Produktfunktionshandbücher

StorageGRID solutions and resources

NetApp
December 12, 2025

Inhalt

Produktfunktionshandbücher

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

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

Übersicht über StorageGRID

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

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

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

StorageGRID Scale

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

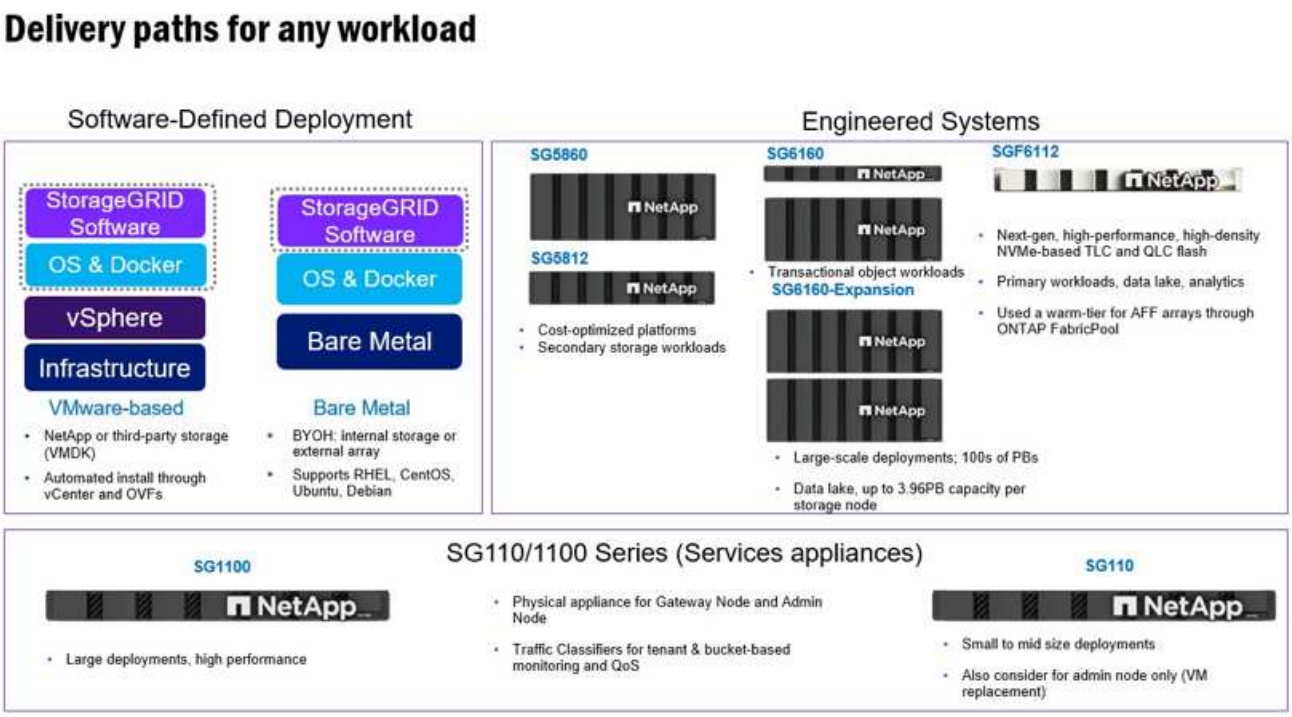
Der Admin-Knoten enthält die Verwaltungsschnittstelle, einen zentralen Punkt für Metriken und Protokollierung und verwaltet die Konfiguration der StorageGRID Komponenten. Der Admin-Knoten enthält außerdem einen integrierten Load Balancer für den S3-API-Zugriff.

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

Ein Speicherknoten kann wie folgt bereitgestellt werden:

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

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



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

StorageGRID und Ausfall-Domains

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

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

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

Objektdaten und Metadaten

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

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

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

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

Objektmetadaten enthalten Informationen wie die folgenden:

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

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

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

Erasure Coding

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

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

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

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

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

Metadatenkonsistenz

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

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

Die in StorageGRID verfügbaren Bucket-Konsistenzoptionen sind:

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

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

Konsistenz von Objektdaten

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

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

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

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

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

Lastverteilung

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

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

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

Anforderungen für Zero RPO mit StorageGRID

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

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

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

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

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

Synchrone Implementierungen an mehreren Standorten

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

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

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

Zusammenfassung:

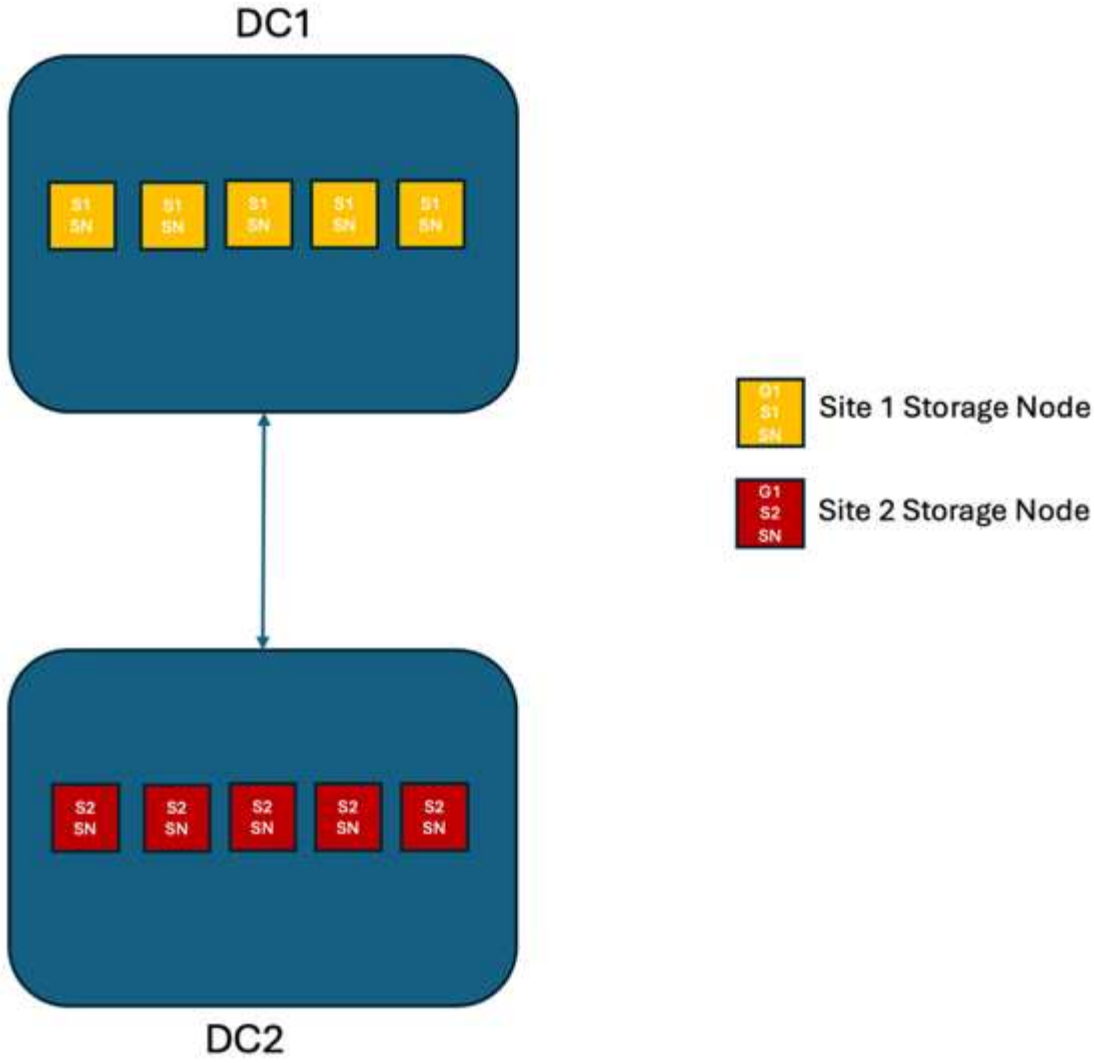
- Die Grid-interne Replizierung umfasst sowohl synchrone als auch asynchrone Replizierung, die mithilfe des ILM-Aufnahmeverhaltens und der Konsistenzkontrolle für Metadaten konfigurierbar ist.
- Die Replizierung zwischen dem Grid erfolgt nur asynchron.

Bereitstellung über mehrere Standorte in einem einzigen Grid

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

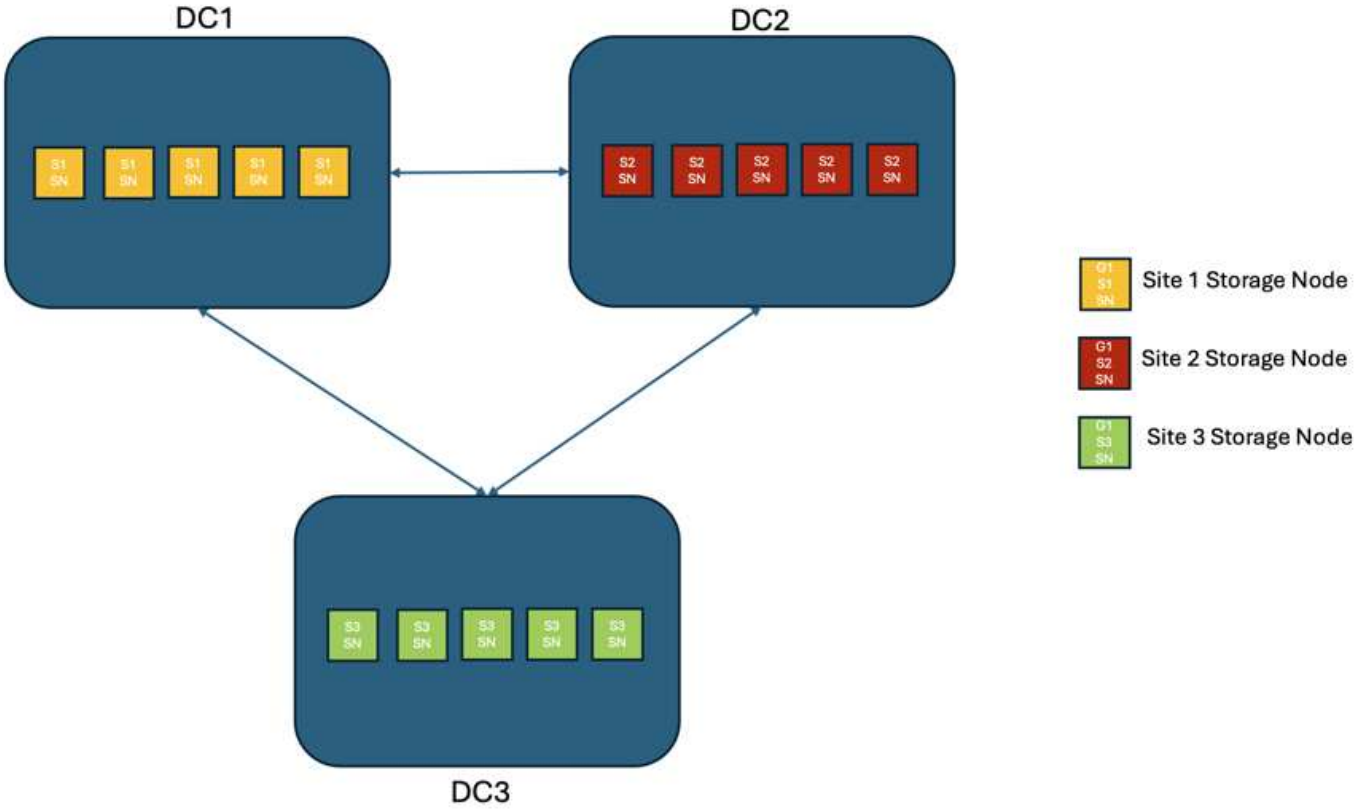
Szenario 1:

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



Szenario 2:

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



Ausfallszenarien für mehrere Standorte

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

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

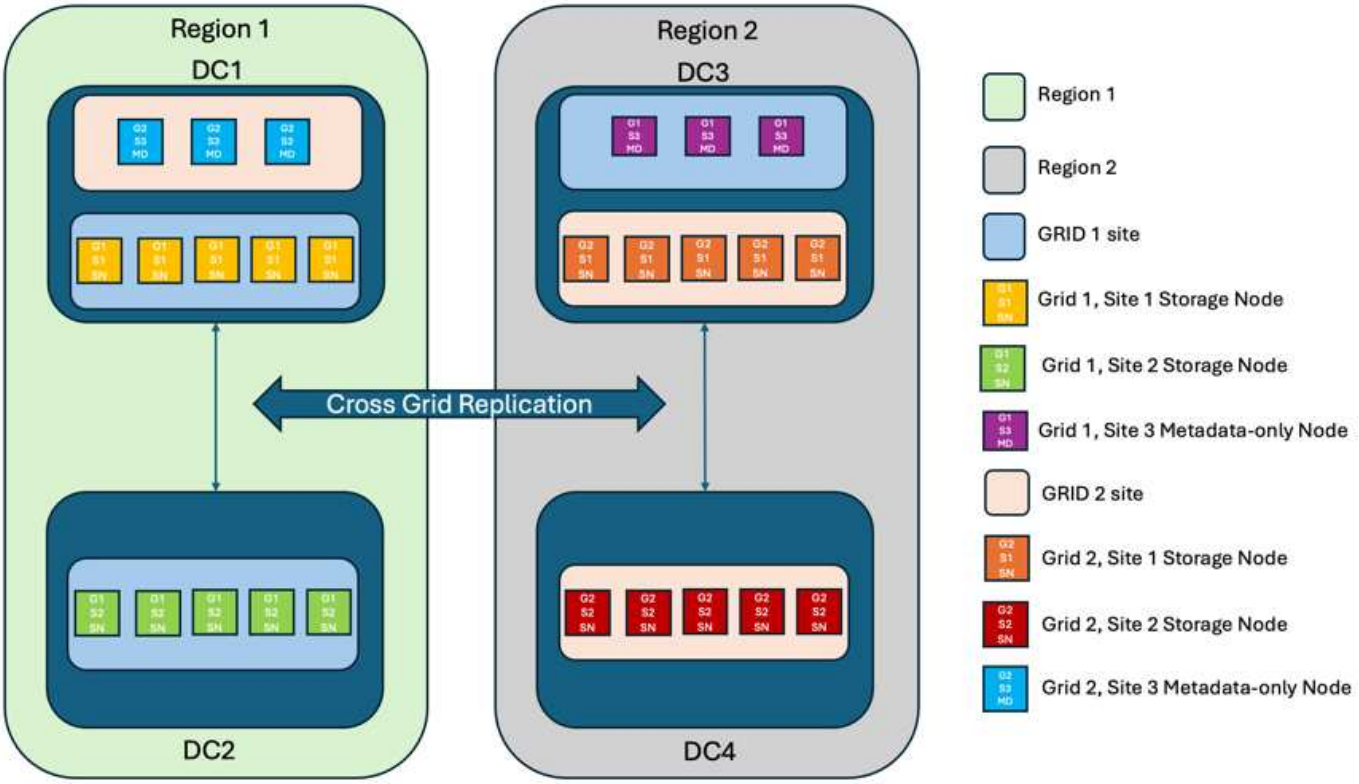
Ausfall	Ergebnis an zwei Standorten + Vermächtnis Starke globale Präsenz	Ergebnis von 3 oder mehr Standorten + Quorum Strong Global
Von jedem verbleibenden Standort aus einen Standort und einen Node	Es existieren nur zwei Standorte. Siehe: Einzelner Standort plus ein einzelner Knoten.	Der Betrieb wird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

Eine Multi-Grid-Implementierung an mehreren Standorten

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

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

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



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

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

Ausfallszenarien für mehrere Standorte und Grids

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

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

Schlussfolgerung

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

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

Cloud Storage Pool für AWS oder Google Cloud erstellen

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

Was Sie benötigen

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

Schritte

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

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

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

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

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

   Es sind zwei Formate zulässig:

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

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

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

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

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

Erwartetes Ergebnis

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

Von Jonathan Wong

Cloud Storage Pool für Azure Blob Storage erstellen

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

Was Sie benötigen

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

Schritte

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

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

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

   Es sind zwei Formate zulässig:

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

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

6. Geben Sie den Azure-Containernamen ein.

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

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

Erwartetes Ergebnis

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

Von Jonathan Wong

Verwenden Sie einen Cloud Storage Pool für Backups

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

Was Sie benötigen

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

Schritte

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

Erwartetes Ergebnis

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

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

Von Jonathan Wong

Konfigurieren Sie den Integrationsservice für die StorageGRID Suche

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

Einführung

StorageGRID unterstützt drei Arten von Plattform-Services.

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

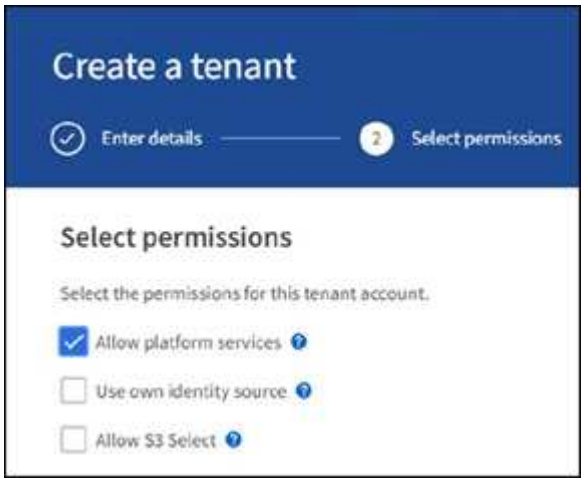
Plattform-Services werden vom S3-Mandanten über die Mandanten-Manager-UI konfiguriert. Weitere Informationen finden Sie unter "Überlegungen bei der Verwendung von Plattform-Services".

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

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

Erstellung von Mandanten und Aktivierung von Plattform-Services

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



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

   Dies führt Sie zur Seite Tenant Manager.

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

Integrationsservices mit Amazon OpenSearch suchen

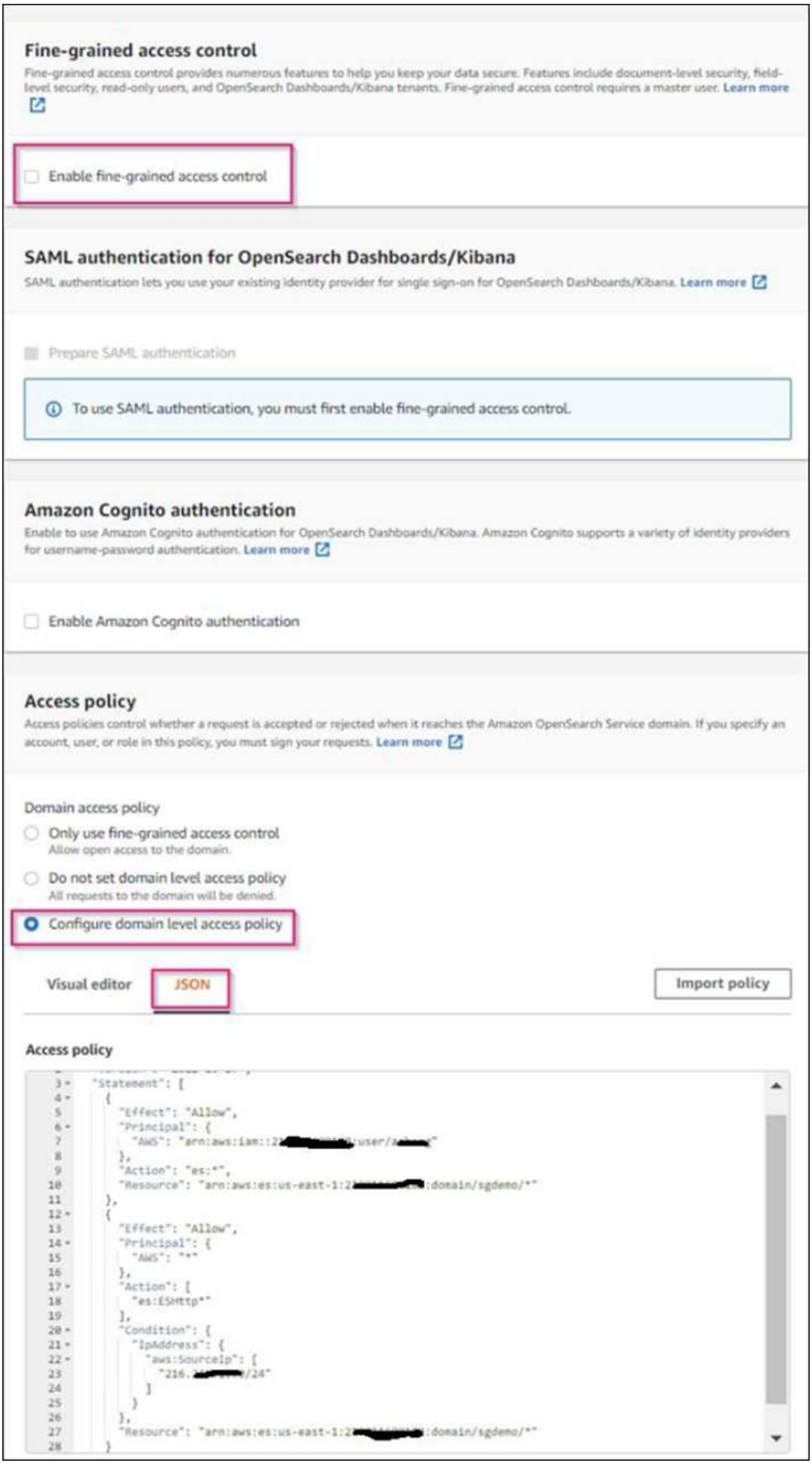
Einrichtung des Amazon OpenSearch Service (ehemals Elasticsearch)

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

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

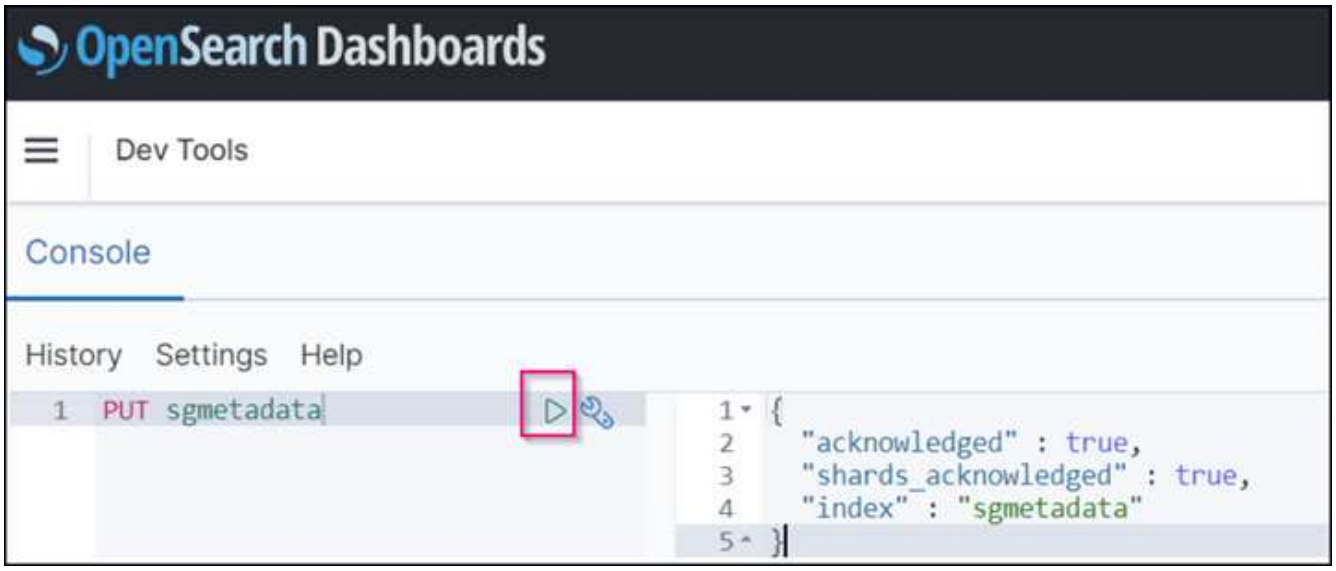
1. Erstellen Sie mithilfe der Anweisungen von eine neue Domäne "AWS OpenSearch Service – erste Schritte", Mit Ausnahme der folgenden:
   - Schritt 4: Domain-Name: Sgdemo
   - Schritt 10: Feinkörnige Zugriffssteuerung: Deaktivieren Sie die Option Enable Fine-genarainable Access Control.
   - Schritt 12: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

```
{

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

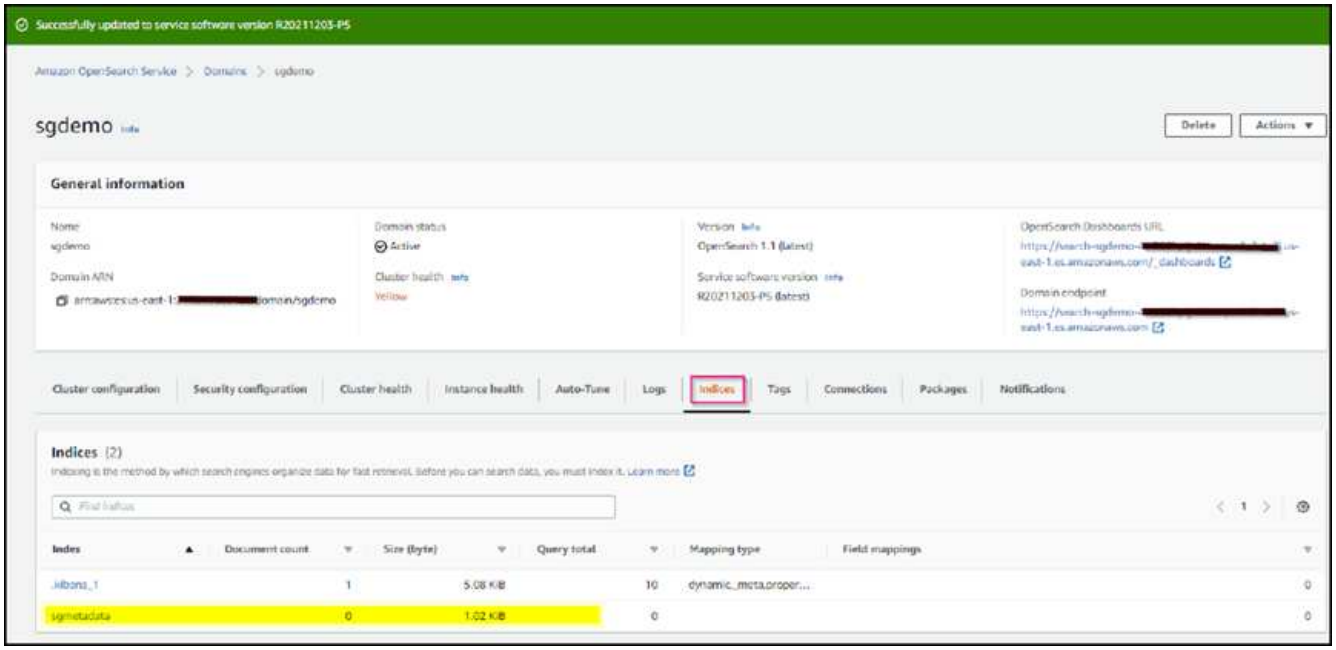

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more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

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

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



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

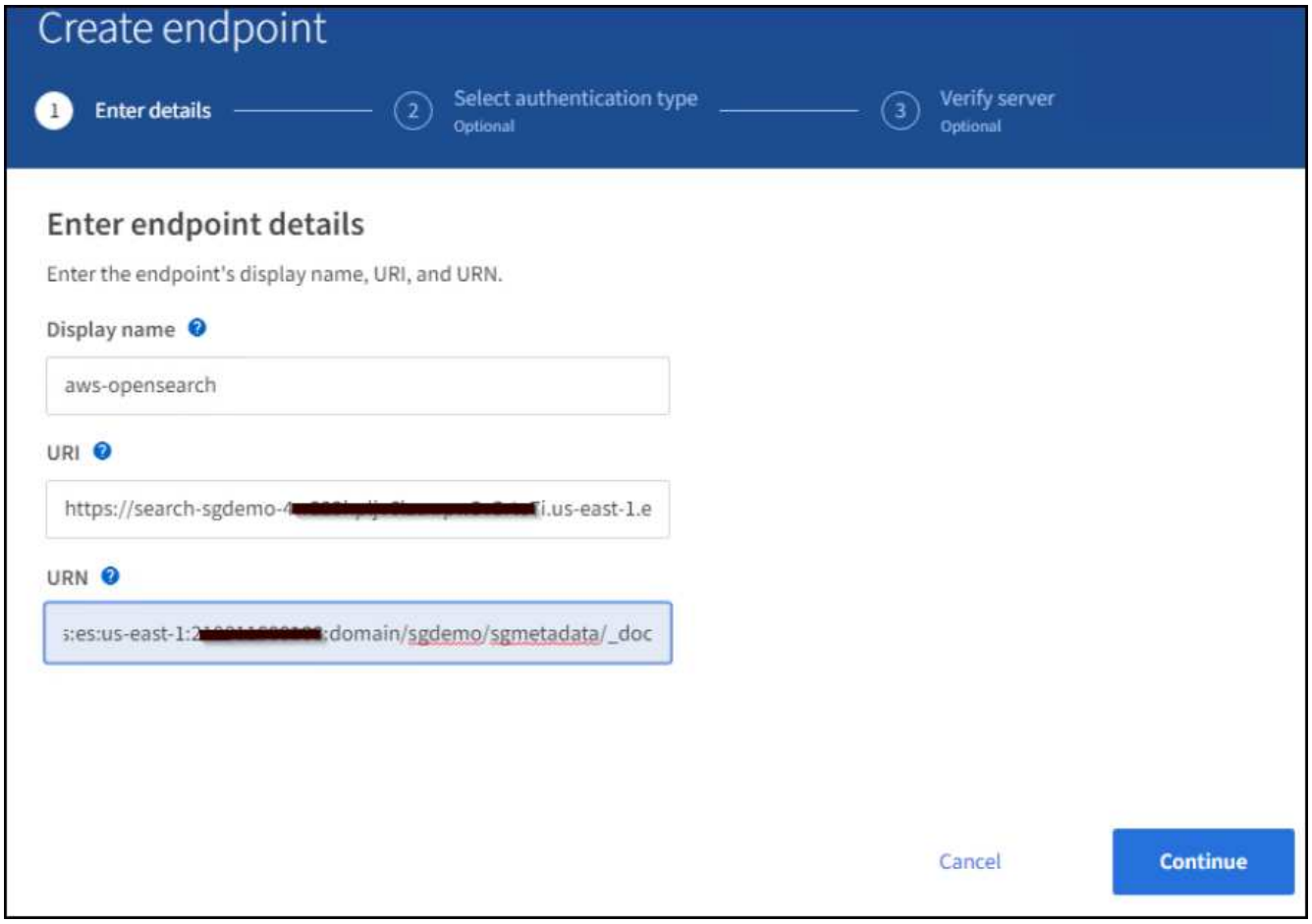


Endpoint-Konfiguration für Plattform-Services

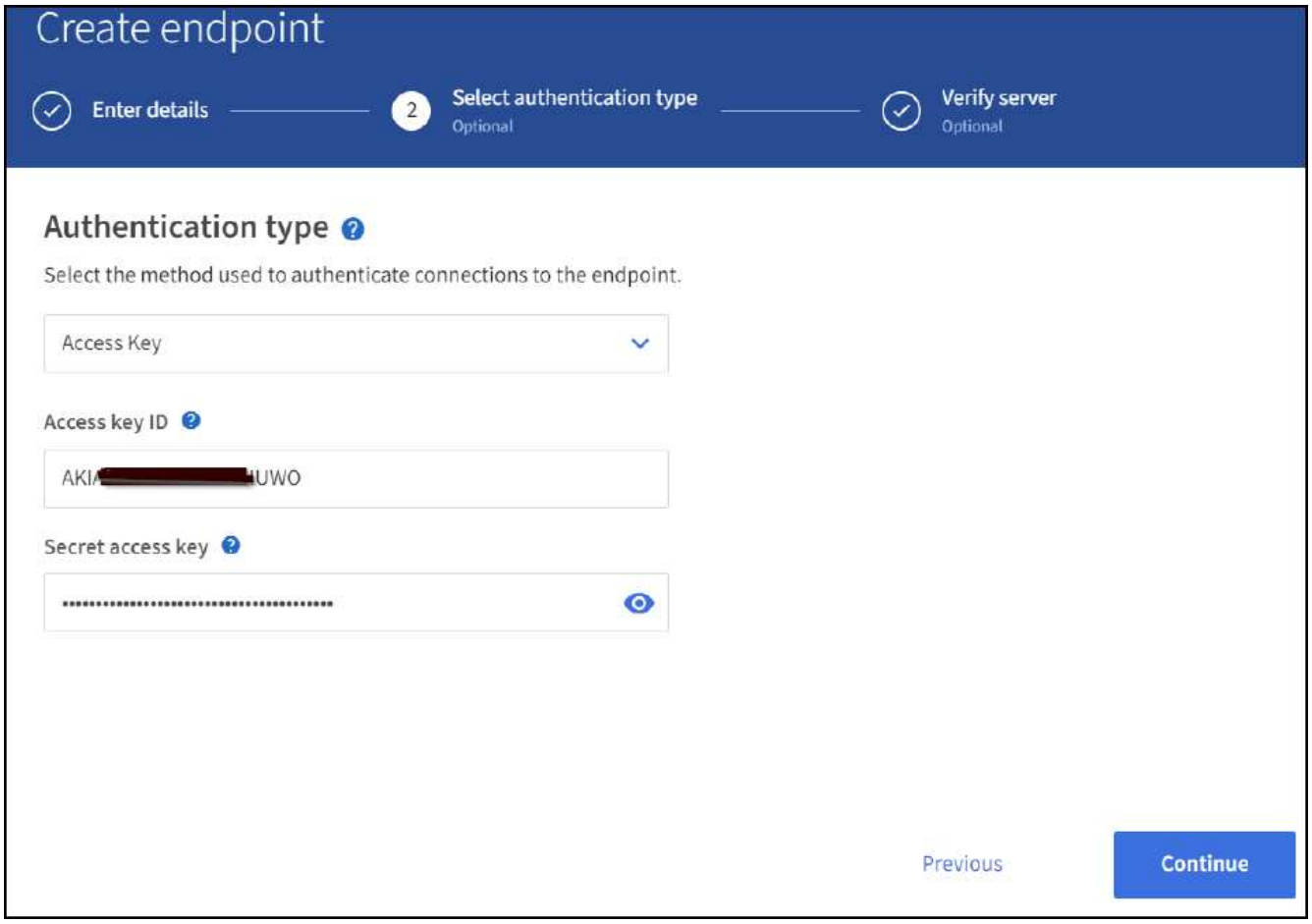
Gehen Sie wie folgt vor, um die Endpunkte der Plattformservices zu konfigurieren:

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

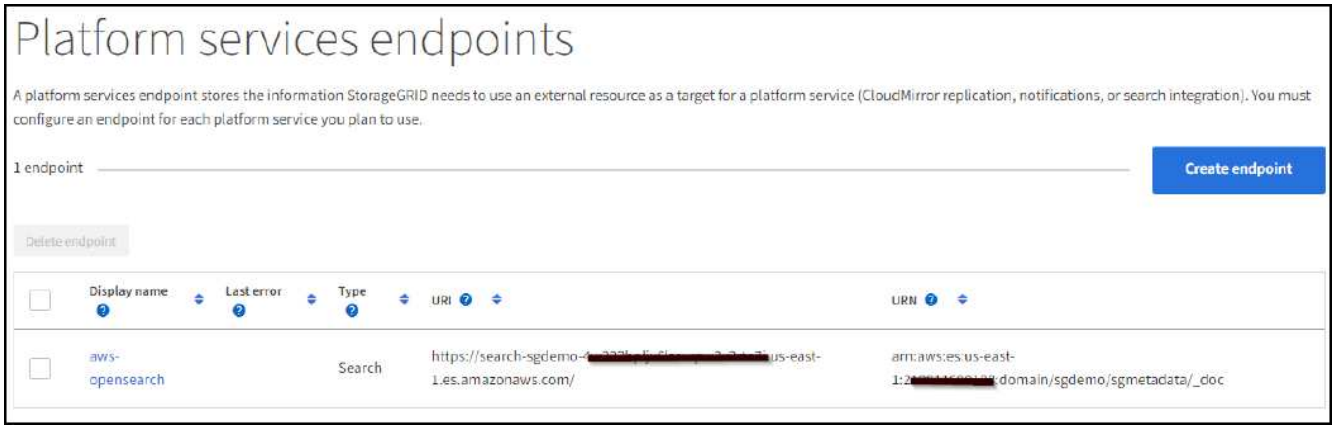
     In diesem Beispiel wird URN `arn:aws:es:us-east-1:211234567890:domain/sgdemo /sgmedata/_doc`.



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



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



Suchintegrations-Services für On-Premises-Elasticsearch

Elasticsearch-Einrichtung vor Ort

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

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

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

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

```
sudo systemctl enable docker
```

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

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

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

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

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

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

Elasticsearch Service | Self-managed

Install and run Elasticsearch

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

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

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

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

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

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

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

Install and run Kibana

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

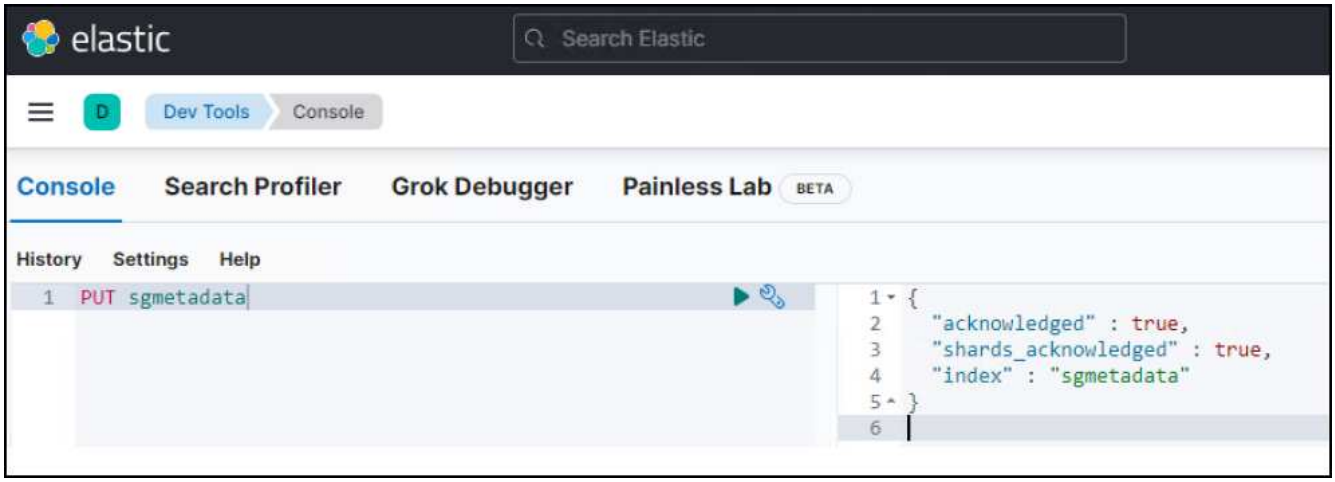
1. In a new terminal session, run:

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

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

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

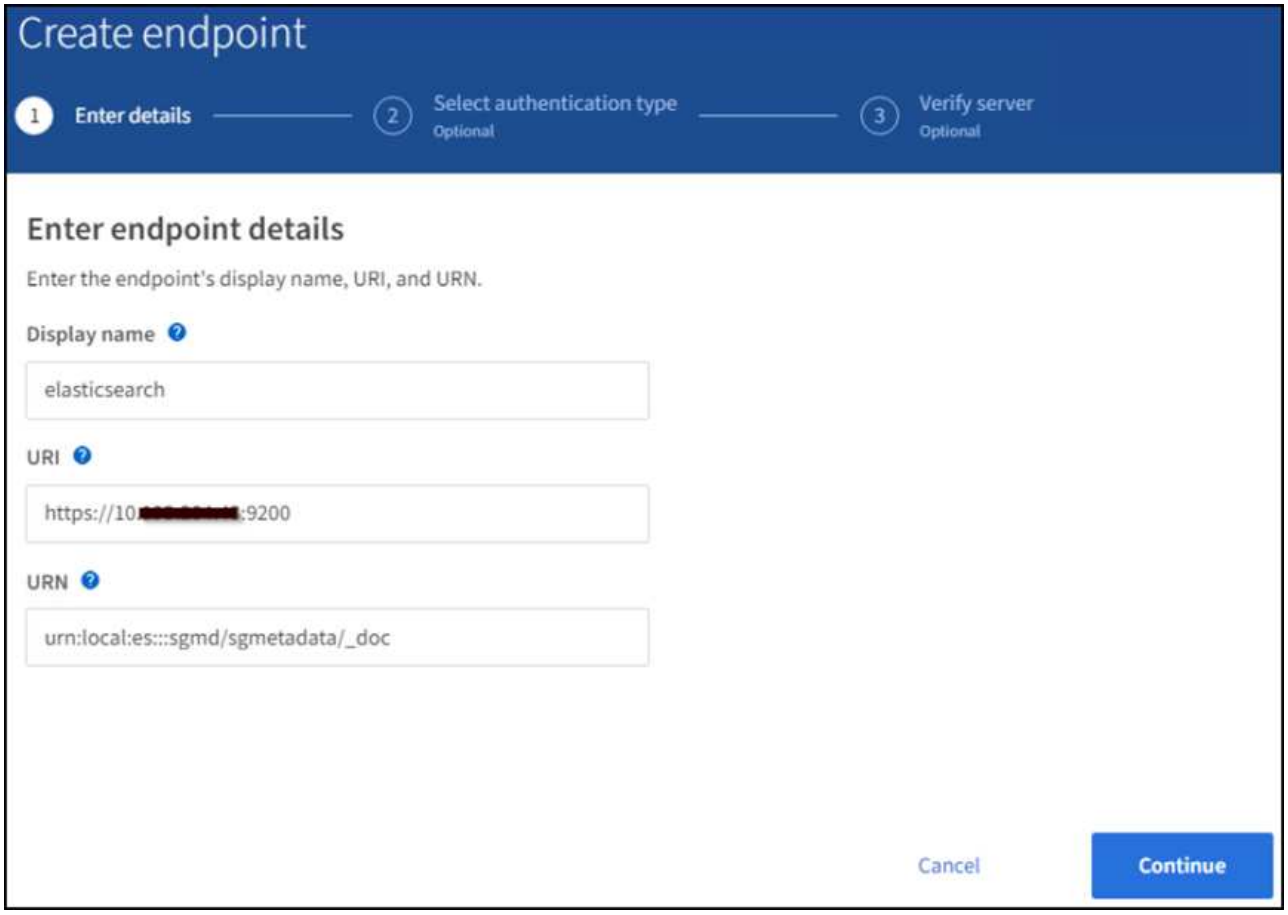
3. Nachdem der Kibana-Docker-Container gestartet wurde, wird der URL-Link aufgerufen `https://0.0.0.0:5601` Wird in der Konsole angezeigt. Ersetzen Sie 0.0.0.0 durch die Server-IP-Adresse in der URL.
4. Melden Sie sich mit dem Benutzernamen bei der Kibana-Benutzeroberfläche an `elastic` Und das Passwort,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



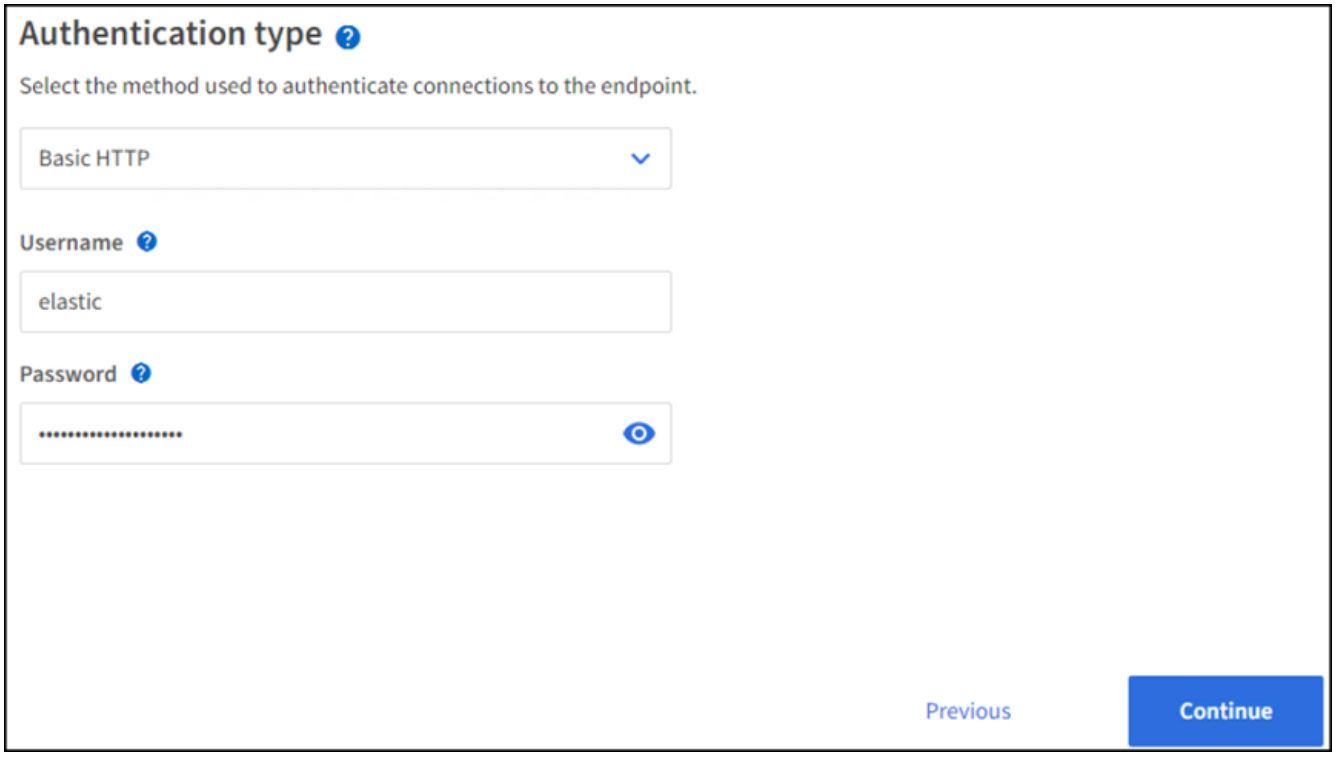
Endpoint-Konfiguration für Plattform-Services

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

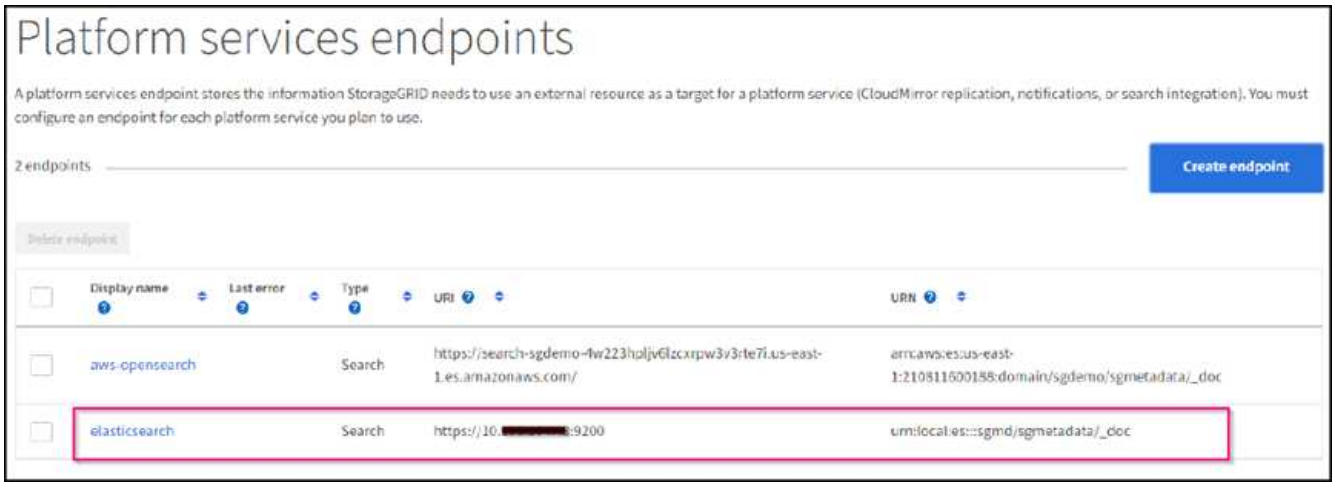
1. In Tenant Manager wechseln Sie zu STORAGE (S3) > Plattform-Services-Endpunkten
2. Klicken Sie auf Endpunkt erstellen, geben Sie Folgendes ein und klicken Sie dann auf Weiter:
   - Beispiel für Anzeigename: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
   - URNE: `urn: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



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



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



Konfiguration des integrierten Service für die Bucket-Suche

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

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

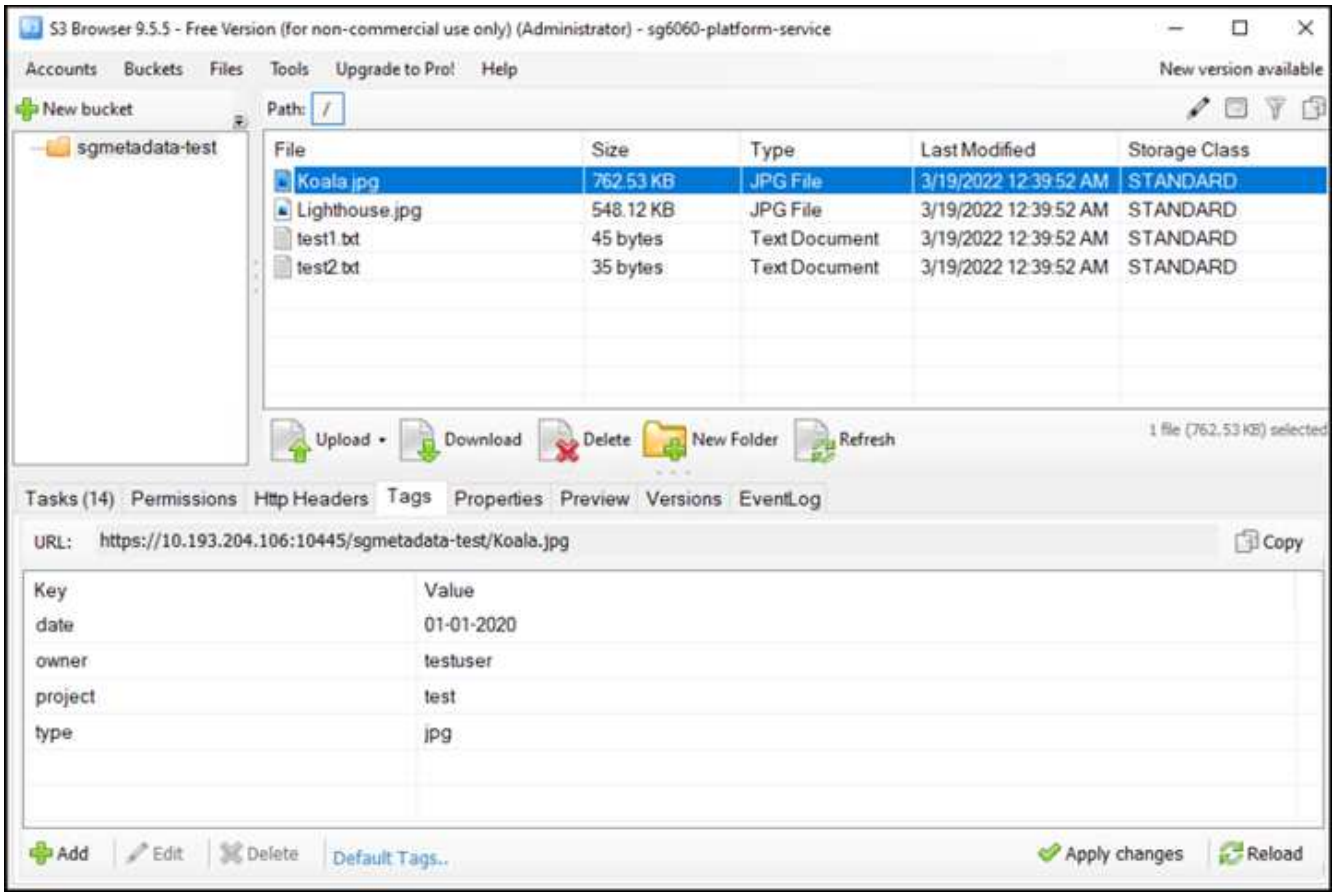
1. Wählen Sie in Tenant Manager „STORAGE(S3)“ > „Buckets“
2. Klicken Sie auf Create Bucket. Geben Sie den Bucket-Namen ein (z. B. `sgmetadata-test`) Und akzeptieren Sie die Standardeinstellung `us-east-1` Werden.
3. Klicken Sie Auf Weiter > Bucket Erstellen.
4. Um die Seite „Bucket-Übersicht“ aufzurufen,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

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

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

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

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



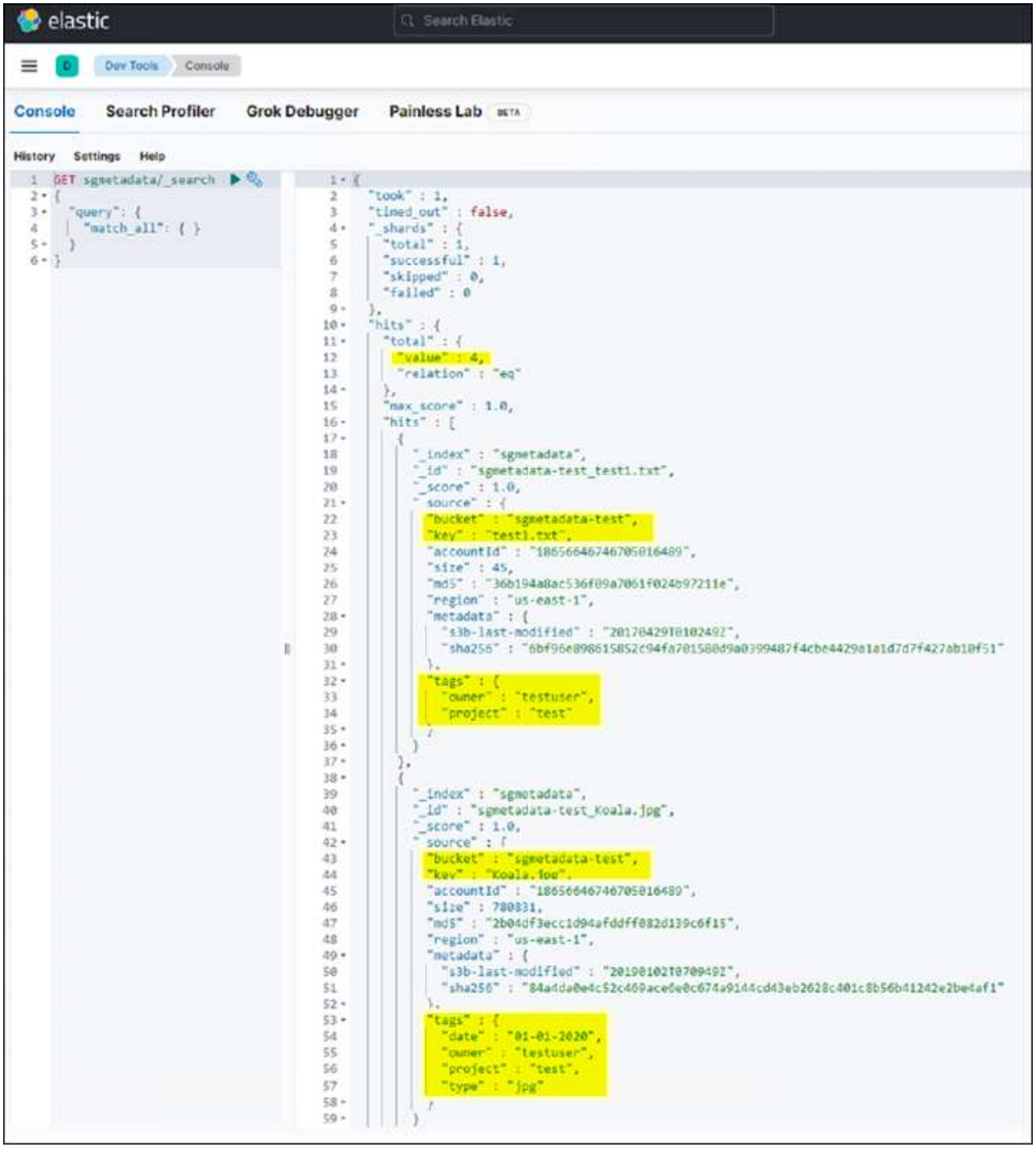
7. Verwenden Sie die Kibana UI, um zu überprüfen, ob die Objektmetadaten in den Index der sgmetadaten geladen wurden.

   a. Wählen Sie im Menü Verwaltung > Entwicklungstools.

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

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

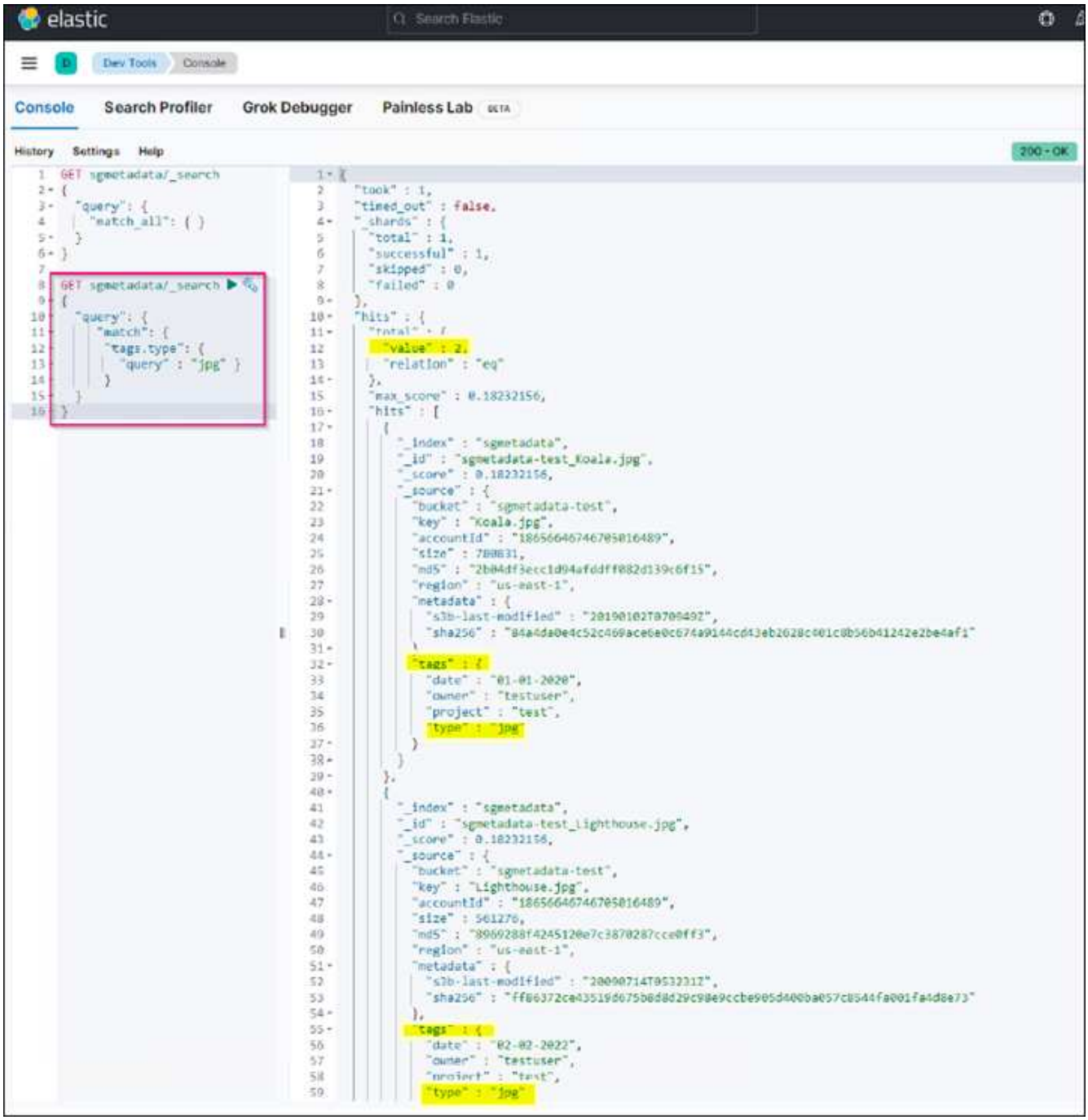
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



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

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

+



Wo Sie weitere Informationen finden

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

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

Von Angela Cheng

Node-Klonen

Überlegungen und Performance von Node-Klonen

Überlegungen zu Node-Klonen

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

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

Schätzungen der Performance von Node-Klonen

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

DDP8

SG5612/SG5712/SG5812 → BELIEBIG

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

SG5660 → SG5760/SG5860

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

SG5660 → SG6060/SG6160

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

SG5760/SG5860 → SG5760/SG5860

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

SG5760/SG5860 → SG6060/SG6160

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

SG6060/SG6160 → SG6060/SG6160

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

DDP16

SG5760/SG5860 → SG5760/SG5860

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

SG5760/SG5860 → SG6060/SG6160

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

SG6060/SG6160 → SG6060/SG6160

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

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

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

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

Von Aron Klein

Standortverlagerung von Grid-Standorten und standortweites Netzwerkänderungsverfahren

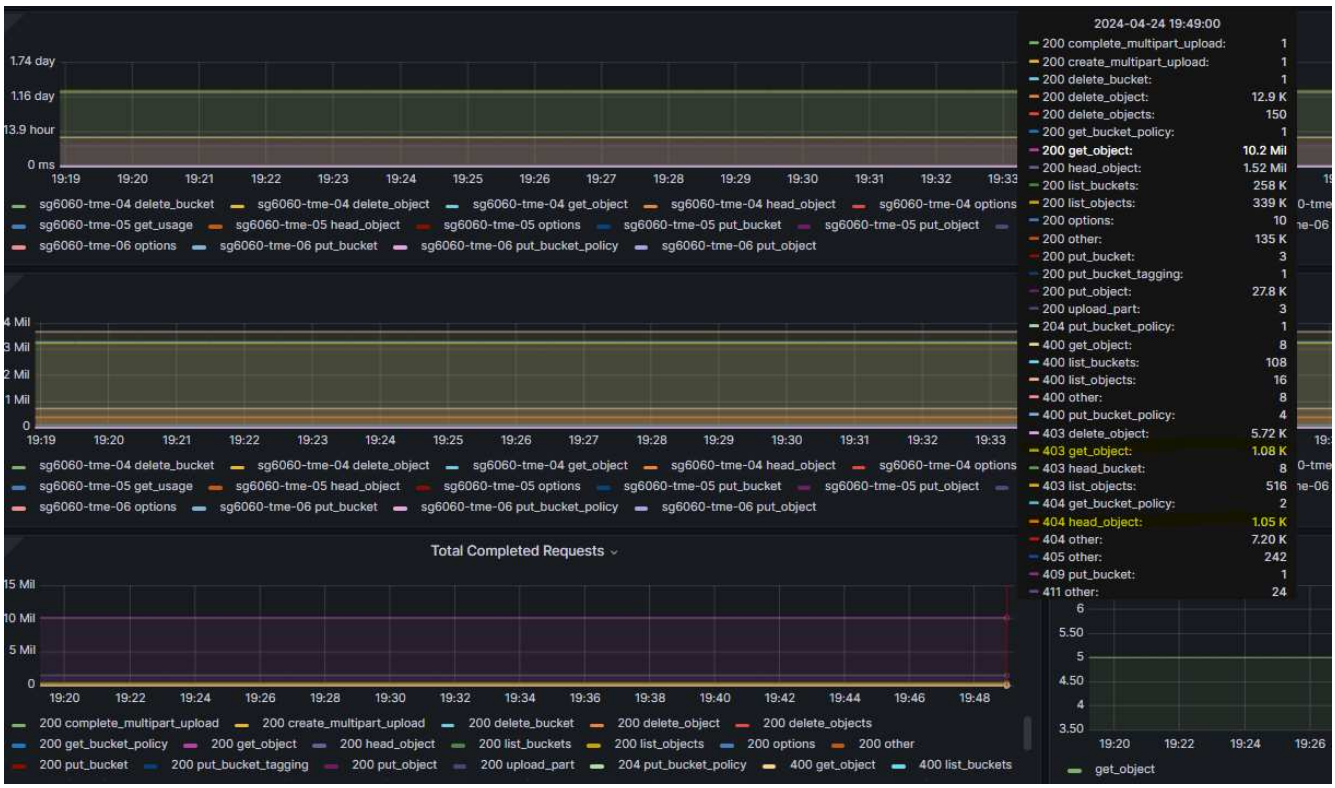
Dieser Leitfaden beschreibt die Vorbereitung und das Verfahren für den Standortwechsel in einem Grid mit mehreren Standorten von StorageGRID. Sie sollten über ein vollständiges Verständnis dieser Vorgehensweise verfügen und im Voraus planen, um einen reibungslosen Prozess zu gewährleisten und Unterbrechungen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

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

Überlegungen vor Standortverlagerung

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

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



Verfahren zum Ändern der Grid-IP-Adresse vor Standortverlagerung

Schritte

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

```
Editing: Node IP/subnet and gateway

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

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

b. Wählen Sie 5, um die Änderungen anzuzeigen

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

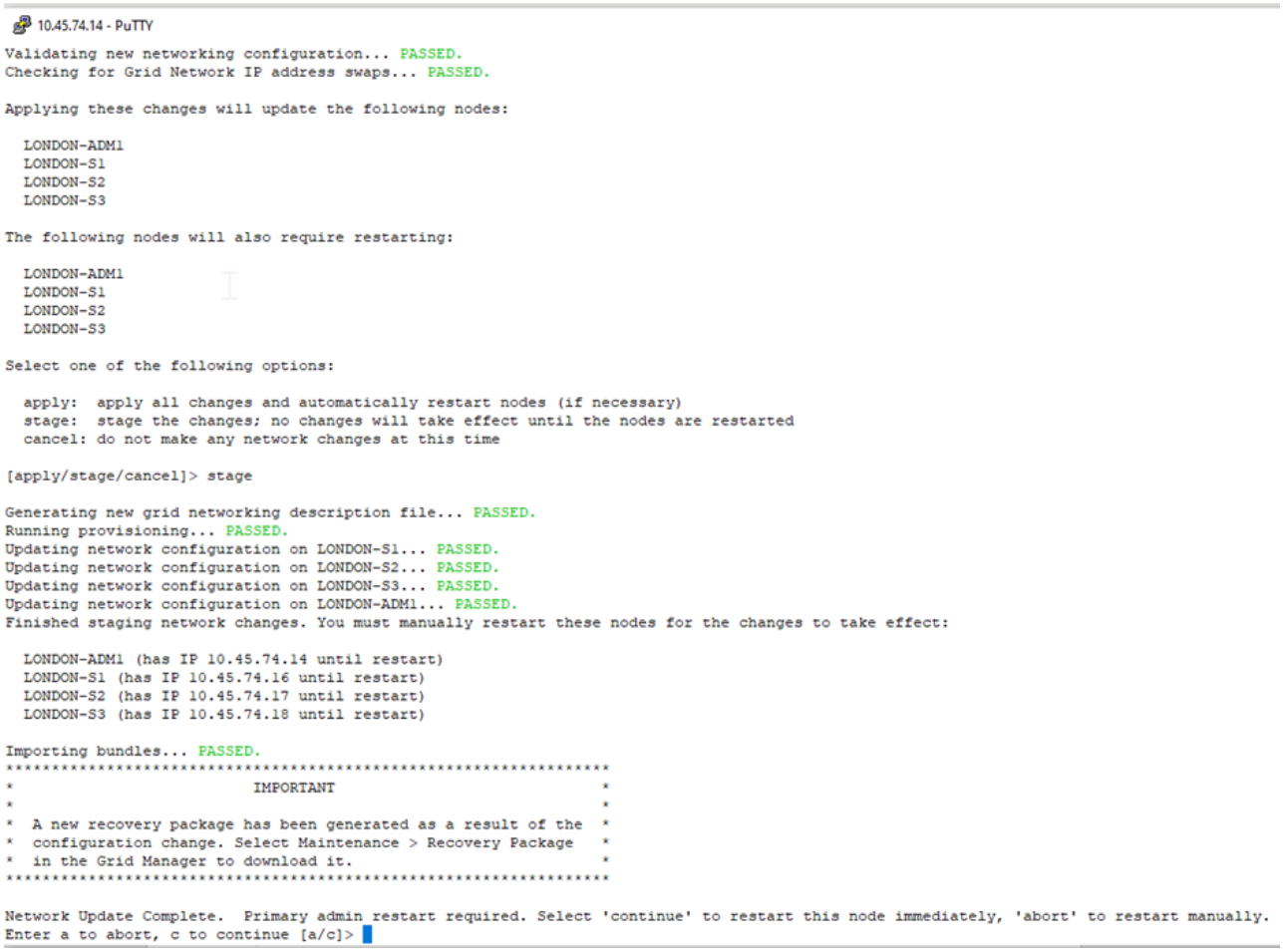
c. Wählen Sie 10, um die Änderung zu validieren und anzuwenden.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection: 10
```

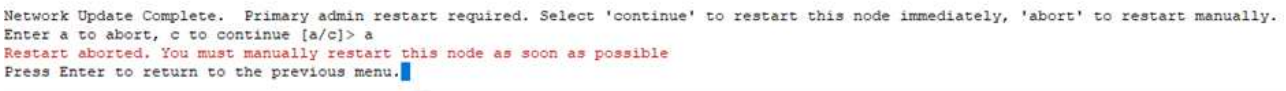
d. In diesem Schritt muss **Stufe** ausgewählt werden.

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

Applying these changes will update the following nodes:

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

The following nodes will also require restarting:

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

Select one of the following options:

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

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

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



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



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

VLAN-Änderung der Appliance

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

Schritte

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

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

Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

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

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

Demo Zur Migration

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

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

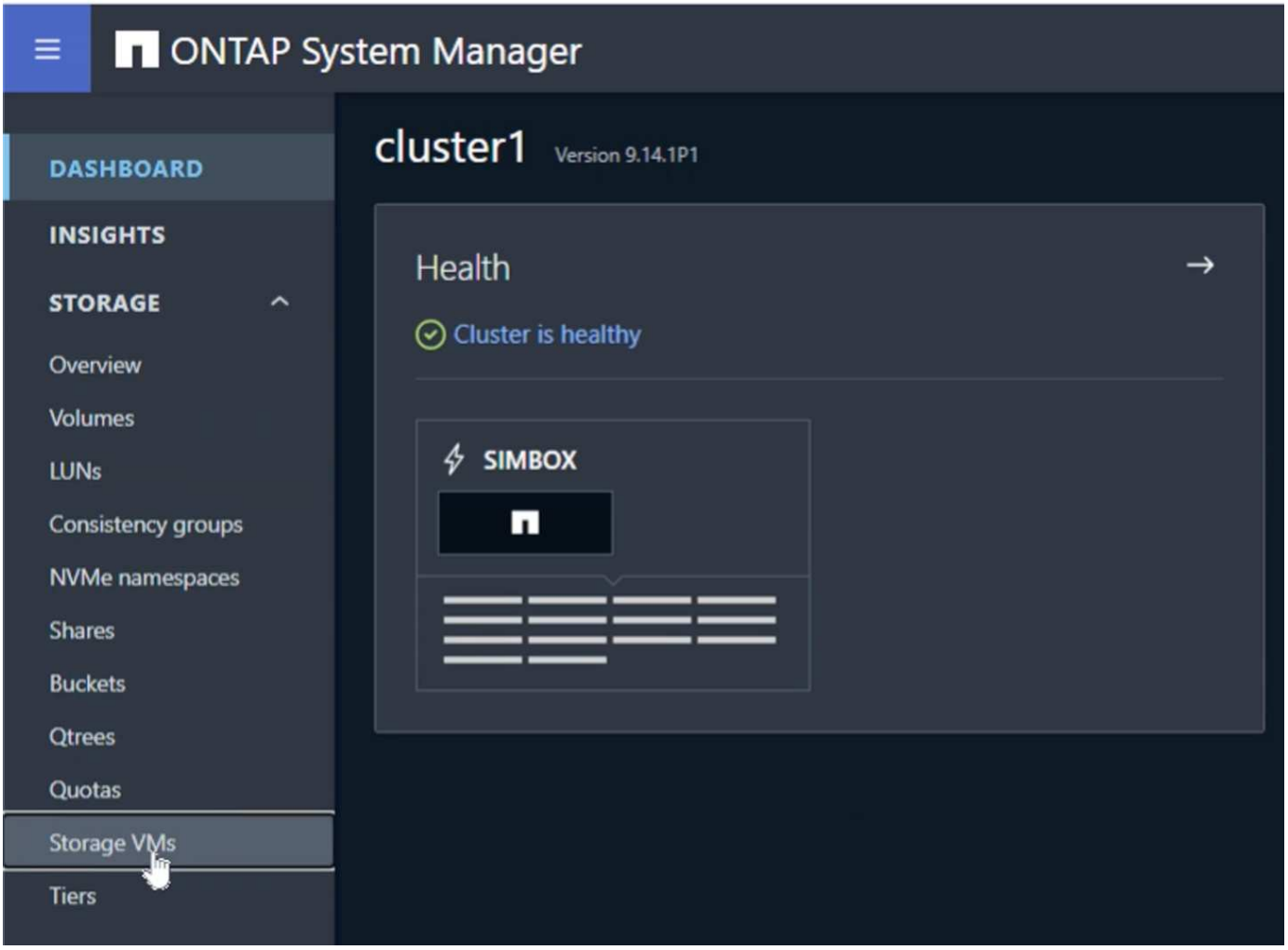
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

ONTAP wird vorbereitet

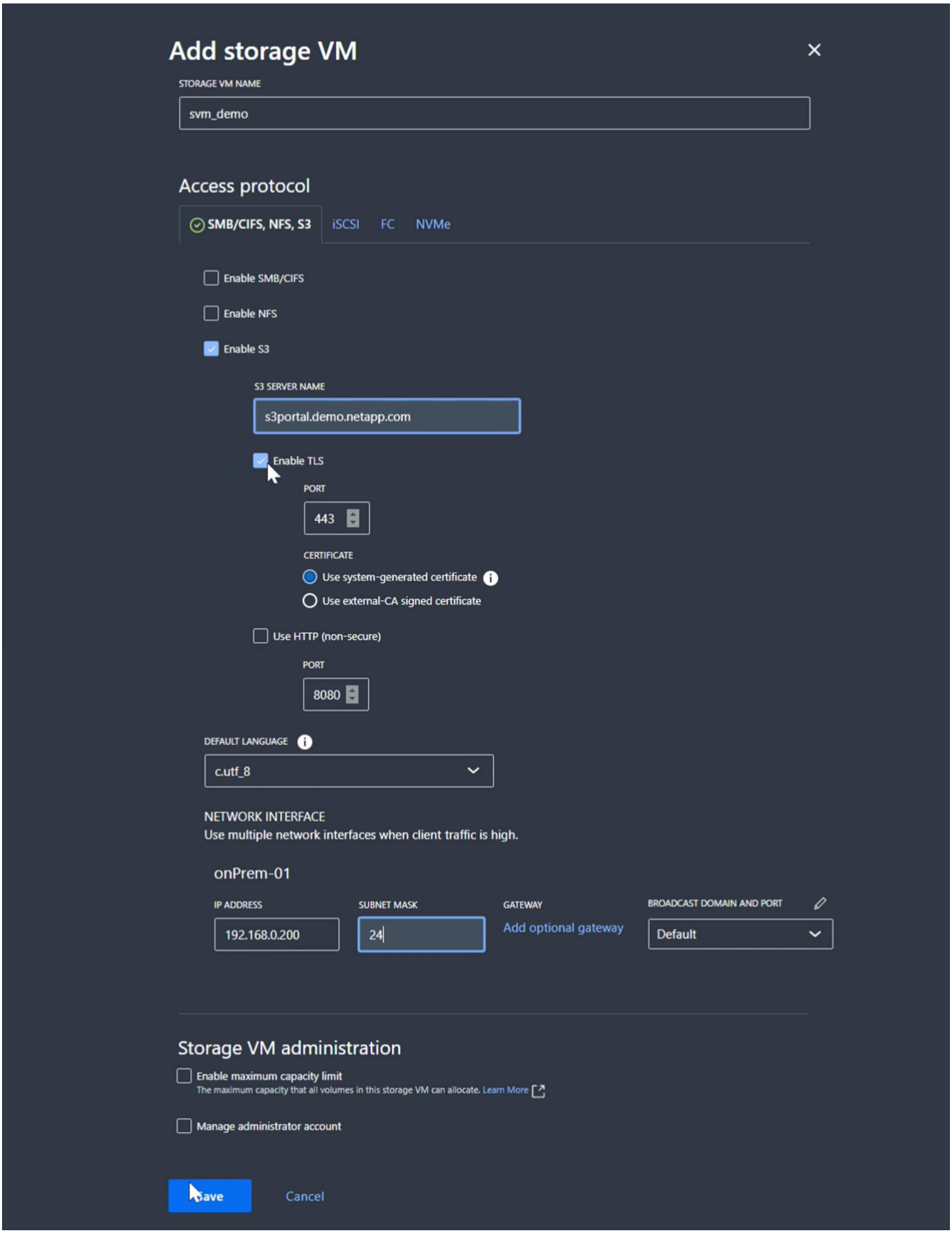
Für Demonstrationszwecke werden ein SVM Objektspeicher-Server, Benutzer, Gruppen, Gruppenrichtlinien und Buckets erstellt.

Erstellen Sie die virtuelle Speichermaschine

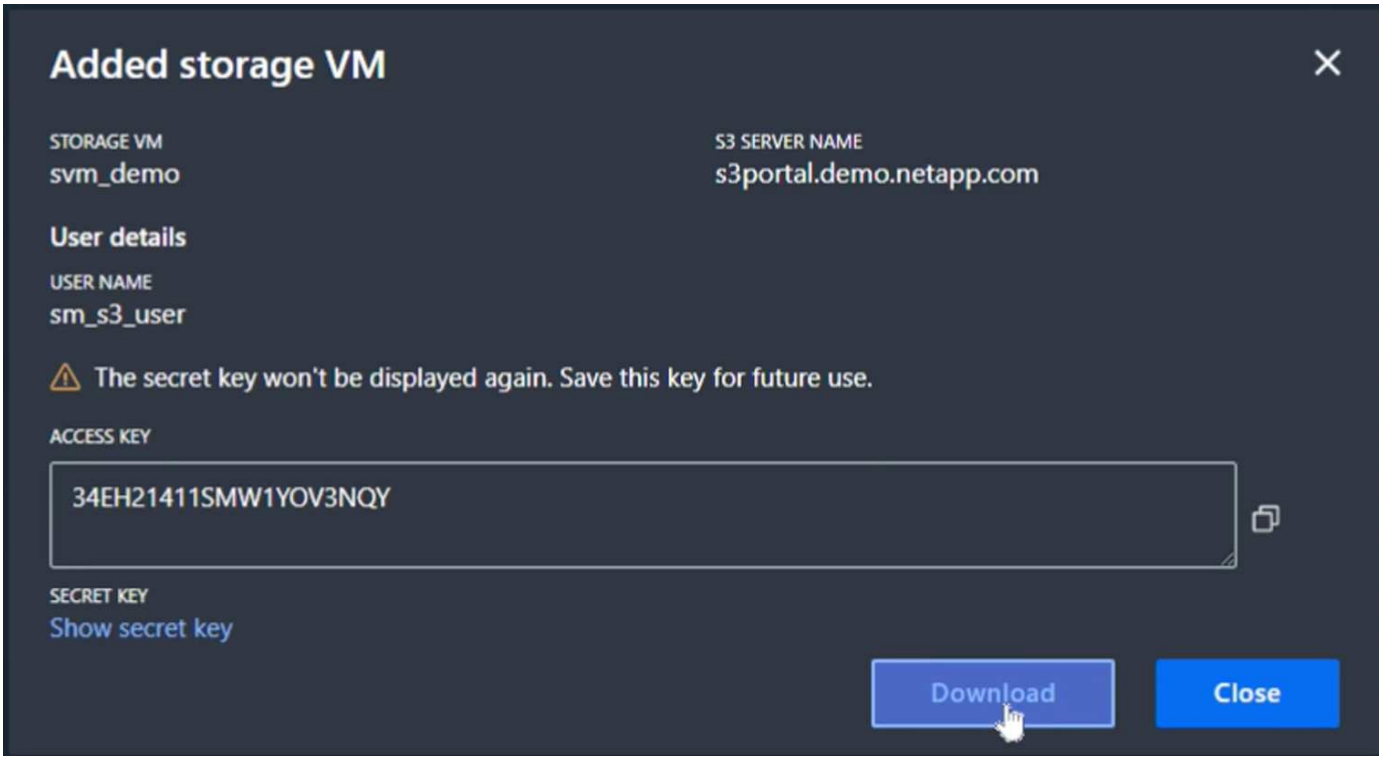
Navigieren Sie im ONTAP System Manager zu Storage VMs und fügen Sie eine neue Storage VM hinzu.



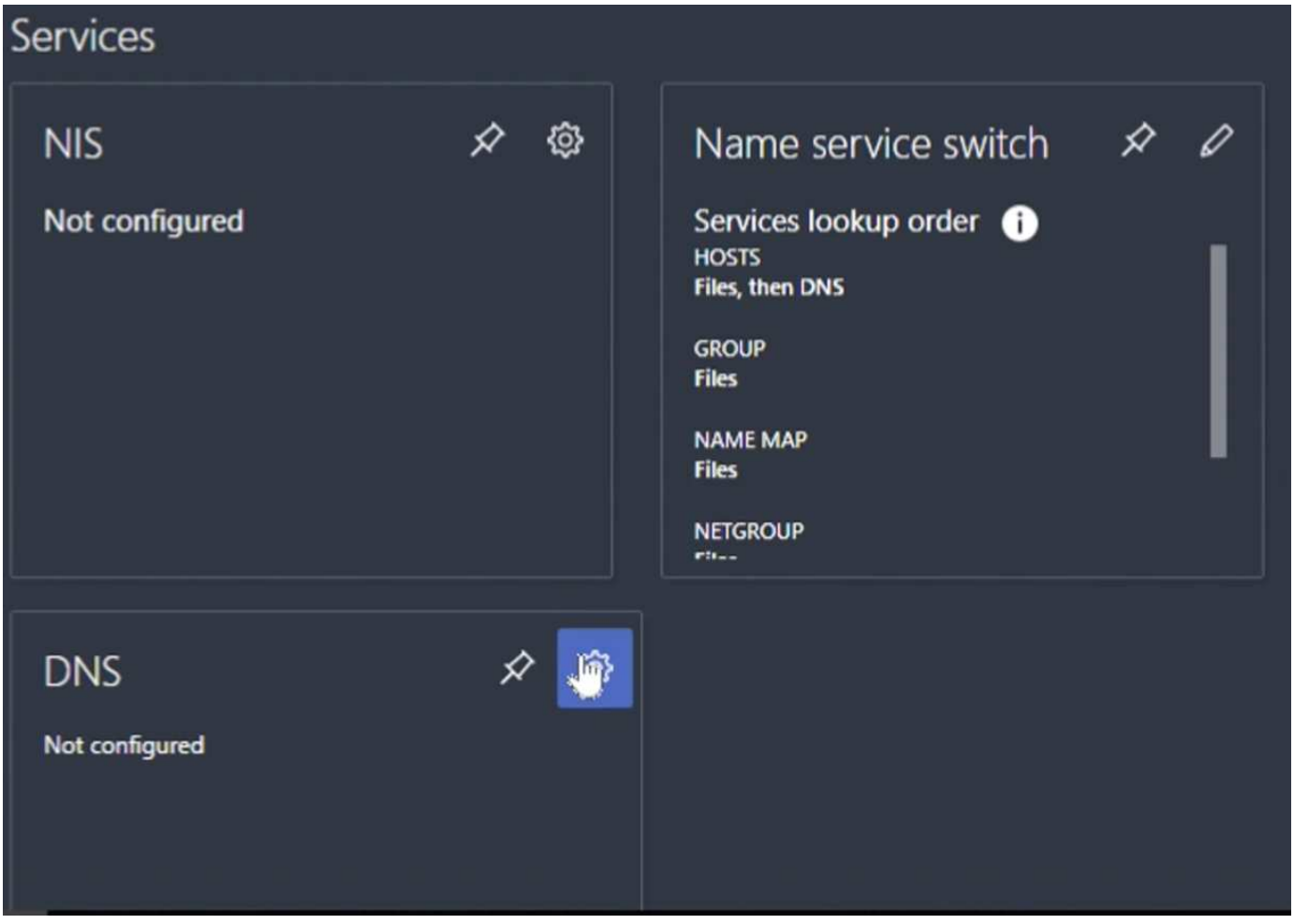
Aktivieren Sie die Kontrollkästchen „S3 aktivieren“ und „TLS aktivieren“, und konfigurieren Sie die HTTP(S)-Ports. Definieren Sie die IP-Adresse und die Subnetzmaske und definieren Sie das Gateway und die Broadcast-Domäne, wenn Sie nicht den Standard oder die in Ihrer Umgebung erforderlichen Standards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



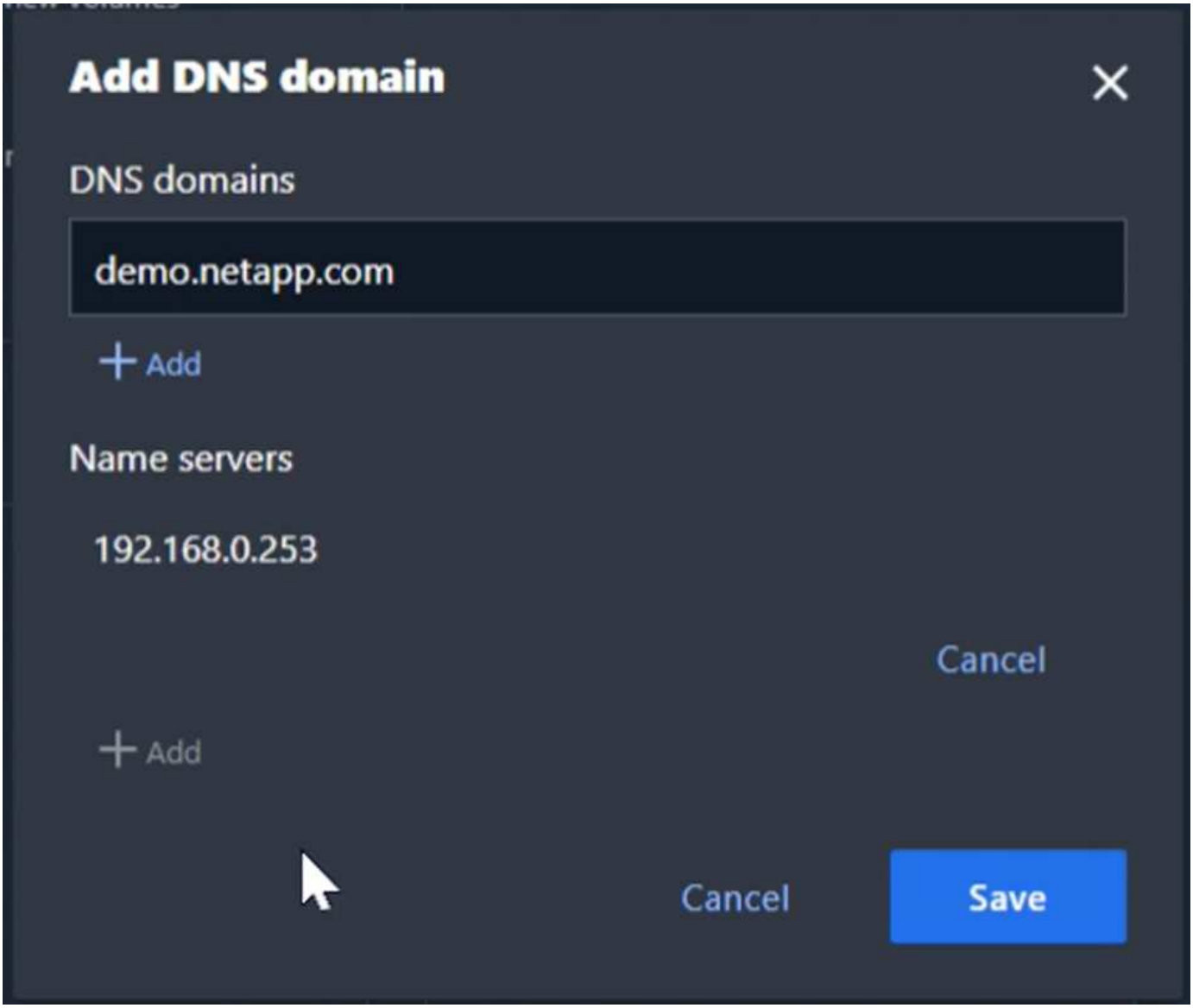
Im Rahmen der SVM-Erstellung wird ein Benutzer erstellt. Laden Sie die S3-Schlüssel für diesen Benutzer herunter, und schließen Sie das Fenster.



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

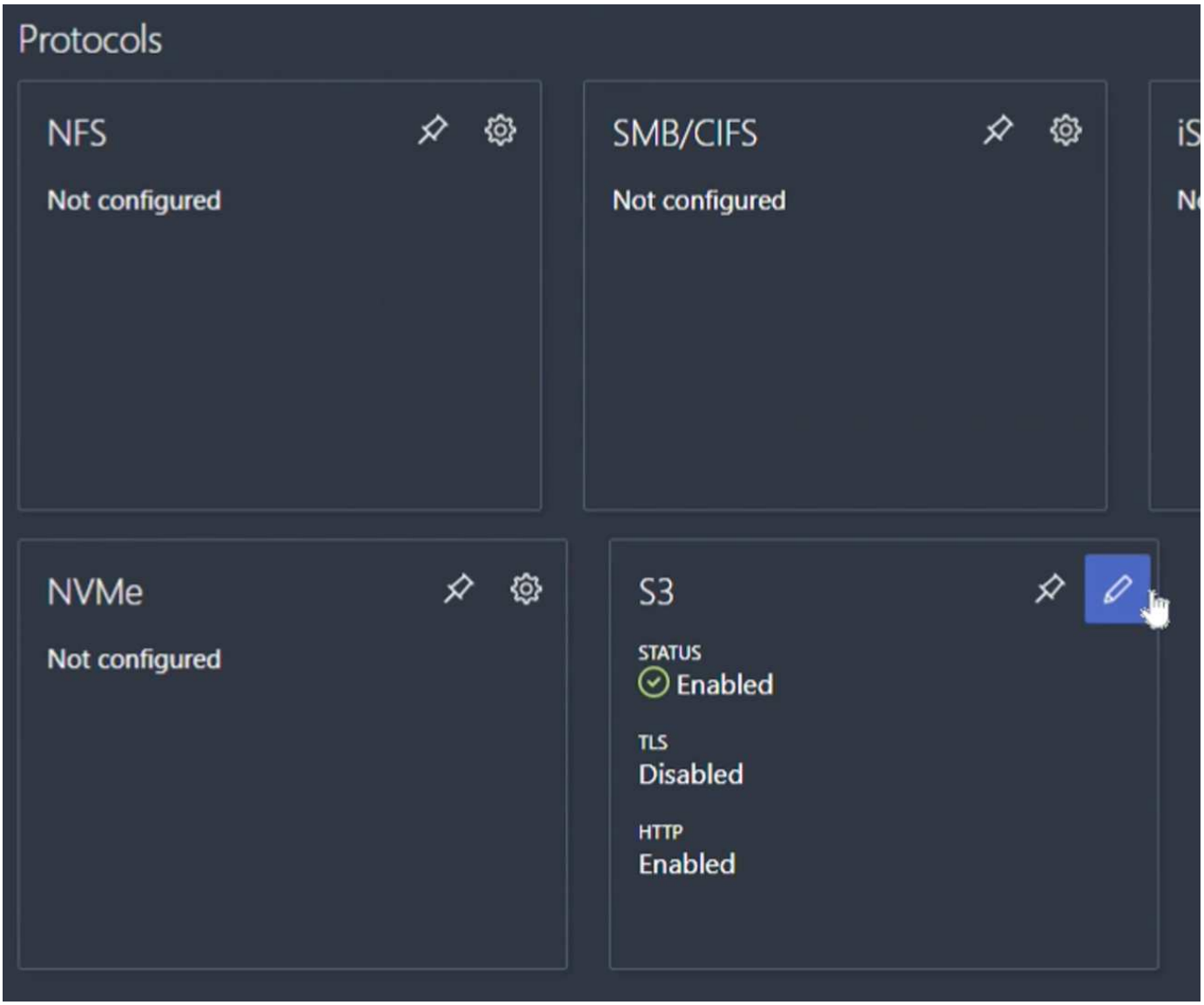


Definieren Sie den DNS-Namen und die IP-Adresse.

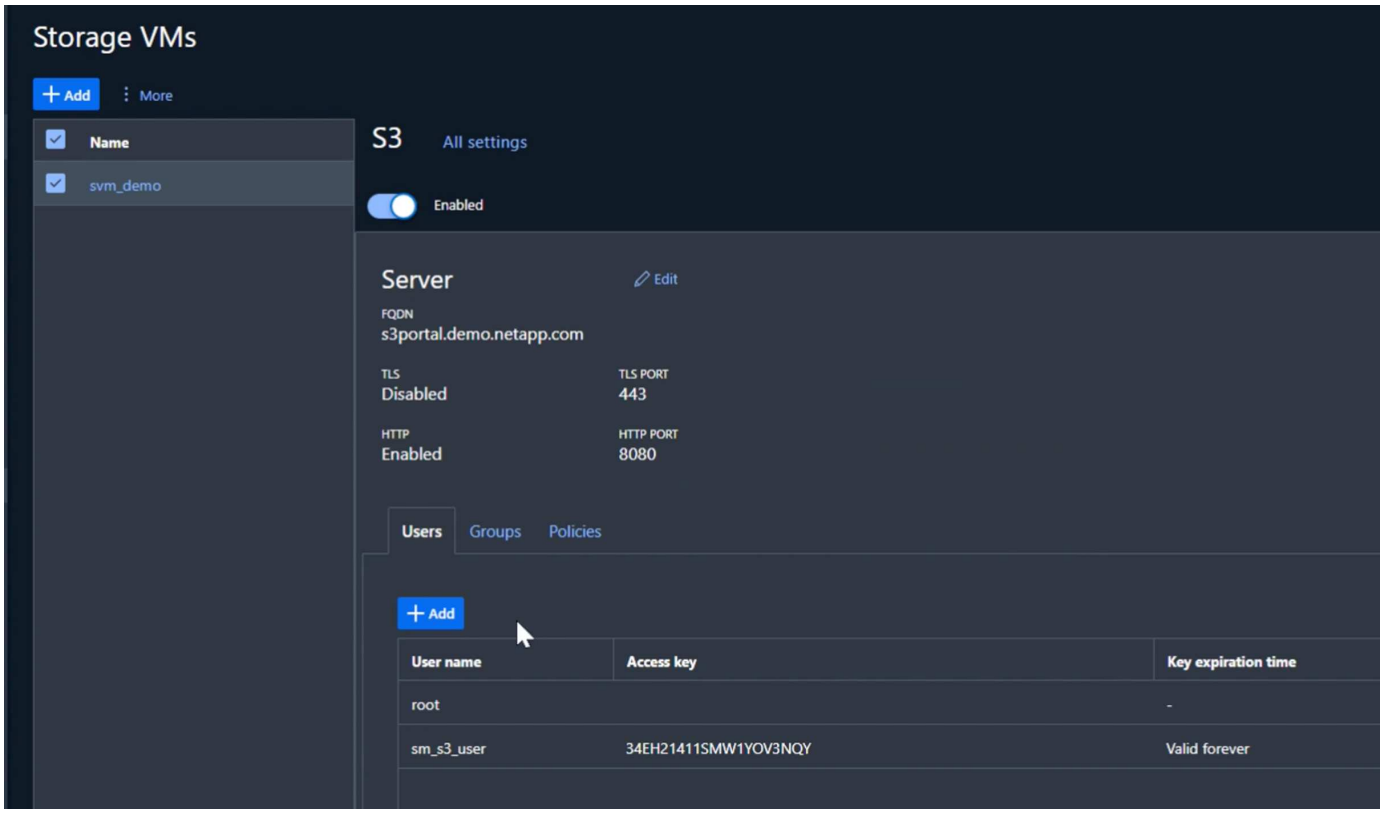


SVM S3-Benutzer erstellen

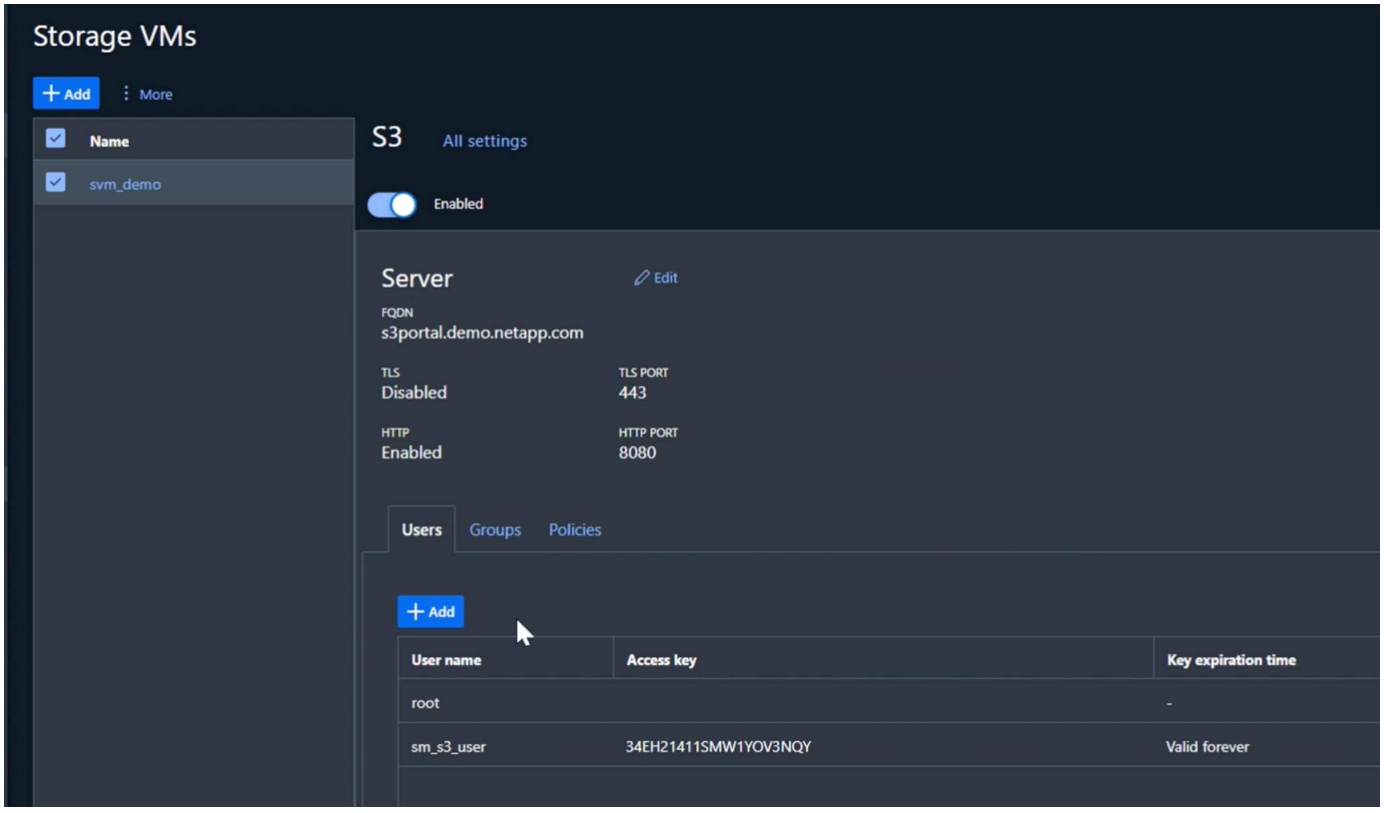
Jetzt können wir die S3-Benutzer und -Gruppe konfigurieren. Bearbeiten Sie die S3-Einstellungen.



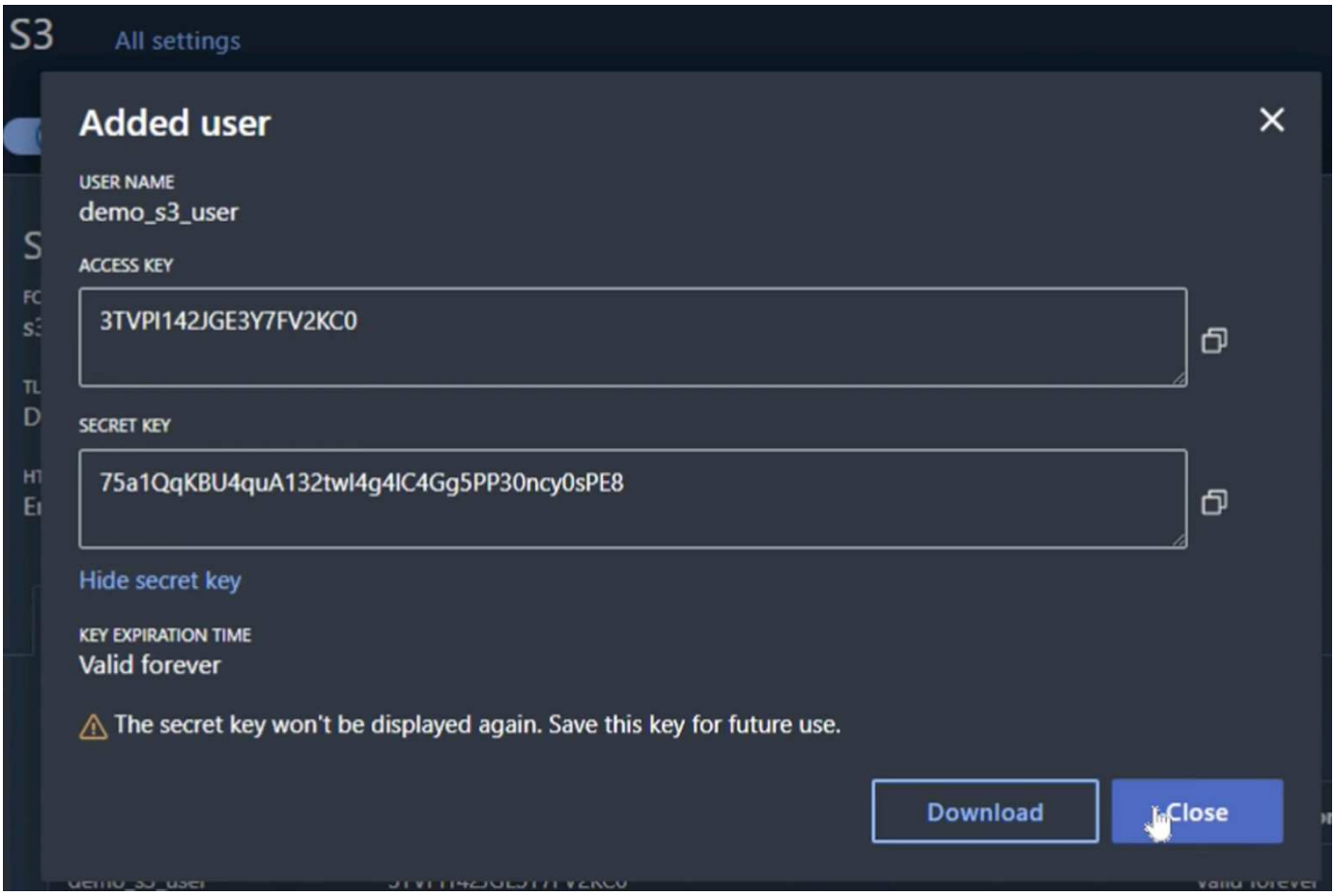
Neuen Benutzer hinzufügen.



Geben Sie den Benutzernamen und den Ablauf des Schlüssels ein.

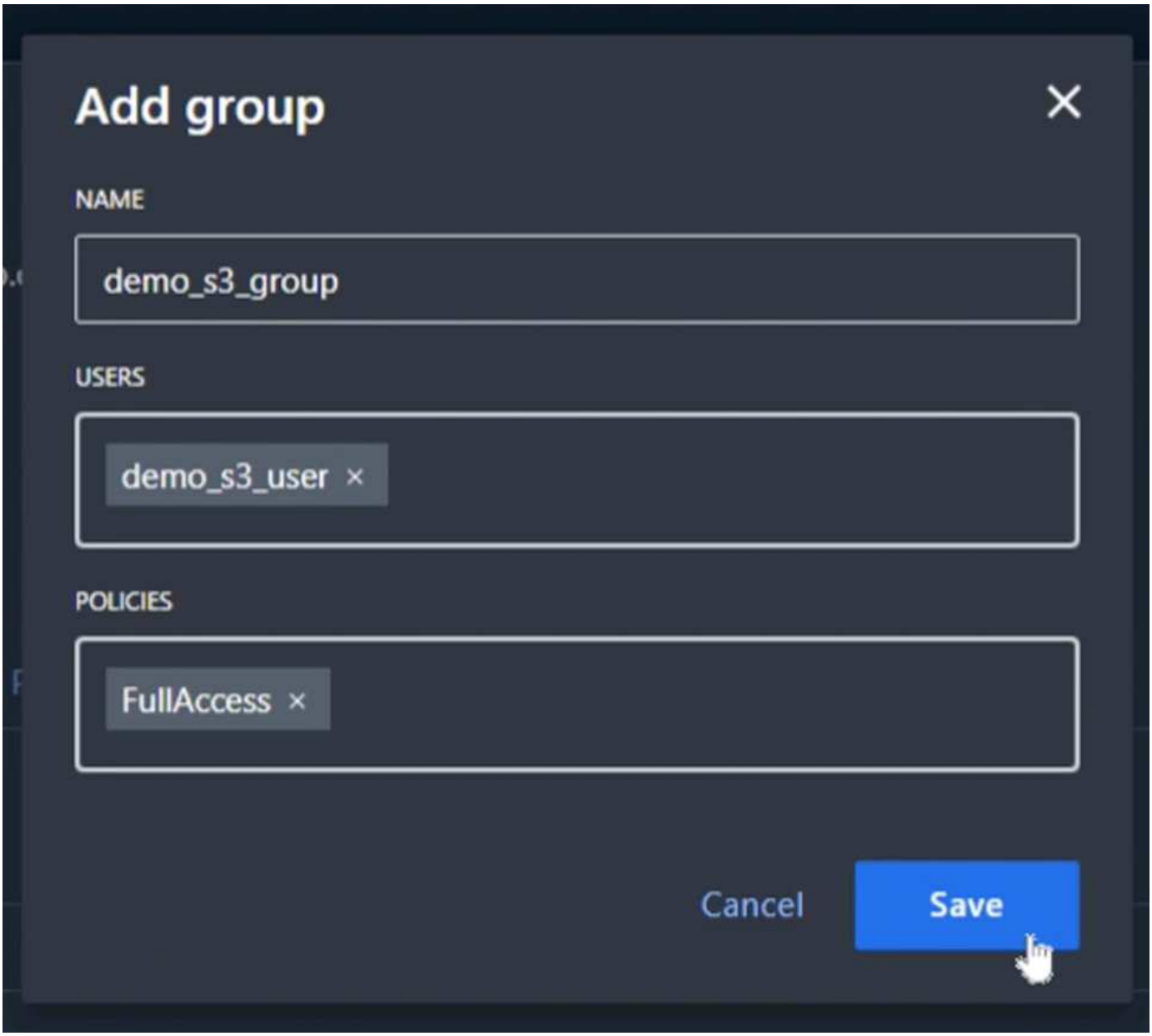


Laden Sie die S3-Schlüssel für den neuen Benutzer herunter.



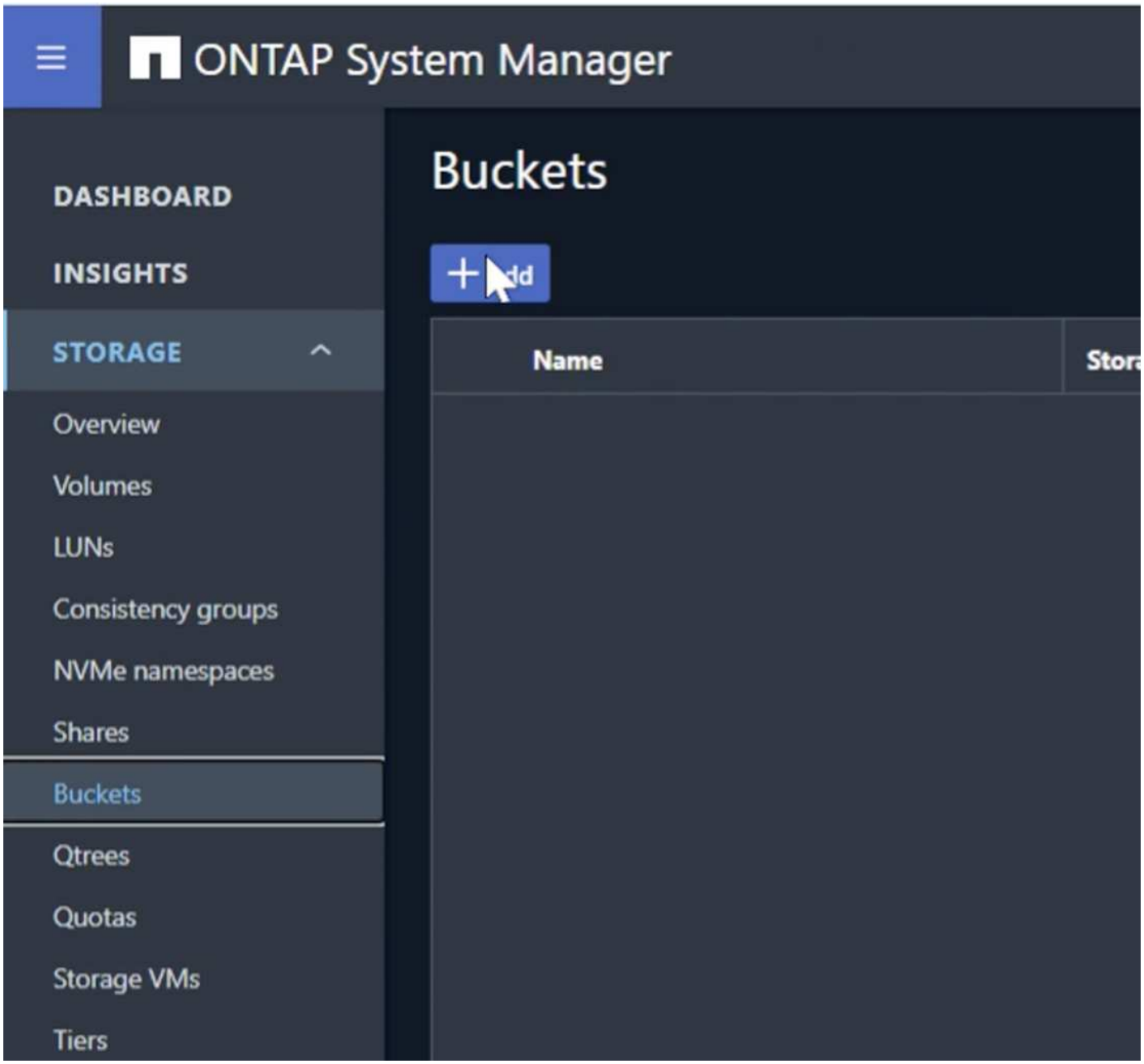
SVM S3-Gruppe erstellen

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

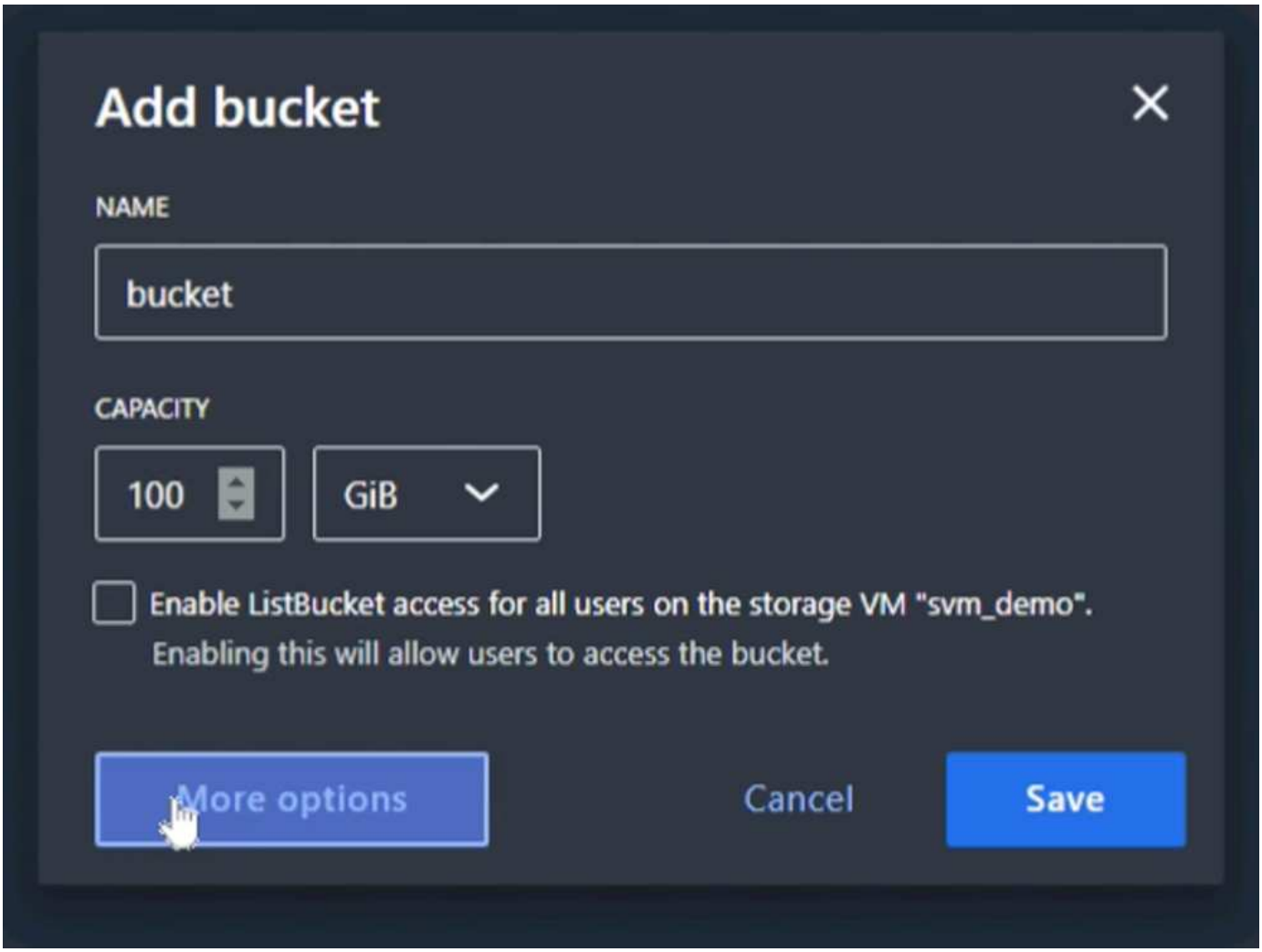


Erstellung von SVM S3 Buckets

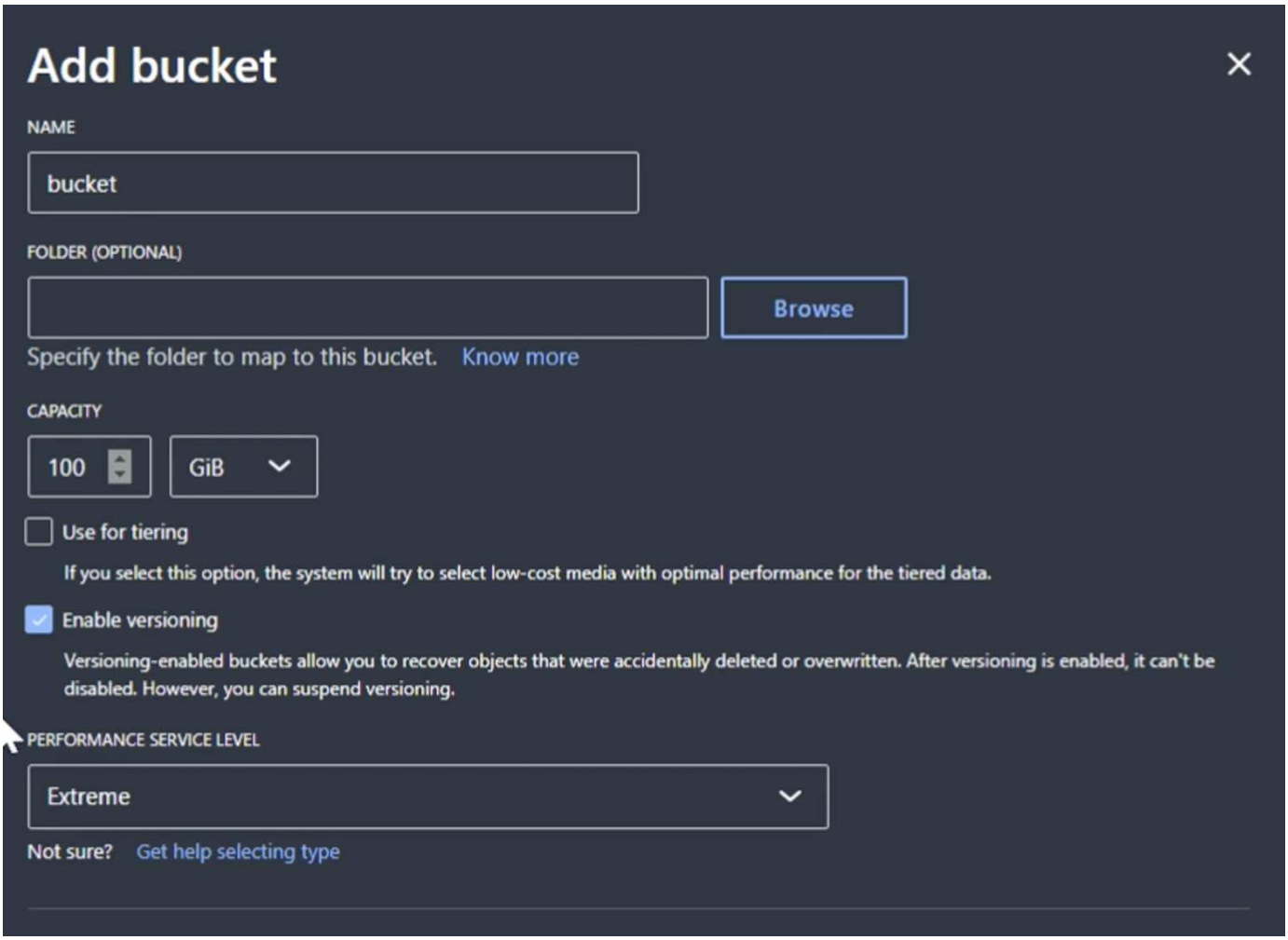
Navigieren Sie zum Bereich „Buckets“, und klicken Sie auf die Schaltfläche „+Hinzufügen“.



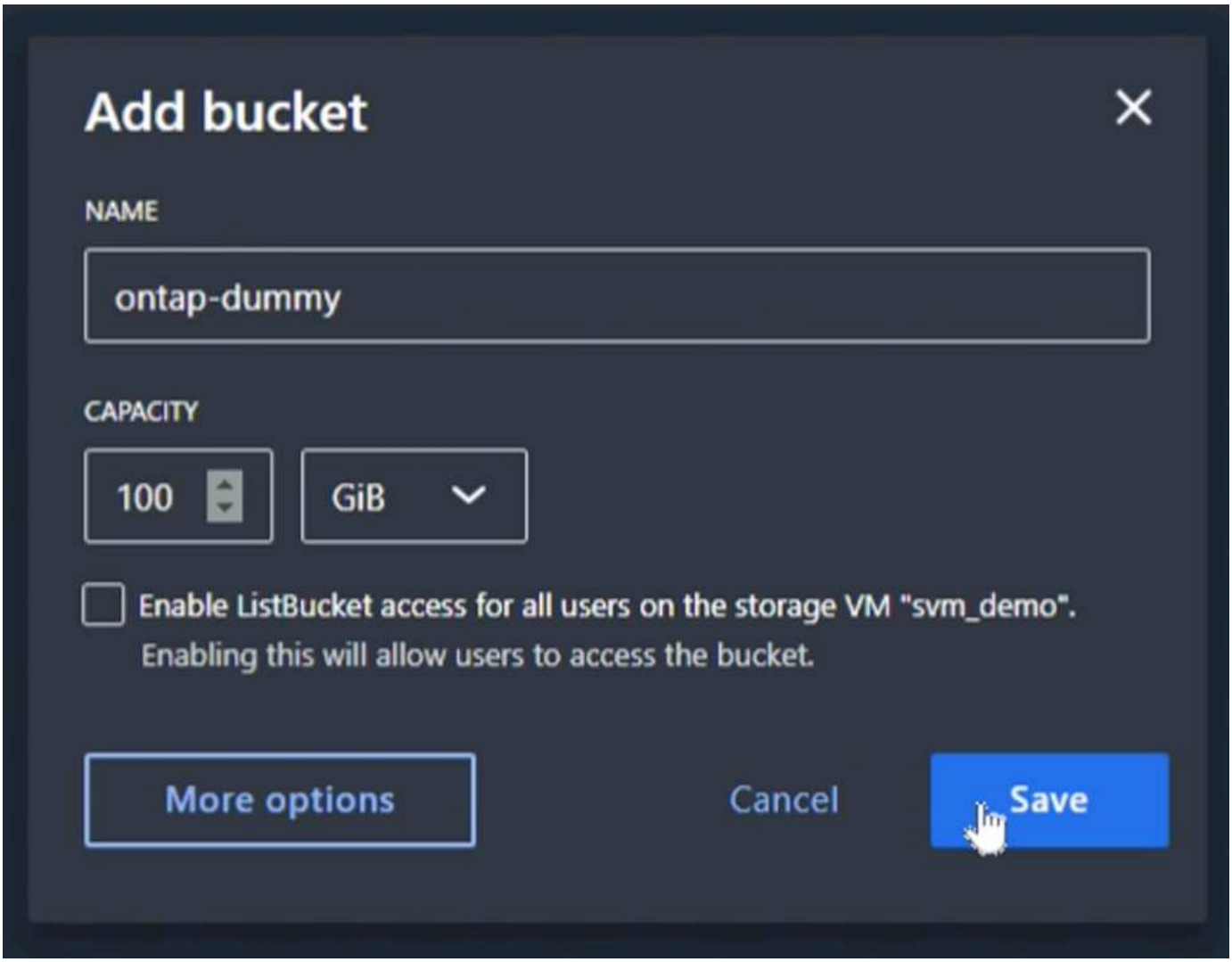
Geben Sie einen Namen und eine Kapazität ein, und deaktivieren Sie das Kontrollkästchen „Zugriff auf ListBucket aktivieren…“. Klicken Sie anschließend auf die Schaltfläche „Weitere Optionen“.



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



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



Von Rafael Guedes und Aron Klein

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

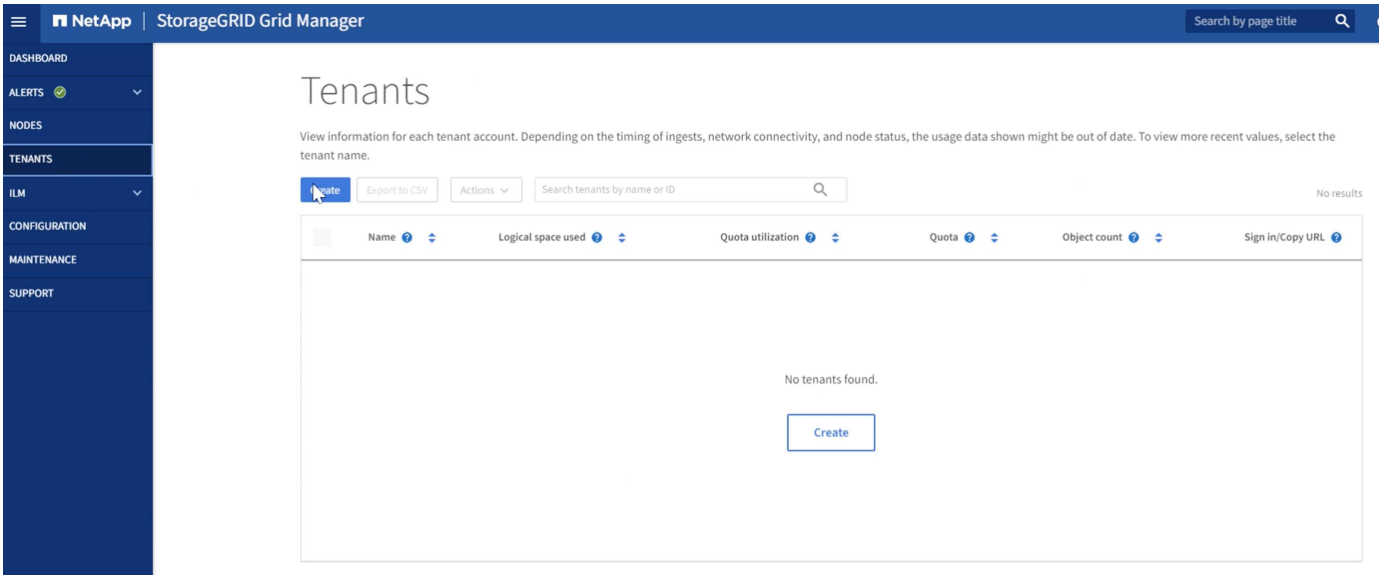
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

StorageGRID wird vorbereitet

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

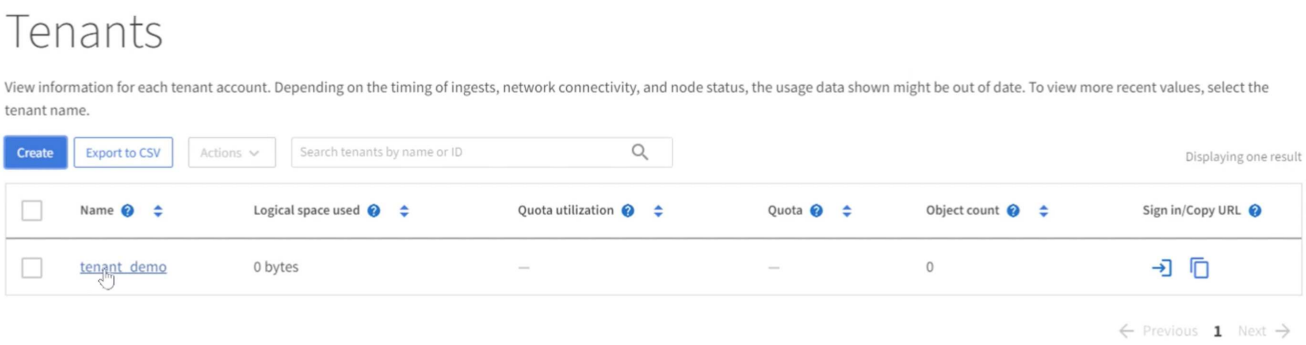
Erstellen Sie die Serviceeinheit

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

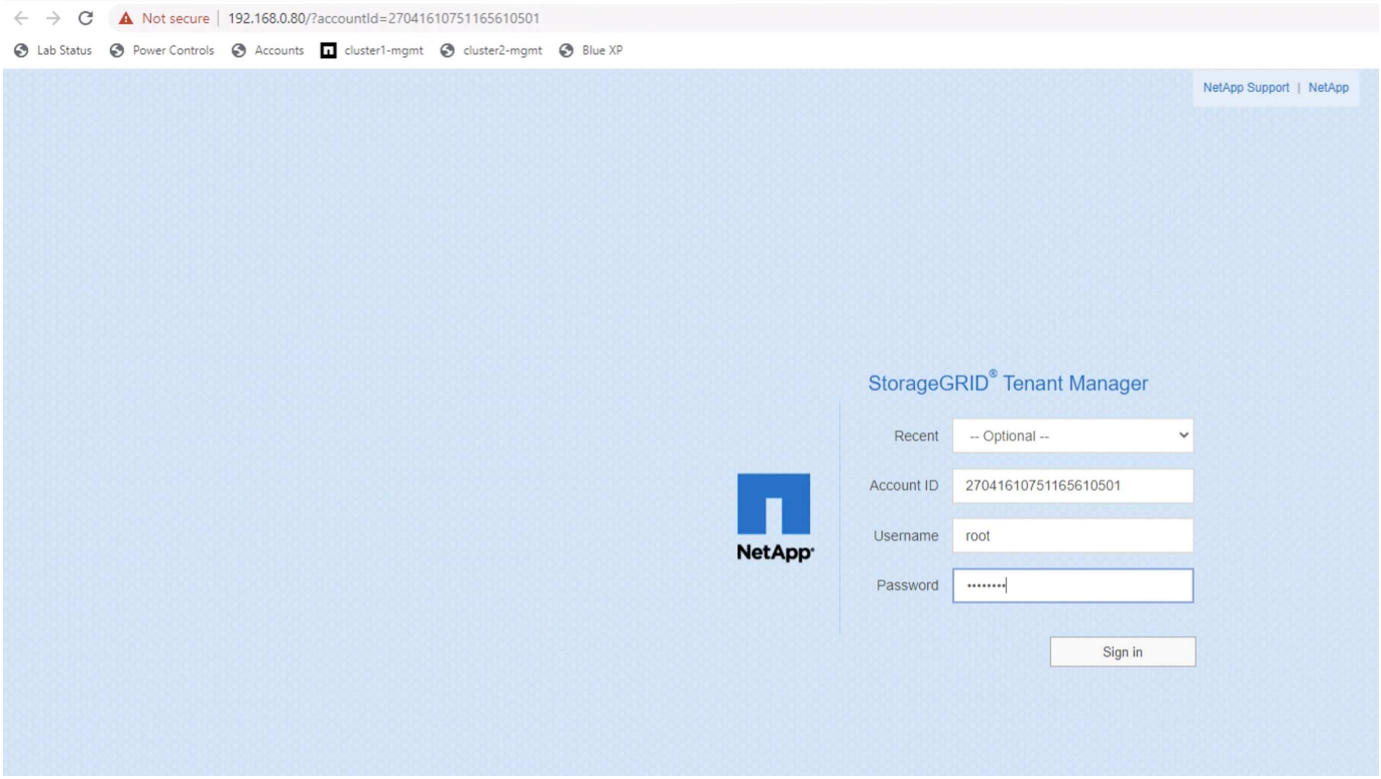


Geben Sie die Details für den Mandanten ein, indem Sie einen Mandantennamen angeben, und wählen Sie S3 für den Clienttyp aus. Es ist kein Kontingent erforderlich. Plattformdienste müssen nicht ausgewählt oder S3-Auswahl zugelassen werden. Sie können wählen, ob Sie eine eigene Identitätsquelle verwenden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

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

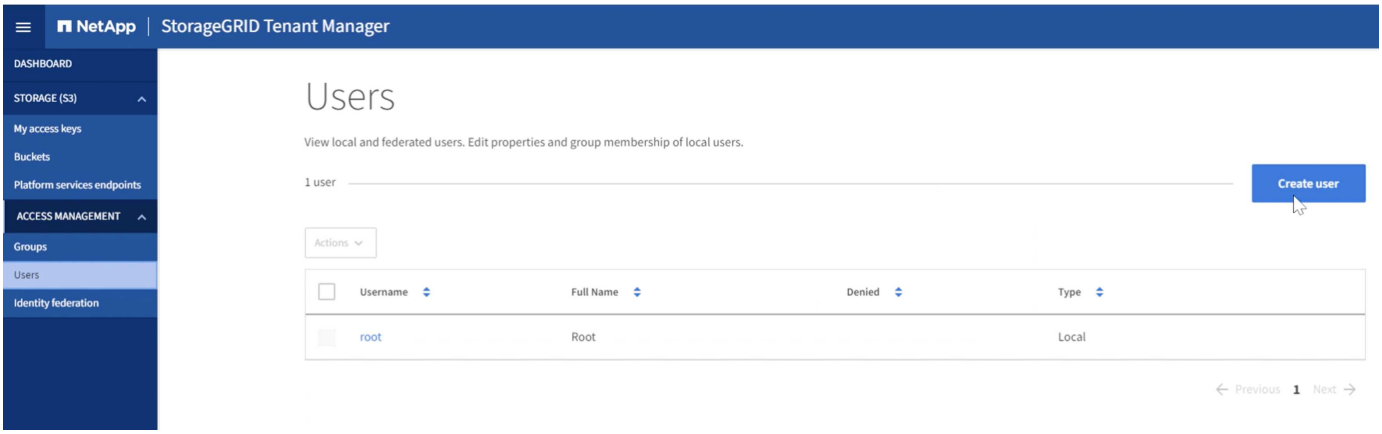


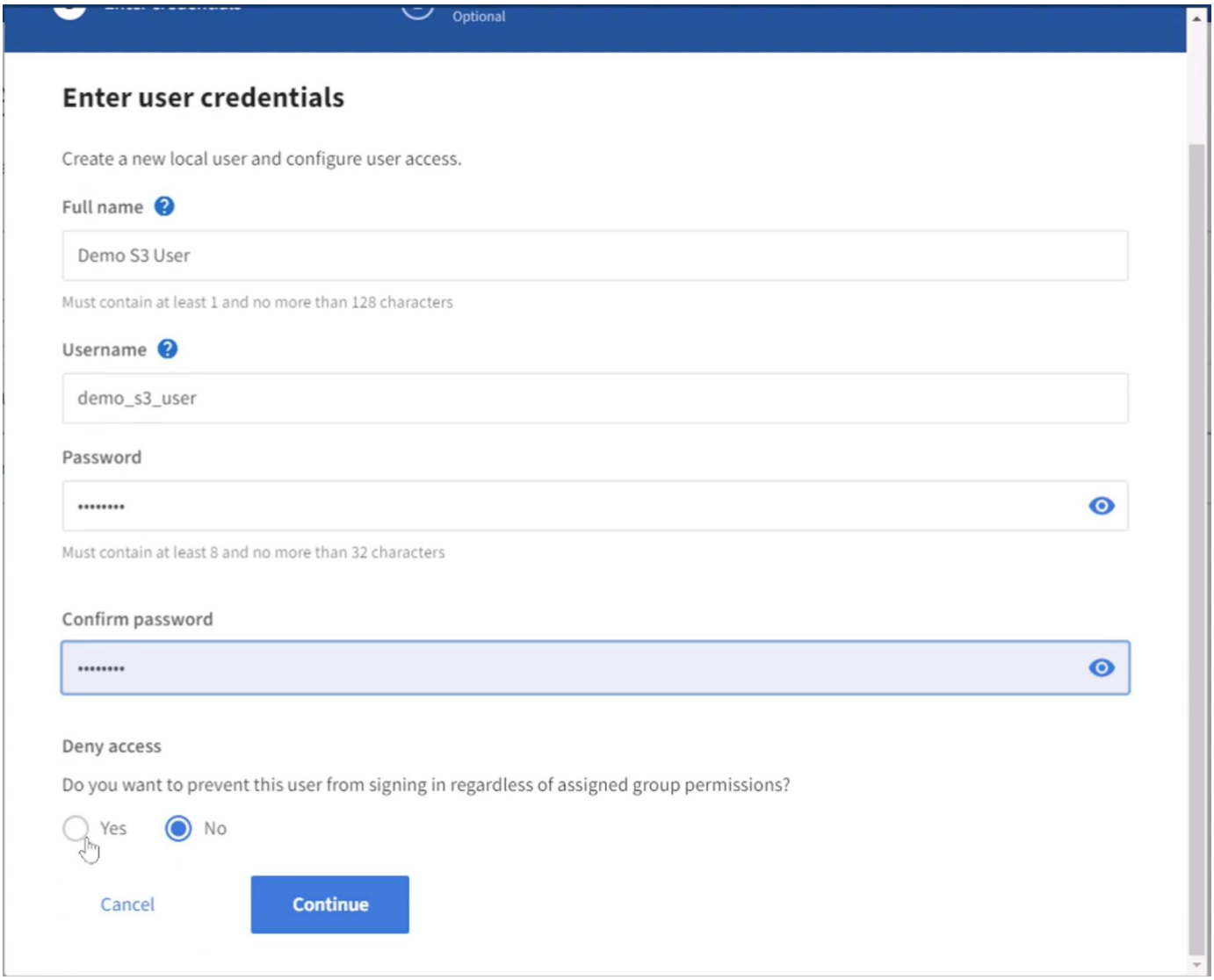
Dadurch gelangen Sie zur Anmeldung beim Mandantenportal. Speichern Sie die URL für die zukünftige Verwendung, und geben Sie die Anmeldedaten des Stammbenutzers ein.



Erstellen Sie den Benutzer

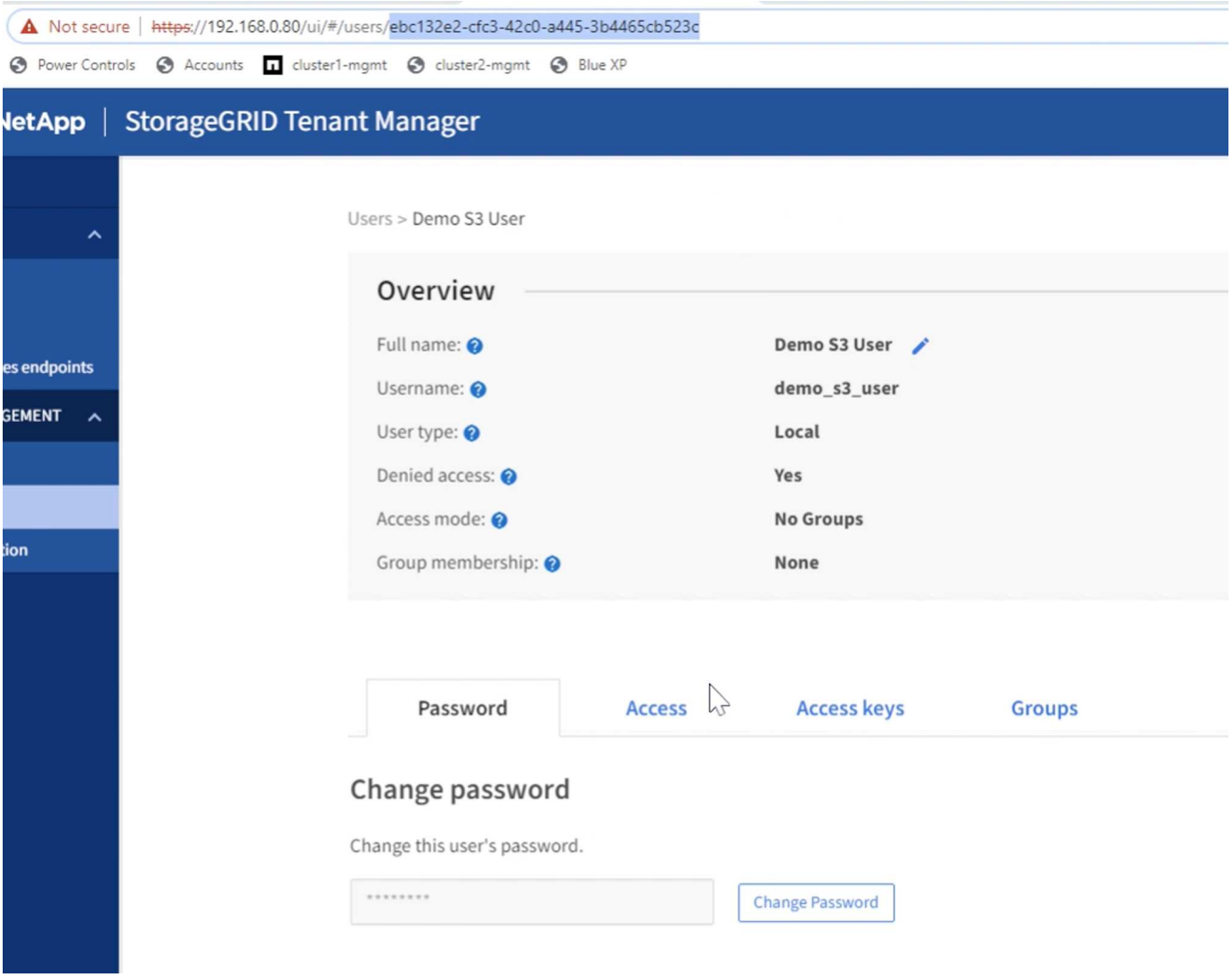
Navigieren Sie zur Registerkarte Benutzer, und erstellen Sie einen neuen Benutzer.



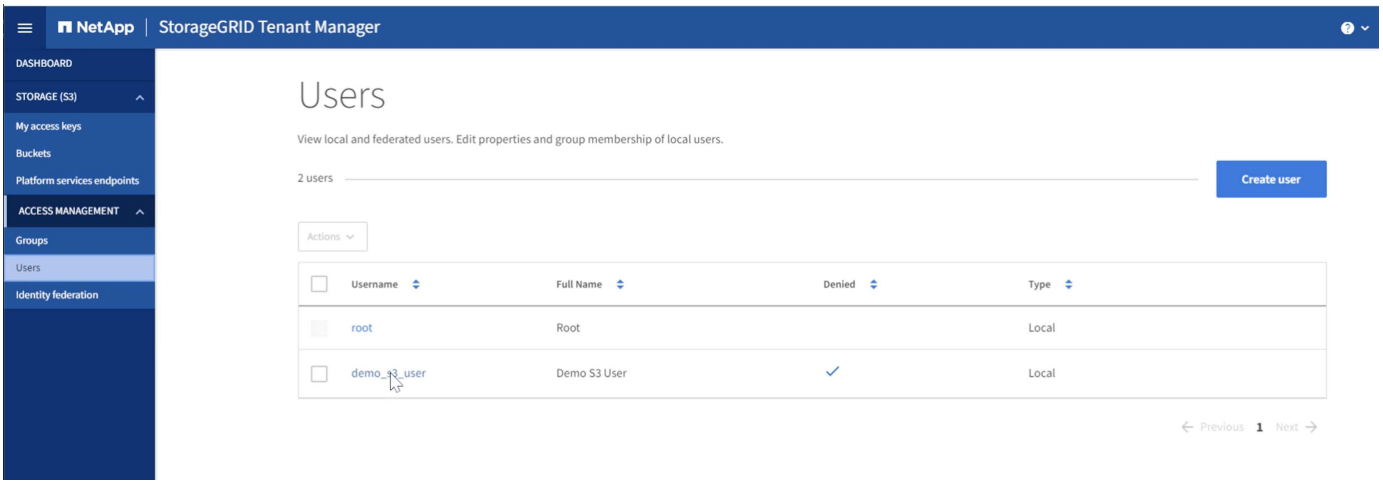


Nachdem der neue Benutzer erstellt wurde, klicken Sie auf den Benutzernamen, um die Details des Benutzers zu öffnen.

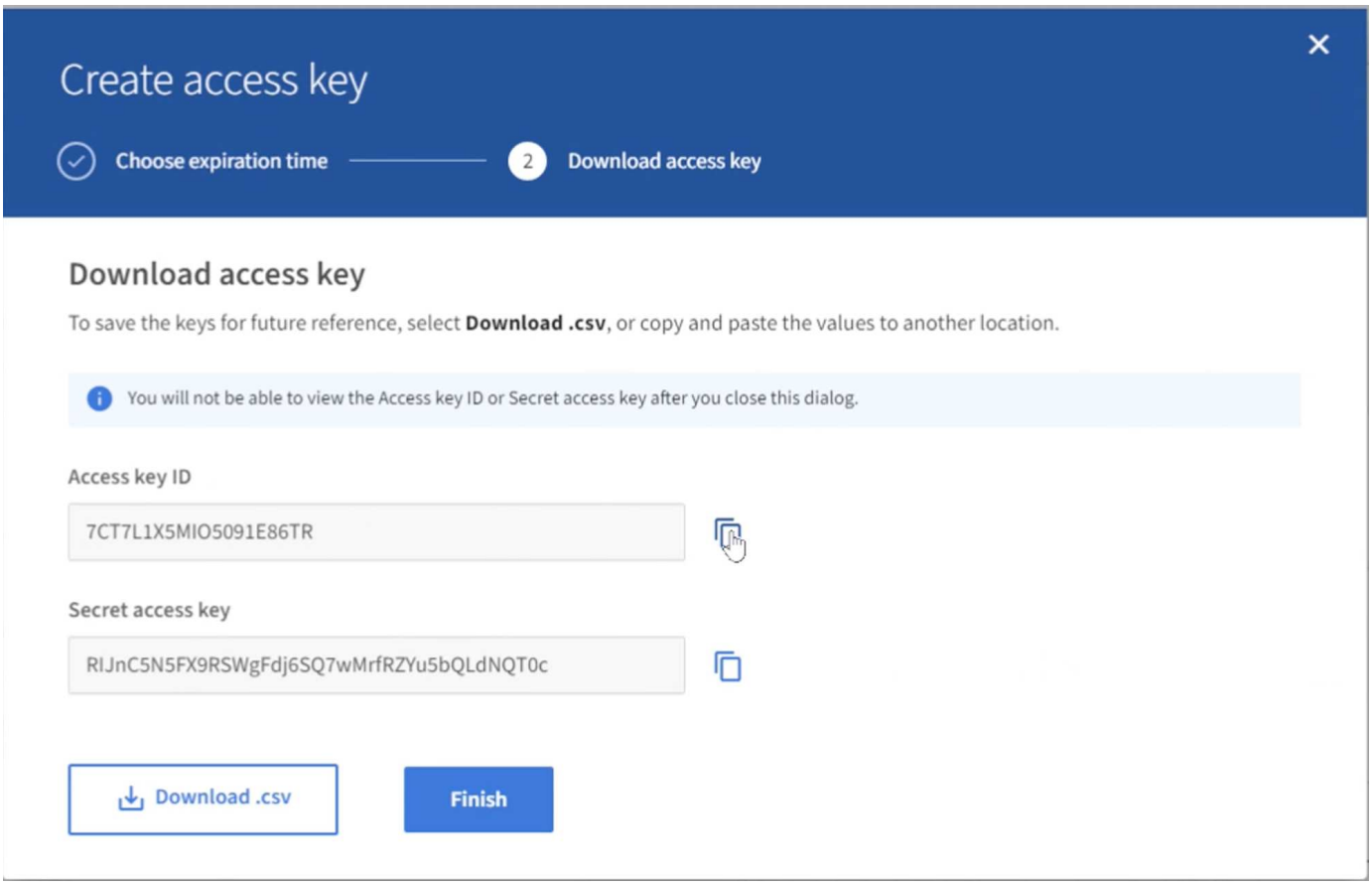
Kopieren Sie die Benutzer-ID aus der URL, die später verwendet werden soll.



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

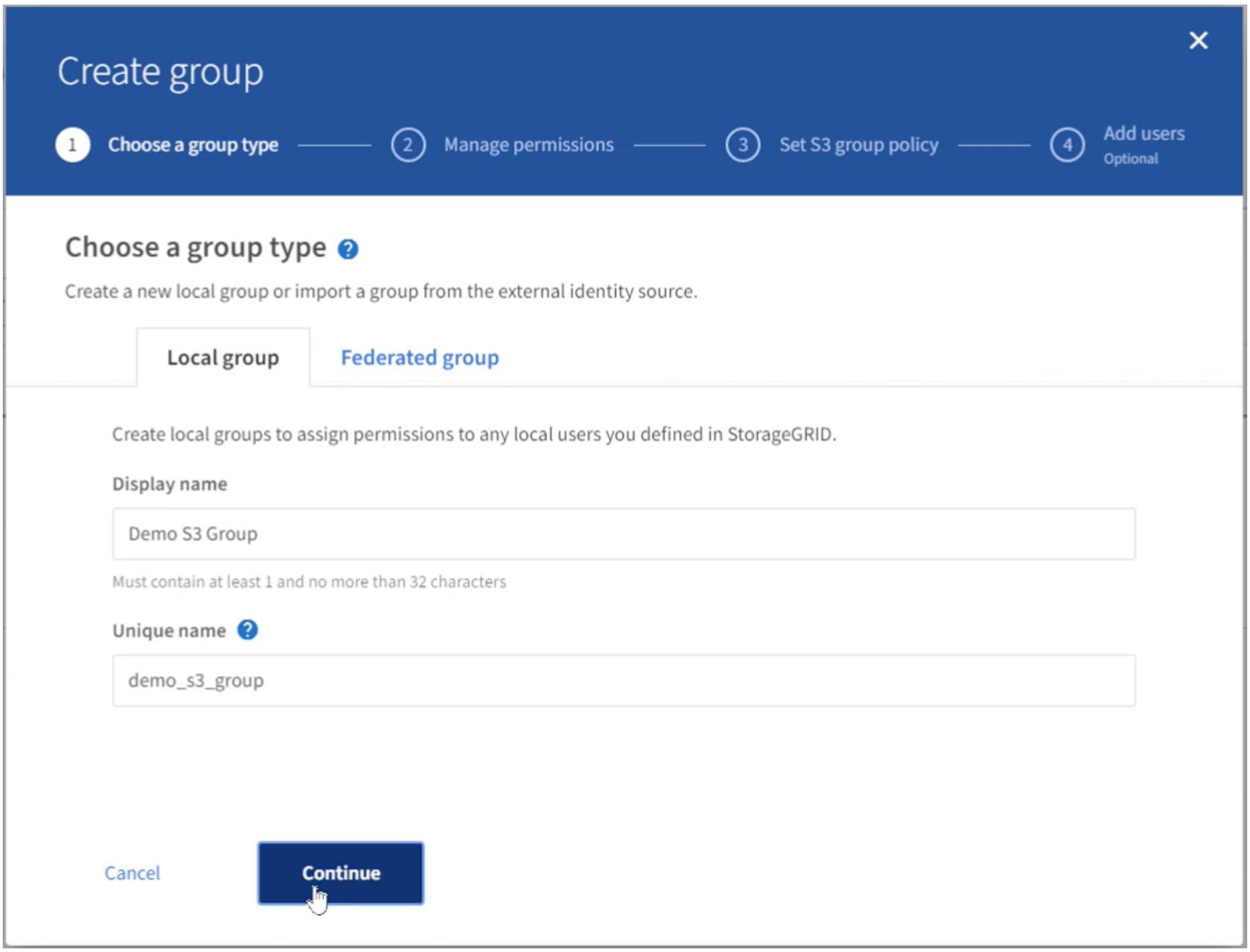


Wählen Sie die Registerkarte „Zugriffsschlüssel“ aus und klicken Sie auf die Schaltfläche „Schlüssel erstellen“. Es ist nicht notwendig, eine Verfallszeit einzustellen. Laden Sie die S3-Schlüssel herunter, da sie nach dem Schließen des Fensters nicht mehr abgerufen werden können.

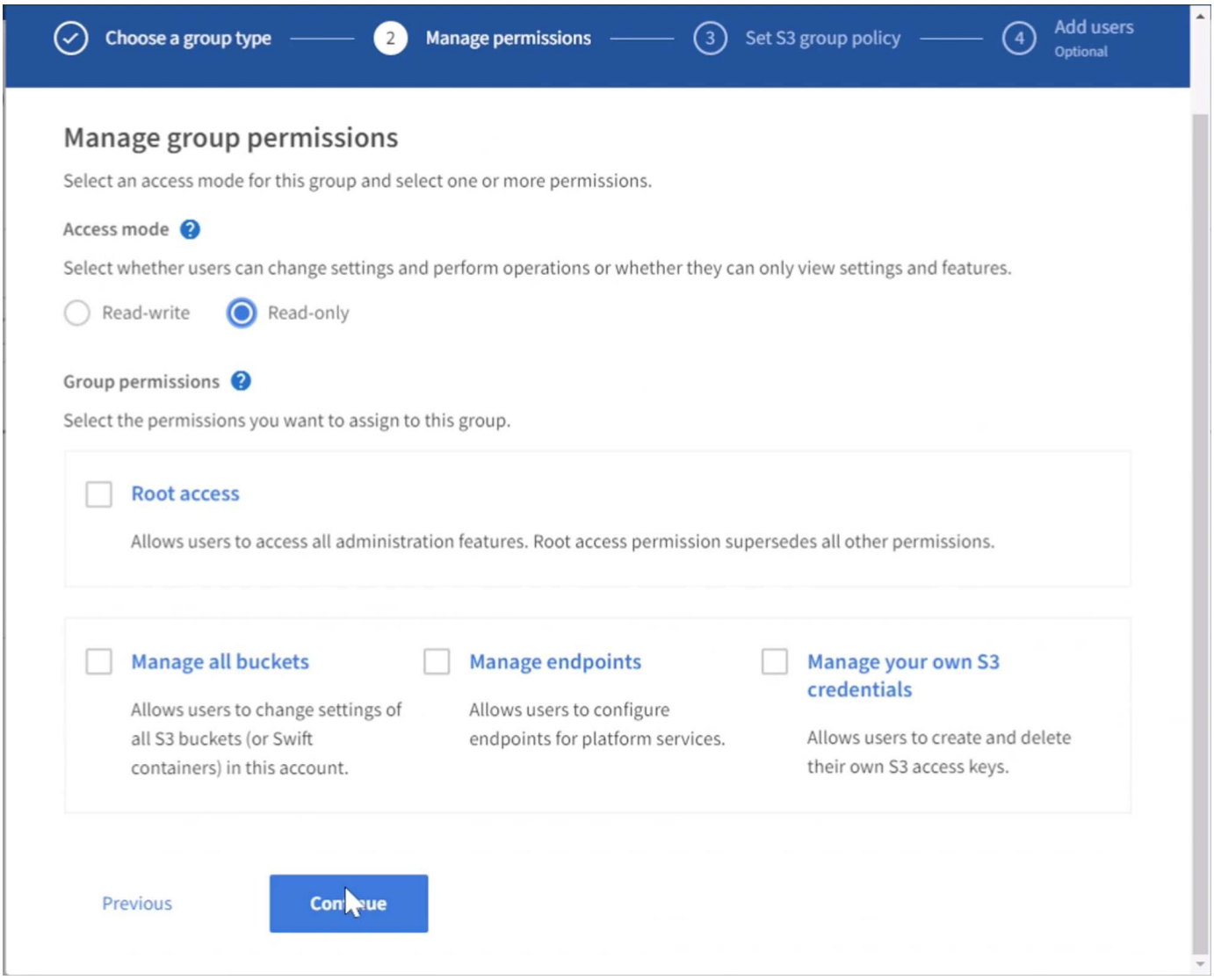


Erstellen Sie die Sicherheitsgruppe

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

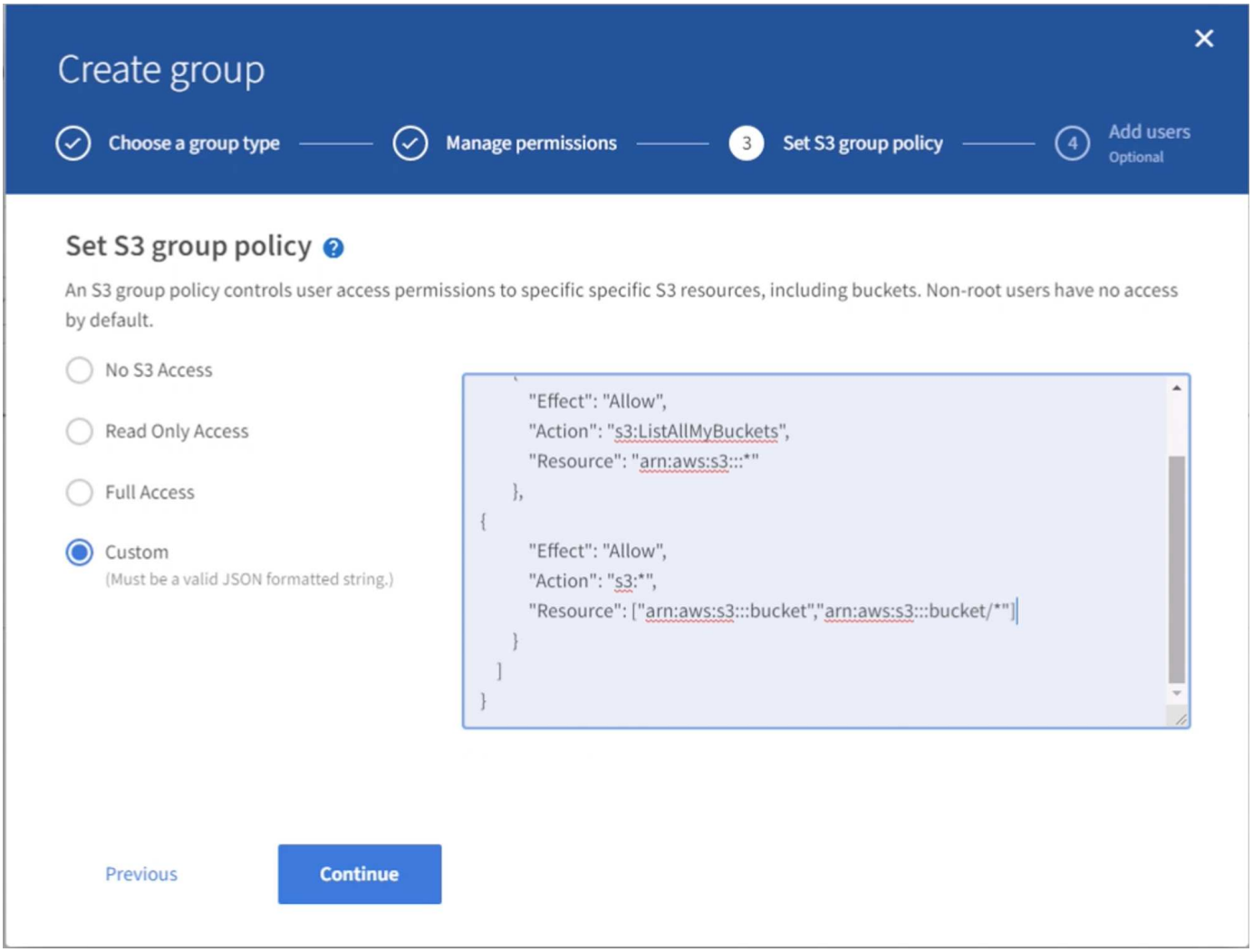


Legen Sie die Gruppenberechtigungen auf schreibgeschützt fest. Dies sind die Berechtigungen der Mandanten-UI, nicht die S3-Berechtigungen.

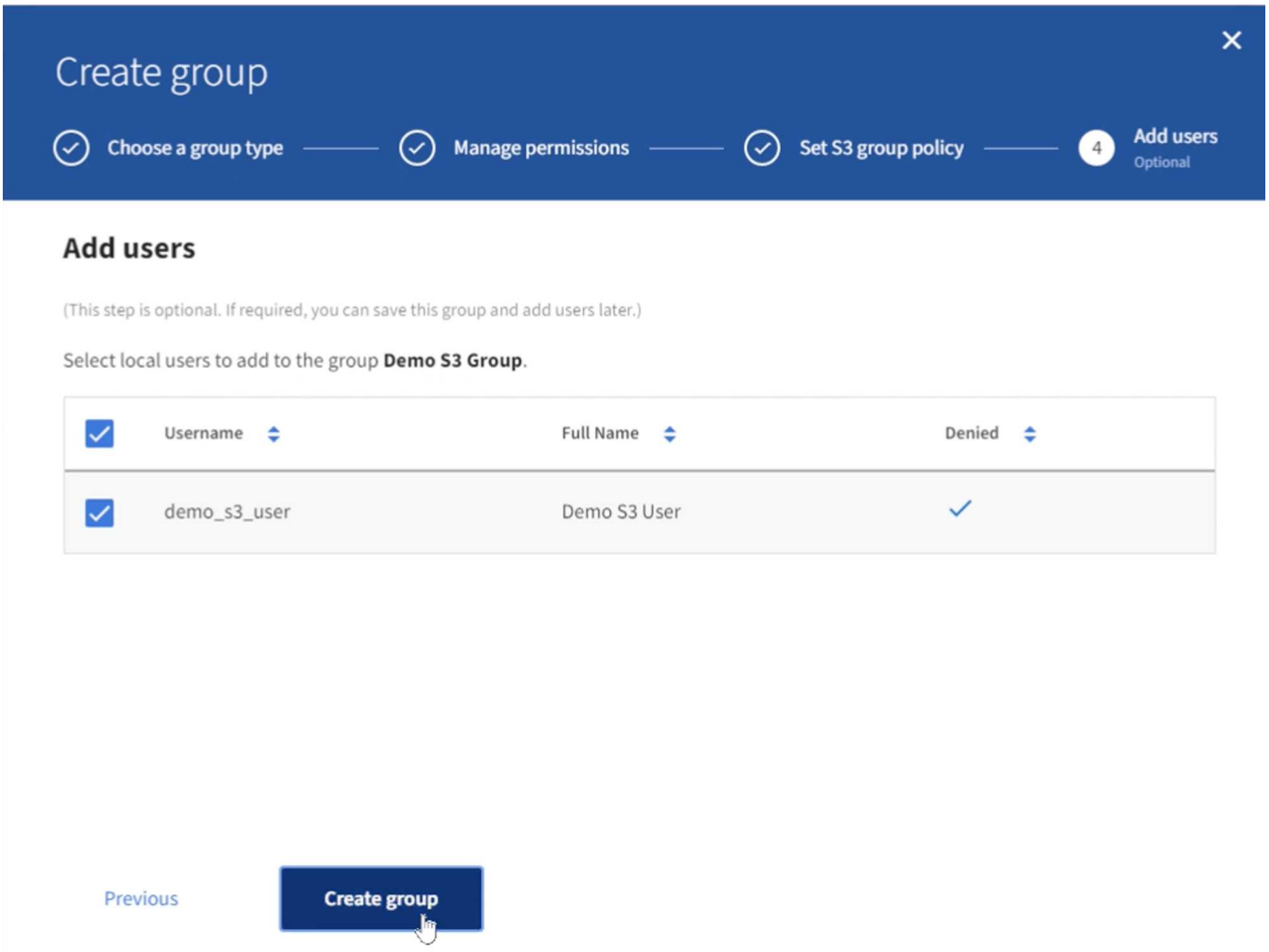


S3 Berechtigungen werden über die Gruppenrichtlinie (IAM-Richtlinie) gesteuert. Legen Sie die Gruppenrichtlinie auf Benutzerdefiniert fest, und fügen Sie die json-Richtlinie in das Feld ein. Diese Richtlinie ermöglicht Benutzern dieser Gruppe, die Buckets des Mandanten aufzulisten und alle S3-Vorgänge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

```
{
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
        "Action": "s3:*",
        "Resource": ["arn:aws:s3:::bucket","arn:aws:s3:::bucket/*"]
      }
    ]
}
```

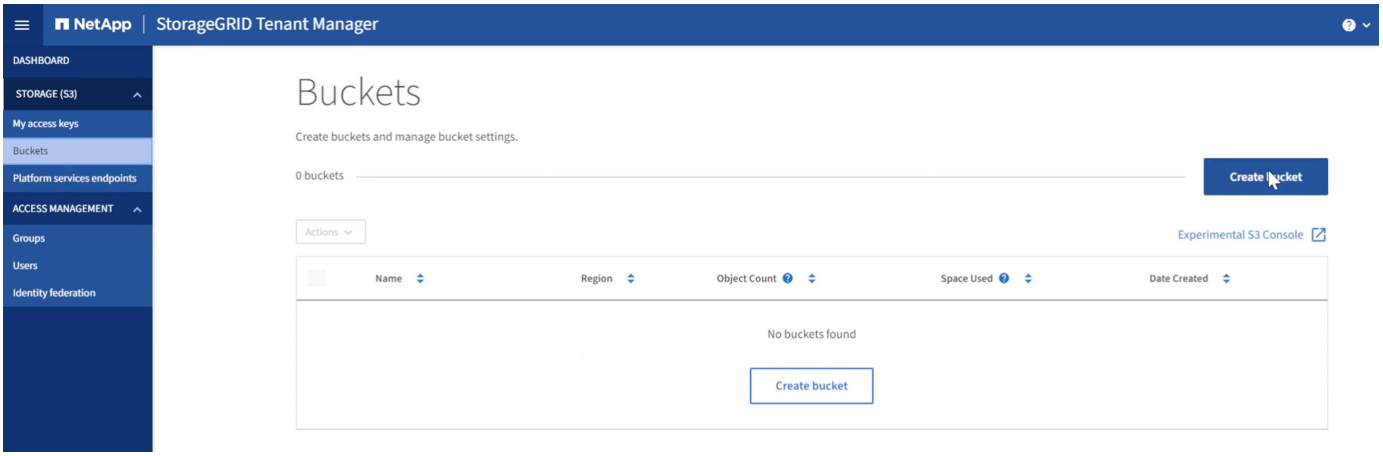


Fügen Sie schließlich den Benutzer zur Gruppe hinzu, und beenden Sie den Vorgang.

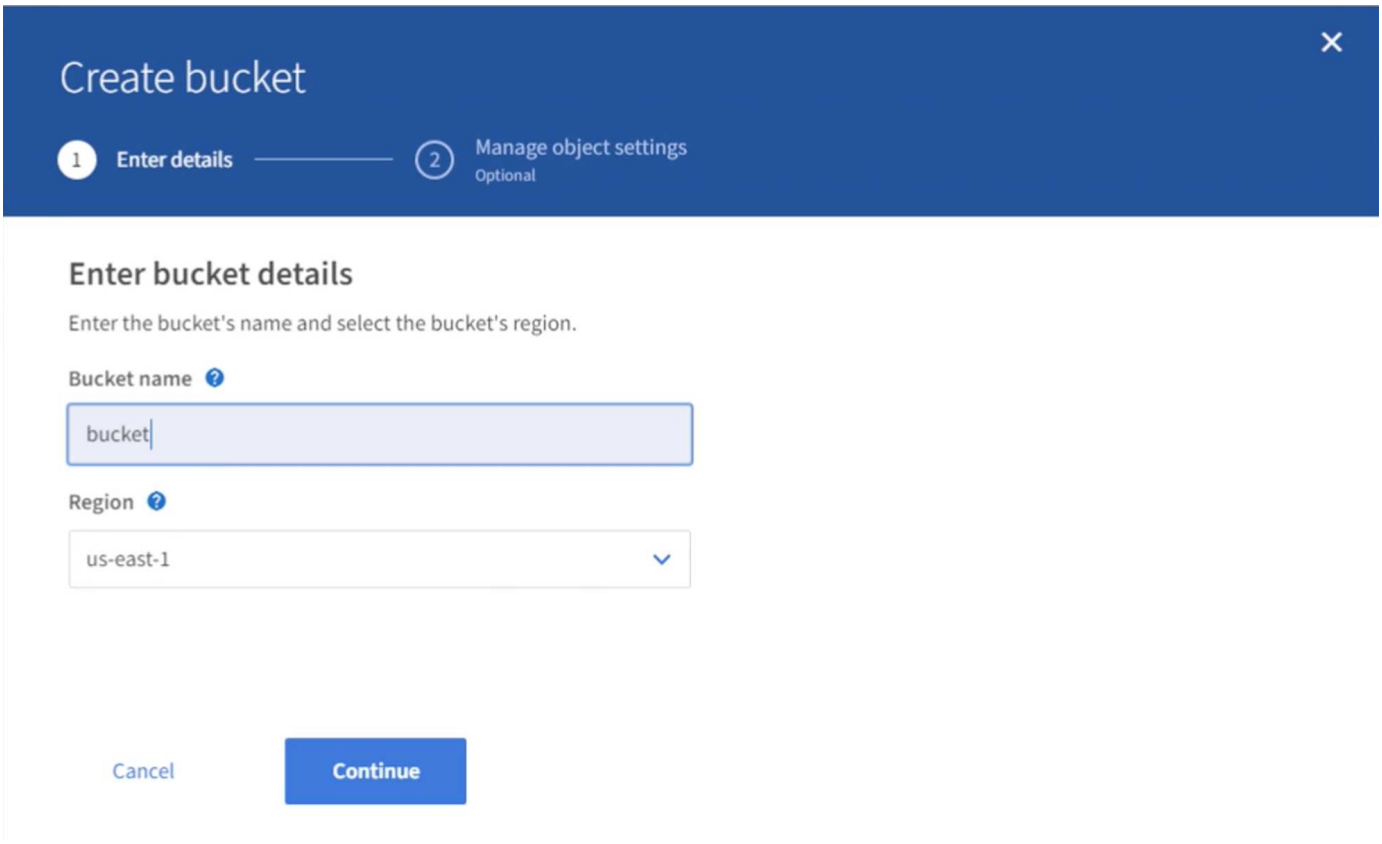


Erstellen Sie zwei Buckets

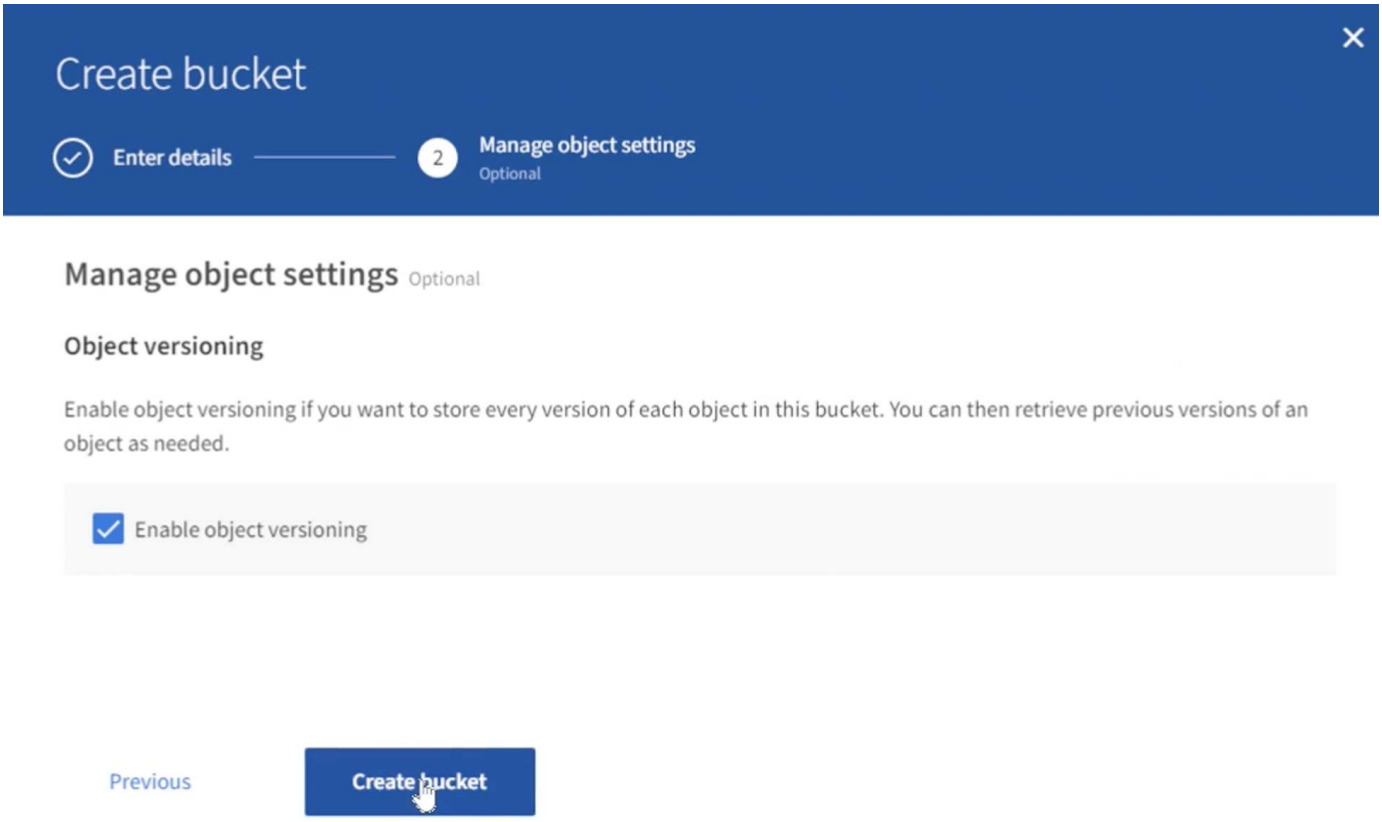
Navigieren Sie zur Registerkarte „Buckets“, und klicken Sie auf die Schaltfläche „Bucket erstellen“.



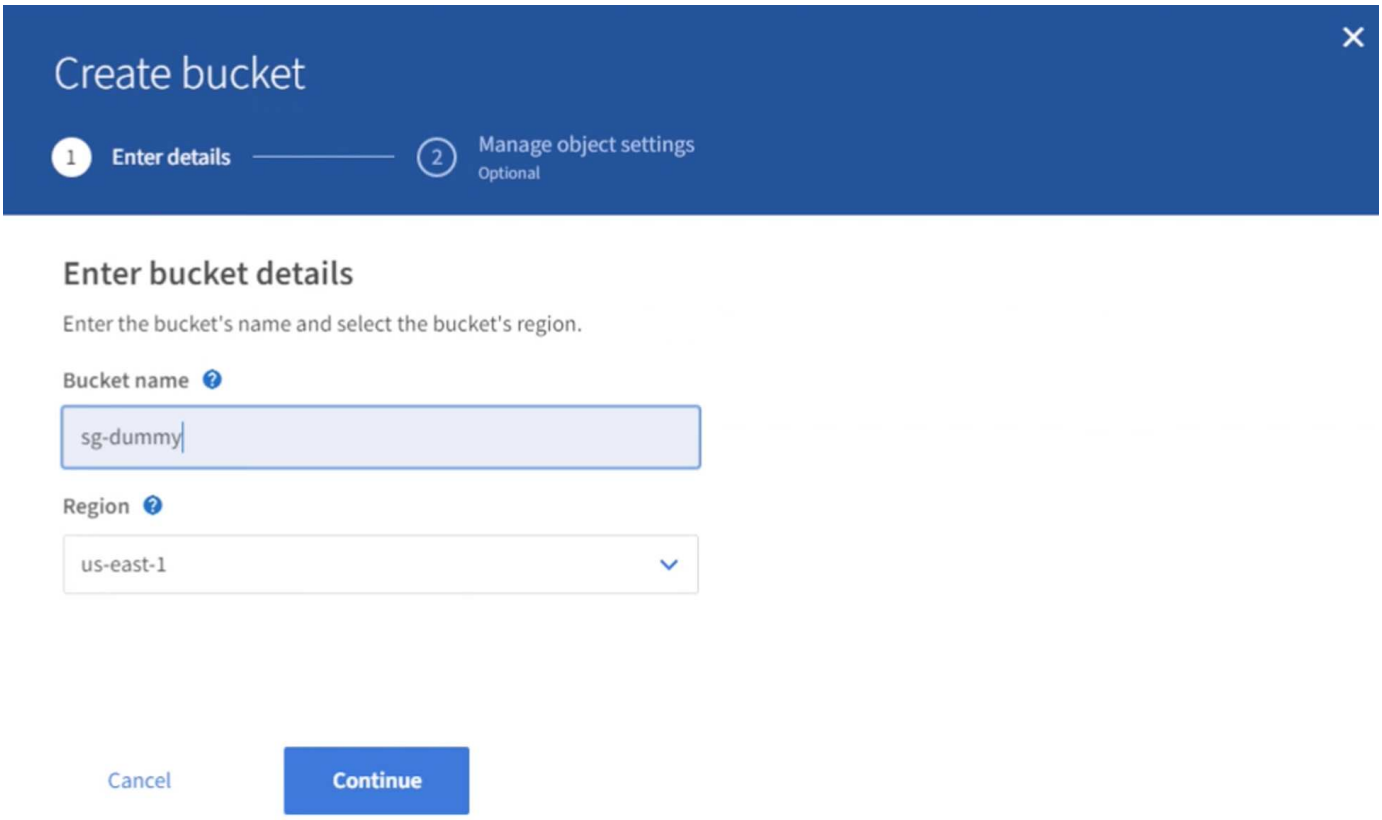
Definieren Sie den Bucket-Namen und die Region.



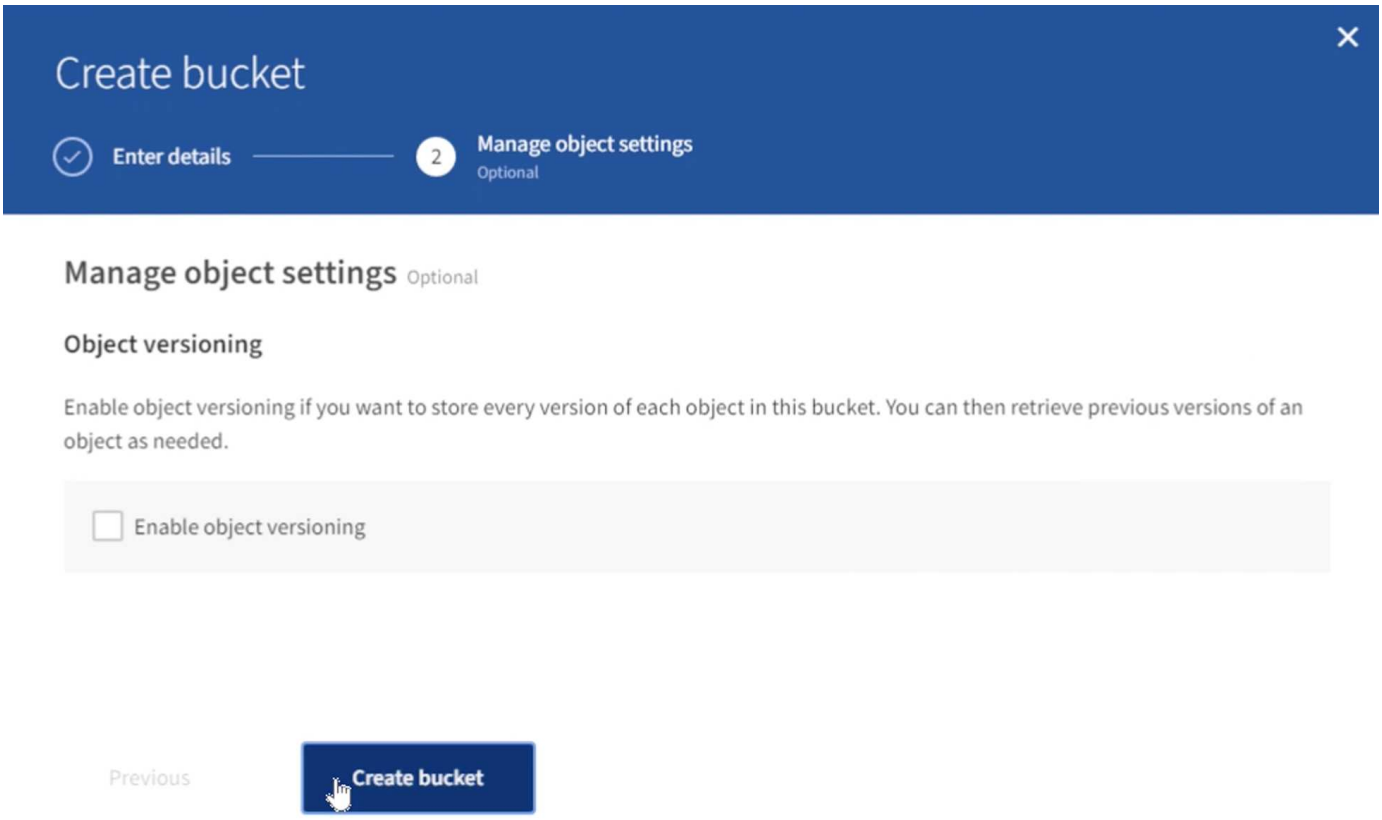
Aktivieren Sie in diesem ersten Bucket die Versionierung.



Erstellen Sie nun einen zweiten Bucket ohne aktivierte Versionierung.



Aktivieren Sie die Versionierung für diesen zweiten Bucket nicht.



Von Rafael Guedes und Aron Klein

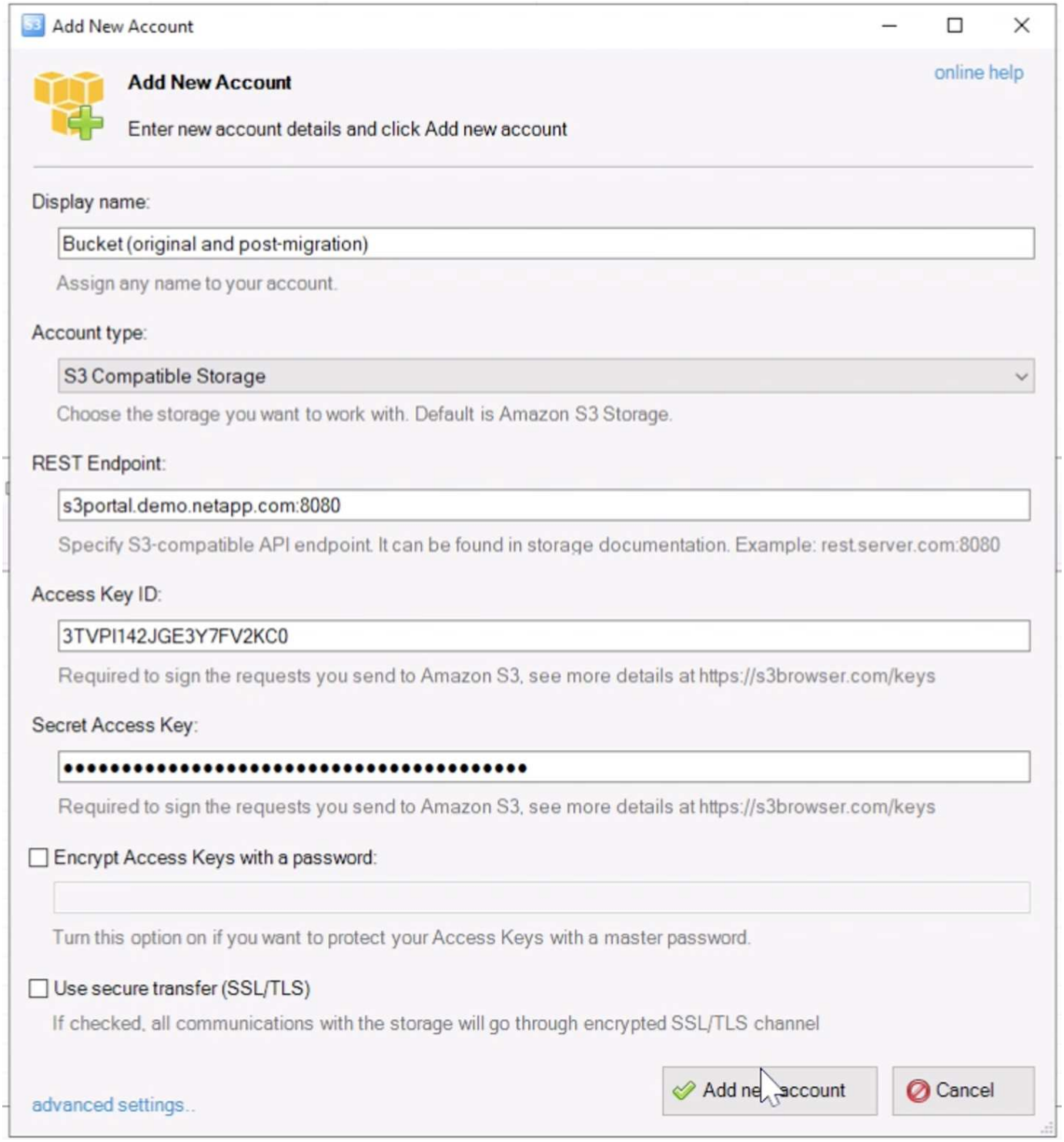
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

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

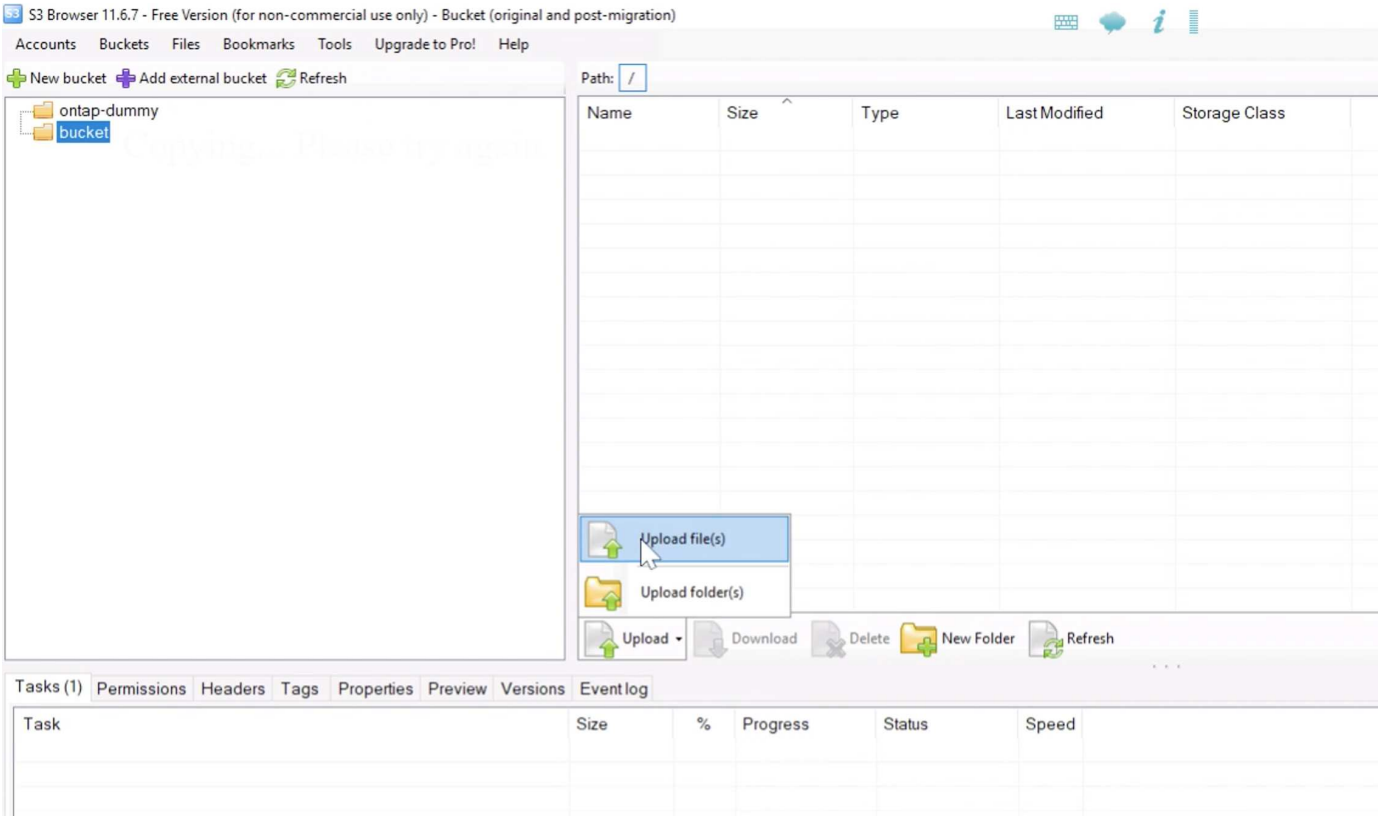
Füllen Sie den Quelleimer aus

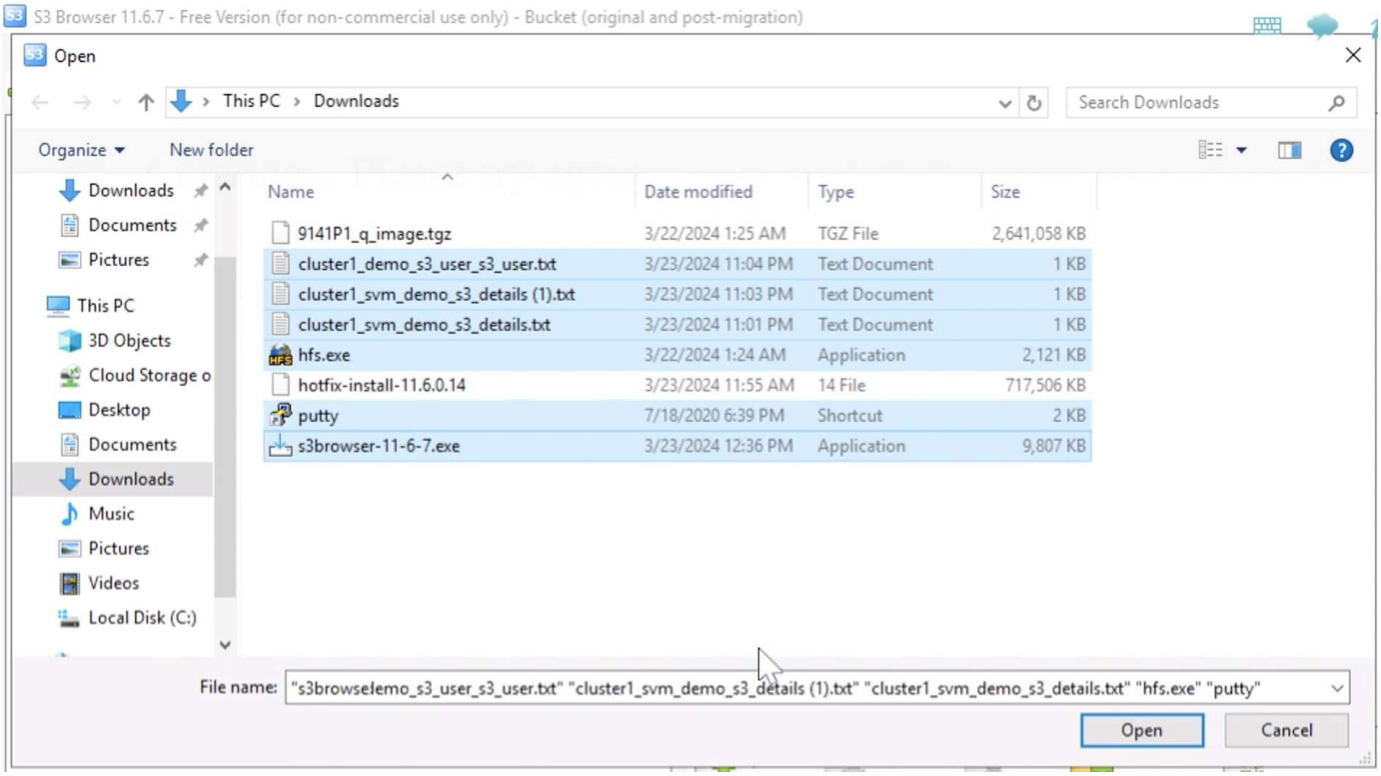
Lassen Sie uns einige Objekte in den Quell-ONTAP-Bucket legen. Wir verwenden S3Browser für diese Demo, aber Sie können jedes Tool verwenden, mit dem Sie vertraut sind.

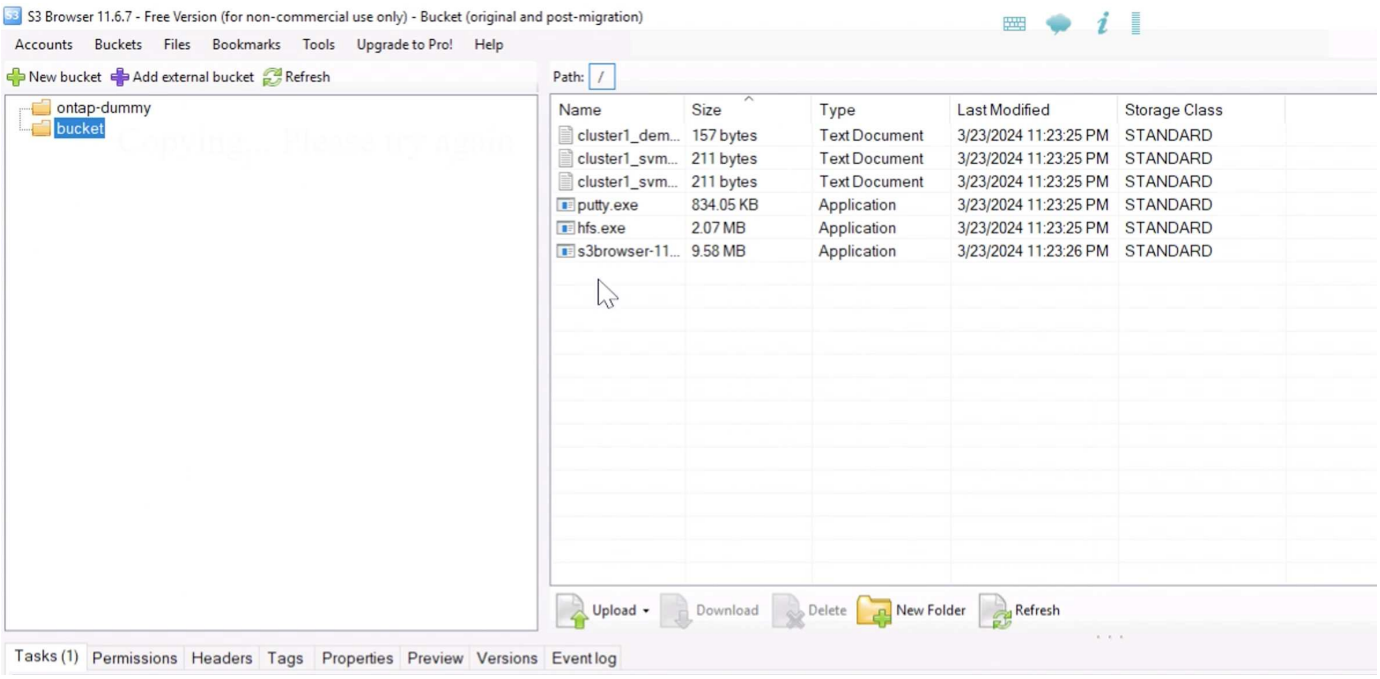
Konfigurieren Sie S3Browser mithilfe der oben erstellten ONTAP-Benutzer-s3-Schlüssel, um eine Verbindung zu Ihrem ONTAP-System herzustellen.



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

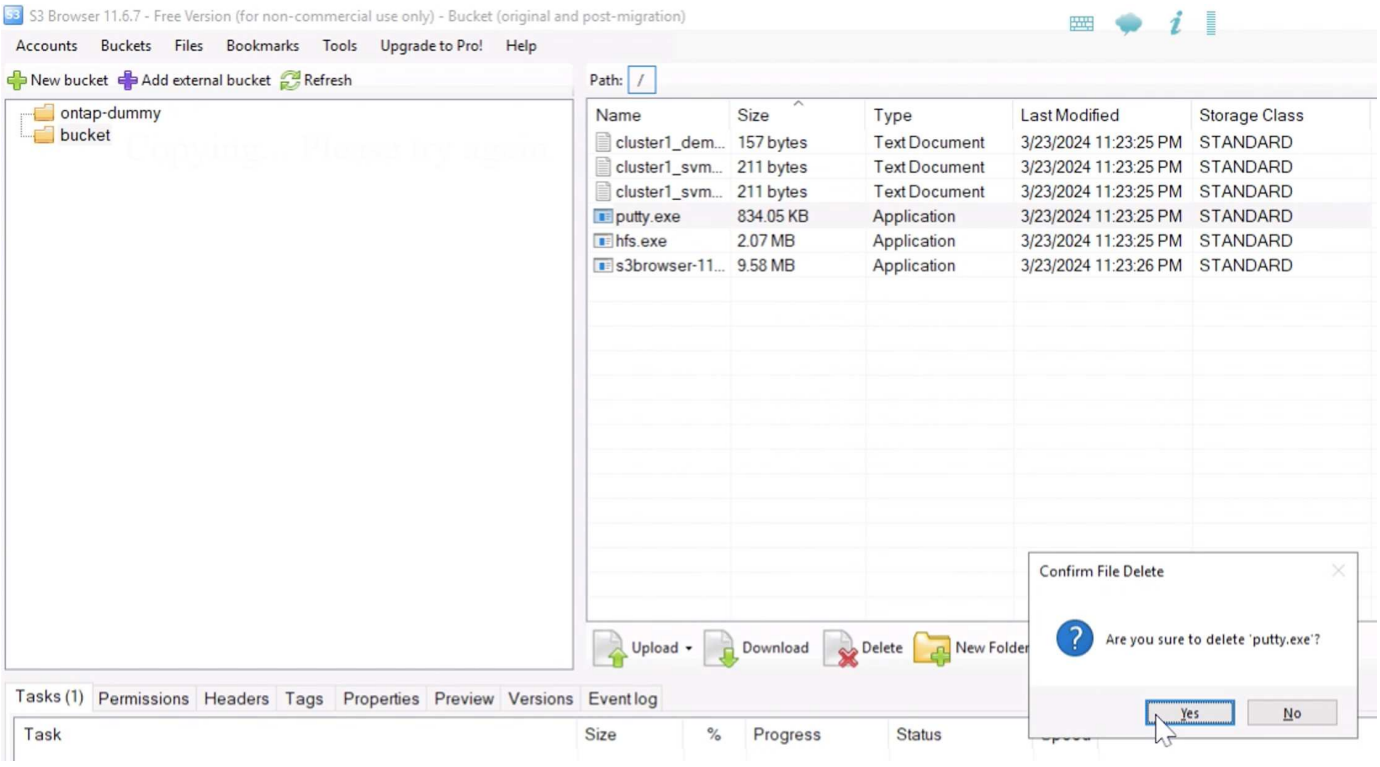

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)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


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

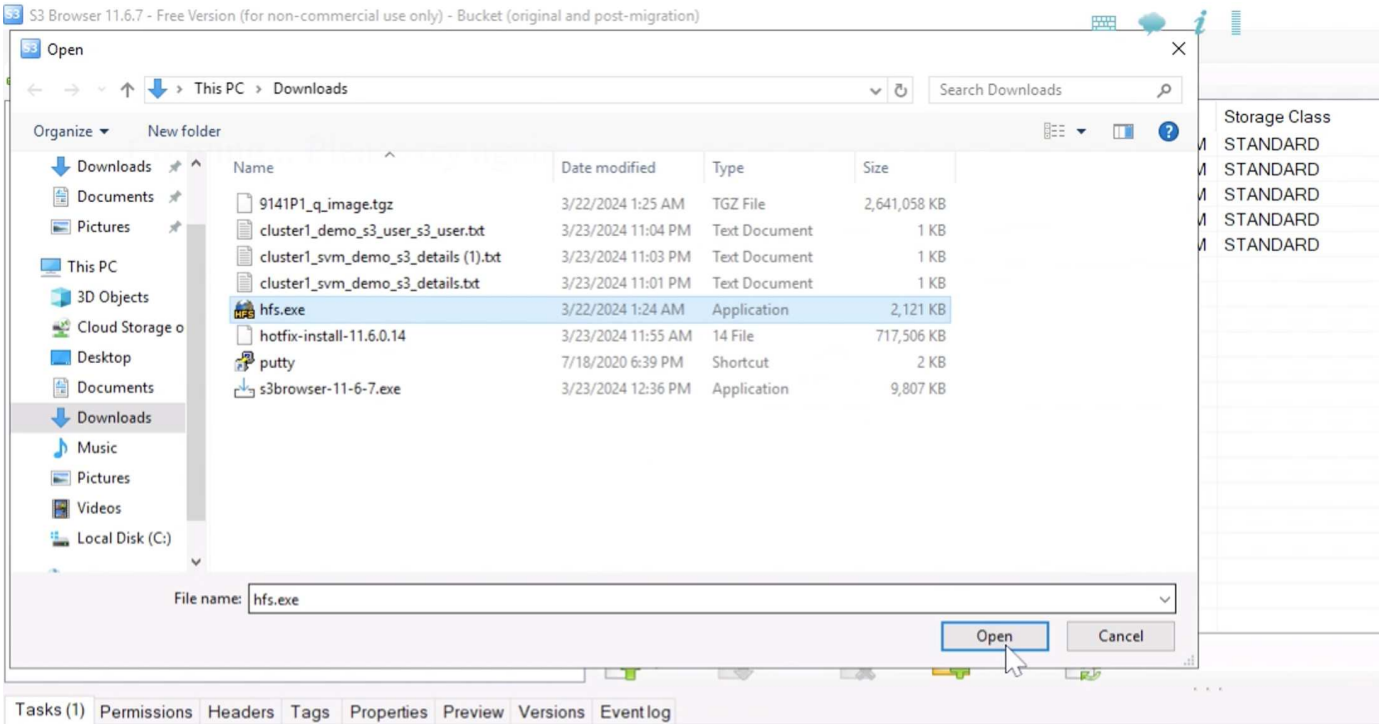


Lassen Sie uns nun einige Objektversionen im Bucket erstellen.

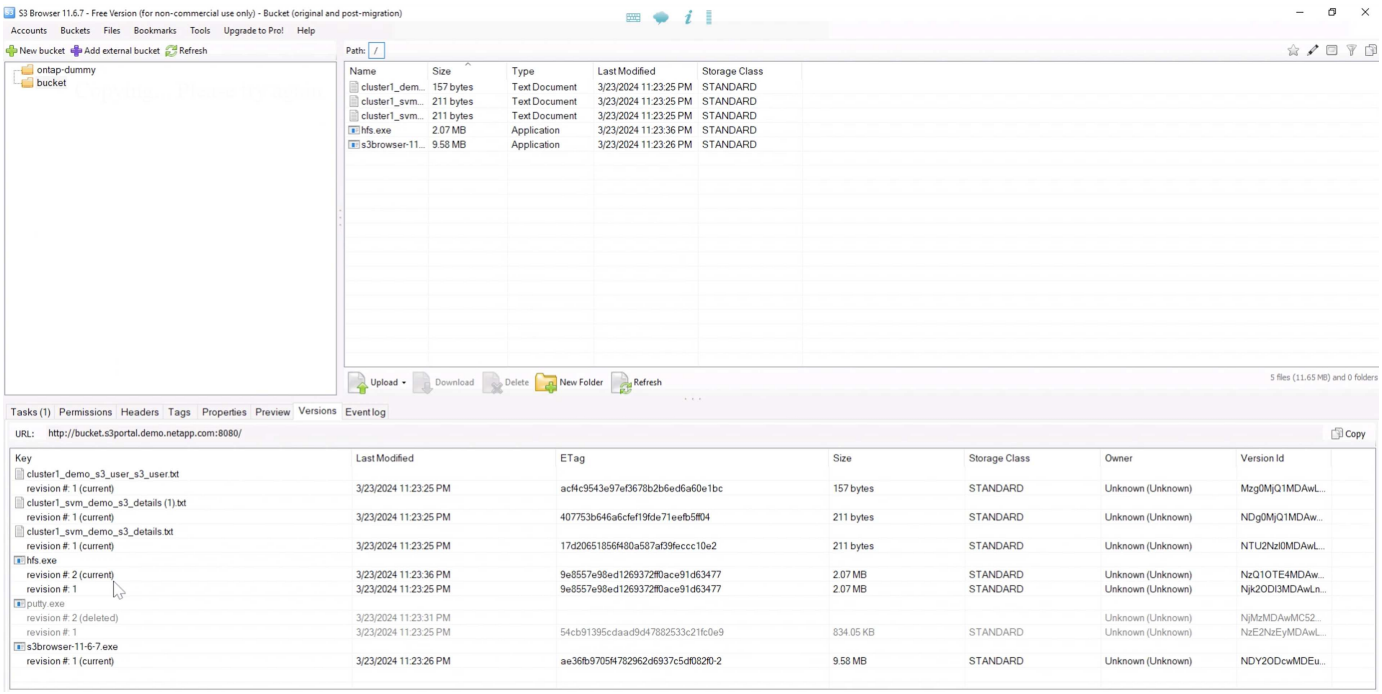
Eine Datei löschen.



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



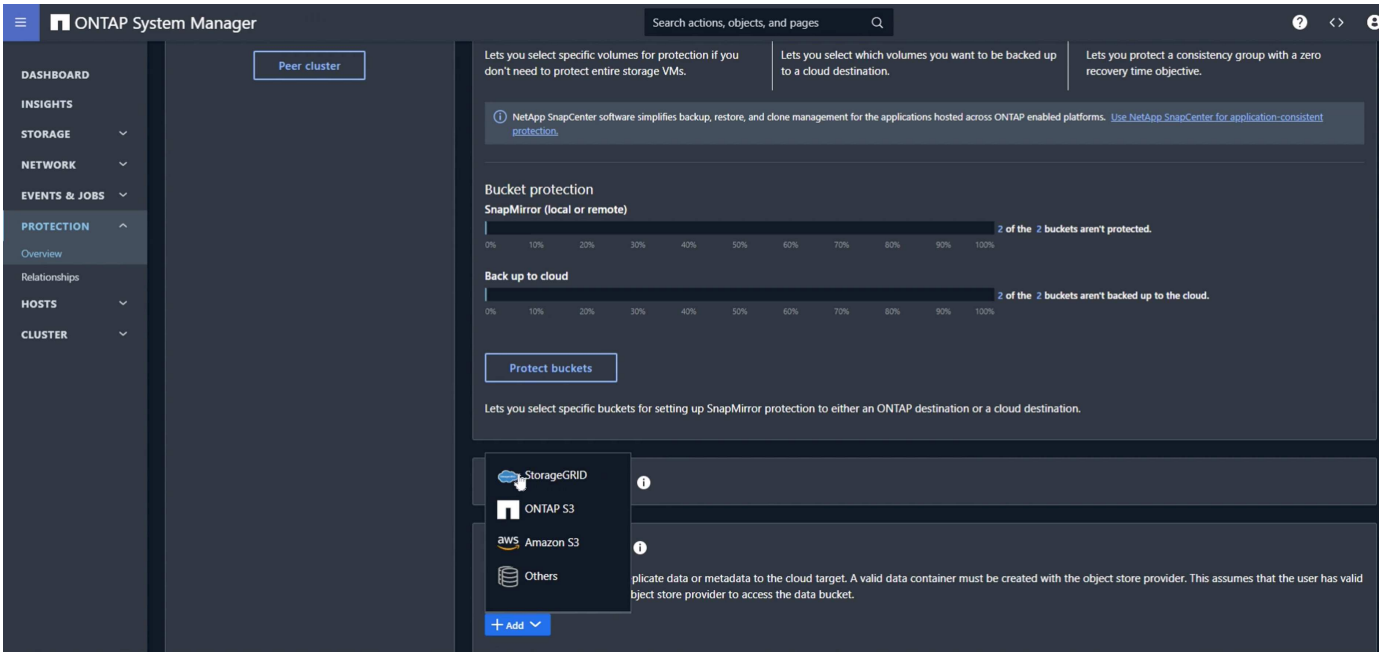
In S3Browser können wir die Versionen der Objekte anzeigen, die wir gerade erstellt haben.



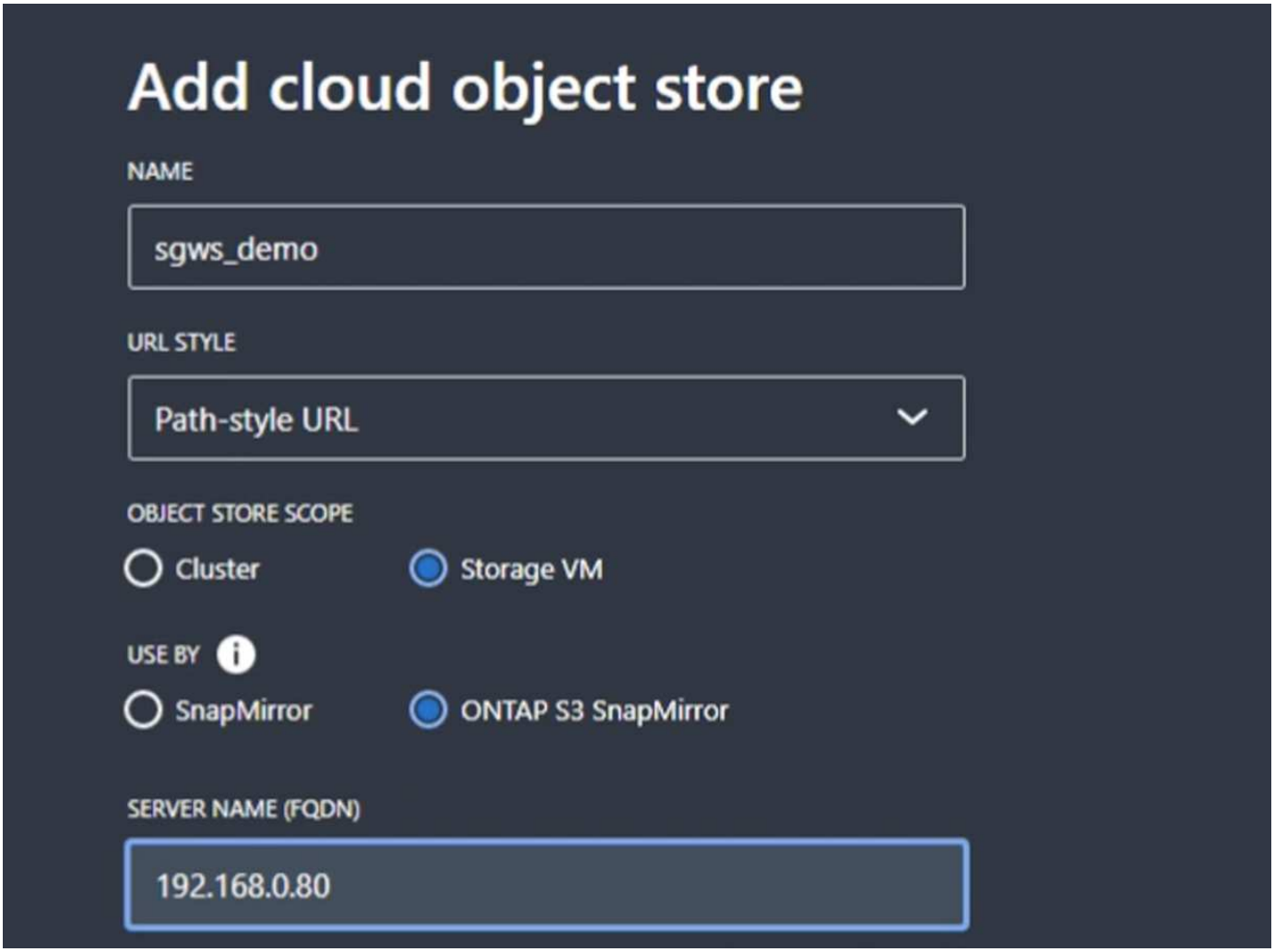
Festlegen der Replikationsbeziehung

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

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



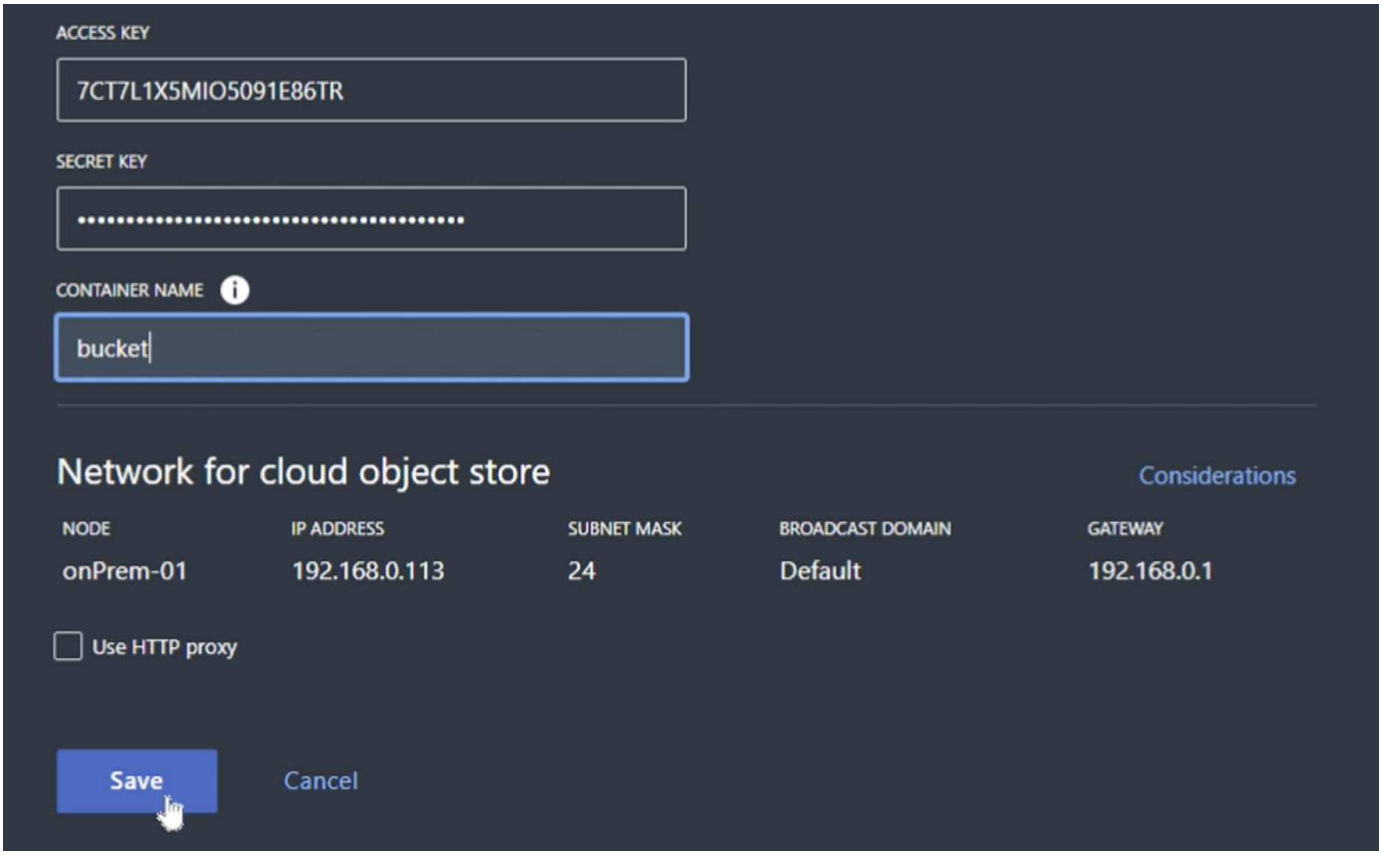
Geben Sie die StorageGRID-Informationen ein, indem Sie einen Namen, URL-Stil (für diese Demo verwenden wir Pfad-styl URLs). Setzen Sie den Umfang des Objektspeichers auf „Storage VM“.



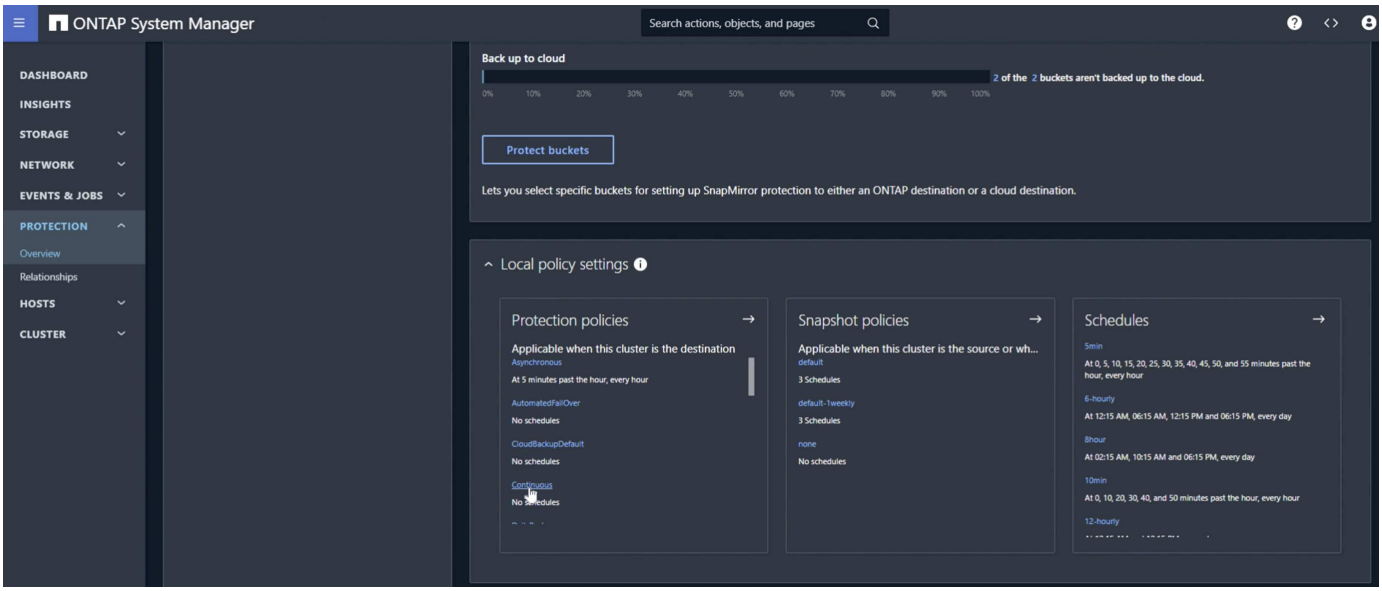
Wenn Sie SSL verwenden, legen Sie hier den Load Balancer-Endpunkt-Port fest und kopieren Sie das

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

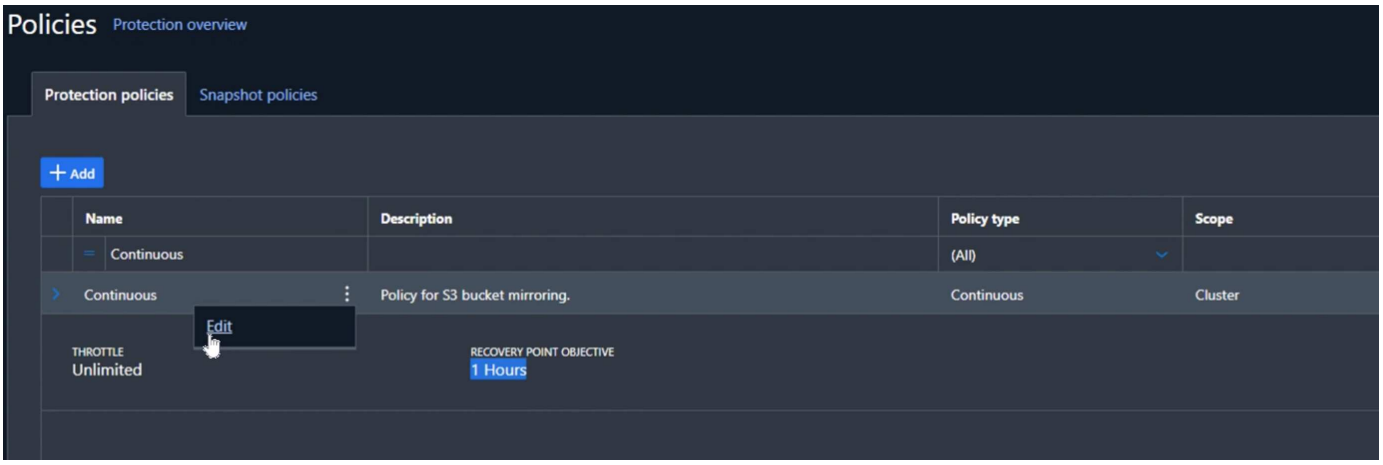
Geben Sie die S3-Benutzerschlüssel und den Bucket-Namen der StorageGRID aus der obigen StorageGRID-Konfiguration für das Ziel ein.



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



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

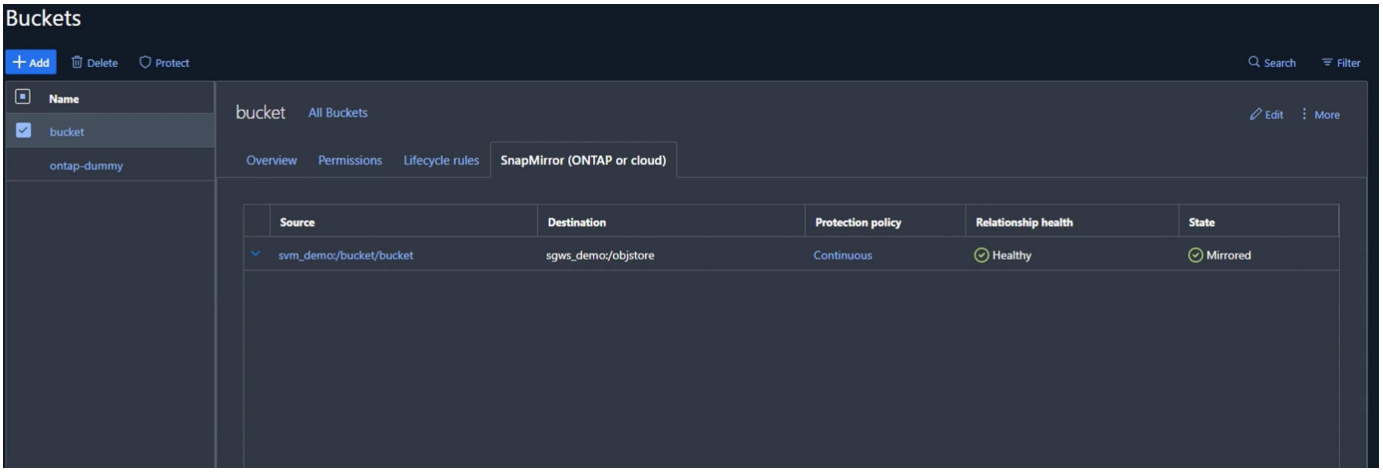


Jetzt können wir SnapMirror konfigurieren, um den Bucket zu replizieren.

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

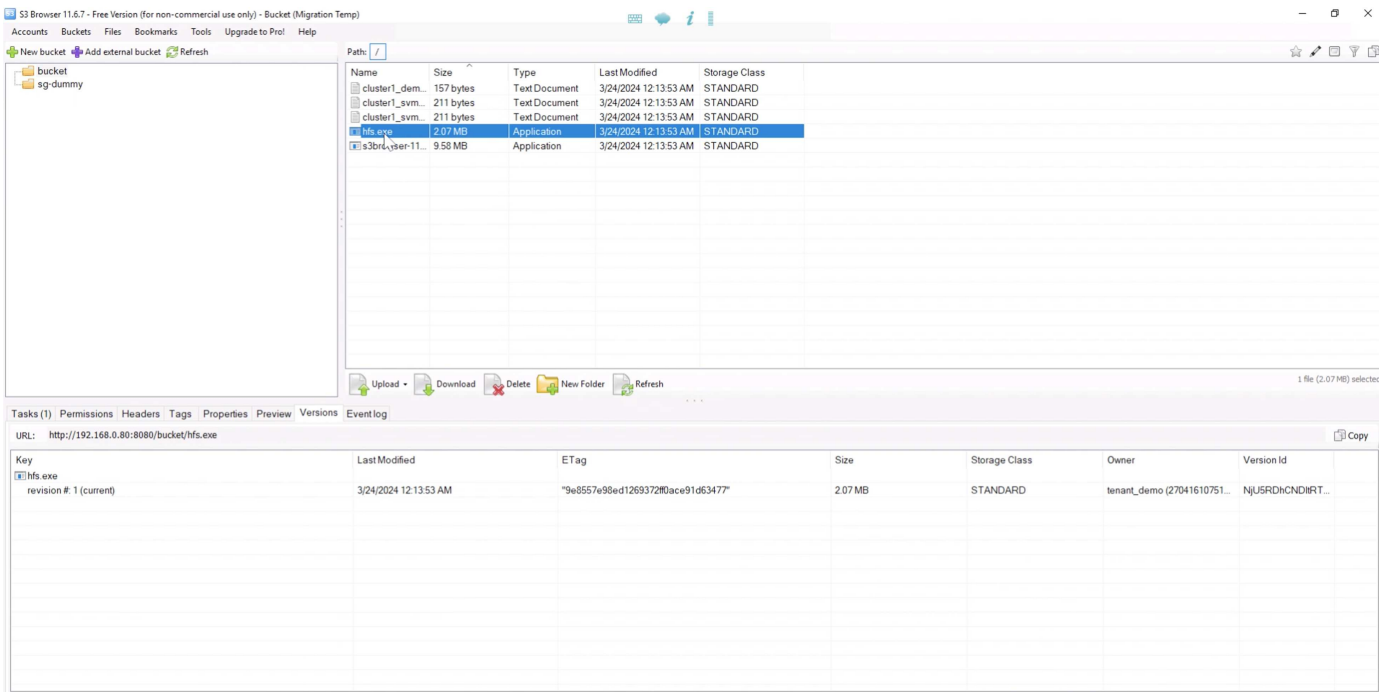
Der Bucket zeigt nun ein Wolkensymbol in der Bucket-Liste unter Schutz an.

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

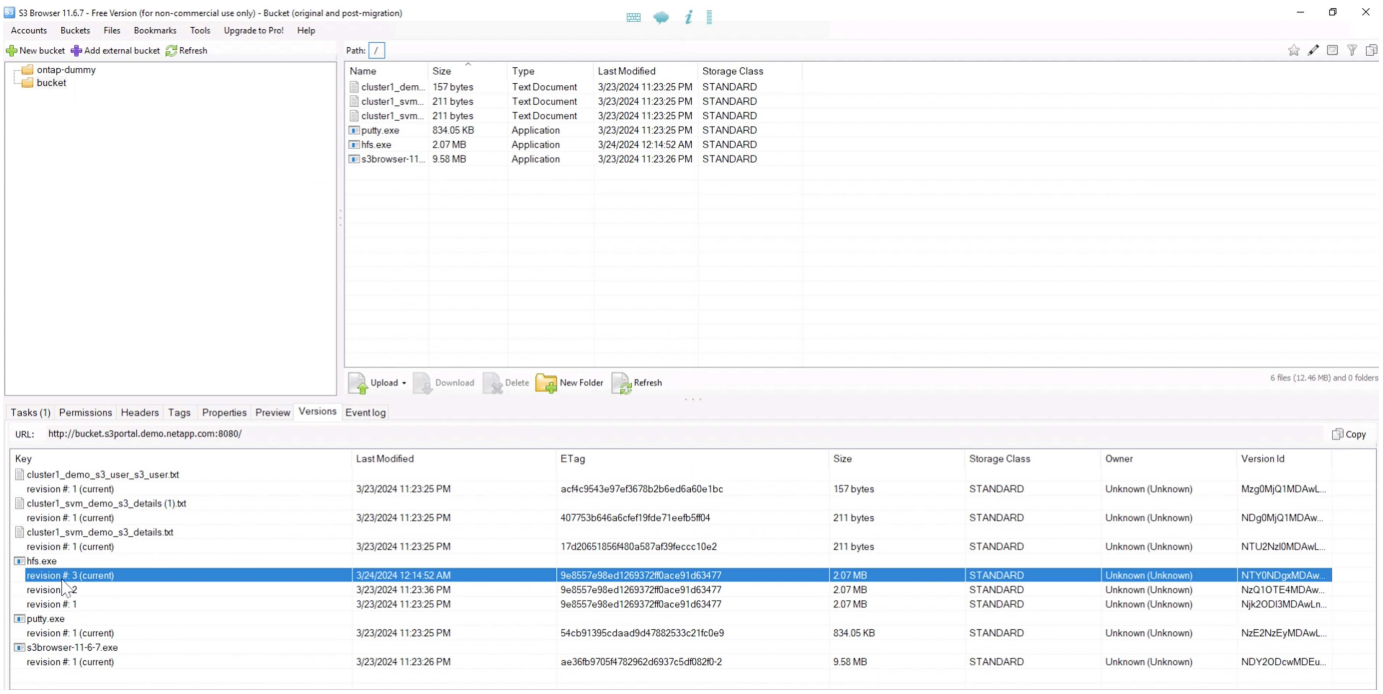


Details zur Replikation

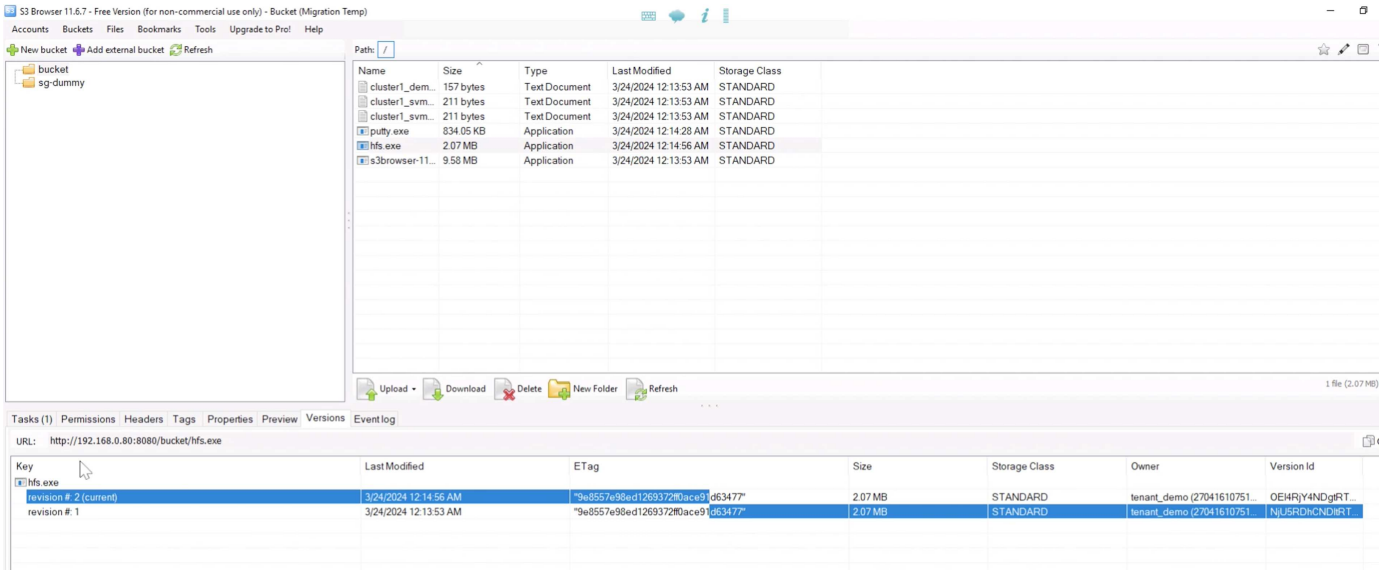
Wir verfügen jetzt über einen erfolgreich replizierenden Bucket von ONTAP zu StorageGRID. Aber was ist eigentlich Replikation? Unsere Quelle und unser Ziel sind beide versionierte Buckets. Replizieren die vorherigen Versionen auch an das Zielsystem? Wenn wir uns unseren StorageGRID-Bucket mit S3Browser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



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



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



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

Von Rafael Guedes und Aron Klein

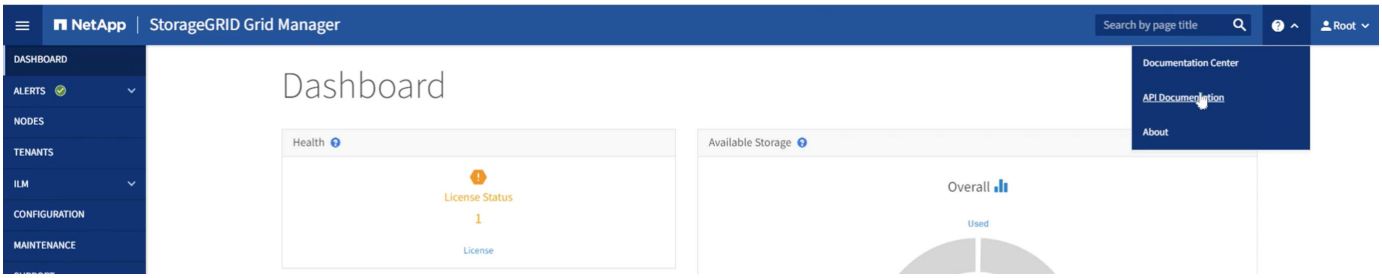
Die Lösung ermöglicht S3 der Enterprise-Klasse durch die nahtlose Migration von objektbasiertem Storage von ONTAP S3 zu StorageGRID

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

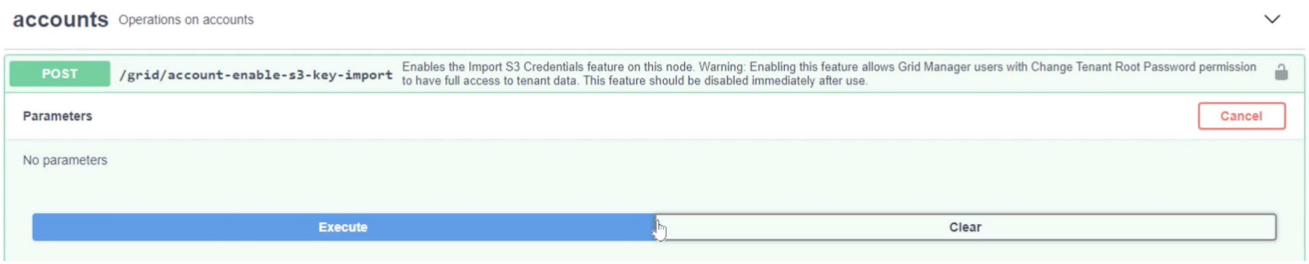
Migrieren Sie S3 Schlüssel

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

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

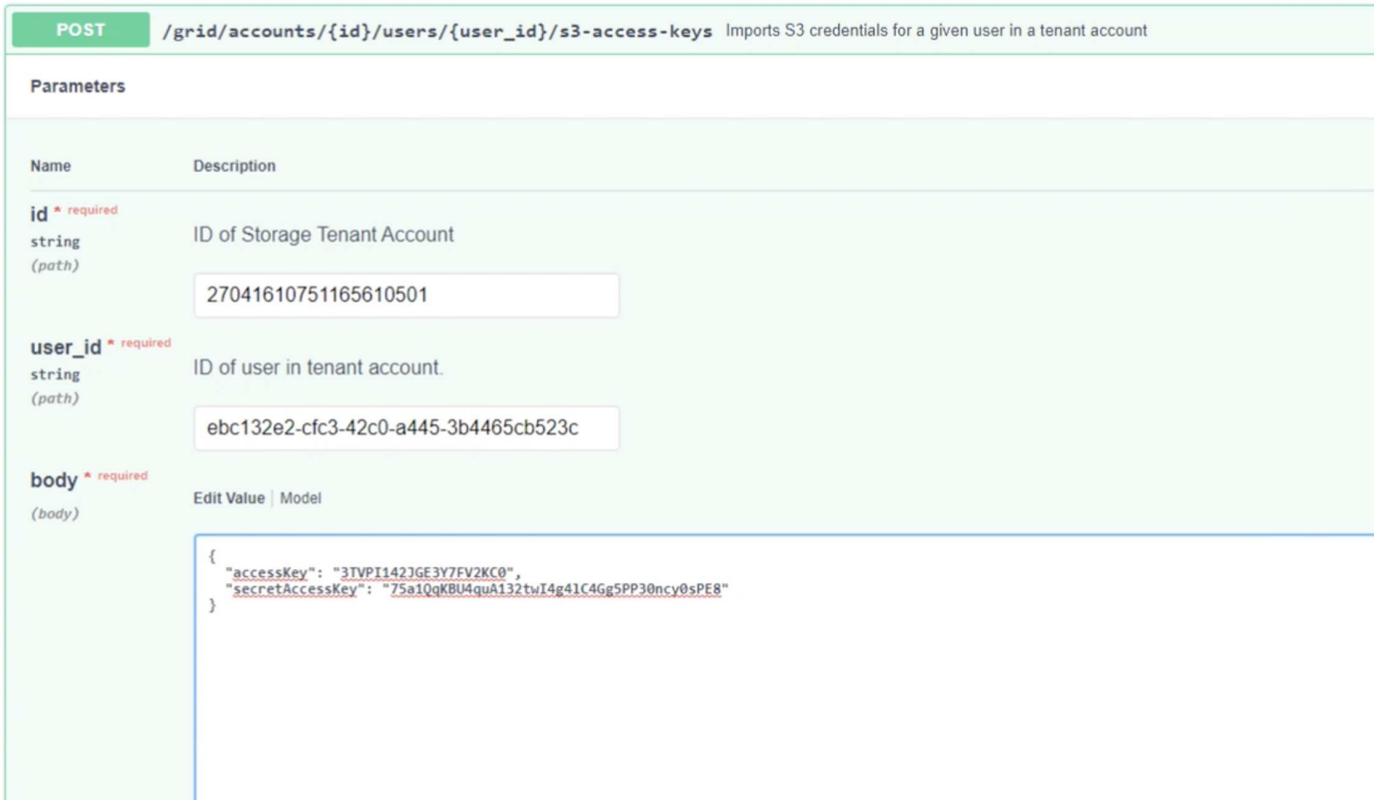


Erweitern Sie den Abschnitt "Accounts", wählen Sie "POST /Grid/Account-enable-s3-key-Import", klicken Sie auf "Try it out" und klicken Sie dann auf die Schaltfläche Ausführen.

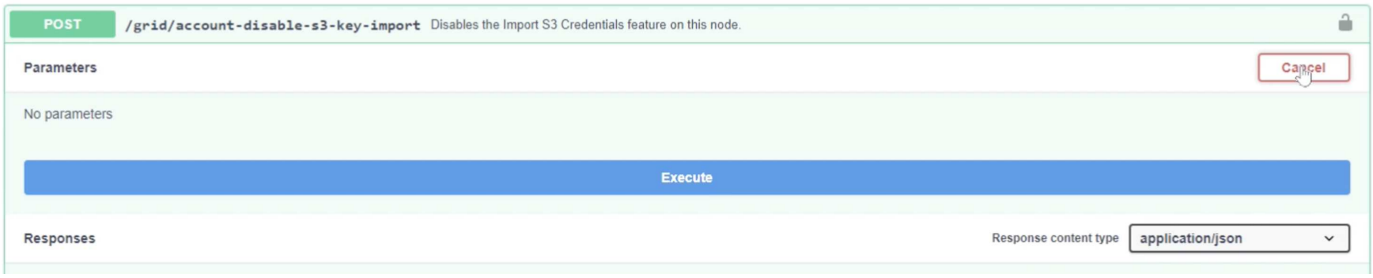


Scrollen Sie jetzt noch unter „Accounts" nach unten zu „POST /Grid/Accounts/{id}/users/{user_id}/s3-Access-keys"

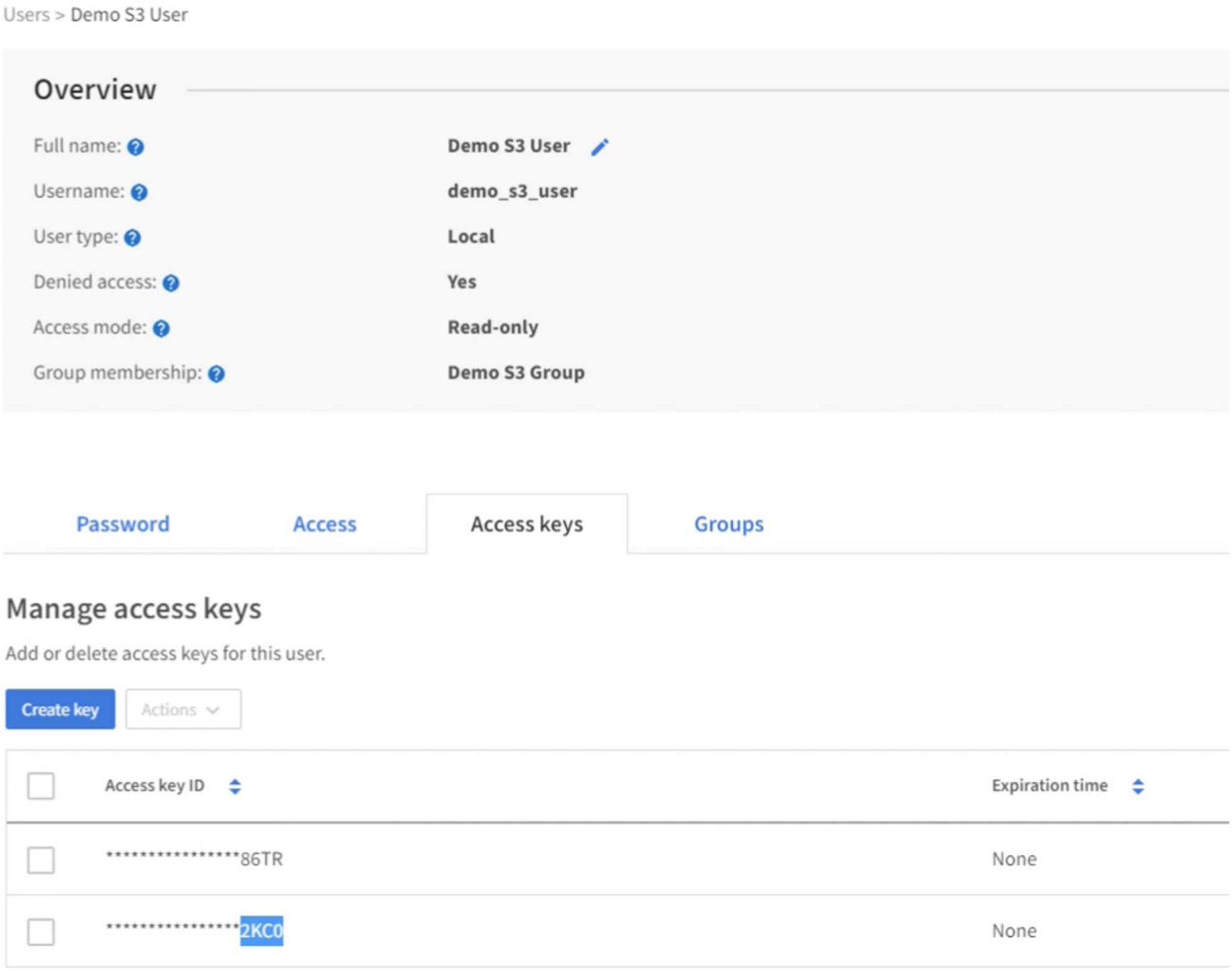
Hier werden wir die Mieter-ID und die Benutzer-Konto-ID eingeben, die wir zuvor gesammelt haben. Füllen Sie die Felder und die Schlüssel von unserem ONTAP-Benutzer in der json-Box. Sie können den Ablauf der Schlüssel einstellen, oder entfernen Sie die " , "läuft ab": 123456789" und klicken Sie auf Ausführen.



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



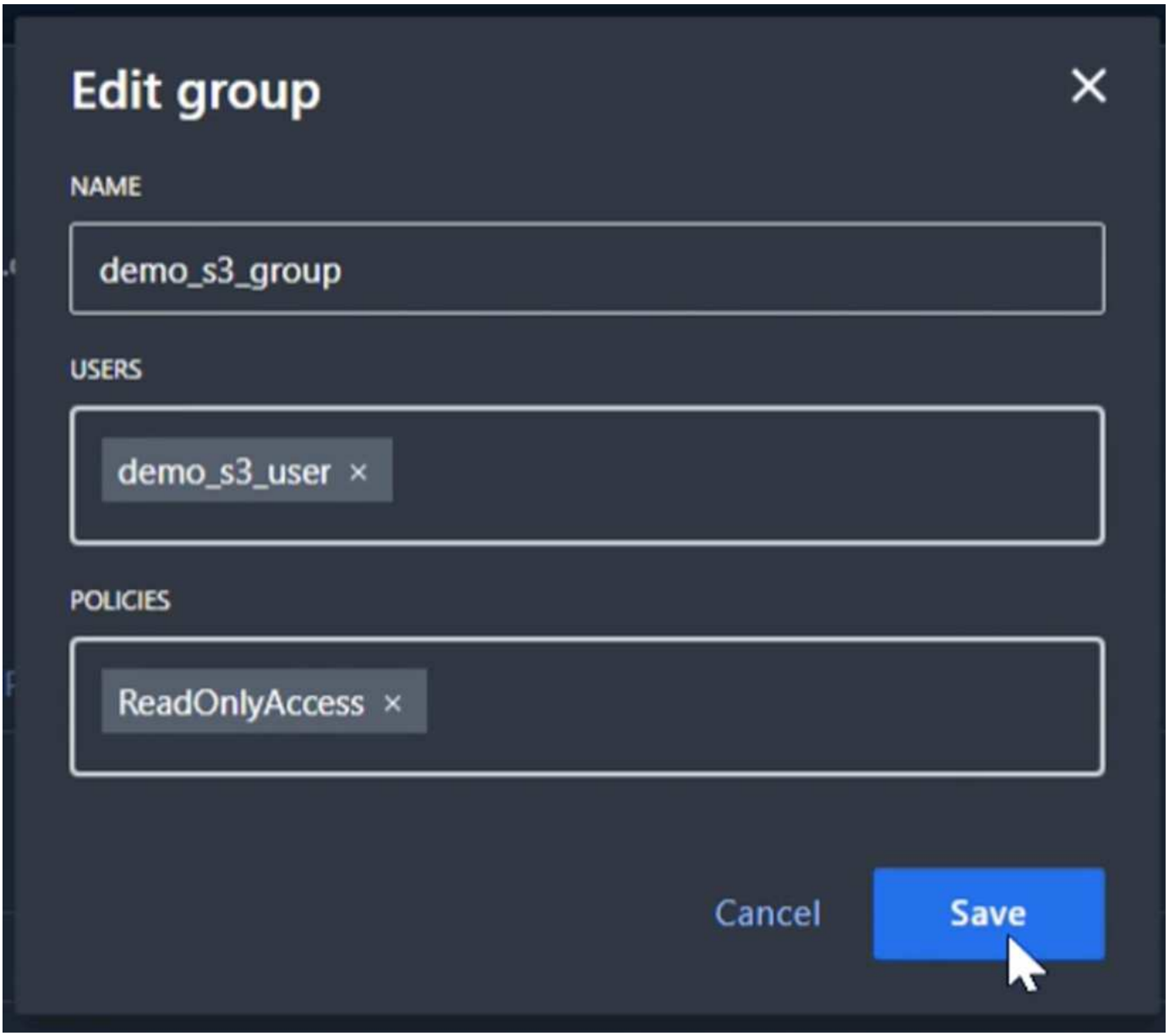
Wenn wir uns das Benutzerkonto in der Mandantenmanager-UI ansehen, sehen wir, dass der neue Schlüssel hinzugefügt wurde.



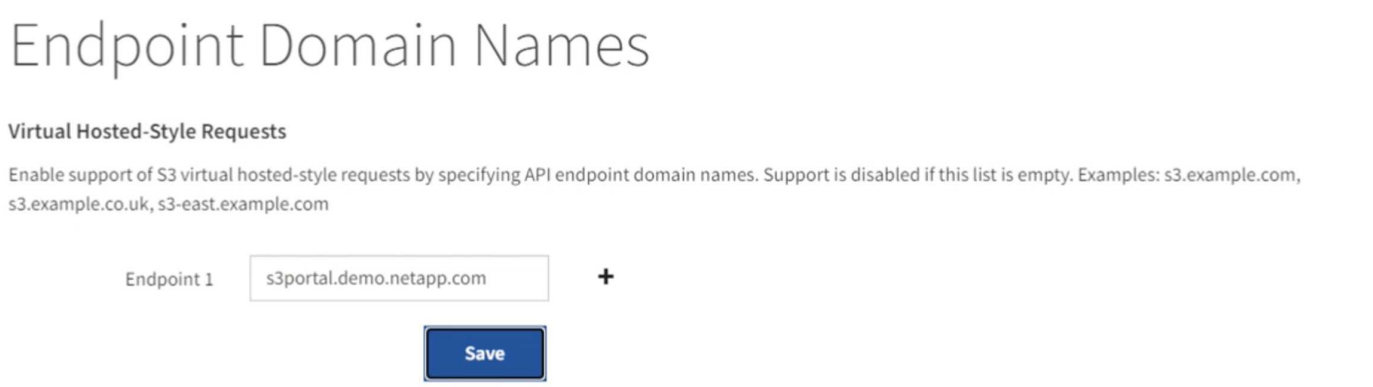
Der letzte Cut-Over

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

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



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



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

Von Rafael Guedes und Aron Klein