プラットフォームサービスのエンドポイントを管理する

StorageGRID software

NetApp
December 03, 2025

目次

プラットフォーム サービスのエンドポイントを管理する

プラットフォーム サービスのエンドポイントを構成する

バケットのプラットフォーム サービスを構成する前に、プラットフォーム サービスの宛先となるエンドポイントを少なくとも 1 つ構成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管理者によってテナントごとに有効化されます。プラットフォーム サービス エンドポイントを作成または使用するには、ストレージ ノードが外部エンドポイント リソースにアクセスできるようにネットワークが構成されているグリッド内で、エンドポイントの管理権限またはルート アクセス権限を持つテナント ユーザーである必要があります。 1 つのテナントに対して、最大 500 個のプラットフォーム サービス エンドポイントを構成できます。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 エンドポイントは、 StorageGRID が外部の宛先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複製する場合は、StorageGRID がAmazon の宛先バケットにアクセスするために必要な情報と認証情報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。

各タイプのプラットフォーム サービスには独自のエンドポイントが必要であるため、使用する予定のプラットフォーム サービスごとに少なくとも 1 つのエンドポイントを構成する必要があります。プラットフォーム サービス エンドポイントを定義した後、サービスを有効にするために使用される構成 XML で、エンドポイントの URN を宛先として使用します。

複数のソース バケットの宛先として同じエンドポイントを使用できます。たとえば、複数のソース バケットを構成して、オブジェクト メタデータを同じ検索統合エンドポイントに送信するようにすることで、複数のバケットにわたって検索を実行できるようになります。また、ソースバケットを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 1 つの Amazon Simple Notification Service (Amazon SNS) トピックに送信し、オブジェクトの削除に関する通知を 2 番目の Amazon SNS トピックに送信するといったことが可能になります。

CloudMirror レプリケーションのエンドポイント

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ています。これらのバケットは、Amazon Web Services、同じまたはリモートのStorageGRIDデプロイメント、あるいは別のサービスでホストされている場合があります。

通知のエンドポイント

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、もしあなたが `ssl.client.auth` に設定 `required`Kafka ブローカー構成では、Kafka エンドポイント構成の問題が発生する可能性がありま

す。

検索統合サービスのエンドポイント

StorageGRID は、Elasticsearch クラスターを表す検索統合エンドポイントをサポートしています。これらの Elasticsearch クラスターは、ローカルデータセンターに配置することも、AWS クラウドやその他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、特定の Elasticsearch 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する必要があります。そうしないと、エンドポイントの作成は失敗します。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 エンドポイントの URN を指定します

プラットフォーム サービス エンドポイントを作成するときは、一意のリソース名 (URN) を指定する必要があります。プラットフォーム サービスの構成 XML を作成するときに、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。

StorageGRID は、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にそれを検証します。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、アクセスでき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エンドポイントのURNは、次のいずれかで始まる必要があります。 `arn:aws`または `urn:mysite`、 次のように：

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

たとえば、 StorageGRIDでホストされているCloudMirrorエンドポイントのURNを指定する場合、URNは次のようになります。 `urn:sgws` 。

URN の次の要素は、次のようにプラットフォーム サービスの種類を指定します。

サービス	タイプ
CloudMirrorレプリケーション	`s3`

サービス	タイプ
通知	`sns`または `kafka`
検索統合	`es`

たとえば、 StorageGRIDでホストされているCloudMirrorエンドポイントのURNを引き続き指定するには、以下を追加します。 `s3`取得するため `urn:sgws:s3`。

URN の最後の要素は、宛先 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` 注: Elasticsearch クラスターがインデックスを自動的に作成するように設定されていない場合は、エンドポイントを作成する前に手動でインデックスを作成する必要があります。

AWS および GCP でホストされているサービスの URN

AWS および GCP エンティティの場合、完全な URN は有効な AWS ARN です。例えば：

- 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、 `domain-name`リテラル文字列を含める必要があります `domain/`、ここに示すように。

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、URN の 3 番目と最後の位置に必要な要素が含まれていれば、有効で一意の URN を作成する任意の方法で URN を指定できます。オプションで指定された要素は空白のままにしておくことも、リソースを識別して URN を一意にする方法で指定することもできます。例えば：

- CloudMirror レプリケーション:

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

StorageGRIDでホストされているCloudMirrorエンドポイントの場合、次の文字で始まる有効な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
```

ローカルにホストされた検索統合エンドポイントの場合、 `domain-name`エンドポイントの URN が一意である限り、要素には任意の文字列を指定できます。

プラットフォーム サービス エンドポイントを作成する

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 つ作成する必要があります。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されま

した。

- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。
- 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が作成されました。
  - 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: 宛先クラスターがインデックスを自動的に作成するように構成されていない場合の Elasticsearch インデックス。
- 宛先リソースに関する情報は次の通りです。
  - URI (Uniform Resource Identifier) 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予定の場合は、グリッド管理者に問い合わせて、入力する必要がある値を確認してください。

  - ユニークリソース名 (URN)

    "プラットフォーム サービス エンドポイントの URN を指定します"

  - 認証資格情報（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では、次の資格情報を使用できます。

- アクセスキー: アクセスキーIDとシークレットアクセスキー
- 基本的なHTTP: ユーザー名とパスワード

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 エンドポイントの場合、次の認証情報を使用できます。

- アクセスキー: アクセスキーIDとシークレットアクセスキー
- CAP (C2S アクセス ポータル): 一時資格情報 URL、サーバーおよび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キー 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、次の認証情報を使用できます。

- アクセスキー: 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、次の資格情報を使用できます。

- SASL/PLAIN: ユーザー名とパスワード
- SASL/SCRAM-SHA-256: ユーザー名とパスワード
- SASL/SCRAM-SHA-512: ユーザー名とパスワード

    - セキュリティ証明書（カスタム CA 証明書を使用している場合）

- Elasticsearch セキュリティ機能が有効になっている場合は、接続テストのためのクラスター監視権限と、ドキュメント更新のためのインデックス書き込み権限またはインデックスとインデックス削除の両方の権限が付与されます。

手順

1. ストレージ **(S3)** > プラットフォーム サービス 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、エンドポイント ページにリストされるときにエンドポイント名の横に表示されるため、名前にその情報を含める必要はありません。

4. **URI** フィールドに、エンドポイントの一意のリソース識別子 (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の場合はポート443、HTTP URIの場合はポート80（ほとんどのエンドポイント）
- HTTPS および HTTP URI 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高可用性（HA）グループの仮想IP（VIP）のDNSエントリを表し、 `10443`ロード バランサーのエンドポイントで定義されたポートを表します。

> 可能な限り、単一障害点を回避するために、負荷分散ノードの 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。 **URN** フィールドにバケット名を含めます。

5. エンドポイントの一意のリソース名 (URN) を入力します。

> エンドポイントを作成した後は、エンドポイントの URN を変更することはできません。

6. *続行*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資格情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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 スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー
基本的なHTTP	ユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • 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 エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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 スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー
CAP（C2Sアクセスポータル）	証明書とキーを使用して、宛先への接続を認証します。	• 一時認証情報URL • サーバーCA証明書（PEMファイルのアップロード） • クライアント証明書（PEMファイルのアップロード） • 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） • クライアントの秘密鍵のパスフレーズ（オプション）

Amazon SNSエンドポイント

Amazon SNS エンドポイントの認証情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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 スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー

Kafkaエンドポイント

Kafka エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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ー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード
SASL/SCRAM-SHA-256	チャレンジ レスポンス プロトコルと SHA-256 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード
SASL/SCRAM-SHA-512	チャレンジ レスポンス プロトコルと SHA-512 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード

ユーザー名とパスワードが Kafka クラスターから取得された委任トークンから派生している場合は、委任された認証を使用する を選択します。

8. *続行*を選択します。
9. *サーバーの検証*のラジオ ボタンを選択して、エンドポイントへの TLS 接続を検証する方法を選択します。

証明書検証の種類	説明
カスタムCA証明書を使用する	カスタム 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コピーして、[CA 証明書] テキスト ボックスに貼り付けます。
オペレーティング システムの CA 証明書を使用する	接続を保護するには、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 証明書を使用します。
証明書を検証しない	TLS 接続に使用される証明書が検証されていません。このオプションは安全ではありません。

10. *エンドポイントのテストと作成*を選択します。
    - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功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に失敗した場合、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、*エンドポイントのテストと作成*を選択します。

> 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場合、エンドポイントの作成は失敗します。 StorageGRID管理者に問い合わせてください。

エンドポイントを構成したら、その URN を使用してプラットフォーム サービスを構成できます。

関連情報

- "プラットフォーム サービス エンドポイントの URN を指定します"
- "CloudMirrorレプリケーションを構成する"
- "イベント通知の設定"
- "検索統合サービスを構成する"

プラットフォーム サービス エンドポイントのテスト接続

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、エンドポイントの接続をテストして、宛先リソースが存在し、指定した資格情報を使用してアクセスできることを検証できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

タスク概要

StorageGRID は、資格情報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 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、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

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。

3. *テスト接続*を選択します。

   - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功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に失敗した場合、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、[構成] を選択して情報を更新します。次に、[テストして変更を保存]を選択します。

プラットフォーム サービス エンドポイントを編集する

プラットフォーム サービス エンドポイントの構成を編集して、名前、URI、その他の詳細を変更できます。たとえば、期限切れの資格情報を更新したり、フェイルオーバーのためにバックアップ Elasticsearch インデックスを指すように URI を変更したりする必要がある場合があります。プラットフォーム サービス エンドポイントの URN を変更することはできません。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

手順

1. ストレージ **(S3)** > プラットフォーム サービス 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、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

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. *構成*を選択します。
4. 必要に応じて、エンドポイントの構成を変更します。

   エンドポイントを作成した後は、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、**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 キーを貼り付けて、必要に応じてキーを変更します。変更をキャンセルする必要がある場合は、「**S3** キー編集を元に戻す」を選択します。
- CAP (C2S アクセス ポータル) 認証の場合、一時的な資格情報の URL またはオプションのクライアント秘密キーのパスフレーズを変更し、必要に応じて新しい証明書とキー ファイルをアップロードします。

> クライアントの秘密キーは、OpenSSL 暗号化形式または暗号化されていない秘密キー形式である必要があります。

d. 必要に応じて、サーバーの検証方法を変更します。

5. *テストして変更を保存*を選択します。
   - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功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に失敗した場合、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、[テストして変更を保存] 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する

関連付けられているプラットフォーム サービスを使用したくなくなった場合は、エンドポイントを削除できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

手順

1. ストレージ **(S3)** > プラットフォーム サービス 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、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

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、その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付けられたプラットフォーム サービスが無効になります。まだ完了していないリクエストはすべて削除されます。削除された URN を参照しないようにバケット構成を変更するまで、新しいリクエストは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。

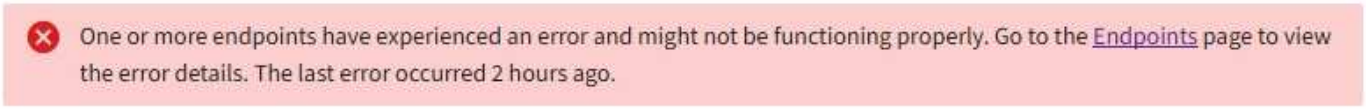
4. *エンドポイントの削除*を選択します。

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

StorageGRID がプラットフォーム サービス エンドポイントとの通信を試行する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。プラットフォーム サービス エンドポイント ページの [最後のエラー] 列には、エラーが発生した時間が表示されます。エンドポイントの資格情報に関連付けられた権限が正しくない場合、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する

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、Tenant Manager ダッシュボードに警告メッセージが表示されます。エラーの詳細を確認するには、プラットフォーム サービス エンドポイント ページにアクセスしてください。



ダッシュボードに表示されるのと同じエラーが、プラットフォーム サービス エンドポイント ページの上部にも表示されます。より詳細なエラー メッセージを表示するには:

手順

1. エンドポイントのリストから、エラーが発生している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のみが表示され、エラーが発生した時間を示します。赤いXアイコンを含むエラー過去 7 日以内に発生しました。

エラーがまだ発生しているか確認する

一部のエラーは、解決された後も 最後のエラー 列に引き続き表示される場合があります。エラーが最新であるかどうかを確認するか、解決済みのエラーをテーブルから強制的に削除するには、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。

*テスト接続*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し、現在の資格情報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を解決する

エンドポイントの詳細ページの 最後のエラー メッセージを使用すると、エラーの原因を特定するのに役立ちます。エラーによっては、問題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があります。たと

えば、適切なアクセス権限がないかアクセス キーの有効期限が切れているためにStorageGRID が宛先 S3 バケットにアクセスできない場合、CloudMirroring エラーが発生する可能性があります。メッセージは「エンドポイント資格情報または宛先アクセスのいずれかを更新する必要があります」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、[テストして変更を保存] 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、現在の資格情報でアクセス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構成を編集します。
4. 接続 > *接続テスト*を選択します。

権限が不十分なエンドポイント認証情報

StorageGRID は、プラットフォーム サービス エンドポイントを検証する際に、エンドポイントの資格情報を使用して宛先リソースに接続できることを確認し、基本的な権限チェックを実行します。ただし、StorageGRID は、特定のプラットフォーム サービス操作に必要なすべての権限を検証するわけではありません。このため、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) が発生した場合は、エンドポイントの資格情報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する"
- "プラットフォーム サービス エンドポイントのテスト接続"
- "プラットフォーム サービス エンドポイントを編集する"

著作権に関する情報

商標に関する情報