



# プラットフォームサービスエンドポイントを設定する

## StorageGRID 11.8

NetApp  
May 17, 2024

# 目次

プラットフォームサービスエンドポイントを設定する	1
プラットフォームサービスエンドポイントとは何ですか。	1
CloudMirror レプリケーション用のエンドポイント	1
通知用のエンドポイント	1
検索統合サービスのエンドポイント	2
プラットフォームサービスのエンドポイントの URN を指定してください	2
プラットフォームサービスエンドポイントを作成します	4
プラットフォームサービスエンドポイントの接続をテストします	11
プラットフォームサービスエンドポイントを編集します	13
プラットフォームサービスエンドポイントを削除します	15
プラットフォームサービスのエンドポイントエラーのトラブルシューティングを行います	16

# プラットフォームサービスエンドポイントを設定する

バケットのプラットフォームサービスを設定する前に、少なくとも 1 つのエンドポイントをプラットフォームサービスのデスティネーションとして設定する必要があります。

プラットフォームサービスへのアクセスは、StorageGRID 管理者がテナント単位で有効にします。プラットフォームサービスエンドポイントを作成または使用するには、ストレージノードが外部のエンドポイントリソースにアクセスできるようネットワークが設定されているグリッドで、Manage Endpoints または Root Access 権限を持つテナントユーザである必要があります。1 つのテナントに対して設定できるプラットフォームサービスエンドポイントは最大 500 個です。詳細については、StorageGRID 管理者にお問い合わせください。

## プラットフォームサービスエンドポイントとは何ですか。

プラットフォームサービスエンドポイントを作成するときは、StorageGRID が外部のデスティネーションにアクセスするために必要な情報を指定します。

たとえば、StorageGRID バケットから Amazon S3 バケットにオブジェクトをレプリケートする場合は、StorageGRID が Amazon のデスティネーションバケットにアクセスするために必要な情報とクレデンシャルを含むプラットフォームサービスエンドポイントを作成します。

プラットフォームサービスのタイプごとに独自のエンドポイントが必要なため、使用する各プラットフォームサービスについて少なくとも 1 つのエンドポイントを設定する必要があります。プラットフォームサービスエンドポイントの定義が完了したら、サービスを有効にするための設定 XML でエンドポイントの URN をデスティネーションとして指定します。

同じエンドポイントを複数のソースバケットのデスティネーションとして使用できます。たとえば、複数のバケット間で検索を実行できるように、複数のソースバケットが同じ検索統合エンドポイントにオブジェクトメタデータを送信するように設定できます。複数のエンドポイントをターゲットとして使用するようにソースバケットを設定することもできます。これにより、オブジェクトの作成に関する通知をある Amazon Simple Notification Service (Amazon SNS) トピックに送信したり、オブジェクトの削除に関する通知を別の Amazon SNS トピックに送信したりできます。

## CloudMirror レプリケーション用のエンドポイント

StorageGRID は、S3 バケットを表すレプリケーションエンドポイントをサポートします。このバケットは、Amazon Web Services、同一またはリモートの StorageGRID 環境、あるいは別のサービスでホストされている可能性があります。

## 通知用のエンドポイント

StorageGRID は、Amazon SNS および Kafka エンドポイントをサポートしています。Simple Queue Service (SQS) または AWS Lambda エンドポイントはサポートされていません。

Kafka エンドポイントでは、相互 TLS はサポートされていません。その結果、`ssl.client.auth` をに設定します `required` Kafka ブローカーの設定では、原因 Kafka エンドポイントの設定に問題がある可能性があります。

# 検索統合サービスのエンドポイント

StorageGRID は、Elasticsearch クラスタを表す検索統合エンドポイントをサポートします。Elasticsearch クラスタは、ローカルデータセンターに配置することも、AWSクラウドなどの別の場所でホストすることもできます。

検索統合エンドポイントは、Elasticsearch の特定のインデックスとタイプを参照します。StorageGRID でエンドポイントを作成する前に、Elasticsearch でインデックスを作成しておく必要があります。作成していない場合、エンドポイントの作成に失敗します。エンドポイントを作成する前にタイプを作成する必要はありません。StorageGRID は、オブジェクトメタデータをエンドポイントに送信するときに必要に応じてタイプを作成します。

関連情報

["StorageGRID の管理"](#)

## プラットフォームサービスのエンドポイントの URN を指定してください

プラットフォームサービスエンドポイントを作成するときは、Unique Resource Name（URN）を指定する必要があります。プラットフォームサービスの設定XMLを作成するときは、URNを使用してエンドポイントを参照します。各エンドポイントの URN は一意である必要があります。

プラットフォームサービスエンドポイントは、作成時に StorageGRID で検証されます。プラットフォームサービスエンドポイントを作成する前に、エンドポイントで指定されたリソースが存在し、アクセス可能であることを確認してください。

### URN 要素

プラットフォームサービスのエンドポイントのURNは、いずれかで開始する必要があります `arn:aws` または `urn:mysite`、次のようにします。

- サービスがAmazon Web Services（AWS）でホストされている場合は、を使用します `arn:aws`
- サービスがGoogle Cloud Platform（GCP）でホストされている場合は、を使用します `arn:aws`
- サービスがローカルでホストされている場合は、を使用します `urn:mysite`

たとえば、StorageGRID でホストされるCloudMirrorエンドポイントのURNを指定する場合、URNはで始まる可能性があります `urn:sgws`。

URN の次の要素では、次のようにプラットフォームサービスのタイプを指定します。

サービス	を入力します
CloudMirror レプリケーション	s3
通知	sns または kafka

サービス	を入力します
検索統合	es

たとえば、StorageGRID でホストされるCloudMirrorエンドポイントのURNを指定する場合は、と指定します  
s3 をダウンロードしてください urn:sgws:s3。

URN の最後の要素は、デスティネーション URI の特定のターゲットリソースを識別します。

サービス	特定のリソース
CloudMirror レプリケーション	bucket-name
通知	sns-topic-name または kafka-topic-name
検索統合	domain-name/index-name/type-name  <ul style="list-style-type: none"> <li>注： Elasticsearch クラスタが * NOT * である場合、インデックスを自動的に作成するように設定されているため、エンドポイントを作成する前にインデックスを手動で作成する必要があります。</li> </ul>

## AWS と GCP でホストされるサービスの URN

AWS と GCP のエンティティの場合、完全な URN は有効な AWS ARN です。例：

- CloudMirror レプリケーション：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 検索統合：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



AWS検索統合エンドポイントの場合は、を参照してください domain-name リテラル文字列を含める必要があります `domain/` を参照してください。

## ローカルでホストされるサービスの URN

クラウド サービス ではなくローカルでホストされるサービスを使用する場合は、URN の 3 番目と最後の必

須要素が含まれていて、有効かつ一意な URN が作成されるのであれば、どのような方法で URN を指定してもかまいません。となっている要素はオプションで空白にすることも、リソースを識別して一意な URN の作成に役立つ任意の情報を指定することもできます。例：

- CloudMirror レプリケーション：

```
urn:mysite:s3:optional:optional:bucket-name
```

StorageGRID でホストされるCloudMirrorエンドポイントの場合は、で始まる有効なURNを指定できます  
urn:sgws：

```
urn:sgws:s3:optional:optional:bucket-name
```

- 通知：

Amazon Simple Notification Serviceエンドポイントを指定します。

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Kafkaエンドポイントを指定します。

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- 検索統合：

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



ローカルでホストされる検索統合エンドポイントの場合は、を参照してください domain-name エンドポイントのURNが一意であるかぎり、Elementには任意の文字列を指定できません。

## プラットフォームサービスエンドポイントを作成します

プラットフォームサービスを有効にする前に、正しいタイプのエンドポイントを少なくとも 1 つ作成しておく必要があります。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

- プラットフォームサービスエンドポイントによって参照されるリソースを作成しておきます。
  - CloudMirror レプリケーション： S3 バケット
  - イベント通知： Amazon Simple Notification Service（Amazon SNS）またはKafkaトピック
  - 検索通知： インデックスを自動的に作成するようにデスティネーションクラスタが設定されていない場合、 Elasticsearch インデックス。
- デスティネーションリソースに関する情報を確認しておきます。
  - Uniform Resource Identifier（URI）のホストとポート



StorageGRID システムでホストされているバケットを CloudMirror レプリケーションのエンドポイントとして使用する場合は、グリッド管理者に問い合わせて入力が必要な値を決定してください。

- Unique Resource Name（URN）

"プラットフォームサービスのエンドポイントの URN を指定してください"

- 認証クレデンシャル（必要な場合）：

#### 検索統合エンドポイント

検索統合エンドポイントには、次のクレデンシャルを使用できます。

- Access Key：アクセスキー ID とシークレットアクセスキー
- 基本 HTTP 認証：ユーザ名とパスワード

#### CloudMirrorレプリケーションエンドポイント

CloudMirrorレプリケーションでは、次のクレデンシャルを使用できます。

- Access Key：アクセスキー ID とシークレットアクセスキー
- CAP（C2S Access Portal）：一時的なクレデンシャル URL、サーバ証明書とクライアント証明書、クライアントキー、およびオプションのクライアント秘密鍵パスフレーズ。

#### Amazon SNSエンドポイント

Amazon SNSエンドポイントの場合は、次のクレデンシャルを使用できます。

- Access Key：アクセスキー ID とシークレットアクセスキー

#### Kafkaエンドポイント

Kafkaエンドポイントの場合は、次のクレデンシャルを使用できます。

- SASL/plain：ユーザ名とパスワード
- SASL/SCRAM-SHA-256：ユーザ名とパスワード
- SASL/SCRAM-SHA-512：ユーザ名とパスワード

- セキュリティ証明書（カスタム CA 証明書を使用する場合）

- Elasticsearchセキュリティ機能が有効になっている場合は、接続テスト用のmonitor cluster権限と、ドキュメント更新用のwrite index権限、またはindex権限とdelete index権限の両方があります。

#### 手順

1. ストレージ（S3） \* > \* プラットフォームサービスのエンドポイント \* を選択します。プラットフォームサービスエンドポイントページが表示されます。
2. [\* エンドポイントの作成 \*] を選択します。
3. エンドポイントとその目的を簡単に説明する表示名を入力します。

エンドポイントがサポートするプラットフォームサービスのタイプは、[Endpoints]ページのエンドポイント名の横に表示されるため、この情報を名前に含める必要はありません。

4. [\* URI\*] フィールドに、エンドポイントの Unique Resource Identifier （URI）を指定します。

次のいずれかの形式を使用します。

```
https://host:port
http://host:port
```

ポートを指定しない場合は、次のデフォルトポートが使用されます。

- HTTPS URIにはポート443、HTTP URIにはポート80（ほとんどのエンドポイント）
- HTTPSおよびHTTP URI用のポート9092（Kafkaエンドポイントのみ）

たとえば、StorageGRID でホストされているバケットの URI は次のようになります。

```
https://s3.example.com:10443
```

この例では、s3.example.com StorageGRID ハイアベイラビリティ（HA）グループの仮想IP（VIP）のDNSエントリ、およびを表します 10443 ロードバランサエンドポイントで定義されたポートを表します。



単一点障害（Single Point of Failure）を回避するために、可能な限りロードバランシングノードのHAグループに接続する必要があります。

同様に、AWS でホストされているバケットの URI は次のようになります。

```
https://s3-aws-region.amazonaws.com
```



エンドポイントがCloudMirrorレプリケーションサービスに使用される場合は、URIにバケット名を含めないでください。バケット名は「\* URN \*」フィールドに含める必要があります。

5. エンドポイントの Unique Resource Name （URN）を入力します。





エンドポイントの作成後にエンドポイントのURNを変更することはできません。

6. 「\* Continue \*」を選択します。
7. [認証タイプ]\*の値を選択します。

### 検索統合エンドポイント

検索統合エンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"><li>• アクセスキー ID</li><li>• シークレットアクセスキー</li></ul>
基本 HTTP	ユーザ名とパスワードを使用して、デスティネーションへの接続を認証します。	<ul style="list-style-type: none"><li>• ユーザ名</li><li>• パスワード</li></ul>

### CloudMirrorレプリケーションエンドポイント

CloudMirrorレプリケーションエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"><li>• アクセスキー ID</li><li>• シークレットアクセスキー</li></ul>

認証タイプ	説明	クレデンシャル
CAP（C2S Access Portal）	証明書とキーを使用してデスティネーションへの接続を認証します。	<ul style="list-style-type: none"> <li>• 一時的な資格情報 URL</li> <li>• サーバ CA 証明書（ PEM ファイルのアップロード）</li> <li>• クライアント証明書（ PEM ファイルのアップロード）</li> <li>• クライアント秘密鍵（ PEM ファイルのアップロード、 OpenSSL 暗号化形式、または暗号化されていない秘密鍵形式）</li> <li>• クライアント秘密鍵のパスフレーズ（オプション）</li> </ul>

#### Amazon SNSエンドポイント

Amazon SNSエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"> <li>• アクセスキー ID</li> <li>• シークレットアクセスキー</li> </ul>

#### Kafkaエンドポイント

Kafkaエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
SASL/プレーン	プレーンテキストのユーザ名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>• ユーザ名</li> <li>• パスワード</li> </ul>

認証タイプ	説明	クレデンシャル
SASL/SCRAM-SHA-256	チャレンジ応答プロトコルとSHA-256ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>パスワード</li> </ul>
SASL/SCRAM-SHA-512	チャレンジ応答プロトコルとSHA-512ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>パスワード</li> </ul>

ユーザ名とパスワードがKafkaクラスタから取得した委任トークンから取得されたものである場合は、\* Use delegation taken authentication \*を選択します。

- 「\* Continue \*」を選択します。
- Verify server \* のラジオボタンを選択して、エンドポイントへの TLS 接続の検証方法を選択します。

×

Create endpoint

✓ Enter details

✓ Select authentication type  
Optional

3 Verify server  
Optional

### Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

☒ Use custom CA certificate
☐ Use operating system CA certificate
☐ Do not verify certificate

```

-----BEGIN CERTIFICATE-----
abdefghijkl1123456780ABCDEFGHIJKL
123456/7890ABCDEFabdefghijklABCD
-----END CERTIFICATE-----

```

Previous

Test and create endpoint

証明書検証のタイプ	説明
カスタム CA 証明書を使用する	カスタムのセキュリティ証明書を使用します。この設定を選択した場合は、カスタムセキュリティ証明書を * CA 証明書 * テキストボックスにコピーして貼り付けます。
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。このオプションはセキュアではありません。

10. [\* テストとエンドポイントの作成 \*] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、\* エンドポイントの詳細に戻る \* を選択して情報を更新します。次に、「\* Test」を選択し、エンドポイントを作成します。\*



テナントアカウントでプラットフォームサービスが有効になっていないと、エンドポイントの作成が失敗します。StorageGRID 管理者にお問い合わせください。

エンドポイントの設定が完了したら、その URN を使用してプラットフォームサービスを設定できます。

#### 関連情報

["プラットフォームサービスのエンドポイントの URN を指定してください"](#)

["CloudMirror レプリケーションを設定します"](#)

["イベント通知を設定する"](#)

["検索統合サービスを設定する"](#)

## プラットフォームサービスエンドポイントの接続をテストします

プラットフォームサービスへの接続が変更された場合は、エンドポイントへの接続をテストして、デスティネーションリソースが存在すること、および指定したクレデンシャルでアクセスできることを確認できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

このタスクについて

StorageGRID は、クレデンシャルに正しい権限があるかどうかを検証しません。

#### 手順

1. ストレージ（S3） \* > \* プラットフォームサービスのエンドポイント \* を選択します。

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

## Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name <sup>?</sup>	Last error <sup>?</sup>	Type <sup>?</sup>	URI <sup>?</sup>	URN <sup>?</sup>
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	<span>✖</span> 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. 接続をテストするエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

## Overview

Display name:

my-endpoint-1

Type:

S3 Bucket

URI:

http://10.96.104.167:10443

URN:

urn:sgws:s3:::bucket1

Connection

Configuration

### Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

3. [ 接続のテスト \* ] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、「 \* Configuration \* 」を選択して情報を更新します。次に、[ テスト ] を選択し、変更を保存します。 \*

## プラットフォームサービスエンドポイントを編集します

プラットフォームサービスエンドポイントの設定を編集して、名前、URI、またはその他の詳細を変更できます。たとえば、期限切れのクレデンシャルを更新したり、フェールオーバー用のバックアップ Elasticsearch インデックスを指すように URI を変更したりすることが必要な場合があります。プラットフォームサービスエンドポイントのURNは変更できません。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

手順

1. ストレージ（S3） \* > \* プラットフォームサービスのエンドポイント \* を選択します。

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントの

リストが表示されます。

## Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ?	Last error ?	Type ?	URI ?	URN ?
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	<span>✖</span> 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. 編集するエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

3. 「\* Configuration \*」を選択します。

4. 必要に応じて、エンドポイントの設定を変更します。



エンドポイントの作成後にエンドポイントのURNを変更することはできません。

a. エンドポイントの表示名を変更するには、編集アイコンを選択します

b. 必要に応じて、URI を変更します。

c. 必要に応じて、認証タイプを変更します。

- アクセスキー認証の場合は、必要に応じて「\* S3 キーの編集」を選択し、新しいアクセスキー ID とシークレットアクセスキーを貼り付けることで、キーを変更します。変更をキャンセルする必要がある場合は、\* Revert S3 key edit \* を選択します。
- CAP（C2S Access Portal）認証の場合は、一時的なクレデンシャル URL またはオプションのクライアント秘密鍵パスフレーズを変更し、必要に応じて新しい証明書と鍵ファイルをアップロードします。



クライアント秘密鍵は、OpenSSL 暗号化形式または暗号化されていない秘密鍵形式である必要があります。

d. 必要に応じて、サーバを検証する方法を変更します。



5. [ 変更のテストと保存 \*] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エンドポイントを変更してエラーを修正し、[ 変更のテストと保存 ] を選択します。

## プラットフォームサービスエンドポイントを削除します

関連するプラットフォームサービスが不要になった場合は、エンドポイントを削除できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "エンドポイントまたはRoot Access権限を管理します"。

手順

1. ストレージ（S3） \* > \* プラットフォームサービスのエンドポイント \* を選択します。

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

## Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

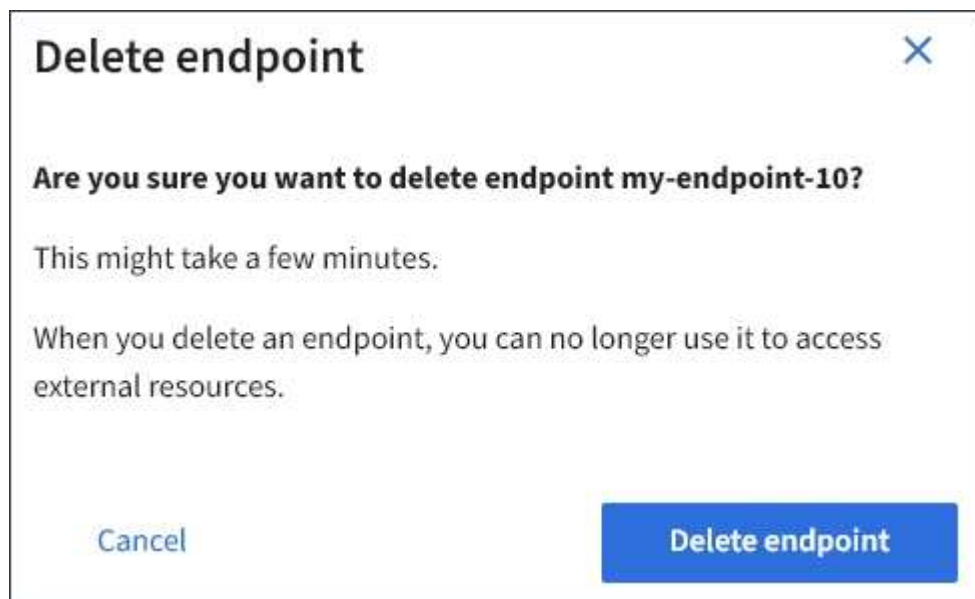
2. 削除する各エンドポイントのチェックボックスを選択します。



使用中のプラットフォームサービスエンドポイントを削除すると、エンドポイントを使用するすべてのバケットに対して、関連するプラットフォームサービスが無効になります。完了していない要求はすべて破棄されます。新しい要求は、削除された URN を参照しないようにバケット設定を変更するまで、引き続き生成されます。StorageGRID はこれらの要求を回復不能なエラーとして報告します。

3. [\* アクション \* > \* エンドポイントの削除 \*] を選択します。

確認メッセージが表示されます。



4. [\* エンドポイントの削除 \*] を選択します。

## プラットフォームサービスのエンドポイントエラーのトラブルシューティングを行います

StorageGRID がプラットフォームサービスエンドポイントと通信しようとしたときにエラーが発生すると、ダッシュボードにメッセージが表示されます。Platform services Endpoints ページの Last error 列は、エラーが発生してから時間を示します。エンドポイントのクレデンシャルに関連付けられている権限が正しくない場合は、エラーは表示されません。

### エラーが発生したかどうかを確認します

過去7日以内にプラットフォームサービスエンドポイントエラーが発生した場合は、Tenant Managerダッシュボードにアラートメッセージが表示されます。プラットフォームサービスのエンドポイントページに移動して、エラーの詳細を確認できます。




One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

ダッシュボードに表示されるのと同じエラーは、[Platform services Endpoints]ページの上部にも表示されま

す。詳細なエラーメッセージを表示するには、次の手順を実行します

#### 手順

1. エンドポイントのリストで、エラーが発生したエンドポイントを選択します。
2. エンドポイントの詳細ページで、\* 接続 \* を選択します。このタブには、エンドポイントの最新のエラーと、エラーが発生してから経過時間が表示されます。赤の X アイコンを含むエラー  過去 7 日以内に発生しました。

### Overview

Display name: **my-endpoint-2**

Type: **Search**

URI: **http://10.96.104.30:9200**

URN: **urn:sgws:es:::mydomain/sveloso/\_doc**

Connection


Configuration

### Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

### Last error details

 2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

## エラーがまだ最新であるかどうかを確認します

一部のエラーは、解決後も「\* Last error \*」列に引き続き表示される場合があります。エラーが現在発生しているかどうかを確認したり、解決済みのエラーをテーブルから強制的に削除したりするには、次の手順を実行します。

#### 手順

1. エンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

2. 接続 > 接続テスト \* を選択します。

[ 接続のテスト \* ] を選択すると、StorageGRID はプラットフォームサービスエンドポイントが存在すること、および現在のクレデンシャルでアクセスできることを検証します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

## エンドポイントエラーの解決

エンドポイントの詳細ページの「\* Last error \*」メッセージを使用して、エラーの原因を特定できます。一部のエラーでは、問題を解決するためにエンドポイントの編集が必要になります。たとえば、StorageGRID に正しいアクセス権限がないか、アクセスキーが期限切れになっているためにデスティネーションの S3 バケットにアクセスできない場合、CloudMirror のエラーが発生することがあります。メッセージは「Either the endpoint credentials or the destination access needs to be updated」で、詳細は「AccessDenied」または「InvalidAccessKeyId」です。

エラーを解決するためにエンドポイントを編集する必要がある場合は、「\* 変更のテストと保存 \*」を選択すると、StorageGRID によって更新されたエンドポイントが検証され、現在のクレデンシャルで到達できることが確認されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

### 手順

1. エンドポイントを選択します。
2. エンドポイントの詳細ページで、\* 構成 \* を選択します。
3. 必要に応じてエンドポイントの設定を編集します。
4. 接続 > 接続テスト \* を選択します。

## 必要な権限がないエンドポイントクレデンシャルです

StorageGRID によるプラットフォームサービスエンドポイントの検証では、エンドポイントのクレデンシャルを使用してデスティネーションリソースに接続できること、および基本的な権限チェックを実行できることが確認されます。ただし、StorageGRID では、特定のプラットフォームサービス処理に必要なすべての権限が検証されるわけではありません。そのため、プラットフォームサービスを使用しようとしたときにエラー（「403 Forbidden」など）が表示された場合は、エンドポイントのクレデンシャルに関連付けられている権限を確認してください。

### 関連情報

- ["StorageGRIDの管理>プラットフォームサービスのトラブルシューティング"](#)
- ["プラットフォームサービスエンドポイントを作成します"](#)
- ["プラットフォームサービスエンドポイントの接続をテストします"](#)
- ["プラットフォームサービスエンドポイントを編集します"](#)

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. 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。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>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。