



Mandantenverwaltungs-API

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/de-de/storagegrid-120/tenant/understanding-tenant-management-api.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Inhalt

- Mandantenverwaltungs-API 1
 - Erfahren Sie mehr über die StorageGRID Tenant Management API 1
 - API Operationen. 1
 - `${post_edited_translations.segment}`. 2
 - API-Anfragen ausführen. 3
 - StorageGRID Tenant Management API-Versionierung 4
 - `${post_edited_translations.segment}`. 5
 - Eine API-Version für eine Anfrage angeben. 5
 - Schutz vor Cross-Site Request Forgery in StorageGRID 5

Mandantenverwaltungs-API

Erfahren Sie mehr über die StorageGRID Tenant Management API

Sie können Systemmanagement-Aufgaben 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 wie Benutzer schneller zu erstellen.

Die Tenant Management API:

- Verwendet die Swagger Open-Source-API-Plattform. Swagger bietet eine intuitive Benutzeroberfläche, die Entwicklern und Nicht-Entwicklern die Interaktion mit der API ermöglicht. Die Swagger Benutzeroberfläche bietet vollständige Details und Dokumentationen für jede API-Operation.
- Verwendet "[Versionierung zur Unterstützung unterbrechungsfreier Upgrades](#)".

`${post_edited_translations.segment}`

1. Im Tenant Manager anmelden.
2. Oben im Tenant Manager das Hilfesymbol auswählen und anschließend **API documentation** auswählen.

API Operationen

`${post_edited_translations.segment}`

- **Konto:** Operationen am aktuellen Mandantenkonto, einschließlich Abruf von Speichernutzungsinformationen.
- **auth:** Operationen zur Durchführung der Benutzersitzungsauthentifizierung.

Die Tenant Management API unterstützt das Bearer Token Authentifizierungsschema. Für eine Tenant-Anmeldung werden Benutzername, Passwort und accountId im JSON-Body der Authentifizierungsanfrage bereitgestellt (das heißt, `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header nachfolgender API-Anfragen angegeben werden ("Authorization: Bearer token").

Informationen zur Verbesserung der Sicherheit bei der Authentifizierung finden Sie unter "[Schutz vor Cross-Site Request Forgery](#)".



Wenn Single Sign-On (SSO) für das StorageGRID System aktiviert ist, sind andere Schritte zur Authentifizierung erforderlich. Siehe "[Anleitung zur Verwendung der Grid Management API](#)".

- **config:** Operationen im Zusammenhang mit der Produkteinführung und den Versionen der Tenant Management API. Es ist möglich, die Produktversionsnummer und die von dieser Version unterstützten Hauptversionen der API aufzulisten.
- **Container:** Vorgänge an S3-Buckets.
- **deactivated-features:** Vorgänge zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.

- **Endpunkte:** Operationen zur Verwaltung eines Endpunkts. Endpunkte ermöglichen es einem S3-Bucket, einen externen Dienst für StorageGRID CloudMirror Replikation, Benachrichtigungen oder Suchintegration zu verwenden.
- **grid-federation-connections:** Vorgänge an grid-federation-connections und gridübergreifender Replikation.
- **Gruppen:** Operationen zur Verwaltung lokaler Mandantengruppen und zum Abrufen föderierter Mandantengruppen aus einer externen Identitätsquelle.
- `${post_edited_translations.segment}`
- **ilm:** Vorgänge an den Einstellungen für das Information Lifecycle Management (ILM).
- **Regionen:** Operationen zur Ermittlung der Regionen, die für das StorageGRID System konfiguriert wurden.
- **s3:** Operationen zur Verwaltung von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-object-lock:** Vorgänge an globalen S3 Object Lock-Einstellungen, die zur Unterstützung der Einhaltung gesetzlicher Vorschriften verwendet werden.
- **Benutzer:** Vorgänge zum Anzeigen und Verwalten von Mandantenbenutzern.

`${post_edited_translations.segment}`

Beim Erweitern der einzelnen API-Operationen werden die jeweilige HTTP-Aktion, die Endpunkt-URL, eine Liste aller erforderlichen oder optionalen Parameter, ein Beispiel für den Anfragetext (falls erforderlich) und die möglichen Antworten angezeigt.

groups

Operations on groups

GET

/org/groups

Lists Tenant User Groups

Parameters

Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses

Response content type

application/json

Code	Description
200	Example Value Model <pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" }</pre>

of_thought

API-Anfragen ausführen



Alle API-Operationen, die Sie über die API-Dokumentationswebseite durchführen, sind Live-Operationen. Es ist darauf zu achten, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Schritte

1. `${post_edited_translations.segment}`
2. Es ist zu ermitteln, ob die Anforderung zusätzliche Parameter wie eine Gruppen- oder Benutzer-ID erfordert. Anschließend sind diese Werte abzurufen. Möglicherweise muss zuerst eine andere API-Anforderung gesendet werden, um die benötigten Informationen zu erhalten.

3. Es kann geprüft werden, ob der Beispiel-Anfragetext angepasst werden muss. Ist dies der Fall, steht **Model** zur Verfügung, um die Anforderungen für jedes Feld anzuzeigen.
4. **Ausprobieren** auswählen.
5. Alle erforderlichen Parameter können angegeben oder der Anfragetext nach Bedarf angepasst werden.
6. **Ausführen** auswählen.
7. Der Antwortcode gibt Aufschluss darüber, ob die Anfrage erfolgreich war.

StorageGRID Tenant Management API-Versionierung

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

Beispielsweise gibt diese Request-URL die Version 4 der API an.

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

Die Hauptversion der API wird erhöht, wenn Änderungen vorgenommen werden, die nicht mit älteren Versionen kompatibel sind. Die Nebenversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen kompatibel sind. Kompatible Änderungen umfassen 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	<code>\${post_edited_translations.segmen ent}</code>	Neue Version
<code>\${post_edited_translations.segmen tj}</code>	2,1	2,2
Nicht kompatibel mit älteren Versionen	2,1	3,0

Bei der erstmaligen Installation der StorageGRID Software ist nur die neueste Version der API aktiviert. Wenn jedoch ein Upgrade auf eine neue Funktionsversion von StorageGRID erfolgt, bleibt der Zugriff auf die ältere API-Version für mindestens eine StorageGRID Funktionsversion erhalten.



Sie können die unterstützten Versionen konfigurieren. Im Abschnitt **config** der Swagger API-Dokumentation "[Grid Management API](#)" finden sich weitere Informationen. Die Unterstützung für die ältere Version sollte nach der Aktualisierung aller API-Clients auf die neuere Version deaktiviert werden.

Veraltete Anfragen werden auf folgende Weise als veraltet gekennzeichnet:

- Der Antwortheader ist „Deprecated: true“.
- Der JSON-Antworttext enthält "deprecated": true
- Eine Warnung bezüglich veralteter Technologien wird in nms.log hinzugefügt. Zum Beispiel:

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

`${post_edited_translations.segment}`

Die `GET /versions` API-Anfrage gibt eine Liste der unterstützten API-Hauptversionen zurück. 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
  ]
}
```

Eine API-Version für eine Anfrage angeben

Sie können die API-Version mit einem Pfadparameter (`/api/v4`) oder einem Header (`Api-Version: 4`) angeben. Wenn beide Werte angegeben werden, überschreibt der Wert im Header den Wert im Pfad.

```
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 in StorageGRID

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

`${post_edited_translations.segment}`

StorageGRID schützt vor CSRF-Angriffen durch die Verwendung von CSRF-Tokens. 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 den Parameter `csrfToken` während der Authentifizierung auf `true` fest. Der Standardwert 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 dieser Wert auf „true“ festgelegt ist, wird ein `GridCsrfToken`-Cookie mit einem zufälligen Wert für Anmeldungen beim Grid Manager gesetzt, und das `AccountCsrfToken`-Cookie wird mit einem zufälligen Wert für Anmeldungen beim Tenant Manager gesetzt.

`${post_edited_translations.segment}`

- Der `X-Csrf-Token-Header`, wobei der Wert des Headers auf den Wert des `CSRF-Token-Cookies` festgelegt ist.
- Für Endpunkte, die einen formuliarcodierten Body akzeptieren: Ein `csrfToken` formuliarcodierter Anfragekörperparameter.

Um den CSRF-Schutz zu konfigurieren, kann die ["Grid Management API"](#) oder ["Mandantenverwaltungs-API"](#) verwendet werden.



`${post_edited_translations.segment}`

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN 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.