負荷分散の管理

StorageGRID 11.8

NetApp
May 17, 2024

目次

負荷分散の管理

ロードバランシングに関する考慮事項

ロードバランシングを使用して、S3およびSwiftクライアントからの取り込みと読み出しのワークロードを処理できます。

ロードバランシングとは何ですか？

クライアントアプリケーションがStorageGRID システムでデータを保存または取得する際、StorageGRID はロードバランサを使用して取り込みと読み出しのワークロードを管理します。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 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 Transport Layer Security （ 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セキュアな接続を確立します。

各ノード上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際に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。

> 推奨されるロードバランシングメカニズムは StorageGRID ロードバランササービスですが、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、ネットアップの担当者にお問い合わせいただくか、を参照してください "TR-4626 ：『 StorageGRID Third-party and global load balancers 』"。

必要なロードバランシングノードの数

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ロードバランササービスを使用するノードが 2 つ以上必要です。たとえば、サイトに 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ているとします。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する場合でも、各ロードバランシング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があることを確認します。

ロードバランサ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、ロードバランササービスを含むノードへのアクセスに送受信クライアントアプリケーション要求が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またはSwift）、バインドモード、および必要に応じて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、* configuration **>** Network **>** Load balancer endpoints *を選択するか、FabricPool and S3のセットアップウィザードを実行します。手順：

- "ロードバランサエンドポイントを設定する"
- "S3セットアップウィザードを使用します"
- "FabricPool セットアップウィザードを使用します"

ポートに関する考慮事項

ロードバランサ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のデフォルトで10433になりますが、未使用の外部ポートを1~65535の範囲で指定できます。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で使用されているポートは許可されません。を参照してください "ネットワークポートのリファレンス"。

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 の間の接続では、Transport Layer Security（TLS）暗号化を使用する必要があります。TLS暗号化を使用せずにStorageGRID に接続することはサポートされていますが、特に本番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場合は、*[HTTPS]*を選択する必要があります。

ロードバランサ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指定する必要があります。ロードバランサエンドポイントの作成時には、次の3つのオプションのいずれかを使用できます。

- 署名済み証明書をアップロードする（推奨）。この証明書には、公的に信頼された認証局または民間の認証局（CA）が署名できます。一般に信頼されているCAサーバ証明書を使用して接続を保護することを推奨します。生成される証明書とは異なり、CAによって署名された証明書は無停止でローテーションでき、有効期限の問題を回避できます。

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

  - カスタムサーバ証明書ファイル。
  - カスタムサーバ証明書の秘密鍵ファイル。
  - 必要に応じて、各中間発行認証局の証明書のCAバンドル。
- 自己署名証明書の生成。
- グローバル**StorageGRID S3**および**Swift**証明書を使用します。この証明書をロードバランサエンドポイント用に選択するには、事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。を参照してください "S3 および Swift API 証明書を設定する"。

どのような価値が必要か？

証明書を作成するには、S3またはSwiftクライアントアプリケーション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アドレスを把握しておく必要があります。

証明書の*サブジェクト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が含まれている必要があります。例：

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

必要に応じて、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および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： `*.storagegrid.example.com` ワイルドカード*を使用して表します `adm1.storagegrid.example.com` および `gn1.storagegrid.example.com`。

S3仮想ホスト形式の要求を使用する場合は、証明書ごとに* Alternative Name *エントリも含める必要があります "S3エンドポイントのドメイン名" ワイルドカード名も含めて、を設定しておきます。例：

```
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、を参照してください "サーバ証明書のセキュリティ強化ガイドライン"。

また、セキュリティ証明書の名前ごとにDNSエントリを定義する必要があります。

期限切れになる証明書の管理方法を教えてください。

S3アプリケーションとStorageGRID 間の接続の保護に使用した証明書の有効期限が切れると、アプリケーションからStorageGRID に一時的にアクセスできなくなる可能性があります。

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。

- 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があれば、注意深く監視します。たとえば、* Expiration of load balancer endpoint certificate や Expiration of global server certificate for S3 and Swift API *アラートなどです。
- StorageGRID アプリケーションとS3アプリケーションの証明書のバージョンは常に同期しておいてください。ロードバランサエンドポイントに使用する証明書を交換または更新する場合は、S3アプリケーションで使用される同等の証明書を交換または更新する必要があります。
- 公開署名されたCA証明書を使用する。CAによって署名された証明書を使用する場合は、有効期限が近い証明書を無停止で交換できます。
- 自己署名StorageGRID 証明書を生成した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では、ロードバランサ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している場合、クライアントアプリケーションは、許可されたIPアドレスまたはそれに対応するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用している場合にのみ、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スを制限する必要がないかぎり、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イス。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、クライアントは管理ノードのIPアドレス（または対応するFQDN）または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、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StorageGRID テナントアカウント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）、各エンドポイントで許可またはブロックされたテナントのリストを指定できます。

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をより適切に分離できます。たとえば、この機能を使用して、あるテナントが所有する最高機密または高度に機密性の高いマテリアルに他のテナントから完全に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は、クライアント要求で使用されたアクセスキーからテナントが決定されます。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（匿名アクセスなど）は、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の仕組みを理解するには、次の例を参考にしてください。

1. 次の2つのロードバランサエンドポイントを作成しておきます。
   - *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。
   - * Top secret * endpoint：ポート10444を使用し、* Top secret *テナントにのみアクセスを許可します。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. 。 `top-secret.pdf` は、* Top secret *テナントが所有するバケット内にあります。

にアクセスします `top-secret.pdf`、* Top secret *テナントのユーザは、にGET要求を問題 できます `https://w.x.y.z:10444/top-secret.pdf`。このテナントには10444エンドポイントの使用が許可されているため、ユーザ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が同じURLに対して同じ要求を発行すると、すぐに「Access Denied」というメッセージが表示されます。クレデンシャル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

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。エンドポイントを使用してGrid Manager、Tenant Manager、またはその両方にアクセスすることもできます。

> Swiftクライアントアプリケーションのサポートは廃止され、今後のリリースで削除される予定です。

作業を開始する前に

- 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"。
- を使用することができます "rootアクセス権限"。
- を確認しておきます "ロードバランシングに関する考慮事項"。
- 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に使用されるロードバランサ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 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"。

ロードバランサエンドポイントを作成します

S3またはSwiftクライアントの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。管理インターフェイスの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、および信頼されてい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します

手順

1. [* configuration * > * Network * > * Load Balancer Endpoints *] 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、*[Management interface]*タブを選択します。
4. 「 * Create * 」を選択します。

エンドポイントの詳細を入力します

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タイプ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
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	ロードバランシングに使用する StorageGRID ポート。最初に作成するエンドポイントのデフォルトは10433ですが、未使用の外部ポート（1～65535）を入力できます。 「* 80 」または「 8443 *」と入力した場合、ポート8443を解放していないかぎり、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。次に、ポート8443をS3エンドポイントとして使用すると、ゲートウェイノードと管理ノードの両方でポートが設定されます。
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。 • 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。

管理インターフェイス

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	Grid Manager、Tenant Manager、またはその両方へのアクセスに使用するStorageGRIDポート。 • Grid Manager：* 8443* • Tenant Manager：* 9443 * • Grid ManagerとTenant Managerの両方：* 443 * 注：これらのプリセットポートまたは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
Untrusted Client Network の略	このエンドポイントに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、No *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いています。 注：ロードバランサエンドポイントの作成時に、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いたり閉じたりするように設定できます。

1. 「 * Continue * 」を選択します。

綴じモードを選択します

手順

1. 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ドモードを選択します。

   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をここに示します。

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スを制限する必要がないかぎり、*グローバル*設定を使用してください。
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、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。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、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イス	クライアントがこのエンドポイントにアクセスするには、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（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、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれか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（管理インターフェイスエンドポイントのデフォルト）	クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードの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 はこの優先順位に従って、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*。

管理インターフェイ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

> 管理インターフェイスエンドポイントがテナントアクセスを制御できるのは、エンドポイントに Tenant Managerのインターフェイスタイプ。

手順

1. [Tenant access]*ステップで、次のいずれかを選択します。

フィールド	説明
Allow all tenants（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ら、ロードバランサ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します	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るのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択し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で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。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

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。

     このオプションは、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に置き換えている場合を除き、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"。

   - 管理インターフェイス証明書を使用。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。
- 証明書の秘密鍵：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。拡張子を付けてファイルを保存します `.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ます。カスタム証明書は、S3およびSwiftクライアント、または管理インターフェイスとエンドポイントの間の以降のすべての新規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。

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（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、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
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 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:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

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。拡張子を付けてファイルを保存します `.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およびSwiftクライアント、または管理インターフェイスとこのエンドポイントの間の以降のすべての新規接続に使用されます。

完了後

手順

1. DNSを使用する場合は、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（FQDN）を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。

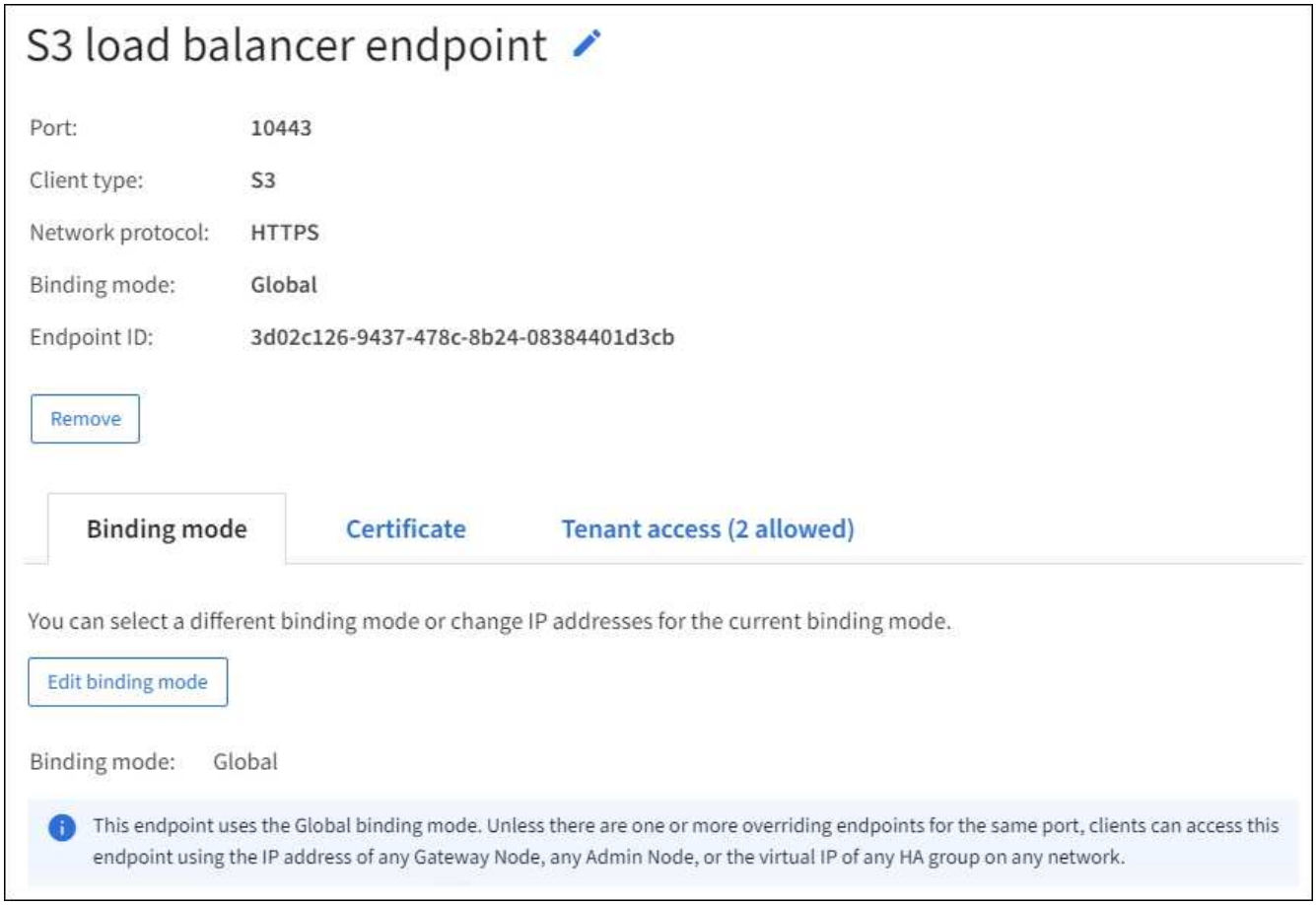
2. エンドポイントへの接続に必要な情報を S3 クライアントと Swift クライアントに提供します。

- 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。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。表示される情報は、エンドポイントのタイプとその設定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、[Load balancer Endpoints]ページの*[Actions]*メニューを使用します。

管理インターフェイスエンドポイントのポートの編集中にGrid Managerへのアクセスが失われた場合は、URLとポートを更新してアクセスを回復してください。

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。
エンドポイントポートの編集	a. エンドポイントのチェックボックスを選択します。 b. >[Edit endpoint port]*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（ Save ）] を選択します。	*n/a*
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。

タスク	[アクション] メニュー	詳細ページ
テナントアクセスを編集します	a. エンドポイントのチェックボックスを選択します。 b. >[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、また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、また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。

> 管理インターフェイスエンドポイントの削除中にGrid Managerへのアクセスが失われた場合は、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、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。