Mandanten verwalten

StorageGRID software

NetApp
October 21, 2025

Inhalt

Mandanten verwalten

Was sind Mieterkonten?

Mit einem Mandantenkonto können Sie die REST-API des Simple Storage Service (S3) verwenden, um Objekte in einem StorageGRID -System zu speichern und abzurufen.

Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "StorageGRID 11.8: Mandanten verwalten" .

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

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

Mandantenkonten können verwendet werden, um gespeicherte Objekte nach verschiedenen Entitäten zu trennen. Beispielsweise können mehrere Mandantenkonten für einen der folgenden Anwendungsfälle verwendet werden:

- **Anwendungsfall für Unternehmen:** Wenn Sie ein StorageGRID -System in einer Unternehmensanwendung verwalten, möchten Sie den Objektspeicher des Grids möglicherweise nach den verschiedenen Abteilungen in Ihrer Organisation trennen. In diesem Fall könnten Sie Mandantenkonten für die Marketingabteilung, die Kundensupportabteilung, die Personalabteilung usw. erstellen.

  Wenn Sie das S3-Clientprotokoll verwenden, können Sie S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen in einem Unternehmen zu trennen. Sie müssen keine Mieterkonten verwenden. Siehe Anweisungen zur Implementierung"S3-Buckets und Bucket-Richtlinien" für weitere Informationen.

- **Anwendungsfall für Dienstanbieter:** Wenn Sie ein StorageGRID -System als Dienstanbieter verwalten, können Sie den Objektspeicher des Grids nach den verschiedenen Entitäten trennen, die den Speicher in Ihrem Grid mieten. In diesem Fall würden Sie Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. erstellen.

Weitere Informationen finden Sie unter "Verwenden eines Mandantenkontos" .

Wie erstelle ich ein Mieterkonto?

Verwenden Sie den Grid-Manager, um ein Mandantenkonto zu erstellen. Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Grundlegende Informationen, einschließlich Mandantenname, Clienttyp (S3) und optionalem Speicherkontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformdienste verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Föderationsverbindung verwenden kann.
- Der anfängliche Root-Zugriff für den Mandanten, basierend darauf, ob das StorageGRID -System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign-On (SSO) verwendet.

Darüber hinaus können Sie die S3-Objektsperreinstellung für das StorageGRID -System aktivieren, wenn S3-

Mandantenkonten gesetzliche Anforderungen erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und verwalten.

Wofür wird Tenant Manager verwendet?

Nachdem Sie das Mandantenkonto erstellt haben, können sich Mandantenbenutzer beim Mandantenmanager anmelden, um beispielsweise die folgenden Aufgaben auszuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid geteilt)
- Verwalten von Gruppen und Benutzern
- Verwenden Sie die Grid-Föderation für Kontoklone und Cross-Grid-Replikation
- S3-Zugriffsschlüssel verwalten
- Erstellen und Verwalten von S3-Buckets
- Verwenden Sie S3-Plattformdienste
- Verwenden Sie S3 Select
- Überwachen der Speichernutzung

Während S3-Tenant-Benutzer mit dem Tenant Manager S3-Zugriffsschlüssel und Buckets erstellen und verwalten können, müssen sie zum Aufnehmen und Verwalten von Objekten eine S3-Clientanwendung verwenden. Sehen"Verwenden Sie die S3 REST-API" für Details.

Erstellen Sie ein Mieterkonto

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Speicher in Ihrem StorageGRID System zu steuern.

Die Schritte zum Erstellen eines Mandantenkontos variieren je nachdem, ob"Identitätsföderation" Und"Einmaliges Anmelden" konfiguriert sind und ob das Grid Manager-Konto, das Sie zum Erstellen des Mandantenkontos verwenden, zu einer Administratorgruppe mit Root-Zugriffsberechtigung gehört.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriff oder Mandantenkontenberechtigung" .
- Wenn das Mandantenkonto die für den Grid Manager konfigurierte Identitätsquelle verwendet und Sie einer föderierten Gruppe Root-Zugriffsberechtigungen für das Mandantenkonto erteilen möchten, haben Sie diese föderierte Gruppe in den Grid Manager importiert. Sie müssen dieser Administratorgruppe keine Grid Manager-Berechtigungen zuweisen. Sehen "Verwalten von Administratorgruppen" .
- Wenn Sie einem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in ein anderes Grid mithilfe einer Grid-Föderationsverbindung erlauben möchten:
  - Du hast"die Grid-Föderation-Verbindung konfiguriert" .
  - Der Status der Verbindung ist **Verbunden**.
  - Sie verfügen über Root-Zugriffsberechtigung.
  - Sie haben die Überlegungen für"Verwaltung der zulässigen Mandanten für die Grid-Föderation" .
  - Wenn das Mandantenkonto die für Grid Manager konfigurierte Identitätsquelle verwendet, haben Sie in beiden Grids dieselbe föderierte Gruppe in Grid Manager 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 in beiden Rastern vorhanden ist, wird der Mandant nicht zum Ziel repliziert.

Zugriff auf den Assistenten

Schritte

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

Details eingeben

Schritte

1. Geben Sie die Details zum Mieter ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Beim Anlegen des Mandantenkontos erhält dieses eine eindeutige, 20-stellige Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mieters. Wenn Sie einen Mandanten erstellen, der eine Grid-Föderation-Verbindung verwendet, können Sie dieses Feld optional verwenden, um zu ermitteln, welcher der Quellmandant und welcher der Zielmandant ist. Beispielsweise wird diese Beschreibung für einen in Grid 1 erstellten Mandanten auch für den in Grid 2 replizierten Mandanten angezeigt: „Dieser Mandant wurde in Grid 1 erstellt.“
Client-Typ	Der Typ des Clientprotokolls, das dieser Mandant verwenden wird, entweder **S3** oder **Swift**. **Hinweis**: Die Unterstützung für Swift-Clientanwendungen ist veraltet und wird in einer zukünftigen Version entfernt.
Speicherkontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent verfügt, geben Sie einen numerischen Wert für das Kontingent und die Einheiten ein.

2. Wählen Sie **Weiter**.

Berechtigungen auswählen

Schritte

1. Wählen Sie optional die grundlegenden Berechtigungen aus, die dieser Mandant haben soll.

Für einige dieser Berechtigungen gelten zusätzliche Anforderungen. Um Einzelheiten zu erfahren, wählen Sie das Hilfesymbol für jede Berechtigung aus.

Erlaubnis	Falls ausgewählt…
Plattformdienste zulassen	Der Mieter kann S3-Plattformdienste wie CloudMirror verwenden. Sehen "Plattformdienste für S3-Mandantenkonten verwalten" .
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für föderierte Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie"konfiguriertes SSO" für Ihr StorageGRID System.
S3-Auswahl zulassen	Der Mandant kann S3 SelectObjectContent-API-Anfragen stellen, um Objektdaten zu filtern und abzurufen. Sehen "Verwalten von S3 Select für Mandantenkonten" . **Wichtig**: SelectObjectContent-Anfragen können die Leistung des Load Balancers für alle S3-Clients und alle Mandanten verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

2. Wählen Sie optional die erweiterten Berechtigungen aus, die dieser Mandant haben soll.

Erlaubnis	Falls ausgewählt…
Grid-Föderation-Verbindung	Der Mieter kann eine Grid-Föderation-Verbindung nutzen, die: • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer von diesem Raster (dem *Quellraster*) in das andere Raster in der ausgewählten Verbindung (das *Zielraster*) geklont werden. • Ermöglicht diesem Mandanten, die Cross-Grid-Replikation zwischen entsprechenden Buckets auf jedem Grid zu konfigurieren. Sehen "Verwalten der zulässigen Mandanten für die Grid-Föderation" .
S3-Objektsperre	Erlauben Sie dem Mandanten, bestimmte Funktionen von S3 Object Lock zu verwenden: • **Maximale Aufbewahrungsdauer festlegen** definiert, wie lange neue Objekte, die diesem Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. • **Compliance-Modus zulassen** verhindert, dass Benutzer während der Aufbewahrungsfrist geschützte Objektversionen überschreiben oder löschen.

3. Wählen Sie **Weiter**.

Definieren Sie den Root-Zugriff und erstellen Sie einen Mandanten

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

2. Wählen Sie **Mandanten erstellen**.

   Es wird eine Erfolgsmeldung angezeigt und der neue Mandant wird auf der Seite „Mandanten“ aufgeführt. Informationen zum Anzeigen von Mandantendetails und Überwachen der Mandantenaktivität finden Sie unter"Überwachen Sie die Mieteraktivität" .

   Das Anwenden von Mandanteneinstellungen im gesamten Grid kann je nach Netzwerkkonnektivität, Knotenstatus und Cassandra-Vorgängen 15 Minuten oder länger dauern.

3. Wenn Sie für den Mandanten die Berechtigung **Grid-Föderationsverbindung verwenden** ausgewählt haben:
   a. Bestätigen Sie, dass ein identischer Mandant in das andere Grid in der Verbindung repliziert wurde. Die Mandanten in beiden Grids verfügen über dieselbe 20-stellige Konto-ID, denselben Namen, dieselbe Beschreibung, dasselbe Kontingent und dieselben Berechtigungen.

      Wenn die Fehlermeldung „Mandant ohne Klon erstellt“ angezeigt wird, lesen Sie die Anweisungen in"Beheben von Grid-Föderationsfehlern" .

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

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

Beim Mandanten Sign in (optional)

Bei Bedarf können Sie sich jetzt beim neuen Mandanten anmelden, um die Konfiguration abzuschließen, oder Sie können sich später beim Mandanten anmelden. Die Anmeldeschritte hängen davon ab, ob Sie über den Standardport (443) oder einen eingeschränkten Port beim Grid Manager angemeldet sind. Sehen "Zugriffskontrolle an externer Firewall" .

Jetzt Sign in

Wenn Sie verwenden…	Machen Sie Folgendes…
Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	1. Wählen Sie * Als Root Sign in *. Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets, Identitätsföderation, Gruppen und Benutzern angezeigt. 2. Wählen Sie die Links aus, um das Mandantenkonto zu konfigurieren. Jeder Link öffnet die entsprechende Seite im Mandantenmanager. Um die Seite zu vervollständigen, sehen Sie sich die"Anleitung zur Nutzung von Mieterkonten" .
Port 443 und Sie haben kein Passwort für den lokalen Root-Benutzer festgelegt	Wählen Sie * Sign in* aus und geben Sie die Anmeldeinformationen für einen Benutzer in der Verbundgruppe mit Root-Zugriff ein.
Ein eingeschränkter Port	1. Wählen Sie **Fertig** 2. Wählen Sie in der Mandantentabelle **Eingeschränkt** aus, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren. Die URL für den Tenant Manager hat dieses Format: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`ist ein vollqualifizierter Domänenname oder die IP-Adresse eines Admin-Knotens ◦ `*port*`ist der Tenant-Only-Port ◦ `*20-digit-account-id*`ist die eindeutige Konto-ID des Mandanten

Später Sign in

Wenn Sie verwenden…	Machen Sie eines davon …
Port 443	• Wählen Sie im Grid Manager **MIETER** und rechts neben dem Mandantennamen * Sign in* 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 vollqualifizierter Domänenname oder die IP-Adresse eines Admin-Knotens ◦ `*20-digit-account-id*`ist die eindeutige Konto-ID des Mandanten

Wenn Sie verwenden…	Machen Sie eines davon …
Ein eingeschränkter Port	• Wählen Sie im Grid Manager **MIETER** und dann **Eingeschränkt** aus. • 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 vollqualifizierter Domänenname oder die IP-Adresse eines Admin-Knotens ◦ `*port*`ist der eingeschränkte Port nur für Mandanten ◦ `*20-digit-account-id*`ist die eindeutige Konto-ID des Mandanten

Konfigurieren des Mandanten

Befolgen Sie die Anweisungen in"Verwenden eines Mandantenkontos" zur Verwaltung von Mandantengruppen und Benutzern, S3-Zugriffsschlüsseln, Buckets, Plattformdiensten sowie Kontoklonen und Cross-Grid-Replikation.

Mieterkonto bearbeiten

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

Wenn ein Mandant über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie Mandantendetails von jedem Grid in der Verbindung aus bearbeiten. Änderungen, die Sie in der Verbindung an einem Raster vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Mieterdetails zwischen den Rastern genau synchron halten möchten, nehmen Sie in beiden Rastern die gleichen Änderungen vor. Sehen "Verwalten Sie die zulässigen Mandanten für die Grid-Föderation-Verbindung" .

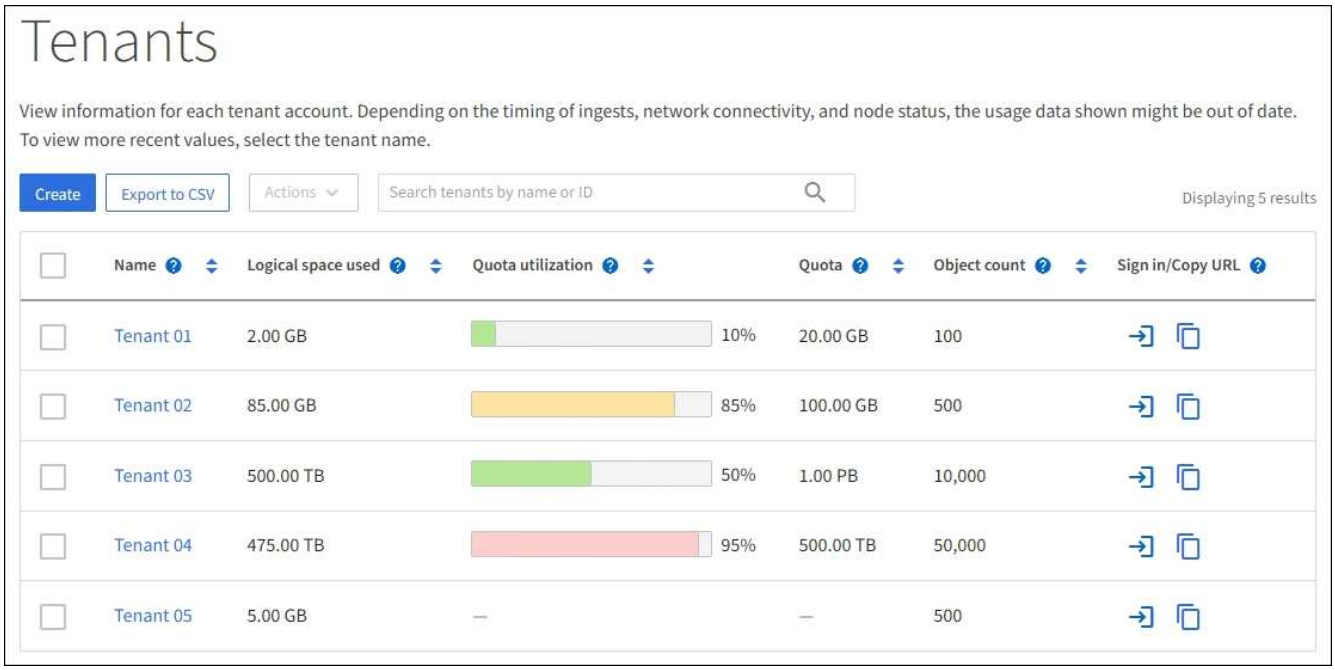
Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriff oder Mandantenkontenberechtigung" .

Das Anwenden von Mandanteneinstellungen im gesamten Grid kann je nach Netzwerkkonnektivität, Knotenstatus und Cassandra-Vorgängen 15 Minuten oder länger dauern.

Schritte

1. Wählen Sie **MIETER** aus.



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

   Verwenden Sie das Suchfeld, um nach einem Mieter anhand seines Namens oder seiner Mieter-ID zu suchen.

3. Wählen Sie den Mandanten aus. Sie können einen der folgenden Schritte ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **Aktionen** > **Bearbeiten**.
   - Wählen Sie den Mandantennamen aus, um die Detailseite anzuzeigen, und wählen Sie **Bearbeiten**.
4. Ändern Sie optional die Werte für diese Felder:
   - **Name**
   - **Beschreibung**
   - **Speicherkontingent**
5. Wählen Sie **Weiter**.
6. Aktivieren oder deaktivieren Sie die Berechtigungen für das Mandantenkonto.
   - Wenn Sie **Plattformdienste** für einen Mandanten deaktivieren, der sie bereits verwendet, funktionieren die Dienste, die er für seine S3-Buckets konfiguriert hat, nicht mehr. Es wird keine Fehlermeldung an den Mieter gesendet. Wenn der Mandant beispielsweise die CloudMirror-Replikation für einen S3-Bucket konfiguriert hat, kann er zwar weiterhin Objekte im Bucket speichern, es werden jedoch keine Kopien dieser Objekte mehr im externen S3-Bucket erstellt, den er als Endpunkt konfiguriert hat. Sehen "Plattformdienste für S3-Mandantenkonten verwalten" .
   - Ändern Sie die Einstellung **Eigene Identitätsquelle verwenden**, um festzulegen, ob das Mandantenkonto seine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

     Wenn **Eigene Identitätsquelle verwenden** lautet:

     - Deaktiviert und ausgewählt: Der Mandant hat seine eigene Identitätsquelle bereits 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.
    - Aktivieren oder deaktivieren Sie die Berechtigung **S3 Select zulassen** nach Bedarf. Sehen "Verwalten von S3 Select für Mandantenkonten" .
    - So entfernen Sie die Berechtigung **Grid-Föderationsverbindung verwenden**:
        i. Wählen Sie die Registerkarte **Grid-Föderation**.
        ii. Wählen Sie **Berechtigung entfernen**.
    - So fügen Sie die Berechtigung **Grid-Föderationsverbindung verwenden** hinzu:
        i. Wählen Sie die Registerkarte **Grid-Föderation**.
        ii. Aktivieren Sie das Kontrollkästchen **Grid-Föderationsverbindung verwenden**.
        iii. Wählen Sie optional **Vorhandene lokale Benutzer und Gruppen klonen** aus, um sie in das Remote-Raster zu klonen. Wenn Sie möchten, können Sie den laufenden Klonvorgang anhalten oder den Klonvorgang wiederholen, wenn das Klonen einiger lokaler Benutzer oder Gruppen nach Abschluss des letzten Klonvorgangs fehlgeschlagen ist.
    - So legen Sie eine maximale Aufbewahrungsdauer fest oder aktivieren den Compliance-Modus:

        Bevor Sie diese Einstellungen verwenden können, muss die S3-Objektsperre im Raster aktiviert sein.

        i. Wählen Sie die Registerkarte **S3-Objektsperre**.
        ii. Geben Sie für **Maximale Aufbewahrungsdauer festlegen** einen Wert ein und wählen Sie den Zeitraum aus dem Pulldown-Menü aus.
        iii. Aktivieren Sie das Kontrollkästchen für **Compliance-Modus zulassen**.

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

Möglicherweise müssen Sie das Kennwort für den lokalen Root-Benutzer eines Mandanten ändern, wenn der Root-Benutzer vom Konto ausgeschlossen ist.

Bevor Sie beginnen

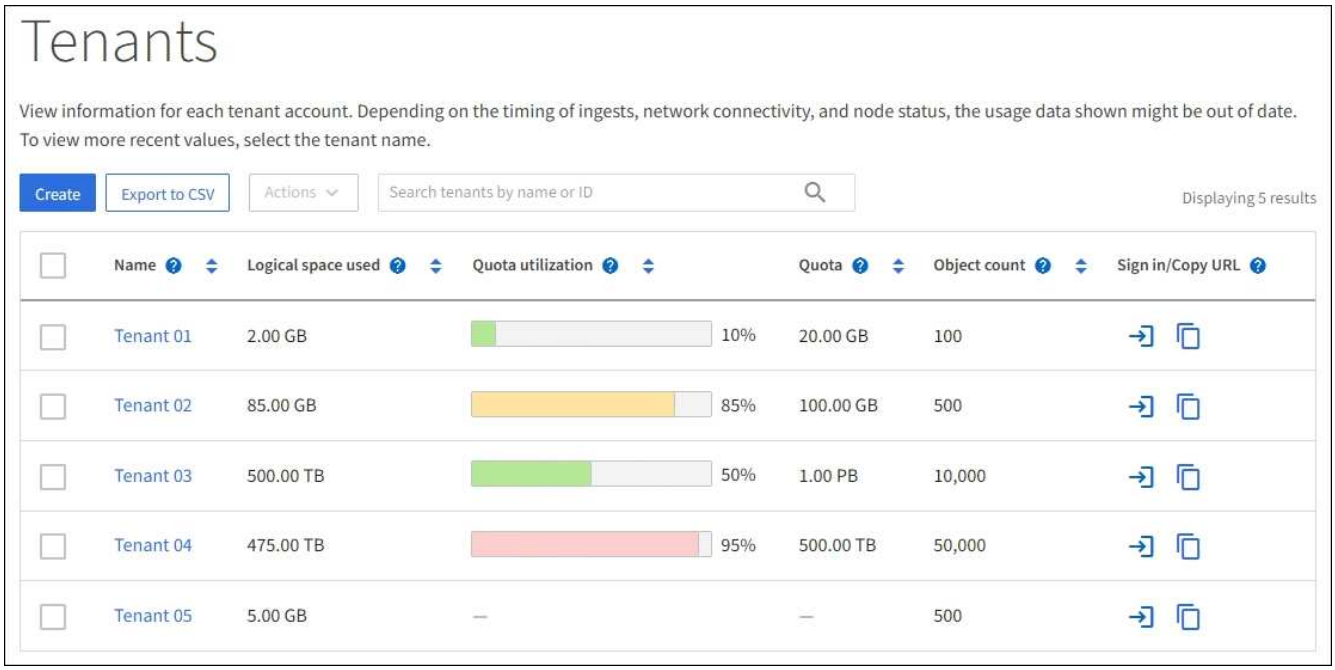
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

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

Schritte

1. Wählen Sie **MIETER** aus.



2. Wählen Sie das Mandantenkonto aus. Sie können einen der folgenden Schritte ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **Aktionen** > **Root-Passwort ändern**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Aktionen** > **Root-Passwort ändern**.
3. Geben Sie das neue Passwort für das Mieterkonto ein.
4. Wählen Sie **Speichern**.

Mieterkonto löschen

Sie können ein Mieterkonto löschen, wenn Sie dem Mieter den Zugriff auf das System dauerhaft entziehen möchten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben alle mit dem Mandantenkonto verknüpften S3-Buckets und -Objekte entfernt.
- Wenn der Mieter eine Grid-Föderation-Verbindung verwenden darf, haben Sie die Überlegungen für"Löschen eines Mandanten mit der Berechtigung „Grid-Föderationsverbindung verwenden“" .

Schritte

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

   Verwenden Sie das Suchfeld, um nach einem Mieter anhand seines Namens oder seiner Mieter-ID zu suchen.

3. Um mehrere Mandanten zu löschen, aktivieren Sie die Kontrollkästchen und wählen Sie **Aktionen** > **Löschen**.

4. Um einen einzelnen Mandanten zu löschen, führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen und wählen Sie **Aktionen** > **Löschen**.
   - Wählen Sie den Mandantennamen aus, um die Detailseite anzuzeigen, und wählen Sie dann **Aktionen** > **Löschen**.
5. Wählen Sie **Ja**.

Plattformdienste verwalten

Was sind Plattformdienste?

Zu den Plattformdiensten gehören CloudMirror-Replikation, Ereignisbenachrichtigungen und der Suchintegrationsdienst.

Wenn Sie Plattformdienste für S3-Mandantenkonten aktivieren, müssen Sie Ihr Grid so konfigurieren, dass Mandanten auf die externen Ressourcen zugreifen können, die zur Verwendung dieser Dienste erforderlich sind.

CloudMirror-Replikation

Der StorageGRID CloudMirror-Replikationsdienst wird verwendet, um bestimmte Objekte aus einem StorageGRID Bucket an ein angegebenes externes Ziel zu spiegeln.

Sie können beispielsweise die CloudMirror-Replikation verwenden, um bestimmte Kundendatensätze in Amazon S3 zu spiegeln und dann AWS-Dienste nutzen, um Analysen Ihrer Daten durchzuführen.

> Die CloudMirror-Replikation weist einige wichtige Ähnlichkeiten und Unterschiede zur Cross-Grid-Replikationsfunktion auf. Weitere Informationen finden Sie unter"Vergleichen Sie Cross-Grid-Replikation und CloudMirror-Replikation" .

> Die CloudMirror-Replikation wird nicht unterstützt, wenn im Quell-Bucket S3 Object Lock aktiviert ist.

Benachrichtigungen

Bucket-spezifische Ereignisbenachrichtigungen werden verwendet, um Benachrichtigungen über bestimmte an Objekten ausgeführte Aktionen an einen angegebenen externen Kafka-Cluster oder Amazon Simple Notification Service zu senden.

Sie können beispielsweise Warnmeldungen konfigurieren, die an Administratoren gesendet werden, wenn ein Objekt zu einem Bucket hinzugefügt wird, wobei die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verknüpft sind.

> Obwohl die Ereignisbenachrichtigung für einen Bucket mit aktivierter S3-Objektsperre konfiguriert werden kann, werden die S3-Objektsperre-Metadaten (einschließlich „Aufbewahrungsdatum“ und „Legal Hold“-Status) der Objekte nicht in die Benachrichtigungsnachrichten aufgenommen.

Suchintegrationsdienst

Der Suchintegrationsdienst wird verwendet, um S3-Objektmetadaten an einen angegebenen Elasticsearch-

Index zu senden, wo die Metadaten mithilfe des externen Dienstes gesucht oder analysiert werden können.

Sie können Ihre Buckets beispielsweise so konfigurieren, dass S3-Objektmetadaten an einen Remote-Elasticsearch-Dienst gesendet werden. Anschließend können Sie Elasticsearch verwenden, um Bucket-übergreifende Suchen durchzuführen und anspruchsvolle Analysen der in Ihren Objektmetadaten vorhandenen Muster durchzuführen.

> Obwohl die Elasticsearch-Integration für einen Bucket mit aktivierter S3 Object Lock konfiguriert werden kann, werden die S3 Object Lock-Metadaten (einschließlich „Retain Until Date“ und „Legal Hold“-Status) der Objekte nicht in die Benachrichtigungsnachrichten aufgenommen.

Plattformdienste geben Mietern die Möglichkeit, externe Speicherressourcen, Benachrichtigungsdienste sowie Such- oder Analysedienste mit ihren Daten zu verwenden. Da sich der Zielspeicherort für Plattformdienste normalerweise außerhalb Ihrer StorageGRID -Bereitstellung befindet, müssen Sie entscheiden, ob Sie Mandanten die Nutzung dieser Dienste gestatten möchten. In diesem Fall müssen Sie die Verwendung von Plattformdiensten aktivieren, wenn Sie Mandantenkonten erstellen oder bearbeiten. Sie müssen Ihr Netzwerk außerdem so konfigurieren, dass die von den Mandanten generierten Plattformdienstnachrichten ihre Ziele erreichen können.

Empfehlungen zur Nutzung von Plattformdiensten

Beachten Sie vor der Verwendung von Plattformdiensten die folgenden Empfehlungen:

- Wenn für einen S3-Bucket im StorageGRID -System sowohl die Versionierung als auch die CloudMirror-Replikation aktiviert ist, sollten Sie auch die S3-Bucket-Versionierung für den Zielendpunkt aktivieren. Dadurch kann die CloudMirror-Replikation ähnliche Objektversionen auf dem Endpunkt generieren.
- Sie sollten nicht mehr als 100 aktive Mandanten mit S3-Anfragen verwenden, die CloudMirror-Replikation, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren Leistung des S3-Clients führen.
- Anfragen an einen Endpunkt, die nicht abgeschlossen werden können, werden auf maximal 500.000 Anfragen in die Warteschlange gestellt. Dieses Limit wird gleichmäßig unter den aktiven Mietern aufgeteilt. Damit neu hinzukommende Mieter nicht ungerechterweise benachteiligt werden, ist es neuen Mietern gestattet, diese Grenze von 500.000 vorübergehend zu überschreiten.

Ähnliche Informationen

- "Plattformdienste verwalten"
- "Konfigurieren der Speicherproxyeinstellungen"
- "StorageGRID überwachen"

Netzwerk und Ports für Plattformdienste

Wenn Sie einem S3-Mandanten die Verwendung von Plattformdiensten gestatten, müssen Sie die Vernetzung für das Grid konfigurieren, um sicherzustellen, dass Nachrichten der Plattformdienste an ihre Ziele übermittelt werden können.

Sie können Plattformdienste für ein S3-Mandantenkonto aktivieren, wenn Sie das Mandantenkonto erstellen oder aktualisieren. Wenn Plattformdienste aktiviert sind, kann der Mandant Endpunkte erstellen, die als Ziel für CloudMirror-Replikation, Ereignisbenachrichtigungen oder Suchintegrationsnachrichten aus seinen S3-Buckets dienen. Diese Plattformdienstnachrichten werden von Speicherknoten, die den ADC-Dienst ausführen, an die Zielendpunkte gesendet.

Beispielsweise können Mandanten die folgenden Arten von Zielendpunkten konfigurieren:

- Ein lokal gehosteter Elasticsearch-Cluster
- Eine lokale Anwendung, die den Empfang von Amazon Simple Notification Service-Nachrichten unterstützt
- Ein lokal gehosteter Kafka-Cluster
- Ein lokal gehosteter S3-Bucket auf derselben oder einer anderen Instanz von StorageGRID
- Ein externer Endpunkt, z. B. ein Endpunkt auf Amazon Web Services.

Um sicherzustellen, dass Nachrichten der Plattformdienste zugestellt werden können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die die ADC-Speicherknoten enthalten. Sie müssen sicherstellen, dass die folgenden Ports zum Senden von Plattformdienstnachrichten an die Zielendpunkte verwendet werden können.

Standardmäßig werden Nachrichten der Plattformdienste über die folgenden Ports gesendet:

- **80**: Für Endpunkt-URIs, die mit http beginnen (die meisten Endpunkte)
- **443**: Für Endpunkt-URIs, die mit https beginnen (die meisten Endpunkte)
- **9092**: Für Endpunkt-URIs, die mit http oder https beginnen (nur Kafka-Endpunkte)

Mandanten können beim Erstellen oder Bearbeiten eines Endpunkts einen anderen Port angeben.

> Wenn eine StorageGRID Bereitstellung als Ziel für die CloudMirror-Replikation verwendet wird, werden Replikationsnachrichten möglicherweise auf einem anderen Port als 80 oder 443 empfangen. Stellen Sie sicher, dass der von der StorageGRID Zielbereitstellung für S3 verwendete Port im Endpunkt angegeben ist.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie außerdem"Konfigurieren der Speicherproxyeinstellungen" um das Senden von Nachrichten an externe Endpunkte zu ermöglichen, beispielsweise an einen Endpunkt im Internet.

Ähnliche Informationen

"Verwenden eines Mandantenkontos"

Pro Site-Zustellung von Plattformdienstnachrichten

Alle Vorgänge der Plattformdienste werden pro Site durchgeführt.

Das heißt, wenn ein Mandant einen Client verwendet, um einen S3-API-Erstellungsvorgang für ein Objekt auszuführen, indem er eine Verbindung zu einem Gateway-Knoten am Rechenzentrumsstandort 1 herstellt, wird die Benachrichtigung über diese Aktion ausgelöst und vom Rechenzentrumsstandort 1 gesendet.

Wenn der Client anschließend einen S3-API-Löschvorgang für dasselbe Objekt vom Rechenzentrumsstandort 2 aus durchführt, wird die Benachrichtigung über die Löschaktion ausgelöst und vom Rechenzentrumsstandort 2 gesendet.

Stellen Sie sicher, dass das Netzwerk an jedem Standort so konfiguriert ist, dass Nachrichten der Plattformdienste an ihre Ziele übermittelt werden können.

Fehlerbehebung bei Plattformdiensten

Die in Plattformdiensten verwendeten Endpunkte werden von Mandantenbenutzern im Mandanten-Manager erstellt und verwaltet. Wenn ein Mandant jedoch Probleme bei der Konfiguration oder Verwendung von Plattformdiensten hat, können Sie möglicherweise den Grid-Manager zur Lösung des Problems verwenden.

Probleme mit neuen Endpunkten

Bevor ein Mandant Plattformdienste nutzen kann, muss er mithilfe des Mandanten-Managers einen oder mehrere Endpunkte erstellen. Jeder Endpunkt stellt ein externes Ziel für einen Plattformdienst dar, beispielsweise einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Amazon Simple Notification Service-Thema, ein Kafka-Thema oder einen lokal oder auf AWS gehosteten Elasticsearch-Cluster. Jeder Endpunkt enthält sowohl den Standort der externen Ressource als auch die für den Zugriff auf diese Ressource erforderlichen Anmeldeinformationen.

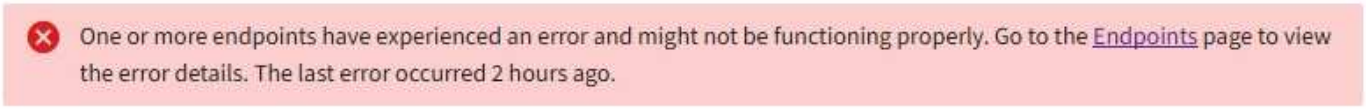
Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID -System, ob der Endpunkt vorhanden ist und mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Wenn die Endpunktvalidierung fehlschlägt, wird in einer Fehlermeldung der Grund für das Fehlschlagen der Endpunktvalidierung erläutert. Der Mandantenbenutzer sollte das Problem beheben und dann erneut versuchen, den Endpunkt zu erstellen.

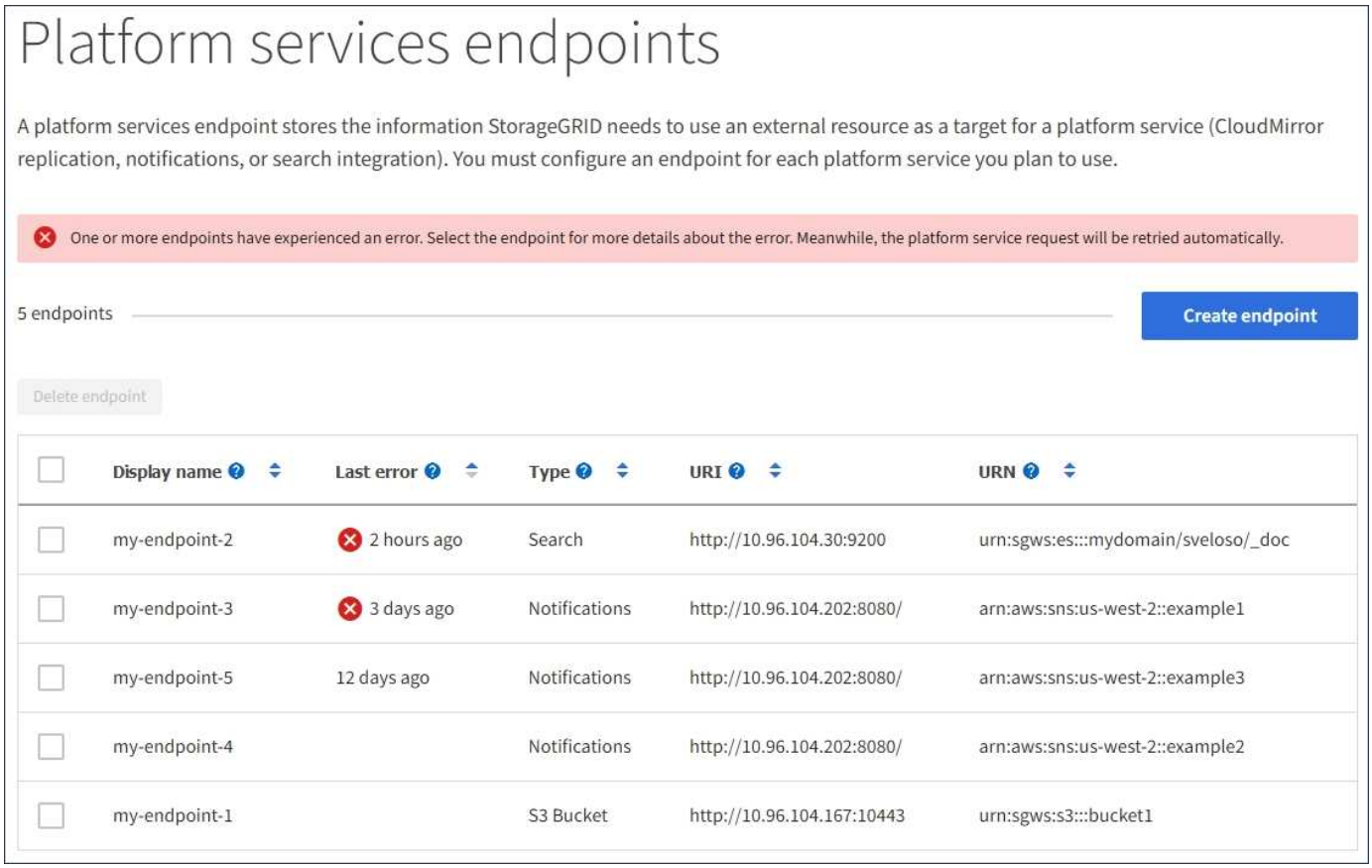
> ⓘ Die Endpunkterstellung schlägt fehl, wenn die Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn beim Versuch von StorageGRID , einen vorhandenen Endpunkt zu erreichen, ein Fehler auftritt, wird auf dem Dashboard im Tenant Manager eine Meldung angezeigt.



Mandantenbenutzer können auf der Seite „Endpunkte“ die neueste Fehlermeldung für jeden Endpunkt überprüfen und feststellen, wie lange der Fehler her ist. In der Spalte **Letzter Fehler** wird für jeden Endpunkt die aktuellste Fehlermeldung angezeigt und angegeben, wie lange der Fehler her ist. Fehler, die Folgendes beinhalten: Symbol ist innerhalb der letzten 7 Tage aufgetreten.



Einige Fehlermeldungen in der Spalte **Letzter Fehler** enthalten möglicherweise eine Protokoll-ID in Klammern. Ein Grid-Administrator oder der technische Support kann anhand dieser ID detailliertere Informationen zum Fehler im bycast.log finden.

Probleme im Zusammenhang mit Proxyservern

Wenn Sie eine"Speicherproxy" zwischen Speicherknoten und Plattformdienst-Endpunkten können Fehler auftreten, wenn Ihr Proxydienst keine Nachrichten von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxyservers, um sicherzustellen, dass plattformdienstbezogene Nachrichten nicht blockiert werden.

Feststellen, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Endpunktfehler aufgetreten sind, wird im Dashboard im Tenant Manager eine Warnmeldung angezeigt. Weitere Einzelheiten zum Fehler finden Sie auf der Seite „Endpunkte“.

Clientvorgänge schlagen fehl

Einige Probleme mit Plattformdiensten können dazu führen, dass Clientvorgänge im S3-Bucket fehlschlagen. Beispielsweise schlagen S3-Clientvorgänge fehl, wenn der interne Dienst „Replicated State Machine“ (RSM) angehalten wird oder wenn zu viele Nachrichten der Plattformdienste zur Zustellung in der Warteschlange stehen.

So überprüfen Sie den Status der Dienste:

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***site*** > ***Storage Node*** > **SSM** > **Services**.

Behebbare und nicht behebbare Endpunktfehler

Nachdem Endpunkte erstellt wurden, können aus verschiedenen Gründen Fehler bei Plattform-Serviceanforderungen auftreten. Einige Fehler können durch Benutzereingriff behoben werden. Behebbare Fehler können beispielsweise aus folgenden Gründen auftreten:

- Die Anmeldeinformationen des Benutzers wurden gelöscht oder sind abgelaufen.
- Der Ziel-Bucket existiert nicht.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn StorageGRID auf einen behebbaren Fehler stößt, wird die Plattform-Serviceanforderung so lange wiederholt, bis sie erfolgreich ist.

Andere Fehler sind nicht behebbar. Beispielsweise tritt ein nicht behebbarer Fehler auf, wenn der Endpunkt gelöscht wird.

Wenn StorageGRID auf einen nicht behebbaren Endpunktfehler stößt:

- Gehen Sie im Grid Manager zu **Support** > **Tools** > **Metriken** > **Grafana** > **Übersicht über Plattformdienste**, um Fehlerdetails anzuzeigen.
- Gehen Sie im Tenant Manager zu **STORAGE (S3)** > **Platform Services Endpoints**, um die Fehlerdetails anzuzeigen.
- Überprüfen Sie die `/var/local/log/bycast-err.log` für zugehörige Fehler. Speicherknoten mit dem ADC-Dienst enthalten diese Protokolldatei.

Nachrichten der Plattformdienste können nicht zugestellt werden

Wenn beim Ziel ein Problem auftritt, das die Annahme von Plattformdienstnachrichten verhindert, ist der Clientvorgang für den Bucket zwar erfolgreich, die Plattformdienstnachricht wird jedoch nicht zugestellt. Dieser Fehler kann beispielsweise auftreten, wenn die Anmeldeinformationen am Ziel aktualisiert werden, sodass StorageGRID sich nicht mehr beim Zieldienst authentifizieren kann.

Suchen Sie nach zugehörigen Warnungen.

Geringere Leistung bei Plattformdienstanfragen

Die StorageGRID Software drosselt möglicherweise eingehende S3-Anfragen für einen Bucket, wenn die Rate, mit der die Anfragen gesendet werden, die Rate überschreitet, mit der der Zielendpunkt die Anfragen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand an Anfragen besteht, die darauf warten, an den Zielendpunkt gesendet zu werden.

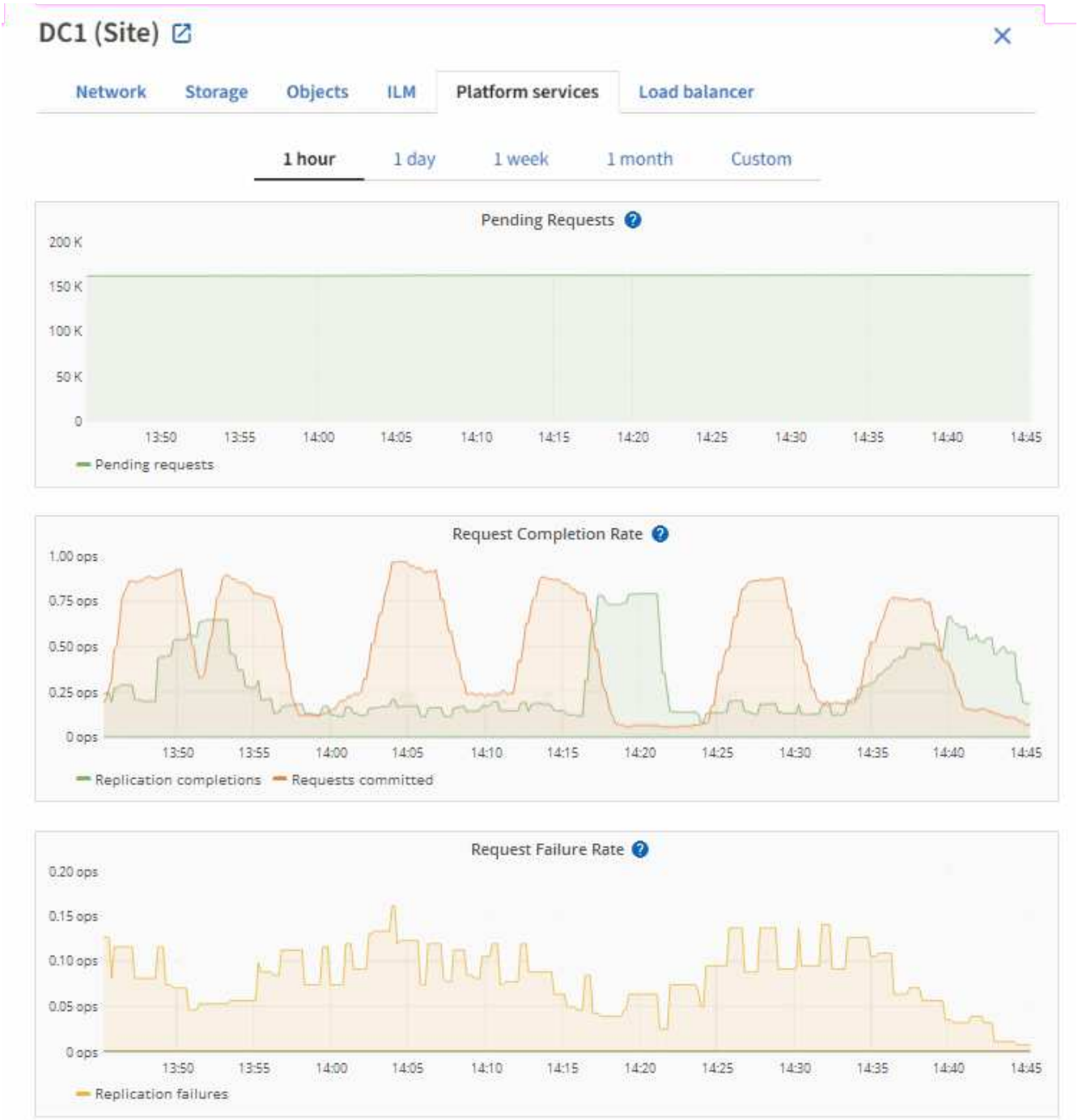
Der einzige sichtbare Effekt besteht darin, dass die Ausführung eingehender S3-Anfragen länger dauert. Wenn Sie eine deutlich langsamere Leistung feststellen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Wenn der Rückstand an Anfragen weiter wächst, schlagen Client-S3-Operationen (wie etwa PUT-Anfragen) letztendlich fehl.

Bei CloudMirror-Anfragen ist die Leistung des Zielendpunkts wahrscheinlicher beeinträchtigt, da diese Anfragen in der Regel mehr Datenübertragungen beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Plattformdienstanforderungen schlagen fehl

So zeigen Sie die Anforderungsfehlerrate für Plattformdienste an:

1. Wählen Sie **NODES**.
2. Wählen Sie ***site*** > **Plattformdienste**.
3. Sehen Sie sich das Diagramm zur Anforderungsfehlerrate an.



Warnung: Nicht verfügbare Plattformdienste

Die Warnung **Plattformdienste nicht verfügbar** weist darauf hin, dass an einem Standort keine Plattformdienstvorgänge ausgeführt werden können, da zu wenige Speicherknoten mit dem RSM-Dienst ausgeführt werden oder verfügbar sind.

Der RSM-Dienst stellt sicher, dass Plattformdienstanforderungen an ihre jeweiligen Endpunkte gesendet werden.

Um diese Warnung zu beheben, ermitteln Sie, welche Speicherknoten am Standort den RSM-Dienst enthalten. (Der RSM-Dienst ist auf Speicherknoten vorhanden, die auch den ADC-Dienst enthalten.) Stellen Sie dann sicher, dass die einfache Mehrheit dieser Speicherknoten ausgeführt wird und verfügbar ist.

> Wenn an einem Standort mehr als ein Speicherknoten ausfällt, der den RSM-Dienst enthält, gehen alle ausstehenden Plattformdienstanforderungen für diesen Standort verloren.

Zusätzliche Anleitung zur Fehlerbehebung für Plattformdienst-Endpunkte

Weitere Informationen finden Sie unter**Verwenden Sie ein Mandantenkonto › Beheben Sie Probleme mit Plattformdienst-Endpunkten** .

Ähnliche Informationen

"Fehlerbehebung beim StorageGRID -System"

Verwalten von S3 Select für Mandantenkonten

Sie können bestimmten S3-Mandanten erlauben, S3 Select zu verwenden, um SelectObjectContent-Anfragen für einzelne Objekte auszugeben.

S3 Select bietet eine effiziente Möglichkeit, große Datenmengen zu durchsuchen, ohne dass für die Suche eine Datenbank und zugehörige Ressourcen bereitgestellt werden müssen. Außerdem werden die Kosten und die Latenz beim Abrufen von Daten reduziert.

Was ist S3 Select?

Mit S3 Select können S3-Clients SelectObjectContent-Anfragen verwenden, um nur die benötigten Daten aus einem Objekt zu filtern und abzurufen. Die StorageGRID -Implementierung von S3 Select umfasst eine Teilmenge der Befehle und Funktionen von S3 Select.

Überlegungen und Anforderungen zur Verwendung von S3 Select

Anforderungen an die Netzverwaltung

Der Grid-Administrator muss den Mandanten die S3 Select-Berechtigung erteilen. Wählen Sie **S3 Select zulassen**, wenn"Erstellen eines Mandanten" oder"Bearbeiten eines Mandanten" .

Anforderungen an das Objektformat

Das abzufragende Objekt muss eines der folgenden Formate aufweisen:

- **CSV**. Kann unverändert verwendet oder in GZIP- oder BZIP2-Archive komprimiert werden.
- **Parkett**. Zusätzliche Anforderungen für Parquet-Objekte:
  - S3 Select unterstützt nur spaltenweise Komprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Ganzobjektkomprimierung für Parquet-Objekte.
  - S3 Select unterstützt keine Parquet-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
  - Die maximale unkomprimierte Zeilengruppengröße beträgt 512 MB.
  - Sie müssen die im Schema des Objekts angegebenen Datentypen verwenden.

- Sie können die logischen Typen INTERVAL, JSON, LIST, TIME oder UUID nicht verwenden.

Endpunktanforderungen

Die SelectObjectContent-Anforderung muss an einen"StorageGRID Lastenausgleichsendpunkt" .

Die vom Endpunkt verwendeten Admin- und Gateway-Knoten müssen einer der folgenden sein:

- Ein Dienst-Appliance-Knoten
- Ein VMware-basierter Softwareknoten
- Ein Bare-Metal-Knoten, auf dem ein Kernel mit aktivierter Cgroup v2 ausgeführt wird

Allgemeine Überlegungen

Abfragen können nicht direkt an Speicherknoten gesendet werden.

> SelectObjectContent-Anfragen können die Leistung des Load Balancers für alle S3-Clients und alle Mandanten verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Siehe die"Anweisungen zur Verwendung von S3 Select" .

Zum Ansehen"Grafana-Diagramme" Wählen Sie für S3 Select-Operationen im Zeitverlauf **SUPPORT** > **Tools** > **Metrics** im Grid Manager.