負荷分散を管理する
StorageGRID software

NetApp
December 03, 2025

目次

負荷分散を管理する

負荷分散に関する考慮事項

負荷分散を使用して、S3 クライアントからの取り込みおよび取得ワークロードを処理できます。

負荷分散とは何ですか?

クライアント アプリケーションがStorageGRIDシステムからデータを保存または取得する場合、StorageGRID はロード バランサを使用して取り込みおよび取得のワークロードを管理します。負荷分散は、複数のストレージ ノードにワークロードを分散することで、速度と接続容量を最大化します。

StorageGRIDロード バランサ サービスは、すべての管理ノードとすべてのゲートウェイ ノードにインストールされ、レイヤー 7 のロード バランシングを提供します。クライアント要求のトランスポート層セキュリティ (TLS) 終了を実行し、要求を検査し、ストレージ ノードへの新しい安全な接続を確立します。

各ノードのロード バランサ サービスは、クライアント トラフィックをストレージ ノードに転送するときに独立して動作します。重み付けプロセスを通じて、ロード バランサ サービスは、CPU 可用性が高いストレージ ノードに、より多くの要求をルーティングします。

> 推奨される負荷分散メカニズムとしてはStorageGRID Load Balancer サービスがありますが、代わりにサードパーティのロード バランサを統合することもできます。詳細については、NetAppのアカウント担当者にお問い合わせいただくか、 "TR-4626: StorageGRIDサードパーティおよびグローバルロードバランサー" 。

負荷分散ノードはいくつ必要ですか?

一般的なベスト プラクティスとして、 StorageGRIDシステムの各サイトには、ロード バランサ サービスを備えた 2 つ以上のノードを含める必要があります。たとえば、サイトには 2 つのゲートウェイ ノード、または管理ノードとゲートウェイ ノードの両方が含まれる場合があります。サービス アプライアンス、ベア メタル ノード、仮想マシン (VM) ベースのノードのいずれを使用しているかに関係なく、各負荷分散ノードに適切なネットワーク、ハードウェア、または仮想化インフラストラクチャがあることを確認します。

ロードバランサーエンドポイントとは何ですか?

ロード バランサ エンドポイントは、受信および送信クライアント アプリケーション要求がロード バランサ サービスを含むノードにアクセスするために使用するポートとネットワーク プロトコル (HTTPS または HTTP) を定義します。エンドポイントは、クライアント タイプ (S3)、バインディング モード、およびオプションで許可またはブロックされたテナントのリストも定義します。

ロード バランサ エンドポイントを作成するには、[構成] > [ネットワーク] > [ロード バランサ エンドポイント] を選択するか、 FabricPoolおよび S3 セットアップ ウィザードを完了します。手順については、以下をご覧ください。

- "ロードバランサのエンドポイントを構成する"
- "S3セットアップウィザードを使用する"
- "FabricPoolセットアップウィザードを使用する"

港湾に関する考慮事項

ロード バランサー エンドポイントのポートは、最初に作成するエンドポイントではデフォルトで 10433 に設定されますが、1 ～ 65535 の間の未使用の外部ポートを任意に指定できます。ポート 80 または 443 を使用する場合、エンドポイントはゲートウェイ ノード上のロード バランサ サービスのみを使用します。これらのポートは管理ノードで予約されています。複数のエンドポイントに同じポートを使用する場合は、エンドポイントごとに異なるバインディング モードを指定する必要があります。

他のグリッド サービスによって使用されるポートは許可されません。参照"ネットワークポートリファレンス"。

ネットワークプロトコルに関する考慮事項

ほとんどの場合、クライアント アプリケーションとStorageGRID間の接続には、トランスポート層セキュリティ (TLS) 暗号化を使用する必要があります。 TLS 暗号化なしでのStorageGRIDへの接続はサポートされていますが、特に実稼働環境では推奨されません。 StorageGRIDロード バランサ エンドポイントのネットワーク プロトコルを選択するときは、**HTTPS** を選択する必要があります。

ロードバランサのエンドポイント証明書に関する考慮事項

ロード バランサー エンドポイントのネットワーク プロトコルとして **HTTPS** を選択した場合は、セキュリティ証明書を提供する必要があります。ロード バランサ エンドポイントを作成するときは、次の 3 つのオプションのいずれかを使用できます。

- 署名された証明書をアップロードします **(**推奨**)**。この証明書は、公的に信頼された証明機関 (CA) またはプライベート証明機関 (CA) によって署名できます。接続を保護するために公的に信頼された CA サーバー証明書を使用するのがベスト プラクティスです。生成された証明書とは対照的に、CA によって署名された証明書は中断することなくローテーションできるため、有効期限の問題を回避するのに役立ちます。

  ロード バランサ エンドポイントを作成する前に、次のファイルを取得する必要があります。

  - カスタム サーバー証明書ファイル。
  - カスタム サーバー証明書の秘密キー ファイル。
  - オプションで、各中間発行証明機関からの証明書の CA バンドル。
- 自己署名証明書を生成します。
- グローバル**StorageGRID S3** 証明書を使用します。ロード バランサーのエンドポイントにこの証明書を選択する前に、この証明書のカスタム バージョンをアップロードまたは生成する必要があります。見る"S3 API証明書を設定する"。

どのような値が必要ですか**?**

証明書を作成するには、S3 クライアント アプリケーションがエンドポイントにアクセスするために使用するすべてのドメイン名と IP アドレスを知っておく必要があります。

証明書の **Subject DN** (識別名) エントリには、クライアント アプリケーションがStorageGRIDに使用する完全修飾ドメイン名を含める必要があります。例えば：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

必要に応じて、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。例えば、`*.storagegrid.example.com` *ワイルドカードを使用して `adm1.storagegrid.example.com` そして `gn1.storagegrid.example.com`。

S3仮想ホスト形式のリクエストを使用する場合は、証明書には各リクエストの*別名*エントリも含める必要があります。"S3エンドポイントドメイン名"ワイルドカード名を含め、構成したすべての名前。例えば：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

ドメイン名にワイルドカードを使用する場合は、"サーバー証明書の強化ガイドライン" 。

セキュリティ証明書内の名前ごとに DNS エントリを定義する必要もあります。

期限切れの証明書をどのように管理すればよいですか?

S3 アプリケーションとStorageGRID間の接続を保護するために使用される証明書の有効期限が切れると、アプリケーションは一時的にStorageGRIDへのアクセスを失う可能性があります。

証明書の有効期限の問題を回避するには、次のベスト プラクティスに従ってください。

- ロードバランサエンドポイント証明書の有効期限 や **S3 API** のグローバルサーバー証明書の有効期限 アラートなど、証明書の有効期限が近づいていることを警告するアラートを注意深く監視します。
- StorageGRIDと S3 アプリケーションの証明書のバージョンを常に同期させます。ロードバランサーのエンドポイントに使用される証明書を置き換えたり更新したりする場合は、S3 アプリケーションで使用される同等の証明書も置き換えたり更新したりする必要があります。
- 公的に署名された CA 証明書を使用します。 CA によって署名された証明書を使用する場合は、期限が近づいている証明書を中断せずに置き換えることができます。
- 自己署名のStorageGRID証明書を生成していて、その証明書の有効期限が近づいている場合は、既存の証明書の有効期限が切れる前に、 StorageGRIDと S3 アプリケーションの両方で証明書を手動で置き換える必要があります。

バインディングモードに関する考慮事項

バインディング モードを使用すると、ロード バランサー エンドポイントへのアクセスに使用できる IP アドレスを制御できます。エンドポイントがバインディング モードを使用する場合、クライアント アプリケーションは、許可された IP アドレスまたは対応する完全修飾ドメイン名 (FQDN) を使用する場合にのみエンドポイントにアクセスできます。他の IP アドレスまたは FQDN を使用するクライアント アプリケーションはエンドポイントにアクセスできません。

次のいずれかのバインディング モードを指定できます。

- グローバル (デフォルト): クライアント アプリケーションは、任意のゲートウェイ ノードまたは管理ノードの IP アドレス、任意のネットワーク上の任意の HA グループの仮想 IP (VIP) アドレス、または対応する FQDN を使用してエンドポイントにアクセスできます。エンドポイントのアクセシビリティを制限する必要がない限り、この設定を使用します。
- **HA** グループの仮想 **IP**。クライアント アプリケーションは、HA グループの仮想 IP アドレス (または対応する FQDN) を使用する必要があります。

- ノード インターフェース。クライアントは、選択したノード インターフェイスの IP アドレス (または対応する FQDN) を使用する必要があります。
- ノード タイプ。選択したノードのタイプに基づいて、クライアントは任意の管理ノードの IP アドレス (または対応する FQDN) または任意のゲートウェイ ノードの IP アドレス (または対応する FQDN) のいずれかを使用する必要があります。

テナントアクセスに関する考慮事項

テナント アクセスは、どのStorageGRIDテナント アカウントがロード バランサ エンドポイントを使用してバケットにアクセスできるかを制御できるオプションのセキュリティ機能です。すべてのテナントにエンドポイントへのアクセスを許可するか (デフォルト)、エンドポイントごとに許可またはブロックするテナントのリストを指定することもできます。

この機能を使用すると、テナントとそのエンドポイント間のセキュリティ分離を強化できます。たとえば、この機能を使用すると、あるテナントが所有する極秘または機密性の高い資料に他のテナントがまったくアクセスできないようにすることができます。

> アクセス制御の目的で、テナントはクライアント要求で使用されるアクセス キーから決定されます。要求の一部としてアクセス キーが提供されていない場合 (匿名アクセスの場合など)、バケット所有者を使用してテナントが決定されます。

テナントアクセスの例

このセキュリティ機能がどのように機能するかを理解するには、次の例を検討してください。

1. 次のように 2 つのロード バランサ エンドポイントを作成しました。
   - パブリック エンドポイント: ポート 10443 を使用し、すべてのテナントへのアクセスを許可します。
   - トップシークレット エンドポイント: ポート 10444 を使用し、トップシークレット テナントへのアクセスのみを許可します。他のすべてのテナントはこのエンドポイントへのアクセスをブロックされます。
2. その `top-secret.pdf`*極秘*テナントが所有するバケット内にあります。

アクセスするには `top-secret.pdf`*Top secret*テナントのユーザーはGETリクエストを発行して `https://w.x.y.z:10444/top-secret.pdf`。このテナントは 10444 エンドポイントの使用を許可されているため、ユーザーはオブジェクトにアクセスできます。ただし、他のテナントに属するユーザーが同じ URL に対して同じリクエストを発行すると、直ちにアクセス拒否メッセージが表示されます。資格情報と署名が有効であってもアクセスは拒否されます。

CPUの可用性

各管理ノードとゲートウェイ ノード上のロード バランサ サービスは、S3 トラフィックをストレージ ノードに転送するときに独立して動作します。重み付けプロセスを通じて、ロード バランサ サービスは、CPU 可用性が高いストレージ ノードに、より多くの要求をルーティングします。ノードの CPU 負荷情報は数分ごとに更新されますが、重み付けはより頻繁に更新される場合があります。ノードが 100% の使用率を報告したり、使用率を報告できなかったりする場合でも、すべてのストレージ ノードには最小の基本重み値が割り当てられます。

場合によっては、CPU の可用性に関する情報は、ロード バランサ サービスが配置されているサイトに限定されます。

ロードバランサのエンドポイントを構成する

ロード バランサー エンドポイントは、ゲートウェイおよび管理ノード上のStorageGRID ロード バランサーに接続するときに S3 クライアントが使用できるポートとネットワーク プロトコルを決定します。エンドポイントを使用して、グリッド マネージャー、テナント マネージャー、またはその両方にアクセスすることもできます。

このバージョンのドキュメント サイトから Swift の詳細は削除されました。見る "S3とSwiftクライアント接続を構成する"。

開始する前に

- グリッドマネージャ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"ルートアクセス権限"。
- あなたは、"負荷分散に関する考慮事項" 。
- ロードバランサーのエンドポイントに使用するポートを以前に再マップした場合は、"ポートの再マップを削除しました" 。
- 使用を計画している高可用性 (HA) グループを作成しました。 HA グループは推奨されますが、必須ではありません。見る"高可用性グループの管理" 。
- ロードバランサのエンドポイントが"S3 Select の S3 テナント"ただし、ベアメタル ノードの IP アドレスまたは FQDN は使用できません。 S3 Select に使用されるロードバランサーエンドポイントには、サービスアプライアンスと VMware ベースのソフトウェアノードのみが許可されます。
- 使用する予定の VLAN インターフェイスを構成しました。見る"VLANインターフェースを構成する" 。
- HTTPS エンドポイント (推奨) を作成する場合は、サーバー証明書の情報があります。

  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 分かかる場合があります。

  - 証明書をアップロードするには、サーバー証明書、証明書の秘密キー、およびオプションで CA バンドルが必要です。
  - 証明書を生成するには、S3 クライアントがエンドポイントにアクセスするため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。件名（識別名）も知っておく必要があります。
  - StorageGRID S3 API 証明書 (ストレージ ノードへの直接接続にも使用可能) を使用する場合は、デフォルトの証明書を外部証明機関によって署名されたカスタム証明書にすでに置き換えています。見る"S3 API証明書を設定する" 。

ロードバランサエンドポイントを作成する

各 S3 クライアント 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)、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。管理インターフェイス ロード バランサ エンドポイントは、ポート、インターフェイス タイプ、および信頼できないクライアント ネットワークを指定します。

ウィザードにアクセスする

手順

1. 構成 > ネットワーク > ロード バランサー エンドポイント を選択します。
2. S3 または Swift クライアントのエンドポイントを作成するには、**S3** または **Swift** クライアント タブを選択します。
3. Grid Manager、Tenant Manager、またはその両方にアクセスするためのエンドポイントを作成するには、*管理インターフェイス*タブを選択します。
4. *作成*を選択します。

エンドポイントの詳細を入力してください

手順

1. 適切な手順を選択して、作成するエンドポイントの種類の詳細を入力します。

S3 または **Swift** クライアント

フィールド	説明
Name	エンドポイントの説明的な名前。ロード バランサー エンドポイント ページの表に表示されます。
ポート	負荷分散に使用するStorageGRIDポート。このフィールドは、最初に作成するエンドポイントに対してデフォルトで 10433 に設定されますが、1 ～ 65535 の未使用の外部ポートを入力できます。 **80** または **8443** を入力すると、ポート 8443 を解放していない限り、エンドポイントはゲートウェイ ノードでのみ構成されます。次に、ポート 8443 を S3 エンドポイントとして使用できるようになり、ポートはゲートウェイ ノードと管理ノードの両方で設定されます。
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**)。
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。 • 安全な TLS 暗号化通信には **HTTPS** を選択します (推奨)。エンドポイントを保存する前に、セキュリティ証明書を添付する必要があります。 • 安全性の低い暗号化されていない通信の場合は **HTTP** を選択します。非本番グリッドには HTTP のみを使用します。

管理インターフェイス

フィールド	説明
Name	エンドポイントの説明的な名前。ロード バランサー エンドポイント ページの表に表示されます。
ポート	Grid Manager、Tenant Manager、またはその両方にアクセスするために使用するStorageGRIDポート。 • グリッドマネージャー: **8443** • テナントマネージャー: **9443** • グリッドマネージャとテナントマネージャの両方: **443** 注: これらのプリセット ポートまたはその他の使用可能なポートを使用できます。
インターフェイス タイプ	このエンドポイントを使用してアクセスするStorageGRIDインターフェイスのラジオ ボタンを選択します。

フィールド	説明
信頼できないクライアントネットワーク	このエンドポイントを信頼されていないクライアント ネットワークからアクセスできるようにする場合は、[はい] を選択します。それ以外の場合は、[いいえ]を選択します。 「はい」を選択すると、信頼されていないすべてのクライアント ネットワークでポートが開きます。 注: ロード バランサ エンドポイントを作成するときにのみ、信頼されていないクライアント ネットワークに対してポートを開くか閉じるかを構成できます。

1. *続行*を選択します。

バインディングモードを選択する

手順

1. エンドポイントのバインディング モードを選択して、任意の IP アドレスまたは特定の 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エンドポイントにアクセスする方法を制御します。

   一部のバインディング モードは、クライアント エンドポイントまたは管理インターフェイス エンドポイントのいずれかで使用できます。両方のエンドポイント タイプのすべてのモードがここにリストされます。

モード	説明
グローバル（クライアントエンドポイントのデフォルト）	クライアントは、任意のゲートウェイ ノードまたは管理ノードの IP アドレス、任意のネットワーク上の任意の HA グループの仮想 IP (VIP) アドレス、または対応する FQDN 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シビリティを制限する必要がない限り、*グローバル*設定を使用します。
HAグループの仮想IP	クライアントはこのエンドポイントにアクセスするために、HA グループの仮想 IP アドレス (または対応する FQDN) を使用する必要があります。 このバインディング モードのエンドポイントは、エンドポイントに選択した HA グループが重複していない限り、すべて同じポート番号を使用できます。
ノードインターフェース	クライアントは、このエンドポイントにアクセスするために、選択したノード インターフェイスの IP アドレス (または対応する FQDN) を使用する必要があります。
ノードタイプ（クライアントエンドポイントのみ）	選択したノードのタイプに基づいて、クライアントは、このエンドポイントにアクセスするために、任意の管理ノードの IP アドレス (または対応する FQDN) または任意のゲートウェイ ノードの IP アドレス (または対応する FQDN) を使用する必要があります。

モード	説明
すべての管理ノード（管理インターフェースエンドポイントのデフォルト）	クライアントはこのエンドポイントにアクセスするために、任意の管理ノードの IP アドレス (または対応する FQDN) を使用する必要があります。

複数のエンドポイントが同じポートを使用する場合、 StorageGRID は次の優先順位を使用して、使用するエンドポイントを決定します: **HA** グループの仮想 **IP** > ノード インターフェイス > ノード タイプ > グローバル。

管理インターフェース エンドポイントを作成する場合は、管理ノードのみが許可されます。

2. **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。

   管理インターフェイス エンドポイントを作成する場合は、管理ノードにのみ関連付けられている VIP を選択します。

3. 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。
4. ノード タイプ を選択した場合は、プライマリ管理ノードと非プライマリ管理ノードの両方を含む管理ノード、またはゲートウェイ ノードのいずれかを選択します。

テナントアクセスを制御する

管理インターフェースエンドポイントは、エンドポイントがテナントマネージャーのインターフェースタイプ。

手順

1. テナント アクセス ステップでは、次のいずれかを選択します。

フィールド	説明
すべてのテナントを許可する（デフォルト）	すべてのテナント アカウントは、このエンドポイントを使用してバケットにアクセスできます。 テナント アカウントをまだ作成していない場合は、このオプションを選択する必要があります。テナント アカウントを追加した後、ロード バランサー エンドポイントを編集して、特定のアカウントを許可またはブロックできます。
選択したテナントを許可する	選択されたテナント アカウントのみがこのエンドポイントを使用してバケットにアクセスできます。
選択したテナントをブロック	選択されたテナント アカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントはこのエンドポイントを使用できます。

2. **HTTP** エンドポイントを作成する場合は、証明書を添付する必要はありません。新しいロードバランサー

エンドポイントを追加するには、[作成] を選択します。次に、終了後の操作 。それ以外の場合は、[続行] を選択して証明書を添付します。

証明書を添付する

手順

1. **HTTPS** エンドポイントを作成する場合は、エンドポイントに添付するセキュリティ証明書の種類を選択します。

   証明書は、S3 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 サービス間の接続を保護します。

   - 証明書をアップロード。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。
   - *証明書を生成*します。カスタム証明書を生成するため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 証明書を使用します*。ストレージノードへの直接接続にも使用できるグローバル S3 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。

     グリッド CA によって署名されたデフォルトの S3 API 証明書を、外部証明機関によって署名されたカスタム証明書に置き換えていない限り、このオプションを選択することはできません。見る"S3 API証明書を設定する" 。

   - 管理インターフェース証明書を使用します。管理ノードへの直接接続にも使用できるグローバル管理インターフェイス証明書を使用する場合は、このオプションを選択します。
2. StorageGRID S3 証明書を使用していない場合は、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

a. *証明書のアップロード*を選択します。

b. 必要なサーバー証明書ファイルをアップロードします。

- サーバー証明書: PEM エンコードされたカスタム サーバー証明書ファイル。
- 証明書の秘密鍵: カスタムサーバー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 ビット以上である必要があります。

- **CA** バンドル: 各中間発行証明機関 (CA) から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され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、各証明書は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 を選択するか、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。

  証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

  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 **PEM** のコピー」または「**CA** バンドル **PEM** のコピー」を選択します。

d. *作成*を選択します。+ ロードバランサーエンドポイントが作成されます。カスタム証明書は、S3 クライアントまたは管理インターフェースとエンドポイント間の後続のすべての新しい接続に使用されます。

証明書を生成する

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。

フィールド	説明
ドメイン名	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（任意）	証明書所有者の X.509 サブジェクトまたは識別名 (DN)。 このフィールドに値が入力されない場合、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。

フィールド	説明
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. *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。

  証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

  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 **PEM** のコピー」を選択します。

e. *作成*を選択します。

ロード バランサー エンドポイントが作成されます。カスタム証明書は、S3 クライアントまたは管理インターフェースとこのエンドポイント間の以降のすべての新しい接続に使用されます。

終了後の操作

手順

1. DNS を使用する場合は、 StorageGRIDの完全修飾ドメイン名 (FQDN) をクライアントが接続に使用する各 IP アドレスに関連付けるレコードが DNS に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 グループを構成している場合、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 グループを使用していない場合、クライアントはゲートウェイ 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すべての必要なエンドポイント ドメイン名を参照していることも確認する必要があります。

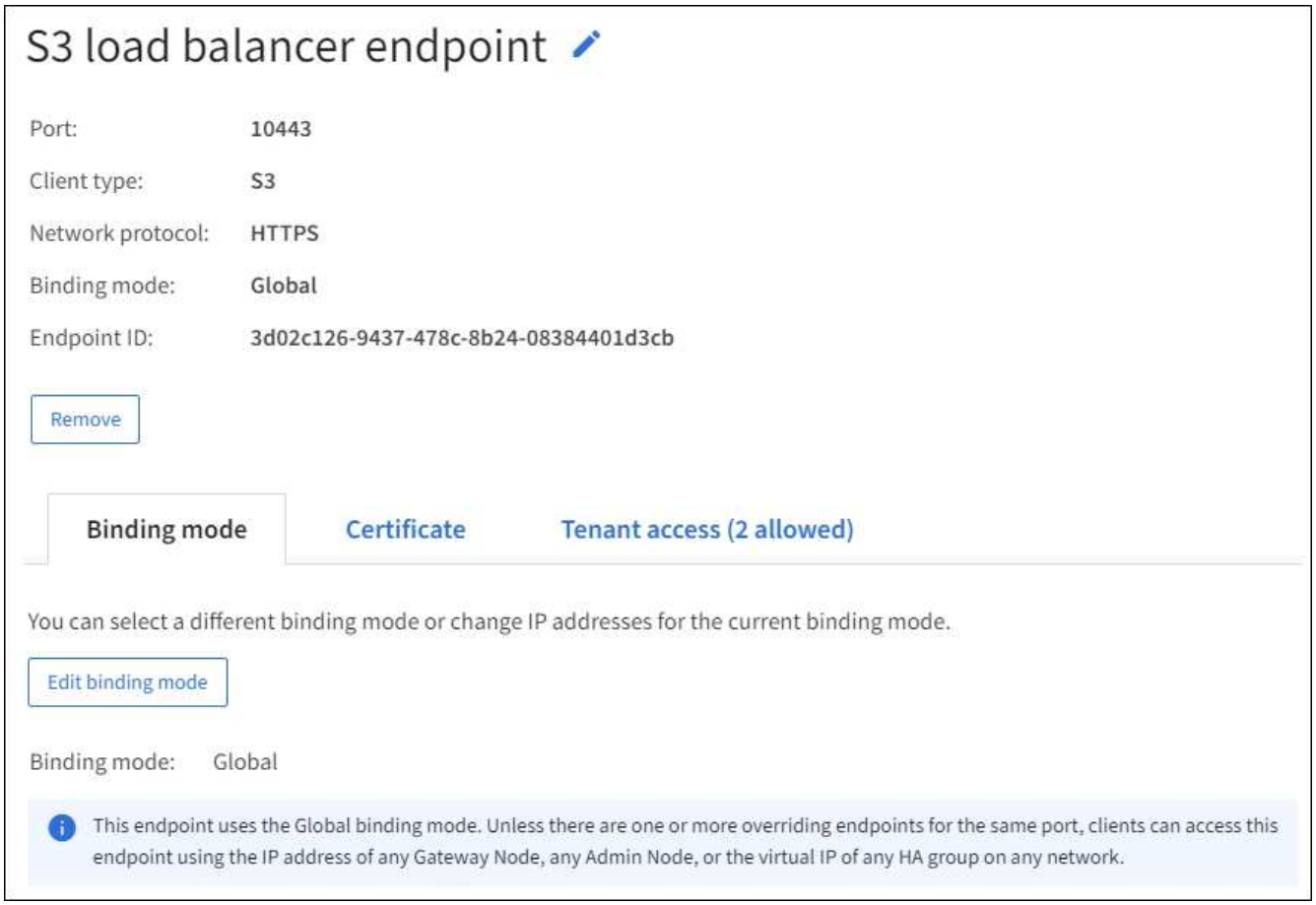
2. エンドポイントに接続するために必要な情報を S3 クライアントに提供します。

- 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

ロードバランサのエンドポイントの表示と編集

セキュリティ保護されたエンドポイントの証明書メタデータなど、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。エンドポイントの特定の設定を変更できます。

- すべてのロード バランサー エンドポイントの基本情報を表示するには、「ロード バランサー エンドポイント」ページの表を確認します。
- 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。表示される情報は、エンドポイントの種類と構成方法によって異なります。



- エンドポイントを編集するには、ロード バランサー エンドポイント ページの アクション メニューを使用します。

管理インターフェースのエンドポイントのポート編集中に Grid Manager へのアクセスを失った場合は、URL とポートを更新して再度アクセスできるようにします。

エンドポイントを編集した後、変更がすべてのノードに適用されるまで最大 15 分ほどかかる場合があります。

Task	[操作]メニュー	詳細ページ
エンドポイント名を編集	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てください。 d. *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. 編集アイコンを選択。 c. 新しい名前を入力してください。 d. *保存*を選択します。
エンドポイントポートを編集	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 > *エンドポイントポートの編集*を選択します c. 有効なポート番号を入力してください。 d. *保存*を選択します。	該当なし
エンドポイントバインディングモードを編集する	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 バインディング モードの編集 を選択します。 c. 必要に応じてバインディング 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. *バインディングモードの編集*を選択します。 c. 必要に応じてバインディング 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する	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 S3 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 S3 証明書の使用を開始します。 e. *変更を保存*を選択します。

Task	[操作]メニュー	詳細ページ
テナントアクセスの編集	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 > テナント アクセスの編集 を選択します。 c. 別のアクセス オプションを選択するか、リストからテナントを選択または削除するか、あるいはその両方を実行します。 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. テナント アクセス タブを選択します。 c. テナント アクセスの編集 を選択します。 d. 別のアクセス オプションを選択するか、リストからテナントを選択または削除するか、あるいはその両方を実行します。 e. *変更を保存*を選択します。

ロードバランサのエンドポイントを削除する

アクション 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ことも、詳細ページから 1 つのエンドポイントを削除することもできます。

> クライアントの中断を防ぐには、ロードバランサーエンドポイントを削除する前に、影響を受ける S3 クライアントアプリケーションを更新してください。別のロード バランサー 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するように各クライアントを更新します。必要な証明書情報も必ず更新してください。

> 管理インターフェースのエンドポイントを削除中に Grid Manager にアクセスできなくなった場合は、URL を更新します。

- 1 つ以上のエンドポイントを削除するには:
  a. ロード バランサー 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オンにします。
  b. アクション > *削除*を選択します。
  c. 「OK」を選択します。
- 詳細ページからエンドポイントを 1 つ削除するには:
  a. ロード バランサー 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。

著作権に関する情報

商標に関する情報