負荷分散の管理
StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid-116/admin/managing-load-balancing.html on April 10, 2024. Always check docs.netapp.com for the latest.

目次

負荷分散の管理 1
ロードバランシングの管理：概要 1
ロードバランシングの仕組み - ロードバランササービス 1
ロードバランサエンドポイントを設定する 2
ロードバランシングの仕組み - CLB サービス（廃止） 12

負荷分散の管理

ロードバランシングの管理：概要

StorageGRID のロードバランシング機能を使用して、 S3 / Swift クライアントからの取り込み / 読み出しワークロードを処理できます。ロードバランシングは、複数のストレージノードにワークロードと接続を分散することで、速度と接続容量を最大化します。

次の方法でクライアントワークロードの負荷を分散できます。

- 管理ノードとゲートウェイノードにインストールされているロードバランササービスを使用します。ロードバランササービスはレイヤ 7 のロードバランシングを提供し、クライアント要求の TLS ターミネーション、要求の検査、およびストレージノードへの新しいセキュアな接続の確立を実施します。これは推奨されるロードバランシングメカニズムです。

  を参照してください ロードバランシングの仕組み - ロードバランササービス。

- ゲートウェイノードにのみインストールされている、廃止された Connection Load Balancer （ CLB ）サービスを使用します。CLB サービスはレイヤ 4 のロードバランシングを提供し、リンクコストをサポートします。

  を参照してください ロードバランシングの仕組み - CLB サービス（廃止）。

- サードパーティ製ロードバランサを統合します。詳細については、ネットアップのアカウント担当者にお問い合わせください。

ロードバランシングの仕組み - ロードバランササービス

ロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランシングを有効にするには、Grid Manager を使用してロードバランサエンドポイントを設定する必要があります。

ロードバランサエンドポイントは管理ノードまたはゲートウェイノードにのみ設定できます。これらのノードタイプにはロードバランササービスが含まれているためです。ストレージノードまたはアーカイブノードにエンドポイントを設定することはできません。

各ロードバランサエンドポイントは、ポート、ネットワークプロトコル（ HTTP または HTTPS ）、クライアントタイプ（ S3 または Swift ）、およびバインドモードを指定します。HTTPS エンドポイントにはサーバ証明書が必要です。バインドモードでは、エンドポイントポートのアクセスを次のように制限できます。

- 特定のハイアベイラビリティ（ HA ）グループの仮想 IP アドレス（ VIP ）
- 特定の管理ノードとゲートウェイノードの特定のネットワークインターフェイス

ポートに関する考慮事項

クライアントは、ロードバランササービスを実行しているノードに設定された任意のエンドポイントにアクセスできます。ただしポート 80 と 443 は例外で、管理ノードではこれらのノードが予約されているため、これらのポートに設定されたエンドポイントはゲートウェイノードでのみロードバランシング処理をサポートしま

す。

ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。の手順に従います ポートの再マッピングを削除。

> CLB サービスは廃止されました。

CPU の可用性

S3 / Swift トラフィックをストレージノードに転送する際、各管理ノードおよびゲートウェイノード上のロードバランササービスは独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。ノード CPU 負荷情報は数分ごとに更新されますが、重み付けがより頻繁に更新される場合があります。ノードの使用率が 100% になった場合や、ノードの利用率のレポートに失敗した場合でも、すべてのストレージノードには最小限のベースとなる重みの値が割り当てられます。

CPU の可用性に関する情報が、ロードバランササービスが配置されているサイトに制限されている場合があります。

ロードバランサエンドポイントを設定する

ゲートウェイノードと管理ノードの StorageGRID ロードバランサに接続する際に使用できるポートとネットワークプロトコル S3 / Swift クライアントは、ロードバランサエンドポイントで決まります。

必要なもの

- を使用して Grid Manager にサインインします サポートされている Web ブラウザ。
- Root アクセス権限が割り当てられている。
- ロードバランサエンドポイントに使用するポートを再マッピングした場合は、を使用します ポートの再マッピングを削除しました。
- 使用するハイアベイラビリティ（ HA ）グループを作成しておきます。HA グループを推奨しますが、必須ではありません。を参照してください ハイアベイラビリティグループを管理します。
- ロードバランサエンドポイントがで使用される場合 S3 Select 用の S3 テナントベアメタルノードの IP アドレスまたは FQDN を使用しないでください。S3 Select に使用するロードバランサエンドポイントには、 SG100 または SG1000 アプライアンスと VMware ベースのソフトウェアノードのみが許可されます。
- 使用する VLAN インターフェイスを設定しておきます。を参照してください VLAN インターフェイスを設定します。
- HTTPS エンドポイントを作成する場合（推奨）は、サーバ証明書の情報が必要です。

  > エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

  - 証明書をアップロードするには、サーバ証明書、証明書の秘密鍵、および必要に応じて CA バンドルが必要です。

- 証明書を生成するには、 S3 または Swift クライアントがエンドポイントへのアクセスに使用するすべてのドメイン名と IP アドレスが必要です。また、件名（識別名）も知っている必要があります。
- StorageGRID の S3 および Swift API 証明書（ストレージノードへの直接の接続にも使用できます）を使用する場合は、デフォルトの証明書を外部の認証局によって署名されたカスタム証明書に置き換えておく必要があります。を参照してくださいS3 および Swift API 証明書を設定する。

  証明書では、ワイルドカードを使用して、ロードバランササービスを実行しているすべての管理ノードとゲートウェイノードの完全修飾ドメイン名を表すことができます。たとえば '*.storagegrid.*example*.com は '*wildcard を使用して 'adm1.storagegrid.*example*.com と gn1.storagegrid.*example*.com を表しますを参照してください S3 API エンドポイントのドメイン名を設定。

ロードバランサエンドポイントを作成します

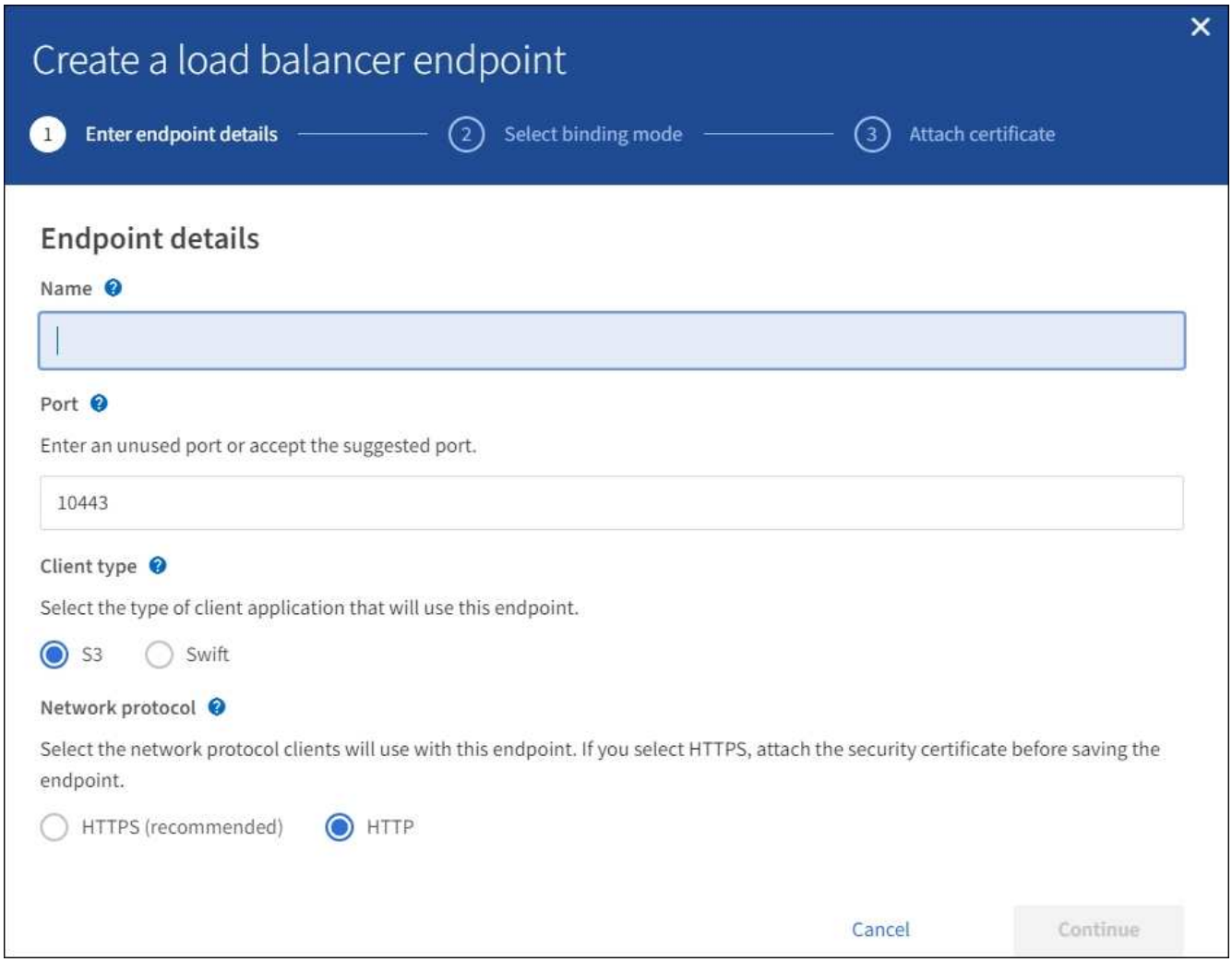
各ロードバランサエンドポイントは、ポート、クライアントタイプ（ S3 または Swift ）、およびネットワークプロトコル（ HTTP または HTTPS ）を指定します。

ウィザードにアクセスします

1. [* configuration * > * Network * > * Load Balancer Endpoints *] を選択します。
2. 「 * Create * 」を選択します。

エンドポイントの詳細を入力します

1. エンドポイントの詳細を入力します。



フィールド	説明
名前	エンドポイントのわかりやすい名前。ロードバランサエンドポイントのページのテーブルに表示されます。
ポート	クライアントが管理ノードおよびゲートウェイノード上のロードバランササービスへの接続に使用するポート。 推奨されるポート番号をそのまま使用するか、別のグリッドサービスで使用されていない外部ポートを入力します。1~65535 の値を入力します。 「 * 80 * 」または「 * 443 * 」と入力すると、エンドポイントはゲートウェイノードにのみ設定されます。これらのポートは管理ノードで予約されています。 を参照してください ネットワークのガイドライン 外部ポートについては、を参照してください。
クライアントタイプ	このエンドポイントを使用するクライアントアプリケーションのタイプ。 * S3 * または * Swift * 。

フィールド	説明
ネットワークプロトコル	クライアントがこのエンドポイントに接続するときに使用するネットワークプロトコル。 • セキュアな TLS 暗号化通信を実現するには、「 * HTTPS * 」を選択します（推奨）。エンドポイントを保存するには、セキュリティ証明書を接続する必要があります。 • セキュアで暗号化されていない通信を行うには、「 * HTTP 」を選択します非本番環境のグリッドにのみ HTTP を使用してください。

2. 「 * Continue * 」を選択します。

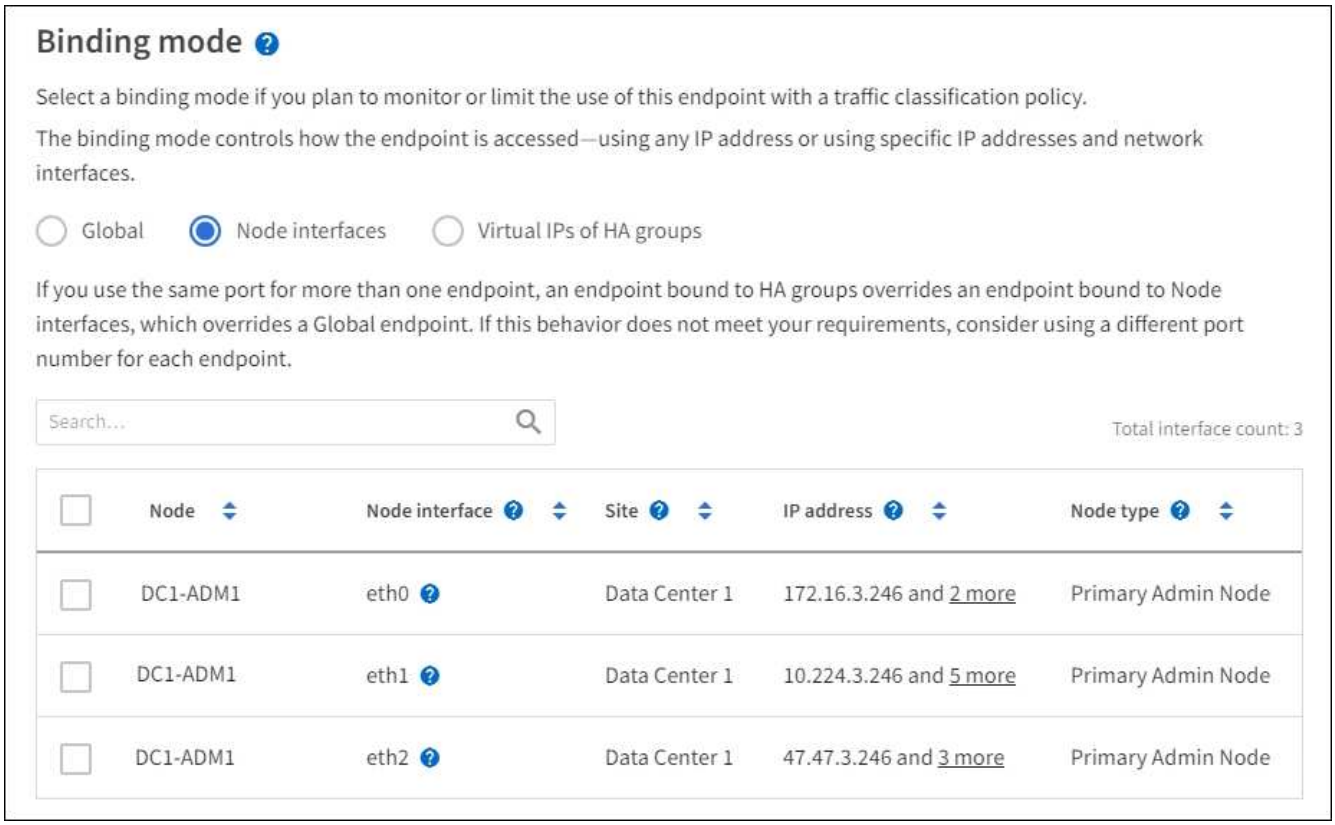
バインドモードを選択します

1. エンドポイントへのアクセス方法を制御するには、エンドポイントのバインディングモードを選択します。

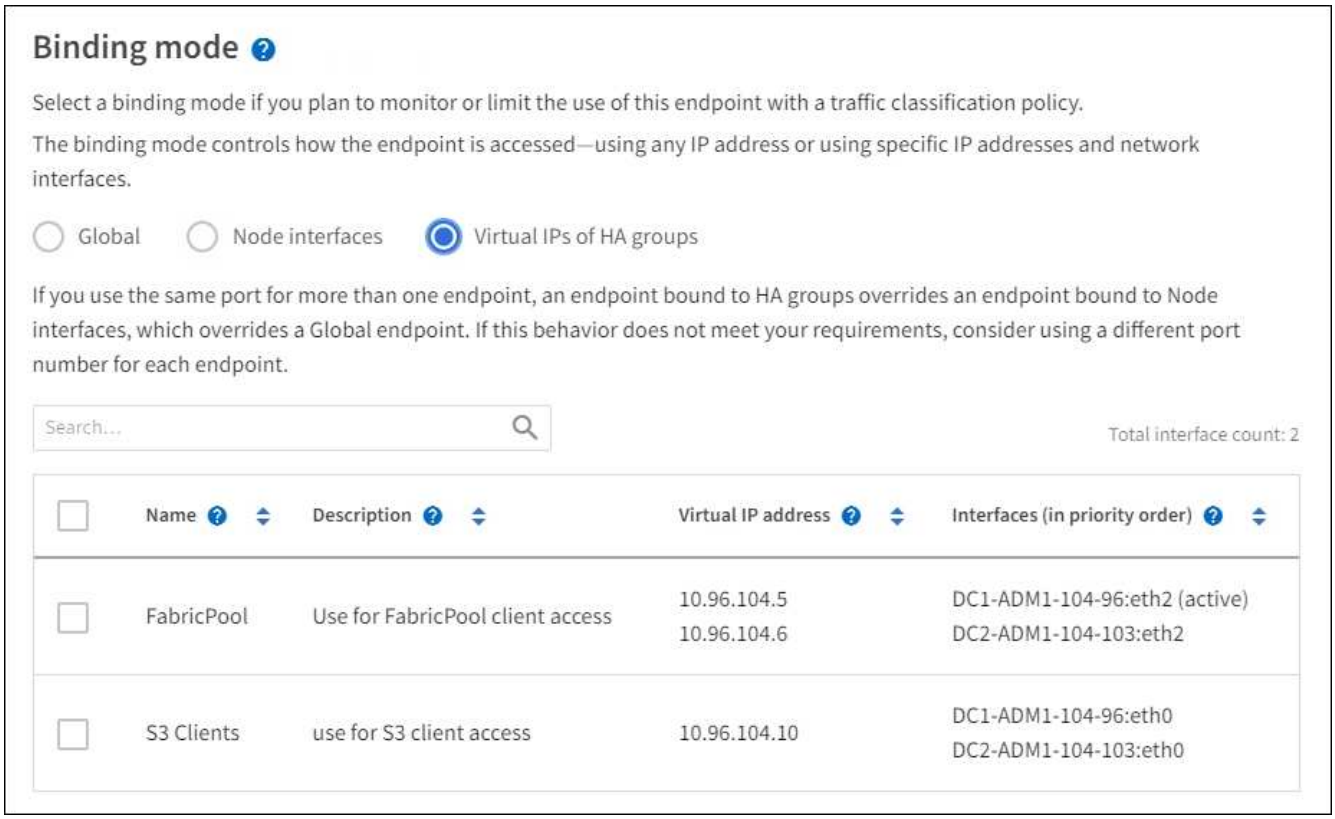
オプション	説明
グローバル（デフォルト）	クライアントは、ネットワーク上の任意の HA グループの完全修飾ドメイン名（ FQDN ）、ゲートウェイノードまたは管理ノードの IP アドレス、または仮想 IP アドレスを使用してエンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がある場合を除き、 * グローバル * 設定（デフォルト）を使用します。
ノードインターフェイス	クライアントは、選択したノードの IP アドレスとネットワークインターフェイスを使用してこのエンドポイントにアクセスする必要があります。
HA グループの仮想 IP	クライアントは、 HA グループの仮想 IP アドレスを使用してこのエンドポイントにアクセスする必要があります。 このバインドモードのエンドポイントは、エンドポイントに対して選択した HA グループが重ならないかぎり、すべて同じポート番号を使用できます。 このモードのエンドポイントは、エンドポイントに対して選択したインターフェイスが重ならないかぎり、すべて同じポート番号を使用できます。

> 複数のエンドポイントで同じポートを使用する場合、 HA グループの仮想 IP * モードを使用するエンドポイントは、 * ノードインターフェイス * モードを使用するエンドポイントよりも優先されます。これにより、 * グローバル * モードを使用するエンドポイントは無効になります。

2. ノードインターフェイス * を選択した場合は、このエンドポイントに関連付ける管理ノードまたはゲートウェイノードごとに 1 つ以上のノードインターフェイスを選択します。



3. HA グループの仮想 IP * を選択した場合は、 1 つ以上の HA グループを選択します。



4. HTTP * エンドポイントを作成する場合、証明書を接続する必要はありません。Create * を選択して、新しいロードバランサエンドポイントを追加します。次に、に進みます 完了後。それ以外の場合は、「 * Continue * 」を選択して証明書を添付します。

証明書を添付します

1. * HTTPS * エンドポイントを作成する場合は、エンドポイントに接続するセキュリティ証明書のタイプを選択します。

   この証明書は、 S3 および Swift クライアントと、管理ノードまたはゲートウェイノード上のロードバランササービスの間の接続を保護します。

   - * 証明書のアップロード * 。アップロードするカスタム証明書がある場合は、このオプションを選択します。
   - * 証明書の生成 * 。カスタム証明書の生成に必要な値がある場合は、このオプションを選択します。
   - * StorageGRID S3 および Swift 証明書を使用 * 。グローバルな S3 および Swift API 証明書を使用する場合は、このオプションを選択します。この証明書は、ストレージノードへの直接接続にも使用できます。

     グリッド CA によって署名されたデフォルトの S3 および Swift API 証明書を、外部の認証局によって署名されたカスタム証明書で置き換えないと、このオプションは選択できません。を参照してくださいS3 および Swift API 証明書を設定する。

2. StorageGRID S3 および Swift 証明書を使用しない場合は、証明書をアップロードまたは生成します。

証明書をアップロードする

a. [証明書のアップロード] を選択します。

b. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ： PEM エンコードのカスタムサーバ証明書ファイル。
- **Certificate private key**: カスタムサーバ証明書の秘密鍵ファイル (`.key`) 。

> EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局（ CA ）の証明書を含む単一のオプションファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

c. [* 証明書の詳細 *] を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合は、各証明書が独自のタブに表示されます。

- 証明書ファイルを保存するには、 * 証明書のダウンロード * を選択します。証明書バンドルを保存するには、 * CA バンドルのダウンロード * を選択します。

  証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「 .pem 」を付けて保存します。

例： 'storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. 「 * Create * 」を選択します。+ ロードバランサエンドポイントが作成された。カスタム証明書は、 S3 / Swift クライアントとエンドポイントの間の以降のすべての新しい接続に使用されます。

証明書の生成

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

- * Domain name * ：証明書に含める 1 つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。
- **IP** ：証明書に含める 1 つ以上の IP アドレス。
- * 件名 * ：証明書所有者の X.509 サブジェクトまたは識別名（ DN ）。
- **days valid**: 証明書の有効期限が切れる作成後の日数

c. [*Generate （生成）] を選択します

d. 生成された証明書のメタデータを表示するには、 [証明書の詳細] を選択します。

- 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

  証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「 .pem 」を付けて保存します。

例： 'storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

e. 「 * Create * 」を選択します。

ロードバランサエンドポイントが作成されます。カスタム証明書は、 S3 / Swift クライアントとこのエンドポイントの間の以降のすべての新しい接続に使用されます。

[終了後**]**をクリックします

1. ドメインネームシステム（ DNS ）を使用する場合は、 DNS に、クライアントが接続に使用する各 IP アドレスに StorageGRID の完全修飾ドメイン名を関連付けるレコードが含まれていることを確認します。

   DNS レコードに入力する IP アドレスは、負荷分散ノードの HA グループを使用しているかどうかによって異なります。

   - HAグループを設定した場合、クライアントはそのHAグループの仮想IPアドレスに接続します。
   - HAグループを使用しない場合、クライアントはいずれかのゲートウェイノードまたは管理ノードのIPアドレスを使用してStorageGRID ロードバランササービスに接続します。

     また、 DNS レコードが、ワイルドカード名を含む、必要なすべてのエンドポイントドメイン名を参照していることを確認する必要があります。

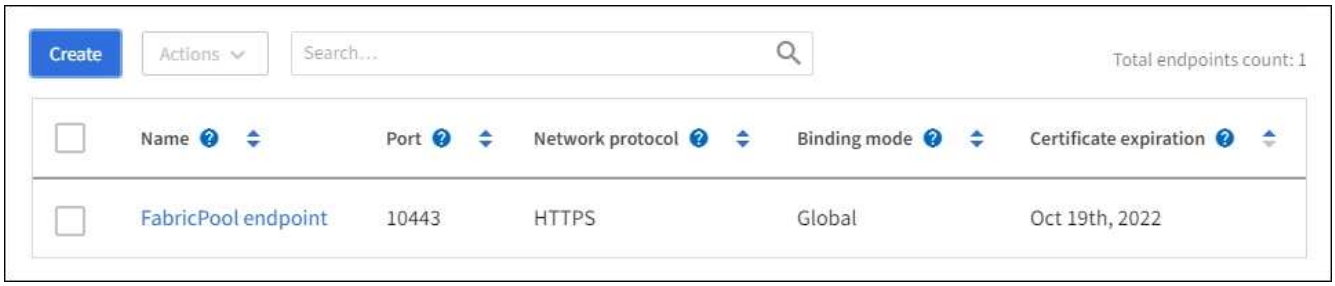
2. エンドポイントへの接続に必要な情報を S3 クライアントと Swift クライアントに提供します。
   - ポート番号
   - 完全修飾ドメイン名または IP アドレス
   - 必要な証明書の詳細

ロードバランサエンドポイントを表示および編集します

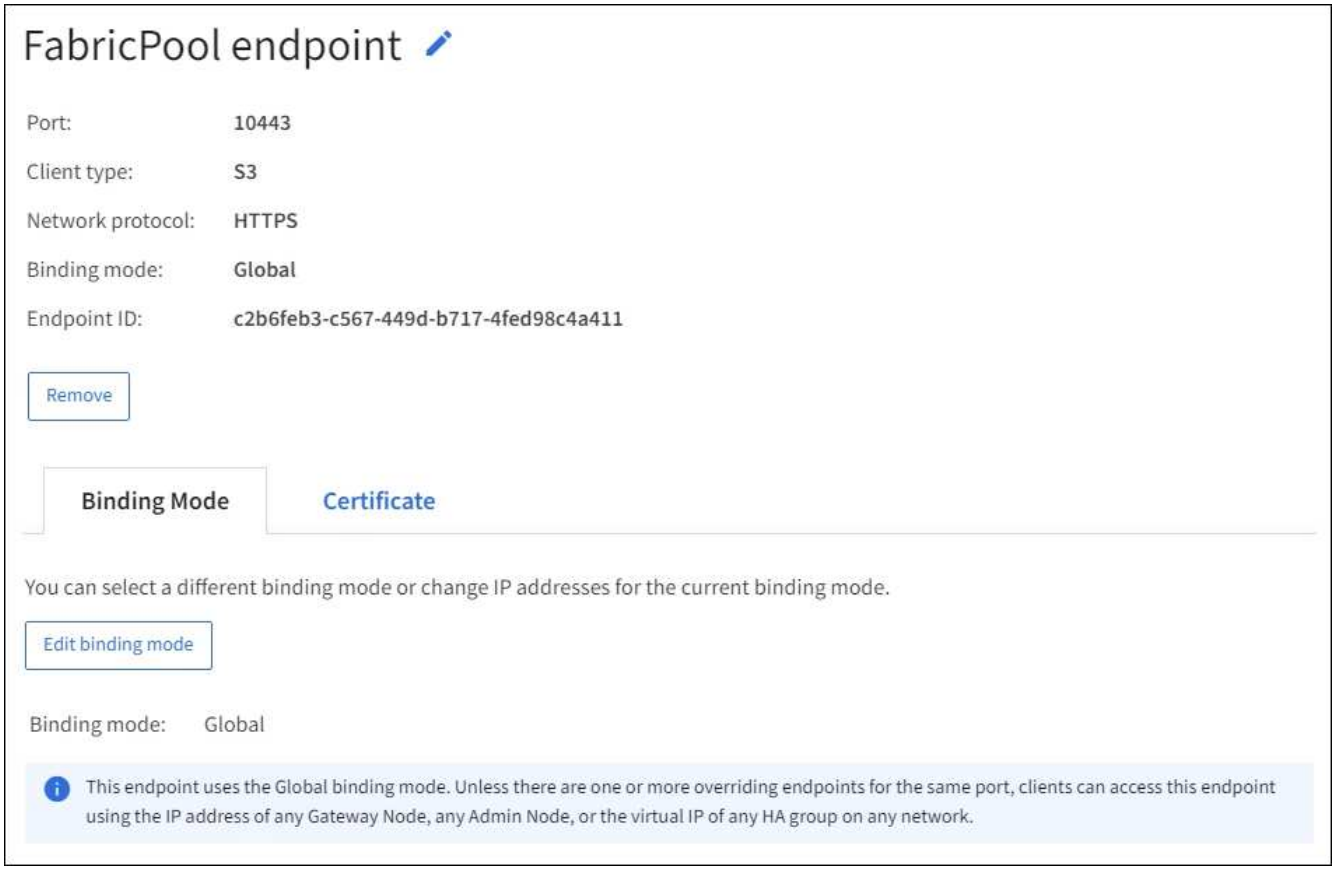
既存のロードバランサエンドポイントの詳細を表示できます。これには、セキュアなエンドポイントの証明書メタデータも含まれます。また、エンドポイントの名前またはバインドモードを変更して、関連付けられている証明書を更新することもできます。

サービスタイプ（ S3 または Swift ）、ポート、またはプロトコル（ HTTP または HTTPS ）を変更することはできません。

- すべてのロードバランサエンドポイントの基本情報を表示するには、 Load Balancer Endpoints ページのテーブルを確認します。



- 証明書メタデータを含む、特定のエンドポイントに関するすべての詳細を表示するには、テーブルでエンドポイントの名前を選択します。



- エンドポイントを編集するには、 [ロードバランサエンドポイント（ Load Balancer Endpoints ）] ページの [* アクション * （ * Actions * ）] メニューを使用するか、特定のエンドポイントの詳細ページを使用します。

> エンドポイントの編集後、変更がすべてのノードに適用されるまでに最大 15 分かかる場合があります。

タスク	[アクション] メニュー	詳細ページ
エンドポイント名を編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * > * エンドポイント名の編集 *] を選択します。 c. 新しい名前を入力します。 d. [保存（ Save ）] を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. 編集アイコンを選択します 。 c. 新しい名前を入力します。 d. [保存（ Save ）] を選択します。
エンドポイントバインドモードを編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * （ Actions * ）] > [* エンドポイントバインドモードの編集（ Edit Endpoint binding mode ）] c. 必要に応じて、バインドモードを更新します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. 「 * バインドモードを編集」を選択します。 c. 必要に応じて、バインドモードを更新します。 d. 「変更を保存」を選択します。
エンドポイント証明書を編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * > * エンドポイント証明書の編集 *] を選択します。 c. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバルな S3 および Swift 証明書の使用を開始します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. [* 証明書 *] タブを選択します。 c. [証明書の編集] を選択します。 d. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバルな S3 および Swift 証明書の使用を開始します。 e. 「変更を保存」を選択します。

ロードバランサエンドポイントを削除する

[* アクション * （ Actions * ）] メニューを使用して 1 つ以上のエンドポイントを削除するか、または詳細ページから 1 つのエンドポイントを削除できます。

> クライアントの停止を回避するには、影響を受ける S3 または Swift クライアントアプリケーションを更新してからロードバランサエンドポイントを削除します。各クライアントを更新して、別のロードバランサエンドポイントに割り当てられたポートを使用して接続します。必要な証明書情報も必ず更新してください。

- 1 つ以上のエンドポイントを削除するには、次の手順
  a. Load Balancer ページで、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。
  b. * アクション * > * 削除 * を選択します。
  c. 「 * OK 」を選択します。

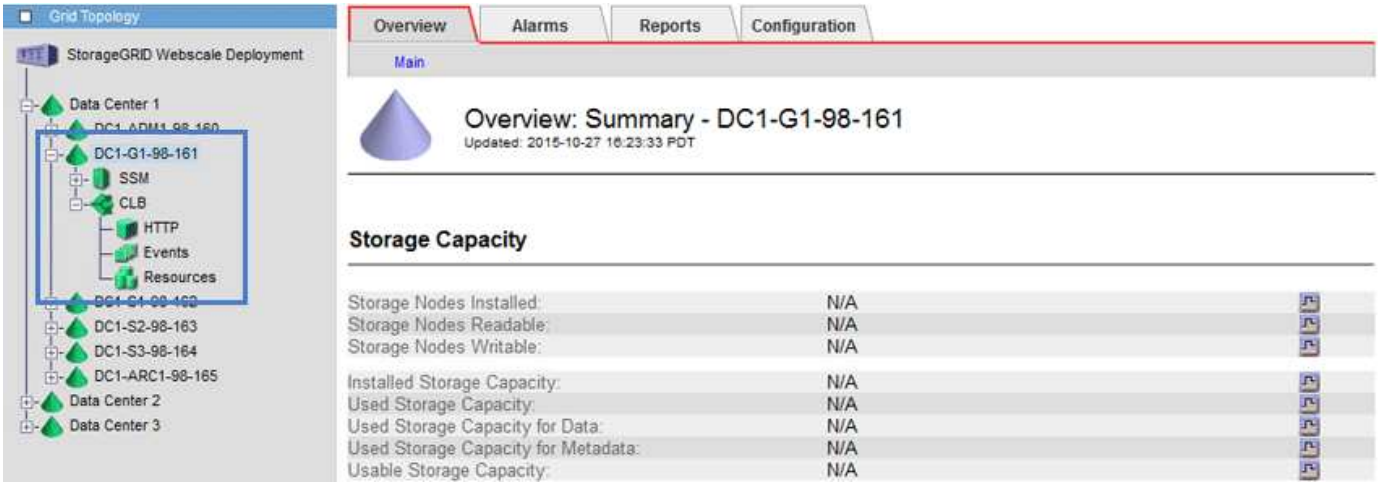
- 詳細ページから 1 つのエンドポイントを削除します。
  a. Load Balancer （ロードバランサ）ページから。エンドポイント名を選択します。
  b. 詳細ページで「 * 削除」を選択します。
  c. 「 * OK 」を選択します。

ロードバランシングの仕組み - CLB サービス（廃止）

ゲートウェイノード上の Connection Load Balancer （ CLB ）サービスは廃止されました。ロードバランササービスが推奨されるロードバランシングメカニズムになりました。

CLB サービスはレイヤ 4 ロードバランシングを使用して、可用性、システムの負荷、および管理者が設定したリンクコストに基づいて、クライアントアプリケーションからの受信 TCP ネットワーク接続を最適なストレージノードに分散します。最適なストレージノードが選択されると、 CLB サービスは双方向のネットワーク接続を確立し、選択されたノードとの間でトラフィックを転送します。CLB は、受信ネットワーク接続を転送するときにグリッドネットワーク設定を考慮しません。

CLB サービスに関する情報を表示するには、 * support * > * Tools * > * Grid topology * を選択し、次に * CLB * およびその下のオプションを選択できるようになるまでゲートウェイノードを拡張します。



CLB サービスを使用する場合は、 StorageGRID システムのリンクコストを設定することを検討してください。

- リンクコストとは
- リンクコストを更新します

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権を有し、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権については、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。