



테넌트 관리 **API** 이해

StorageGRID 11.5

NetApp
April 11, 2024

목차

테넌트 관리 API 이해	1
API 작업	1
작업 세부 정보	2
API 요청을 발급하는 중입니다	3
테넌트 관리 API 버전 관리	4
사이트 간 요청 위조(CSRF)로부터 보호	5

테넌트 관리 API 이해

테넌트 관리자 사용자 인터페이스 대신 테넌트 관리 REST API를 사용하여 시스템 관리 작업을 수행할 수 있습니다. 예를 들어, API를 사용하여 작업을 자동화하거나 사용자와 같은 여러 엔터티를 더 빠르게 생성할 수 있습니다.

테넌트 관리 API는 Swagger 오픈 소스 API 플랫폼을 사용합니다. Swagger는 개발자와 개발자가 아닌 사용자가 API와 상호 작용할 수 있는 직관적인 사용자 인터페이스를 제공합니다. Swagger 사용자 인터페이스는 각 API 작동에 대한 전체 세부 정보와 문서를 제공합니다.

테넌트 관리 API에 대한 Swagger 문서에 액세스하려면 다음을 수행합니다.

단계

1. 테넌트 관리자에 로그인합니다.
2. Tenant Manager 헤더에서 * Help * > * API Documentation * 을 선택합니다.

API 작업

테넌트 관리 API는 사용 가능한 API 작업을 다음 섹션으로 구성합니다.

- * 계정 * — 스토리지 사용 정보를 가져오는 것을 포함하여 현재 테넌트 계정의 작업입니다.
- * auth * — 사용자 세션 인증을 수행하기 위한 작업.

Tenant Management API는 Bearer Token Authentication Scheme을 지원합니다. 테넌트 로그인인 경우 인증 요청의 JSON 본문에 사용자 이름, 암호 및 accountId를 입력합니다(즉, POST /api/v3/authorize)를 클릭합니다. 사용자가 성공적으로 인증되면 보안 토큰이 반환됩니다. 이 토큰은 후속 API 요청 헤더("Authorization: Bearer token")에 제공되어야 합니다.

인증 보안 개선에 대한 자세한 내용은 사이트 간 요청 위조 방지 를 참조하십시오.



StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. StorageGRID 관리 지침은 "SSO(Single Sign-On)가 활성화된 경우 API에 로그인 인증"을 참조하십시오.

- * config * — 제품 릴리스 및 테넌트 관리 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 컨테이너 * — S3 버킷 또는 Swift 컨테이너에서 다음과 같은 작업을 수행합니다.

프로토콜	권한 허용
S3	<ul style="list-style-type: none"> • 준수 및 비준수 버킷 생성 • 레거시 준수 설정 수정 • 객체에 대해 수행된 작업에 대한 정합성 보장 제어 설정 • 버킷의 CORS 구성 생성, 업데이트 및 삭제 • 객체에 대한 마지막 액세스 시간 업데이트를 설정 및 해제합니다 • CloudMirror 복제, 알림 및 검색 통합(메타데이터 알림)을 비롯한 플랫폼 서비스에 대한 구성 설정 관리 • 빈 버킷을 삭제하는 중입니다
스위프트	컨테이너에 사용되는 일관성 수준 설정

- * deactivated - features * — 비활성화된 기능을 보기 위한 작업.
- * 끝점 * — 끝점을 관리하는 작업. 엔드포인트는 S3 버킷이 StorageGRID CloudMirror 복제, 알림 또는 검색 통합에 외부 서비스를 사용할 수 있도록 합니다.
- * 그룹 * — 로컬 테넌트 그룹을 관리하고 외부 ID 소스에서 통합 테넌트 그룹을 검색하는 작업입니다.
- * identity-source * — 외부 ID 소스를 구성하고 통합 그룹 및 사용자 정보를 수동으로 동기화하는 작업.
- * 지역 * — StorageGRID 시스템에 대해 구성된 지역을 결정하는 작업.
- * S3 * — 테넌트 사용자를 위한 S3 액세스 키를 관리하는 운영
- * S3-object-lock * — StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금(규정 준수)을 구성하는 방법을 판별하는 작업
- * 사용자 * — 테넌트 사용자를 보고 관리하는 작업.

작업 세부 정보

각 API 작업을 확장하면 HTTP 동작, 끝점 URL, 필수 또는 선택적 매개 변수 목록, 요청 본문(필요한 경우) 예제 및 가능한 응답을 볼 수 있습니다.

groups Operations on groups

GET /org/groups Lists Tenant User Groups

Parameters Try it out

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

Responses Response content type **application/json** ▾

Code	Description
200	<div style="display: flex; justify-content: space-between;"> Example Value Model </div> <pre> { "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" } </pre>

API 요청을 발급하는 중입니다



API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

단계

1. 요청 세부 정보를 보려면 HTTP 작업을 클릭합니다.
2. 요청에 그룹 또는 사용자 ID와 같은 추가 매개 변수가 필요한지 확인합니다. 그런 다음 이 값을 구합니다. 필요한 정보를 얻기 위해 먼저 다른 API 요청을 발급해야 할 수도 있습니다.
3. 예제 요청 본문을 수정해야 하는지 확인합니다. 이 경우 * Model * 을 클릭하여 각 필드의 요구 사항을 확인할 수 있습니다.

4. 체험하기 * 를 클릭합니다.
5. 필요한 매개 변수를 제공하거나 요청 본문을 필요에 따라 수정합니다.
6. Execute * 를 클릭합니다.
7. 응답 코드를 검토하여 요청이 성공했는지 확인합니다.

관련 정보

["사이트 간 요청 위조\(CSRF\)로부터 보호"](#)

["StorageGRID 관리"](#)

테넌트 관리 API 버전 관리

테넌트 관리 API는 버전 관리를 사용하여 무중단 업그레이드를 지원합니다.

예를 들어 이 요청 URL은 API의 버전 3을 지정합니다.

```
https://hostname_or_ip_address/api/v3/authorize
```

테넌트 관리 API의 주요 버전은 이전 버전과 * 호환되지 않는 _* 변경 사항이 있을 때 충돌합니다. 테넌트 관리 API의 부 버전은 *_이(가) 이전 버전과 호환된다는 변경 사항이 있을 때 충돌합니다. 호환 가능한 변경 사항에는 새 끝점 또는 새 속성 추가가 포함됩니다. 다음 예제에서는 변경 유형에 따라 API 버전을 충돌하는 방법을 보여 줍니다.

API 변경 유형입니다	이전 버전	새 버전
이전 버전과 호환 가능합니다	2.1	2.2
이전 버전과 호환되지 않습니다	2.1	3.0

StorageGRID 소프트웨어를 처음 설치하면 가장 최신 버전의 테넌트 관리 API만 활성화됩니다. 그러나 StorageGRID를 새 기능 릴리즈로 업그레이드하면 하나 이상의 StorageGRID 기능 릴리즈에 대한 이전 API 버전에 계속 액세스할 수 있습니다.

오래된 요청은 다음과 같은 방법으로 더 이상 사용되지 않는 것으로 표시됩니다.

- 응답 헤더가 "DEPRECATED:TRUE"입니다.
- JSON 응답 본문에는 "DEPRECATED"가 포함됩니다. TRUE

현재 릴리즈에서 지원되는 API 버전 확인

다음 API 요청을 사용하여 지원되는 API 주요 버전 목록을 반환합니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

요청에 대한 API 버전을 지정합니다

path 매개 변수를 사용하여 API 버전을 지정할 수 있습니다 (/api/v3) 또는 머리글 (Api-Version: 3)를 클릭합니다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

사이트 간 요청 위조(CSRF)로부터 보호

CSRF 토큰을 사용하여 쿠키를 사용하는 인증을 강화하면 StorageGRID에 대한 CSRF(사이트 간 요청 위조) 공격으로부터 보호할 수 있습니다. Grid Manager 및 Tenant Manager는 이 보안 기능을 자동으로 활성화합니다. 다른 API 클라이언트는 로그인할 때 활성화 여부를 선택할 수 있습니다.

HTTP 양식 POST와 같이 다른 사이트에 대한 요청을 트리거할 수 있는 공격자는 로그인한 사용자의 쿠키를 사용하여 특정 요청을 만들 수 있습니다.

StorageGRID는 CSRF 토큰을 사용하여 CSRF 공격으로부터 보호합니다. 활성화된 경우 특정 쿠키의 내용은 특정 헤더 또는 특정 POST 본문 매개 변수의 내용과 일치해야 합니다.

기능을 활성화하려면 를 설정합니다 csrfToken 매개 변수 대상 true 인증 중. 기본값은 입니다 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"
```

참이면 A입니다 GridCsrfToken 쿠키는 Grid Manager 및 에 대한 로그인에 대한 임의 값으로 설정됩니다 AccountCsrfToken 쿠키는 테넌트 관리자에 대한 로그인에 대한 임의 값으로 설정됩니다.

쿠키가 있는 경우 시스템 상태(POST, PUT, 패치, 삭제)를 수정할 수 있는 모든 요청에 다음 중 하나가 포함되어야 합니다.

- 를 클릭합니다 x-Csrf-Token CSRF 토큰 쿠키의 값으로 설정된 헤더.
- 폼 인코딩된 바디를 수용하는 끝점의 경우: A csrfToken 폼 인코딩된 요청 본문 매개 변수입니다.

추가 예제 및 세부 정보는 온라인 API 설명서를 참조하십시오.



CSRF 토큰 쿠키 세트가 있는 요청도 를 적용합니다 "Content-Type: application/json" JSON 요청 본문을 CSRF 공격에 대한 추가 보호 기능으로 기대하는 모든 요청의 헤더입니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.