Mandantenverwaltungs-API

StorageGRID software

NetApp
October 21, 2025

Inhalt

Mandantenverwaltungs-API

Grundlegendes zur API für die Mandantenverwaltung

Sie können Systemverwaltungsaufgaben mithilfe der Tenant Management REST API anstelle der Tenant Manager-Benutzeroberfläche ausführen. Beispielsweise möchten Sie die API möglicherweise verwenden, um Vorgänge zu automatisieren oder mehrere Entitäten, z. B. Benutzer, schneller zu erstellen.

Die Tenant Management API:

- Verwendet die Open-Source-API-Plattform Swagger. Swagger bietet eine intuitive Benutzeroberfläche, die Entwicklern und Nicht-Entwicklern die Interaktion mit der API ermöglicht. Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.
- Anwendung"Versionierung zur Unterstützung unterbrechungsfreier Upgrades" .

So greifen Sie auf die Swagger-Dokumentation für die Tenant Management API zu:

1. Sign in .
2. Wählen Sie oben im Mandanten-Manager das Hilfesymbol und dann **API-Dokumentation** aus.

API-Operationen

Die Tenant Management API organisiert die verfügbaren API-Operationen in den folgenden Abschnitten:

- **Konto**: Vorgänge auf dem aktuellen Mandantenkonto, einschließlich des Abrufens von Informationen zur Speichernutzung.
- **auth**: Vorgänge zum Durchführen der Benutzersitzungsauthentifizierung.

  Die Tenant Management API unterstützt das Bearer Token Authentication Scheme. Für die Anmeldung als Mandant geben Sie im JSON-Text der Authentifizierungsanfrage einen Benutzernamen, ein Kennwort und eine Konto-ID an (d. h. `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header nachfolgender API-Anfragen bereitgestellt werden („Authorization: Bearer Token“).

  Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter"Schutz vor Cross-Site Request Forgery" .

  > Wenn Single Sign-On (SSO) für das StorageGRID System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte ausführen. Siehe die"Anleitung zur Nutzung der Grid Management API" .

- **config**: Vorgänge im Zusammenhang mit der Produktversion und den Versionen der Tenant Management API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container**: Vorgänge an S3-Buckets oder Swift-Containern.
- **deaktivierte Funktionen**: Vorgänge zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **Endpunkte**: Vorgänge zum Verwalten eines Endpunkts. Endpunkte ermöglichen einem S3-Bucket die

Verwendung eines externen Dienstes für die StorageGRID CloudMirror-Replikation, Benachrichtigungen oder Suchintegration.

- **grid-federation-connections**: Operationen an Grid-Föderationsverbindungen und Cross-Grid-Replikation.
- **Gruppen**: Vorgänge zum Verwalten lokaler Mandantengruppen und zum Abrufen föderierter Mandantengruppen aus einer externen Identitätsquelle.
- **Identitätsquelle**: Vorgänge zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm**: Vorgänge an den Einstellungen des Information Lifecycle Management (ILM).
- **Regionen**: Vorgänge zum Bestimmen, welche Regionen für das StorageGRID -System konfiguriert wurden.
- **s3**: Vorgänge zum Verwalten von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-object-lock**: Vorgänge an globalen S3-Objektsperreinstellungen, die zur Unterstützung der Einhaltung gesetzlicher Vorschriften verwendet werden.
- **Benutzer**: Vorgänge zum Anzeigen und Verwalten von Mandantenbenutzern.

Details zum Vorgang

Wenn Sie die einzelnen API-Vorgänge erweitern, können Sie deren HTTP-Aktion, Endpunkt-URL, eine Liste aller erforderlichen oder optionalen Parameter, ein Beispiel für den Anforderungstext (falls erforderlich) und die möglichen Antworten sehen.

API-Anfragen stellen

> Alle API-Operationen, die Sie über die API-Dokumentationswebseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Sie nicht versehentlich Konfigurationsdaten oder andere Daten erstellen, aktualisieren oder löschen.

Schritte

1. Wählen Sie die HTTP-Aktion aus, um die Anforderungsdetails anzuzeigen.
2. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, beispielsweise eine Gruppen- oder Benutzer-ID. Besorgen Sie sich dann diese Werte. Möglicherweise müssen Sie zuerst eine andere API-Anfrage stellen, um die benötigten Informationen zu erhalten.
3. Stellen Sie fest, ob Sie den Beispielanforderungstext ändern müssen. Wenn ja, können Sie **Modell** auswählen, um die Anforderungen für jedes Feld zu erfahren.
4. Wählen Sie **Ausprobieren**.
5. Geben Sie alle erforderlichen Parameter an oder ändern Sie den Anforderungstext nach Bedarf.
6. Wählen Sie **Ausführen**.
7. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Versionierung der Mandantenverwaltungs-API

Die Tenant Management API verwendet Versionierung, um unterbrechungsfreie Upgrades zu unterstützen.

Diese Anforderungs-URL gibt beispielsweise Version 4 der API an.

`https://hostname_or_ip_address/api/v4/authorize`

Die Hauptversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen *nicht kompatibel* sind. Die Nebenversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen *kompatibel* sind. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften.

Das folgende Beispiel veranschaulicht, wie die API-Version je nach Art der vorgenommenen Änderungen erhöht wird.

Art der Änderung an der API	Alte Version	Neue Version
Kompatibel mit älteren Versionen	2,1	2,2
Nicht kompatibel mit älteren Versionen	2,1	3,0

Wenn Sie die StorageGRID -Software zum ersten Mal installieren, ist nur die neueste Version der API aktiviert. Wenn Sie jedoch auf eine neue Funktionsversion von StorageGRID aktualisieren, haben Sie weiterhin Zugriff auf die ältere API-Version für mindestens eine StorageGRID -Funktionsversion.

> Sie können die unterstützten Versionen konfigurieren. Weitere Informationen finden Sie im Abschnitt **config** der Swagger-API-Dokumentation."Grid-Management-API" für weitere Informationen. Sie sollten die Unterstützung für die ältere Version deaktivieren, nachdem Sie alle API-Clients aktualisiert haben, um die neuere Version zu verwenden.

Veraltete Anfragen werden auf folgende Weise als veraltet gekennzeichnet:

- Der Antwortheader lautet „Deprecated: true“
- Der JSON-Antworttext enthält „deprecated“: true
- Zu nms.log wird eine veraltete Warnung hinzugefügt. Beispiel:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Ermitteln Sie, welche API-Versionen in der aktuellen Version unterstützt werden

Verwenden Sie die `GET /versions` API-Anforderung zum Zurückgeben einer Liste der unterstützten API-Hauptversionen. Diese Anfrage befindet sich im Abschnitt **config** der Swagger-API-Dokumentation.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Angeben einer API-Version für eine Anfrage

Sie können die API-Version mithilfe eines Pfadparameters angeben(`/api/v4`) oder eine Kopfzeile(`Api-Version: 4`). Wenn Sie beide Werte angeben, überschreibt der Header-Wert den Pfadwert.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Schutz vor Cross-Site Request Forgery (CSRF)

Sie können zum Schutz vor Cross-Site Request Forgery (CSRF)-Angriffen auf StorageGRID beitragen, indem Sie CSRF-Token verwenden, um die Authentifizierung mithilfe von Cookies zu verbessern. Der Grid Manager und der Tenant Manager aktivieren diese Sicherheitsfunktion automatisch. Andere API-Clients können bei der Anmeldung auswählen, ob sie diese aktivieren möchten.

Ein Angreifer, der eine Anfrage an eine andere Site auslösen kann (z. B. mit einem HTTP-Formular-POST), kann dafür sorgen, dass bestimmte Anfragen unter Verwendung der Cookies des angemeldeten Benutzers gestellt werden.

StorageGRID schützt durch die Verwendung von CSRF-Token vor CSRF-Angriffen. Wenn diese Option aktiviert ist, muss der Inhalt eines bestimmten Cookies mit dem Inhalt eines bestimmten Headers oder eines bestimmten POST-Body-Parameters übereinstimmen.

Um die Funktion zu aktivieren, legen Sie die `csrfToken` Parameter auf `true` während der Authentifizierung. Die Standardeinstellung ist `false` .

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Wenn dies zutrifft, `GridCsrfToken` Cookie wird mit einem zufälligen Wert für Anmeldungen am Grid Manager gesetzt, und die `AccountCsrfToken` Für die Anmeldung beim Tenant Manager wird ein Cookie mit einem zufälligen Wert gesetzt.

Wenn das Cookie vorhanden ist, müssen alle Anfragen, die den Status des Systems ändern können (POST, PUT, PATCH, DELETE), eines der folgenden Elemente enthalten:

- Der `X-Csrf-Token` Header, wobei der Wert des Headers auf den Wert des CSRF-Token-Cookies gesetzt ist.
- Für Endpunkte, die einen formkodierten Textkörper akzeptieren: A `csrfToken` formcodierter Anforderungstextparameter.

Um den CSRF-Schutz zu konfigurieren, verwenden Sie die"Grid-Management-API" oder"Mandantenverwaltungs-API" .

> Anfragen, für die ein CSRF-Token-Cookie gesetzt ist, erzwingen außerdem den Header „Content-Type: application/json“ für alle Anfragen, die einen JSON-Anforderungstext erwarten, als zusätzlichen Schutz vor CSRF-Angriffen.