



Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier 1
- Best Practices für den Lastausgleich 3
- Best Practices für Hochverfügbarkeitsgruppen 4
- Konfigurieren des DNS-Servers für StorageGRID-IP-Adressen 5
- Erstellen einer HA-Gruppe (High Availability, Hochverfügbarkeit) für FabricPool 5
- Erstellen eines Endpunkts für den Load Balancer für FabricPool 7
- Erstellen eines Mandantenkontos für FabricPool 9
- Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels 10

Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier

Bevor Sie StorageGRID als Cloud Tier für FabricPool hinzufügen können, müssen Sie einige Konfigurationsschritte in StorageGRID ausführen, um bestimmte Werte zu erhalten.

Über diese Aufgabe

In der folgenden Tabelle werden die Informationen aufgeführt, die Sie ONTAP bereitstellen müssen, wenn Sie StorageGRID als Cloud-Tier für FabricPool anhängen. In den Themen in diesem Abschnitt wird erläutert, wie Sie den StorageGRID Grid Manager und den Tenant Manager verwenden, um die Informationen zu erhalten, die Sie benötigen.



Die genauen Feldnamen und der Prozess, den Sie zur Eingabe der erforderlichen Werte in ONTAP verwenden, hängen davon ab, ob Sie die ONTAP CLI (Storage Aggregate Object-Store config create) oder ONTAP System Manager (**Storage > Aggregate & Disks > Cloud Tier**) verwenden.

Weitere Informationen finden Sie im Folgenden:

- ["TR-4598: FabricPool Best Practices für ONTAP 9.8"](#)
- ["ONTAP 9 Dokumentationszentrum"](#)

ONTAP Field	Beschreibung
Objektspeichername	Jeder eindeutige und beschreibende Name. Beispiel: StorageGRID_Cloud_Tier.
Anbietertyp	StorageGRID (System Manager) oder SGWS (CLI).
Port	Der Port, den FabricPool verwenden wird, wenn er eine Verbindung zu StorageGRID herstellt. Sie legen fest, welche Portnummer beim Definieren des StorageGRID Load Balancer-Endpunkts verwendet werden soll. "Erstellen eines Endpunkts für den Load Balancer für FabricPool"

ONTAP Field	Beschreibung
Servername	<p>Der vollständig qualifizierte Domänenname (FQDN) für den StorageGRID Load Balancer-Endpunkt. Beispiel: s3.storagegrid.company.com.</p> <p>Beachten Sie Folgendes:</p> <ul style="list-style-type: none"> • Der hier angegebene Domänenname muss mit dem Domännennamen auf dem CA-Zertifikat übereinstimmen, das Sie für den StorageGRID Load Balancer-Endpunkt hochladen. • Der DNS-Datensatz für diesen Domain-Namen muss jeder IP-Adresse zugeordnet werden, die Sie zum Herstellen einer Verbindung zu StorageGRID verwenden werden. <p>"Konfigurieren des DNS-Servers für StorageGRID-IP-Adressen"</p>
Containername	<p>Der Name des StorageGRID-Buckets, den Sie mit diesem ONTAP-Cluster verwenden werden. Beispiel: fabricpool-bucket. Sie erstellen diesen Bucket im Tenant Manager.</p> <p>Beachten Sie Folgendes:</p> <ul style="list-style-type: none"> • Der Bucket-Name kann nach dem Erstellen der Konfiguration nicht mehr geändert werden. • Für den Bucket ist die Versionierung nicht aktiviert. • Sie müssen einen anderen Bucket für jedes ONTAP Cluster verwenden, für das Daten in StorageGRID verschoben werden sollen. <p>"Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels"</p>
Zugriffsschlüssel und geheimes Passwort	<p>Der Zugriffsschlüssel und der geheime Zugriffsschlüssel für das StorageGRID-Mandantenkonto.</p> <p>Diese Werte generieren Sie im Tenant Manager.</p> <p>"Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels"</p>
SSL	<p>Muss aktiviert sein.</p>
Objektspeicherzertifikat	<p>Das CA-Zertifikat, das Sie beim Erstellen des StorageGRID Load Balancer-Endpunkts hochgeladen haben.</p> <p>Hinweis: Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zwischenzertifikat vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.</p> <p>"Erstellen eines Endpunkts für den Load Balancer für FabricPool"</p>

Nachdem Sie fertig sind

Nachdem Sie die erforderlichen StorageGRID Informationen erhalten haben, können Sie unter ONTAP StorageGRID als Cloud-Tier hinzufügen, die Cloud-Ebene als Aggregat hinzufügen und die Tiering-Richtlinien für Volumes festlegen.

Best Practices für den Lastausgleich

Bevor Sie StorageGRID als FabricPool-Cloud-Tier anhängen, verwenden Sie den StorageGRID Grid-Manager, um mindestens einen Load Balancer-Endpunkt zu konfigurieren.

Was ist die Lastverteilung

Wenn Daten vom FabricPool zu einem StorageGRID System verschoben werden, verwendet StorageGRID einen Load Balancer zum Managen des Aufnahme- und Abrufs-Workloads. Der Lastausgleich maximiert die Geschwindigkeit und die Verbindungskapazität, indem der FabricPool Workload auf mehrere Storage-Nodes verteilt wird.

Der StorageGRID Load Balancer-Service wird auf allen Admin-Nodes und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Sie beendet die TLS-Beendigung von Client-Anforderungen, prüft die Anforderungen und stellt neue sichere Verbindungen zu den Storage-Nodes her.

Der Load Balancer-Service auf jedem Node wird unabhängig ausgeführt, wenn der Client-Datenverkehr an die Storage Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter.

Obwohl der StorageGRID Load Balancer-Service der empfohlene Load-Balancing-Mechanismus ist, können Sie stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie bei Ihrem NetApp Ansprechpartner oder in den folgenden technischen Berichten:

["Optionen zum StorageGRID Load Balancer"](#)



Der separate Connection Load Balancer (CLB)-Service auf Gateway-Nodes ist veraltet und wird nicht mehr für die Verwendung mit FabricPool empfohlen.

Best Practices für den StorageGRID-Lastausgleich

Als allgemeine Best Practice sollte jeder Standort in Ihrem StorageGRID-System zwei oder mehr Nodes mit dem Load Balancer Service umfassen. Ein Standort kann beispielsweise einen Admin-Node und einen Gateway-Node oder sogar zwei Admin-Nodes enthalten. Vergewissern Sie sich, dass für jeden Load-Balancing-Node eine entsprechende Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur vorhanden ist, unabhängig davon, ob Sie SG100- oder SG1000-Servicegeräte, Bare Metal-Nodes oder VM-basierte Nodes verwenden.

Sie müssen einen StorageGRID Load Balancer-Endpunkt konfigurieren, um den Port zu definieren, den Gateway-Knoten und Admin-Knoten für eingehende und ausgehende FabricPool-Anforderungen verwenden werden.

Best Practices für das Endpoint-Zertifikat für Load Balancer

Beim Erstellen eines Endpunkts für den Lastausgleich für die Verwendung mit FabricPool müssen Sie HTTPS als Protokoll verwenden. Sie können dann entweder ein Zertifikat hochladen, das entweder von einer öffentlich

vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert ist, oder Sie können ein selbstsigniertes Zertifikat generieren. Mit dem Zertifikat kann ONTAP sich mit StorageGRID authentifizieren.

Als Best Practice sollten Sie ein CA-Serverzertifikat verwenden, um die Verbindung zu sichern. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden.

Wenn Sie ein CA-Zertifikat zur Verwendung mit dem Endpunkt des Load Balancer anfordern, stellen Sie sicher, dass der Domänenname auf dem Zertifikat mit dem in ONTAP eingegebenen Servernamen für diesen Load Balancer-Endpoint übereinstimmt. Wenn möglich, verwenden Sie einen Platzhalter (*), um virtuelle URLs im Hoststil zu ermöglichen. Beispiel:

```
*.s3.storagegrid.company.com
```

Wenn Sie StorageGRID als FabricPool Cloud Tier hinzufügen, müssen Sie beim ONTAP Cluster dasselbe Zertifikat sowie die Zertifikate „Root“ und „untergeordnete Certificate Authority“ (CA) installieren.



StorageGRID verwendet Serverzertifikate aus verschiedenen Gründen. Wenn Sie eine Verbindung zum Load Balancer-Dienst herstellen, müssen Sie das Object Storage API Service Endpoints Server Certificate nicht hochladen.

Weitere Informationen zum Serverzertifikat für einen Lastausgleichsendpunkt:

- ["Managen des Lastausgleichs"](#)
- ["Härtungsrichtlinien für Serverzertifikate"](#)

Best Practices für Hochverfügbarkeitsgruppen

Bevor Sie StorageGRID als FabricPool Cloud-Tier anhängen, können Sie mithilfe von StorageGRID Grid Manager eine HA-Gruppe (High Availability, Hochverfügbarkeit) konfigurieren.

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist das

Um sicherzustellen, dass der Load Balancer-Service zum Verwalten von FabricPool-Daten immer verfügbar ist, können Sie die Netzwerkschnittstellen mehrerer Admin- und Gateway-Nodes zu einer einzigen Einheit gruppieren, die als HA-Gruppe (High Availability, Hochverfügbarkeit) bezeichnet wird. Wenn der aktive Node in der HA-Gruppe ausfällt, kann der Workload weiterhin von einem anderen Node in der Gruppe gemanagt werden.

Jede HA-Gruppe ermöglicht einen hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes. Beispielsweise bietet eine HA-Gruppe, die aus allen Admin-Nodes besteht, hochverfügbaren Zugriff auf einige Management-Services für Admin-Nodes und den Load-Balancer-Service. Eine HA-Gruppe, die aus nur Gateway-Nodes oder Admin-Nodes und Gateway-Nodes besteht, bietet hochverfügbaren Zugriff auf den Shared Load Balancer Service.

Beim Erstellen einer HA-Gruppe wählen Sie Netzwerkschnittstellen aus, die zum Grid Network (eth0) oder dem Client-Netzwerk (eth2) gehören. Alle Schnittstellen in einer HA-Gruppe müssen sich im selben Netzwerk-Subnetz befinden.

Eine HA-Gruppe behält eine oder mehrere virtuelle IP-Adressen bei, die der aktiven Schnittstelle in der Gruppe hinzugefügt werden. Wenn die aktive Schnittstelle nicht mehr verfügbar ist, werden die virtuellen IP-Adressen

in eine andere Schnittstelle verschoben. Dieser Failover-Prozess dauert in der Regel nur wenige Sekunden und ist schnell genug, dass Client-Applikationen nur geringe Auswirkungen haben und sich auf normale Wiederholungsmuster verlassen können, um den Betrieb fortzusetzen.

Wenn Sie eine HA-Gruppe mit Nodes für den Lastausgleich konfigurieren, stellt FabricPool eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.

Best Practices für Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen)

Die Best Practices zum Erstellen einer StorageGRID HA-Gruppe für FabricPool hängen vom Workload ab:

- Wenn Sie FabricPool für Daten mit primären Workloads verwenden möchten, müssen Sie eine HA-Gruppe erstellen, die mindestens zwei Load-Balancing-Nodes umfasst, um eine Unterbrechung beim Datenabruf zu vermeiden.
- Wenn Sie eine FabricPool Richtlinie für das reine Volume-Tiering nur für Snapshots oder nicht für lokale Performance-Tiers (z. B. Disaster Recovery-Standorte oder NetApp SnapMirror Ziele) verwenden möchten, können Sie eine HA-Gruppe mit nur einem Node konfigurieren.

Diese Anweisungen beschreiben die Einrichtung einer HA-Gruppe für Active-Backup HA (ein Node ist aktiv und ein Node ist ein Backup). Möglicherweise verwenden Sie jedoch lieber DNS Round Robin oder Active-Active HA. Informationen zu den Vorteilen dieser anderen HA-Konfigurationen finden Sie unter ["Konfigurationsoptionen für HA-Gruppen"](#).

Konfigurieren des DNS-Servers für StorageGRID-IP-Adressen

Nach der Konfiguration von Hochverfügbarkeitsgruppen und Endpunkten des Load Balancer müssen Sie sicherstellen, dass das DNS (Domain Name System) für das ONTAP-System einen Datensatz enthält, um den StorageGRID-Servernamen (vollständig qualifizierter Domänenname) der IP-Adresse zuzuordnen, die FabricPool zum Herstellen von Verbindungen verwendet.

Die IP-Adresse, die Sie im DNS-Datensatz eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Load-Balancing-Nodes verwenden:

- Wenn Sie eine HA-Gruppe konfiguriert haben, stellt FabricPool eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, kann FabricPool eine Verbindung zum StorageGRID Load Balancer Service herstellen. Dabei wird die IP-Adresse eines Gateway Node oder eines Admin-Nodes verwendet.

Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

Erstellen einer HA-Gruppe (High Availability, Hochverfügbarkeit) für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, können Sie optional eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) erstellen.

Eine HA-Gruppe besteht aus mindestens einer Netzwerkschnittstellen auf Admin-Nodes, Gateway-Nodes oder beiden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Jede HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes zu ermöglichen.

Weitere Informationen zu dieser Aufgabe. Siehe "[Verwalten von Hochverfügbarkeitsgruppen](#)".

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Hochverfügbarkeitsgruppen**.
2. Wählen Sie eine oder mehrere der Netzwerkschnittstellen aus. Die Netzwerkschnittstellen müssen entweder im Grid Network (eth0) oder im Client Network (eth2) zum selben Subnetz gehören.
3. Weisen Sie einen Knoten als bevorzugter Master zu.

Der bevorzugte Master ist die aktive Schnittstelle, wenn kein Fehler auftritt, der dazu führt, dass die VIP-Adressen einer Backup-Schnittstelle neu zugewiesen werden.

4. Geben Sie bis zu zehn IPv4-Adressen für die HA-Gruppe ein.

Die Adressen müssen sich im IPv4-Subnetz befinden, das von allen Mitgliedschnittstellen gemeinsam genutzt wird.

Create High Availability Group

High Availability Group

Name

Description

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.98.0/23	<input checked="" type="radio"/>
DC1-G1	eth0	10.96.98.0/23	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.98.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1

+

Cancel

Save

Erstellen eines Endpunkts für den Load Balancer für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, konfigurieren Sie einen Endpunkt für den Load Balancer und laden das Endpoint-Zertifikat für den Load Balancer hoch, mit dem die Verbindung zwischen ONTAP und StorageGRID gesichert werden kann.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie haben die folgenden Dateien:

- Serverzertifikat: Die benutzerdefinierte Serverzertifikatdatei.
- Server Certificate Private Key: Die private Schlüsseldatei des benutzerdefinierten Serverzertifikats.
- CA-Paket: Eine einzelne Datei, die die Zertifikate jeder Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

Über diese Aufgabe

Weitere Informationen zu dieser Aufgabe finden Sie unter ["Konfigurieren von Load Balancer-Endpunkten"](#).

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Balancer-Endpunkte Laden**.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Cancel
Save

2. Wählen Sie **Endpunkt hinzufügen**.
3. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Anzeigename	Einen beschreibenden Namen für den Endpunkt
Port	<p>Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist standardmäßig auf 10433 eingestellt, Sie können jedoch alle nicht verwendeten externen Ports eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind.</p> <p>Hinweis: Ports, die von anderen Netzdiensten verwendet werden, sind nicht zulässig. Siehe Liste der Anschlüsse, die für interne und externe Kommunikation verwendet werden:</p> <p>"Referenz für Netzwerk-Ports"</p> <p>Sie müssen diese Portnummer an ONTAP angeben, wenn Sie StorageGRID als FabricPool Cloud Tier anhängen.</p>
Protokoll	Muss HTTPS sein.

Feld	Beschreibung
Endpunktbindungsmodus	<p>Verwenden Sie die Global-Einstellung (empfohlen) oder beschränken Sie die Zugänglichkeit dieses Endpunkts auf einen der folgenden Elemente:</p> <ul style="list-style-type: none"> • Spezifische virtuelle Hochverfügbarkeits-IP-Adressen (VIPs). Verwenden Sie diese Auswahl nur, wenn ein deutlich höheres Maß an Isolierung von Workloads erforderlich ist. • Spezielle Netzwerkschnittstellen bestimmter Nodes.

4. Wählen Sie **Speichern**.

Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

5. Wählen Sie für * Endpoint Service Type* **S3** aus.

6. Wählen Sie **Zertifikat hochladen** (empfohlen) und navigieren Sie anschließend zu Ihrem Serverzertifikat, Ihrem privaten Zertifikatschlüssel und dem CA-Paket.

Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate

Certificate Private Key

CA Bundle

7. Wählen Sie **Speichern**.

Erstellen eines Mandantenkontos für FabricPool

Sie müssen ein Mandantenkonto im Grid Manager for FabricPool Use erstellen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Mandantenkonten ermöglichen Client-Applikationen, Objekte auf StorageGRID zu speichern und abzurufen. Jedes Mandantenkonto verfügt über eine eigene Account-ID, autorisierte Gruppen und Benutzer, Buckets und Objekte.

Sie können dasselbe Mandantenkonto für mehrere ONTAP Cluster verwenden. Oder Sie können bei Bedarf ein dediziertes Mandantenkonto für jedes ONTAP Cluster erstellen.



Bei diesen Anweisungen wird davon ausgegangen, dass Sie Single Sign-On (SSO) für den Grid Manager konfiguriert haben. Wenn Sie kein SSO verwenden, befolgen Sie die Anweisungen für ["Erstellen eines Mandantenkontos, wenn StorageGRID kein SSO verwendet"](#).

Schritte

1. Wählen Sie **Mieter**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Anzeigenamen für das FabricPool-Mandantenkonto ein.
4. Wählen Sie **S3**.
5. Lassen Sie das Kontrollkästchen **Plattformdienste zulassen** aktiviert, um die Nutzung von Plattformdiensten zu aktivieren.

Wenn Plattformservices aktiviert sind, kann ein Mandant Funktionen wie CloudMirror Replizierung verwenden, die auf externe Services zugreifen.

6. Lassen Sie das Feld **Storage Quota** leer.
7. Wählen Sie im Feld **Root Access Group** eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root Access-Berechtigung für den Mandanten zu erhalten.
8. Wählen Sie **Speichern**.

Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels

Bevor Sie StorageGRID mit einem FabricPool-Workload verwenden, müssen Sie einen S3-Bucket für Ihre FabricPool-Daten erstellen. Außerdem müssen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel für das Mandantenkonto erhalten, das Sie für FabricPool verwenden werden.

Was Sie benötigen

- Sie müssen ein Mandantenkonto für die Nutzung von FabricPool erstellt haben.

Über diese Aufgabe

In diesen Anweisungen wird die Verwendung von StorageGRID Mandanten-Manager zur Erstellung eines Buckets beschrieben und Zugriffsschlüssel erhalten. Sie können diese Aufgaben auch mit der Mandantenmanagement-API oder der StorageGRID S3 REST-API ausführen.

Weitere Informationen:

- ["Verwenden Sie ein Mandantenkonto"](#)
- ["S3 verwenden"](#)

Schritte

1. Melden Sie sich beim Tenant Manager an.

Sie können eine der folgenden Aktionen ausführen:

- Wählen Sie auf der Seite Mandantenkonten im Grid Manager den Link **Anmelden** für den Mieter aus, und geben Sie Ihre Anmeldedaten ein.
- Geben Sie die URL für das Mandantenkonto in einem Webbrowser ein, und geben Sie Ihre Anmeldedaten ein.

2. Erstellung eines S3-Buckets für FabricPool-Daten

Sie müssen für jedes zu verwendende ONTAP Cluster einen eindeutigen Bucket erstellen.

- Wählen Sie **STORAGE (S3) > Buckets** aus.
- Wählen Sie **Eimer erstellen**.
- Geben Sie den Namen des StorageGRID-Buckets ein, den Sie mit FabricPool verwenden möchten. Beispiel: `fabricpool-bucket`.



Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

Bucket-Namen müssen folgende Regeln einhalten:

- Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos).
 - Muss DNS-konform sein.
 - Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten.
 - Kann eine Reihe von einer oder mehreren Etiketten sein, wobei angrenzende Etiketten durch einen Zeitraum getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden.
 - Darf nicht wie eine Text-formatierte IP-Adresse aussehen.
 - Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats.
- Wählen Sie die Region für diesen Bucket aus.

Standardmäßig werden alle Buckets im erstellt `us-east-1` Werden.

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name 

Region 

Cancel

Create bucket

- a. Wählen Sie **Eimer erstellen**.
3. Erstellen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel.
 - a. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.
 - b. Wählen Sie **Schlüssel erstellen**.
 - c. Wählen Sie **Zugriffsschlüssel erstellen**.
 - d. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.

Sie geben diese Werte in ONTAP ein, wenn Sie StorageGRID als FabricPool Cloud-Tier konfigurieren.



Wenn Sie in Zukunft einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel erstellen, vergessen Sie nicht, die entsprechenden Werte in ONTAP sofort zu aktualisieren, um sicherzustellen, dass ONTAP Daten unterbrechungsfrei in StorageGRID speichern und abrufen kann.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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