S3およびSwiftクライアント接続の設定

StorageGRID 11.5

NetApp

April 11, 2024

目次

S3およびSwiftクライアント接続の設定

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。

- 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。
- 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や他社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。

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
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

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
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`

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`

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. サポートされているブラウザを使用してGrid Managerにサインインします。
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. [ノード（ Nodes）]を選択し
   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. Show More *をクリックして、IPv6アドレスとインターフェイスマッピングを表示します。

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. * Configuration > Network Settings > High Availability Groups *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 Settings > 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*をクリックします。

      [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 *をクリックします。
   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。

負荷分散の管理

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。

StorageGRID システムでは、次の方法でロードバランシングを実現できます。

- 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。
- ゲートウェイノードにのみインストールされている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。

CLB サービスは廃止されました。

- 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、プロトコル（HTTPまたはHTTPS）、サービスタイプ（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）仮想IPアドレス（VIP）
- 特定の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。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

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。

関連情報

""

ロードバランサエンドポイントの設定

ロードバランサエンドポイントを作成、編集、および削除できます。

ロードバランサエンドポイントの作成

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）、およびサービスタイプ（S3またはSwift）を指定します。HTTPSエンドポイントを作成する場合は、サーバ証明書をアップロードまたは生成する必要があります。

必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ロードバランササービスに使用するポートをすでに再マッピングしている場合は、再マッピングを削除しておく必要があります。

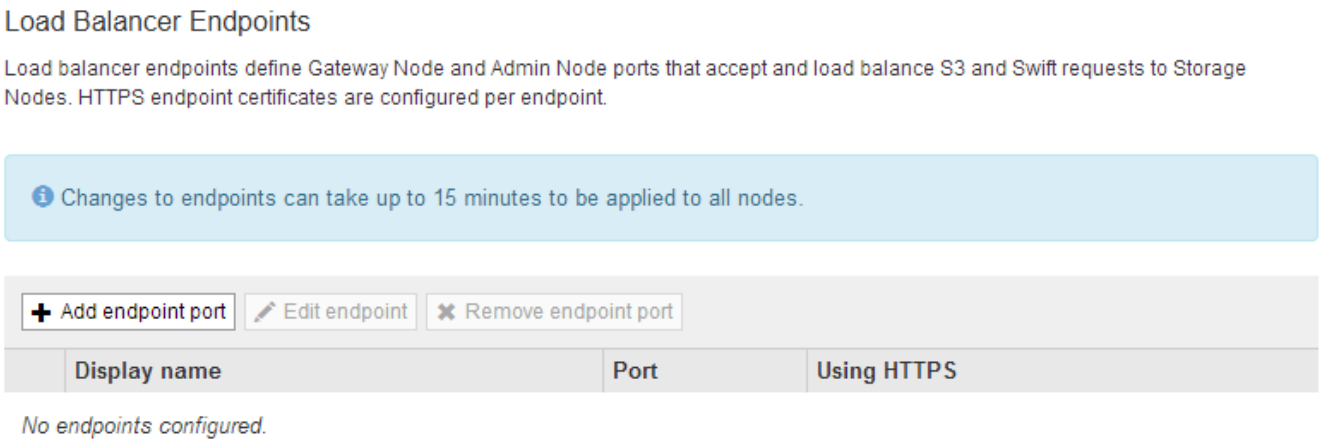
> ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

> CLB サービスは廃止されました。

手順

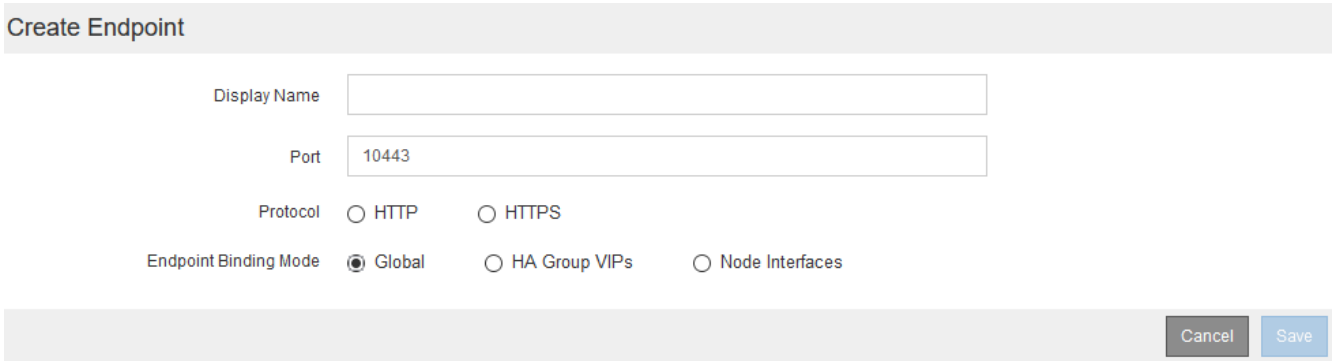
1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。



2. [エンドポイントの追加]を選択します。

   [Create Endpoint]ダイアログボックスが表示されます。



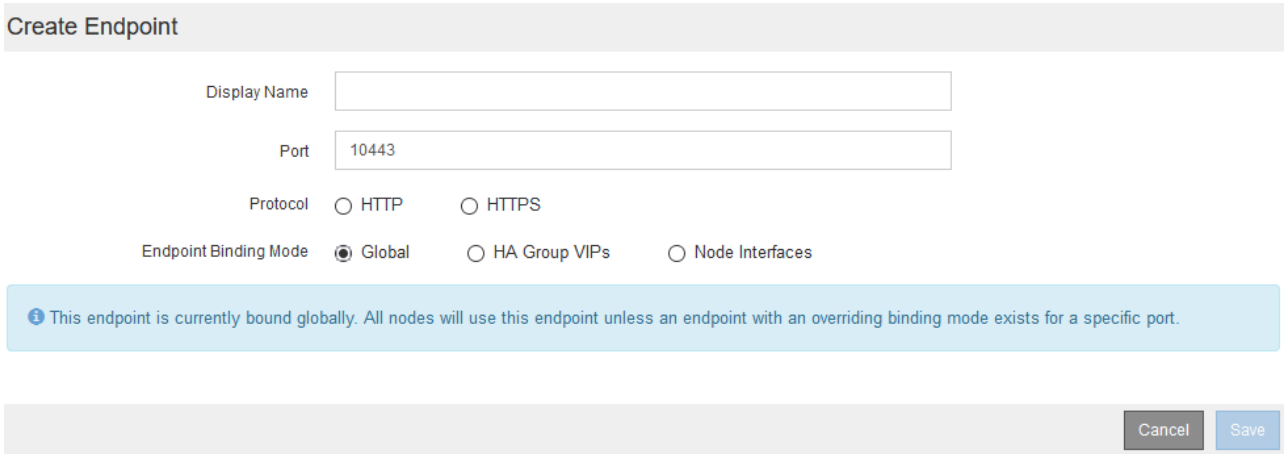
3. ロードバランサエンドポイントのページのリストに表示されるエンドポイントの表示名を入力します。
4. ポート番号を入力するか、あらかじめ入力されているポート番号をそのまま使用します。

   ポート番号80または443は管理ノードで予約されているため、これらのポートを入力すると、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。

   他のグリッドサービスで使用されているポートは使用できません。内部および外部の通信に使用されるポートの一覧については、ネットワークのガイドラインを参照してください。

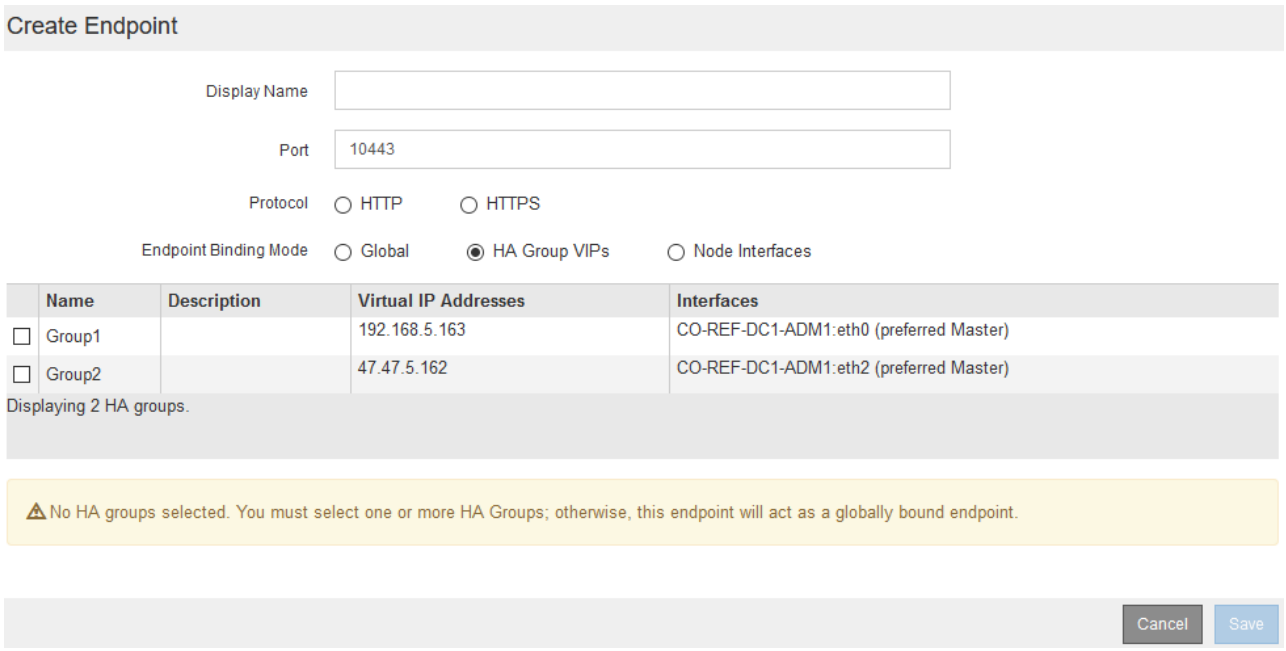
5. このエンドポイントのネットワークプロトコルを指定するには、「* HTTP 」または「 HTTPS *」を選択します。
6. エンドポイントバインディングモードを選択します。

   - * Global *（デフォルト）：指定したポート番号のすべてのゲートウェイノードと管理ノードでエンドポイントにアクセスできます。



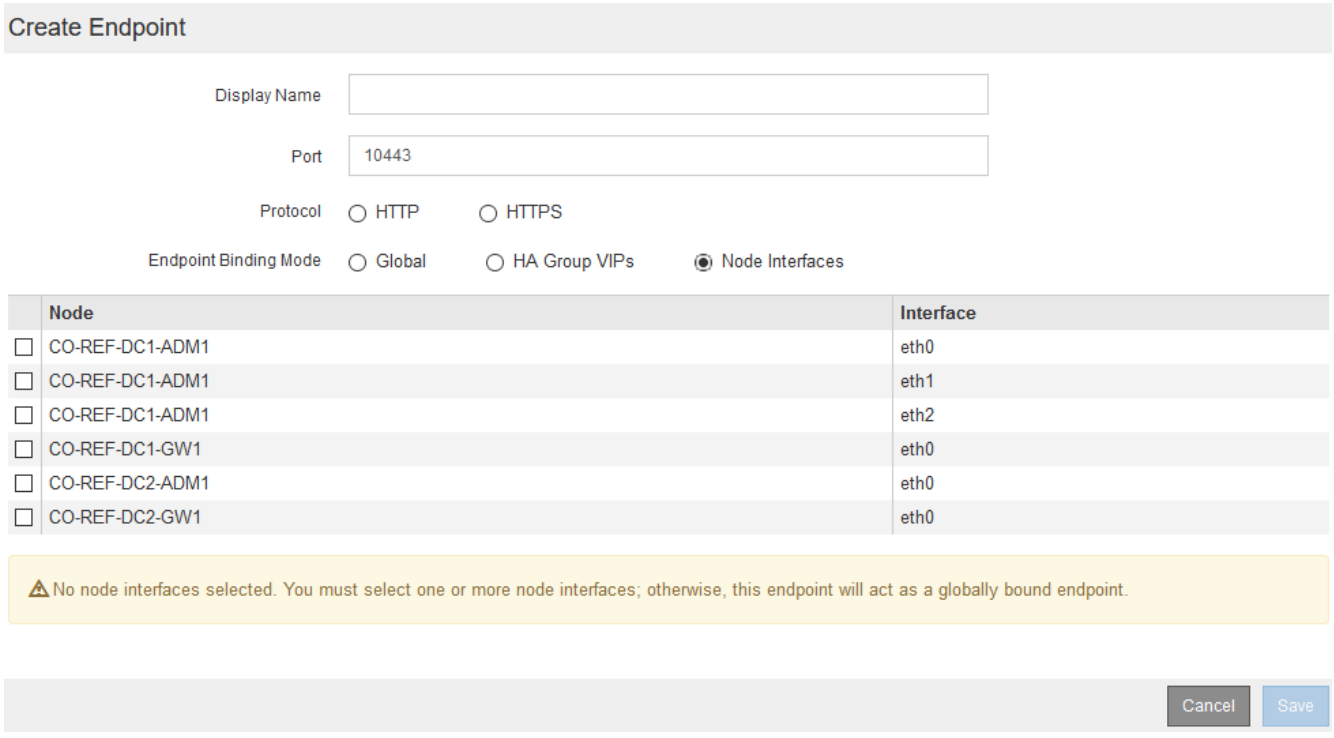
   - * HA Group VIP *：エンドポイントには、選択したHAグループに定義された仮想IPアドレスからのみアクセスできます。このモードで定義されたエンドポイントは、エンドポイントによって定義されたHAグループが互いに重複しないかぎり、同じポート番号を再利用できます。

     仮想IPアドレスが割り当てられたエンドポイントを表示するHAグループを選択します。



◦ ノードインターフェイス：エンドポイントには、指定したノードとネットワークインターフェイスでのみアクセスできます。このモードで定義されたエンドポイントは、相互に重複しないかぎり、同じポート番号を再利用できます。

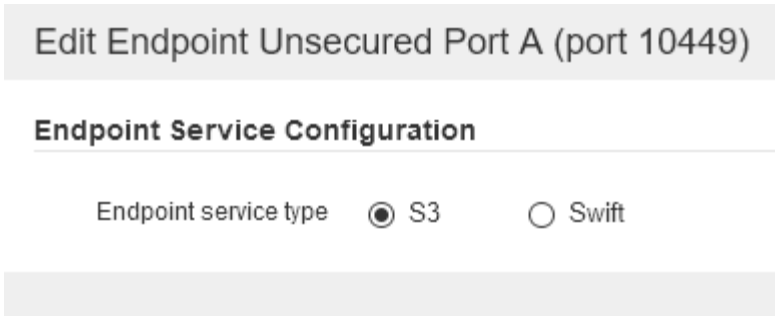
エンドポイントを表示するノードインターフェイスを選択します。



7. [保存（ Save ）] を選択します。

[Edit Endpoint]ダイアログボックスが表示されます。

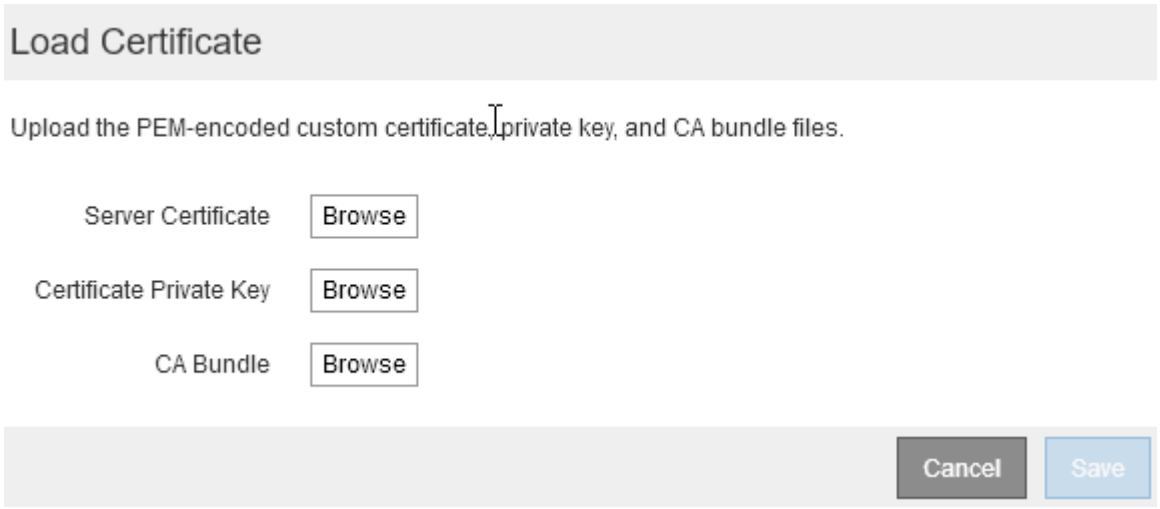
8. エンドポイントで処理するトラフィックのタイプを指定するには、「* S3 」または「 Swift *」を選択します。



9. *HTTP*を選択した場合は、*Save*を選択します。

   セキュアでないエンドポイントが作成されます。ロードバランサエンドポイントのページのテーブルには、エンドポイントの表示名、ポート番号、プロトコル、およびエンドポイントIDが表示されます。

10. [* HTTPS*]を選択し、証明書をアップロードする場合は、[証明書のアップロード]を選択します。



   a. サーバ証明書と証明書の秘密鍵を参照します。

      S3クライアントがS3 APIエンドポイントのドメイン名を使用して接続できるようにするには、クライアントがグリッドへの接続に使用する可能性のあるすべてのドメイン名に一致するマルチドメイン証明書またはワイルドカード証明書を使用します。たとえば、サーバ証明書でドメイン名を使用しているとします `*.example.com`。

"S3 APIエンドポイントのドメイン名を設定しています"

   a. 必要に応じて、CAバンドルを参照します。

   b. [保存（ Save ）] を選択します。

      エンドポイントのPEMでエンコードされた証明書データが表示されます。

11. [* HTTPS*]を選択し、証明書を生成する場合は、[証明書の生成]を選択します。

a. ドメイン名またはIPアドレスを入力します。

   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： `*.sgws.foo.com` ワイルドカード*を使用して表します `gn1.sgws.foo.com` および `gn2.sgws.foo.com`。

"S3 APIエンドポイントのドメイン名を設定しています"

a. 選択するオプション ➕ をクリックして、他のドメイン名またはIPアドレスを追加します。

   ハイアベイラビリティ（HA）グループを使用する場合は、HA仮想IPのドメイン名とIPアドレスを追加します。

b. 必要に応じて、証明書を所有するユーザを識別するために、[X.509 subject]（識別名（DN）とも呼ばれる）を入力します。

c. 必要に応じて、証明書の有効日数を選択します。デフォルトは730日です。

d. [*Generate （生成）] を選択します

   エンドポイントの証明書メタデータとPEMでエンコードされた証明書データが表示されます。

12. [保存（ Save ）] をクリックします。

エンドポイントが作成されます。ロードバランサエンドポイントのページのテーブルには、エンドポイントの表示名、ポート番号、プロトコル、およびエンドポイントIDが表示されます。

関連情報

""

"ネットワークガイドライン"

"ハイアベイラビリティグループの管理"

"信頼されていないクライアントネットワークの管理"

ロードバランサエンドポイントの編集

セキュアでない（HTTP）エンドポイントの場合、エンドポイントのサービスタイプ（S3またはSwift）を変更できます。セキュアな（HTTPS）エンドポイントの場合、エンドポイントのサービスタイプを編集して、セキュリティ証明書を表示または変更できます。

必要なもの

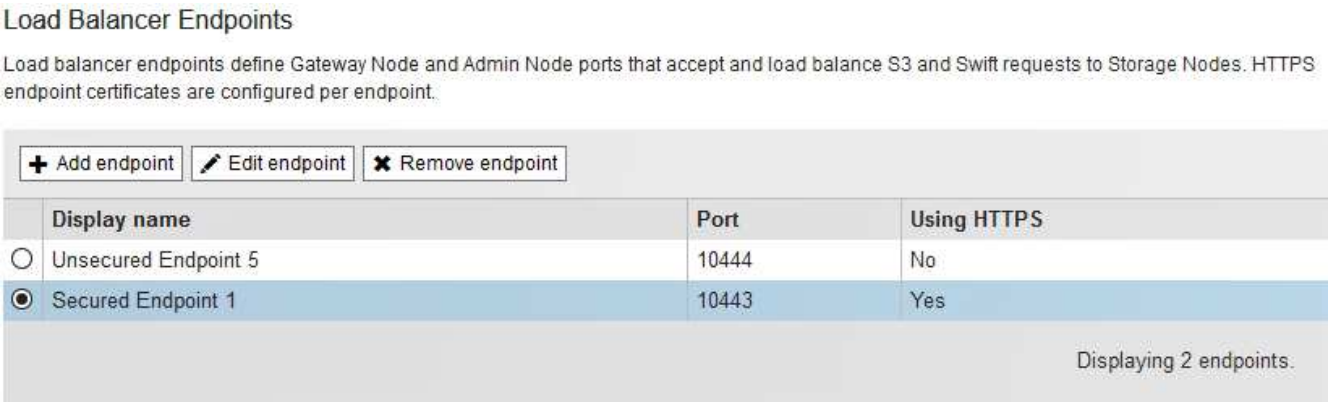
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。既存のエンドポイントがテーブルに表示されます。

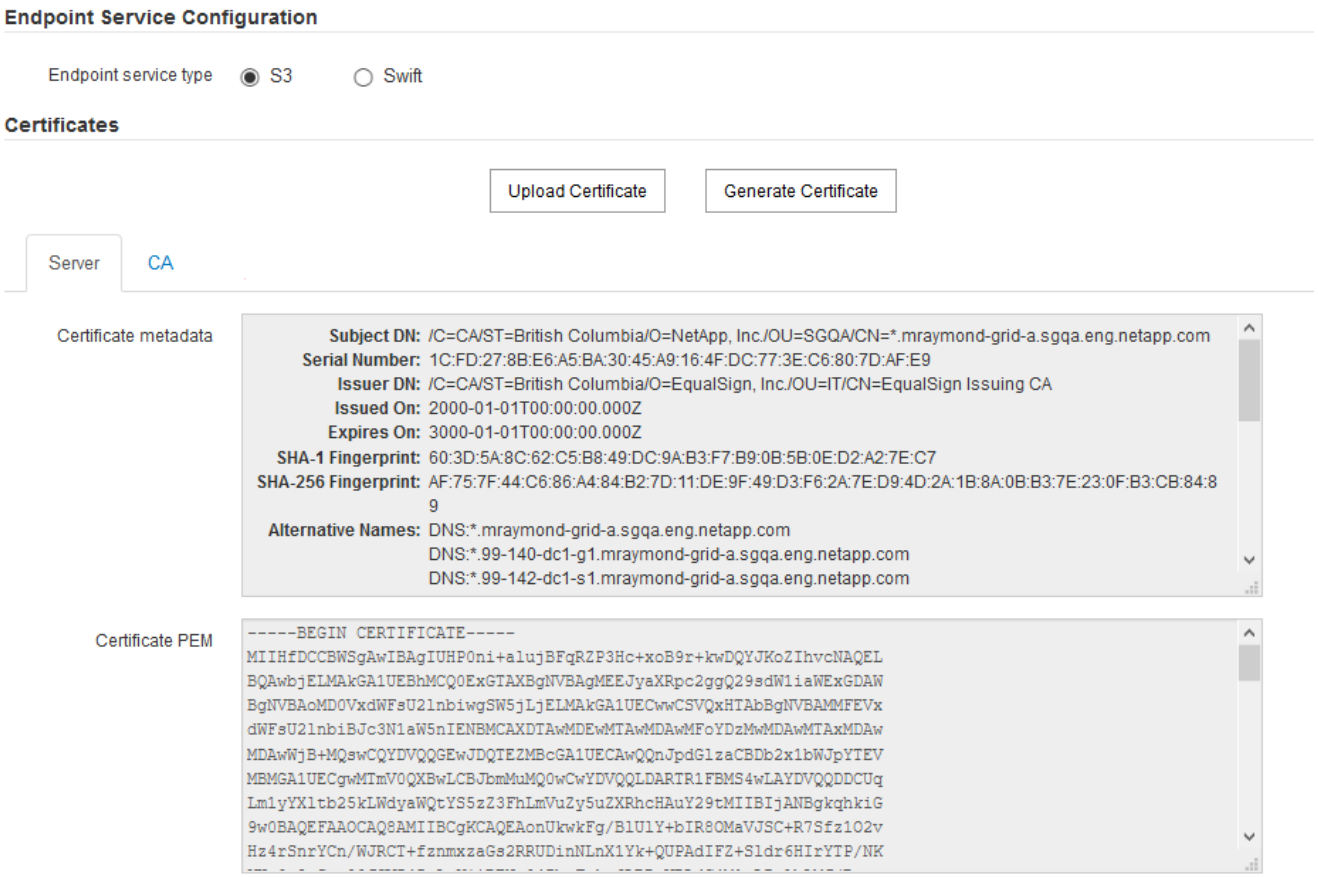
   まもなく期限切れになる証明書を含むエンドポイントが表に示されます。



2. 編集するエンドポイントを選択します。
3. *エンドポイントの編集*をクリックします。

   [Edit Endpoint]ダイアログボックスが表示されます。

   セキュアでない（HTTP）エンドポイントの場合は、ダイアログボックスの[Endpoint Service Configuration]セクションだけが表示されます。セキュア（HTTPS）エンドポイントの場合、次の例に示すように、ダイアログボックスの[Endpoint Service Configuration]セクションと[Certificates]セクションが表示されます。



4. エンドポイントに必要な変更を加えます。

   セキュアでない（HTTP）エンドポイントの場合、次の操作を実行できます。

   - エンドポイントのサービスタイプをS3またはSwiftに変更します。
   - エンドポイントバインディングモードを変更します。セキュアな（HTTPS）エンドポイントの場合、次の操作を実行できます。
   - エンドポイントのサービスタイプをS3またはSwiftに変更します。
   - エンドポイントバインディングモードを変更します。
   - セキュリティ証明書を表示します。
   - 現在の証明書の有効期限が切れたとき、または有効期限が近づいたときに、新しいセキュリティ証明書をアップロードまたは生成します。

     タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。

   既存のエンドポイントのプロトコルを変更する場合は、たとえばHTTPからHTTPSに変更する場合は、新しいエンドポイントを作成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手順に従って、必要なプロトコルを選択します。

5. [保存（ Save ）] をクリックします。

関連情報

[ロードバランサエンドポイントの作成]

ロードバランサエンドポイントの削除

不要になったロードバランサエンドポイントは削除できます。

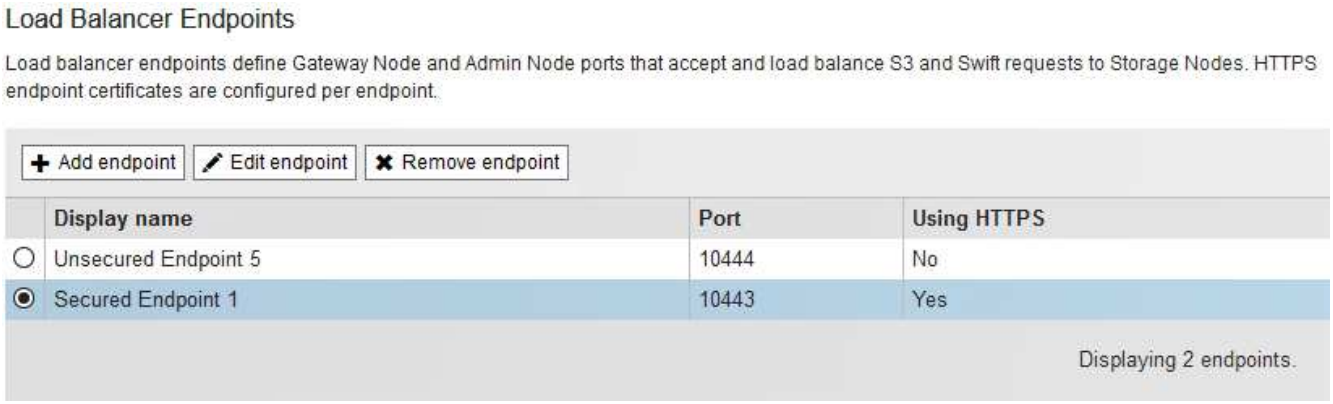
必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。既存のエンドポイントがテーブルに表示されます。



2. 削除するエンドポイントの左側にあるオプションボタンを選択します。
3. [エンドポイントの削除*]をクリックします。

   確認のダイアログボックスが表示されます。

4. [OK] をクリックします。

   エンドポイントが削除されます。

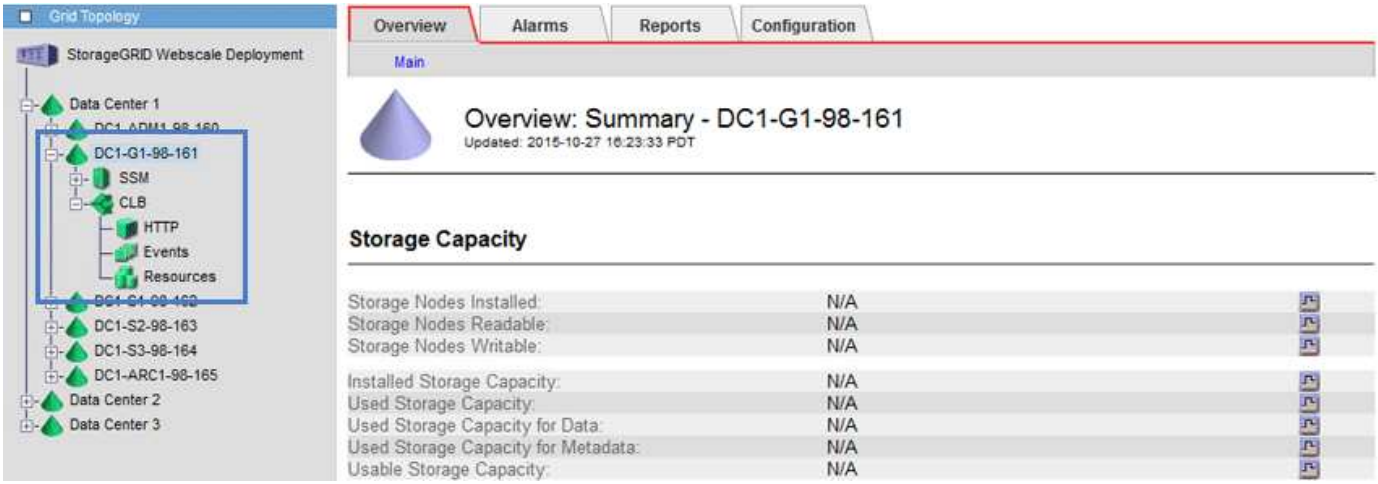
ロードバランシングの仕組み - CLB サービス

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、 CLB *と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。

関連情報

"リンクコストとは"

"リンクコストを更新しています"

信頼されていないクライアントネットワークの管理

クライアントネットワークを使用している場合は、明示的に設定されたエンドポイントでのみインバウンドクライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護できます。

デフォルトでは、各グリッドノードのクライアントネットワークは *trusted_* です。つまり、StorageGRID は、使用可能なすべての外部ポートでの各グリッドノードへのインバウンド接続をデフォルトで信頼します（ネットワークガイドラインの外部通信に関する情報を参照）。

各ノードのクライアントネットワークを「 *untrusted_* 」に指定することで、 StorageGRID システムに対する悪意ある攻撃の脅威を軽減できます。ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートのインバウンド接続だけを受け入れます。

例 1 ：ゲートウェイノードが HTTPS S3 要求のみを受け入れる

ゲートウェイノードで、 HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックを拒否するとします。この場合、次の一般的な手順を実行します。

1. Load Balancer Endpoints ページで、ポート 443 で S3 over HTTPS のロードバランサエンドポイントを設定します。
2. Untrusted Client Networks ページで、ゲートウェイノードのクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ポート 443 での HTTPS S3 要求と ICMP エコー（ ping ）要求を除き、ゲートウェイノードのクライアントネットワーク上のすべてのインバウンドトラフィックが破棄されます。

例 2 ：ストレージノードが S3 プラットフォームサービス要求を送信する

あるストレージノードからのアウトバウンド S3 プラットフォームサービストラフィックは有効にするが、クライアントネットワークでそのストレージノードへのインバウンド接続は禁止するとします。この場合は、次の手順を実行します。

- Untrusted Client Networks ページで、ストレージノード上のクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ストレージノードはクライアントネットワークで受信トラフィックを受け入れなくなりますが、 Amazon Web Services へのアウトバウンド要求は引き続き許可します。

関連情報

"ネットワークガイドライン"

"ロードバランサエンドポイントの設定"

ノードのクライアントネットワークの指定は信頼されていません

クライアントネットワークを使用している場合は、各ノードのクライアントネットワークが信頼されているかどうかを指定できます。拡張で追加した新しいノードのデフォルト設定を指定することもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 管理ノードまたはゲートウェイノードが明示的に設定されたエンドポイントでのみインバウンドトラフィックを受け入れるように設定する場合は、ロードバランサエンドポイントを定義しておきます。

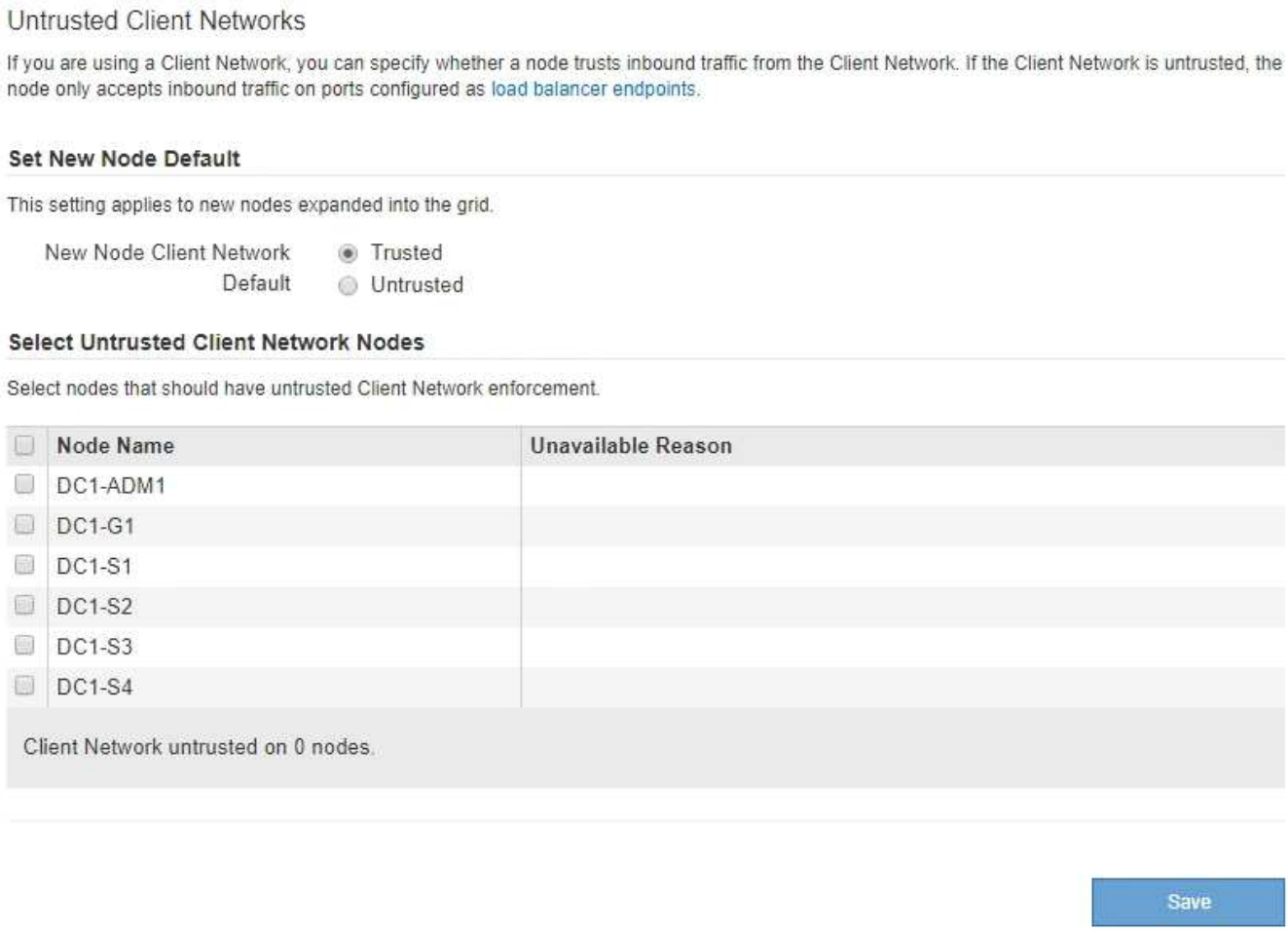
> ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

手順

1. 「* Configuration * Network Settings * Untrusted Client Network *」を選択します。

[Untrusted Client Networks]ページが表示されます。

このページには、StorageGRID システム内のすべてのノードが表示されます。ノードのクライアントネットワークが信頼されている必要がある場合は、 Unavailable Reason 列にエントリが表示されます。



2. Set New Node Default * セクションで、拡張手順 で新しいノードをグリッドに追加するときのデフォルト設定を指定します。

   - * Trusted * ：拡張でノードが追加されるときに、そのクライアントネットワークが信頼されます。
   - * Untrusted * ：拡張でノードが追加されるときに、そのクライアントネットワークは信頼されません。必要に応じて、このページに戻って新しいノードの設定を変更できます。

   この設定は、 StorageGRID システム内の既存のノードには影響しません。

3. Select Untrusted Client Network Nodes * セクションで、明示的に設定されたロードバランサエンドポイントでのみクライアント接続を許可するノードを選択します。

   タイトルのチェックボックスをオンまたはオフにすると、すべてのノードを選択または選択解除できます。

4. [保存（ Save ）] をクリックします。

   新しいファイアウォールルールがすぐに追加され、適用されます。ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

関連情報

"ロードバランサエンドポイントの設定"

ハイアベイラビリティグループの管理

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できます。HAグループを使用して、Grid ManagerとTenant Managerへの可用性の高い接続を提供することもできます。

- "HAグループとは"
- "HAグループの使用方法"
- "HA グループの設定オプション"
- "ハイアベイラビリティグループを作成する"
- "ハイアベイラビリティグループの編集"
- "ハイアベイラビリティグループを削除しています"

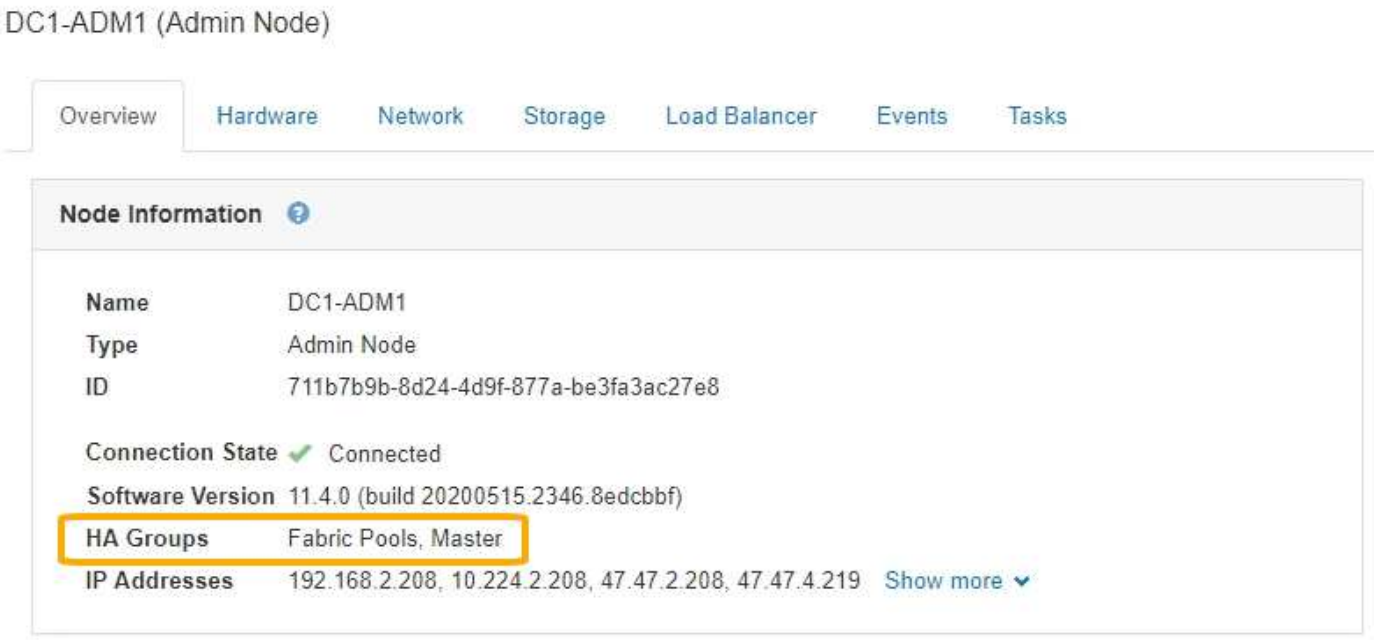
HAグループとは

ハイアベイラビリティグループは、仮想IPアドレス（VIP）を使用してゲートウェイノードまたは管理ノードサービスへのアクティブ/バックアップアクセスを提供します。

HAグループは、管理ノードとゲートウェイノード上の1つ以上のネットワークインターフェイスで構成されます。HAグループを作成するときは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属するネットワークインターフェイスを選択します。HAグループ内のすべてのインターフェイスは、同じネットワークサブネット内に存在する必要があります。

HAグループは、グループ内のアクティブインターフェイスに追加された仮想IPアドレスを1つ以上維持します。アクティブインターフェイスが使用できなくなった場合、仮想IPアドレスは別のインターフェイスに移動します。この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への影響はほとんどなく、通常の再試行で処理を続行できます。

HAグループ内のアクティブインターフェイスがマスターに、他のすべてのインターフェイスは、バックアップとして指定されます。これらの指定を表示するには、* Nodes **>*_node_name >** Overview *を選択します。



HAグループを作成する際には、1つのインターフェイスを優先マスターに指定します。優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。障害が解決されると、VIPアドレスは自動的に優先マスターに戻されます。

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。

HAグループに3つ以上のノードのインターフェイスが含まれている場合、フェイルオーバー中にアクティブインターフェイスは他のノードのインターフェイスに移動する可能性があります。

HAグループの使用方法

ハイアベイラビリティ（HA）グループはいくつかの理由で使用できます。

- 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（優先マスター） • 非プライマリ管理ノード *注：*プライマリ管理ノードが優先マスター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
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またはTenant Managerのサービスで障害が発生しても、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。

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

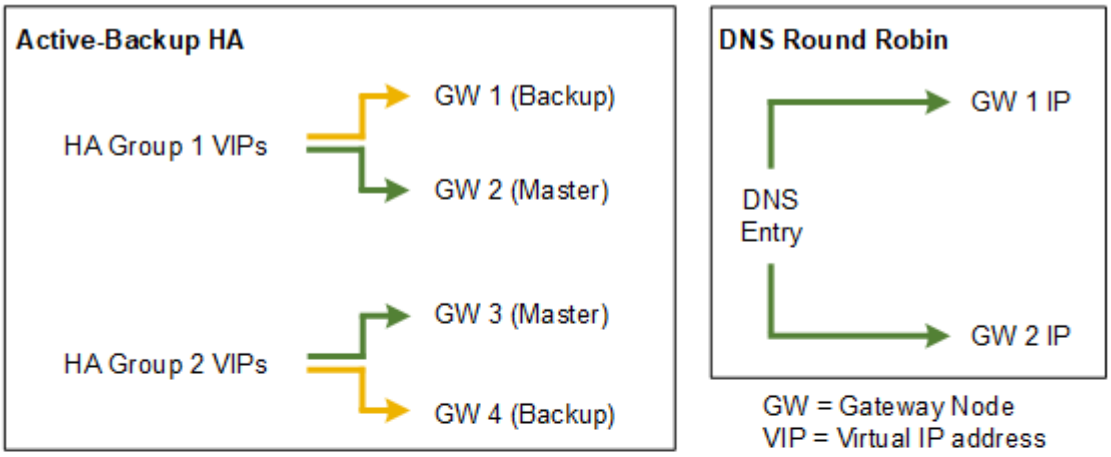
CLB サービスに障害が発生しても、 HA グループ内でフェイルオーバーはトリガーされません。

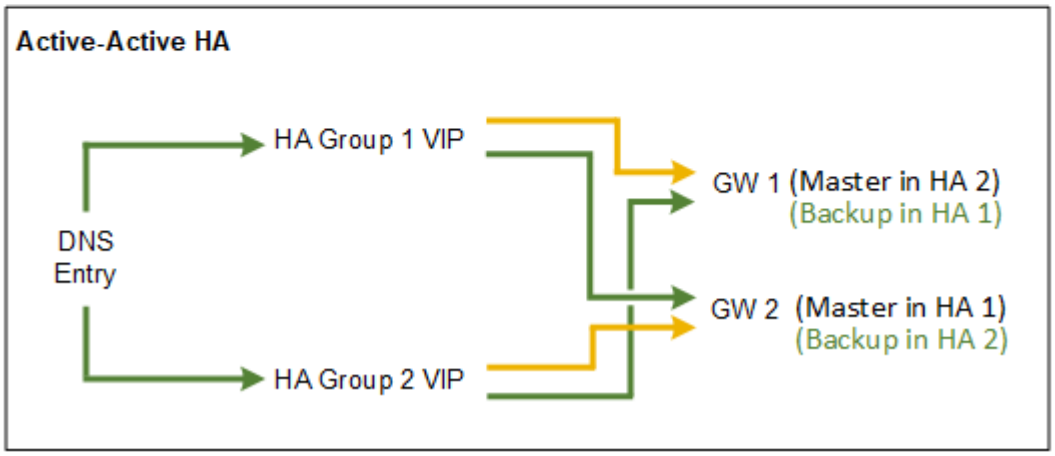
CLB サービスは廃止されました。

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。





「アクティブ/アクティブHA」の例に示すように、複数の重複するHAグループを作成する場合、合計スループットはノード数とHAグループ数が増えるほど上昇します。ノードとHAグループをそれぞれ3つ以上配置すると、1つのノードをオフラインにする必要があるメンテナンス手順の実行中も、いずれかのVIPを使用して処理を継続できます。

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。

設定	利点	欠点
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。
アクティブ/アクティブ	• 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作成する

1つ以上のハイアベイラビリティ（HA）グループを作成して、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

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

HAグループに追加するインターフェイスは次の条件を満たしている必要があります。

- インターフェイスは、ゲートウェイノードまたは管理ノードのものである必要があります。
- インターフェイスはグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属している必要があります。
- インターフェイスには、DHCPではなく固定IPアドレスまたは静的IPアドレスを設定する必要があります。

手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。

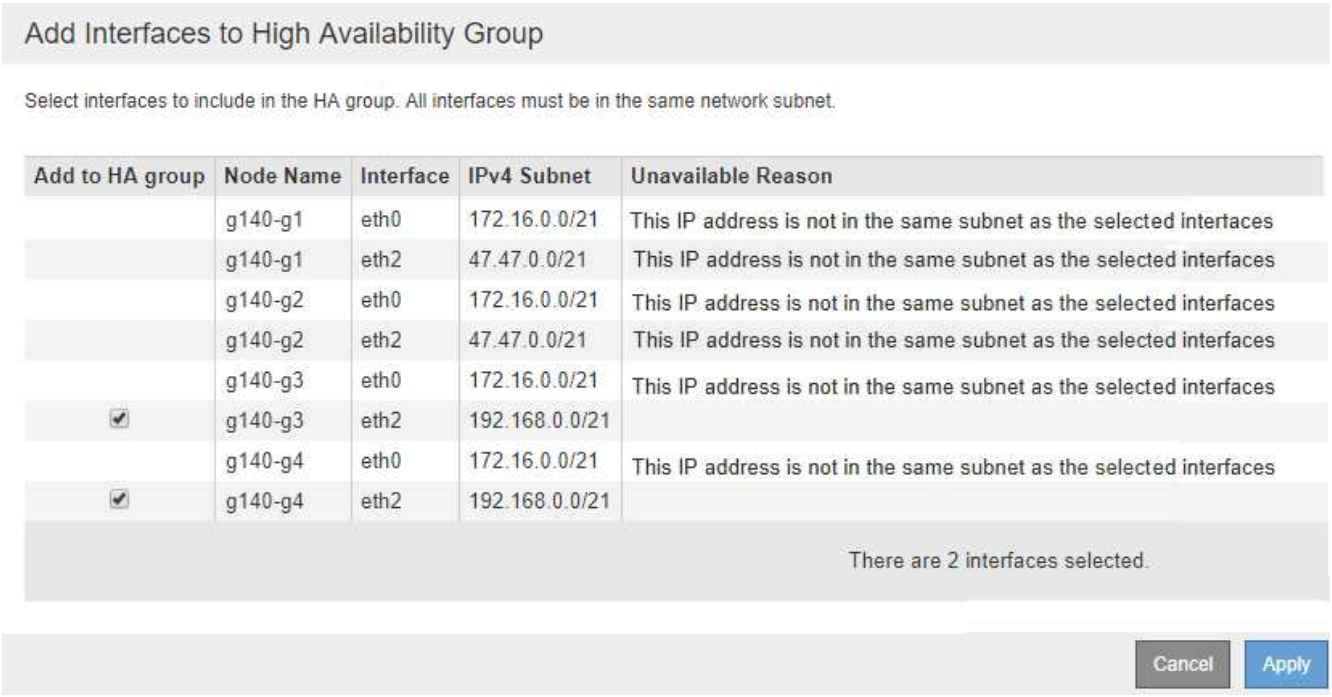
   [High Availability Groups]ページが表示されます。

2. [作成（ Create ）] をクリックします。

   Create High Availability Groupダイアログボックスが表示されます。

3. HAグループの名前を入力し、必要に応じて概要 を入力します。
4. [Select Interfaces]をクリックします。

   Add Interfaces to High Availability Groupダイアログボックスが表示されます。この表には、使用可能なノード、インターフェイス、およびIPv4サブネットが表示されます。



   IPアドレスがDHCPによって割り当てられている場合、インターフェイスはリストに表示されません。

5. Add to HA group *列で、HAグループに追加するインターフェイスのチェックボックスを選択します。

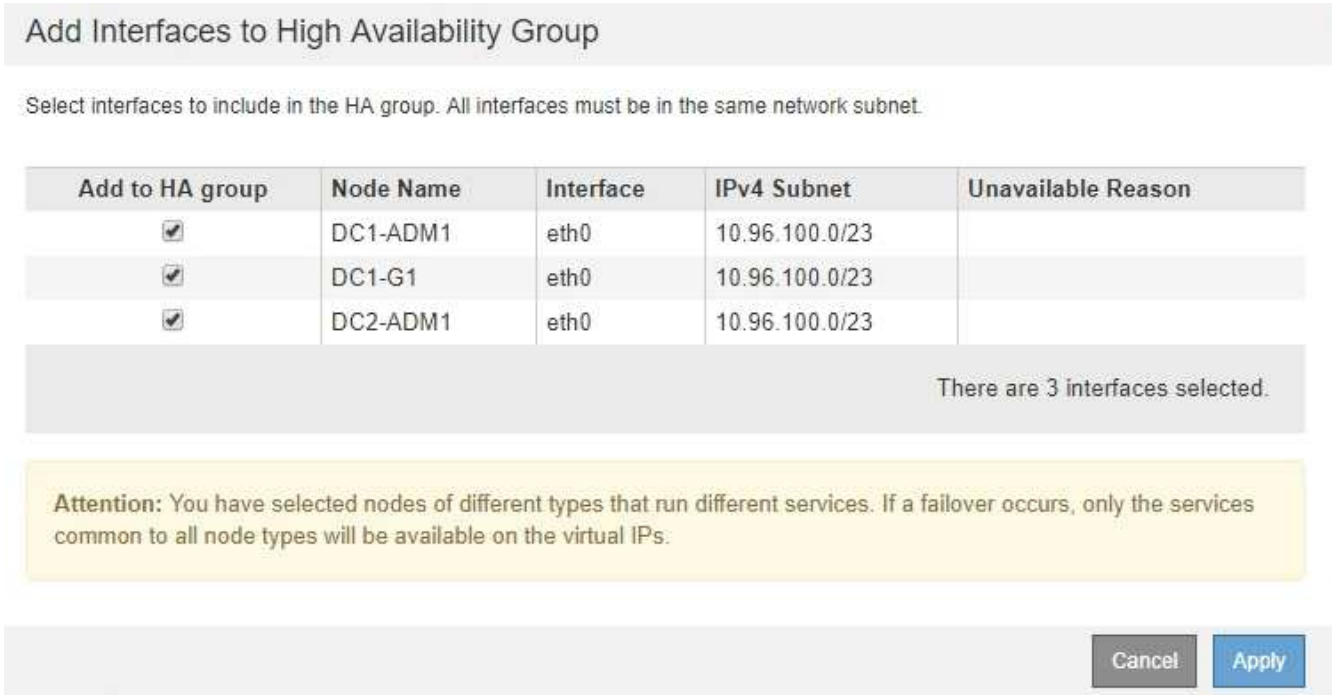
   インターフェイスの選択に関する次のガイドラインに注意してください。

   - インターフェイスを少なくとも 1 つ選択してください。
   - 複数のインターフェイスを選択する場合は、すべてのインターフェイスがグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上に存在する必要があります。
   - すべてのインターフェイスは、同じサブネット内または共通のプレフィックスを持つサブネット内に存在する必要があります。

IPアドレスは最小のサブネット（最大のプレフィックスを持つサブネット）に制限されます。

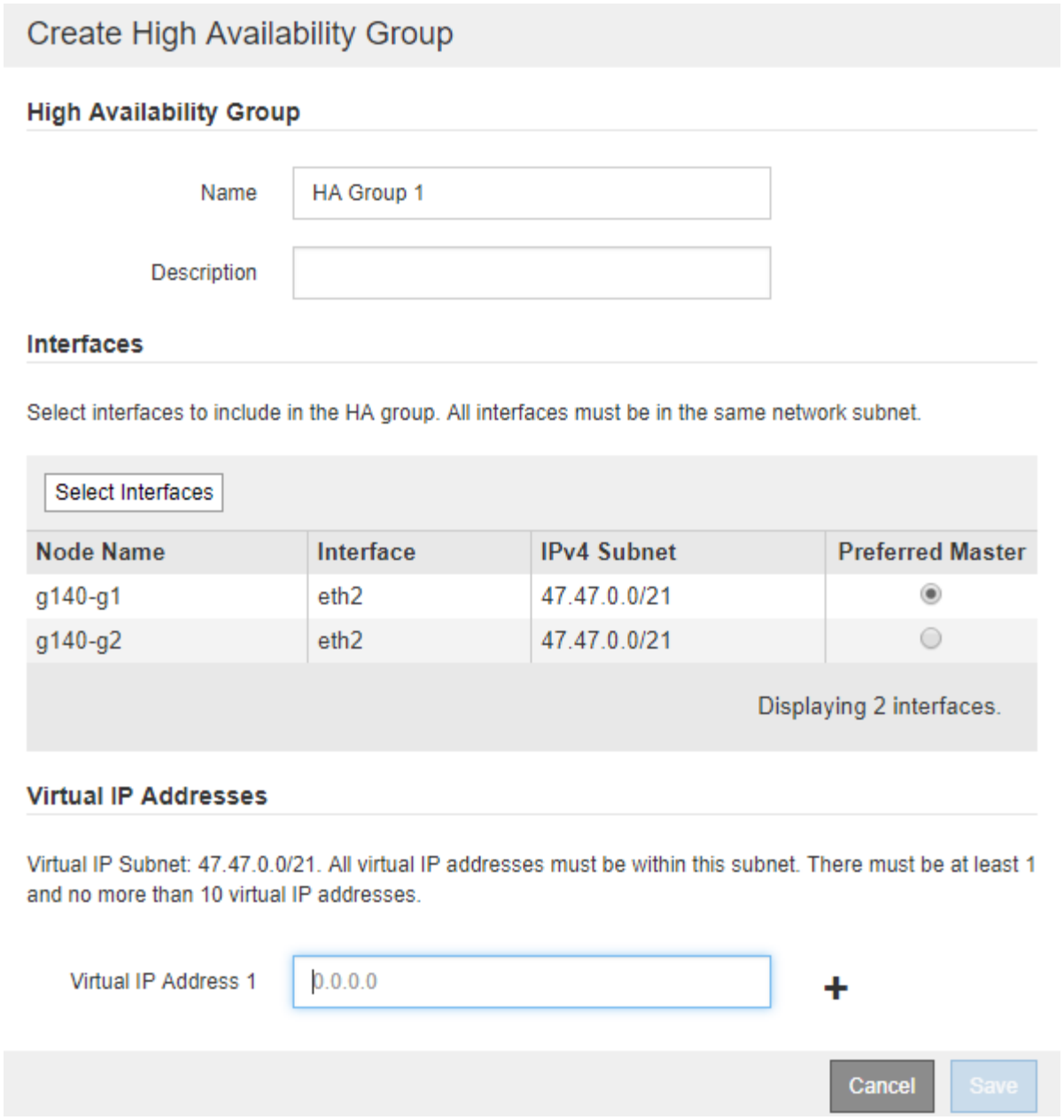
- 異なるタイプのノード上のインターフェイスを選択した場合、フェイルオーバーが発生すると、選択したノードに共通するサービスのみが仮想IPで使用可能になります。
  - Grid ManagerまたはTenant ManagerのHA保護用に2つ以上の管理ノードを選択します。
  - ロードバランササービスのHA保護を利用する場合は、管理ノード、ゲートウェイノード、またはその両方を2つ以上選択します。
  - CLBサービスのHA保護を行うゲートウェイノードを2つ以上選択します。

    CLB サービスは廃止されました。



6. [適用（ Apply ）] をクリックします。

選択したインターフェイスは、Create High Availability GroupページのInterfacesセクションに表示されます。デフォルトでは、リストの最初のインターフェイスが優先マスターとして選択されます。



7. 別のインターフェイスを優先マスターにする場合は、[* Preferred Master*（優先マスター*）]列でそのインターフェイスを選択します。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

   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優先マスターとして選択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。

8. ページの仮想IPアドレスセクションに、HAグループの仮想IPアドレスを1~10個入力します。プラス記号（+）をクリックして、複数のIPアドレスを追加します。

   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。

IPv4アドレスは、すべてのメンバーインターフェイスで共有されるIPv4サブネット内にある必要があります。

9. [保存（ Save ）] をクリックします。

   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。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"VMware をインストールする"

"Ubuntu または Debian をインストールします"

"負荷分散の管理"

ハイアベイラビリティグループの編集

ハイアベイラビリティ（HA）グループを編集して、グループ名や概要 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、仮想IPアドレスを追加または更新したりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

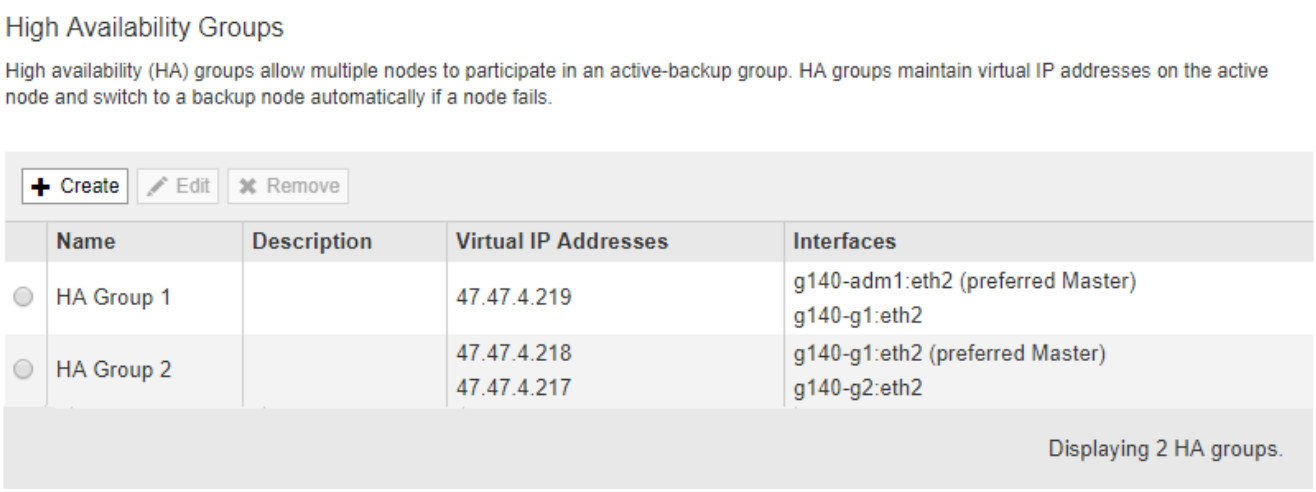
HAグループを編集する理由には、次のようなものがあります。

- 既存のグループにインターフェイスを追加しています。すでにグループに割り当てられている他のインターフェイスと同じサブネット内のインターフェイスのIPアドレスを指定する必要があります。
- HAグループからのインターフェイスの削除たとえば、グリッドネットワークまたはクライアントネットワークのノードのインターフェイスがHAグループで使用されている場合、サイトの開始や手順 のノードの運用停止はできません。

手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。

   [High Availability Groups]ページが表示されます。

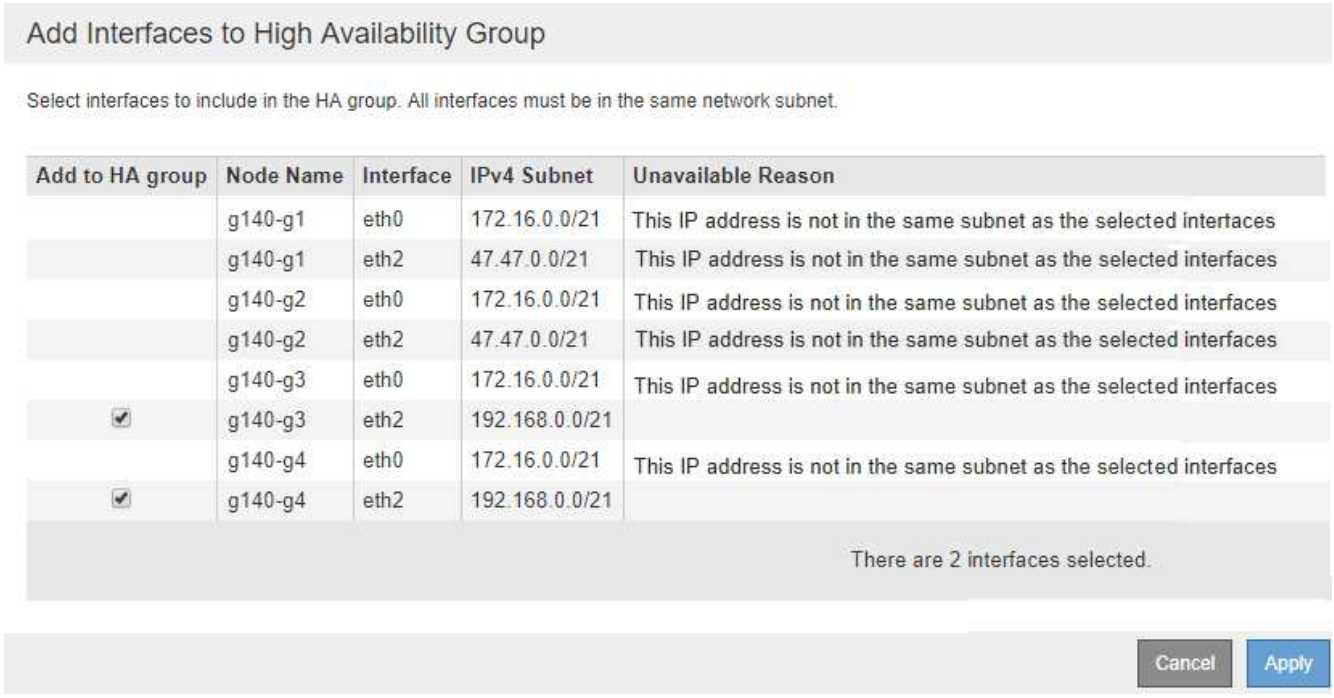


2. 編集するHAグループを選択し、* Edit *をクリックします。

   Edit High Availability Groupダイアログボックスが表示されます。

3. 必要に応じて、グループの名前または概要 を更新します。
4. 必要に応じて、* Select interfaces *をクリックして、HAグループのインターフェイスを変更します。

   Add Interfaces to High Availability Groupダイアログボックスが表示されます。



   IPアドレスがDHCPによって割り当てられている場合、インターフェイスはリストに表示されません。

5. 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。

   インターフェイスの選択に関する次のガイドラインに注意してください。

   ◦ インターフェイスを少なくとも 1 つ選択してください。

- 複数のインターフェイスを選択する場合は、すべてのインターフェイスがグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上に存在する必要があります。
- すべてのインターフェイスは、同じサブネット内または共通のプレフィックスを持つサブネット内に存在する必要があります。

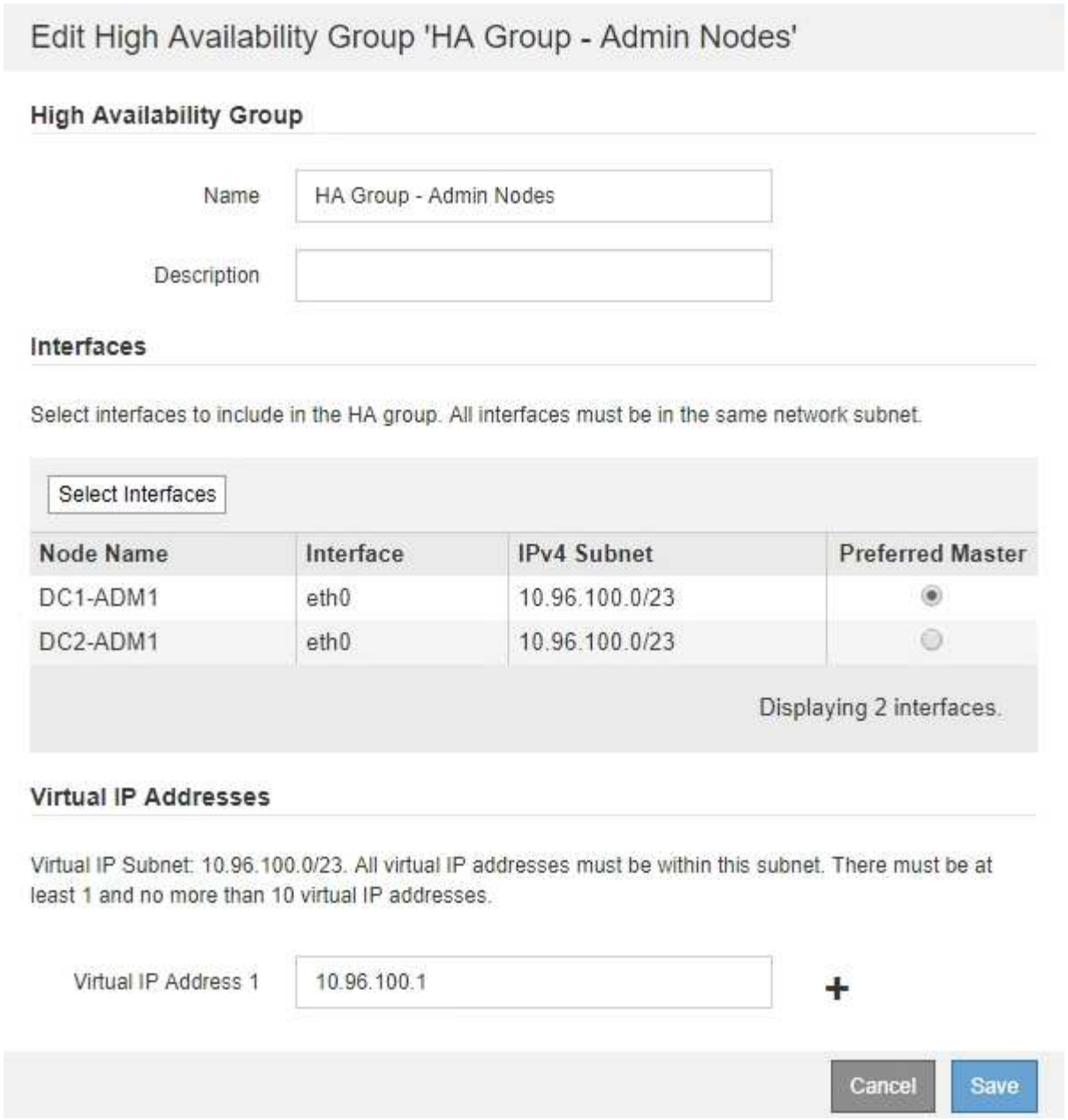
  IPアドレスは最小のサブネット（最大のプレフィックスを持つサブネット）に制限されます。

- 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、フェイルオーバーが発生すると、選択したノードに共通するサービスのみが仮想IPで使用可能になります。
  - Grid ManagerまたはTenant ManagerのHA保護用に2つ以上の管理ノードを選択します。
  - ロードバランササービスのHA保護を利用する場合は、管理ノード、ゲートウェイノード、またはその両方を2つ以上選択します。
  - CLBサービスのHA保護を行うゲートウェイノードを2つ以上選択します。

    CLB サービスは廃止されました。

6. [適用（ Apply ）] をクリックします。

   選択したインターフェイスがページのインターフェイスセクションに表示されます。デフォルトでは、リストの最初のインターフェイスが優先マスターとして選択されます。



7. 別のインターフェイスを優先マスターにする場合は、[* Preferred Master*（優先マスター*）]列でそのインターフェイスを選択します。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

   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優先マスターとして選択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。

8. 必要に応じて、HAグループの仮想IPアドレスを更新します。

   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。

   IPv4アドレスは、すべてのメンバーインターフェイスで共有されるIPv4サブネット内にある必要がありま

す。

9. [保存（ Save ）] をクリックします。

   HAグループが更新されました。

ハイアベイラビリティグループを削除しています

使用しなくなったハイアベイラビリティ（HA）グループを削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

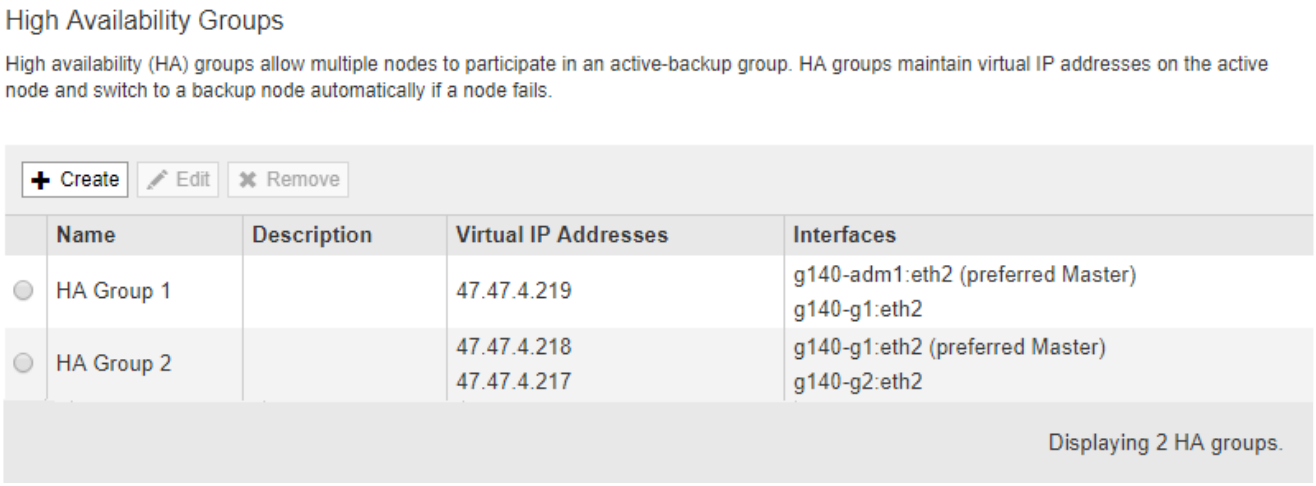
このタスクを実行します

HAグループを削除すると、そのグループのいずれかの仮想IPアドレスを使用するように設定されているS3またはSwiftクライアントはStorageGRID に接続できなくなります。クライアントの停止を回避するには、該当するS3またはSwiftクライアントアプリケーションをすべて更新してからHAグループを削除する必要があります。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、インストール時またはDHCPを使用して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

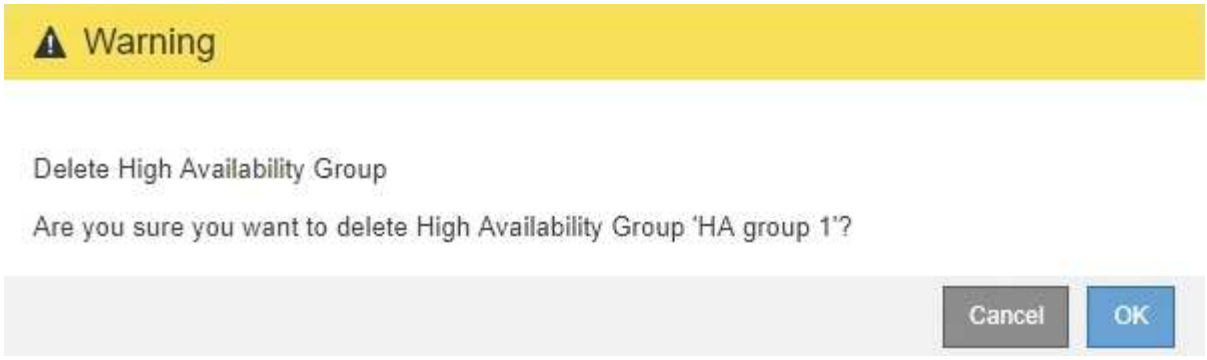
1. * Configuration **>** Network Settings **>** High Availability Groups *を選択します。

   [High Availability Groups]ページが表示されます。



2. 削除するHAグループを選択し、* Remove *をクリックします。

   Delete High Availability Groupという警告が表示されます。



3. [OK] をクリックします。

   HAグループが削除されます。

S3 APIエンドポイントのドメイン名を設定しています

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

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 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ておく必要があります。

  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、エンドポイントがの場合などです `s3.company.com`、HTTPS接続に使用する証明書にが含まれていることを確認する必要があります `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`。

- 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。

クライアントがHTTPS接続に使用する証明書は、クライアントがグリッドに接続する方法によって異なります。

- ロードバランササービスを使用して接続する場合、クライアントは特定のロードバランサエンドポイント用の証明書を使用します。

  各ロードバランサエンドポイントには独自の証明書があり、異なるエンドポイントドメイン名を認識するように各エンドポイントを設定できます。

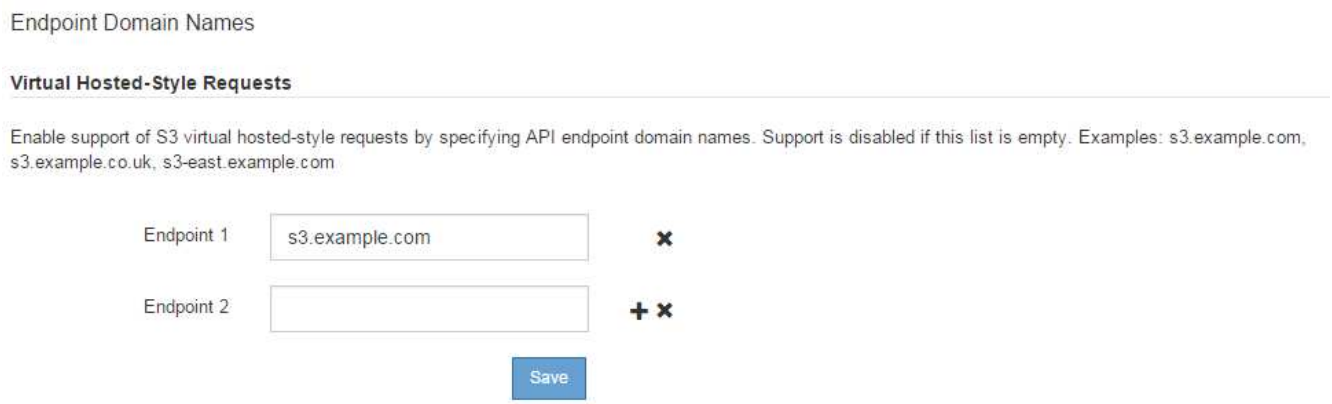
- クライアントがストレージノードまたはゲートウェイノード上のCLBサービスに接続する場合、クライアントは、必要なエンドポイントのドメイン名をすべて追加して更新されたグリッドのカスタムサーバ証明書を使用します。

  CLB サービスは廃止されました。

手順

1. [環境設定]>[ネットワーク設定]>[ドメイン名]を選択します。

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



2. （+）アイコンを使用してフィールドを追加し、* Endpoint *フィールドにS3 APIエンドポイントのドメイン名のリストを入力します。

   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 ）] をクリックします。
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。
   - ロードバランササービスを使用するクライアントの場合は、クライアントが接続するロードバランサ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。

- 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CLBサービスを使用するクライアントの場合は、グリッドのカスタムサーバ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を使用するようになります `bucket.s3.company.com`を指定すると、DNSサーバが正しいエンドポイントに解決され、証明書がエンドポイントを認証します。

関連情報

"S3 を使用する"

"IPアドレスを表示しています"

"ハイアベイラビリティグループを作成する"

"ストレージノードまたはCLBサービスへの接続用のカスタムサーバ証明書を設定する"

"ロードバランサエンドポイントの設定"

クライアント通信での**HTTP**の有効化

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

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 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. 「環境設定*システム設定*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 ）] をクリックします。

関連情報

"ロードバランサエンドポイントの設定"

"S3 を使用する"

"Swift を使用します"

許可するクライアント処理の制御

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

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 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

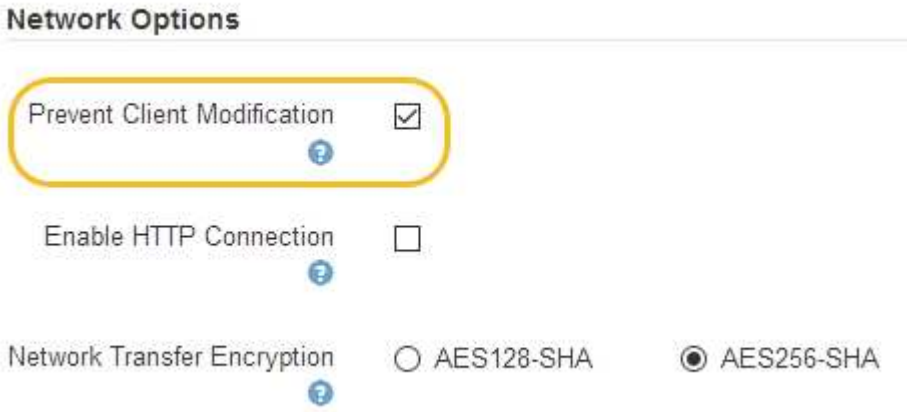
> この設定は、バージョン管理が有効なバケットには適用されません。バージョン管理によって、すでにオブジェクトデータ、ユーザ定義メタデータ、オブジェクトのタグを変更できないようになっています。

- * 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. 「環境設定*システム設定*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 ）] をクリックします。