S3 および Swift クライアント接続を設定します

StorageGRID

NetApp
April 10, 2024

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

目次

S3 および Swift クライアント接続を設定します . . . 1
S3 および Swift クライアント接続について . . . 1
Summary ：クライアント接続の IP アドレスとポート . . . 2
VLAN インターフェイスを設定します . . . 4
ハイアベイラビリティグループを管理します . . . 9
負荷分散の管理 . . . 21
S3 API エンドポイントのドメイン名を設定 . . . 32
クライアント通信で HTTP を有効にします . . . 34
どのクライアント処理を許可するかを制御します . . . 35

S3 および Swift クライアント接続を設定します

S3 および Swift クライアント接続について

グリッド管理者は設定オプションを管理して、 S3 および Swift テナントがクライアントアプリケーションを StorageGRID システムに接続してデータの格納と読み出しを行う方法を制御します。クライアントとテナントのさまざまな要件を満たすために、多数のオプションが用意されています。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 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、または必要に応じて、管理ノードまたはゲートウェイノードのハイアベイラビリティ（ HA ）グループの仮想 IP アドレス
- ゲートウェイノード上の CLB サービス、または必要に応じて、ゲートウェイノードのハイアベイラビリティグループの仮想 IP アドレス

> CLB サービスは廃止されました。StorageGRID 11.3 より前に設定されたクライアントは、ゲートウェイノード上の CLB サービスを引き続き使用できます。ロードバランシングに StorageGRID を使用する他のすべてのクライアントアプリケーションは、ロードバランササービスを使用して接続する必要があります。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます

StorageGRID システムには、必要に応じて次の機能も設定できます。

- * VLAN インターフェイス * ：管理ノードとゲートウェイノードに仮想 LAN （ VLAN ）インターフェイスを作成してクライアントトラフィックとテナントトラフィックを分離し、パーティション化することで、セキュリティ、柔軟性、パフォーマンスを向上させることができます。VLAN インターフェイスを作成したら、ハイアベイラビリティ（ HA ）グループに追加します。
- * ハイアベイラビリティグループ * ：ゲートウェイノードまたは管理ノードのインターフェイスの HA グループを作成してアクティブ / バックアップ構成を作成できます。また、ラウンドロビン DNS やサードパーティ製ロードバランサと複数の HA グループを使用してアクティブ / アクティブ構成を実現することもできます。クライアント接続は、 HA グループの仮想 IP アドレスを使用して確立されます。
- * ロードバランササービス * ：クライアントがロードバランササービスを使用できるようにするには、クライアント接続用のロードバランサエンドポイントを作成します。ロードバランサエンドポイントを作成する際には、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（ S3 または Swift ）、 HTTPS 接続に使用する証明書（該当する場合）を指定します。
- * 信頼されていないクライアントネットワーク * ：信頼されていないクライアントネットワークとして設定することで、クライアントネットワークのセキュリティを強化できます。クライアントネットワークが信頼されていない場合、クライアントはロードバランサエンドポイントを使用して接続する必要があります。

ストレージノードに直接接続するか、 CLB サービス（廃止予定）を使用して StorageGRID に接続するクライアントに対しては、 HTTP の使用を有効にし、 S3 クライアントには S3 API エンドポイントのドメイン名を設定できます。

Summary ：クライアント接続の IP アドレスとポート

クライアントアプリケーションは、グリッドノードの IP アドレスおよびそのノード上のサービスのポート番号を使用して StorageGRID に接続できます。ハイアベイラビリティ（ HA ）グループが設定されている場合は、 HA グループの仮想 IP アドレスを使用してクライアントアプリケーションを接続できます。

このタスクについて

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および接続のタイプごとに使用される IP アドレスとポートを示します。以下の手順では、ロードバランサエンドポイントとハイアベイラビリティ（ HA ）グループがすでに設定されている場合に Grid Manager でこの情報を検索する方法について説明します。

接続が確立される場所	クライアントが接続するサービス	**IP** アドレス	ポート
HA グループ	ロードバランサ	HA グループの仮想 IP アドレス	• ロードバランサエンドポイントのポート
HA グループ	CLB の機能です • 注： * CLB サービスは廃止されました。	HA グループの仮想 IP アドレス	デフォルトの S3 ポート： • HTTPS ： 8082 • HTTP ： 8084 デフォルトの Swift ポート： • HTTPS ： 8083 • HTTP ： 8085
管理ノード	ロードバランサ	管理ノードの IP アドレス	• ロードバランサエンドポイントのポート
ゲートウェイノード	ロードバランサ	ゲートウェイノードの IP アドレス	• ロードバランサエンドポイントのポート

接続が確立される場所	クライアントが接続するサービス	IP アドレス	ポート
ゲートウェイノード	CLB の機能です • 注： * CLB サービスは廃止されました。	ゲートウェイノードの IP アドレス • 注：デフォルトでは、 CLB および LDR の HTTP ポートは有効になっていません。	デフォルトの S3 ポート： • HTTPS ： 8082 • HTTP ： 8084 デフォルトの Swift ポート： • HTTPS ： 8083 • HTTP ： 8085
ストレージノード	LDR	ストレージノードの IP アドレス	デフォルトの S3 ポート： • HTTPS ： 18082 • HTTP ： 18084 デフォルトの Swift ポート： • HTTPS ： 18083 • HTTP ： 18085

例

ゲートウェイノードの HA グループのロードバランサエンドポイントに S3 クライアントを接続するには、次のように構造化された URL を使用します。

- https://*VIP-of-HA-group:LB-endpoint-port*`

たとえば、 HA グループの仮想 IP アドレスが 192.0.2.5 で S3 ロードバランサエンドポイントのポート番号が 10443 の場合、 S3 クライアントは次の URL を使用して StorageGRID に接続できます。

- https://192.0.2.5:10443` にアクセスします

Swift クライアントをゲートウェイノードの HA グループのロードバランサエンドポイントに接続するには、次のように構造化された URL を使用します。

- https://*VIP-of-HA-group:LB-endpoint-port*`

たとえば、 HA グループの仮想 IP アドレスが 192.0.2.6 で、 Swift ロードバランサエンドポイントのポート番号が 10444 の場合、 Swift クライアントは次の URL を使用して StorageGRID に接続できます。

- https://192.0.2.6:10444` にアクセスします

クライアントが StorageGRID への接続に使用する IP アドレスに DNS 名を設定できます。ローカルネットワーク管理者にお問い合わせください。

手順

1. 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。
2. グリッドノードの IP アドレスを確認するには、次の手順を実行します。
   a. [* nodes （ノード）] を選択します
   b. 接続する管理ノード、ゲートウェイノード、またはストレージノードを選択します。
   c. [* Overview * （概要 * ）] タブを選択します。
   d. Node Information セクションで、ノードの IP アドレスを確認します。
   e. IPv6 アドレスとインターフェイスマッピングを表示するには、 * Show More * を選択します。

      クライアントアプリケーションから、リスト内の任意の IP アドレスへの接続を確立できます。

      - * eth0 ： * グリッドネットワーク
      - * eth1 ： * 管理ネットワーク（オプション）
      - * eth2 ： * クライアントネットワーク（オプション）

      表示されている管理ノードまたはゲートウェイノードがハイアベイラビリティグループのアクティブノードである場合は、 HA グループの仮想 IP アドレスが eth2 に表示されます。

3. ハイアベイラビリティグループの仮想 IP アドレスを検索するには、次の手順を実行します。
   a. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。
   b. HA グループの仮想 IP アドレスを表で確認します。
4. ロードバランサエンドポイントのポート番号を確認するには、次の手順を実行します。
   a. [* configuration * > * Network * > * Load Balancer Endpoints *] を選択します。

      Load Balancer Endpoints ページが表示され、設定済みのエンドポイントのリストが表示されます。

   b. エンドポイントを選択し、 * エンドポイントの編集 * を選択します。

      [Edit Endpoint] ウィンドウが開き、エンドポイントに関する追加の詳細が表示されます。

   c. 選択したエンドポイントが正しいプロトコル（ S3 または Swift ）で使用するように設定されていることを確認し、 * Cancel * を選択します。
   d. クライアント接続に使用するエンドポイントのポート番号をメモします。

      ポート番号が 80 または 443 の場合は、管理ノードで予約されているため、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。それ以外のポートはすべて、ゲートウェイノードと管理ノードの両方に設定されます。

VLAN インターフェイスを設定します

管理ノードとゲートウェイノードに仮想 LAN （ VLAN ）インターフェイスを作成し、それらを HA グループとロードバランサエンドポイントで使用してトラフィックを分離

し、セキュリティ、柔軟性、パフォーマンスを向上させることができます。

VLAN インターフェイスに関する考慮事項

- VLAN インターフェイスを作成するには、 VLAN ID を入力し、 1 つ以上のノード上で親インターフェイスを選択します。
- 親インターフェイスは、スイッチでトランクインターフェイスとして設定する必要があります。
- 親インターフェイスは、グリッドネットワーク（ eth0 ）、クライアントネットワーク（ eth2 ）、または VM やベアメタルホスト用の追加のトランクインターフェイス（ ens256 など）です。
- VLAN インターフェイスごとに、特定のノードに対して選択できる親インターフェイスは 1 つだけです。たとえば、グリッドネットワークインターフェイスとクライアントネットワークインターフェイスを同じゲートウェイノード上で同じ VLAN の親インターフェイスとして使用することはできません。
- VLAN インターフェイスが管理ノードトラフィック用で、 Grid Manager および Tenant Manager に関連するトラフィックが含まれている場合は、管理ノード上のインターフェイスのみを選択します。
- VLAN インターフェイスが S3 または Swift クライアントトラフィック用の場合は、管理ノードまたはゲートウェイノード上のインターフェイスを選択します。
- トランクインターフェイスを追加する必要がある場合は、次の詳細を参照してください。
  - * VMware （ノードのインストール後） * ： VMware ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します
  - * RHEL または CentOS （ノードのインストール前） * ： ノード構成ファイルを作成
  - * Ubuntu または Debian （ノードをインストールする前） * ： ノード構成ファイルを作成
  - * RHEL 、 CentOS 、 Ubuntu 、または Debian （ノードのインストール後） * ： Linux ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します

VLAN インターフェイスを作成します

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。
- ネットワークでトランクインターフェイスが設定され、 VM または Linux ノードに接続されている。トランクインターフェイスの名前を確認しておきます。
- 設定する VLAN の ID を確認しておきます。

このタスクについて

ネットワーク管理者が、 1 つ以上のトランクインターフェイスと 1 つ以上の VLAN を設定して、異なるアプリケーションまたはテナントに属するクライアントトラフィックまたは管理トラフィックを分離している場合があります。各 VLAN は、数値 ID またはタグで識別されます。たとえば、ネットワークで FabricPool トラフィックに VLAN 100 を使用し、アーカイブアプリケーションに VLAN 200 を使用しているとします。

グリッドマネージャを使用して、クライアントが特定の VLAN 上の StorageGRID にアクセスできるようにする VLAN インターフェイスを作成できます。VLAN インターフェイスを作成するときは、 VLAN ID を指定し、 1 つ以上のノード上で親（トランク）インターフェイスを選択します。

ウィザードにアクセスします

1. * configuration * > * Network * > * vlan interfaces * を選択します。
2. 「 * Create * 」を選択します。

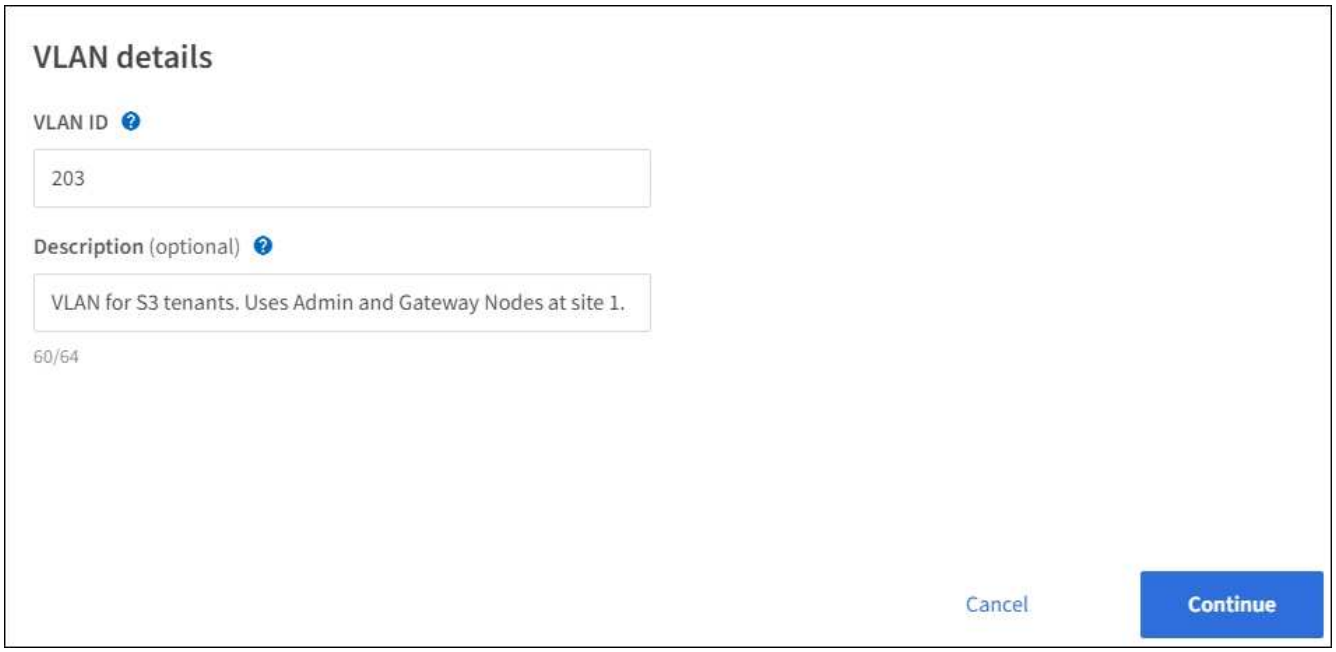
VLAN インターフェイスの詳細を入力します

1. ネットワーク内の VLAN の ID を指定します。1~4094 の値を入力できます。

   VLAN ID は一意である必要はありません。たとえば、あるサイトの管理トラフィックに VLAN ID 200 を使用し、別のサイトのクライアントトラフィックに同じ VLAN ID を使用できます。各サイトに異なる親インターフェイスのセットを持つ個別の VLAN インターフェイスを作成できます。ただし、同じ ID の 2 つの VLAN インターフェイスは、ノード上の同じインターフェイスを共有できません。

   すでに使用されている ID を指定すると、メッセージが表示されます。同じ VLAN ID に対して別の VLAN インターフェイスを引き続き作成することも、 * Cancel * を選択して既存の ID を編集することもできます。

2. 必要に応じて、 VLAN インターフェイスの短い概要 を入力します。



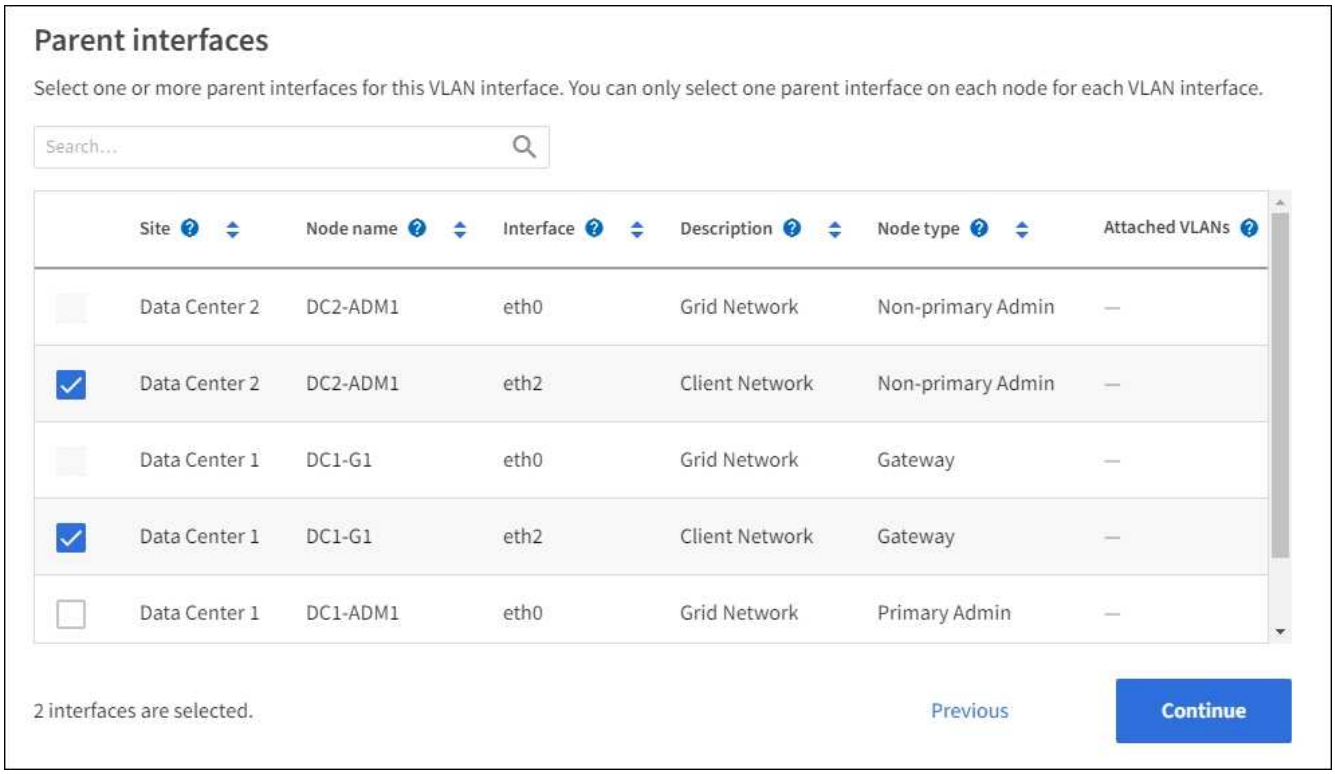
3. 「 * Continue * 」を選択します。

親インターフェイスを選択します

次の表に、グリッドの各サイトのすべての管理ノードとゲートウェイノードで使用可能なインターフェイスを示します。管理ネットワーク（ eth1 ）インターフェイスは親インターフェイスとして使用できず、表示されません。

1. この VLAN を接続する 1 つ以上の親インターフェイスを選択してください。

   たとえば、ゲートウェイノードと管理ノードのクライアントネットワーク（ eth2 ）インターフェイスに VLAN を接続できます。



2. 「 * Continue * 」を選択します。

設定を確認します

1. 構成を確認し、変更を行います。
   - VLAN ID または概要 を変更する必要がある場合は、ページの上部にある *Enter VLAN details * を選択します。
   - 親インターフェイスを変更する必要がある場合は、ページの上部にある「親インターフェイスを選択」を選択するか、「 * 前へ * 」を選択します。
   - 親インターフェイスを削除する必要がある場合は、ごみ箱を選択します 。
2. [保存（ Save ）] を選択します。
3. 新しいインターフェイスが High Availability groups ページで選択されて、ノードの * Network Interfaces * テーブルに表示されるまで、最大 5 分待ちます（ * nodes * > * _parent interface node_name > * Network * ）。

VLAN インターフェイスを編集します

VLAN インターフェイスを編集する場合、次の種類の変更を行うことができます。

- VLAN ID または概要 を変更します。
- 親インターフェイスを追加または削除します。

たとえば、関連付けられているノードの運用を停止する場合、 VLAN インターフェイスから親インターフェイスを削除できます。

次の点に注意してください。

- HA グループで VLAN インターフェイスを使用している場合、 VLAN ID は変更できません。
- HA グループで親インターフェイスが使用されている場合、親インターフェイスを削除することはできません。

  たとえば、 VLAN 200 がノード A および B の親インターフェイスに接続されているとしますHA グループでノード A の VLAN 200 インターフェイスとノード B の eth2 インターフェイスを使用している場合、ノード B の未使用の親インターフェイスを削除できますが、ノード A の使用済みの親インターフェイスを削除することはできません

手順

1. * configuration * > * Network * > * vlan interfaces * を選択します。
2. 編集する VLAN インターフェイスのチェックボックスを選択します。次に、 * アクション * > * 編集 * を選択します。
3. 必要に応じて、 VLAN ID または概要 を更新します。次に、 [* Continue （続行）] を選択します。

   HA グループで VLAN が使用されている場合、 VLAN ID は更新できません。

4. 必要に応じて、チェックボックスをオンまたはオフにして、親インターフェイスを追加したり、未使用のインターフェイスを削除したりします。次に、 [* Continue （続行）] を選択します。
5. 構成を確認し、変更を行います。
6. [保存（ Save ）] を選択します。

VLAN インターフェイスを削除します

1 つ以上の VLAN インターフェイスを削除できます。

HA グループで現在使用されている VLAN インターフェイスは削除できません。HA グループを削除する前に、 VLAN インターフェイスを HA グループから削除する必要があります。

クライアントトラフィックの中断を回避するには、次のいずれかを実行します。

- この VLAN インターフェイスを削除する前に、 HA グループに新しい VLAN インターフェイスを追加してください。
- この VLAN インターフェイスを使用しない新しい HA グループを作成してください。
- 削除する VLAN インターフェイスが現在アクティブインターフェイスである場合は、 HA グループを編集します。削除する VLAN インターフェイスを優先順位リストの一番下に移動します。新しいプライマリインターフェイスとの通信が確立されるまで待ってから、 HA グループから古いインターフェイスを削除します。最後に、そのノードの VLAN インターフェイスを削除します。

手順

1. * configuration * > * Network * > * vlan interfaces * を選択します。
2. 削除する各 VLAN インターフェイスのチェックボックスを選択します。次に、 * アクション * > * 削除 * を選択します。
3. 「 * はい * 」を選択して選択を確定します。

   選択したすべての VLAN インターフェイスが削除されます。VLAN Interfaces ページに、グリーンの成功バナーが表示されます。

ハイアベイラビリティグループを管理します

ハイアベイラビリティ（ **HA** ）グループの管理：概要

複数の管理ノードとゲートウェイノードのネットワークインターフェイスをハイアベイラビリティ（ HA ）グループにまとめることができます。HA グループのアクティブインターフェイスで障害が発生した場合、バックアップインターフェイスがワークロードを管理できます。

HA グループとは何ですか？

ハイアベイラビリティ（ HA ）グループを使用して、 S3 / Swift クライアントに可用性の高いデータ接続を提供したり、 Grid Manager および Tenant Manager への可用性の高い接続を提供したりできます。

各 HA グループは、選択したノードの共有サービスへのアクセスを提供します。

- ゲートウェイノード、管理ノード、またはその両方を含む HA グループは、 S3 クライアントと Swift クライアントに可用性の高いデータ接続を提供します。
- 管理ノードだけで構成される HA グループは、 Grid Manager と Tenant Manager への可用性の高い接続を提供します。
- 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だけで構成された HA グループは、の可用性の高い接続を提供できます S3 Select を使用する S3 テナント。S3 Select を使用する場合は HA グループを推奨しますが、必須ではありません。

HA グループはどのように作成しますか？

1. 1 つ以上の管理ノードまたはゲートウェイノードのネットワークインターフェイスを選択します。ノードに追加したグリッドネットワーク（ eth0 ）インターフェイス、クライアントネットワーク（ eth2 ）インターフェイス、 VLAN インターフェイス、またはアクセスインターフェイスを使用できます。

   DHCP によって割り当てられた IP アドレスがある HA グループにはインターフェイスを追加できません。

2. プライマリインターフェイスとして指定するインターフェイスは 1 つです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。
3. バックアップインターフェイスの優先順位を決定します。
4. グループに仮想 IP （ VIP ）アドレスを 1 ～ 10 個割り当てます。クライアントアプリケーションは、これらの VIP アドレスのいずれかを使用して StorageGRID に接続できます。

手順については、を参照してください ハイアベイラビリティグループを設定する。

アクティブインターフェイスとは何ですか。

通常の運用中は、 HA グループのすべての VIP アドレスが優先順位の最初のインターフェイスであるプライマリインターフェイスに追加されます。プライマリインターフェイスが使用可能な状態であれば、クライアントがグループの任意の VIP アドレスに接続するときに使用されます。つまり、通常の動作中、プライマリ・インターフェイスはグループの「アクティブ」インターフェイスになります。

同様に、通常の動作中は、 HA グループのプライオリティの低いインターフェイスは「 backup 」インターフェイスとして機能します。これらのバックアップインターフェイスは、プライマリ（現在アクティブ）インターフェイスが使用できなくなるまで使用されません。

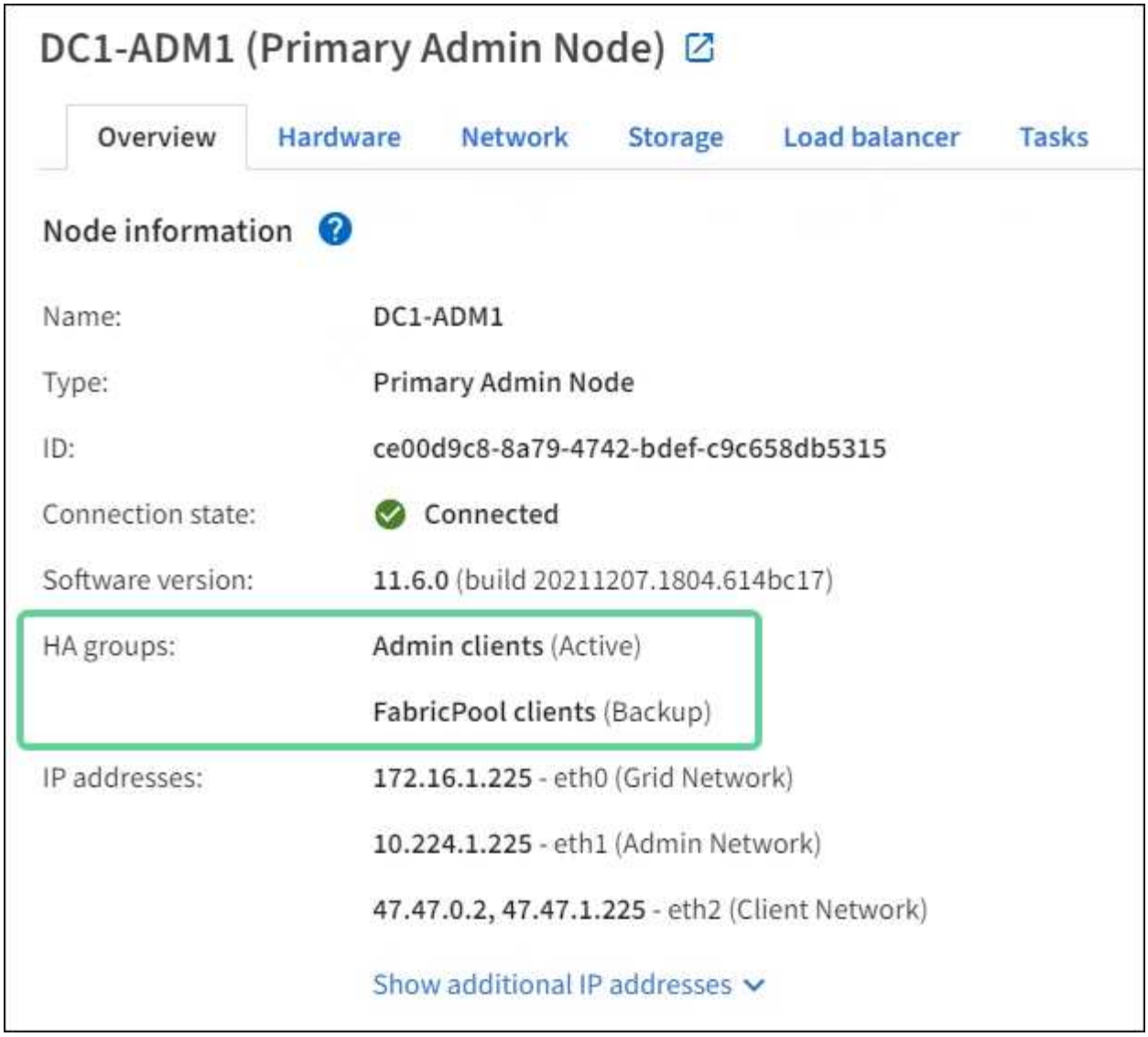
ノードの現在の **HA** グループのステータスを表示します

ノードが HA グループに割り当てられているかどうかを確認し、現在のステータスを確認するには、 * nodes * > * _node_name を選択します。

概要 * タブに HA グループ * のエントリが含まれている場合、そのノードは表示されている HA グループに割り当てられます。グループ名のあとの値は、 HA グループ内のノードの現在のステータスです。

- * Active * ： HA グループは現在このノードでホストされています。
- * バックアップ * ： HA グループは現在このノードを使用していません。バックアップインターフェイスです。
- * 停止 * ：ハイアベイラビリティ（キープアライブ）サービスが手動で停止されているため、このノードで HA グループをホストすることはできません。
- * 障害 * ：次の 1 つ以上が原因でこのノードで HA グループをホストできません：
  - ロードバランサ（ nginx-gw ）サービスがノードで実行されていません。
  - ノードの eth0 または VIP インターフェイスが停止しています。
  - ノードは停止しています。

この例では、プライマリ管理ノードが 2 つの HA グループに追加されています。このノードは、現在、 FabricPool クライアントグループのアクティブインターフェイスであり、クライアントグループのバックアップインターフェイスです。



アクティブインターフェイスに障害が発生するとどうなりますか。

VIP アドレスを現在ホストしているインターフェイスは、アクティブインターフェイスです。HA グループに複数のインターフェイスが含まれている場合にアクティブインターフェイスで障害が発生すると、 VIP アドレスは優先順位に従って、使用可能な最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、使用可能な次のバックアップインターフェイスに VIP アドレスが移動します。

フェイルオーバーは、次のいずれかの理由でトリガーされる可能性があります。

- インターフェイスが設定されているノードが停止する。
- インターフェイスが設定されているノードと他のすべてのノードとの接続が少なくとも 2 分間失われます。
- アクティブインターフェイスが停止する。
- ロードバランササービスが停止する。
- ハイアベイラビリティサービスが停止します。

アクティブインターフェイスをホストするノードの外部でネットワーク障害が発生した場合、フェイルオーバーがトリガーされないことがあります。同様に、 CLB サービス（廃止予定）の障害、またはグリッドマネージャまたはテナントマネージャのサービスの障害によって、フェイルオーバーはトリガーされません。

フェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションにほとんど影響がなく、通常の再試行で処理を続行できます。

障害が解決され、プライオリティの高いインターフェイスが再び使用可能になると、 VIP アドレスはプライオリティの高いインターフェイスに自動的に移動されます。

HA グループの用途

ハイアベイラビリティ（ HA ）グループを使用すると、オブジェクトデータ用および管理用に StorageGRID への可用性の高い接続を提供できます。

- HA グループは、 Grid Manager または Tenant Manager への可用性の高い管理接続を提供します。
- HA グループは、 S3 / Swift クライアントに可用性の高いデータ接続を提供できます。
- インターフェイスが 1 つしかない HA グループでは、多数の VIP アドレスを指定したり、 IPv6 アドレスを明示的に設定したりできます。

HA グループは、グループに含まれるすべてのノードが同じサービスを提供する場合にのみ高可用性を提供できます。HA グループを作成するときは、必要なサービスを提供するタイプのノードからインターフェイスを追加してください。

- * 管理ノード * ：ロードバランササービスが含まれ、 Grid Manager またはテナントマネージャへのアクセスを有効にします。
- * ゲートウェイノード * ：ロードバランササービスと CLB サービス（廃止）が含まれます。

HA グループの目的	このタイプのノードを **HA** グループに追加します
Grid Manager へのアクセス	• プライマリ管理ノード（ * プライマリ * ） • 非プライマリ管理ノード • 注： * プライマリ管理ノードがプライマリインターフェイスである必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。
Tenant Manager のみにアクセスします	• プライマリ管理ノードまたは非プライマリ管理ノード
S3 または Swift クライアントアクセス - ロードバランササービス	• 管理ノード • ゲートウェイノード

HA グループの目的	このタイプのノードを **HA** グループに追加します
の S3 クライアントアクセス S3 選択	• SG100 または SG1000 アプライアンス • VMware ベースのソフトウェアノード • 注： S3 Select を使用する場合は HA グループを推奨しますが、必須ではありません。
S3 または Swift クライアントアクセス - CLB サービス • 注： * CLB サービスは廃止されました。	• ゲートウェイノード

Grid Manager または **Tenant Manager** で **HA** グループを使用する場合の制限事項

Grid Manager サービスまたは Tenant Manager サービスに障害が発生した場合は、 HA グループのフェイルオーバーはトリガーされません。

フェイルオーバーの発生時に Grid Manager または Tenant Manager にサインインしている場合はサインアウトされるため、再度サインインしてタスクを再開する必要があります。

プライマリ管理ノードを使用できない場合は、一部のメンテナンス手順を実行できません。フェイルオーバー中は、 Grid Manager を使用して StorageGRID システムを監視できます。

CLB サービスで **HA** グループを使用する場合の制限事項

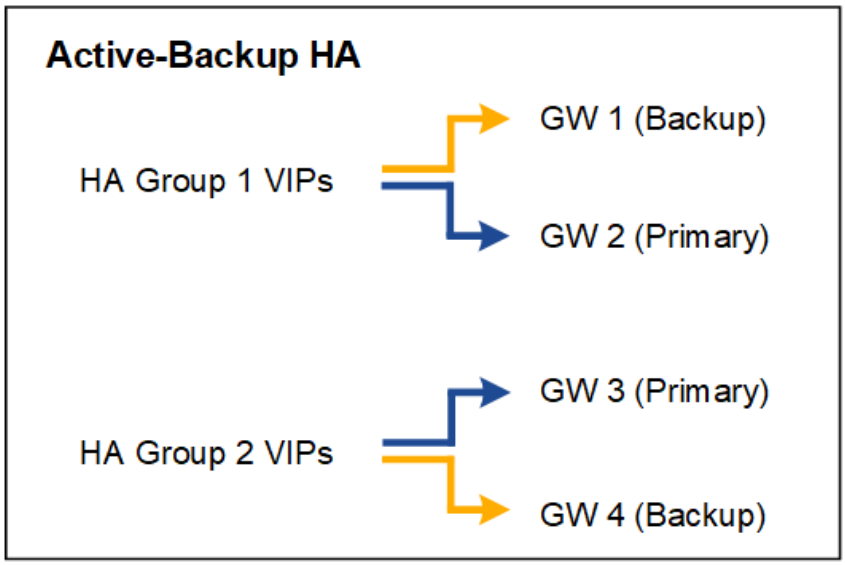
CLB サービスに障害が発生しても、 HA グループ内でフェイルオーバーはトリガーされません。

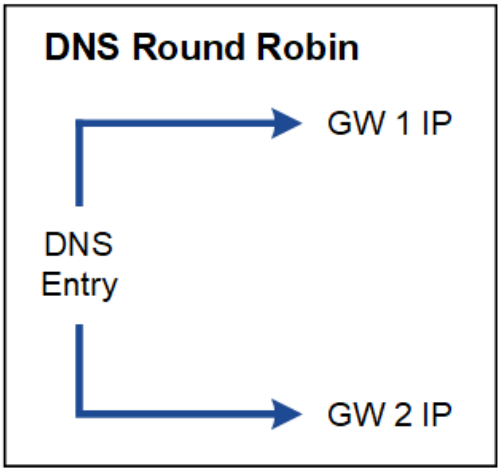
CLB サービスは廃止されました。

HA グループの設定オプション

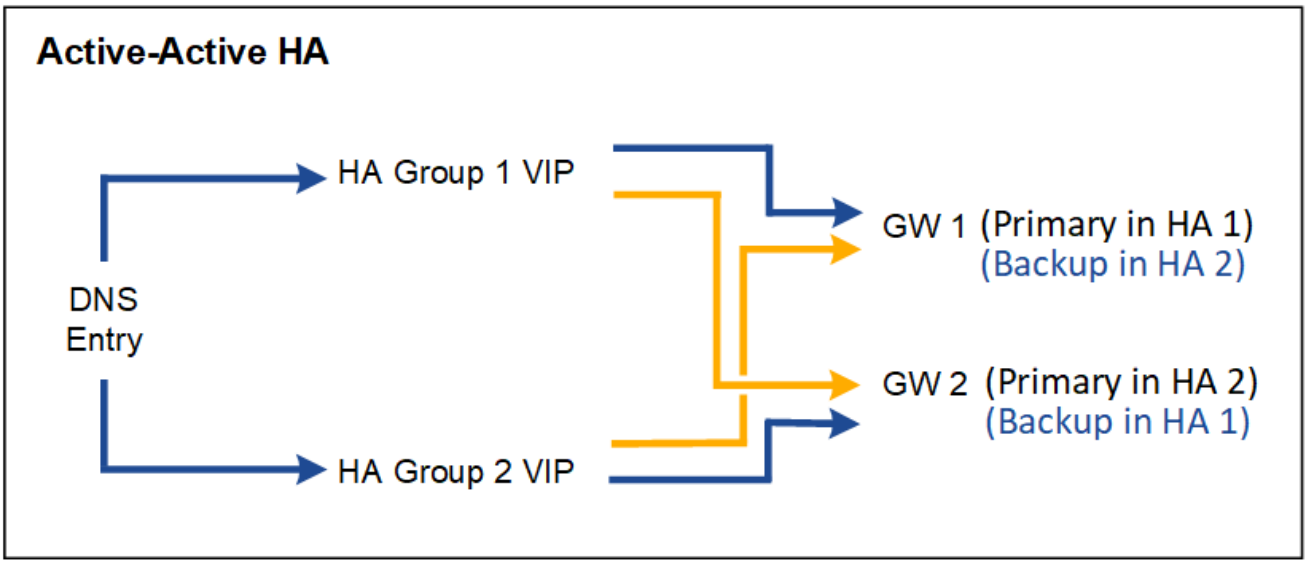
次の図は、 HA グループのさまざまな構成例を示しています。各オプションには長所と短所があります。

次の図では、 HA グループのプライマリインターフェイスが青、 HA グループのバックアップインターフェイスが黄色で示されています。





GW = Gateway Node
VIP = Virtual IP address



次の表は、図に示す各 HA 構成のメリットをまとめたものです。

設定	利点	欠点
アクティブ / バックアップ HA	• StorageGRID で管理され、外部のコンポーネントを必要としません。 • 高速フェイルオーバー。	• HA グループ内の 1 つのノードだけがアクティブです。各 HA グループで少なくとも 1 つのノードがアイドル状態になります。
DNS ラウンドロビン	• 総スループットが向上します。 • アイドル状態のホストはありません。	• クライアントの動作によってはフェイルオーバーが低速になる可能性があります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。

設定	利点	欠点
アクティブ / アクティブ HA	• トラフィックが複数の HA グループに分散されます。 • HA グループの数が増えるほど総スループットが向上します。 • 高速フェイルオーバー。	• 設定がより複雑になります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。

ハイアベイラビリティグループを設定する

ハイアベイラビリティ（ HA ）グループを設定して、管理ノードまたはゲートウェイノード上のサービスへの可用性の高いアクセスを提供できます。

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。
- HA グループで VLAN インターフェイスを使用する場合は、 VLAN インターフェイスを作成しておきます。を参照してください VLAN インターフェイスを設定します。
- HA グループ内のノードに対してアクセスインターフェイスを使用する場合は、インターフェイスを作成しておきます。
  - * Red Hat Enterprise Linux または CentOS （ノードのインストール前） * ： ノード構成ファイルを作成
  - * Ubuntu または Debian （ノードをインストールする前） * ： ノード構成ファイルを作成
  - * Linux （ノードのインストール後） * ： Linux ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します
  - * VMware （ノードのインストール後） * ： VMware ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します

ハイアベイラビリティグループを作成します

ハイアベイラビリティグループを作成する場合は、 1 つ以上のインターフェイスを選択して優先順位順に編成します。次に、グループに 1 つ以上の VIP アドレスを割り当てます。

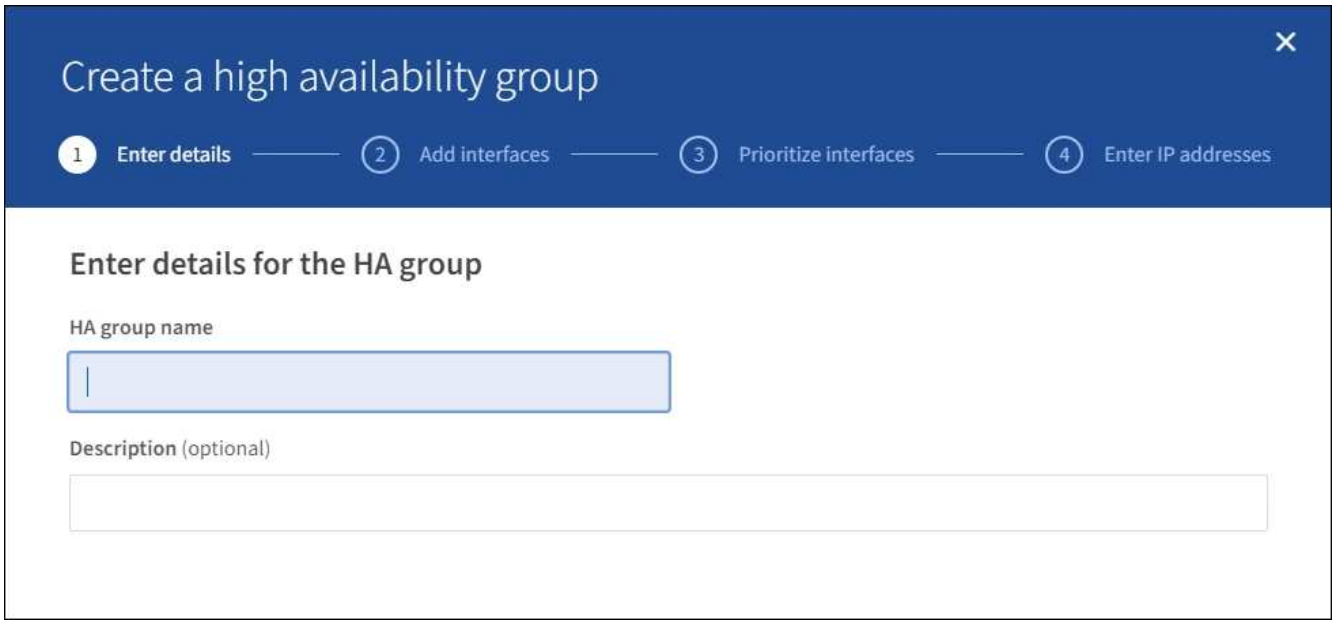
HA グループに含まれるゲートウェイノードまたは管理ノードのインターフェイスを指定する必要があります。HA グループでは、 1 つのノードに対して使用できるインターフェイスは 1 つだけですが、同じノードの他のインターフェイスは他の HA グループで使用できます。

ウィザードにアクセスします

1. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。
2. 「 * Create * 」を選択します。

HA グループの詳細を入力します

1. HA グループの一意の名前を指定してください。

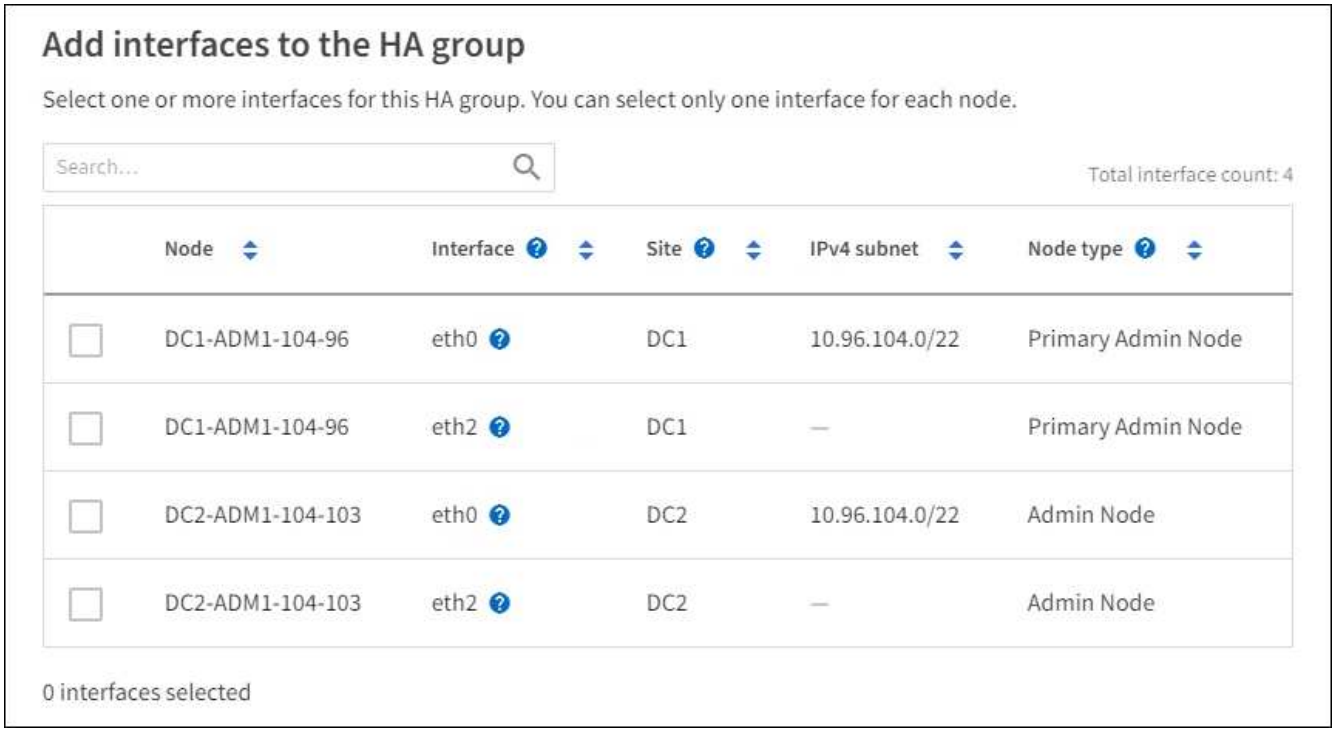


2. 必要に応じて、 HA グループの概要 を入力します。
3. 「 * Continue * 」を選択します。

HA グループにインターフェイスを追加します

1. この HA グループに追加するインターフェイスを 1 つ以上選択してください。

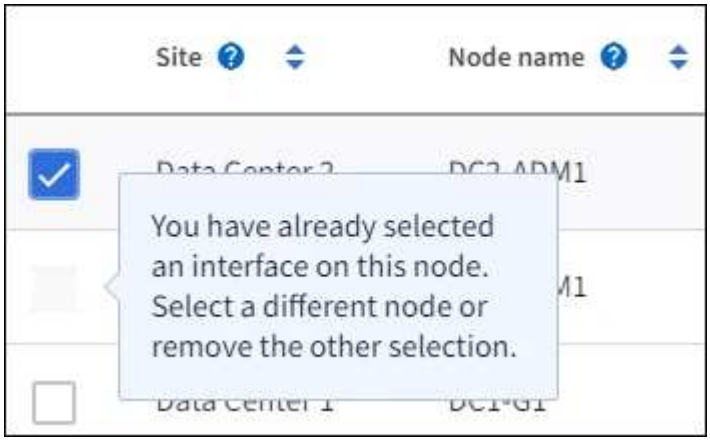
   列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。



VLAN インターフェイスを作成したら、新しいインターフェイスがテーブルに表示されるまで最大 5 分間待ちます。

インターフェイスの選択に関するガイドライン

- インターフェイスを少なくとも 1 つ選択してください。
- ノードに対して選択できるインターフェイスは 1 つだけです。
- HA グループがグリッドマネージャとテナントマネージャを含む管理ノードサービスの HA 保護用である場合は、管理ノード上のインターフェイスのみを選択します。
- HA グループが S3 または Swift クライアントトラフィックの HA 保護のためのものである場合は、管理ノード、ゲートウェイノード、またはその両方のインターフェイスを選択します。
- HA グループが廃止された CLB サービスの HA 保護用である場合は、ゲートウェイノード上のインターフェイスのみを選択します。
- 異なるタイプのノード上のインターフェイスを選択した場合は、情報メモが表示されます。フェイルオーバーが発生すると、以前にアクティブだったノードから提供されたサービスを、新たにアクティブになったノードで使用できなくなる可能性があります。たとえば、バックアップゲートウェイノードでは管理ノードサービスの HA 保護を提供できません。同様に、バックアップ管理ノードでは、プライマリ管理ノードが提供できるすべてのメンテナンス手順を実行することはできません。
- インターフェイスを選択できない場合、そのチェックボックスは無効になります。詳細については、ツールヒントを参照してください。



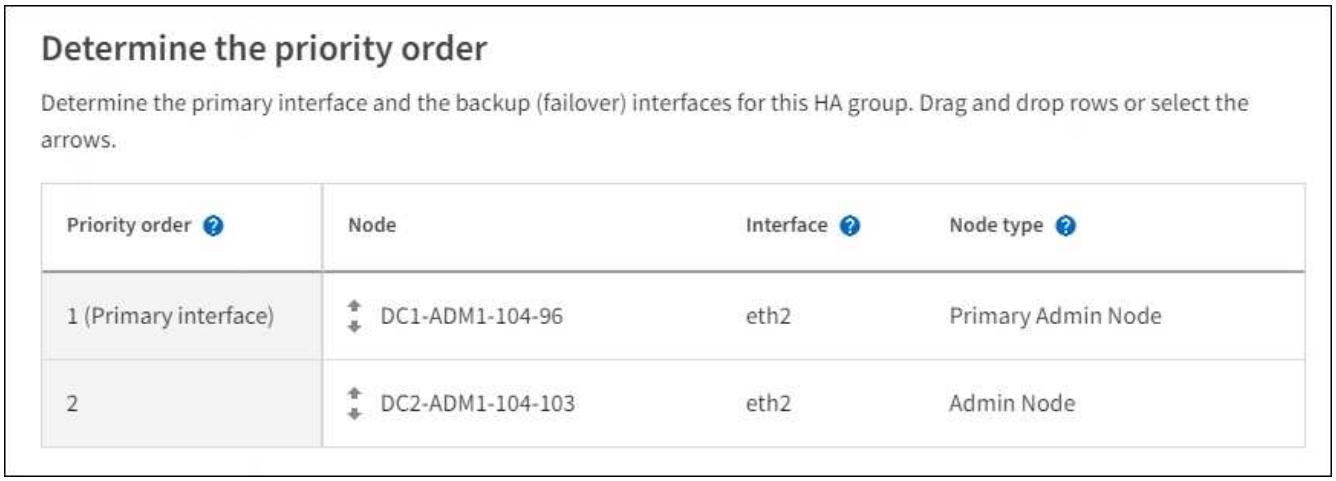
- サブネット値またはゲートウェイが選択した別のインターフェイスと競合している場合、インターフェイスは選択できません。
- 静的 IP アドレスがない場合、設定済みのインターフェイスは選択できません。

2. 「 * Continue * 」を選択します。

優先順位を決定します

1. この HA グループのプライマリインターフェイスとバックアップ（フェイルオーバー）インターフェイスを確認します。

   行をドラッグアンドドロップして、 * 優先順位 * 列の値を変更します。



HA グループが Grid Manager へのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを選択してプライマリインターフェイスにする必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。

HA グループに複数のインターフェイスが含まれている場合にプライマリインターフェイスに障害が発生すると、 VIP アドレスは使用可能な最も優先度の高いインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次に優先度の高いインターフェイスに移動します。

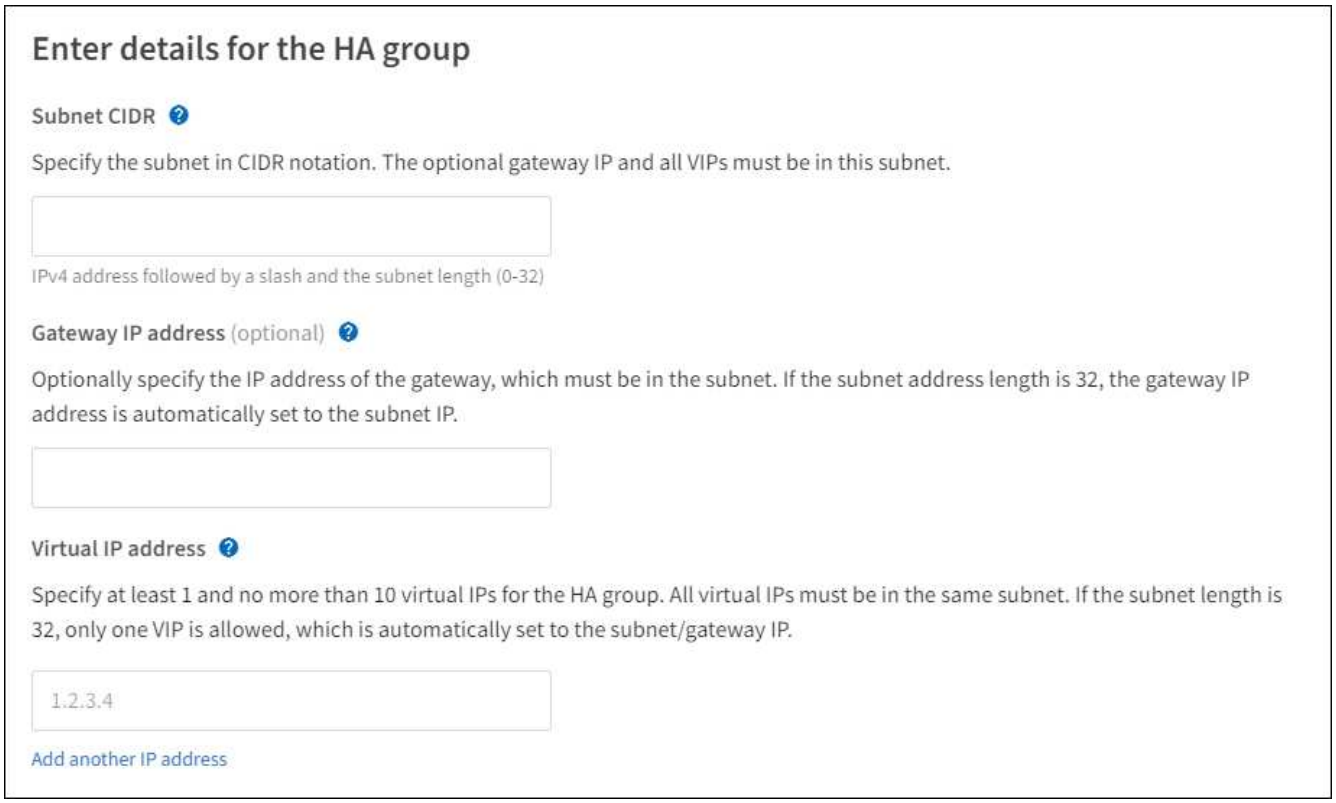
2. 「 * Continue * 」を選択します。

IP アドレスを入力してください

1. [* Subnet CIDR*] フィールドで、 CIDR 表記の VIP サブネット（ IPv4 アドレスの後にスラッシュとサブネットの長さ（ 0 ～ 32 ）を指定します。

   ネットワークアドレスにホストビットを設定しないでください。たとえば '192.160.0/22' のようになります

   32 ビットプレフィックスを使用する場合、 VIP ネットワークアドレスはゲートウェイアドレスおよび VIP アドレスとしても機能します。



2. 必要に応じて、 S3 、 Swift 、管理またはテナントクライアントが別のサブネットからこれらの VIP アドレスにアクセスする場合は、 * ゲートウェイ IP アドレス * を入力します。ゲートウェイアドレスは VIP サブネット内に設定する必要があります。

   クライアントと管理者のユーザは、このゲートウェイを使用して仮想 IP アドレスにアクセスします。

3. HA グループに 1 つ以上の * 仮想 IP アドレス * を入力します。IP アドレスは 10 個まで追加できます。VIP はすべて VIP サブネット内に設定する必要があります。

   IPv4 アドレスを少なくとも 1 つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

4. HA グループの作成 * を選択し、 * 完了 * を選択します。

   HA グループが作成され、設定済みの仮想 IP アドレスを使用できるようになります。

HA グループへの変更がすべてのノードに適用されるまで最大 15 分待ちます。

次のステップ

この HA グループをロードバランシングに使用する場合は、ロードバランサエンドポイントを作成してポートとネットワークプロトコルを決定し、必要な証明書を接続します。を参照してください ロードバランサエンドポイントを設定する。

ハイアベイラビリティグループを編集します

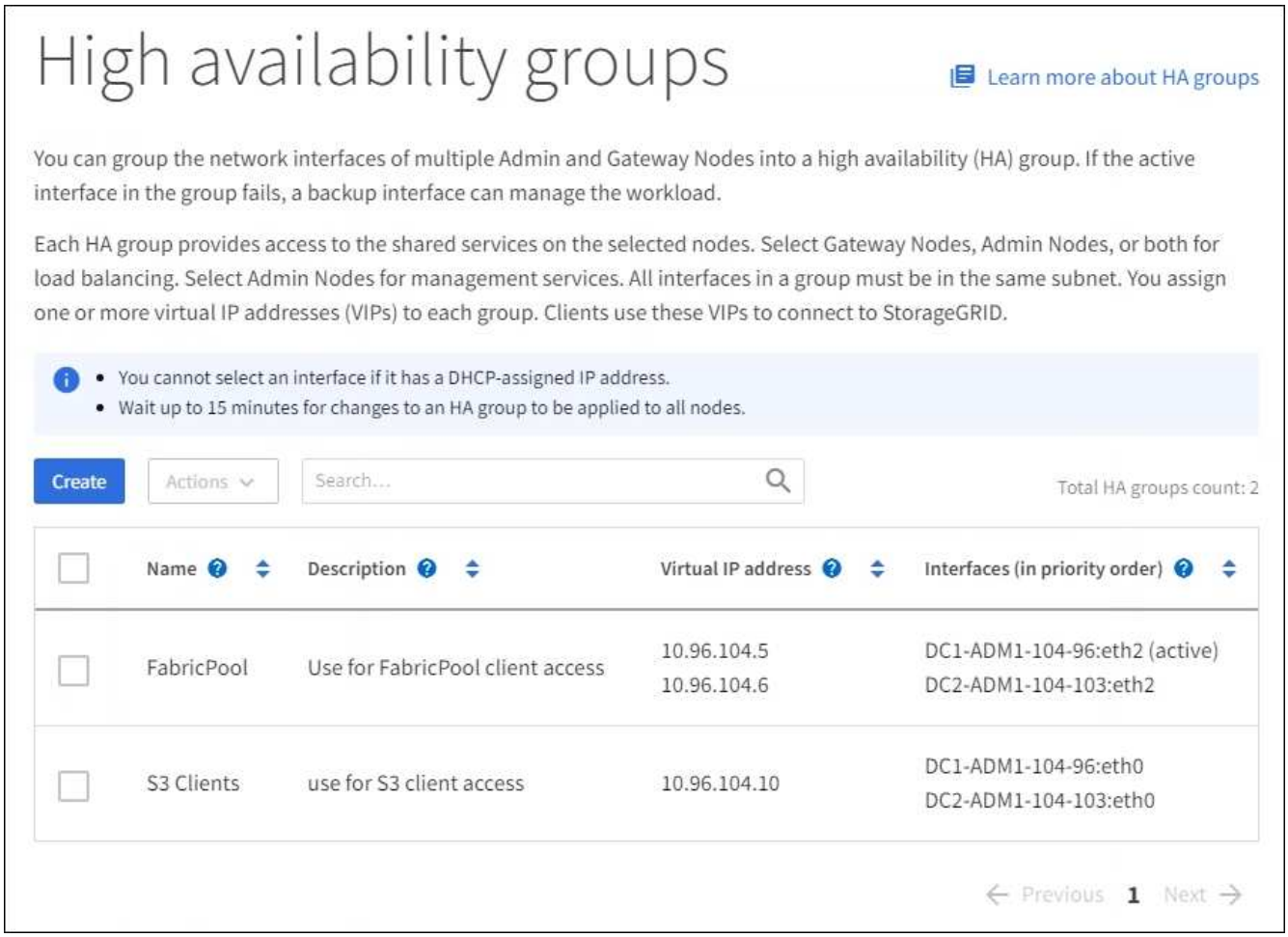
ハイアベイラビリティ（ HA ）グループを編集して、グループ名と概要 を変更したり、インターフェイスを追加または削除したり、優先順位を変更したり、仮想 IP アドレスを追加または更新したりできます。

たとえば、サイトまたはノードの運用停止手順 で、選択したインターフェイスに関連付けられているノードを削除する場合、 HA グループの編集が必要になることがあります。

手順

1. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。

   ハイアベイラビリティグループページには、既存のすべての HA グループが表示されます。



2. 編集する HA グループのチェックボックスを選択します。
3. 更新する内容に基づいて、次のいずれかを実行します。
   - 仮想 IP アドレスを追加または削除するには、 * Actions * > * Edit virtual IP address * を選択します。
   - *Actions * > * Edit HA group * を選択して、グループ名または概要 を更新したり、インターフェイスを追加または削除したり、優先順位を変更したり、 VIP アドレスを追加または削除したりします。
4. [仮想 IP アドレスの編集 *] を選択した場合：
   a. HA グループの仮想 IP アドレスを更新します。
   b. [保存（ Save ）] を選択します。
   c. [完了] を選択します。
5. HA グループの編集 * を選択した場合：
   a. 必要に応じて、グループの名前または概要 を更新します。

b. 必要に応じて、チェックボックスをオンまたはオフにしてインターフェイスを追加または削除します。

> HA グループが Grid Manager へのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを選択してプライマリインターフェイスにする必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません

c. 必要に応じて、行をドラッグアンドドロップして、この HA グループのプライマリインターフェイスとバックアップインターフェイスの優先順位を変更します。

d. 必要に応じて、仮想 IP アドレスを更新します。

e. [保存（ Save ）] を選択し、 [完了（ Finish ）] を選択します。

> HA グループへの変更がすべてのノードに適用されるまで最大 15 分待ちます。

ハイアベイラビリティグループを削除する

ハイアベイラビリティ（ HA ）グループは一度に 1 つ以上削除できます。ただし、 HA グループが 1 つ以上のロードバランサエンドポイントにバインドされている場合は、削除できません。

クライアントの停止を回避するには、 HA グループを削除する前に、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ます。各クライアントを更新して、別の IP アドレスを使用して接続します。たとえば、別の HA グループの仮想 IP アドレスや、インストール時にインターフェイスに設定された IP アドレスなどです。

手順

1. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。
2. 削除する各 HA グループのチェックボックスを選択します。次に、 * Actions * > * Remove HA group * を選択します。
3. メッセージを確認し、「 * HA グループを削除」を選択して選択を確認します。

   選択したすべての HA グループが削除されます。ハイアベイラビリティグループのページに、成功を示す緑色のバナーが表示されます。

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

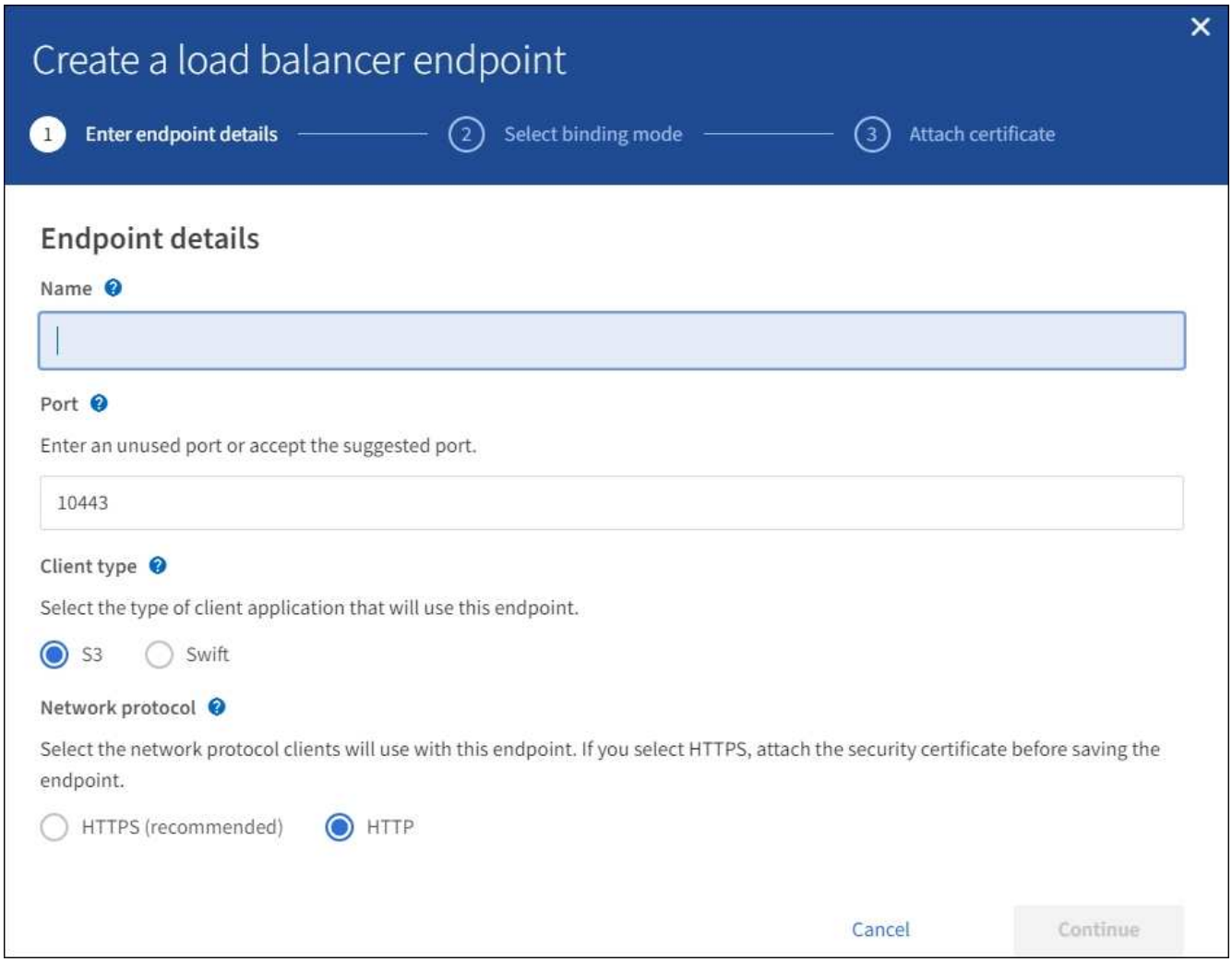
各ロードバランサエンドポイントは、ポート、クライアントタイプ（ S3 または Swift ）、およびネットワークプロトコル（ HTTP または HTTPS ）を指定します。

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。

フィールド	説明
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 * 。
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

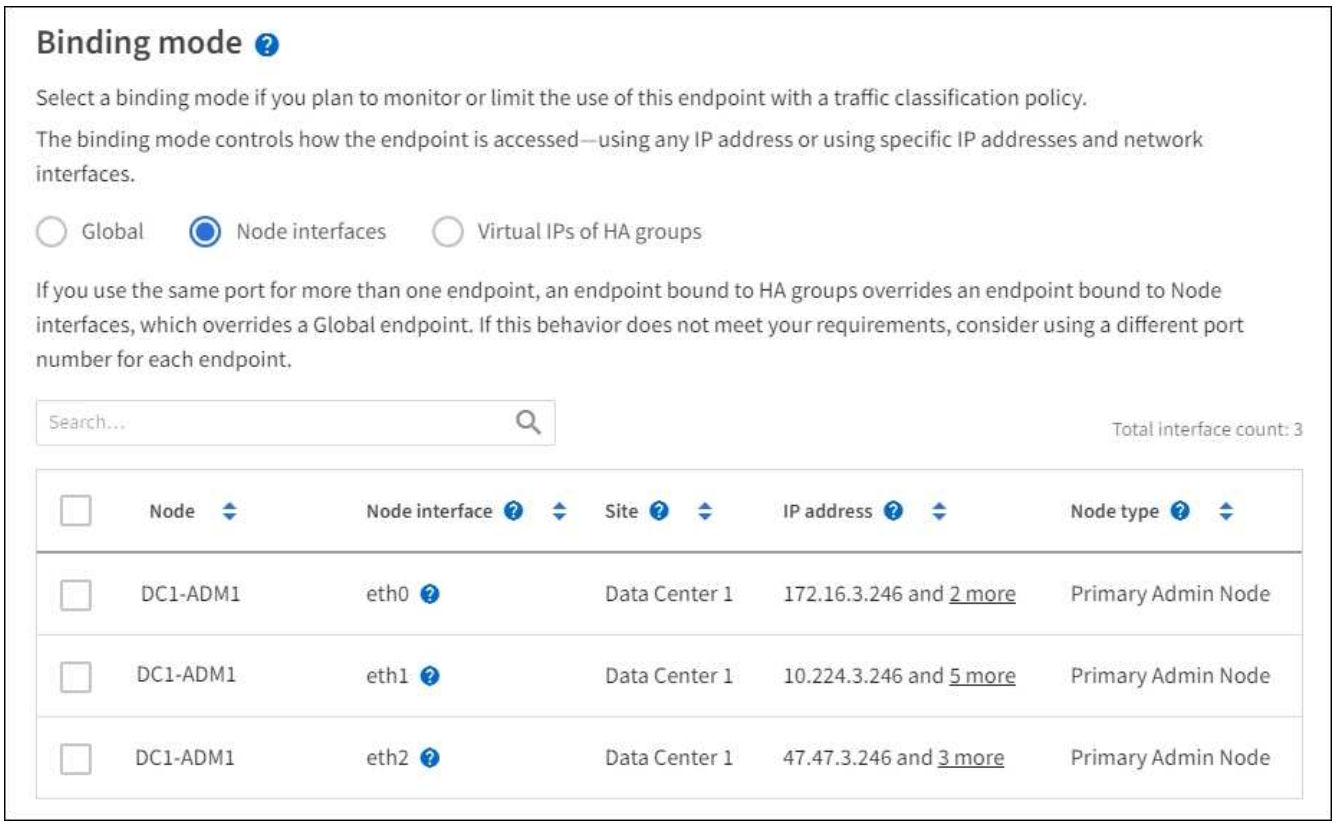
1. エンドポイントへのアクセス方法を制御するには、エンドポイントのバインディングモードを選択します。

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。

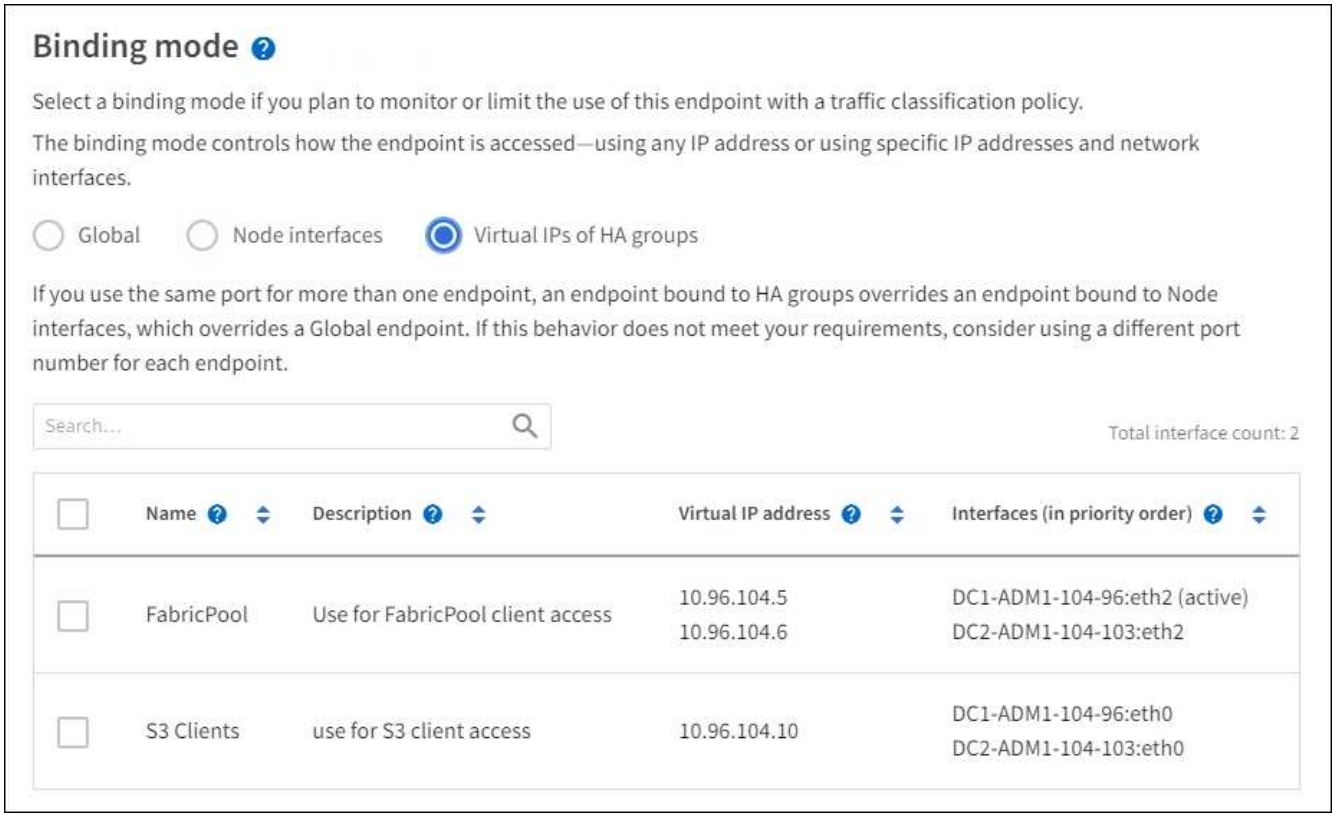
オプション	説明
HA グループの仮想 IP	クライアントは、 HA グループの仮想 IP アドレスを使用してこのエンドポイントにアクセスする必要があります。 このバインドモードのエンドポイントは、エンドポイントに対して選択した HA グループが重ならないかぎり、すべて同じポート番号を使用できます。 このモードのエンドポイントは、エンドポイントに対して選択したインターフェイスが重ならないかぎり、すべて同じポート番号を使用できます。

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。

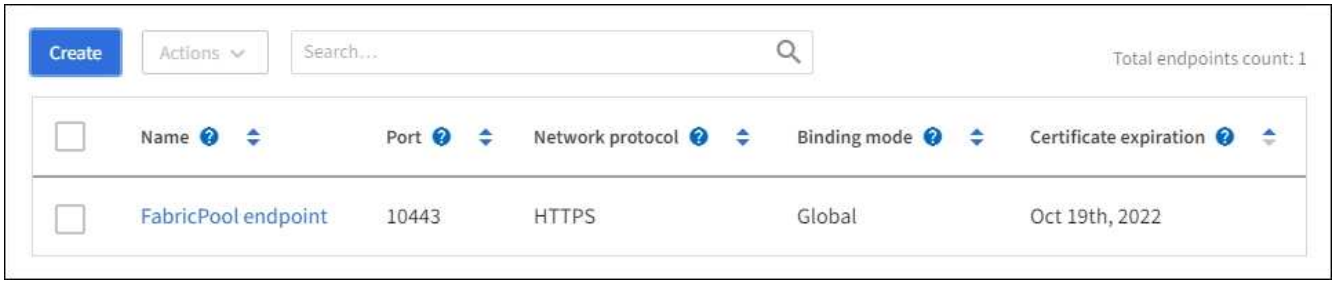
2. エンドポイントへの接続に必要な情報を S3 クライアントと Swift クライアントに提供します。
   - ポート番号
   - 完全修飾ドメイン名または IP アドレス
   - 必要な証明書の詳細

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

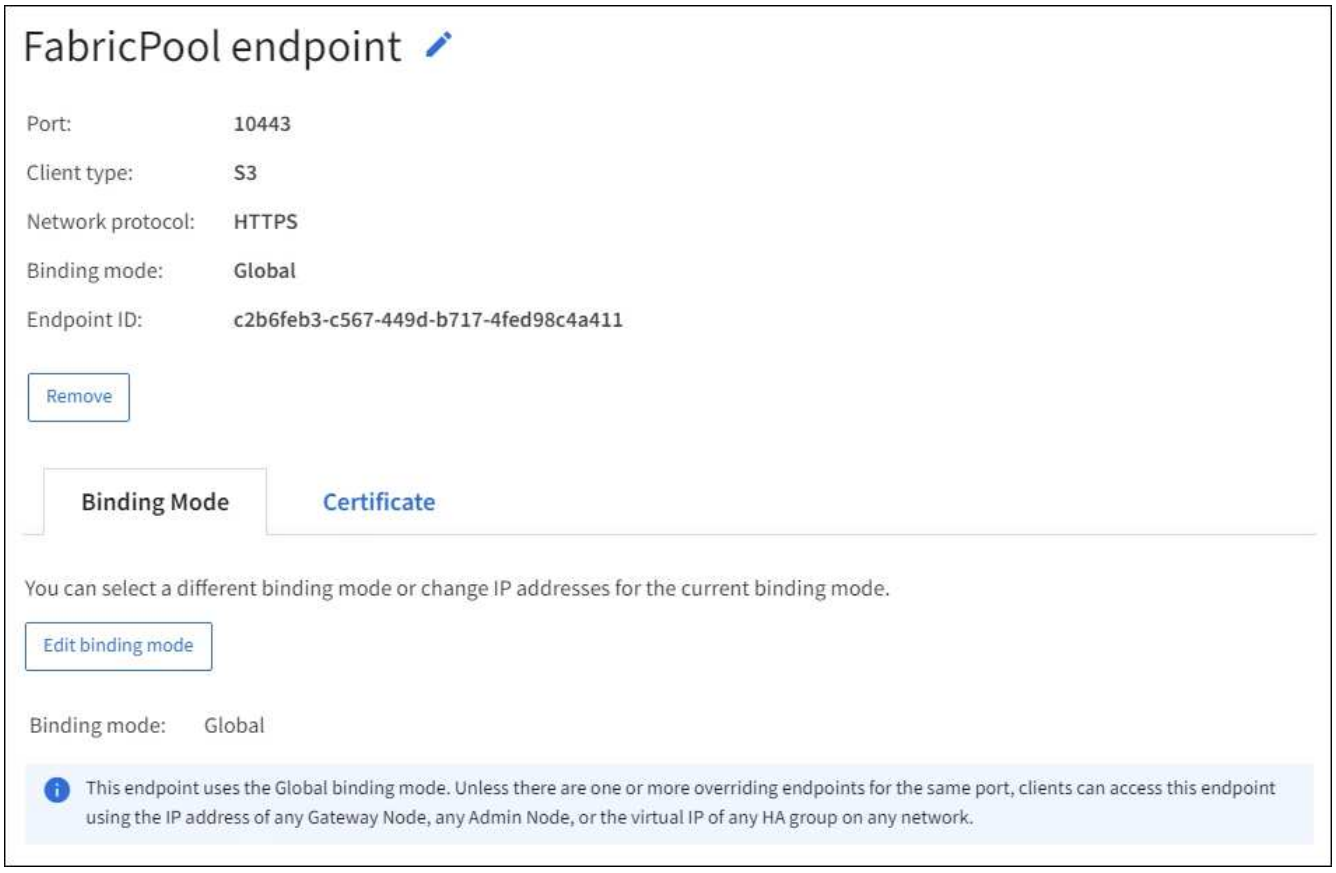
既存のロードバランサエンドポイントの詳細を表示できます。これには、セキュアなエンドポイントの証明書メタデータも含まれます。また、エンドポイントの名前またはバインドモードを変更して、関連付けられている証明書を更新することもできます。

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。

タスク	[アクション] メニュー	詳細ページ
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。

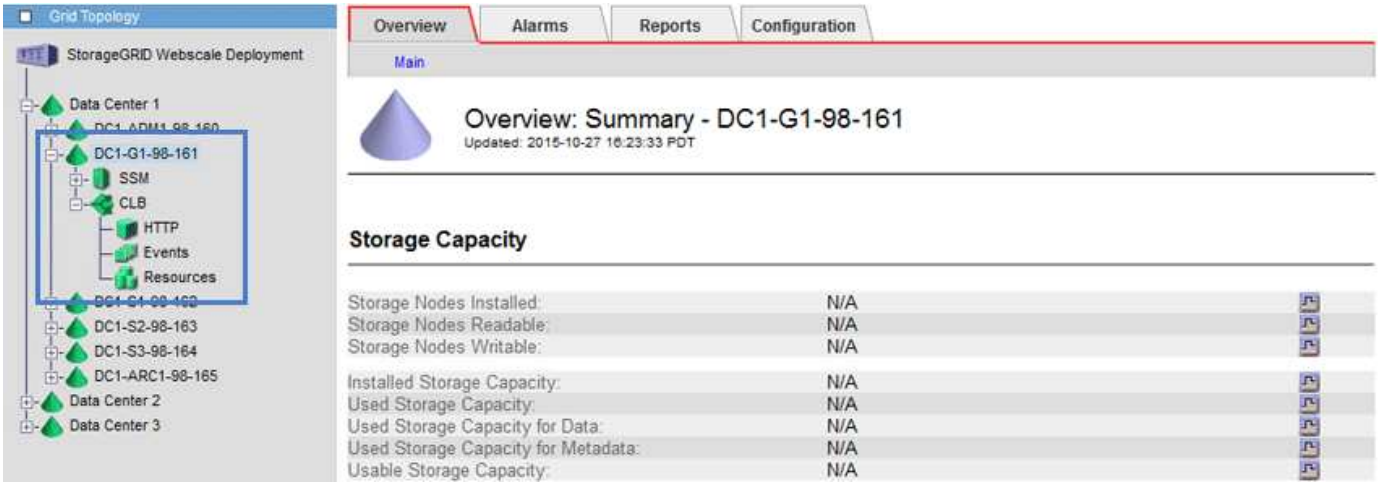
- 1 つ以上のエンドポイントを削除するには、次の手順
  a. Load Balancer ページで、削除する各エンドポイントのチェックボックスを選択します。
  b. * アクション * > * 削除 * を選択します。
  c. 「 * OK 」を選択します。
- 詳細ページから 1 つのエンドポイントを削除します。
  a. Load Balancer （ロードバランサ）ページから。エンドポイント名を選択します。
  b. 詳細ページで「 * 削除」を選択します。
  c. 「 * OK 」を選択します。

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

S3 API エンドポイントのドメイン名を設定

S3 仮想ホスト形式の要求をサポートするには、 Grid Manager を使用して、 S3 クライアントの接続先となるエンドポイントのドメイン名のリストを設定する必要があります。

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。
- 特定のアクセス権限が必要です。
- グリッドのアップグレードが進行中でないことを確認します。

> ドメイン名の設定は、グリッドのアップグレードの進行中は変更しないでください。

このタスクについて

クライアントが S3 エンドポイントのドメイン名を使用できるようにするには、次の作業をすべて実行する必要があります。

- Grid Manager を使用して、 S3 エンドポイントのドメイン名を StorageGRID システムに追加します。
- クライアントが StorageGRID への HTTPS 接続に使用する証明書が、クライアントが必要とするすべてのドメイン名に対して署名されていることを確認します。

  たとえば ' エンドポイントが s3.company.com` の場合 'HTTPS 接続に使用される証明書には 's3.company.com` エンドポイントとエンドポイントのワイルドカード Subject Alternative Name (SAN):*.s3.company.com` が含まれていることを確認する必要があります

- クライアントが使用する DNS サーバを設定します。クライアントが接続に使用する IP アドレスの DNS レコードを含め、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レコードが参照するようにします。

> クライアントは、ゲートウェイノード、管理ノード、またはストレージノードの IP アドレスを使用するか、ハイアベイラビリティグループの仮想 IP アドレスに接続することで、StorageGRID に接続できます。DNS レコードに正しい IP アドレスを追加するためには、クライアントアプリケーションがグリッドに接続する方法を理解しておく必要があります。

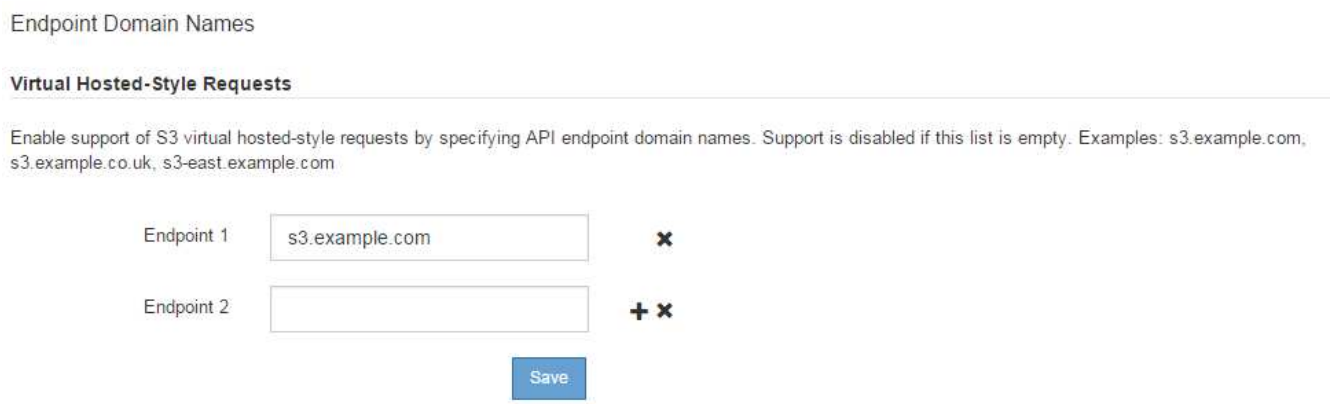
グリッドへの HTTPS 接続を使用するクライアント（推奨）では、次のいずれかの証明書を使用できます。

- ロードバランサエンドポイントに接続するクライアントは、そのエンドポイント用のカスタム証明書を使用できます。各ロードバランサエンドポイントは、異なるエンドポイントドメイン名を認識するように設定できます。
- ロードバランサエンドポイントに接続するクライアント、ストレージノードに直接接続するクライアント、またはゲートウェイノード上の廃止された CLB サービスに直接接続するクライアントは、グローバル S3 および Swift API 証明書をカスタマイズして、必要なエンドポイントのドメイン名をすべて含めることができます。

手順

1. [* configuration * > * Network * > * Domain Names *] を選択します。

   [Endpoint Domain Names] ページが表示されます。



2. S3 API エンドポイントのドメイン名のリストを * Endpoint * フィールドに入力します。を使用します ➕ アイコンをクリックしてフィールドを追加します。

このリストが空の場合、 S3 仮想ホスト形式の要求のサポートは無効になります。

3. [保存（ Save ）] を選択します。
4. クライアントが使用するサーバ証明書が、必要なエンドポイントのドメイン名と一致していることを確認します。
   - クライアントが独自の証明書を使用するロードバランサエンドポイントに接続する場合は、エンドポイントに関連付けられている証明書を更新します。
   - クライアントがグローバルな S3 および Swift API 証明書を使用するロードバランサエンドポイントに接続する場合は、ストレージノードに直接接続するか、またはゲートウェイノード上の CLB サービスに直接接続する場合は、グローバルな S3 および Swift API 証明書を更新します。
5. エンドポイントのドメイン名要求を解決するために必要な DNS レコードを追加します。

結果

これで、クライアントがエンドポイント bucket.s3.company.com` を使用すると、 DNS サーバは正しいエンドポイントに解決し、証明書はエンドポイントを認証します。

関連情報

- S3 を使用する
- IP アドレスを表示します
- ハイアベイラビリティグループを設定する
- 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設定する

クライアント通信で HTTP を有効にします

デフォルトでは、クライアントアプリケーションは、ストレージノードへのすべての接続、またはゲートウェイノード上の廃止された CLB サービスへのすべての接続に、 HTTPS ネットワークプロトコルを使用します。非本番環境のグリッドのテストなどの目的で、これらの接続に対して HTTP を有効にすることもできます。

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。
- 特定のアクセス権限が必要です。

このタスクについて

S3 / Swift クライアントがストレージノードへの HTTP 接続を直接確立する必要がある場合、またはゲートウェイノード上の廃止された CLB サービスへの HTTP 接続を確立する必要がある場合にのみ、このタスクを実行します。

HTTPS 接続のみを使用するクライアント、またはロードバランササービスに接続するクライアントでは、（各ロードバランサエンドポイントで HTTP または HTTPS を使用するように設定できるため）このタスクを実行する必要はありません。詳細については、ロードバランサエンドポイントの設定に関する情報を参照してください。

を参照してください Summary ：クライアント接続の IP アドレスとポート ストレージノードへの接続時、ま

たは HTTP または HTTPS を使用して廃止された CLB サービスへの接続時に使用するポート S3 および Swift クライアントを取得する

要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

手順

1. * 設定 * > * システム * > * グリッドオプション * を選択します。
2. [ネットワークオプション] セクションで、 [* HTTP 接続を有効にする *] チェックボックスをオンにします。

3. [保存（ Save ）] を選択します。

関連情報

- ロードバランサエンドポイントを設定する
- S3 を使用する
- Swift を使用します

どのクライアント処理を許可するかを制御します

PreventClientModification グリッドオプションを選択して、特定の HTTP クライアント処理を拒否することができます。

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。
- 特定のアクセス権限が必要です。

このタスクについて

クライアント変更の禁止は、システム全体の設定です。[クライアント変更を禁止する] オプションを選択すると、次の要求が拒否されます。

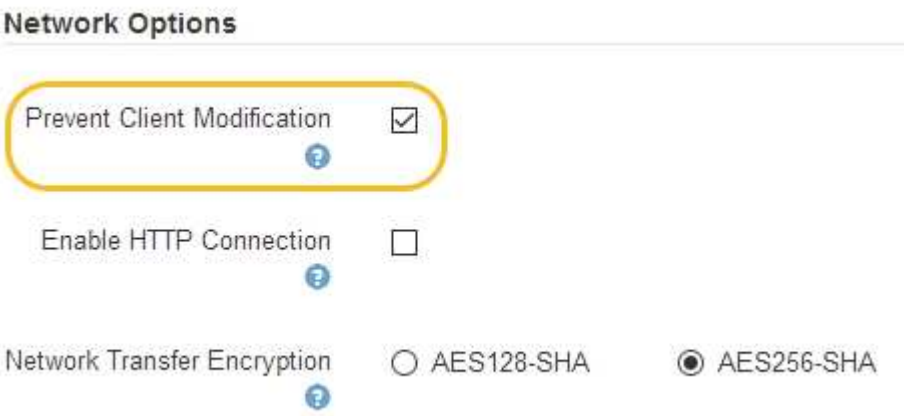
- * S3 REST API *
  - バケットの削除要求
  - 既存オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを変更するすべての要求

この設定は、バージョン管理が有効なバケットには適用されません。バージョン管理によって、すでにオブジェクトデータ、ユーザ定義メタデータ、オブジェクトのタグを変更できないようになっています。

- * Swift REST API *
  - コンテナの削除要求
  - 既存のオブジェクトを変更する要求。たとえば、 Put Overwrite 、 Delete 、 Metadata Update などの処理が拒否されます。

手順

1. * 設定 * > * システム * > * グリッドオプション * を選択します。
2. [ネットワークオプション] セクションで、 [クライアントの変更を禁止する *] チェックボックスをオンにします。



3. [保存（ Save ）] を選択します。

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。