



Verwalten von Mandanten

StorageGRID

NetApp
April 10, 2024

Inhalt

- Verwalten von Mandanten 1
 - Verwalten von Mandanten 1
 - Erstellen eines Mandantenkontos 3
 - Ändern Sie das Passwort für den lokalen Root-Benutzer des Mandanten 9
 - Mandantenkonto bearbeiten 10
 - Mandantenkonto löschen 13
 - Management von Plattform-Services 13
 - Management von S3 Select für Mandantenkonten 22

Verwalten von Mandanten

Verwalten von Mandanten

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3 und Swift-Clients verwenden, um Objekte zu speichern und abzurufen, die Storage-Nutzung zu überwachen und die Aktionen zu managen, die Clients mit Ihrem StorageGRID System durchführen können.

Was sind Mandantenkonten?

Mandantenkonten ermöglichen Client-Applikationen, die die Simple Storage Service (S3) REST-API oder die Swift REST API verwenden, um Objekte auf StorageGRID zu speichern und abzurufen.

Jedes Mandantenkonto unterstützt die Verwendung eines einzelnen Protokolls, das Sie beim Erstellen des Kontos angeben. Zum Speichern und Abrufen von Objekten in einem StorageGRID System mit beiden Protokollen müssen Sie zwei Mandantenkonten erstellen: Eine für S3 Buckets und Objekte, eine für Swift Container und Objekte. Jedes Mandantenkonto hat seine eigene Account-ID, autorisierte Gruppen und Benutzer, Buckets oder Container und Objekte.

Optional können Sie zusätzliche Mandantenkonten erstellen, wenn Sie die auf Ihrem System gespeicherten Objekte durch verschiedene Einheiten trennen möchten. Beispielsweise können Sie in einem der folgenden Anwendungsfälle mehrere Mandantenkonten einrichten:

- **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 mithilfe von S3-Buckets und Bucket-Richtlinien Objekte zwischen den Abteilungen eines Unternehmens trennen. Sie müssen keine Mandantenkonten verwenden. Weitere Informationen finden Sie in den Anweisungen zur Implementierung von S3-Client-Applikationen.

- **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.

Mandantenkonten erstellen und konfigurieren

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

- Zeigt den Namen des Mandantenkontos an.
- Welches Client-Protokoll wird vom Mandantenkonto verwendet (S3 oder Swift).
- Bei S3-Mandantenkonten: Unabhängig davon, ob das Mandantenkonto die Berechtigung hat, Plattform-Services mit S3 Buckets zu verwenden. Wenn Sie Mandantenkonten für die Nutzung von Plattformdiensten zulassen, müssen Sie sicherstellen, dass das Grid für seine Nutzung konfiguriert ist. Siehe „Managing Platform Services“.
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte

oder Petabyte, die für die Mandantenobjekte verfügbar sind. Wenn das Kontingent überschritten wird, kann der Mandant keine neuen Objekte erstellen.



Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.

- Wenn die Identitätsföderation für das StorageGRID-System aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.
- Wenn Single Sign-On (SSO) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.

Nachdem ein Mandantenkonto erstellt wurde, können Sie die folgenden Aufgaben durchführen:

- **Plattformdienste für das Grid verwalten:** Wenn Sie Plattformdienste für Mandantenkonten aktivieren, sollten Sie wissen, wie Plattform-Services-Nachrichten bereitgestellt werden und welche Netzwerkanforderungen die Verwendung von Plattformservices für Ihre StorageGRID-Bereitstellung stellen.
- **Überwachen der Storage-Nutzung eines Mandantenkontos:** Nachdem Mandanten ihre Konten verwenden, können Sie mithilfe von Grid Manager überwachen, wie viel Storage die einzelnen Mandanten verbrauchen.



Die Werte für die Storage-Nutzung eines Mandanten sind möglicherweise nicht mehr aktuell, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

Wenn Sie Quoten für Mieter festgelegt haben, können Sie die Warnung **Tenant Quotenverbrauch hoch** aktivieren, um festzustellen, ob Mieter ihre Quoten verbrauchen. Wenn diese Meldung aktiviert ist, wird diese Meldung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Weitere Informationen finden Sie unter Alerts Referenz in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

- **Client-Vorgänge konfigurieren:** Sie können konfigurieren, wenn einige Arten von Client-Operationen verboten sind.

S3-Mandanten konfigurieren

Nachdem ein S3-Mandantenkonto erstellt wurde, können Mandantenbenutzer auf den Mandanten-Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) und Erstellen lokaler Gruppen und Benutzer
- Verwalten von S3-Zugriffsschlüsseln
- Erstellen und Managen von S3 Buckets
- Monitoring der Storage-Auslastung
- Verwenden von Plattform-Services (falls aktiviert)



Mandantenbenutzer von S3 können mit Mandanten-Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen. Sie müssen jedoch eine S3-Client-Applikation verwenden, um Objekte aufzunehmen und zu managen.

Konfigurieren Sie Swift Mandanten

Nach der Erstellung eines Swift-Mandantenkontos kann der Root-Benutzer des Mandanten auf den Mandanten Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) und Erstellen lokaler Gruppen und Benutzer
- Monitoring der Storage-Auslastung



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.

Verwandte Informationen

[Verwenden Sie ein Mandantenkonto](#)

Erstellen eines Mandantenkontos

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

Wenn Sie ein Mandantenkonto erstellen, geben Sie einen Namen, ein Client-Protokoll und optional ein Storage-Kontingent an. Wenn Single Sign-On (SSO) für StorageGRID aktiviert ist, geben Sie außerdem an, welche föderierte Gruppe Root-Zugriffsberechtigungen hat, um das Mandantenkonto zu konfigurieren. Wenn StorageGRID keine Single-Sign-On verwendet, müssen Sie außerdem angeben, ob das Mandantenkonto seine eigene Identitätsquelle verwendet und das erste Passwort für den lokalen Root-Benutzer des Mandanten konfiguriert.

Der Grid Manager enthält einen Assistenten, der Sie durch die Schritte zum Erstellen eines Mandantenkontos führt. Je nachdem, ob die Schritte variieren [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.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische Zugriffsberechtigungen.
- 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 Admin-Gruppe keine Grid Manager-Berechtigungen zuweisen. Siehe [Anweisungen zum Verwalten von Admin-Gruppen](#).

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen** und geben Sie folgende Informationen für den Mieter ein:
 - a. **Name:** Geben Sie einen Namen für das Mandantenkonto ein. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.

- b. **Beschreibung** (optional): Geben Sie eine Beschreibung ein, mit der Sie den Mieter identifizieren können.
- c. **Client-Typ**: Wählen Sie den Client-Typ von **S3** oder **Swift** aus.
- d. **Speicherkontingent** (optional): Wenn dieser Mieter ein Speicherkontingent haben soll, geben Sie einen numerischen Wert für das Kontingent ein und wählen Sie die richtigen Einheiten (GB, TB oder PB) aus.

Create a tenant

1 Enter details — 2 Select permissions — 3 Define root access

Enter tenant details

Name ?

Description (optional) ?

Client type ?

S3 Swift

Storage quota (optional) ?

GB ▾

Cancel Continue

3. Wählen Sie **Weiter** und konfigurieren Sie den S3- oder Swift-Mandanten.

S3-Mandant

Wählen Sie die entsprechenden Berechtigungen für den Mandanten aus. Einige dieser Berechtigungen haben zusätzliche Anforderungen. Weitere Informationen finden Sie in der Online-Hilfe zu jeder Berechtigung.

- Unterstützung von Plattform-Services
- Eigene Identitätsquelle verwenden (nur bei Nichtverwendung von SSO wählbar)
- S3-Auswahl zulassen (siehe [Management von S3 Select für Mandantenkonten](#))

Swift-Mandant

Wenn der Mieter seine eigene Identitätsquelle verwendet, wählen Sie **eigene Identitätsquelle verwenden** (nur wählbar, wenn SSO nicht verwendet wird).

1. Wählen Sie **Weiter** und definieren Sie den Root-Zugriff für das Mandantenkonto.

Identitätsföderation nicht konfiguriert

1. Geben Sie ein Passwort für den lokalen Root-Benutzer ein.
2. Wählen Sie **Create Tenant**.

SSO aktiviert

Wenn SSO für StorageGRID aktiviert ist, muss der Mandant die für den Grid Manager konfigurierte Identitätsquelle verwenden. Keine lokalen Benutzer können sich anmelden. Sie geben an, welche föderierte Gruppe Root-Zugriffsberechtigungen hat, um das Mandantenkonto zu konfigurieren.

1. Wählen Sie eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root-Zugriffsberechtigung für den Mandanten zu erhalten.



Wenn Sie über ausreichende Berechtigungen verfügen, werden die vorhandenen föderierten Gruppen aus dem Grid Manager aufgelistet, wenn Sie das Feld auswählen. Geben Sie andernfalls den eindeutigen Namen der Gruppe ein.

2. Wählen Sie **Create Tenant**.

SSO ist nicht aktiviert

1. Führen Sie die in der Tabelle beschriebenen Schritte aus, je nachdem, ob der Mandant seine eigenen Gruppen und Benutzer verwaltet oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

Falls der Mandant...	Tun Sie das...
Verwaltung ihrer eigenen Gruppen und Benutzer	<ol style="list-style-type: none">a. Wählen Sie eigene Identitätsquelle verwenden. Hinweis: Wenn dieses Kontrollkästchen aktiviert ist und Sie Identity Federation für Mandantengruppen und Benutzer verwenden möchten, muss der Mandant seine eigene Identitätsquelle konfigurieren. Siehe Anweisungen zur Verwendung von Mandantenkonten.b. Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an, und wählen Sie dann Create Tenant.c. Wählen Sie Anmelden als root, um den Mandanten zu konfigurieren, oder wählen Sie Fertig, um den Mandanten später zu konfigurieren.

Falls der Mandant...	Tun Sie das...
Verwenden Sie die für den Grid Manager konfigurierten Gruppen und Benutzer	<p>a. Führen Sie einen oder beide der folgenden Schritte aus:</p> <ul style="list-style-type: none"> ◦ Wählen Sie eine vorhandene föderierte Gruppe aus dem Grid Manager aus, die über die ursprüngliche Root-Zugriffsberechtigung für den Mandanten verfügen sollte. <p>Hinweis: Wenn Sie über ausreichende Berechtigungen verfügen, werden die vorhandenen föderierten Gruppen aus dem Grid Manager aufgelistet, wenn Sie das Feld auswählen. Geben Sie andernfalls den eindeutigen Namen der Gruppe ein.</p> <ul style="list-style-type: none"> ◦ Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an. <p>b. Wählen Sie Create Tenant.</p>

1. So melden Sie sich jetzt beim Mieter an:

- Wenn Sie über einen eingeschränkten Port auf den Grid Manager zugreifen, wählen Sie in der Mandantentabelle **eingeschränkt** 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
- Wenn Sie am Port 443 auf den Grid Manager zugreifen, aber kein Passwort für den lokalen Root-Benutzer festgelegt haben, wählen Sie in der Tabelle Mandanten des Grid Manager die Option **Anmelden** aus, und geben Sie die Anmeldeinformationen für einen Benutzer in die föderierte Gruppe Root Access ein.
- Wenn Sie auf den Grid Manager auf Port 443 zugreifen und ein Passwort für den lokalen Root-Benutzer festlegen:
 - i. Wählen Sie **Anmelden als root**, um den Mandanten jetzt zu konfigurieren.

Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets oder Containern, Identitätsföderation, Gruppen und Benutzern angezeigt.

Create a tenant ✕

✓ Enter details
✓ Select permissions
✓ Define root access



The tenant Tenant02 was created.

If you're ready to configure the tenant, select **Sign in as root**.

Sign in as root

✓ Signed in

You can now access the Tenant Manager to configure these settings:

- **Buckets** [🔗](#) : Create and manage buckets.
- **Identity federation** [🔗](#) : Configure an external identity source to use federated groups.
- **Groups** [🔗](#) : Manage groups and assign permissions.
- **Users** [🔗](#) : Manage local users and assign users to groups.

Finish

i. 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](#).

ii. Andernfalls wählen Sie **Fertig**, um später auf den Mieter zuzugreifen.

2. So greifen Sie später auf den Mandanten zu:

Sie verwenden...	Führen Sie eine dieser...
Port 443	<ul style="list-style-type: none"> • 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: <pre style="margin-top: 10px;">https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ <i>20-digit-account-id</i> Die eindeutige Account-ID des Mandanten

Sie verwenden...	Führen Sie eine dieser...
Ein eingeschränkter Port	<ul style="list-style-type: none"> • Wählen Sie im Grid Manager die Option MITERS aus, und wählen Sie eingeschränkt. • Geben Sie die URL des Mandanten in einen Webbrowser ein: <code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</code> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ <i>port</i> Ist der ausschließlich auf Mandanten beschränkte Port ◦ <i>20-digit-account-id</i> Die eindeutige Account-ID des Mandanten

Verwandte Informationen

- [Kontrolle des Zugriffs durch Firewalls](#)
- [Management von Plattform-Services für S3-Mandantenkonten](#)

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.

Was Sie benötigen

- 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 Mandantenkonto 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**.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;">10%</div>	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;">85%</div>	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;">50%</div>	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;">95%</div>	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

Die Schaltfläche Aktionen wird aktiviert.

3. Wählen Sie im Dropdown-Menü **Aktionen** die Option **Root-Passwort ändern** aus.

4. Geben Sie das neue Kennwort für das Mandantenkonto ein.

5. Wählen Sie **Speichern**.

Mandantenkonto bearbeiten

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen zu ändern, die Einstellung für die Identitätsquelle zu ändern, Plattformservices zu ermöglichen oder zu verlassen oder ein Speicherkontingent einzugeben.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **MIETER**.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Buttons: [Create](#) [Export to CSV](#) [Actions](#) Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;"></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;"></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;"></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;"></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

Verwenden Sie das Suchfeld, um nach einem Mandantenkonto nach Name oder Mandanten-ID zu suchen.

3. Wählen Sie aus der Dropdown-Liste Aktionen die Option **Bearbeiten** aus.

Dieses Beispiel gilt für ein Raster, in dem keine SSO (Single Sign On) verwendet wird. Dieses Mandantenkonto hat keine eigene Identitätsquelle konfiguriert.

Edit the tenant

1 Enter details

✓ Select permissions

Enter tenant details

Name ?

Description (optional) ?

Description

Client type ?

S3
 Swift

Storage quota (optional) ?

GB ▼

Cancel

Continue

4. Ändern Sie die Werte für diese Felder nach Bedarf:

- **Name**
- **Beschreibung**
- **Client-Typ**
- **Speicherquote**

5. Wählen Sie **Weiter**.

6. Wählen Sie die Berechtigungen für das Mandantenkonto aus, oder heben Sie die Auswahl auf.

- 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.
- Ändern Sie das Kontrollkästchen **nutzt eigene Identitätsquelle**, um zu bestimmen, ob das Mandantenkonto eine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

Wenn das Kontrollkästchen * eigene Identitätsquelle verwendet*:

- Deaktiviert und überprüft, 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 deaktiviert ist, ist SSO für das StorageGRID System aktiviert. Der Mandant muss die Identitätsquelle verwenden, die für den Grid Manager konfiguriert wurde.
- Aktiviert oder deaktiviert **S3 Select** nach Bedarf. Siehe [Management von S3 Select für Mandantenkonten](#).

7. Wählen Sie **Speichern**.

Verwandte Informationen

- [Management von Plattform-Services für S3-Mandantenkonten](#)
- [Verwenden Sie ein Mandantenkonto](#)

Mandantenkonto löschen

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen alle Buckets (S3), Container (Swift) und Objekte, die mit dem Mandantenkonto verknüpft sind, entfernt haben.

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie das Mandantenkonto aus, das gelöscht werden soll.

Verwenden Sie das Suchfeld, um nach einem Mandantenkonto nach Name oder Mandanten-ID zu suchen.

3. Wählen Sie im Dropdown-Menü **Aktionen** die Option **Löschen** aus.
4. Wählen Sie **OK**.

Management von Plattform-Services

Management von Plattform-Services für S3-Mandantenkonten

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 wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

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

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-Objektsperre metadaten (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.
- Anfragen, die nicht abgeschlossen werden können, werden auf maximal 500,000 Anforderungen in die Warteschlange gestellt. Dieses Limit wird gleich von aktiven Mandanten gemeinsam genutzt. Neue Mieter

dürfen diese Grenze von 500,000 vorübergehend überschreiten, so dass neu erstellte Mieter nicht ungerecht bestraft werden.

Verwandte Informationen

- [Verwenden Sie ein Mandantenkonto](#)
- [Konfigurieren Sie Speicher-Proxy-Einstellungen](#)
- [Monitoring und Fehlerbehebung](#)

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 SNS-Meldungen (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

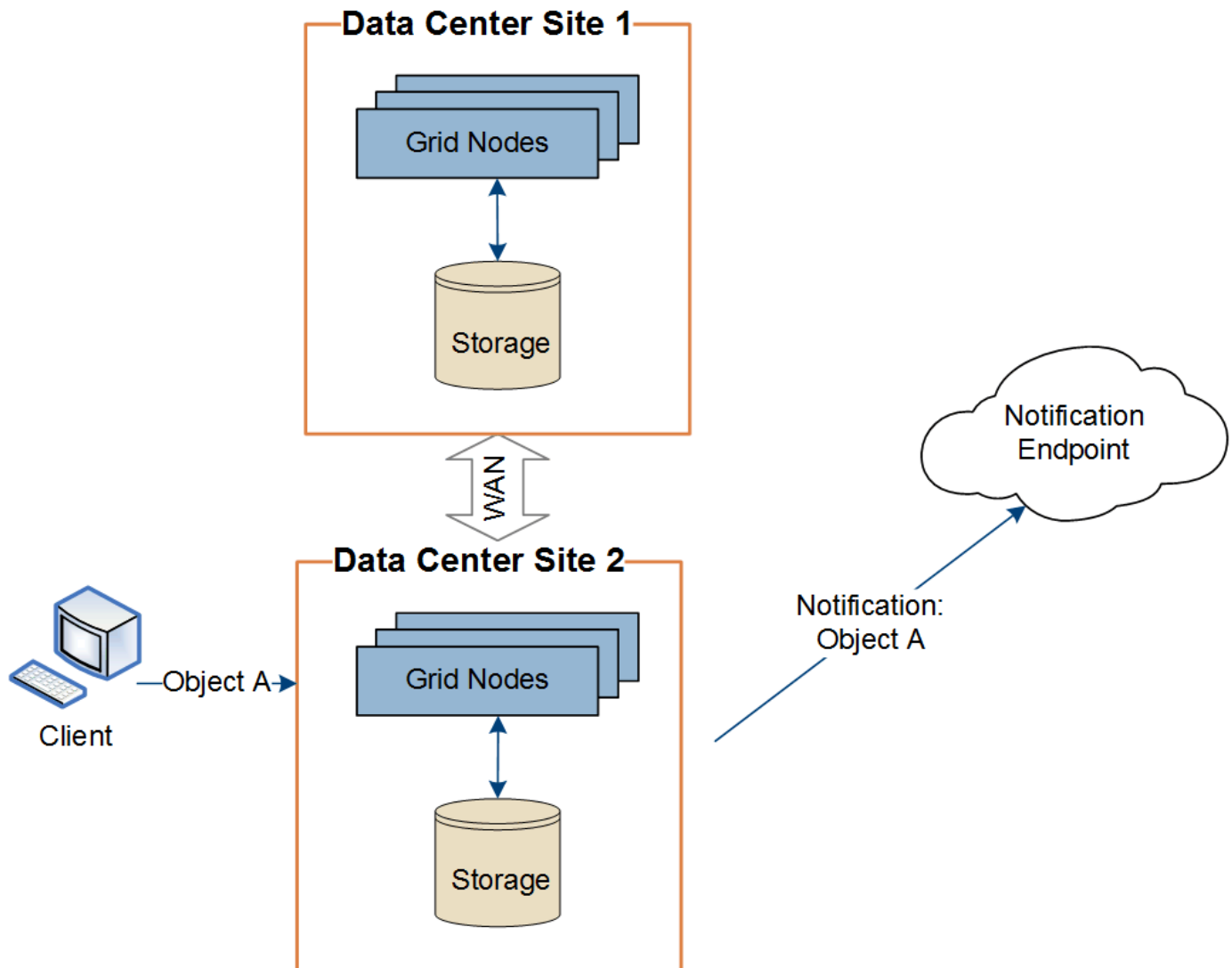
- [Verwenden Sie ein Mandantenkonto](#)

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 Endgeräten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

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



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

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.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

✖ One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ? ↕	Last error ? ↕	Type ? ↕	URI ? ↕	URN ? ↕
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3	✖ 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
<input type="checkbox"/>	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



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 Speicher-Proxy zwischen Speicherknoten und Plattform-Service-Endpunkten konfiguriert haben, treten möglicherweise Fehler auf, wenn Ihr Proxydienst keine Meldungen von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass die Nachrichten für den Plattfordienst nicht blockiert sind.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Endpoint-Fehler aufgetreten sind, wird im Dashboard im Tenant Manager eine Warnmeldung angezeigt. 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.

Behebbar 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.

Plattform-Services-Meldungen 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 von Plattform-Services aufgrund eines nicht behebbaren Fehlers nicht zugestellt werden können, wird der alte 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.

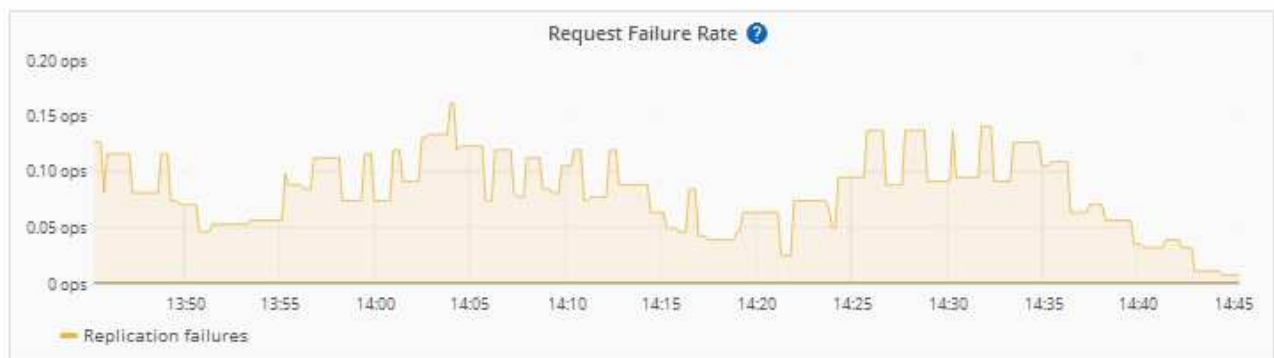
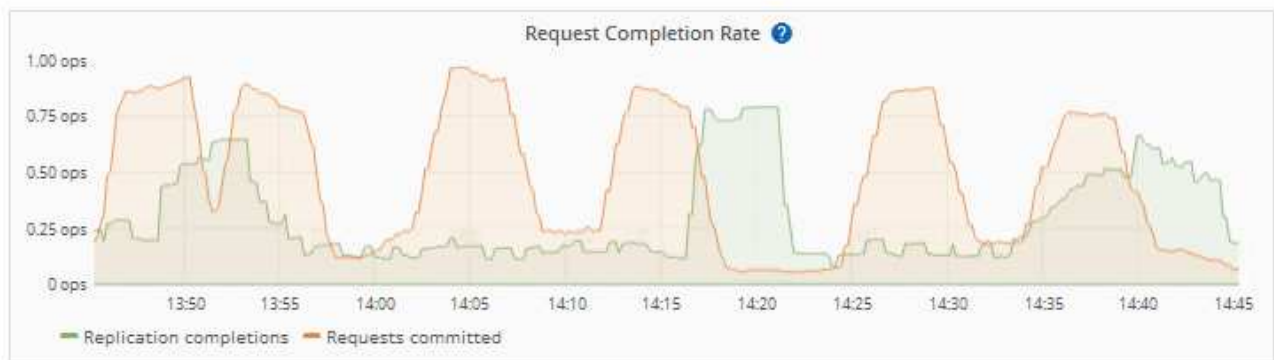
Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahme rate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin 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 Speicherknotten 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 Speicherknotten am Standort den RSM-Service enthalten. (Der RSM-Service ist auf Speicherknotten vorhanden, die auch den ADC-Service enthalten.) Stellen Sie anschließend sicher, dass ein einfacher Großteil dieser Speicherknotten 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 über die Problembehandlung von Endpunkten für Plattfordienste finden Sie in den Anweisungen für [Verwenden eines Mandantenkontos](#).

Verwandte Informationen

- [Monitoring und Fehlerbehebung](#)
- [Konfigurieren Sie Speicher-Proxy-Einstellungen](#)

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

StorageGRID erfordert für S3 Select-Abfragen Folgendes:

- Das Objekt, das Sie abfragen möchten, ist im CSV-Format oder eine komprimierte Datei mit GZIP oder BZIP2, die eine Datei im CSV-Format enthält.
- Mandanten müssen vom Grid-Administrator die S3-Select-Fähigkeit erhalten. Wählen Sie **S3-Auswahl zulassen** aus, wann [Erstellen eines Mandanten](#) Oder [Bearbeiten eines Mandanten](#).
- Die SelectObjectContent-Anforderung muss an ein gesendet werden [Endpunkt des StorageGRID-Load-Balancer](#). Die vom Endpunkt verwendeten Admin- und Gateway-Nodes müssen SG100- oder SG1000-Appliance-Nodes oder VMware-basierte Software-Nodes sein.

Beachten Sie die folgenden Einschränkungen:

- Bare-Metal-Load-Balancer-Nodes werden nicht unterstützt.
- Abfragen können nicht direkt an Speicherknoten gesendet werden.
- Abfragen, die über den veralteten CLB-Dienst gesendet wurden, werden nicht unterstützt.



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 im Zeitdauer aus, wählen Sie im Grid Manager * SUPPORT* **Tools Metrics** aus.

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.