Management von Mandanten

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

Management 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 Mandantenkonten sind

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.

Erstellen und Konfigurieren von Mandantenkonten

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.

  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.

Konfigurieren von S3-Mandanten

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.

Konfiguration von 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 Root-Zugriffsberechtigung ermöglicht 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.

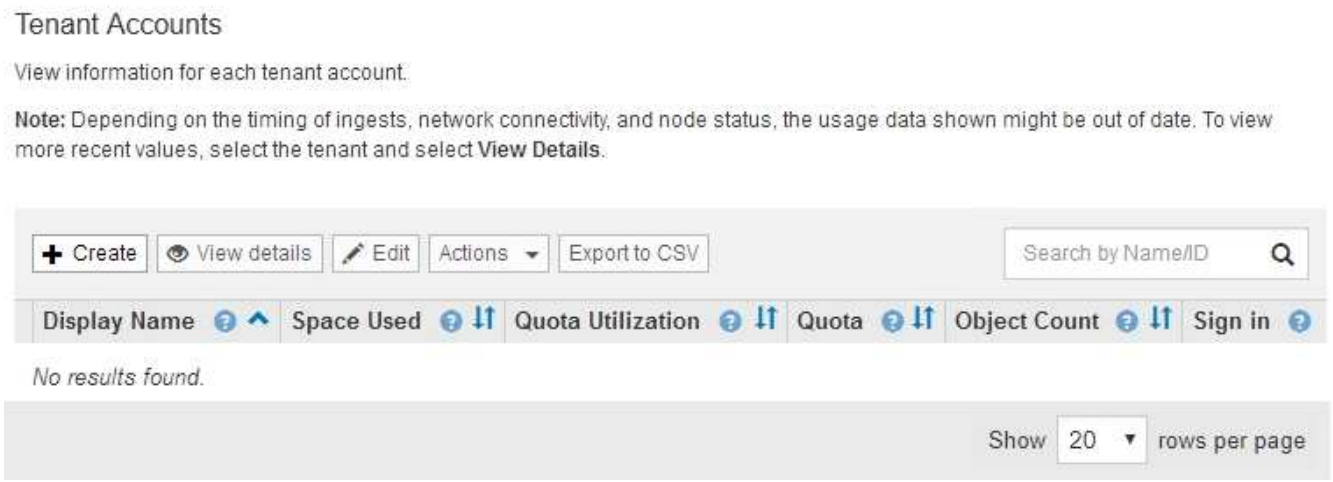
Was Sie benötigen

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

Schritte

1. Wählen Sie **Mieter**.

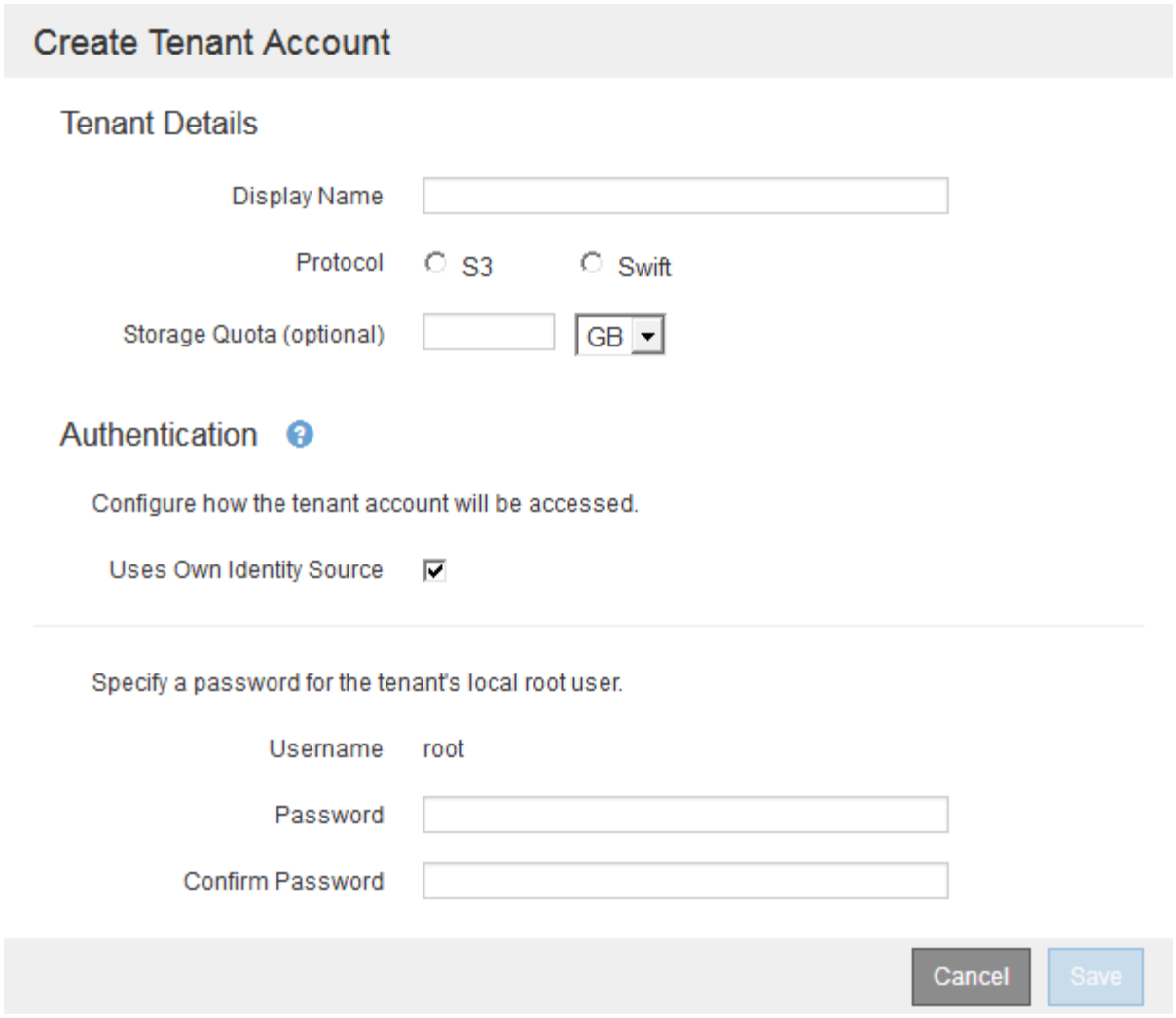
   Die Seite „Mandantenkonten“ wird angezeigt und enthält alle vorhandenen Mandantenkonten.



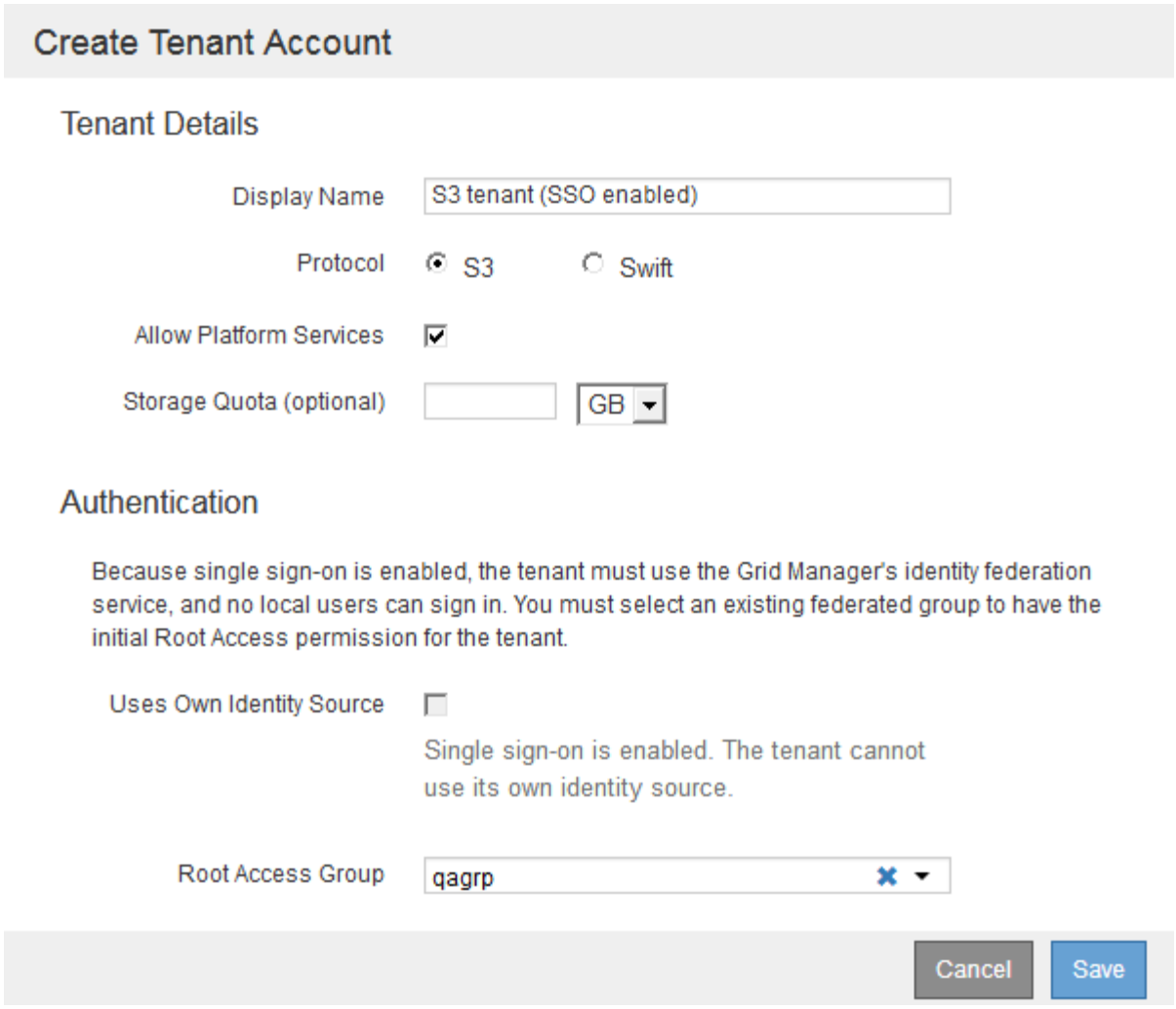
2. Wählen Sie **Erstellen**.

   Die Seite Mandantenkonto erstellen wird angezeigt. Die auf der Seite enthaltenen Felder hängen davon ab, ob Single Sign-On (SSO) für das StorageGRID-System aktiviert wurde.

   - Wenn SSO nicht verwendet wird, sieht die Seite Mandantenkonto erstellen so aus.



- Wenn SSO aktiviert ist, sieht die Seite Mandantenkonto erstellen so aus.



Verwandte Informationen

"Identitätsföderation verwenden"

"Konfigurieren der Single Sign-On-Konfiguration"

Erstellen eines Mandantenkontos, wenn StorageGRID kein SSO verwendet

Wenn Sie ein Mandantenkonto erstellen, geben Sie einen Namen, ein Client-Protokoll und optional ein Storage-Kontingent an. Wenn StorageGRID keine Single Sign On (SSO) verwendet, müssen Sie außerdem angeben, ob das Mandantenkonto seine eigene Identitätsquelle verwendet und das ursprüngliche Passwort für den lokalen Root-Benutzer des Mandanten konfiguriert.

Über diese Aufgabe

Wenn das Mandantenkonto die Identitätsquelle verwendet, die für den Grid Manager konfiguriert wurde, und Sie eine föderierte Gruppe mit Root Access-Berechtigungen für das Mandantenkonto gewähren möchten, müssen Sie diese föderierte Gruppe in den Grid Manager importiert haben. Sie müssen dieser Admin-Gruppe keine Grid Manager-Berechtigungen zuweisen. Siehe Anweisungen für "Verwalten von Admin-Gruppen".

Schritte

1. Geben Sie im Textfeld **Anzeigename** einen Anzeigenamen für dieses Mandantenkonto ein.

Anzeigenamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.

2. Wählen Sie das Client-Protokoll aus, das von diesem Mandantenkonto verwendet wird, entweder **S3** oder **Swift**.
3. Aktivieren Sie für S3-Mandantenkonten das Kontrollkästchen **Platform Services zulassen**, es sei denn, dass dieser Mandant Plattformdienste für S3-Buckets verwendet.

   Wenn Plattformservices aktiviert sind, kann ein Mandant Funktionen wie CloudMirror Replizierung verwenden, die auf externe Services zugreifen. Vielleicht möchten Sie die Verwendung dieser Funktionen deaktivieren, um die Netzwerkbandbreite oder andere Ressourcen einzuschränken, die von einem Mandanten verbraucht werden. Siehe „`MAnaging Platform Services`“.

4. Geben Sie im Textfeld **Speicherkontingent** optional die maximale Anzahl von Gigabyte, Terabyte oder Petabytes ein, die Sie für die Objekte dieses Mandanten bereitstellen möchten. Wählen Sie dann die Einheiten aus der Dropdown-Liste aus.

   Lassen Sie dieses Feld leer, wenn dieser Mieter eine unbegrenzte Quote haben soll.

   > Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar. ILM-Kopien und Erasure Coding tragen nicht zum Umfang des verwendeten Kontingents bei. Wenn das Kontingent überschritten wird, kann das Mandantenkonto keine neuen Objekte erstellen.

   > Um die Storage-Nutzung jedes Mandantenkontos zu überwachen, wählen Sie **Nutzung**. Mandantenkonten können auch ihre eigene Storage-Auslastung von der Konsole im Mandantenmanager oder mit der Mandantenmanagement-API überwachen. Beachten Sie, dass die Storage-Nutzungswerte eines Mandanten möglicherweise nicht mehr aktuell sind, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

5. Wenn der Mandant seine eigenen Gruppen und Benutzer verwaltet, führen Sie diese Schritte aus.
   a. Aktivieren Sie das Kontrollkästchen * verwendet eigene Identitätsquelle* (Standard).

      > Wenn dieses Kontrollkästchen aktiviert ist und Sie einen Identitätsverbund für Mandanten und Benutzer verwenden möchten, muss der Mandant seine eigene Identitätsquelle konfigurieren. Siehe die Anweisungen zur Verwendung von Mandantenkonten.

   b. Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an.
6. Wenn der Mandant die für den Grid Manager konfigurierten Gruppen und Benutzer verwendet, führen Sie die folgenden Schritte aus.
   a. Deaktivieren Sie das Kontrollkästchen * verwendet eigene Identitätsquelle*.
   b. Führen Sie einen oder beide der folgenden Schritte aus:
      - Wählen Sie im Feld Root Access Group eine vorhandene föderierte Gruppe aus dem Grid Manager aus, die über die ursprüngliche Root Access-Berechtigung für den Mandanten verfügen soll.

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

- Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an.

7. Klicken Sie Auf **Speichern**.

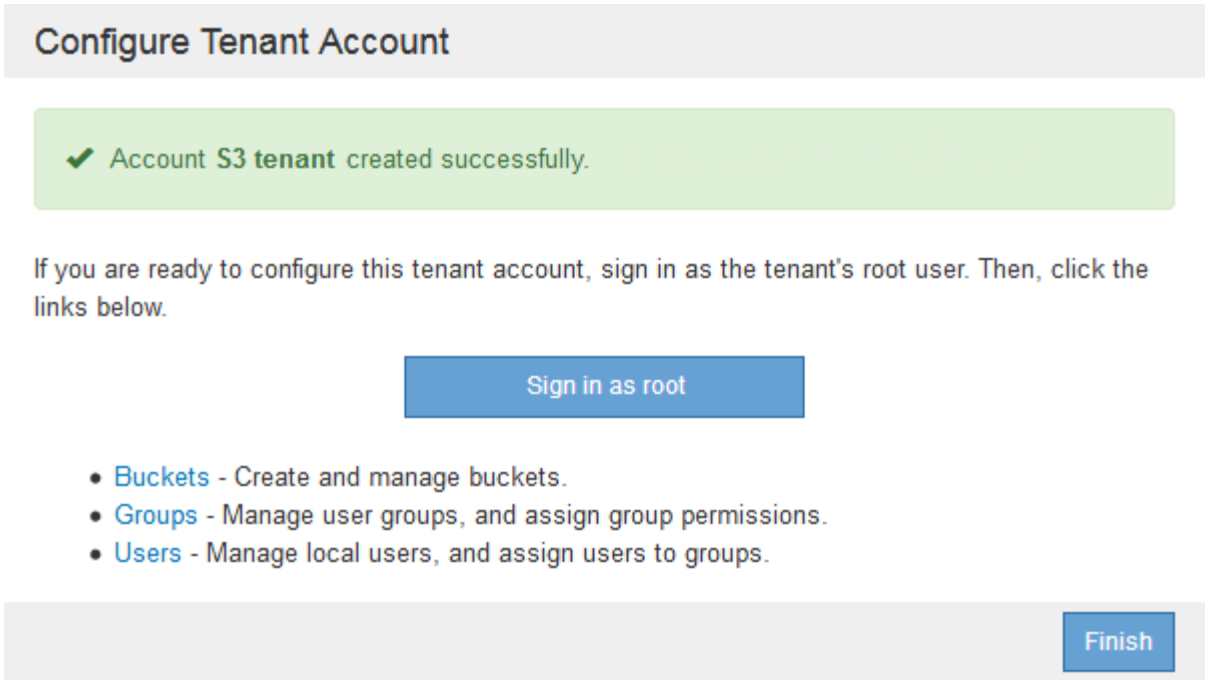
   Das Mandantenkonto wird erstellt.

8. Optional können Sie auf den neuen Mandanten zugreifen. Andernfalls fahren Sie mit dem Schritt für fort Später Zugriff auf den Mandanten.

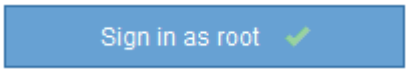
Ihr Unternehmen	Tun Sie das…
Zugriff auf den Grid Manager über einen eingeschränkten Port	Klicken Sie auf **eingeschränkt**, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren. Die URL für den Tenant Manager weist folgendes Format auf: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *`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
Zugriff auf den Grid Manager auf Port 443, Sie haben jedoch kein Passwort für den lokalen Root-Benutzer festgelegt	Klicken Sie auf **Anmelden**, und geben Sie die Anmeldeinformationen für einen Benutzer in die Gruppe Stammzugriff ein.
Zugriff auf den Grid Manager auf Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	Fahren Sie mit dem nächsten Schritt fort melden Sie sich als Root an.

9. Melden Sie sich als Root beim Mandanten an:

   a. Klicken Sie im Dialogfeld Mandantenkonto konfigurieren auf die Schaltfläche **als root** anmelden.



Auf der Schaltfläche wird ein grünes Häkchen angezeigt, das angibt, dass Sie jetzt als Root-Benutzer beim Mandantenkonto angemeldet sind.



a. Klicken Sie auf die Links, um das Mandantenkonto zu konfigurieren.

   Jeder Link öffnet die entsprechende Seite im Tenant Manager. Zum Ausfüllen der Seite lesen Sie die Anweisungen zur Verwendung von Mandantenkonten.

b. Klicken Sie Auf **Fertig Stellen**.

10. um später auf den Mandanten zuzugreifen:

Sie verwenden…	Führen Sie eine dieser…
Port 443	• Wählen Sie im Grid Manager **Mieters** aus und klicken Sie rechts neben dem Mieternamen auf **Anmelden**. • 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

Sie verwenden…	Führen Sie eine dieser…
Ein eingeschränkter Port	• Wählen Sie im Grid Manager die Option **Miters** aus, und klicken Sie auf **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

Verwandte Informationen

"Zugriffskontrolle durch Firewalls"

"Management von Plattform-Services für S3-Mandantenkonten"

"Verwenden Sie ein Mandantenkonto"

Erstellen eines Mandantenkontos, wenn SSO aktiviert ist

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.

Schritte

1. Geben Sie im Textfeld **Anzeigename** einen Anzeigenamen für dieses Mandantenkonto ein.

   Anzeigenamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.

2. Wählen Sie das Client-Protokoll aus, das von diesem Mandantenkonto verwendet wird, entweder **S3** oder **Swift**.
3. Aktivieren Sie für S3-Mandantenkonten das Kontrollkästchen **Platform Services zulassen**, es sei denn, dass dieser Mandant Plattformdienste für S3-Buckets verwendet.

   Wenn Plattformservices aktiviert sind, kann ein Mandant Funktionen wie CloudMirror Replizierung verwenden, die auf externe Services zugreifen. Vielleicht möchten Sie die Verwendung dieser Funktionen deaktivieren, um die Netzwerkbandbreite oder andere Ressourcen einzuschränken, die von einem Mandanten verbraucht werden. Siehe „`MAnaging Platform Services`“.

4. Geben Sie im Textfeld **Speicherkontingent** optional die maximale Anzahl von Gigabyte, Terabyte oder Petabytes ein, die Sie für die Objekte dieses Mandanten bereitstellen möchten. Wählen Sie dann die Einheiten aus der Dropdown-Liste aus.

   Lassen Sie dieses Feld leer, wenn dieser Mieter eine unbegrenzte Quote haben soll.

Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar. ILM-Kopien und Erasure Coding tragen nicht zum Umfang des verwendeten Kontingents bei. Wenn das Kontingent überschritten wird, kann das Mandantenkonto keine neuen Objekte erstellen.

Um die Storage-Nutzung jedes Mandantenkontos zu überwachen, wählen Sie **Nutzung**. Mandantenkonten können auch ihre eigene Storage-Auslastung von der Konsole im Mandantenmanager oder mit der Mandantenmanagement-API überwachen. Beachten Sie, dass die Storage-Nutzungswerte eines Mandanten möglicherweise nicht mehr aktuell sind, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

5. Beachten Sie, dass das Kontrollkästchen * verwendet eigene Identitätsquelle* deaktiviert ist.

   Da SSO aktiviert ist, muss der Mandant die für den Grid Manager konfigurierte Identitätsquelle verwenden. Keine lokalen Benutzer können sich anmelden.

6. Wählen Sie im Feld **Root Access Group** eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root Access-Berechtigung für den Mandanten zu erhalten.

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

7. Klicken Sie Auf **Speichern**.

   Das Mandantenkonto wird erstellt. Die Seite Mandantenkonten wird angezeigt, und es enthält eine Zeile für den neuen Mandanten.

8. Wenn Sie ein Benutzer in der Root Access-Gruppe sind, klicken Sie optional auf den Link **Anmelden**, damit der neue Mandant sofort auf den Tenant Manager zugreift, wo Sie den Mandanten konfigurieren können. Geben Sie andernfalls die URL für den Link **Anmelden** an den Administrator des Mandantenkontos. (Die URL für einen Mandanten ist der vollständig qualifizierte Domain-Name oder die IP-Adresse eines Admin-Knotens, gefolgt von `/?accountId=`*`20-digit-account-id`*.)

   Wenn Sie auf **Anmelden** klicken, jedoch nicht zur Root Access-Gruppe für das Mandantenkonto gehören, wird eine Meldung angezeigt, die Zugriff verweigert.

Verwandte Informationen

"Konfigurieren der Single Sign-On-Konfiguration"

"Management von Plattform-Services für S3-Mandantenkonten"

"Verwenden Sie ein Mandantenkonto"

Ändern des Kennworts für den lokalen Root-Benutzer eines 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 müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

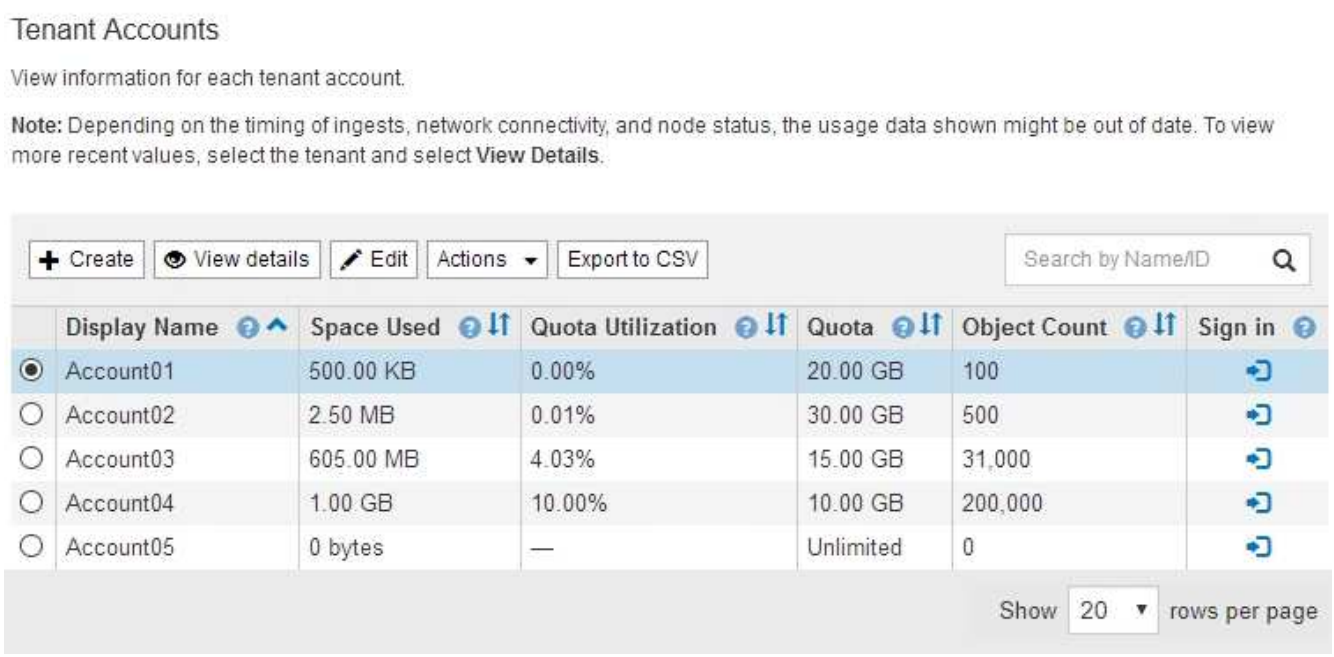
Über diese Aufgabe

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**.

   Die Seite „Mandantenkonten“ wird angezeigt und enthält alle vorhandenen Mandantenkonten.

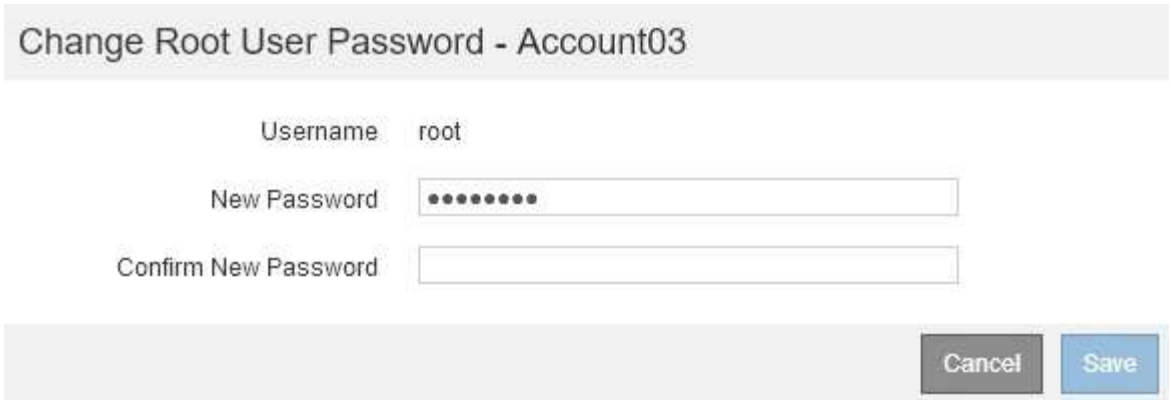


2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

   Die Schaltflächen „Details anzeigen“, „Bearbeiten“ und „Aktionen“ werden 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**.

Verwandte Informationen

"Kontrolle des Administratorzugriffs auf StorageGRID"

Bearbeiten eines Mandantenkontos

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.

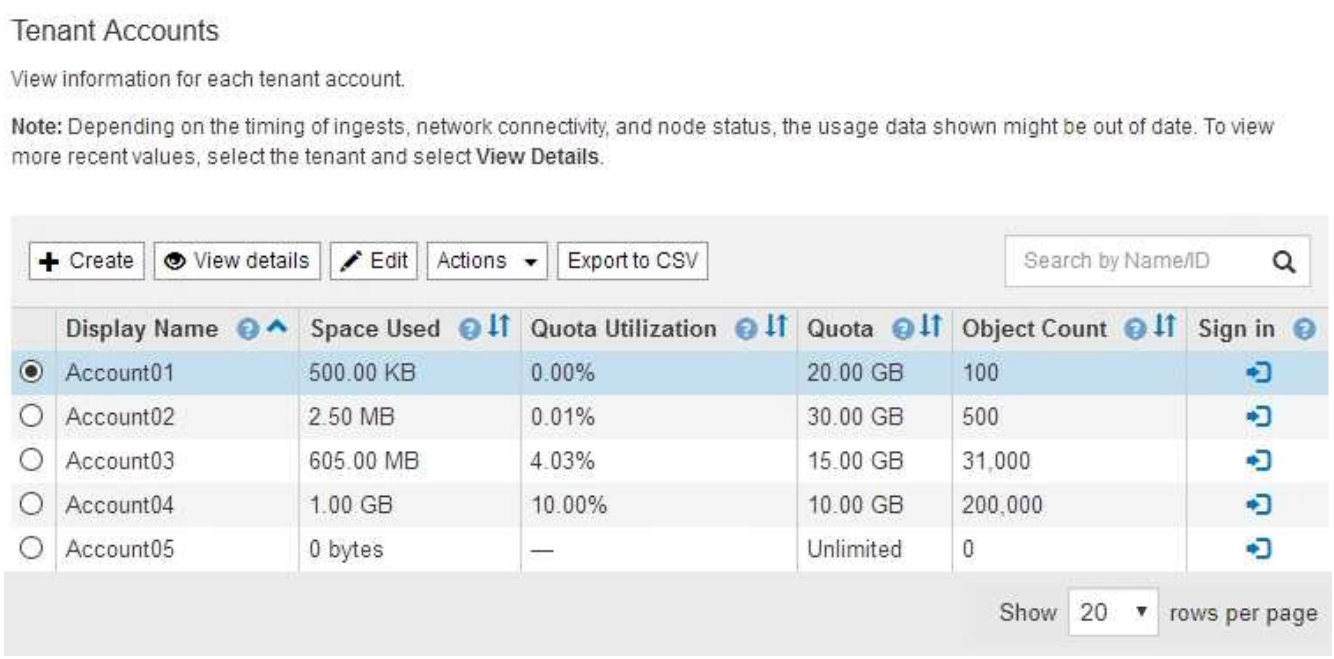
Was Sie benötigen

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

Schritte

1. Wählen Sie **Mieter**.

   Die Seite „Mandantenkonten“ wird angezeigt und enthält alle vorhandenen Mandantenkonten.

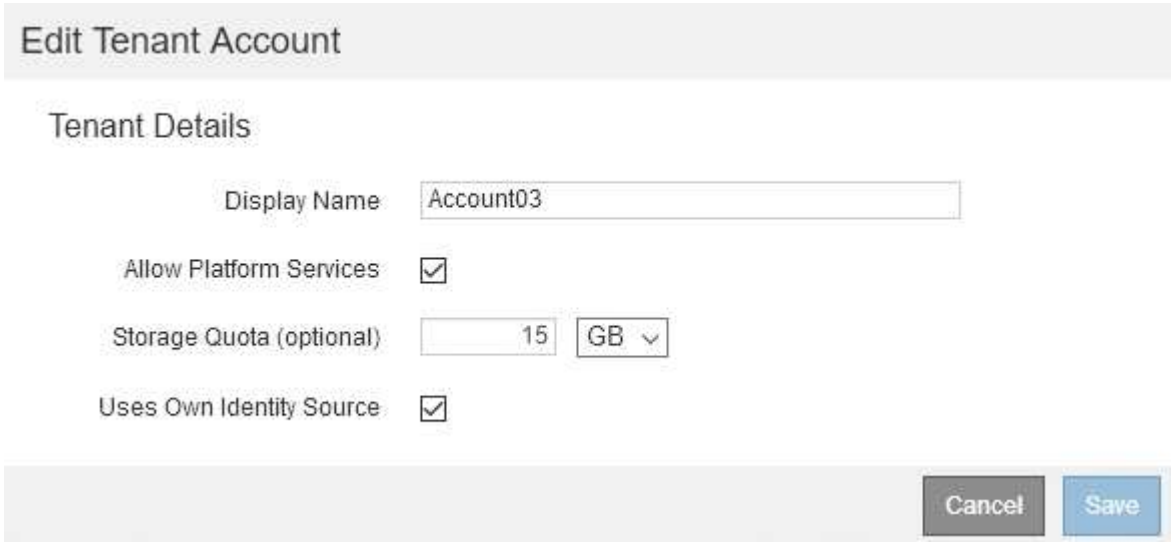


2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

3. Wählen Sie **Bearbeiten**.

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



4. Ändern Sie die Werte für die Felder nach Bedarf.
   a. Ändern Sie den Anzeigenamen für dieses Mandantenkonto.
   b. Ändern Sie die Einstellung des Kontrollkästchen **Plattformdienste zulassen**, um festzustellen, ob das Mandantenkonto Plattformdienste für ihre S3-Buckets verwenden kann.

Wenn Sie Plattform-Services für einen Mandanten deaktivieren, der sie bereits nutzt, funktionieren die Services, die er für seine S3-Buckets konfiguriert hat, nicht mehr. 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.

c. Ändern Sie für **Speicherkontingent** die Anzahl der für die Objekte dieses Mandanten verfügbaren maximalen Gigabytes, Terabyte oder Petabytes, oder lassen Sie das Feld leer, wenn Sie möchten, dass dieser Mieter eine unbegrenzte Quote hat.

   Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar. ILM-Kopien und Erasure Coding tragen nicht zum Umfang des verwendeten Kontingents bei.

   Um die Storage-Nutzung jedes Mandantenkontos zu überwachen, wählen Sie **Nutzung**. Mandantenkonten können auch ihre eigene Nutzung von der Konsole im Mandantenmanager oder mit der Mandantenmanagement-API überwachen. Beachten Sie, dass die Storage-Nutzungswerte eines Mandanten möglicherweise nicht mehr aktuell sind, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

d. Ändern Sie die Einstellung des Checkbox **uses own Identity Source**, um festzustellen, ob das Mandantenkonto eine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

   Wenn das Kontrollkästchen * verwendet eigene Identitätsquelle*:

   - 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.

5. Wählen Sie **Speichern**.

Verwandte Informationen

"Management von Plattform-Services für S3-Mandantenkonten"

"Verwenden Sie ein Mandantenkonto"

Löschen eines Mandantenkontos

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

Was Sie benötigen

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

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

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

Verwandte Informationen

"Kontrolle des Administratorzugriffs auf StorageGRID"

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.

- "Um welche Plattform-Services geht es"
- "Networking und Ports für Plattform-Services"
- "Bereitstellung von Plattform-Services am Standort"
- "Plattform-Services zur Fehlerbehebung"

Um welche Plattform-Services geht es

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-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 müssen Sie die folgenden Empfehlungen beachten:

- 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.
- 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.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Konfigurieren von Speicher-Proxy-Einstellungen"

"Monitor Fehlerbehebung"

Networking und Ports für Plattform-Services

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 Storage Proxy-Einstellungen konfigurieren, damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einen Endpunkt im Internet.

Verwandte Informationen

"Konfigurieren von Speicher-Proxy-Einstellungen"

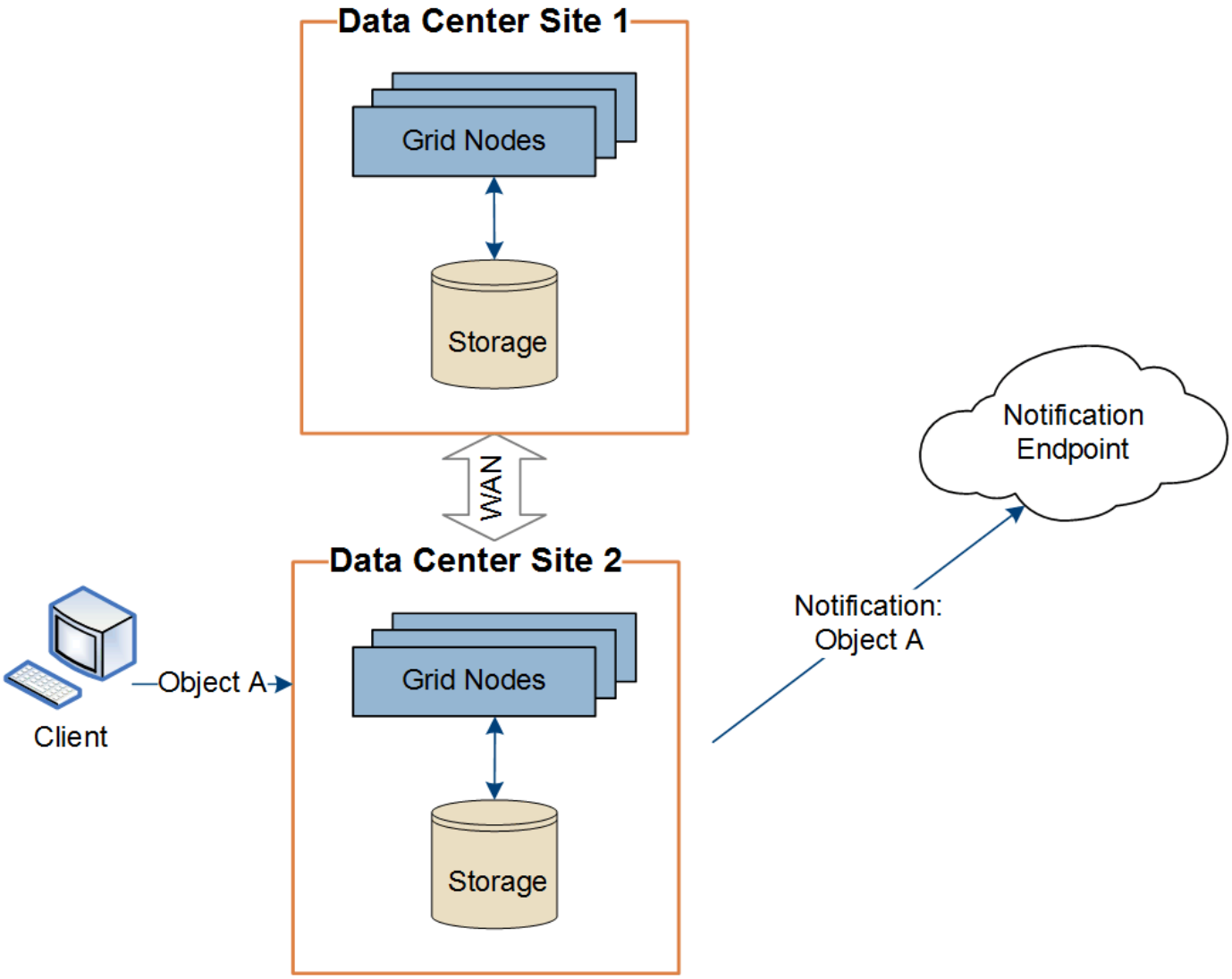
"Verwenden Sie ein Mandantenkonto"

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.

Plattform-Services zur Fehlerbehebung

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

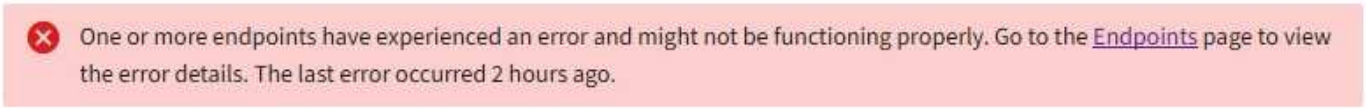
von einem Node an jedem Standort validiert.

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.

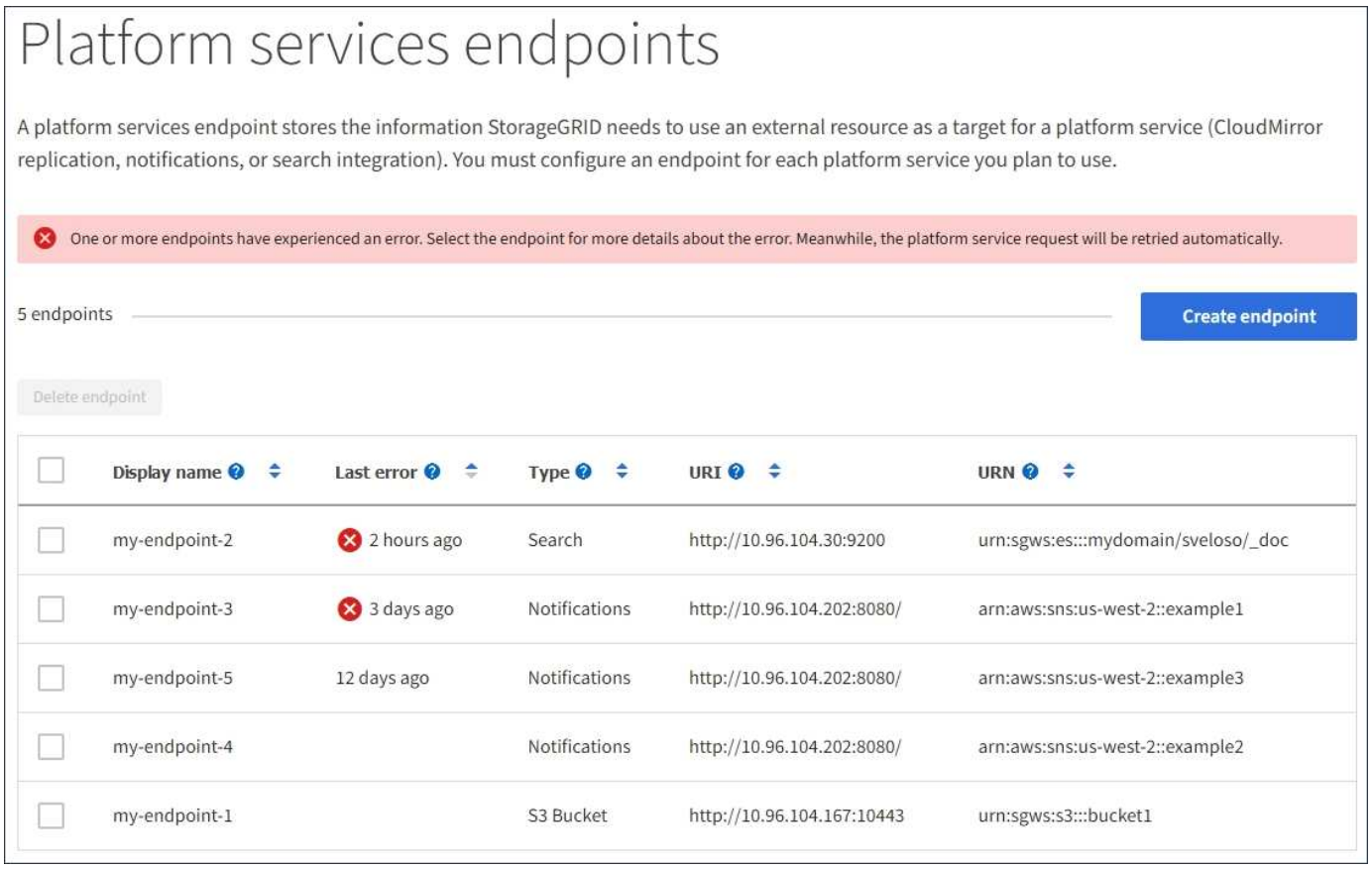
Die Erstellung von Endgeräten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

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.



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 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 Plattformdienst nicht blockiert sind.

Ermitteln, 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 Topology** 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 StorageGRID einen nicht behebbaren Endpunktfehler feststellt, wird der SMTT-Alarm (Total Events) im Grid Manager ausgelöst. So zeigen Sie den Alarm „Ereignisse insgesamt“ an:

1. Wählen Sie **Knoten**.
2. Wählen Sie ***site*** > ***GRID Node*** > **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. Klicken Sie auf **Ereignisanzahl zurücksetzen**.
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 Plattformdienste-Meldungen aufgrund eines nicht behebbaren Fehlers nicht zugestellt werden können, wird der SMTT-Alarm (Total Events) 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. Das Diagramm Fehlerrate anfordern anzeigen.

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 zur Fehlerbehebung bei Endpunkten für Plattformservices finden Sie in den Anweisungen für die Verwendung von Mandantenkonten.

"Verwenden Sie ein Mandantenkonto"

Verwandte Informationen

"Monitor Fehlerbehebung"

"Konfigurieren von Speicher-Proxy-Einstellungen"

Copyright-Informationen

Markeninformationen