StorageGRID® NAS Bridge 2.3

管理APIガイド

2019年11月 | 215-14200_2019-11_ja-jp
ng-gpso-jp-documents@netapp.com

NetApp®

目次

NAS Bridge管理APIについて

NAS Bridge管理APIは、NAS Bridge管理機能へのアクセスを提供します。このAPIは、RESTful Webサービスを基盤としています。管理APIを使用する前に、その設計、アーキテクチャ コンポーネント、および制限事項について理解しておく必要があります。

RESTful Webサービスの基礎

NAS Bridge管理APIは、RESTful Webサービスに基づいています。Representational State Transfer（REST）は、サーバベースのリソースを公開するために確立されたガイドラインです。RESTはNAS Bridgeを管理するための柔軟で拡張性の高い基盤を提供します。

リソースと状態の表示

RESTful Webサービスの核となるのは、次の要素です。

- システムまたはサーバベースのリソースの識別
  すべてのシステムは、リソースを使用し、管理します。リソースには、ファイル、ビジネス情報、プロセス、管理エンティティなどがあります。
- リソースの状態の定義および関連する状態処理
  リソースは必ず複数ある状態のいずれかに該当します。状態の変更に使用される処理を明確に定義する必要があります。

クライアントとサーバの間でメッセージが交換されて、CRUD（Create、Read、Update、Delete）処理に従ってリソースにアクセスしてその状態を変更します。

HTTPメッセージ

Hypertext Transfer Protocol（HTTP）は、Webサービスがリソースに関するメッセージを交換する際に使用するプロトコルです。HTTPメッセージの交換時には、HTTP動詞がリソースおよび対応する状態管理アクションにマッピングされます。

NAS Bridge管理APIはHTTPのサブセットを利用し、次のHTTP動詞を使用します。

- GET
- PUT
- POST
- PATCH
- DELETE

HTTPはステートレスです。このため、関連する一連の要求と応答を1つのIDで関連付けるには、HTTPヘッダーやクッキーなどの追加情報をデータ フローに追加する必要があります。また、HTTPはデフォルトでTCPポート80を使用します。

URIエンドポイント

Uniform Resource Identifier（URI）は、リソースが配置されているエンドポイントの指定に使用します。URIは、一意なリソース名を作成するための一般的なフレームワークです。リソースは、階層型ディレクトリに似た構造で公開されます。

Uniform Resource Locator（URL）は主にWebに適用されるURIの一種で、RESTful Webサービスで使用されます。URLは、リソースの識別および表示されたリソースへのアクセスに使用されます。

JSONの形式

Webクライアントとサーバの間では複数の方法で情報を転送できますが、最も広く使用されている方法はJavaScript Object Notation（JSON）です。JSONは、オブジェクトやアレイなどの単純なデータ構造をプレーン テキストで表すための標準です。NAS Bridge RESTful Webサービスでは、各リソースを記述する状態情報の表示と転送にJSONが使用されています。

複数のアクセス パス

NAS Bridge管理APIには、次のような方法でアクセスできます。

- NAS Bridge**の標準ユーザ インターフェイス**：NAS Bridgeの標準Webユーザ インターフェイスから間接的にAPIにアクセスします。ブラウザを使用してNAS Bridgeの管理IPアドレスにアクセスすると、最初のページにカテゴリ別に分類された管理機能が表示されます。ブラウザは、管理APIにアクセスし、ユーザ インターフェイスの設計に従ってデータを再フォーマットします。つまり、ユーザはNAS Bridgeのユーザ インターフェイスを操作し、ユーザ インターフェイスは対応するAPI呼び出しを作成します。
- **API Docs（Swagger）Webページ**：ブラウザから管理IPアドレスを介してNAS Bridgeにアクセスしたら、[API Docs] Webページ（Swaggerオープン ソース プラットフォームが提供）にアクセスできます。API Docsページでは、ユーザ インターフェイスを使用してパラメータやオプションを変更した場合のAPIの動作を確認しながら、APIの開発を進めることができます。API Docs（Swagger）インターフェイスの表示例については、NAS Bridge管理APIの使用手順を参照してください。

  注意：API Docs Webページを使用して実行するAPI処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

- **カスタム プログラム** - Python、Java、cURLなどの各種プログラミング言語やツールを使用して管理APIにアクセスすることができます。APIを使用するプログラム、スクリプト、またはツールは、RESTful Webサービスのクライアントとして機能します。プログラミング言語を使用すると、APIをより詳しく理解できるだけでなく、NAS Bridgeノードの管理と制御を自動化することができます。

データのアップロード

APIを使用してNAS Bridgeのリカバリ パッケージなどのファイルをアップロードする場合は、マルチパートのコンテンツ タイプでPOSTを実行する必要があります。そうしないと、ファイルはアップロードされません。

APIを使用するための一般的なワークフロー

NAS Bridge管理APIにアクセスする場合は、次の推奨ワークフローに従ってください。

APIセッションを開始すると、認証トークンが生成されます。生成されたトークンは、そのセッション中の各API呼び出しに自動的に挿入されます。APIの呼び出しにはそのつど認証が必要です。

1. ユーザ名とパスワードを指定して、APIセッションを作成します。管理APIにログインすると、認証トークンが自動的に生成されます。
2. 目的のタスクを実行するために必要なその他のAPI呼び出しを、必要な情報を指定して実行します。認証トークンが各API呼び出しに自動的に挿入されます。

3. セッションを削除します。セッションを削除すると、認証トークンがリセットされ、新しいセッションを開始したときには別のトークンが生成されます。

   注意：セキュリティ上の理由から、API呼び出しの完了後にセッションを削除することが重要です。

関連タスク

認証トークンの取得（11ページ）

NAS Bridgeのリソースとオブジェクトの概要

NAS Bridge管理APIでは、各リソース タイプのインスタンスを同時に複数扱うことができます。各インスタンスは1つのオブジェクトと考えることができます。したがって、ある特定のリソース タイプについて、そのリソース インスタンスを1つ以上のオブジェクトの配列とみなすことができます。この設計により、APIからリソース インスタンスに柔軟にアクセスできるだけでなく、アクセスをきめ細かく制御できます。

オブジェクトID

各リソース インスタンスまたはオブジェクトには、一意の識別子（ID）が割り当てられます。オブジェクトIDは整数値です。このIDは、同じリソース タイプ内では一意ですが、システム全体では一意ではありません。たとえば、DNSサーバを作成したときにID「1」が割り当てられ、そのあとにNTPサーバを作成したときにもID「1」が割り当てられる可能性があります。この場合は、リソース タイプが異なるため、同じIDを使用できます。

IDは、一般に追加要求が成功したあとのHTTP応答で返されます。IDは次の場合に必要となります。

- リソース インスタンスの現在のステータスを取得する場合
- あるオブジェクトが別のオブジェクトを参照する状況でリソース インスタンスをリンクする場合
- リソース インスタンスを削除する場合

リソースのステータス概要

各リソース インスタンスにはステータスが関連付けられています。一般に、リソースのステータスは管理APIからアクセスして表示することができます。

NAS Bridgeリソースに使用されるステータス値は次のとおりです。

- NOTIFYING
  基盤のサービスに変更が通知されています。
- COMMITTING
  基盤のサービスが変更のコミットを調整しています。
- ABORTING
  変更が拒否されました。詳細については、アラーム ページとエラー ログ メッセージを確認してください。
- FAILED
  変更が失敗し、すべてのサービスがロールバックを実行しました。詳細については、アラーム ページを確認してください。
- READY
  変更が正常に完了し、リソースが使用可能な状態にあります。

ほとんどの場合、状態の詳細を示すために最初の要求またはアクション タイプがステータスの先頭に追加されます。たとえば、追加要求を発行した場合は、新しいリソースのステータスが一時的に「ADDING / NOTIFYING」になる可能性があります。リソースを削除するときも、同じように状態が構成されます。

非同期処理の仕組み

リソースの作成または削除を行うAPI呼び出しの多くは、それ以外のAPI呼び出しに比べて完了に時間がかかることがあります。NAS Bridgeでは、このようなタイプの要求が非同期的に処理されます。非同期的に処理される呼び出しの場合は、リソース インスタンスのステータスを調べて、要求が完了していることを確認する必要があります。

非同期処理の場合、成功を示す最初のHTTP応答が返された時点では、要求は受け取られていますが、完了しているとはかぎりません。このため、リソースを追加または削除するための非同期要求を行ったあとに、リソース インスタンスをテストして要求が完了していることを確認する必要があります。

注：特定のAPI呼び出しが非同期的に処理されるかどうかを判別するには、API Docs（Swagger）Webページのドキュメントを参照してください。このページの「Implementation Notes」セクション（存在する場合）に、詳細が表示されます。

追加要求のあとのリソース ステータスの確認

リソースを追加するAPI呼び出しを実行したあとに、リソースのステータスをポーリングして要求が完了したことを確認する必要があります。新しいリソースのステータスがREADYであれば、要求は完了しています。

非同期的にリソースを追加する場合は、必要な認証トークンを作成したあとに、次のプロセスを実行します。

1. リソースを追加するAPIを呼び出します。
2. 要求が正常に受け取られたことを示すHTTP応答を受信します。
3. HTTP応答からリソースIDを抽出します。
4. 決まった時間内で、次の手順（ループ サイクル）を繰り返し実行します。
   a. IDに基づいてリソースの現在のステータスを取得します。
   b. リソースのステータスがREADYでない場合は、もう一度ループを実行します。
   c. リソースのステータスがFAILED UPDATEまたはFAILED ADDの場合は、処理を中止し、問題を修正してから（例：障害が発生したリソースを削除する）、もう一度ループを実行します。
5. リソースのステータスがREADYになったら、ループを停止できます。
6. リソースのステータスがREADYになる前にループが（任意のタイムアウト値に従って）タイムアウトした場合は、エラーを報告します。

削除要求のあとのリソースの削除の確認

リソースを削除するAPI呼び出しを実行したら、リソースをポーリングして削除されたことを確認する必要があります。リソースが存在していなければ、要求は完了しています。

非同期的にリソースを削除する場合は、必要な認証トークンを作成したあとに、次のプロセスを実行します。

1. リソースを削除するAPI呼び出しを実行します。

2. 要求が正常に受け取られたことを示すHTTP応答を受信します。
3. タイミング ループ内で、サイクルごとに次の操作を実行します。
   a. IDに基づいてリソースの現在のステータスを取得します。
   b. リソースが見つかった場合（HTTPコード200）は、もう一度ループを実行します。
4. GET要求で「Not Found」（HTTPコード404）が返されたら、ループを停止できます。
5. リソースがまだ存在するときにポーリング ループが（任意のタイムアウト値に従って）タイムアウトした場合は、エラーを報告します。

APIでサポートされるリソース タイプの概要

NAS Bridge管理APIを使用する際に、サポートされているRESTfulリソース タイプを確認しておく必要があります。API呼び出しは、リソース タイプに応じて分類されます。

API呼び出しの一覧、および各呼び出しの詳細については、API Docs（Swagger）Webページを参照してください。管理APIに対する更新や変更に関する情報については、リリース ノートを参照してください。

管理API呼び出しは、次のリソース タイプに基づいて分類されています。

- Active Directoryコントローラ
- アラート設定
- AutoSupport（ASUP）サービス
- キャッシュ デバイス
- 設定のエクスポート（リカバリ パッケージ）
- デバッグ
- 運用停止
- ディスク
- DNSサーバ
- ファイルシステム
- 指標
- ネットワーク インターフェイス
- ネットワーク論理インターフェイス（ネットワークLIF）
- ネットワーク ルート
- NTPサーバ
- オブジェクト ストア
- パスワード
- プロキシ サーバ
- リブート

- セッション
- SMTPサーバ（Eメール サーバ）
- ストレージAPI証明書
- システム イベント
- システム情報
- アップグレードされたディスクのアクティベーション
- アップグレード
- ユーザ

APIへのアクセスとその使用

次の手順は、API Docs（Swagger）Webページを使用してNAS Bridge管理APIにアクセスする方法です。代わりに、プログラミング言語や他のコマンドライン ツールを使用することもできます。

API Docs Webページへのアクセス

API Docs（Swagger）Webページには、NAS Bridgeのユーザ インターフェイスからアクセスします。

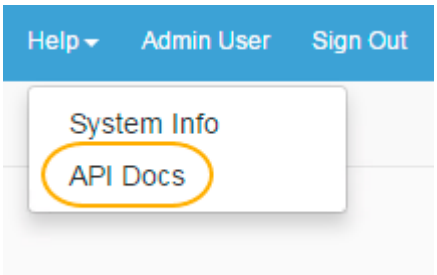
開始する前に

NAS Bridgeの管理IPアドレスまたはドメイン名を確認しておく必要があります。

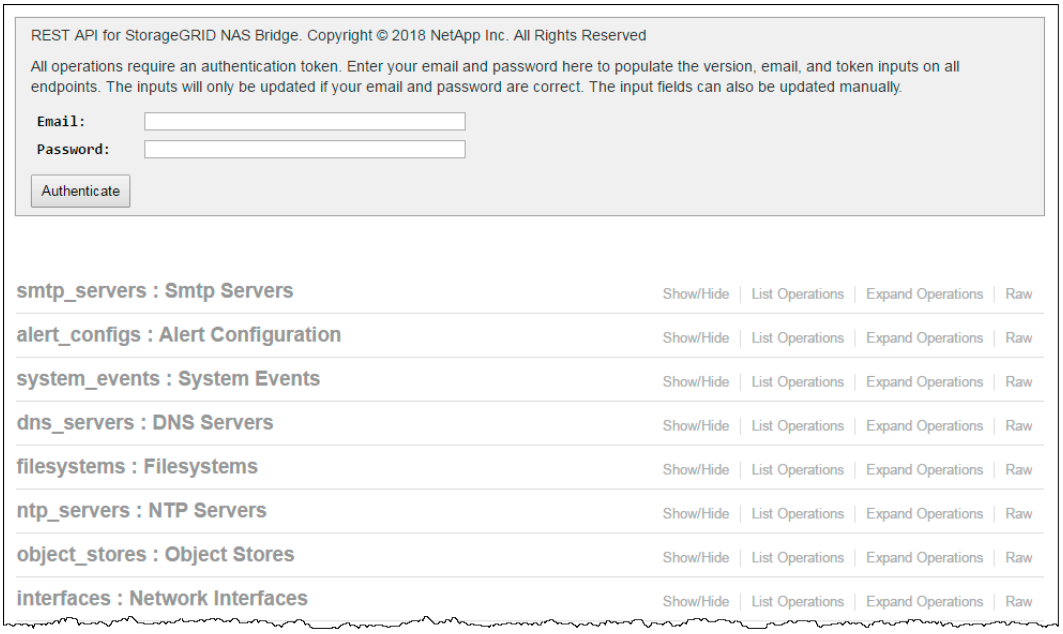
手順

1. NAS Bridgeにログインします。
2. Webページの右上にある**[Help]**をクリックします。

   [Help]メニューが表示されます。
3. **[API Docs]**をクリックします。



新しいタブに[API Docs]ページが表示されます。ページの上部には、管理APIを使用する際に必要となる認証トークンを取得するためのログイン ダイアログがあります。ログイン ダイアログの下に、API呼び出しがリソース カテゴリ別に表示されます。



関連タスク

認証トークンの取得（11ページ）

関連資料

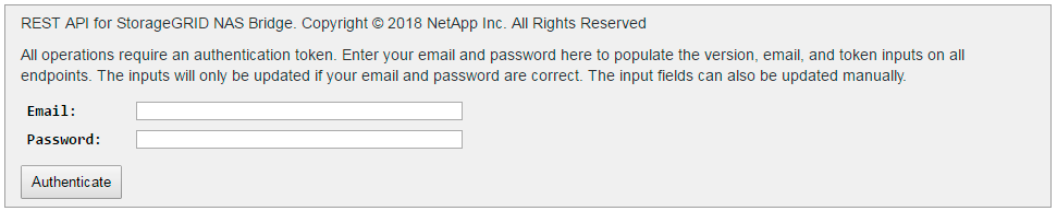
*API*でサポートされるリソース タイプの概要（8ページ）

認証トークンの取得

管理APIを使用するには、最初に認証トークンを取得する必要があります。

手順

1. API Docsページの上部にユーザのEメール アドレスとパスワードを入力します。

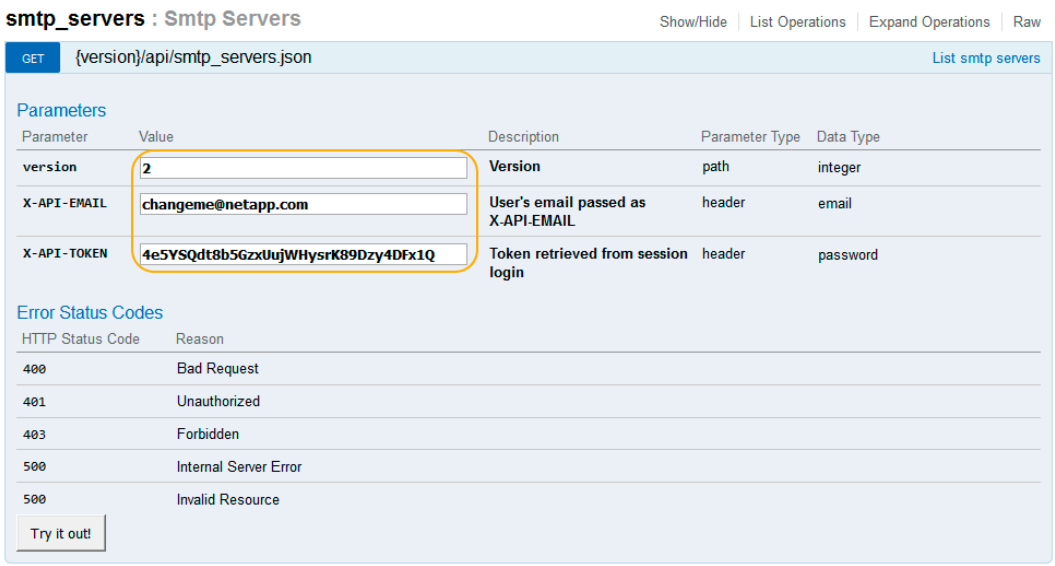


2. **[Authenticate]**をクリックします。

   ログイン情報が正しい場合は認証トークンが生成され、このセッション中に呼び出すすべてのAPIエンドポイントに対して次の処理が実行されます。

   - 認証トークンが[X-API-TOKEN]フィールドに自動的に挿入されます。
   - ログインに使用したEメール アドレスが[X-API-EMAIL]フィールドに自動的に挿入されます。
   - APIバージョンが[version]フィールドに挿入されます。

例



関連タスク

API Docs Webページへのアクセス（10ページ）

APIの呼び出しの詳細の把握

API Docs（Swagger）Webページには、すべてのAPI呼び出しの詳細情報が掲載されています。すべてのAPI呼び出しが共通の形式で文書化されて表示されます。1つのAPI呼び出しについて理解すれば、他のAPI呼び出しの詳細も同様に解釈できるようになります。

手順

1. メインのAPI Docsページで、**[sessions]**をクリックします。
2. **[POST]**をクリックして、認証トークンを要求するために使用するAPI呼び出しの詳細を表示します。

3. ページ全体を確認し、API呼び出しおよび入力が必要な項目について理解します。

HTTP動詞とURL、必要な入力パラメータ、HTTPステータス コード、および実装メモを確認しておきます。

APIを使用した単純なタスクの実行

APIの理解を深めるには、API Docs（Swagger） Webページを使用して、システム イベントの作成などの簡単なタスクを実行する必要があります。

開始する前に

ブラウザからAPI Docs Webページにアクセスする方法を確認しておく必要があります。また、管理者アカウントのクレデンシャル（ユーザ名とパスワード）を確認しておきます。

注意：API Docs Webページを使用して実行するAPI処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. APIをテストするためのシステム イベント メッセージの作成（13ページ）
2. 認証トークンのリセット（17ページ）

関連タスク

*API Docs Web*ページへのアクセス（10ページ）

APIをテストするためのシステム イベント メッセージの作成

管理APIをテストする簡単な方法は、システム イベント（アラーム）ログにメッセージを作成することです。

開始する前に

API Docs（Swagger）ページにログインしている必要があります。これにより、認証トークン、Eメール アドレス、APIバージョンが各APIエンドポイントの対応するフィールドに自動的に挿入されます。

タスク概要

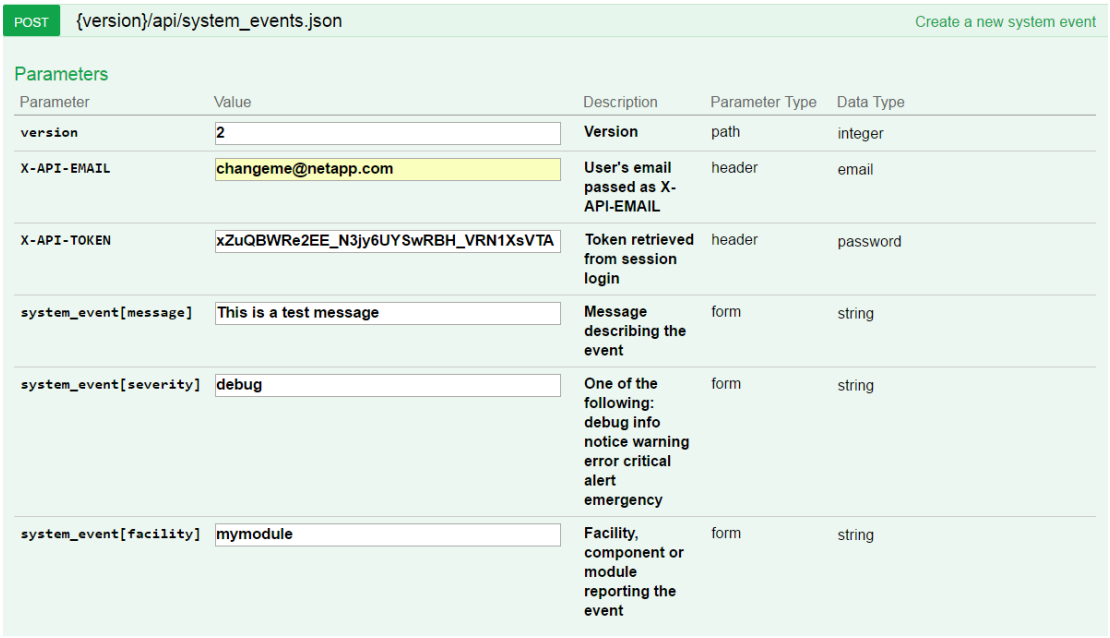
システム イベントを作成するには、API Docsページを使用します。イベントが作成されたら、次の2つの方法でメッセージを表示できます。

- API Docs（Swagger）ページのGET関数を使用する
- NAS Bridgeのユーザ インターフェイスを使用する

手順

1. API Docsページで、**[system_events]**をクリックします。
2. **[POST]**をクリックして、新しいシステム イベントを作成するために使用するAPI呼び出しを表示します。

   POST API呼び出しが表示されます。Webページの上部で正常にログインした場合は、バージョン、Eメール アドレス（ユーザ アカウント）、認証トークンが自動的にページに入力されます。
3. テスト メッセージ、重大度（値のリストから選択）、およびテスト ファシリティを入力します。



POST {version}/api/system_events.json — Create a new system event

Parameters

Parameter	Value	Description	Parameter Type	Data Type
version	2	Version	path	integer
X-API-EMAIL	changeme@netapp.com	User's email passed as X-API-EMAIL	header	email
X-API-TOKEN	xZuQBWRe2EE_N3jy6UYSwRBH_VRN1XsVTA	Token retrieved from session login	header	password
system_event[message]	This is a test message	Message describing the event	form	string
system_event[severity]	debug	One of the following: debug info notice warning error critical alert emergency	form	string
system_event[facility]	mymodule	Facility, component or module reporting the event	form	string

4. **[Try it out]**をクリックします。

Request URL

```
https://10.96.104.166:443/2/api/system_events.json
```

Response Body


```
{
  "response": {
    "id": 40,
    "severity": "debug",
    "facility": "mymodule",
    "message": "This is a test message",
    "created_at": "2017-11-10T22:39:23.110Z",
    "updated_at": "2017-11-10T22:39:23.110Z",
    "config": null,
    "config_id": null
  }
}
```

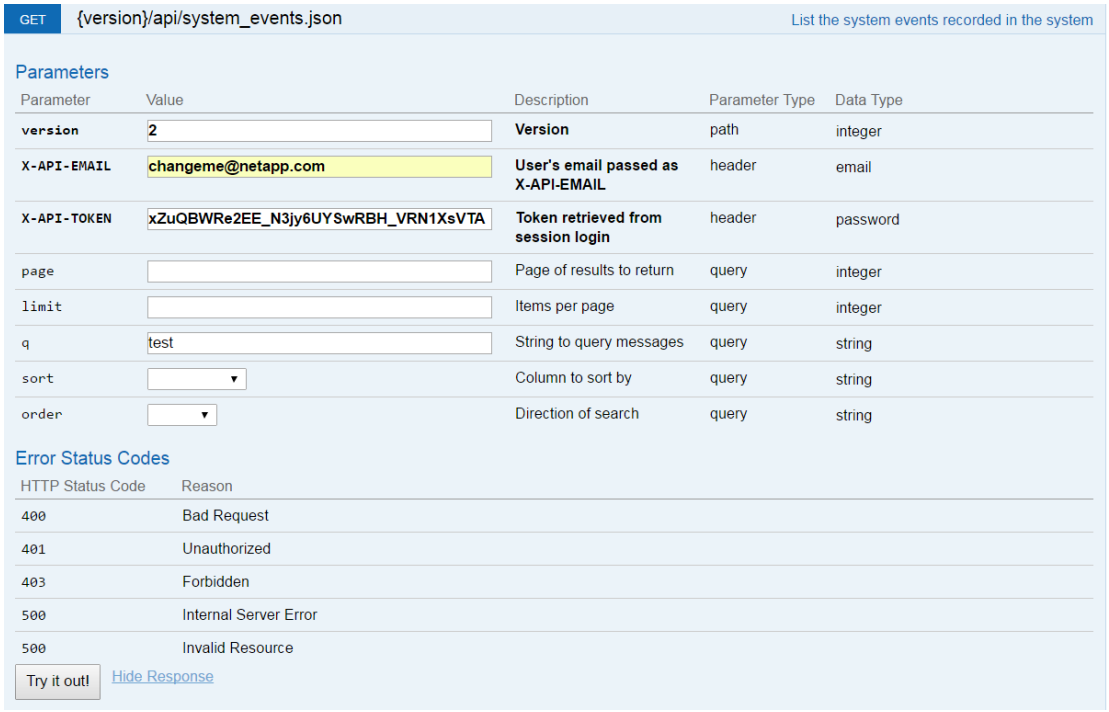

Response Code

```
200
```

応答コード200は成功を示します。

5. 新しいメッセージが作成されたことを確認するために、次の作業を行います。

   - API Docsページで、**[system_events]** > **[GET]**をクリックし、Eメール アドレスと認証トークンのフィールドが設定されていることを確認します。qパラメータを使用して、作成したメッセージ テキストの全体または一部を含むメッセージだけに結果が限定されるようにします。次に、**[Try it out]**をクリックして作成したメッセージをリストします。



GET {version}/api/system_events.json — List the system events recorded in the system

Parameters

Parameter	Value	Description	Parameter Type	Data Type
version	2	**Version**	path	integer
X-API-EMAIL	changeme@netapp.com	**User's email passed as X-API-EMAIL**	header	email
X-API-TOKEN	xZuQBWRe2EE_N3jy6UYSwRBH_VRN1XsVTA	**Token retrieved from session login**	header	password
page		Page of results to return	query	integer
limit		Items per page	query	integer
q	test	String to query messages	query	string
sort		Column to sort by	query	string
order		Direction of search	query	string

Error Status Codes

HTTP Status Code	Reason
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error
500	Invalid Resource

Try it out! Hide Response

Request URL

```
https://10.96.104.166:443/2/api/system_events.json?q=test
```

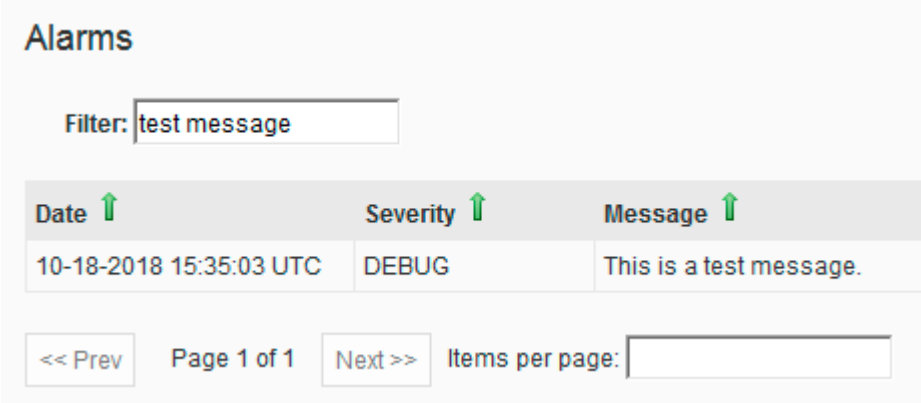
Response Body


```
    {
      "id": 40,
      "severity": "debug",
      "facility": "mymodule",
      "message": "This is a test message",
      "created_at": "2017-11-10T22:39:23.000Z",
      "updated_at": "2017-11-10T22:39:23.000Z",
      "config": null,
      "config_id": null
    }
  ],
  "count": 8,
  "pagination": {
    "current": 1,
    "previous": null,
    "next": null,
    "per_page": 25,
    "pages": 1,
    "count": 8
  }
```


Response Code

```
200
```

- NAS Bridgeのユーザ インターフェイスで、**[Alarms]**をクリックし、イベントをフィルタリングまたはソートして、投稿（POST）したメッセージを見つけます。



関連タスク

認証トークンの取得（11ページ）

認証トークンのリセット

API呼び出しが完了したあとに、認証トークンをリセットする必要があります。こうしてトークンが再利用されないようにすることで、システムのセキュリティが向上します。

開始する前に

次のパラメータを確認しておく必要があります。

- 有効な認証トークン。トークンを取得すると、APIエンドポイントの必須フィールドに自動的に挿入されます。
- 認証トークンの作成時に使用した管理者のEメール アドレス（ユーザ アカウント）。

手順

1. [API Docs]ページで、**[sessions]**をクリックします。
2. **[DELETE]**をクリックして、認証トークンをリセットするために使用するAPI呼び出しを表示します。

   DELETE API呼び出しが表示されます。Webページの上部で正常にログインした場合は、バージョン、Eメール アドレス（ユーザ アカウント）、認証トークンが自動的にページに入力されます。
3. **[Try it out!]**をクリックします。

   応答コード204は、トークンが削除されたことを示します。

著作権に関する情報

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.A.

このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によ って保護されている場合があります。

ここに記載されている「データ」は商用品目（FAR 2.101で定義）に該当し、その所有権はネットアップに帰属します。米国政府は、データが提供される際の米国政府との契約に関連し、かつ当該契約が適用される範囲においてのみ「データ」を使用するための、非独占的、譲渡不可、サブライセンス不可、世界共通の限定的な取り消し不可のライセンスを保有します 。ここに記載されている場合を除き、書面によるネットアップの事前の許可なく、「データ」を使用、開示、複製、変更、実行、または表示することは禁止されています。米国国防総省のライセンス権限は、DFARS 252.227-7015（b）項に規定されている権限に制限されます。

商標に関する情報

NetApp、NetAppのロゴ、ネットアップの商標一覧のページに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

http://www.netapp.com/jp/legal/netapptmlist.aspx

マニュアルの更新について

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメール アドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitterアカウントもあります。

本マニュアルの改善についてご提案がある場合は、次のアドレスまでコメントをEメールでお送りください。

ng-gpso-jp-documents@netapp.com

その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティング システム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。