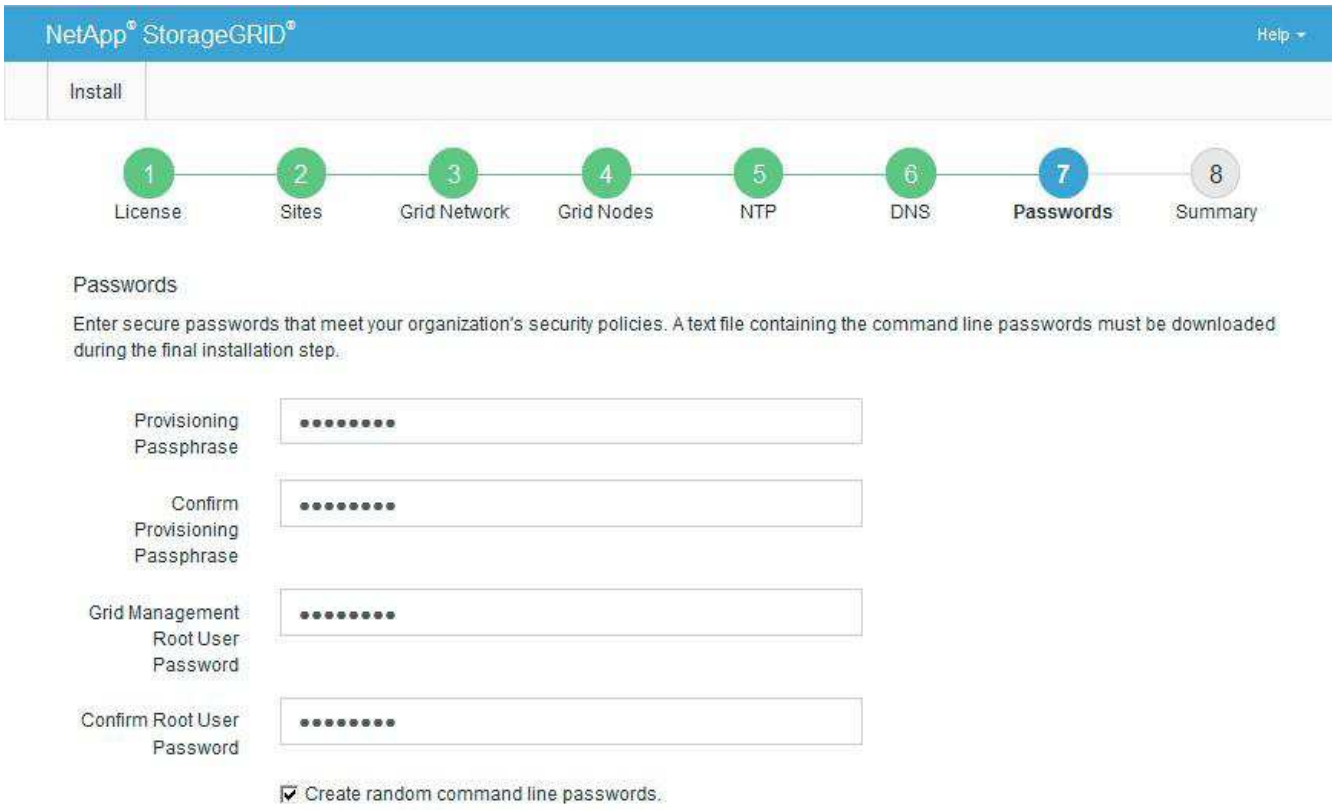
Geben Sie die Systemkennwörter für StorageGRID an

Erfahren Sie, wie Sie Ihr StorageGRID-System sichern, indem Sie die Passphrase für das Provisioning und das Root-Benutzerpasswort für das Grid-Management festlegen.

So geben Sie die Passwörter ein, die zum Schutz Ihres StorageGRID-Systems verwendet werden sollen:

Schritte

1. Geben Sie in Provisioning Passphrase die Provisionierungs-Passphrase ein, die für Änderungen an der Grid-Topologie des StorageGRID-Systems erforderlich ist. Sie sollten dieses Kennwort an einem sicheren Ort speichern.
2. Geben Sie unter Provisionierungspassphrase bestätigen die Provisionierungs-Passphrase erneut ein.
3. Geben Sie unter Grid Management Root User Password das Passwort ein, das für den Zugriff auf Grid Manager als Root-Benutzer verwendet werden soll.
4. Geben Sie unter Root-Benutzerpasswort bestätigen das Grid Manager-Kennwort erneut ein.



5. Wenn Sie ein Raster für Proof-of-Concept- oder Demo-Zwecke installieren, deaktivieren Sie die Option „Random Command Line Passwords erstellen“.

   Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Deaktivieren Sie die Option Random Command Line Passwords erstellen nur für Demo-Raster, wenn Sie Standardpasswörter verwenden möchten, um über die Befehlszeile mithilfe des Root- oder Administratorkontos auf Grid-Nodes zuzugreifen.

   > Wenn Sie auf der Seite Zusammenfassung auf Installieren klicken, werden Sie aufgefordert, die Wiederherstellungspaket-Datei herunterzuladen (`sgws-recovery-package-id-revision.zip`). Sie müssen diese Datei herunterladen, um die Installation abzuschließen. Die Passwörter für den Zugriff auf das System werden in der in der Recovery Package-Datei enthaltenen Datei gespeichert `Passwords.txt` .

6. Klicken Sie Auf Weiter.

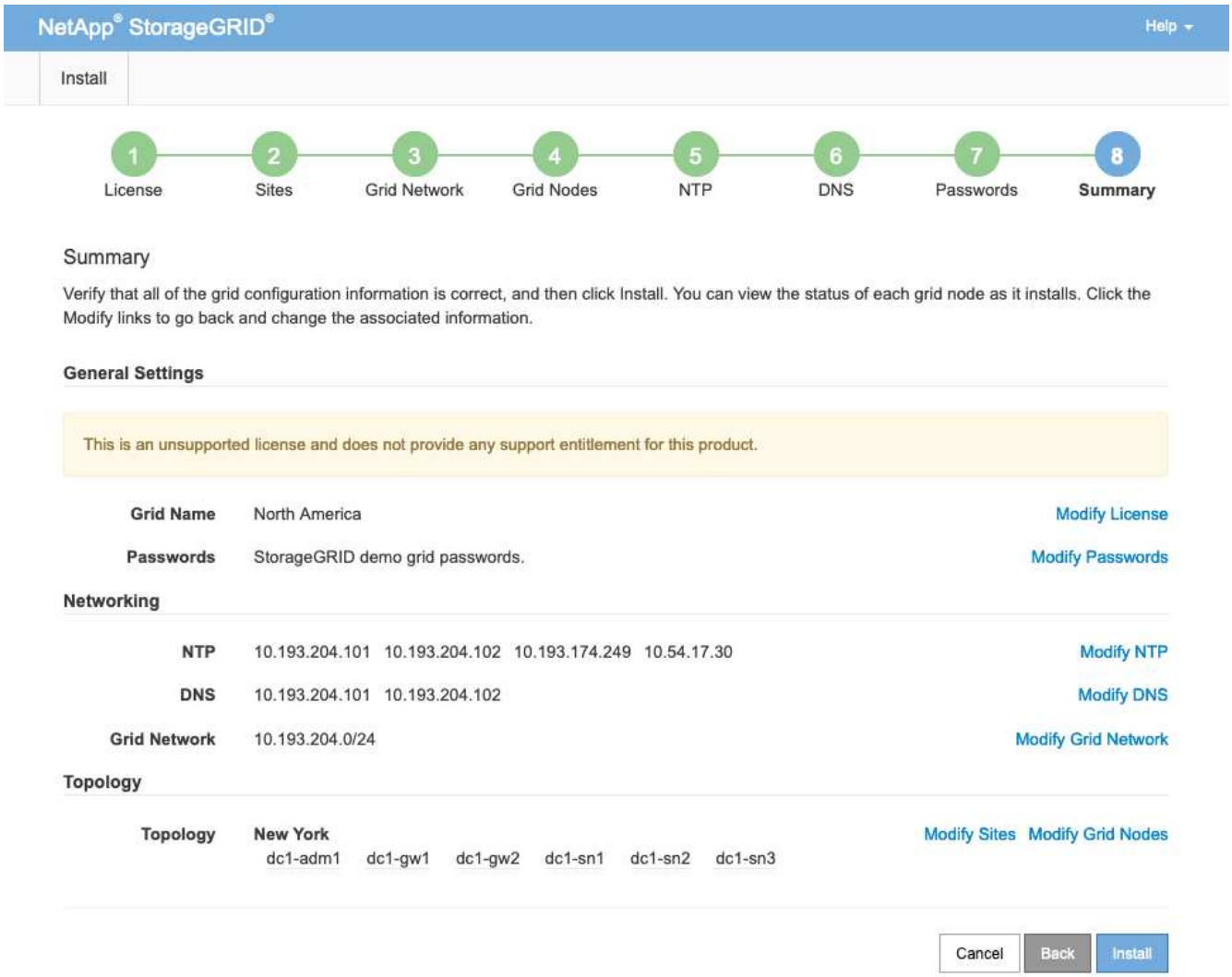
Überprüfen Sie die Konfiguration und schließen Sie die StorageGRID Installation ab

Erfahren Sie, wie Sie die Grid-Konfigurationsinformationen validieren und den StorageGRID Installationsprozess abschließen.

Um sicherzustellen, dass die Installation erfolgreich abgeschlossen wird, überprüfen Sie die von Ihnen eingegebenen Konfigurationsinformationen sorgfältig. Auszuführende Schritte:

Schritte

1. Zeigen Sie die Übersichtsseite an.



2. Vergewissern Sie sich, dass alle Informationen zur Grid-Konfiguration korrekt sind. Verwenden Sie die Links zum Ändern auf der Seite Zusammenfassung, um zurück zu gehen und Fehler zu beheben.
3. Klicken Sie Auf Installieren.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf Installieren klicken. Wenn die Verbindung unterbrochen wird, stellen Sie sicher, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Weitere Informationen finden Sie unter „Netzwerkinstallation und -Bereitstellung“.

4. Klicken Sie Auf Wiederherstellungspaket Herunterladen.

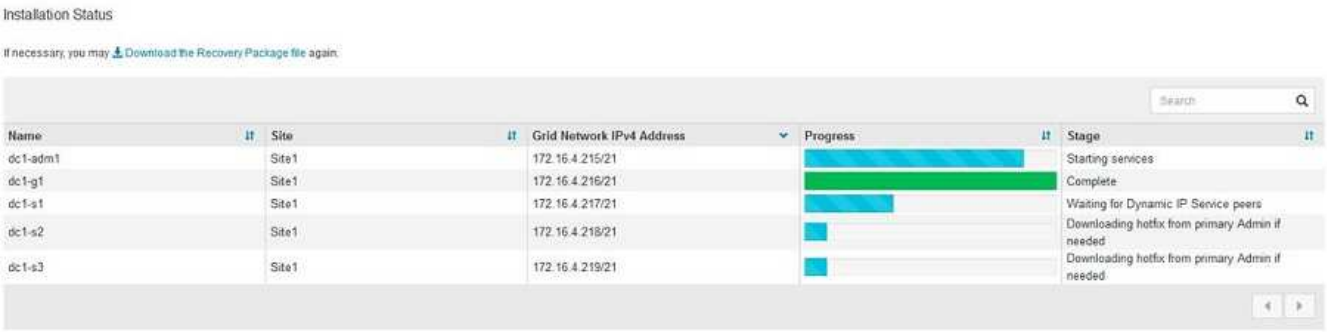
   Wenn die Installation bis zu dem Punkt fortschreitet, an dem die Rastertopologie definiert ist, werden Sie aufgefordert, die Wiederherstellungspaket-Datei herunterzuladen (`.zip`) und zu bestätigen, dass Sie auf den Inhalt dieser Datei zugreifen können. Sie müssen die Wiederherstellungspaket-Datei herunterladen, damit Sie das StorageGRID-System wiederherstellen können, falls ein oder mehrere Grid-Nodes ausfallen.

   Vergewissern Sie sich, dass Sie den Inhalt der Datei extrahieren und anschließend an zwei sicheren und separaten Speicherorten speichern können `.zip` .

Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

5. Wählen Sie die Option Ich habe die Wiederherstellungspaket-Datei erfolgreich heruntergeladen und verifiziert, und klicken Sie dann auf Weiter.

Wenn die Installation noch läuft, wird die Seite Installationsstatus geöffnet. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



Wenn die komplette Phase für alle Grid-Knoten erreicht ist, wird die Anmeldeseite für Grid Manager geöffnet.

6. Melden Sie sich beim Grid Manager als Root-Benutzer mit dem Passwort an, das Sie bei der Installation angegeben haben.

Upgrade von Bare-Metal-Nodes in StorageGRID

Erfahren Sie mehr über den Upgrade-Prozess für Bare-Metal-Nodes in StorageGRID.

Der Upgrade-Prozess für Bare-Metal-Nodes unterscheidet sich von dem für Appliances oder VMware Nodes. Bevor Sie ein Upgrade eines Bare-Metal-Knotens durchführen, müssen Sie zunächst die RPM-Dateien auf allen Hosts aktualisieren, bevor Sie das Upgrade über die GUI ausführen.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

Jetzt können Sie mit dem Software-Upgrade über die GUI fortfahren.

TR-4907: Konfigurieren Sie StorageGRID mit veritas Enterprise Vault

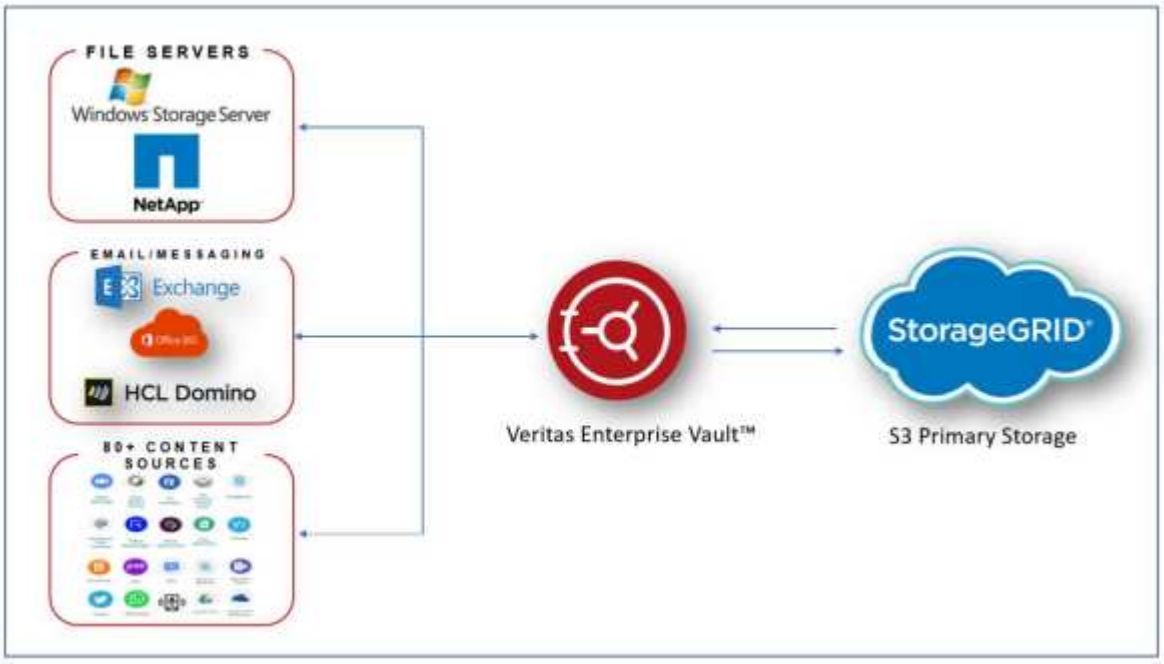
Einführung in die Konfiguration von StorageGRID für Site Failover

Erfahren Sie, wie veritas Enterprise Vault StorageGRID als primäres Storage-Ziel für Disaster Recovery verwendet.

Diese Konfigurationsanleitung enthält die Schritte zur Konfiguration von NetApp® StorageGRID® als primäres Speicherziel mit veritas Enterprise Vault. Es wird auch beschrieben, wie StorageGRID für ein Standort-Failover in einem Disaster Recovery-Szenario (DR) konfiguriert wird.

Referenzarchitektur von NetApp dar

StorageGRID bietet ein lokales, S3-kompatibles Cloud-Backup-Ziel für veritas Enterprise Vault. Die folgende Abbildung zeigt die Architektur von veritas Enterprise Vault und StorageGRID.



Wo Sie weitere Informationen finden

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

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/

- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Konfigurieren Sie StorageGRID und veritas Enterprise Vault

Erfahren Sie, wie Sie grundlegende Konfigurationen für StorageGRID 11.5 oder höher und veritas Enterprise Vault 14.1 oder höher implementieren.

Dieser Konfigurationsleitfaden basiert auf StorageGRID 11.5 und Enterprise Vault 14.1. Für WORM-Modus (Write Once, Read Many) wurde Storage mit S3 Object Lock, StorageGRID 11.6 und Enterprise Vault 14.2.2 verwendet. Weitere Details zu diesen Richtlinien finden Sie auf der "StorageGRID-Dokumentation" Seite oder bei einem StorageGRID Experten.

Voraussetzungen für die Konfiguration von StorageGRID und veritas Enterprise Vault

- Bevor Sie StorageGRID mit veritas Enterprise Vault konfigurieren, überprüfen Sie die folgenden Voraussetzungen:

> Für WORM Storage (Objektsperre) ist StorageGRID 11.6 oder höher erforderlich.

- veritas Enterprise Vault 14.1 oder höher ist installiert.

> Für WORM Storage (Object Lock) ist Enterprise Vault ab Version 14.2.2 erforderlich.

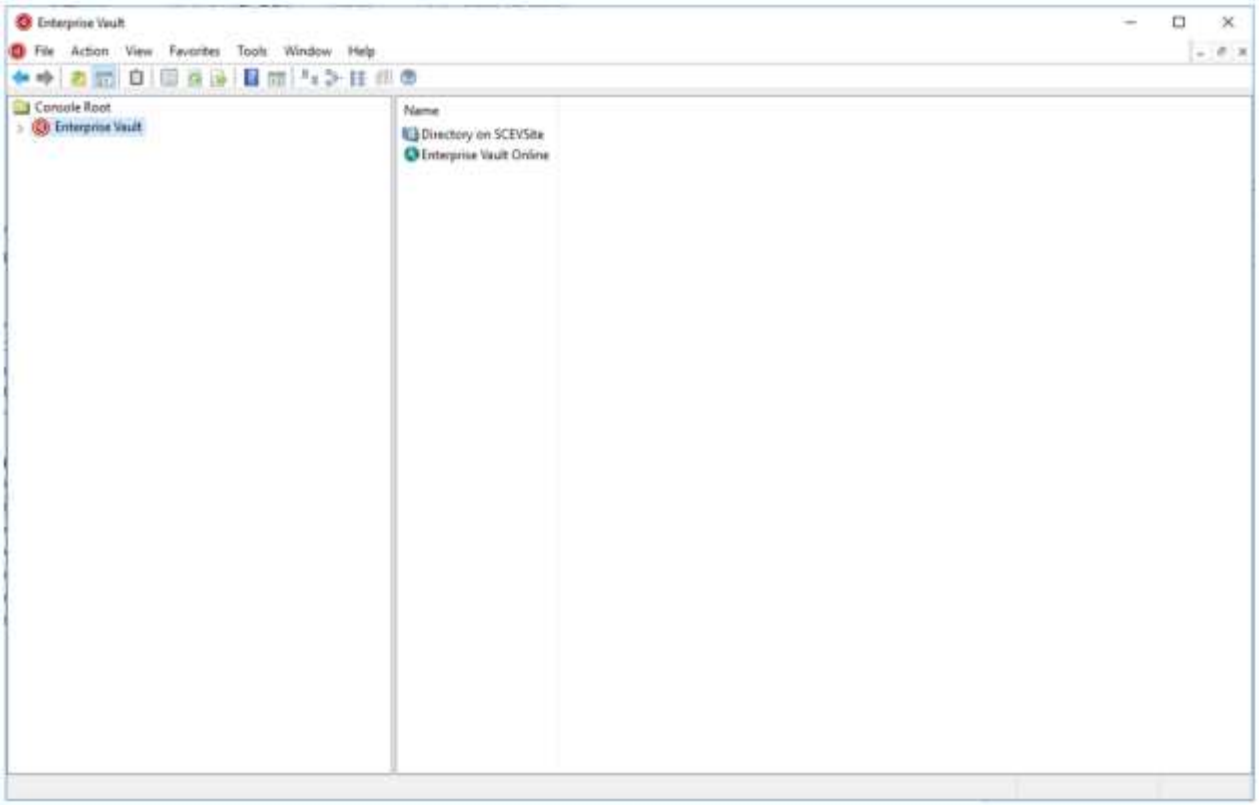
- Vault-Speichergruppen und ein Vault-Speicher wurden erstellt. Weitere Informationen finden Sie im veritas Enterprise Vault Administration Guide.
- Ein StorageGRID-Mandant, Zugriffsschlüssel, geheimer Schlüssel und Bucket wurden erstellt.
- Ein StorageGRID-Load-Balancer-Endpunkt wurde erstellt (entweder HTTP oder HTTPS).
- Wenn Sie ein selbstsigniertes Zertifikat verwenden, fügen Sie das selbstsignierte StorageGRID-CA-Zertifikat zu den Enterprise Vault-Servern hinzu. Weitere Informationen finden Sie in diesem "Artikel der veritas Knowledge Base".
- Aktualisieren Sie die aktuelle Enterprise Vault-Konfigurationsdatei, und wenden Sie sie an, um unterstützte Speicherlösungen wie NetApp StorageGRID zu ermöglichen. Weitere Informationen finden Sie in diesem "Artikel der veritas Knowledge Base".

Konfigurieren Sie StorageGRID mit veritas Enterprise Vault

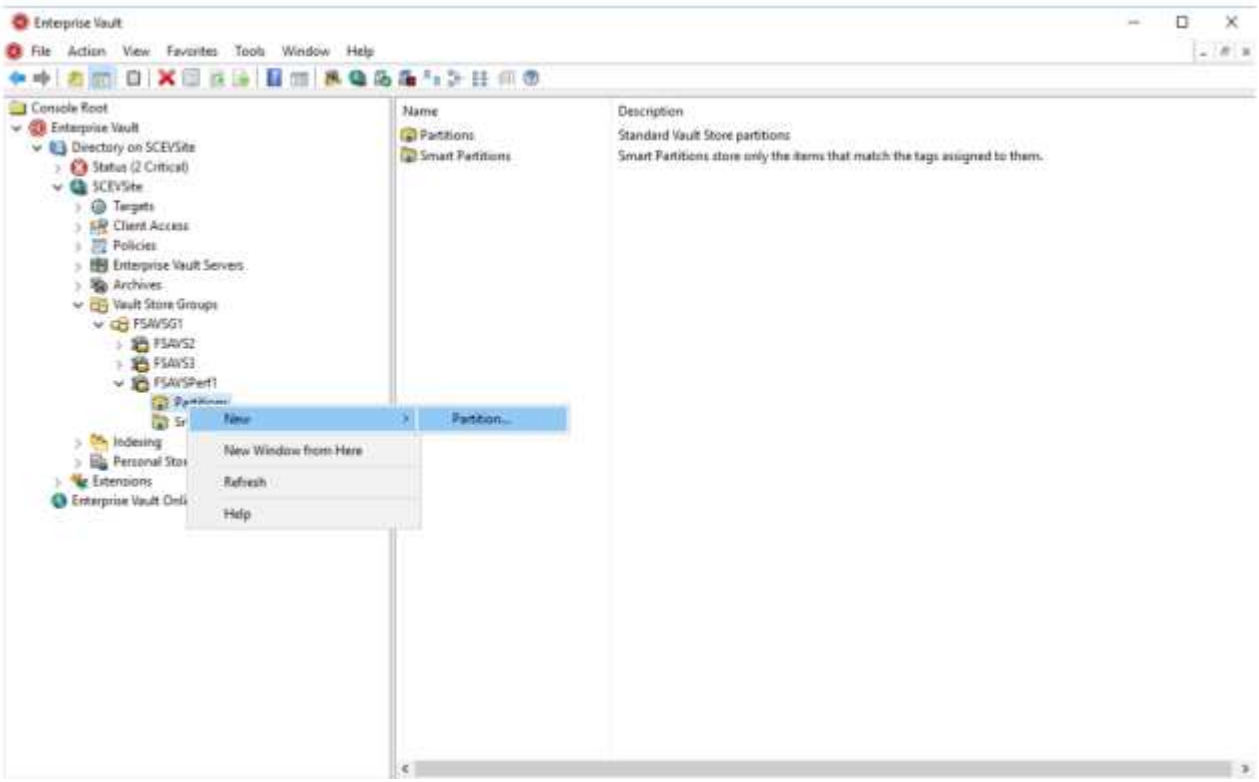
So konfigurieren Sie StorageGRID mit veritas Enterprise Vault:

Schritte

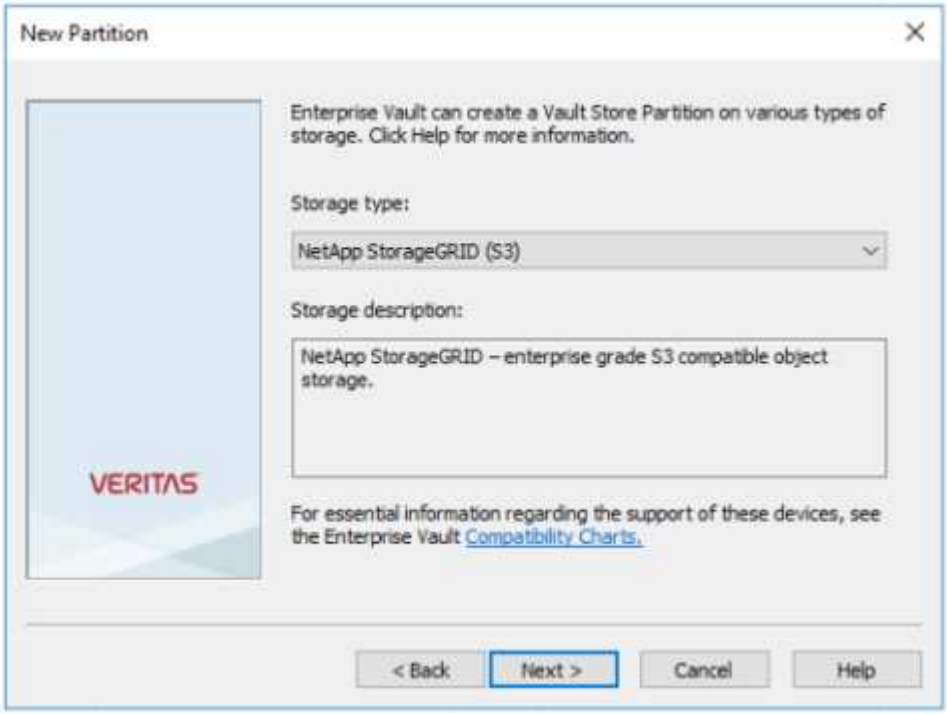
1. Starten Sie die Enterprise Vault Administration-Konsole.



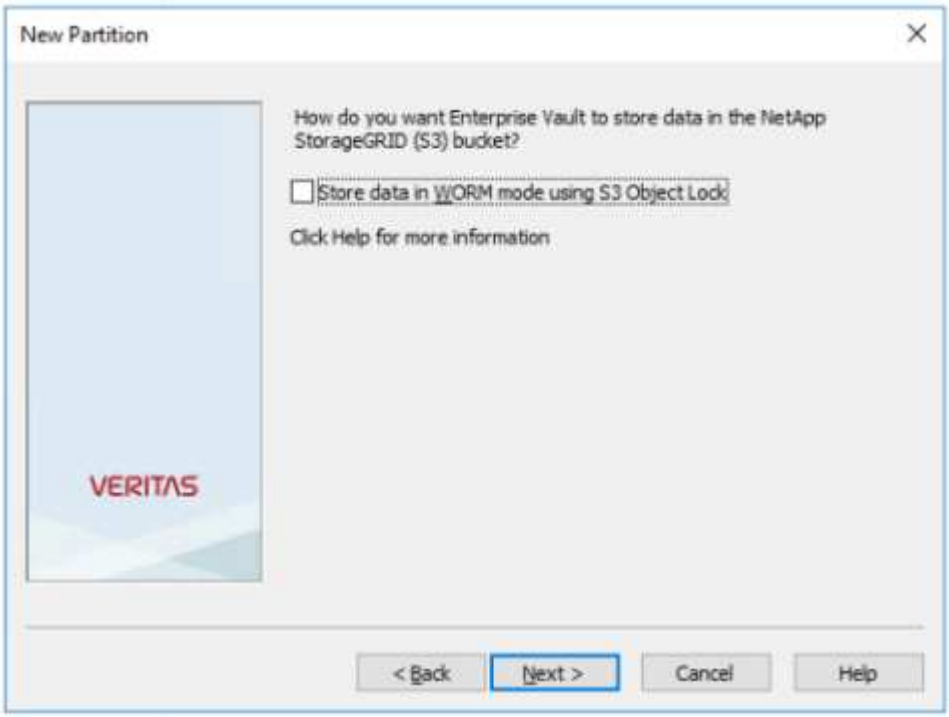
2. Erstellen Sie eine neue Vault-Speicherpartition im entsprechenden Vault-Speicher. Erweitern Sie den Ordner Vault Store Groups und anschließend den entsprechenden Vault-Speicher. Klicken Sie mit der rechten Maustaste auf Partition, und wählen Sie MENU:New[Partition].



3. Folgen Sie dem Assistenten zum Erstellen neuer Partitionen. Wählen Sie aus dem Dropdown-Menü Speichertyp die Option NetApp StorageGRID (S3) aus. Klicken Sie Auf Weiter.

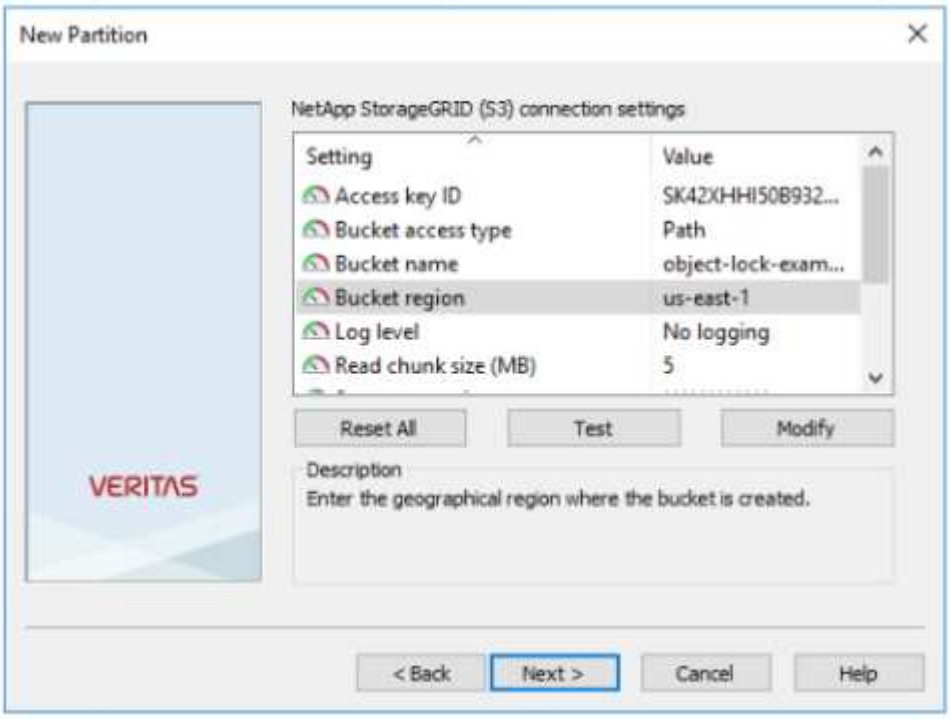


4. Lassen Sie die Option Daten im WORM-Modus mit S3 Objektsperre speichern deaktiviert. Klicken Sie Auf Weiter.



5. Geben Sie auf der Seite Verbindungseinstellungen folgende Informationen ein:
   - Zugriffsschlüssel-ID
   - Geheimer Zugriffsschlüssel
   - Service-Host-Name: Stellen Sie sicher, dass der in StorageGRID konfigurierte Load Balancer-Endpunkt (LBE)-Port (z. B. https://<hostname>:<LBE_port>) einbezogen wird.

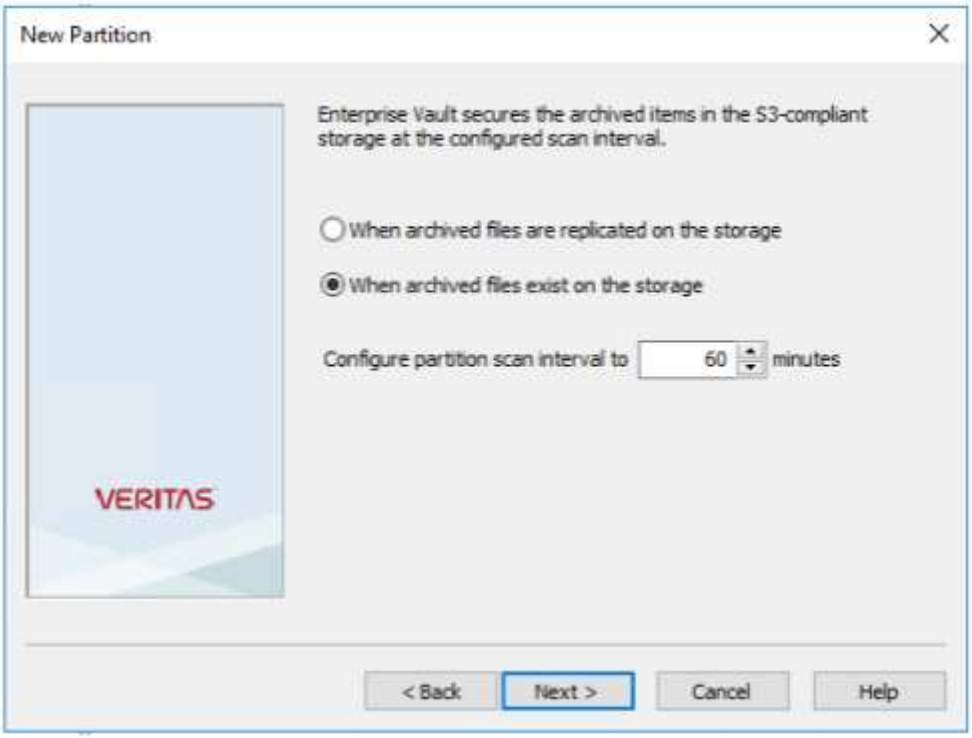
- Bucket-Name: Name des zuvor erstellten Ziel-Buckets. veritas Enterprise Vault erstellt den Bucket nicht.
- Bucket-Region: `us-east-1` Ist der Standardwert.



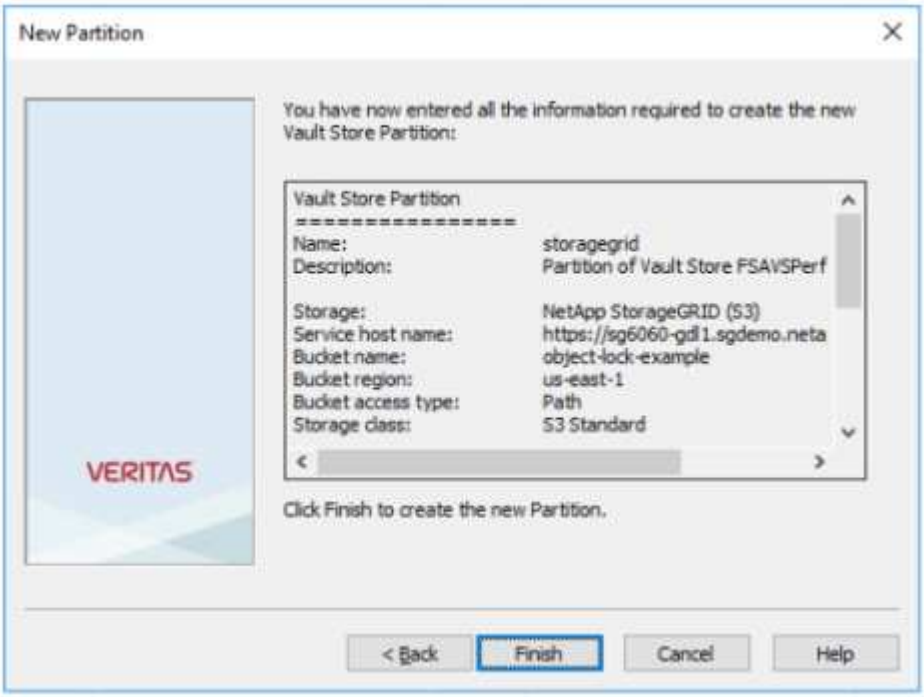
6. Um die Verbindung zum StorageGRID-Bucket zu überprüfen, klicken Sie auf Test. Überprüfen Sie, ob der Verbindungstest erfolgreich war. Klicken Sie auf OK und dann auf Weiter.

7. StorageGRID unterstützt den S3-Replizierungsparameter nicht. Zum Schutz Ihrer Objekte verwendet StorageGRID Regeln für Information Lifecycle Management (ILM), um Datensicherungsschemata festzulegen – mehrere Kopien oder Erasure Coding. Wählen Sie die Option Wenn archivierte Dateien im

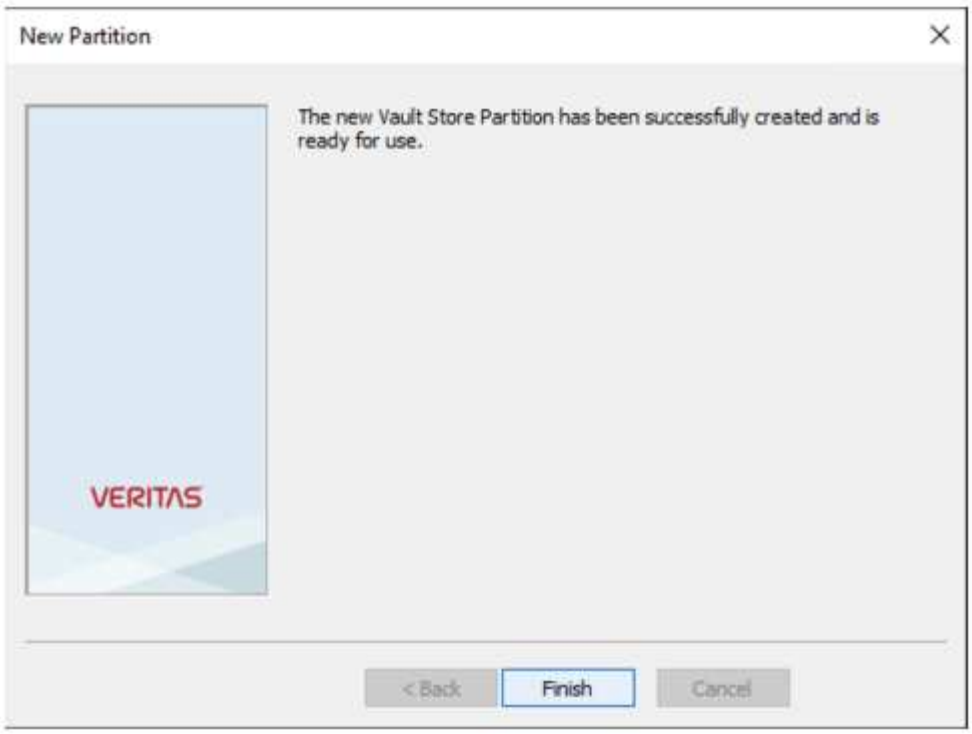
Speicher vorhanden sind aus, und klicken Sie auf Weiter.



8. Überprüfen Sie die Informationen auf der Übersichtsseite, und klicken Sie auf Fertig stellen.



9. Nachdem die neue Vault-Speicherpartition erfolgreich erstellt wurde, können Sie Daten in Enterprise Vault mit StorageGRID als primärem Speicher archivieren, wiederherstellen und suchen.



Konfigurieren Sie die StorageGRID S3 Objektsperre für WORM Storage

Erfahren Sie, wie Sie StorageGRID für WORM-Storage mit S3 Object Lock konfigurieren.

Voraussetzungen für die Konfiguration von StorageGRID für WORM Storage

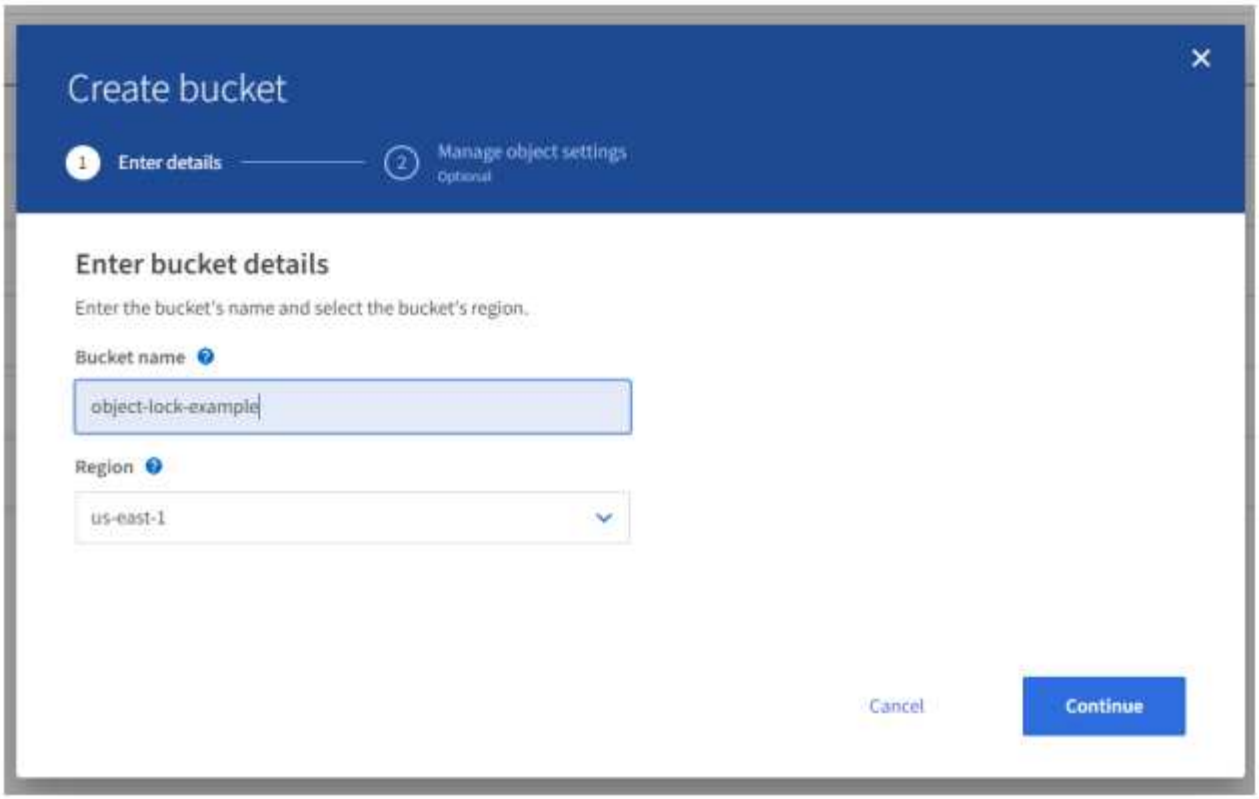
Bei WORM-Storage verwendet StorageGRID S3 Objektsperre, um Objekte zwecks Compliance aufzubewahren. Dies erfordert StorageGRID 11.6 oder höher. Dabei wurde die standardmäßige S3 Object Lock Bucket-Aufbewahrung eingeführt. Enterprise Vault erfordert außerdem Version 14.2.2 oder höher.

Konfigurieren Sie die standardmäßige Bucket-Aufbewahrung von StorageGRID S3 Object Lock

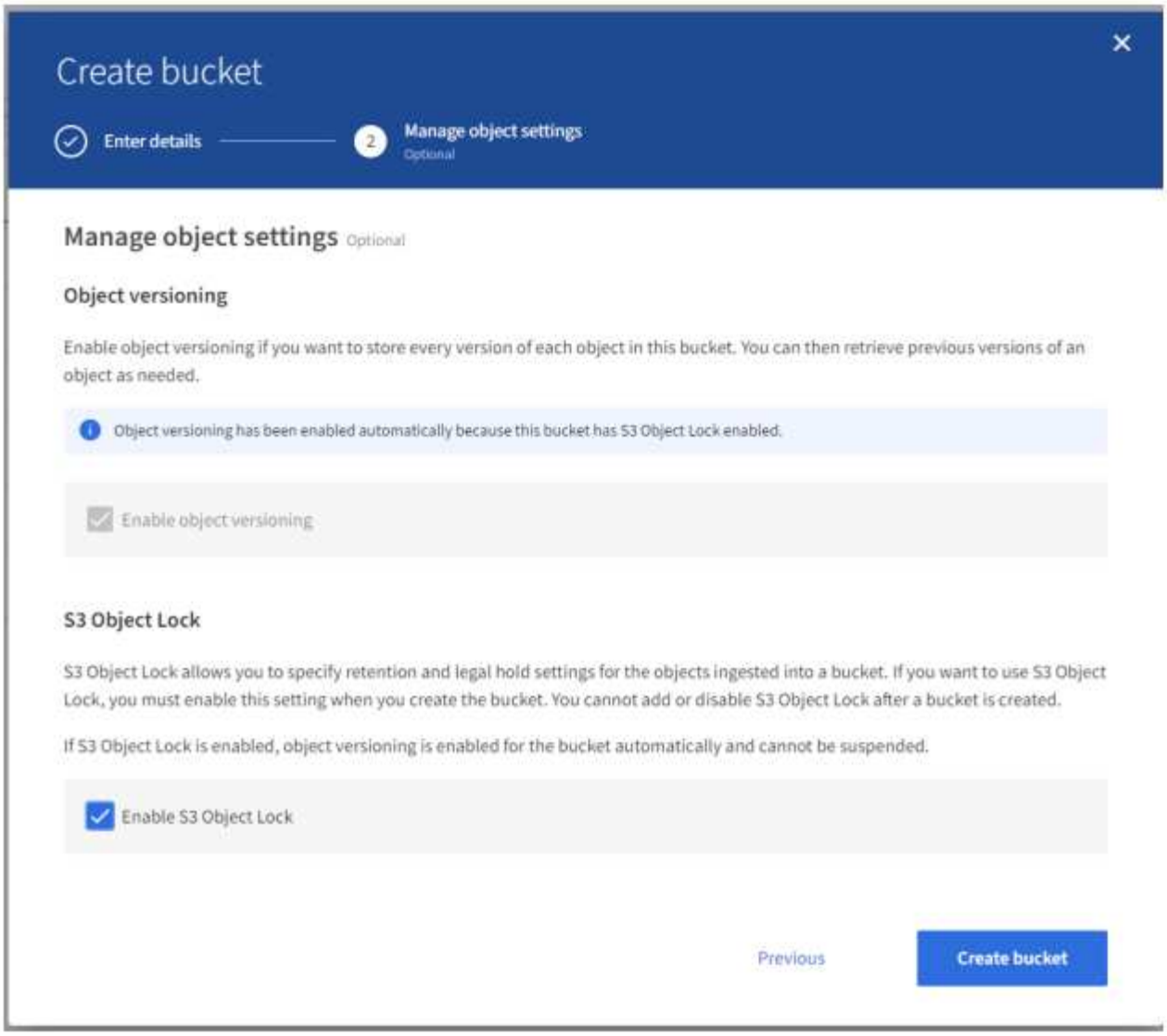
Führen Sie die folgenden Schritte aus, um die standardmäßige Bucket-Aufbewahrung von StorageGRID S3 Object Lock zu konfigurieren:

Schritte

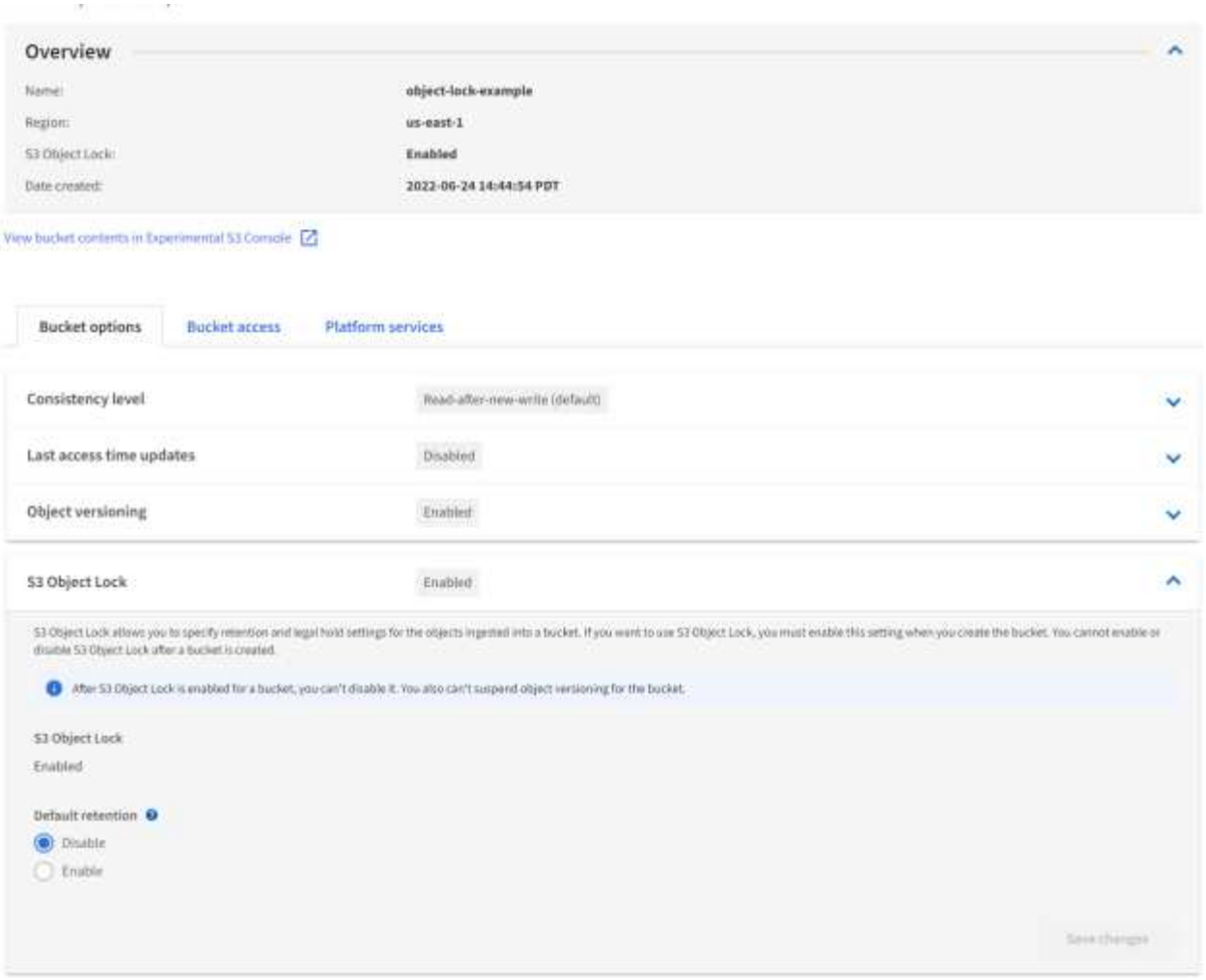
1. Erstellen Sie in StorageGRID-Mandantenmanager einen Bucket, und klicken Sie auf Fortfahren



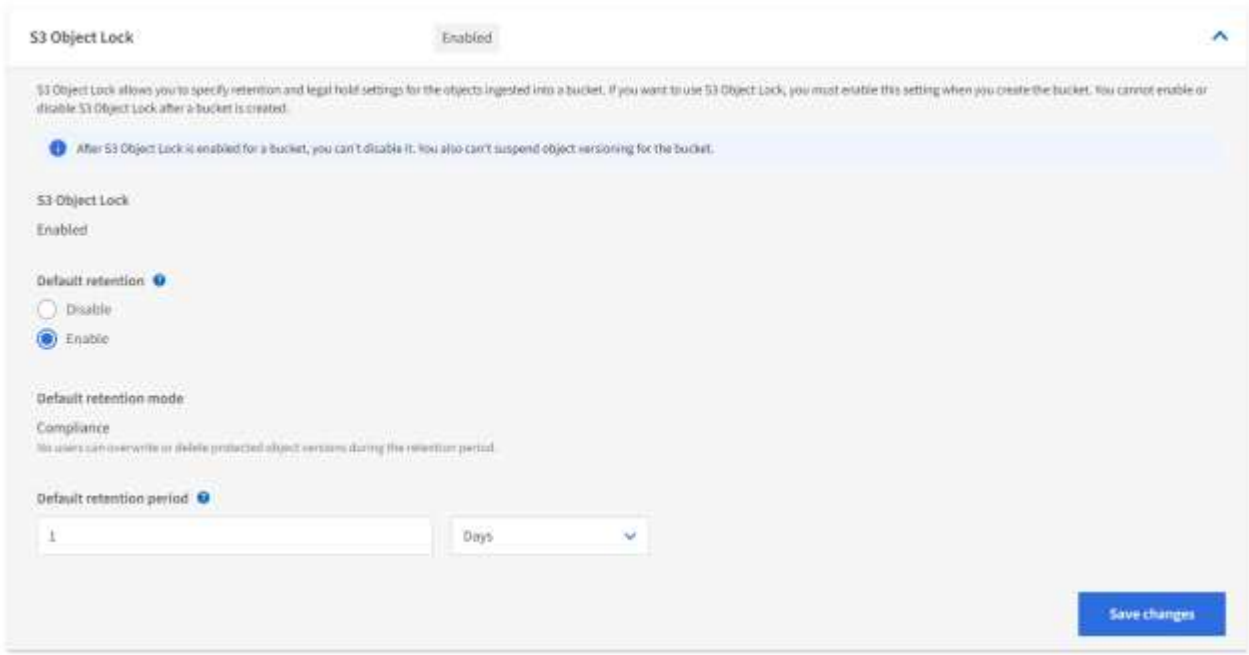
2. Wählen Sie die Option S3-Objektsperre aktivieren aus, und klicken Sie auf Bucket erstellen.



3. Nachdem der Bucket erstellt wurde, wählen Sie den Bucket aus, um die Bucket-Optionen anzuzeigen. Erweitern Sie die Dropdown-Option S3 Object Lock.



4. Wählen Sie unter Standardaufbewahrung die Option Aktivieren aus, und legen Sie eine Standardaufbewahrungsfrist von 1 Tag fest. Klicken Sie Auf Änderungen Speichern.



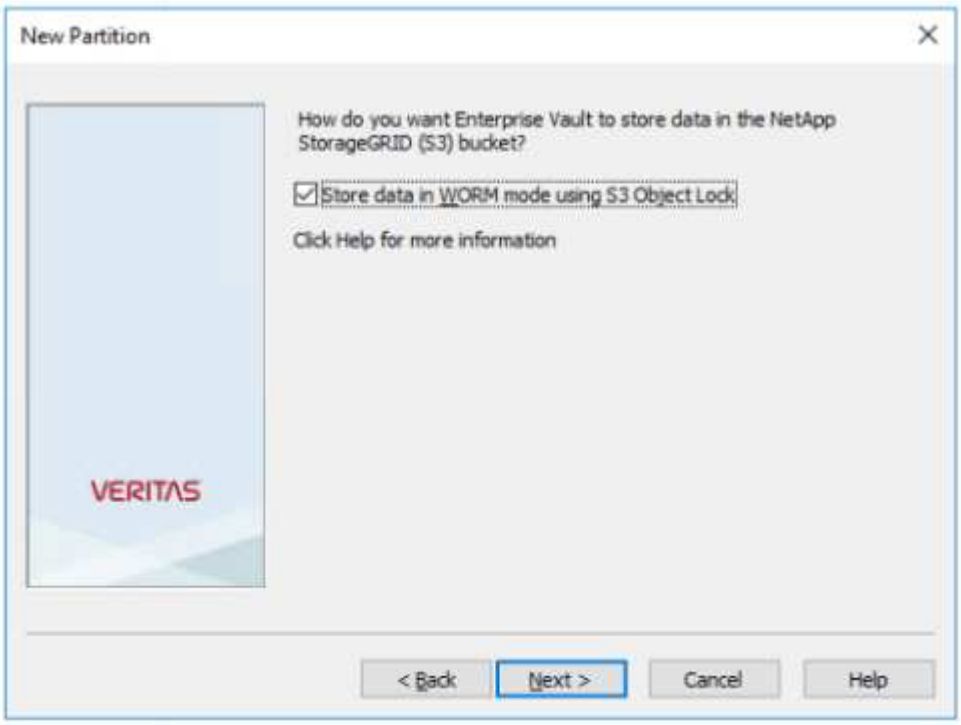
Der Bucket kann jetzt von Enterprise Vault zur Speicherung von WORM-Daten verwendet werden.

Enterprise Vault Konfigurieren

Gehen Sie wie folgt vor, um Enterprise Vault zu konfigurieren:

Schritte

1. Wiederholen Sie die Schritte 1-3 im "Basiskonfiguration" Abschnitt, wählen Sie jedoch diesmal die Option Daten im WORM-Modus mit S3 Objektsperre speichern. Klicken Sie Auf Weiter.



2. Stellen Sie bei der Eingabe der S3 Bucket-Verbindungseinstellungen sicher, dass Sie den Namen eines S3-Buckets eingeben, für den die S3 Object Lock Default Retention aktiviert ist.
3. Testen Sie die Verbindung, um die Einstellungen zu überprüfen.

Konfigurieren Sie StorageGRID-Standort-Failover für Disaster Recovery

Erfahren Sie, wie Sie ein StorageGRID-Standort-Failover in einem Disaster-Recovery-Szenario konfigurieren.

Eine Implementierung einer StorageGRID-Architektur hat gemein mehrere Standorte. Standorte können entweder aktiv/aktiv oder aktiv/Passiv für DR sein. Stellen Sie in einem DR-Szenario sicher, dass veritas Enterprise Vault die Verbindung zu seinem primären Speicher (StorageGRID) aufrechterhalten kann und bei einem Standortausfall weiterhin Daten aufnehmen und abrufen kann. Dieser Abschnitt enthält allgemeine Konfigurationsanleitungen für eine aktiv/Passiv-Bereitstellung an zwei Standorten. Detaillierte Informationen zu diesen Richtlinien finden Sie auf der "StorageGRID-Dokumentation" Seite oder bei einem StorageGRID Experten.

Voraussetzungen für die Konfiguration von StorageGRID mit veritas Enterprise Vault

Überprüfen Sie vor dem Konfigurieren des StorageGRID-Standort-Failover die folgenden Voraussetzungen:

- Es gibt eine StorageGRID-Bereitstellung an zwei Standorten, z. B. Standort 1 und STANDORT 2.
- Es wurde an jedem Standort ein Admin-Node erstellt, auf dem der Load Balancer ausgeführt wird, oder ein Gateway-Node zum Lastausgleich.
- Ein Endpunkt des StorageGRID Load Balancer wurde erstellt.

Konfigurieren Sie das StorageGRID Site Failover

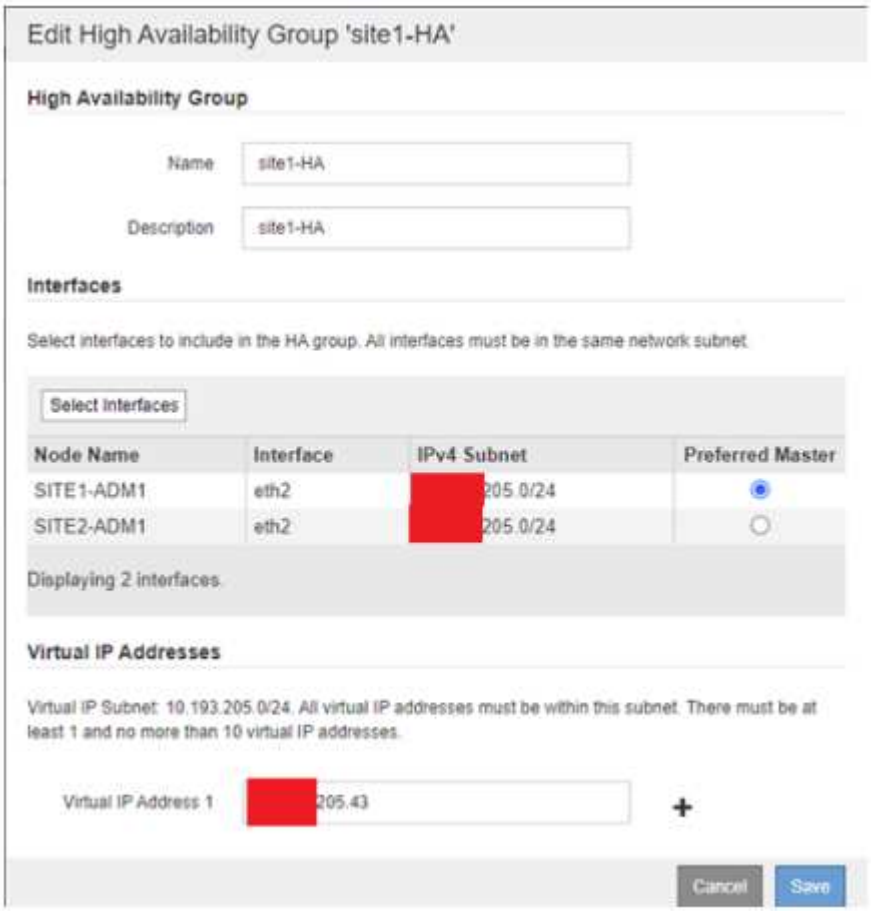
Führen Sie zum Konfigurieren des StorageGRID-Standort-Failover die folgenden Schritte aus:

Schritte

1. Konfigurieren Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit), um die Verbindung zu StorageGRID bei Standortausfällen sicherzustellen. Klicken Sie in der StorageGRID-Grid-Manager-Oberfläche (GMI) auf Konfiguration, Hochverfügbarkeitsgruppen und + Erstellen.

   [Vertias/veritas-create-High-Availability-Group]

2. Geben Sie die erforderlichen Informationen ein. Klicken Sie auf Schnittstellen auswählen und schließen Sie sowohl die Netzwerkschnittstellen von SITE 1 als auch von SITE2 ein, wobei SITE 1 (der primäre Standort) der bevorzugte Master ist. Weisen Sie eine virtuelle IP-Adresse innerhalb desselben Subnetzes zu. Klicken Sie auf Speichern .

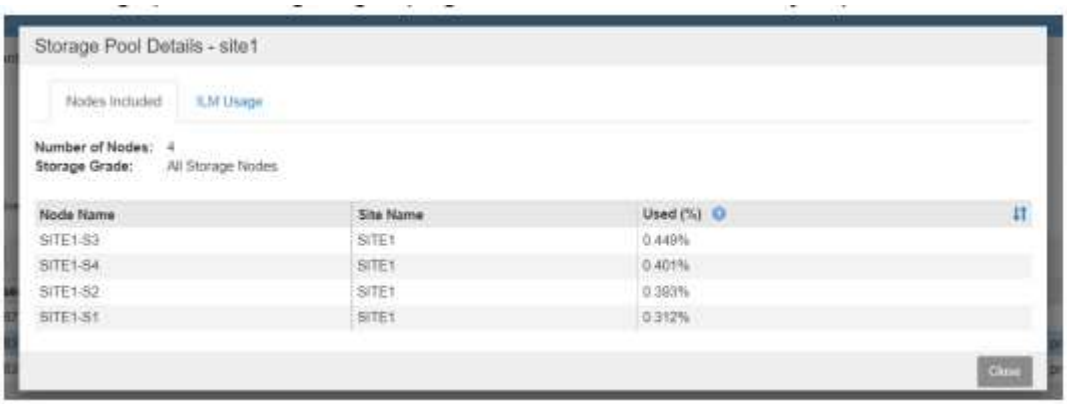


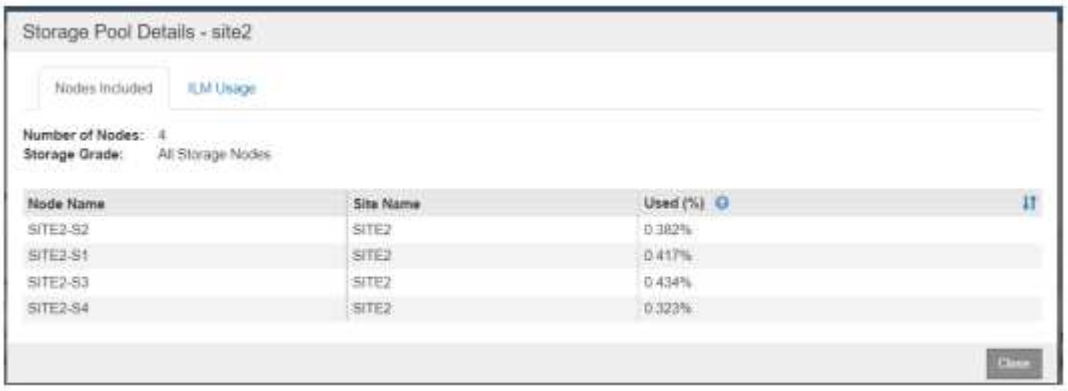
3. Diese virtuelle IP (VIP)-Adresse sollte dem S3-Hostnamen zugeordnet werden, der während der Partitionskonfiguration von veritas Enterprise Vault verwendet wird. Die VIP-Adresse löst Datenverkehr an STANDORT 1 auf. Während STANDORT 1-Fehler leitet die VIP-Adresse den Datenverkehr transparent an STANDORT 2 um.

4. Stellen Sie sicher, dass die Daten sowohl an STANDORT 1 als auch an STANDORT 2 repliziert werden. So sind die Objektdaten auch bei Ausfall von STANDORT 1 von SITE2 aus verfügbar. Dazu müssen zunächst die Speicherpools konfiguriert werden.

   Klicken Sie in StorageGRID GMI auf ILM, Speicherpools und dann auf Erstellen. Folgen Sie dem Assistenten, um zwei Speicherpools zu erstellen: Einen für STANDORT 1 und einen anderen für STANDORT 2.

   Storage-Pools sind logische Gruppen von Nodes, die zur Definition der Objektplatzierung verwendet werden





5. Klicken Sie in StorageGRID GMI auf ILM, Regeln und dann auf + Erstellen. Befolgen Sie den Assistenten, um eine ILM-Regel zu erstellen, die eine Kopie angibt, die pro Standort mit einem ausgewogenen Aufnahmeverhalten gespeichert werden soll.

6. Fügen Sie die ILM-Regel einer ILM-Richtlinie hinzu und aktivieren Sie die Richtlinie.

Diese Konfiguration hat das folgende Ergebnis:

- Eine virtuelle S3-Endpunkt-IP, wobei STANDORT 1 der primäre und STANDORT 2 der sekundäre Endpunkt ist. Wenn STANDORT 1 ausfällt, erfolgt ein Failover der VIP auf STANDORT 2.
- Wenn archivierte Daten von veritas Enterprise Vault gesendet werden, stellt StorageGRID sicher, dass eine Kopie auf SITE 1 gespeichert wird und eine andere DR-Kopie in SITE2 gespeichert wird. Wenn STANDORT 1 ausfällt, wird Enterprise Vault weiterhin von STANDORT 2 aufgenommen und abgerufen.

Beide Konfigurationen sind für veritas Enterprise Vault transparent. Der S3-Endpunkt, der Bucket-Name, die Zugriffsschlüssel usw. sind identisch. Es ist nicht notwendig, die S3-Verbindungseinstellungen auf der veritas Enterprise Vault-Partition neu zu konfigurieren.