Verwalten von Mandanten

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-117/admin/managing-tenants.html on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

Verwalten von Mandanten . . . 1
Mandanten managen: Übersicht . . . 1
Was sind Mandantenkonten? . . . 1
Wie erstelle ich ein Mandantenkonto? . . . 1
Wofür wird Tenant Manager verwendet? . . . 2
Erstellen Sie ein Mandantenkonto . . . 2
Greifen Sie auf den Assistenten zu . . . 3
Geben Sie Details ein . . . 3
Wählen Sie Berechtigungen aus . . . 4
Root-Zugriff definieren und Mandanten erstellen . . . 5
Beim Mandanten anmelden (optional) . . . 6
Konfigurieren Sie den Mandanten . . . 7
Mandantenkonto bearbeiten . . . 7
Ändern Sie das Passwort für den lokalen Root-Benutzer des Mandanten . . . 9
Mandantenkonto löschen . . . 10
Management von Plattform-Services . . . 10
Verwaltung von Plattformservices für Mandanten: Übersicht . . . 10
Netzwerk und Ports für Plattformservices . . . 12
Bereitstellung von Plattform-Services am Standort . . . 13
Fehlerbehebung bei Plattform-Services . . . 14
Management von S3 Select für Mandantenkonten . . . 19
Was ist S3 Select? . . . 19
Überlegungen und Anforderungen bei der Verwendung von S3 Select . . . 19

Verwalten von Mandanten

Mandanten managen: Übersicht

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3 und Swift-Clients zum Speichern und Abrufen von Objekten verwenden.

Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Was sind Mandantenkonten?

Ein Mandantenkonto ermöglicht Ihnen, entweder die Simple Storage Service (S3) REST-API oder die Swift REST-API zu verwenden, um Objekte in einem StorageGRID System zu speichern und abzurufen.

Jedes Mandantenkonto verfügt über föderierte oder lokale Gruppen, Benutzer, S3 Buckets oder Swift Container und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte durch verschiedene Einheiten zu trennen. Beispielsweise können für einen der folgenden Anwendungsfälle mehrere Mandantenkonten verwendet werden:

- **Anwendungsbeispiel für Unternehmen:** Wenn Sie ein StorageGRID-System in einer Enterprise-Anwendung verwalten, sollten Sie den Objekt-Storage des Grid möglicherweise von den verschiedenen Abteilungen Ihres Unternehmens trennen. In diesem Fall können Sie Mandantenkonten für die Marketingabteilung, die Kundenbetreuung, die Personalabteilung usw. erstellen.

  Wenn Sie das S3-Client-Protokoll verwenden, können Sie S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen eines Unternehmens zu trennen. Sie müssen keine Mandantenkonten verwenden. Siehe Anweisungen zur Implementierung "S3-Buckets und Bucket-Richtlinien" Finden Sie weitere Informationen.

- **Anwendungsbeispiel Service Provider:** Wenn Sie ein StorageGRID-System als Service-Provider verwalten, können Sie den Objekt-Storage des Grid durch die verschiedenen Entitäten verteilen, die den Storage auf Ihrem Grid leasen. In diesem Fall würden Sie Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. erstellen.

Weitere Informationen finden Sie unter "Verwenden Sie ein Mandantenkonto".

Wie erstelle ich ein Mandantenkonto?

Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Grundlegende Informationen, einschließlich Mandantenname, Client-Typ (S3 oder Swift) und optionalem Storage-Kontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformservices verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Verbundverbindung verwenden kann.
- Der erste Root-Zugriff für den Mandanten basiert darauf, ob das StorageGRID System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign On (SSO) verwendet.

Darüber hinaus können Sie die S3-Objektsperrung für das StorageGRID-System aktivieren, wenn S3-Mandantenkonten gesetzliche Vorgaben erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und managen.

Wofür wird Tenant Manager verwendet?

Nachdem Sie das Mandantenkonto erstellt haben, können sich Mandantenbenutzer beim Tenant Manager anmelden, um Aufgaben wie die folgenden auszuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Grid-Verbund für Account-Klone und Grid-übergreifende Replizierung verwenden
- Managen von S3-Zugriffsschlüsseln
- S3 Buckets erstellen und managen
- Verwenden Sie S3-Plattformservices
- Verwenden Sie S3 Select
- Monitoring der Storage-Auslastung

> Benutzer von S3-Mandanten können mit dem Tenant Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen, müssen jedoch Objekte mit einer S3-Client-Applikation aufnehmen und managen. Siehe "S3-REST-API VERWENDEN" Entsprechende Details.

> Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Berechtigung Root-Zugriff erlaubt Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

Erstellen Sie ein Mandantenkonto

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Storage in Ihrem StorageGRID-System zu kontrollieren.

Die Schritte zum Erstellen eines Mandantenkontos variieren je nachdem, ob "Identitätsföderation" Und "Single Sign On" Sind konfiguriert und ob das Grid Manager-Konto, das Sie zum Erstellen des Mandantenkontos verwenden, einer Admin-Gruppe mit Root-Zugriffsberechtigung angehört.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie verfügen über die Berechtigung Root-Zugriff oder Mandantenkonten.
- Wenn das Mandantenkonto die für den Grid Manager konfigurierte Identitätsquelle verwendet und Sie einer föderierten Gruppe Root-Zugriffsberechtigungen für das Mandantenkonto gewähren möchten, haben Sie diese föderierte Gruppe in den Grid Manager importiert. Sie müssen dieser Administratorgruppe keine Grid Manager-Berechtigungen zuweisen. Siehe "Managen von Admin-Gruppen".
- Wenn Sie einem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in einem anderen Grid über eine Grid-Federation-Verbindung ermöglichen möchten:

- Das ist schon "Grid Federation-Verbindung konfiguriert".
- Der Status der Verbindung lautet **connected**.
- Sie haben Root-Zugriffsberechtigung.
- Sie haben die Überlegungen für überprüft "Verwalten der zulässigen Mandanten für den Grid-Verbund".
- Wenn das Mandantenkonto die Identitätsquelle verwendet, die für Grid Manager konfiguriert wurde, haben Sie dieselbe Verbundgruppe in Grid Manager auf beiden Grids importiert.

  Wenn Sie den Mandanten erstellen, wählen Sie diese Gruppe aus, um die anfängliche Root-Zugriffsberechtigung für die Quell- und Zielmandantenkonten zu erhalten.

Wenn diese Administratorgruppe vor dem Erstellen des Mandanten nicht auf beiden Grids vorhanden ist, wird der Mandant nicht am Ziel repliziert.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen**.

Geben Sie Details ein

Schritte

1. Geben Sie Details für die Serviceeinheit ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, 20-stellige Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten. Wenn Sie einen Mandanten erstellen, der eine Grid-Federation-Verbindung verwendet, können Sie optional mithilfe dieses Felds ermitteln, welcher der Quell-Tenant ist und welcher der Zielmandant ist. Beispielsweise wird diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den Mandanten angezeigt, der in Grid 2 repliziert wurde: „Dieser Mandant wurde in Grid 1 erstellt.“
Client-Typ	Der Typ des Client-Protokolls, das dieser Mandant verwendet, entweder **S3** oder **Swift**. **Hinweis**: Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.
Storage-Kontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent, einen numerischen Wert für das Kontingent und die Einheiten verfügt.

2. Wählen Sie **Weiter**.

Wählen Sie Berechtigungen aus

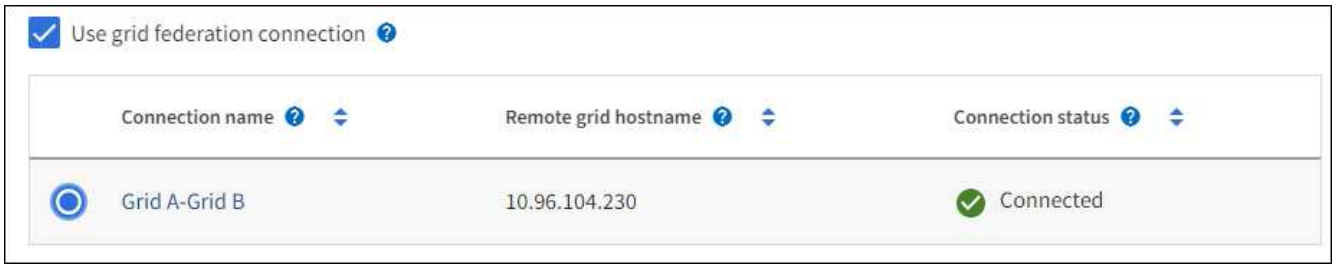
Schritte

1. Wählen Sie optional alle Berechtigungen aus, die dieser Tenant haben soll.

   Einige dieser Berechtigungen haben zusätzliche Anforderungen. Für Details wählen Sie das Hilfesymbol für jede Berechtigung aus.

Berechtigung	Wenn ausgewählt…
Unterstützung von Plattform-Services	Der Mandant kann S3-Plattformservices wie CloudMirror verwenden. Siehe "Management von Plattform-Services für S3-Mandantenkonten".
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für verbundene Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie dies haben "SSO konfiguriert" Für Ihr StorageGRID-System.
S3 Select zulassen	Der Mandant kann S3 SelectObjectContent API-Anforderungen ausgeben, um Objektdaten zu filtern und abzurufen. Siehe "Management von S3 Select für Mandantenkonten". **Wichtig**: SelectObjectContent Requests können die Load Balancer Performance für alle S3 Clients und alle Tenants verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.
Netzverbundverbindung verwenden	Der Mandant kann eine Grid Federation-Verbindung verwenden. Auswahl dieser Option: • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer aus diesem Raster (das *source Grid*) in das andere Raster der ausgewählten Verbindung (das *Destination Grid*) geklont werden. • Ermöglicht diesem Mandanten, die Grid-übergreifende Replizierung zwischen entsprechenden Buckets in jedem Grid zu konfigurieren. Siehe "Verwalten Sie die zulässigen Mandanten für den Grid-Verbund". **Hinweis**: Sie können nur **Grid Federation connection** verwenden auswählen, wenn Sie einen neuen S3-Mandanten erstellen; Sie können diese Berechtigung nicht für einen vorhandenen Mandanten auswählen.

2. Wenn Sie **Grid Federation connection** verwenden ausgewählt haben, wählen Sie eine der verfügbaren Grid Federation-Verbindungen aus.



3. Wählen Sie **Weiter**.

Root-Zugriff definieren und Mandanten erstellen

Schritte

1. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System Identitätsföderation, Single Sign-On (SSO) oder beides verwendet.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

2. Wählen Sie **Create Tenant**.

   Eine Erfolgsmeldung wird angezeigt, und die neue Serviceeinheit wird auf der Seite „Serviceeinheiten“ aufgeführt. Informationen zum Anzeigen von Mandantendetails und zum Überwachen der Mandantenaktivität finden Sie unter "Überwachen Sie die Mandantenaktivität".

3. Wenn Sie die Berechtigung **Grid Federation connection** für den Mieter verwenden ausgewählt haben:
   a. Vergewissern Sie sich, dass ein identischer Mandant auf das andere Grid in der Verbindung repliziert wurde. Die Mandanten in beiden Grids haben die gleiche 20-stellige Konto-ID, den gleichen Namen, die gleiche Beschreibung, das gleiche Kontingent und die gleichen Berechtigungen.

      Wenn die Fehlermeldung „`Tenant created without a Clone`,“ angezeigt wird, lesen Sie die Anweisungen in "Fehler beim Grid-Verbund beheben".

   b. Wenn Sie beim Definieren des Root-Zugriffs ein lokales Root-Benutzerpasswort angegeben haben, "Ändern Sie das Passwort für den lokalen Root-Benutzer" Für den replizierten Mandanten.

      Ein lokaler Root-Benutzer kann sich erst bei Tenant Manager im Zielraster anmelden, wenn das Passwort geändert wurde.

Beim Mandanten anmelden (optional)

Sie können sich nach Bedarf jetzt beim neuen Mandanten anmelden, um die Konfiguration abzuschließen, oder sich später beim Mandanten anmelden. Die Schritte zur Anmeldung hängen davon ab, ob Sie über den Standardport (443) oder einen eingeschränkten Port beim Grid Manager angemeldet sind. Siehe "Kontrolle des Zugriffs über externe Firewall".

Jetzt anmelden

Sie verwenden…	Tun Sie das…
Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	1. Wählen Sie **als root anmelden**. Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets, Identitätsverbünden, Gruppen und Benutzern angezeigt. 2. Wählen Sie die Links aus, um das Mandantenkonto zu konfigurieren. Jeder Link öffnet die entsprechende Seite im Tenant Manager. Informationen zum Ausfüllen der Seite finden Sie im "Anweisungen zur Verwendung von Mandantenkonten".
Port 443 und Sie haben kein Passwort für den lokalen Root-Benutzer festgelegt	Wählen Sie **Anmelden**, und geben Sie die Anmeldeinformationen für einen Benutzer in der Gruppe Root Access Federated ein.
Ein eingeschränkter Port	1. Wählen Sie **Fertig Stellen** 2. Wählen Sie **eingeschränkt** in der Tabelle Tenant aus, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren. Die URL für den Tenant Manager weist folgendes Format auf: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *`port`* Ist der reine Mandantenport ◦ *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten

Melden Sie sich später an

Sie verwenden…	Führen Sie eine dieser…
Port 443	• Wählen Sie im Grid Manager **MIETERS** aus und wählen Sie **Anmelden** rechts neben dem Mieternamen aus. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten
Ein eingeschränkter Port	• Wählen Sie im Grid Manager die Option **MITERS** aus, und wählen Sie **eingeschränkt**. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *`port`* Ist der ausschließlich auf Mandanten beschränkte Port ◦ *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten

Konfigurieren Sie den Mandanten

Befolgen Sie die Anweisungen unter "Verwenden Sie ein Mandantenkonto" Zum Management von Mandantengruppen und -Benutzern managen Sie S3-Zugriffsschlüssel, Buckets, Plattform-Services sowie Konto-Klone und Grid-Replizierung.

Mandantenkonto bearbeiten

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen, das Speicherkontingent oder die Berechtigungen für Mandanten zu ändern.

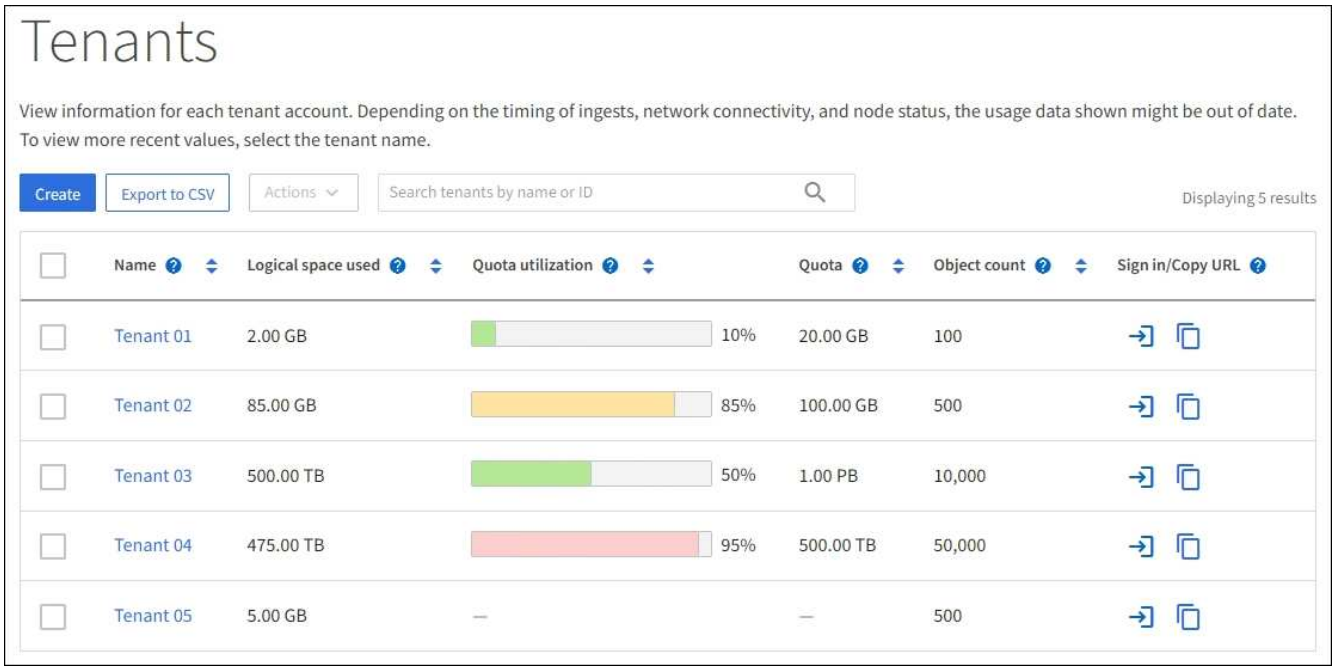
Wenn ein Mandant über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Mandantendetails von beiden Rastergittern in der Verbindung bearbeiten. Änderungen, die Sie an einem Raster in der Verbindung vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Details der Serviceeinheit zwischen den Rastern exakt synchronisieren möchten, nehmen Sie die gleichen Änderungen an beiden Rastern vor. Siehe "Verwalten Sie die zulässigen Mandanten für die Grid Federation-Verbindung".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie verfügen über die Berechtigung Root-Zugriff oder Mandantenkonten.

Schritte

1. Wählen Sie **MIETER**.



2. Suchen Sie das Mandantenkonto, das Sie bearbeiten möchten.

   Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Wählen Sie den Mandanten aus. Sie können eine der folgenden Aktionen ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **actions** > **Edit**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Bearbeiten**.
4. Ändern Sie optional die Werte für diese Felder:
   - **Name**
   - **Beschreibung**
   - **Speicherquote**
5. Wählen Sie **Weiter**.
6. Wählen oder deaktivieren Sie die Berechtigungen für das Mandantenkonto.
   - Wenn Sie **Platform Services** für einen Mandanten deaktivieren, der diese bereits nutzt, werden die Dienste, die er für seine S3-Buckets konfiguriert hat, nicht mehr funktionieren. Es wird keine Fehlermeldung an den Mandanten gesendet. Wenn der Mandant beispielsweise die Replizierung von CloudMirror für einen S3-Bucket konfiguriert hat, können sie Objekte weiterhin im Bucket speichern, doch werden Kopien dieser Objekte nicht mehr im externen S3-Bucket erstellt, den sie als Endpunkt konfiguriert haben. Siehe "Management von Plattform-Services für S3-Mandantenkonten".
   - Ändern Sie die Einstellung **verwendet eigene Identitätsquelle**, um zu bestimmen, ob das Mandantenkonto seine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

     Wenn **eigene Identitätsquelle verwendet** ist:

- Deaktiviert und ausgewählt, hat der Mandant bereits seine eigene Identitätsquelle aktiviert. Ein Mandant muss seine Identitätsquelle deaktivieren, bevor er die für den Grid Manager konfigurierte Identitätsquelle verwenden kann.
- Deaktiviert und nicht ausgewählt, SSO ist für das StorageGRID-System aktiviert. Der Mandant muss die Identitätsquelle verwenden, die für den Grid Manager konfiguriert wurde.

◦ Wählen oder deaktivieren Sie die Berechtigung **allow S3 Select** nach Bedarf. Siehe "Management von S3 Select für Mandantenkonten".

◦ Um die Berechtigung **use Grid Federation connection** zu entfernen, folgen Sie den Anweisungen für "Entfernen der Berechtigung eines Mandanten zur Verwendung des Grid-Verbunds".

Ändern Sie das Passwort für den lokalen Root-Benutzer des Mandanten

Möglicherweise müssen Sie das Passwort für den lokalen Root-Benutzer eines Mandanten ändern, wenn der Root-Benutzer aus dem Konto gesperrt ist.

Bevor Sie beginnen

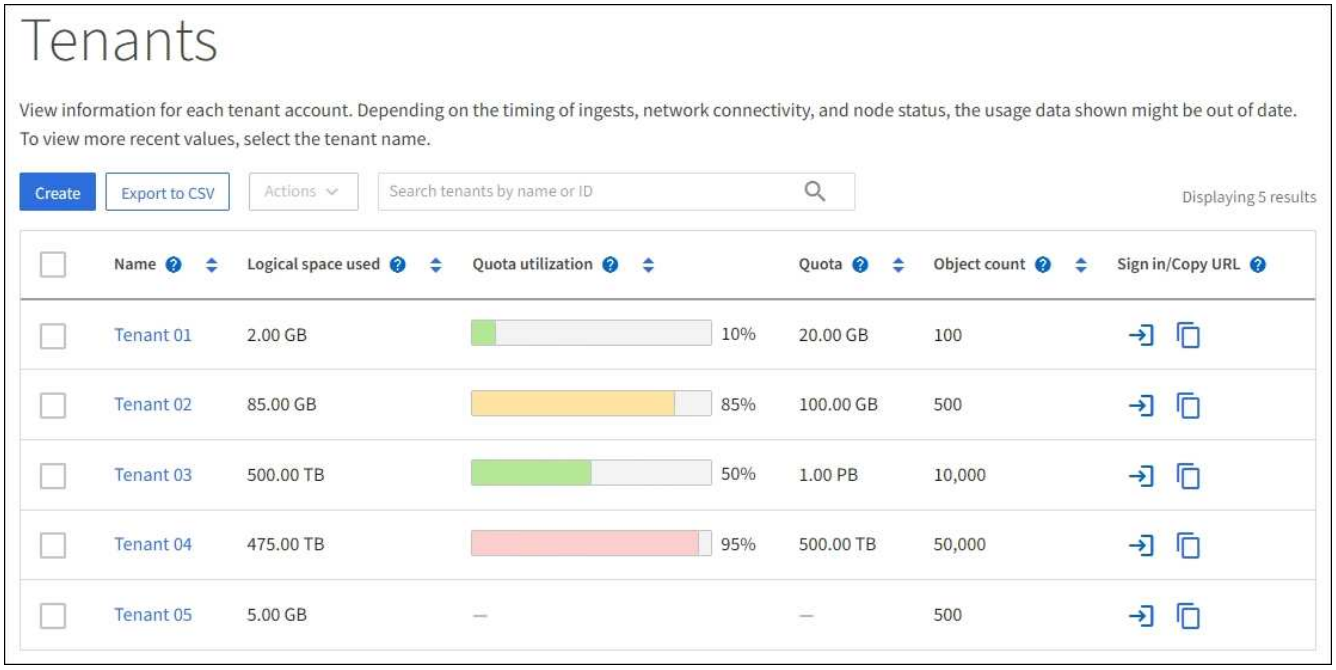
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandanten-Konto anmelden. Um Root-Benutzeraufgaben auszuführen, müssen Benutzer einer föderierten Gruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. Wählen Sie **MIETER**.



2. Wählen Sie das Mandantenkonto aus. Sie können eine der folgenden Aktionen ausführen:

◦ Aktivieren Sie das Kontrollkästchen für den Mandanten, und wählen Sie **actions** > **root-Passwort**

ändern.

- Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **actions** > **root password ändern**.

3. Geben Sie das neue Kennwort für das Mandantenkonto ein.
4. Wählen Sie **Speichern**.

Mandantenkonto löschen

Sie können ein Mandantenkonto löschen, wenn Sie den Zugriff des Mandanten auf das System dauerhaft entfernen möchten.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben alle Buckets (S3), Container (Swift) und Objekte entfernt, die dem Mandantenkonto zugeordnet sind.
- Wenn der Mandant eine Grid Federation-Verbindung verwenden darf, haben Sie die Überlegungen für geprüft "Löschen eines Mandanten mit der Berechtigung Grid Federation verwenden".

Schritte

1. Wählen Sie **MIETER**.
2. Suchen Sie das oder die Konten, die Sie löschen möchten.

   Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Um mehrere Mandanten zu löschen, aktivieren Sie die Kontrollkästchen und wählen **Aktionen** > **Löschen**.
4. Führen Sie einen der folgenden Schritte aus, um eine einzelne Serviceeinheit zu löschen:
   - Aktivieren Sie das Kontrollkästchen, und wählen Sie **Aktionen** > **Löschen**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie dann **actions** > **Delete** aus.
5. Wählen Sie **Ja**.

Management von Plattform-Services

Verwaltung von Plattformservices für Mandanten: Übersicht

Wenn Sie Plattformservices für S3-Mandantenkonten aktivieren, müssen Sie Ihr Grid so konfigurieren, dass Mandanten auf die externen Ressourcen zugreifen können, die für die Nutzung dieser Services erforderlich sind.

Was sind Plattform-Services?

Zu den Plattform-Services zählen die CloudMirror-Replizierung, Ereignisbenachrichtigungen und der Such-Integrationsservice.

Dank dieser Services können Mandanten die folgenden Funktionen mit ihren S3 Buckets nutzen:

- **CloudMirror Replikation**: Der StorageGRID CloudMirror Replikationsservice wird verwendet, um bestimmte Objekte von einem StorageGRID-Bucket auf ein bestimmtes externes Ziel zu spiegeln.

  So können Sie beispielsweise CloudMirror Replizierung verwenden, um spezifische Kundendaten in Amazon S3 zu spiegeln und anschließend AWS Services für Analysen Ihrer Daten nutzen.

  > Die CloudMirror-Replizierung weist einige wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter "Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung".

  > Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

- **Benachrichtigungen**: Pro Bucket werden Ereignisbenachrichtigungen verwendet, um Benachrichtigungen über bestimmte Aktionen zu senden, die an Objekte an einen bestimmten externen Amazon Simple Notification Service™ (Amazon SNS) durchgeführt werden.

  Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.

  > Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

- **Suchintegrationsdienst**: Der Suchintegrationsdienst dient dazu, S3-Objektmetadaten an einen bestimmten Elasticsearch-Index zu senden, in dem die Metadaten mit dem externen Dienst durchsucht oder analysiert werden können.

  Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.

  > Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperrmetadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

Dank Plattform-Services können Mandanten externe Storage-Ressourcen, Benachrichtigungsservices und Such- oder Analyseservices für ihre Daten nutzen. Da sich der Zielstandort für Plattformservices in der Regel außerhalb Ihrer StorageGRID-Implementierung befindet, müssen Sie entscheiden, ob die Nutzung dieser Services durch Mandanten gestattet werden soll. Wenn Sie dies tun, müssen Sie die Verwendung von Plattform-Services aktivieren, wenn Sie Mandantenkonten erstellen oder bearbeiten. Sie müssen auch Ihr Netzwerk so konfigurieren, dass die von Mandanten generierten Plattformservices Meldungen ihre Ziele erreichen können.

Empfehlungen für die Nutzung von Plattform-Services

Vor der Verwendung von Plattform-Services sollten Sie sich der folgenden Empfehlungen bewusst sein:

- Wenn in einem S3-Bucket im StorageGRID System sowohl die Versionierung als auch die CloudMirror-Replizierung aktiviert sind, sollten Sie für den Zielendpunkt auch die S3-Bucket-Versionierung aktivieren. So kann die CloudMirror-Replizierung ähnliche Objektversionen auf dem Endpunkt generieren.
- Sie sollten nicht mehr als 100 aktive Mandanten mit S3-Anfragen verwenden, die CloudMirror-Replizierung, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren S3-Client-Performance führen.
- Anforderungen an einen Endpunkt, die nicht abgeschlossen werden können, werden in die Warteschlange für maximal 500,000 Anfragen gestellt. Dieses Limit wird gleich von aktiven Mandanten gemeinsam genutzt. Neue Mandanten dürfen dieses Limit von 500,000 vorübergehend überschreiten, sodass neu erstellte Mandanten nicht unfair bestraft werden.

Verwandte Informationen

- "Verwenden Sie ein Mandantenkonto"
- "Konfigurieren Sie Speicher-Proxy-Einstellungen"
- "Monitoring von StorageGRID"

Netzwerk und Ports für Plattformservices

Wenn ein S3-Mandant Plattformservices verwendet, müssen Sie das Netzwerk für das Grid konfigurieren, um sicherzustellen, dass Plattformservices-Meldungen an seine Ziele gesendet werden können.

Sie können Plattformservices für ein S3-Mandantenkonto aktivieren, wenn Sie das Mandantenkonto erstellen oder aktualisieren. Wenn Plattformservices aktiviert sind, kann der Mandant Endpunkte erstellen, die als Ziel für die CloudMirror-Replizierung, Ereignisbenachrichtigungen oder Integrationsmeldungen aus seinen S3-Buckets dienen. Diese Plattform-Services-Meldungen werden von Storage-Nodes gesendet, die den ADC-Service an die Ziel-Endpunkte ausführen.

Beispielsweise können Mandanten die folgenden Typen von Ziel-Endpunkten konfigurieren:

- Ein lokal gehostetes Elasticsearch-Cluster ausführen
- Eine lokale Anwendung, die den Empfang von Amazon SNS-Nachrichten (Simple Notification Service) unterstützt
- Ein lokal gehosteter S3-Bucket auf derselben oder einer anderen Instanz von StorageGRID
- Einem externen Endpunkt wie einem Endpunkt auf Amazon Web Services

Um sicherzustellen, dass Meldungen von Plattformservices bereitgestellt werden können, müssen Sie das Netzwerk oder die Netzwerke mit den ADC-Speicherknoten konfigurieren. Sie müssen sicherstellen, dass die folgenden Ports zum Senden von Plattformservices-Meldungen an die Ziel-Endpunkte verwendet werden können.

Standardmäßig werden Plattform-Services-Meldungen an die folgenden Ports gesendet:

- **80**: Für Endpunkt-URIs, die mit http beginnen
- **443**: Für Endpunkt-URIs, die mit https beginnen

Mandanten können bei der Erstellung oder Bearbeitung eines Endpunkts einen anderen Port angeben.

Wenn eine StorageGRID-Bereitstellung als Ziel für die CloudMirror-Replikation verwendet wird, können Replikationsmeldungen auf einem anderen Port als 80 oder 443 empfangen werden. Vergewissern Sie sich, dass der von der Ziel-StorageGRID-Implementierung für S3 verwendete Port im Endpunkt angegeben ist.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch "Konfigurieren Sie Speicher-Proxy-Einstellungen" Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

Verwandte Informationen

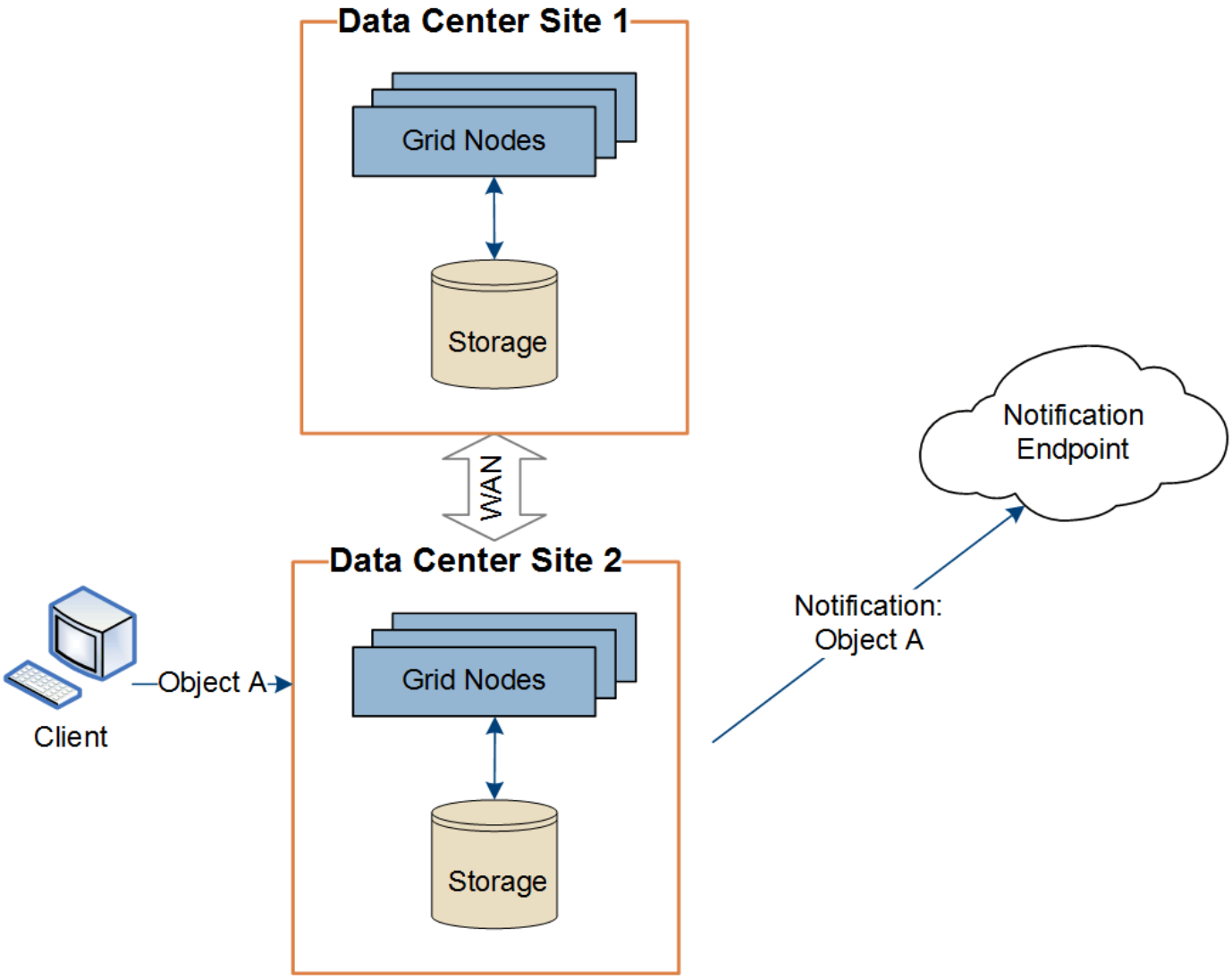
- "Verwenden Sie ein Mandantenkonto"

Bereitstellung von Plattform-Services am Standort

Alle Vorgänge von Plattform-Services werden am Standort durchgeführt.

Wenn ein Mandant einen Client verwendet, um einen S3 API Create-Vorgang für ein Objekt durch eine Verbindung zu einem Gateway-Node an Datacenter Standort 1 durchzuführen, wird die Benachrichtigung über diese Aktion von Datacenter Standort 1 ausgelöst und gesendet.

Wenn der Client anschließend einen S3-API-Löschvorgang auf demselben Objekt von Data Center Site 2 aus durchführt, wird die Benachrichtigung über die Löschaktion ausgelöst und von Data Center Site 2 gesendet.



Stellen Sie sicher, dass das Netzwerk an jedem Standort so konfiguriert ist, dass Plattformdienste-Meldungen an ihre Ziele gesendet werden können.

Fehlerbehebung bei Plattform-Services

Die in Plattform-Services verwendeten Endpunkte werden von Mandantenbenutzern im Mandanten-Manager erstellt und gewartet. Falls jedoch Probleme bei der Konfiguration oder Verwendung von Plattformservices bei einem Mandanten auftreten, können Sie das Problem mithilfe des Grid Manager beheben.

Probleme mit neuen Endpunkten

Bevor ein Mandant Plattform-Services nutzen kann, muss er mithilfe des Mandanten-Manager einen oder mehrere Endpunkte erstellen. Jeder Endpunkt stellt ein externes Ziel für einen Plattform-Service dar, wie einen StorageGRID S3 Bucket, einen Amazon Web Services Bucket, ein Thema „Simple Notification Service“ oder ein Elasticsearch-Cluster, der lokal oder in AWS gehostet wird. Jeder Endpunkt umfasst sowohl den Standort der externen Ressource als auch die für den Zugriff auf diese Ressource erforderlichen Zugangsdaten.

Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID System, ob der Endpunkt vorhanden ist und ob er mit den angegebenen Zugangsdaten erreicht werden kann. Die Verbindung zum Endpunkt wird

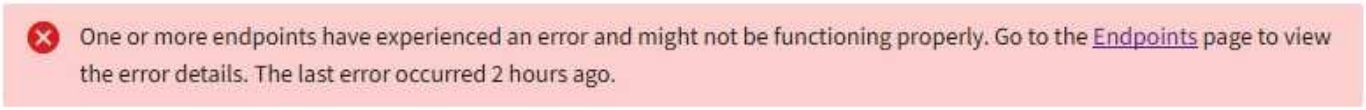
von einem Node an jedem Standort validiert.

Wenn die Endpoint-Validierung fehlschlägt, erklärt eine Fehlermeldung, warum die Endpoint-Validierung fehlgeschlagen ist. Der Mandantenbenutzer sollte das Problem lösen, und versuchen Sie dann erneut, den Endpunkt zu erstellen.

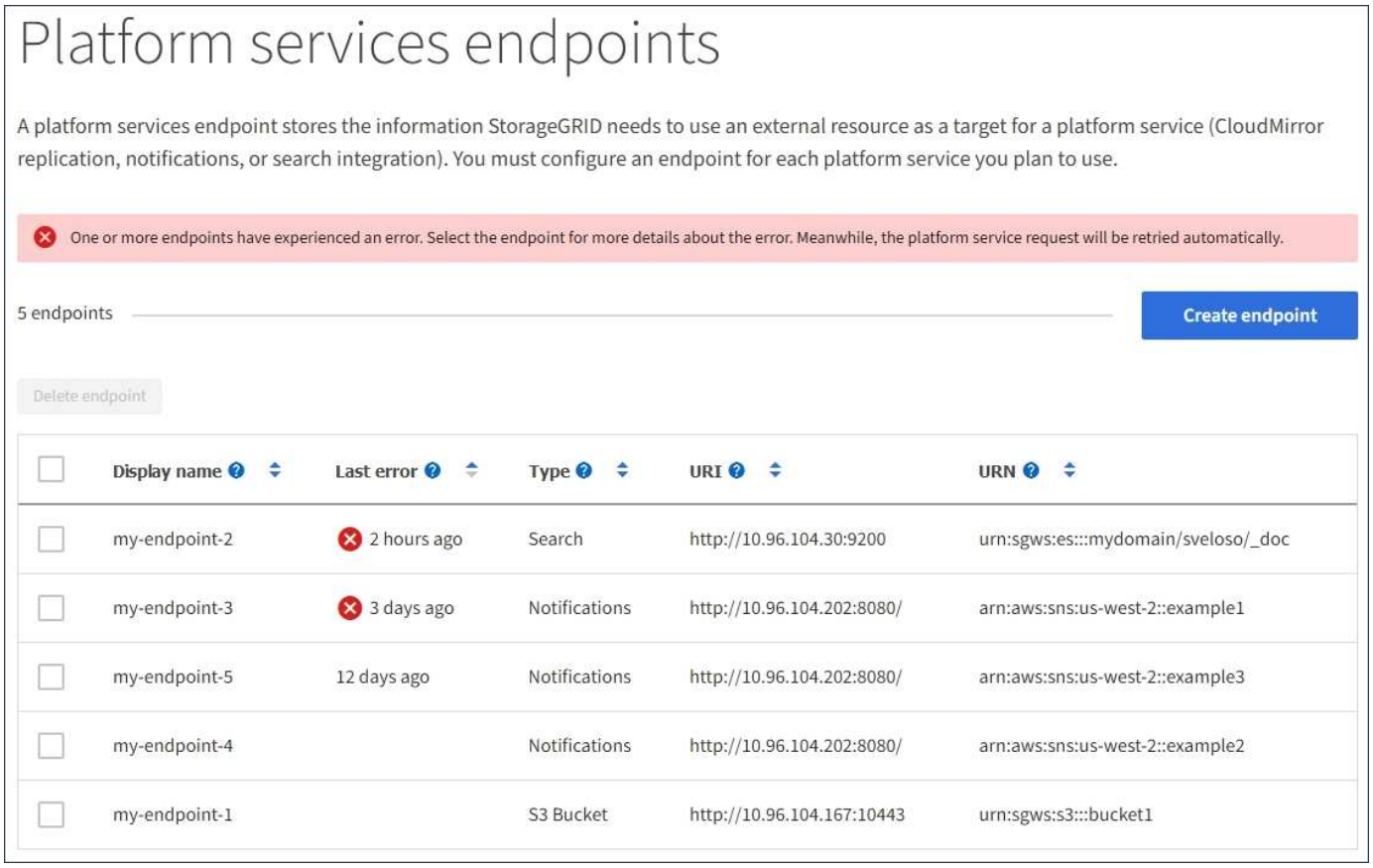
Die Erstellung von Endpunkten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn ein Fehler auftritt, wenn StorageGRID versucht, einen vorhandenen Endpunkt zu erreichen, wird im Mandantenmanager eine Meldung auf dem Dashboard angezeigt.



Mandantenbenutzer können auf der Seite Endpunkte die aktuellste Fehlermeldung für jeden Endpunkt lesen und herausfinden, wie lange der Fehler bereits aufgetreten ist. Die Spalte **Letzter Fehler** zeigt die aktuellste Fehlermeldung für jeden Endpunkt an und gibt an, wie lange der Fehler aufgetreten ist. Fehler, die das enthalten Das Symbol trat innerhalb der letzten 7 Tage auf.



Einige Fehlermeldungen in der Spalte **Letzter Fehler** können eine LOGID in Klammern enthalten. Ein Grid-Administrator oder technischer Support kann diese ID verwenden, um ausführlichere Informationen über den Fehler im bycast.log zu finden.

Probleme im Zusammenhang mit Proxy-Servern

Wenn Sie einen konfiguriert haben "Storage-Proxy" Zwischen Storage-Nodes und Plattform-Service-Endpunkten können Fehler auftreten, wenn Ihr Proxy-Service keine Meldungen von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass keine Nachrichten im Zusammenhang mit dem Plattformdienst blockiert werden.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Endpunktfehler aufgetreten sind, zeigt das Dashboard im Tenant Manager eine Warnmeldung an. Sie können die Seite Endpoints aufrufen, um weitere Details über den Fehler zu sehen.

Client-Betrieb schlägt fehl

Einige Probleme bei Plattform-Services können zum Ausfall von Client-Operationen auf dem S3-Bucket führen. Beispielsweise schlägt der S3-Client-Betrieb fehl, wenn der interne RSM-Service (Replicated State Machine) ausfällt oder es zu viele Plattformservices-Nachrichten in Warteschlange für die Lieferung gibt.

So überprüfen Sie den Status der Dienste:

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site*** > ***Storage Node*** > **SSM** > **Services** aus.

Behebbare und nicht wiederherstellbare Endpunktfehler

Nach der Erstellung von Endpunkten können Fehler bei Plattformservice-Anfragen aus verschiedenen Gründen auftreten. Einige Fehler lassen sich durch Benutzereingriffe wiederherstellen. Beispielsweise können behebbare Fehler aus den folgenden Gründen auftreten:

- Die Anmeldedaten des Benutzers wurden gelöscht oder abgelaufen.
- Der Ziel-Bucket ist nicht vorhanden.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn bei StorageGRID ein wiederherstellbarer Fehler auftritt, wird die Serviceanfrage für die Plattform erneut versucht, bis sie erfolgreich ist.

Andere Fehler können nicht behoben werden. Beispielsweise tritt ein nicht behebbarer Fehler auf, wenn der Endpunkt gelöscht wird.

Wenn bei StorageGRID ein nicht behebbarer Endpunktfehler auftritt, wird im Grid Manager der alte Alarm „Total Events“ (SMTT) ausgelöst. So zeigen Sie den alten Alarm „Ereignisse insgesamt“ an:

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site*** > ***Node*** > **SSM** > **Events** aus.
3. Letztes Ereignis oben in der Tabelle anzeigen.

   Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

4. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
5. Wählen Sie die Registerkarte **Konfiguration**, um die Ereignisanzahl zurückzusetzen.
6. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.

7. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts erneut auszulösen.

   Der Mieter kann die vorhandenen Werte erneut einreichen, um unerwünschte Änderungen zu vermeiden.

Nachrichten zu Plattform-Services können nicht bereitgestellt werden

Wenn im Ziel ein Problem auftritt, das verhindert, dass Plattformdienste-Meldungen akzeptiert werden, wird der Client-Vorgang auf dem Bucket erfolgreich ausgeführt, die Plattform-Services-Meldung wird jedoch nicht geliefert. Dieser Fehler kann z. B. auftreten, wenn die Anmeldeinformationen auf dem Ziel aktualisiert werden, sodass sich StorageGRID nicht mehr beim Ziel-Service authentifizieren kann.

Wenn Meldungen zu Plattformdiensten aufgrund eines nicht behebbaren Fehlers nicht zugestellt werden können, wird der Legacy-Alarm „Total Events (SMTT)“ im Grid Manager ausgelöst.

Langsamere Performance für Plattform-Service-Anfragen

StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten.

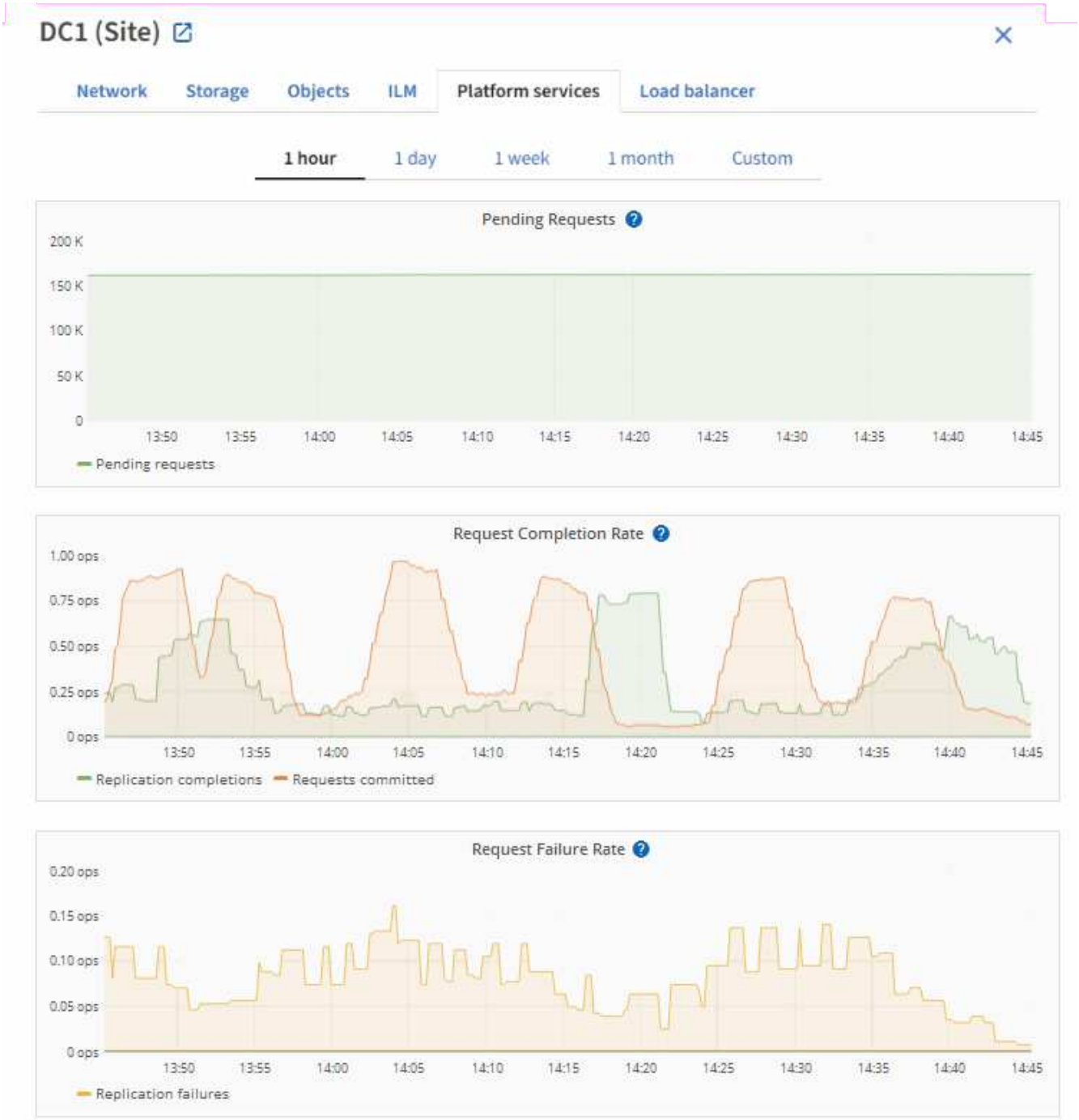
Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich.

CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Plattformdienstanfragen schlagen fehl

So zeigen Sie die Ausfallrate der Anfrage für Plattformdienste an:

1. Wählen Sie **KNOTEN**.
2. Wählen Sie ***site*** > **Platform Services**.
3. Zeigen Sie das Diagramm Fehlerrate anfordern an.



Plattformdienste – Warnung nicht verfügbar

Die Warnmeldung **Platform Services nicht verfügbar** zeigt an, dass an einem Standort keine Plattformservicevorgänge ausgeführt werden können, da zu wenige Speicherknoten mit dem RSM-Dienst ausgeführt oder verfügbar sind.

Der RSM-Dienst stellt sicher, dass Plattformserviceanforderungen an die jeweiligen Endpunkte gesendet werden.

Um diese Warnmeldung zu beheben, legen Sie fest, welche Speicherknoten am Standort den RSM-Service enthalten. (Der RSM-Service ist auf Speicherknoten vorhanden, die auch den ADC-Service enthalten.) Stellen Sie anschließend sicher, dass ein einfacher Großteil dieser Speicherknoten ausgeführt und verfügbar ist.

Wenn mehr als ein Speicherknoten, der den RSM-Dienst enthält, an einem Standort ausfällt, verlieren Sie alle ausstehenden Plattformserviceanforderungen für diesen Standort.

Zusätzliche Anleitung zur Fehlerbehebung für Endpunkte von Plattformservices

Weitere Informationen finden Sie unter **Verwenden Sie ein Mandantenkonto › Troubleshooting der Endpunkte für Plattformservices**.

Verwandte Informationen

- "Fehlerbehebung für das StorageGRID-System"

Management von S3 Select für Mandantenkonten

Bestimmte S3-Mandanten können S3 Select verwenden, um SelectObjectContent-Anfragen für einzelne Objekte auszulösen.

S3 Select bietet eine effiziente Möglichkeit, große Datenmengen zu durchsuchen, ohne eine Datenbank und zugehörige Ressourcen bereitstellen zu müssen, um die Suche zu ermöglichen. Es senkt auch die Kosten und die Latenz beim Abrufen der Daten.

Was ist S3 Select?

Mit S3 Select können S3-Clients SelectObjectContent-Anfragen verwenden, um nur die von einem Objekt benötigten Daten zu filtern und abzurufen. Die StorageGRID Implementierung von S3 Select enthält eine Untergruppe von S3 Select-Befehlen und -Funktionen.

Überlegungen und Anforderungen bei der Verwendung von S3 Select

Grid-Administrationsanforderungen

Der Grid-Administrator muss Mandanten die Möglichkeit S3 Select erteilen. Wählen Sie **S3-Auswahl zulassen** aus, wann "Erstellen eines Mandanten" Oder "Bearbeiten eines Mandanten".

Anforderungen an das Objektformat

Das Objekt, das Sie abfragen möchten, muss eines der folgenden Formate aufweisen:

- **CSV**. Kann wie ist verwendet oder in GZIP- oder BZIP2-Archiven komprimiert werden.
- **Parkett**. Zusätzliche Anforderungen an Parkett-Objekte:
  - S3 Select unterstützt nur Spaltenkomprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Komprimierung ganzer Objekte für Parkett-Objekte.
  - S3 Select unterstützt keine Parkett-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
  - Die maximale Größe der nicht komprimierten Zeilengruppe beträgt 512 MB.
  - Sie müssen die im Objektschema angegebenen Datentypen verwenden.
  - Sie können KEINE logischen TYPEN VON INTERVALL, JSON, LISTE, ZEIT oder UUID verwenden.

Anforderungen an Endpunkte

Die SelectObjectContent-Anforderung muss an ein gesendet werden "Endpunkt des StorageGRID-Load-Balancer".

Die vom Endpunkt verwendeten Admin- und Gateway-Nodes müssen einen der folgenden sein:

- Ein SG100- oder SG1000-Appliance-Node
- Ein auf VMware basierender Software-Node
- Ein Bare-Metal-Knoten, auf dem ein Kernel mit aktivierter cgroup v2 ausgeführt wird

Allgemeine Überlegungen

Abfragen können nicht direkt an Storage-Nodes gesendet werden.

> SelectObjectContent-Anforderungen können die Load Balancer-Performance für alle S3-Clients und alle Mandanten reduzieren. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Siehe "Anweisungen zur Verwendung von S3 Select".

Um sie anzuzeigen "Grafana-Diagramme" Für S3 Wählen Sie im Grid Manager Operationen über die Zeit aus, wählen Sie im Grid Manager * SUPPORT* > **Tools** > **Metriken**.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.