クライアント接続を構成する
StorageGRID software

NetApp
December 03, 2025

目次

クライアント接続を構成する 1
S3クライアント接続を構成する 1
構成タスク 1
StorageGRIDをクライアントアプリケーションに接続するために必要な情報 2
S3 クライアントのセキュリティ 3
まとめ 3
StorageGRIDがクライアントアプリケーションにセキュリティを提供する仕組み 4
TLSライブラリでサポートされているハッシュおよび暗号化アルゴリズム 5
S3セットアップウィザードを使用する 5
S3 セットアップウィザードの使用: 考慮事項と要件 5
S3 セットアップウィザードにアクセスして完了する 6
HAグループの管理 14
高可用性 (HA) グループとは何ですか? 15
HA グループはどのように使用されますか? 17
HAグループの構成オプション 18
高可用性グループを構成する 20
負荷分散を管理する 25
負荷分散に関する考慮事項 25
ロードバランサのエンドポイントを構成する 29
S3エンドポイントのドメイン名を設定する 40
S3エンドポイントドメイン名を追加する 42
S3エンドポイントのドメイン名を変更する 42
S3エンドポイントドメイン名を削除する 42
概要: クライアント接続の IP アドレスとポート 43
URLの例 43
IPアドレスを見つける場所 44

クライアント接続を構成する

S3クライアント接続を構成する

グリッド管理者は、S3 クライアント アプリケーションがStorageGRIDシステムに接続してデータを保存および取得する方法を制御する構成オプションを管理します。

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 "StorageGRID 11.8: S3およびSwiftクライアント接続の設定"。

構成タスク

1. クライアント アプリケーションがStorageGRIDに接続する方法に基づいて、 StorageGRIDで前提条件となるタスクを実行します。

必要なタスク

以下のものを取得する必要があります:

- IPアドレス
- ドメイン名
- SSL証明書

オプションタスク

オプションで、以下を設定します。

- アイデンティティ連携
- SSO

1. StorageGRIDを使用して、アプリケーションがグリッドに接続するために必要な値を取得します。 S3 セットアップ ウィザードを使用するか、各StorageGRIDエンティティを手動で構成することができます。+

S3セットアップウィザードを使用する

S3 セットアップ ウィザードの手順に従います。

手動で設定する

1. 高可用性グループを作成する
2. ロードバランサエンドポイントを作成する
3. テナントアカウントを作成する
4. バケットとアクセスキーを作成する
5. ILMルールとポリシーを構成する

1. S3 アプリケーションを使用して、 StorageGRIDへの接続を完了します。 DNS エントリを作成し、使用する予定のドメイン名に IP アドレスを関連付けます。

   必要に応じて、追加のアプリケーションセットアップを実行します。

2. アプリケーションとStorageGRIDで継続的なタスクを実行し、オブジェクト ストレージを長期にわたって管理および監視します。

StorageGRIDをクライアントアプリケーションに接続するために必要な情報

StorageGRID をS3 クライアント アプリケーションに接続する前に、 StorageGRIDで設定手順を実行し、特定の値を取得する必要があります。

どのような値が必要ですか**?**

次の表は、 StorageGRIDで設定する必要がある値と、それらの値が S3 アプリケーションおよび DNS サーバーによって使用される場所を示しています。

Value	値が設定される場所	価値が使われる場所
仮想IP（VIP）アドレス	StorageGRID > HAグループ	DNSエントリ
ポート	StorageGRID > ロードバランサエンドポイント	クライアントアプリケーション
SSL証明書	StorageGRID > ロードバランサエンドポイント	クライアントアプリケーション
サーバー名（FQDN）	StorageGRID > ロードバランサエンドポイント	• クライアントアプリケーション • DNSエントリ
S3 アクセスキー ID とシークレットアクセスキー	StorageGRID > テナントとバケット	クライアントアプリケーション
バケット/コンテナ名	StorageGRID > テナントとバケット	クライアントアプリケーション

これらの値を取得するにはどうすればいいでしょうか**?**

要件に応じて、次のいずれかの方法で必要な情報を取得できます。

- *"S3 セットアップウィザード" *。 S3 セットアップ ウィザードを使用すると、 StorageGRIDで必要な値を簡単に構成でき、S3 アプリケーションを構成するときに使用できる 1 つまたは 2 つのファイルを出力できます。ウィザードは必要な手順をガイドし、設定がStorageGRID のベスト プラクティスに準拠していることを確認できるようにします。

S3 アプリケーションを構成する場合は、特別な要件があることがわかっている場合や実装に大幅なカスタマイズが必要になる場合を除き、S3 セットアップ ウィザードを使用することをお勧めします。

- *"FabricPoolセットアップ ウィザード" *。 S3 セットアップ ウィザードと同様に、 FabricPoolセットアップ ウィザードを使用すると、必要な値をすばやく設定し、 ONTAPでFabricPoolクラウド層を設定するときに使用できるファイルを出力できます。

StorageGRID をFabricPoolクラウド層のオブジェクト ストレージ システムとして使用することを計画している場合は、特別な要件があることがわかっている場合や実装に大幅なカスタマイズが必要であることがない限り、 FabricPoolセットアップ ウィザードを使用することをお勧めします。

- 項目を手動で設定します。 S3 アプリケーションに接続していて、S3 セットアップ ウィザードを使用しない場合は、手動で構成を実行して必要な値を取得できます。次の手順を実行します。
  a. S3 アプリケーションに使用する高可用性 (HA) グループを構成します。見る"高可用性グループを構成する" 。
  b. S3 アプリケーションが使用するロードバランサーエンドポイントを作成します。見る"ロードバランサのエンドポイントを構成する" 。
  c. S3 アプリケーションが使用するテナント アカウントを作成します。見る"テナントアカウントを作成する" 。
  d. S3 テナントの場合は、テナント アカウントにサインインし、アプリケーションにアクセスする各ユーザーのアクセス キー ID とシークレット アクセス キーを生成します。見る"独自のアクセスキーを作成する" 。
  e. テナント アカウント内に 1 つ以上の S3 バケットを作成します。 S3については、"S3バケットを作成する" 。
  f. 新しいテナントまたはバケット/コンテナに属するオブジェクトに特定の配置指示を追加するには、新しい ILM ルールを作成し、そのルールを使用する新しい ILM ポリシーをアクティブ化します。見る"ILMルールを作成する"そして"ILMポリシーを作成する"。

S3 クライアントのセキュリティ

StorageGRIDテナント アカウントは、S3 クライアント アプリケーションを使用してオブジェクト データをStorageGRIDに保存します。クライアント アプリケーションに実装されているセキュリティ対策を確認する必要があります。

まとめ

次のリストは、S3 REST API のセキュリティの実装方法をまとめたものです。

接続セキュリティ
: TLS

サーバー認証
: システム CA によって署名された X.509 サーバー証明書または管理者によって提供されたカスタム サーバー証明書

クライアント認証

S3 アカウントのアクセスキー ID とシークレットアクセスキー

クライアント許可

バケットの所有権と適用可能なすべてのアクセス制御ポリシー

StorageGRIDがクライアントアプリケーションにセキュリティを提供する仕組み

S3 クライアント アプリケーションは、ゲートウェイ ノードまたは管理ノード上のロード バランサ サービスに接続するか、ストレージ ノードに直接接続できます。

- ロードバランサーサービスに接続するクライアントは、接続方法に応じてHTTPSまたはHTTPを使用できます。"ロードバランサのエンドポイントを構成する" 。

  HTTPS は安全な TLS 暗号化通信を提供するため、推奨されます。エンドポイントにセキュリティ証明書を添付する必要があります。

  HTTP は安全性が低く、暗号化されていない通信を提供するため、非本番環境またはテスト グリッドにのみ使用する必要があります。

- ストレージ ノードに接続するクライアントは、HTTPS または HTTP も使用できます。

  HTTPS がデフォルトであり、推奨されます。

  HTTPは安全性が低く、暗号化されていない通信を提供しますが、オプションで"有効"非本番環境またはテスト グリッド用。

- StorageGRIDとクライアント間の通信は TLS を使用して暗号化されます。
- ロード バランサ エンドポイントが HTTP 接続または HTTPS 接続を受け入れるように構成されているかどうかに関係なく、グリッド内のロード バランサ サービスとストレージ ノード間の通信は暗号化されます。
- クライアントは以下を提供する必要があります"HTTP認証ヘッダー"REST API 操作を実行するためにStorageGRIDを使用します。

セキュリティ証明書とクライアントアプリケーション

いずれの場合も、クライアント アプリケーションは、グリッド管理者がアップロードしたカスタム サーバー証明書またはStorageGRIDシステムによって生成された証明書を使用して TLS 接続を行うことができます。

- クライアント アプリケーションが Load Balancer サービスに接続すると、ロード バランサー エンドポイント用に構成された証明書が使用されます。各ロード バランサ エンドポイントには独自の証明書（グリッド管理者がアップロードしたカスタム サーバ証明書、またはエンドポイントの構成時にグリッド管理者がStorageGRIDで生成した証明書）があります。

  見る"負荷分散に関する考慮事項" 。

- クライアント アプリケーションがストレージ ノードに直接接続する場合、 StorageGRIDシステムのインストール時にストレージ ノード用に生成されたシステム生成サーバ証明書 (システム証明機関によって署名されている)、またはグリッド管理者によってグリッド用に提供される単一のカスタム サーバ証明書のいずれかを使用します。見る"カスタムS3 API証明書を追加する" 。

クライアントは、TLS 接続を確立するために使用する証明書に署名した証明機関を信頼するように構成する必要があります。

TLSライブラリでサポートされているハッシュおよび暗号化アルゴリズム

StorageGRIDシステムは、クライアント アプリケーションが TLS セッションを確立するときに使用できる暗号スイートのセットをサポートしています。暗号を構成するには、構成 > セキュリティ > セキュリティ設定に移動し、**TLS** および **SSH** ポリシー を選択します。

サポートされている**TLS**のバージョン

StorageGRID はTLS 1.2 と TLS 1.3 をサポートしています。

SSLv3 および TLS 1.1 (またはそれ以前のバージョン) はサポートされなくなりました。

S3セットアップウィザードを使用する

S3 セットアップウィザードの使用: 考慮事項と要件

S3 セットアップ ウィザードを使用して、 StorageGRID をS3 アプリケーションのオブジェクト ストレージ システムとして設定できます。

S3 セットアップウィザードを使用する場合

S3 セットアップ ウィザードは、S3 アプリケーションで使用するためにStorageGRIDを構成する各手順をガイドします。ウィザードを完了する過程で、S3 アプリケーションに値を入力するために使用できるファイルをダウンロードします。ウィザードを使用すると、システムをより迅速に構成し、設定がStorageGRID のベスト プラクティスに準拠していることを確認できます。

もしあなたが"ルートアクセス権限"StorageGRID Grid Manager の使用を開始するときに S3 セットアップ ウィザードを完了することも、後でいつでもウィザードにアクセスして完了することもできます。要件に応じて、必要な項目の一部またはすべてを手動で設定し、ウィザードを使用して S3 アプリケーションに必要な値を組み立てることもできます。

ウィザードを使用する前に

ウィザードを使用する前に、これらの前提条件が満たされていることを確認してください。

IPアドレスを取得し、**VLAN**インターフェースを設定する

高可用性 (HA) グループを構成する場合は、S3 アプリケーションが接続するノードと、使用されるStorageGRIDネットワークがわかります。また、サブネット CIDR、ゲートウェイ IP アドレス、仮想 IP (VIP) アドレスに入力する値もわかっています。

仮想 LAN を使用して S3 アプリケーションからのトラフィックを分離する予定の場合は、VLAN インターフェイスはすでに構成されています。見る"VLANインターフェースを構成する" 。

ID連携と**SSO**を構成する

StorageGRIDシステムで ID フェデレーションまたはシングル サインオン (SSO) を使用する予定の場合は、これらの機能が有効になっています。また、S3 アプリケーションが使用するテナント アカウントのルート アクセス権を持つフェデレーション グループも把握しています。見る"アイデンティティフェデレ

ーションを使用する"そして"シングルサインオンを構成する"。

ドメイン名の取得と設定

StorageGRIDに使用する完全修飾ドメイン名 (FQDN) がわかっていること。ドメイン ネーム サーバー (DNS) エントリは、この FQDN を、ウィザードを使用して作成する HA グループの仮想 IP (VIP) アドレスにマッピングします。

S3仮想ホスト形式のリクエストを使用する予定の場合は、"設定されたS3エンドポイントドメイン名" 。仮想ホスト形式のリクエストを使用することをお勧めします。

ロードバランサとセキュリティ証明書の要件を確認する

StorageGRIDロード バランサを使用する予定の場合は、ロード バランシングに関する一般的な考慮事項を確認しておきます。アップロードする証明書、または証明書を生成するために必要な値があります。

外部 (サードパーティ) ロード バランサー エンドポイントを使用する予定の場合は、そのロード バランサーの完全修飾ドメイン名 (FQDN)、ポート、および証明書が必要です。

グリッドフェデレーション接続を構成する

S3 テナントがグリッド フェデレーション接続を使用してアカウント データを複製し、バケット オブジェクトを別のグリッドに複製できるようにする場合は、ウィザードを開始する前に次の点を確認してください。

- あなたが持っている"グリッドフェデレーション接続を構成しました"。
- 接続のステータスは*接続済み*です。
- ルートアクセス権限があります。

S3 セットアップウィザードにアクセスして完了する

S3 セットアップ ウィザードを使用して、 StorageGRID をS3 アプリケーションで使用するように構成できます。セットアップ ウィザードは、アプリケーション がStorageGRIDバケットにアクセスしてオブジェクトを保存するために必要な値を提供します。

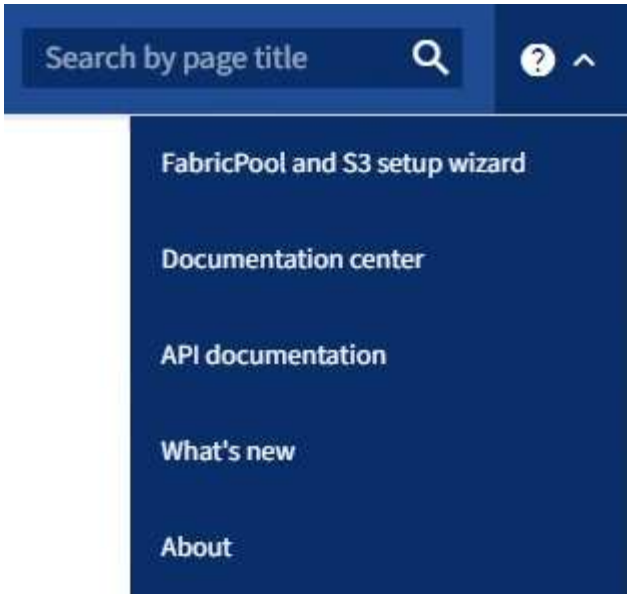
開始する前に

- あなたは"ルートアクセス権限"。
- あなたは、"考慮事項と要件"ウィザードを使用するためのものです。

ウィザードにアクセスする

手順

1. グリッドマネージャーにSign inには、"サポートされているウェブブラウザ" 。
2. ダッシュボードに * FabricPoolおよび S3 セットアップ ウィザード* バナーが表示された場合は、バナー内のリンクを選択します。バナーが表示されなくなった場合は、グリッド マネージャーのヘッダー バーからヘルプ アイコンを選択し、* FabricPoolおよび S3 セットアップ ウィザード* を選択します。



3. FabricPoolおよび S3 セットアップ ウィザード ページの S3 アプリケーション セクションで、[今すぐ構成] を選択します。

ステップ **1/6: HA** グループを構成する

HA グループは、それぞれにStorageGRID Load Balancer サービスが含まれるノードの集合です。 HA グループには、ゲートウェイ ノード、管理ノード、またはその両方を含めることができます。

HA グループを使用すると、S3 データ接続を利用可能な状態に保つことができます。 HA グループ内のアクティブ インターフェイスに障害が発生した場合、バックアップ インターフェイスが S3 操作にほとんど影響を与えずにワークロードを管理できます。

このタスクの詳細については、"高可用性グループの管理" 。

手順

1. 外部ロードバランサーを使用する予定の場合は、HA グループを作成する必要はありません。 *この手順をスキップ*を選択して、ステップ 2/6: ロードバランサーのエンドポイントを構成する 。
2. StorageGRIDロード バランサを使用するには、新しい HA グループを作成するか、既存の HA グループを使用することができます。

HAグループを作成する

a. 新しい HA グループを作成するには、*HA グループの作成*を選択します。

b. *詳細を入力*手順では、次のフィールドに入力します。

フィールド	説明
HAグループ名	この HA グループの一意の表示名。
説明（オプション）	この HA グループの説明。

c. *インターフェースの追加*手順では、この HA グループで使用するノード インターフェースを選択します。

列ヘッダーを使用して行を並べ替えるか、検索語を入力してインターフェイスをより速く見つけます。

1 つ以上のノードを選択できますが、各ノードに対して選択できるインターフェースは 1 つだけです。

d. *インターフェースの優先順位付け*手順では、この HA グループのプライマリ インターフェースとバックアップ インターフェースを決定します。

行をドラッグして、「優先順位」列の値を変更します。

リストの最初のインターフェースはプライマリ インターフェースです。障害が発生しない限り、プライマリ インターフェイスはアクティブ インターフェイスになります。

HA グループに複数のインターフェイスが含まれており、アクティブ インターフェイスに障害が発生した場合、仮想 IP (VIP) アドレスは優先順位の最初のバックアップ インターフェイスに移動します。そのインターフェースに障害が発生した場合、VIP アドレスは次のバックアップ インターフェースに移動し、これが繰り返されます。障害が解決されると、VIP アドレスは利用可能な最も優先度の高いインターフェースに戻ります。

e. **IP** アドレスを入力 の手順では、次のフィールドに入力します。

フィールド	説明
サブネットCIDR	CIDR 表記の VIP サブネットのアドレス (IPv4 アドレスの後にスラッシュとサブネットの長さ (0 ～ 32) が続きます)。 ネットワーク アドレスにはホスト ビットを設定しないでください。例： `192.16.0.0/22` 。
ゲートウェイIPアドレス（オプション）	StorageGRID へのアクセスに使用される S3 IP アドレスがStorageGRID VIP アドレスと同じサブネット上にない場合は、 StorageGRID VIP ローカル ゲートウェイ IP アドレスを入力します。ローカル ゲートウェイ IP アドレスは VIP サブネット内にある必要があります。

フィールド	説明
仮想IPアドレス	HA グループ内のアクティブ インターフェイスに、少なくとも 1 個、最大 10 個の VIP アドレスを入力します。すべての VIP アドレスは VIP サブネット内にある必要があります。 少なくとも 1 つのアドレスは IPv4 である必要があります。必要に応じて、追加の IPv4 および IPv6 アドレスを指定できます。

f. **HA** グループの作成 を選択し、完了 を選択して S3 セットアップ ウィザードに戻ります。

g. *続行*を選択して、ロードバランサーのステップに進みます。

既存の**HA**グループを使用する

a. 既存の HA グループを使用するには、「**HA** グループの選択」から HA グループ名を選択します。

b. *続行*を選択して、ロードバランサーのステップに進みます。

ステップ **2/6:** ロードバランサーのエンドポイントを構成する

StorageGRID はロード バランサを使用してクライアント アプリケーションからのワークロードを管理します。負荷分散により、複数のストレージ ノード間の速度と接続容量が最大化されます。

すべてのゲートウェイおよび管理ノードに存在するStorageGRIDロード バランサ サービスを使用することも、外部 (サードパーティ) ロード バランサに接続することもできます。 StorageGRIDロード バランサの使用をお勧めします。

このタスクの詳細については、"負荷分散に関する考慮事項" 。

StorageGRIDロード バランサ サービスを使用するには、* StorageGRIDロード バランサ* タブを選択し、使用するロード バランサ エンドポイントを作成または選択します。外部ロード バランサを使用するには、[外部ロード バランサ] タブを選択し、すでに構成したシステムの詳細を入力します。

エンドポイントを作成する

手順

1. ロード バランサー エンドポイントを作成するには、[エンドポイントの作成] を選択します。
2. エンドポイントの詳細を入力 ステップで、次のフィールドに入力します。

フィールド	説明
Name	エンドポイントの説明的な名前。
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、未使用の外部ポートを入力できます。 80 または 443 を入力すると、これらのポート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 ノードでのみ構成されます。 注意: 他のグリッド サービスで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"。
クライアントタイプ	**S3** である必要があります。
ネットワークプロトコル	「HTTPS」を選択します。 注: TLS 暗号化なしでのStorageGRIDとの通信はサポートされていますが、推奨されません。

3. バインディング モードの選択 ステップで、バインディング モードを指定します。バインディング モードは、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。

モード	説明
グローバル（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 (デフォルト) 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。

モード	説明
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	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。

4. 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。
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。

5. *証明書の添付*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
証明書をアップロードする（推奨）	このオプションを使用して、CA 署名付きサーバー証明書、証明書の秘密キー、およびオプションの CA バンドルをアップロードします。
証明書を生成する	このオプションを使用して、自己署名証明書を生成します。見る"ロードバランサのエンドポイントを構成する"入力内容の詳細については、こちらをご覧ください。
StorageGRID S3証明書を使用する	このオプションは、 StorageGRIDグローバル証明書のカスタム バージョンをすでにアップロードまたは生成している場合にのみ使用してください。見る"S3 API証明書を設定する"詳細については。

6. *完了*を選択して、S3 セットアップ ウィザードに戻ります。
7. *続行*を選択して、テナントとバケットのステップに進みます。

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。

既存のロードバランサエンドポイントを使用する

手順

1. 既存のエンドポイントを使用するには、「ロードバランサー エンドポイントの選択」からその名前を選択します。
2. *続行*を選択して、テナントとバケットのステップに進みます。

外部ロードバランサを使用する

手順

1. 外部ロードバランサーを使用するには、次のフィールドに入力します。

フィールド	説明
FQDN	外部ロード バランサーの完全修飾ドメイン名 (FQDN)。
ポート	S3 アプリケーションが外部ロードバランサーに接続するために使用するポート番号。
Certificate	外部ロードバランサーのサーバー証明書をコピーして、このフィールドに貼り付けます。

2. *続行*を選択して、テナントとバケットのステップに進みます。

ステップ**3/6:** テナントとバケットを作成する

テナントは、S3 アプリケーションを使用してStorageGRIDにオブジェクトを保存および取得できるエンティティです。各テナントには、独自のユーザー、アクセス キー、バケット、オブジェクト、および特定の機能セットがあります。

バケットは、テナントのオブジェクトとオブジェクト メタデータを保存するために使用されるコンテナです。テナントには多くのバケットが存在する可能性がありますが、ウィザードを使用すると、テナントとバケットを最も迅速かつ簡単に作成できます。後でバケットを追加したりオプションを設定したりする必要がある場合は、テナント マネージャーを使用できます。

このタスクの詳細については、"テナントアカウントを作成する"そして"S3バケットを作成する"。

手順

1. テナント アカウントの名前を入力します。

   テナント名は一意である必要はありません。テナント アカウントが作成されると、一意の数値アカウント ID が割り当てられます。

2. StorageGRIDシステムが使用するかどうかに基づいて、テナントアカウントのルートアクセスを定義します。"アイデンティティフェデレーション" 、"シングルサインオン（SSO）" 、またはその両方。

オプション	これをする
アイデンティティ連携が有効になっていない場合	ローカル ルート ユーザーとしてテナントにサインインするときに使用するパスワードを指定します。
アイデンティティ連携が有効になっている場合	a. 既存のフェデレーショングループを選択して"ルートアクセス権限"テナントのために。 b. 必要に応じて、ローカル ルート ユーザーとしてテナントにサインインするときに使用するパスワードを指定します。
ID連携とシングルサインオン（SSO）の両方が有効になっている場合	既存のフェデレーショングループを選択して"ルートアクセス権限"テナントのために。ローカル ユーザーはサインインできません。

3. ウィザードでルート ユーザーのアクセス キー ID とシークレット アクセス キーを作成する場合は、[ルート ユーザーの S3 アクセス キーを自動的に作成する] を選択します。

   テナントの唯一のユーザーがルート ユーザーである場合は、このオプションを選択します。他のユーザーがこのテナントを使用する場合、"テナントマネージャーを使用する"キーと権限を設定します。

4. 今すぐこのテナントのバケットを作成する場合は、「このテナントのバケットを作成」を選択します。

   > グリッドに対して S3 オブジェクト ロックが有効になっている場合、この手順で作成されたバケットでは S3 オブジェクト ロックは有効になりません。この S3 アプリケーションに S3 オブジェクトロック バケットを使用する必要がある場合は、今すぐバケットの作成を選択しないでください。代わりに、テナントマネージャーを使用して"バケットを作成する"後で。

   a. S3 アプリケーションが使用するバケットの名前を入力します。例： `s3-bucket` 。

      バケットを作成した後は、バケット名を変更することはできません。

   b. このバケットの*リージョン*を選択します。

      デフォルトの地域を使用する(`us-east-1`) 将来的に ILM を使用してバケットのリージョンに基づいてオブジェクトをフィルタリングする予定がない限り、このポリシーは適用されません。

5. *作成して続行*を選択します。

ステップ**4/6:** データのダウンロード

データのダウンロード手順では、1 つまたは 2 つのファイルをダウンロードして、構成した内容の詳細を保存できます。

手順

1. ルートユーザーの **S3** アクセス キーを自動的に作成する を選択した場合は、次のいずれかまたは両方を実行します。
   - *アクセスキーをダウンロード*を選択してダウンロードします `.csv`テナント アカウント名、アクセス キー ID、シークレット アクセス キーを含むファイル。

◦ コピーアイコン（) をクリックして、アクセス キー ID とシークレット アクセス キーをクリップボードにコピーします。

2. *設定値をダウンロード*を選択してダウンロードします `.txt`ロードバランサのエンドポイント、テナント、バケット、およびルートユーザーの設定を含むファイル。
3. この情報を安全な場所に保存してください。

> 両方のアクセス キーをコピーするまでこのページを閉じないでください。このページを閉じると、キーは使用できなくなります。この情報はStorageGRIDシステムからデータを取得するために使用される可能性があるため、必ず安全な場所に保存してください。

4. プロンプトが表示されたら、チェックボックスを選択して、キーをダウンロードまたはコピーしたことを確認します。
5. *続行*を選択して、ILM ルールとポリシーのステップに進みます。

ステップ **5/6: S3** の **ILM** ルールと **ILM** ポリシーを確認する

情報ライフサイクル管理 (ILM) ルールは、 StorageGRIDシステム内のすべてのオブジェクトの配置、期間、および取り込み動作を制御します。 StorageGRIDに含まれる ILM ポリシーは、すべてのオブジェクトの複製コピーを 2 つ作成します。このポリシーは、少なくとも 1 つの新しいポリシーをアクティブ化するまで有効です。

手順

1. ページに記載されている情報を確認します。
2. 新しいテナントまたはバケットに属するオブジェクトに特定の指示を追加する場合は、新しいルールと新しいポリシーを作成します。見る"ILMルールを作成する"そして"ILMポリシーを使用する"。
3. *これらの手順を確認し、実行する必要があることを理解しました*を選択します。
4. 次に何をすべきかを理解していることを示すために、チェックボックスを選択します。
5. *続行*を選択して*概要*に進みます。

ステップ**6/6:** レビューの概要

手順

1. 概要を確認します。
2. 次の手順では、S3 クライアントに接続する前に必要になる可能性のある追加の構成について説明しているので、詳細をメモしておいてください。たとえば、「* root としてSign in*」を選択すると、テナント マネージャに移動し、テナント ユーザーを追加したり、追加のバケットを作成したり、バケット設定を更新したりできます。
3. *完了*を選択します。
4. StorageGRIDからダウンロードしたファイルまたは手動で取得した値を使用してアプリケーションを構成します。

HAグループの管理

高可用性 (HA) グループとは何ですか?

高可用性 (HA) グループは、S3 クライアントに高可用性のデータ接続を提供し、グリッド マネージャーおよびテナント マネージャーに高可用性の接続を提供します。

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高可用性 (HA) グループにグループ化できます。 HA グループ内のアクティブ インターフェイスに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。

各 HA グループは、選択したノード上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 クライアントに高可用性のデータ接続を提供します。
- 管理ノードのみを含む HA グループは、グリッド マネージャとテナント マネージャへの高可用性接続を提供します。
- 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を含むHAグループは、高可用性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 グループが推奨されますが、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。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、またはノードに追加したアクセス 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 アドレスがある場合、HA グループにインターフェイスを追加することはできません。

2. 1 つのインターフェースをプライマリ インターフェースとして指定します。障害が発生しない限り、プライマリ インターフェイスはアクティブ インターフェイスになります。
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 1 ～ 10 個の仮想 IP (VIP) アドレスを割り当てます。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、"高可用性グループを構成する" 。

アクティブインターフェースとは何ですか?

通常の動作中、HA グループのすべての VIP アドレスは、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である限り、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そのインターフェイスが使用されます。つまり、通常の操作中は、プライマリ インターフェイスがグループの「アクティブ」インターフェイスになります。

同様に、通常の操作中は、HA グループの優先度の低いインターフェースは「バックアップ」インターフェー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った場合を除き、使用されません。

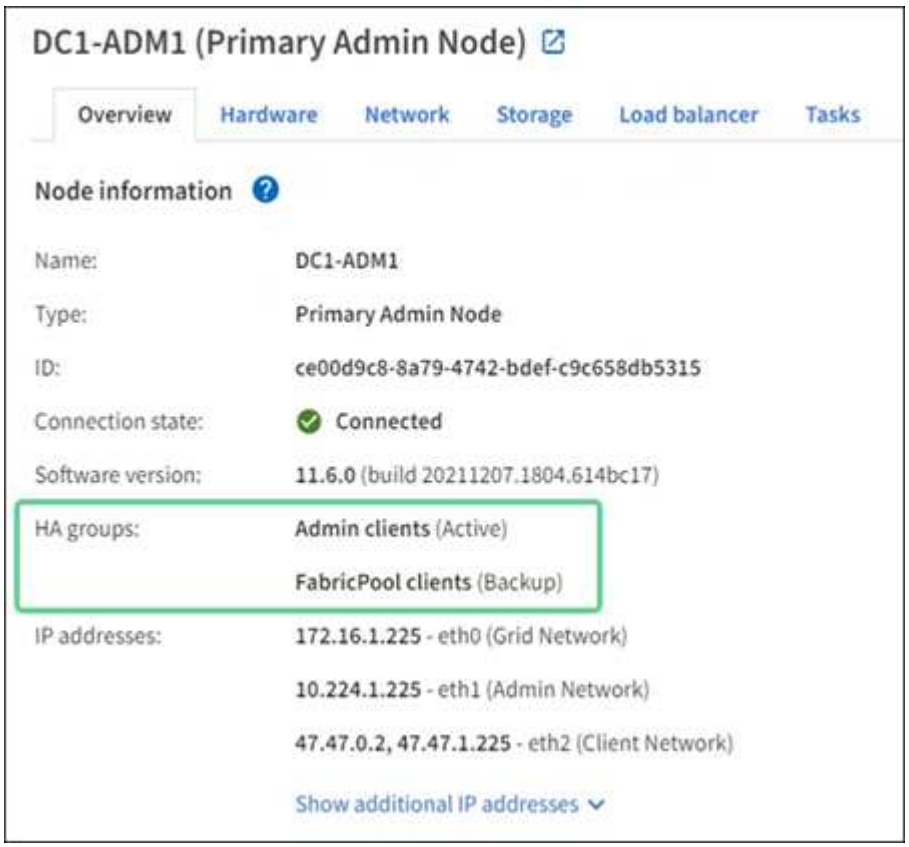
ノードの現在のHAグループのステータスを表示する

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*** 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、ノードはリストされている HA グループに割り当てられます。グループ名の後の値は、HA グループ内のノードの現在のステータスです。

- アクティブ: 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。これはバックアップ インターフェイスです。
- 停止: 高可用性 (keepalived) サービスが手動で停止されているため、このノードで HA グループをホストできません。
- 障害: 次の 1 つ以上の理由により、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) サービスがノード上で実行されていません。
  - ノードの eth0 または VIP インターフェースがダウンしています。
  - 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、管理クライアント グループのアクティブ インターフェイスであり、 FabricPool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**?**

現在 VIP アドレスをホストしているインターフェースがアクティブ インターフェースです。 HA グループに

複数のインターフェイスが含まれており、アクティブ インターフェイスに障害が発生した場合、VIP アドレスは優先順位に従って最初に使用可能なバックアップ インターフェイスに移動します。そのインターフェースに障害が発生した場合、VIP アドレスは次の利用可能なバックアップ インターフェースに移動し、これが繰り返されます。

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。

- インターフェースが設定されているノードがダウンします。
- インターフェイスが設定されているノードは、少なくとも 2 分間、他のすべてのノードとの接続を失います。
- アクティブ インターフェースがダウンします。
- ロード バランサー サービスが停止します。
- 高可用性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外部のネットワーク障害によってフェイルオーバーがトリガーされない場合があります。同様に、フェイルオーバーは、Grid Manager または Tenant Manager のサービスによってトリガーされません。

フェイルオーバー プロセスは通常、数秒しかかからず、クライアント アプリケーションへの影響がほとんどなく、通常の再試行動作によって操作を続行できるほど高速です。

障害が解決され、より優先度の高いインターフェイスが再び使用可能になると、VIP アドレスは使用可能な最も優先度の高いインターフェイスに自動的に移動されます。

HA グループはどのように使用されますか?

高可用性 (HA) グループを使用すると、オブジェクト データおよび管理用途のためにStorageGRIDへの高可用性接続を提供できます。

- HA グループは、グリッド マネージャまたはテナント マネージャへの高可用性の管理接続を提供できます。
- HA グループは、S3 クライアントに高可用性のデータ接続を提供できます。
- インターフェースが 1 つだけ含まれる HA グループでは、多数の VIP アドレスを提供したり、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ノードの種類からインターフェイスを追加します。

- 管理ノード: ロード バランサ サービスを含め、グリッド マネージャまたはテナント 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 サービスを含めます。

HAグループの目的	このタイプのノードをHAグループに追加する
グリッドマネージャーへのアクセス	• 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はプライマリ 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からのみ実行できます。
テナントマネージャーのみへのアクセス	• プライマリまたは非プライマリ管理ノード
S3 クライアントアクセス - ロードバランサーサービス	• 管理ノード • ゲートウェイノード
S3クライアントアクセス"S3セレクト"	• サービスアプライアンス • VMwareベースのソフトウェアノード 注意: S3 Select を使用する場合は HA グループが推奨されますが、必須ではありません。

グリッド マネージャーまたはテナント マネージャーで **HA** グループを使用する際の制限

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

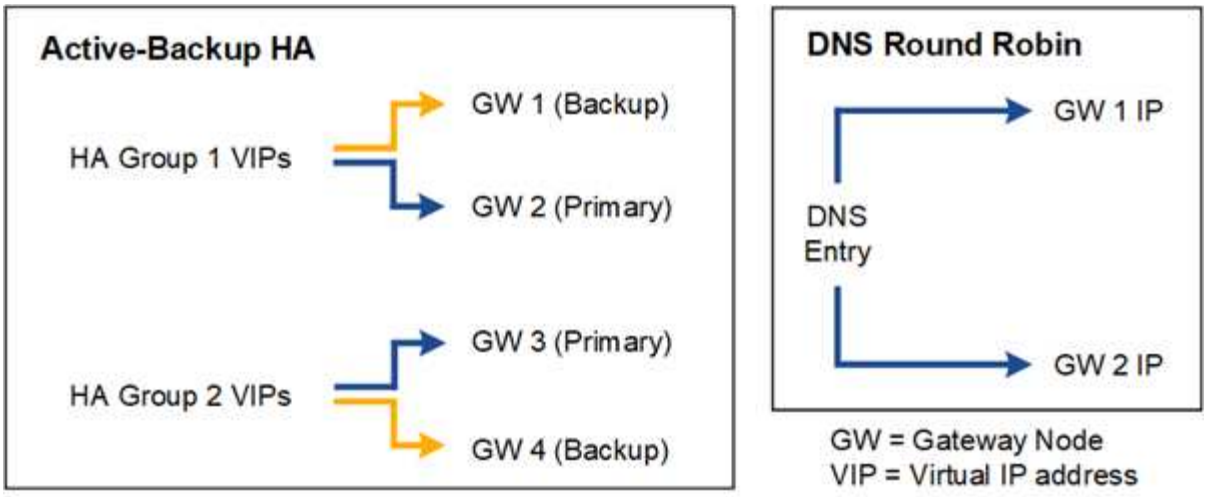
フェイルオーバーが発生したときに Grid Manager または Tenant Manager にサインインしている場合は、サインアウトされるため、タスクを再開するには再度サインインする必要があります。

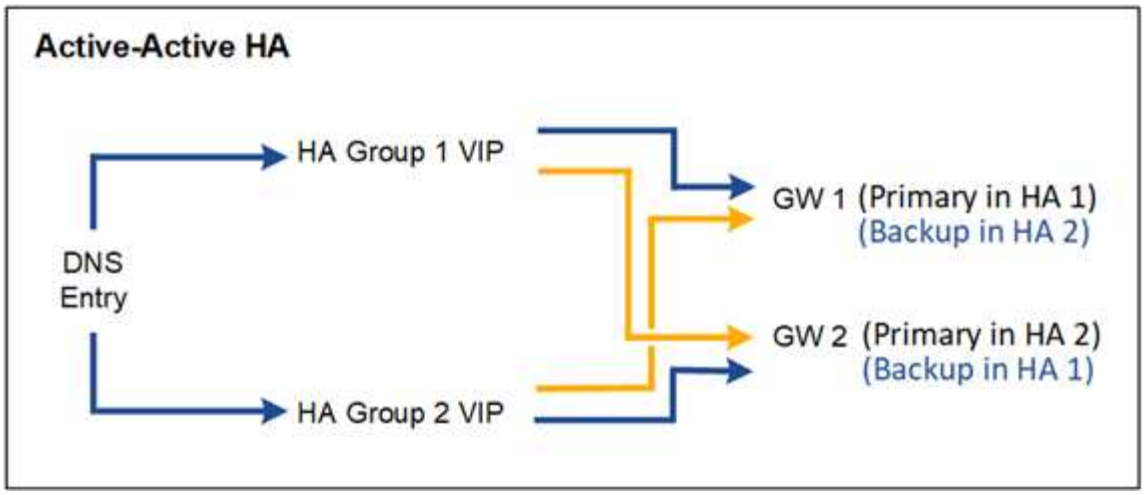
プライマリ管理ノードが利用できない場合、一部のメンテナンス手順は実行できません。フェイルオーバー中は、Grid Manager を使用してStorageGRIDシステムを監視できます。

HAグループの構成オプション

次の図は、HA グループを構成するさまざまな方法の例を示しています。それぞれの選択肢には長所と短所があります。

図では、青は HA グループ内のプライマリ インターフェイスを示し、黄色は HA グループ内のバックアップ インターフェイスを示します。





この表は、図に示されている各 HA 構成の利点をまとめたものです。

構成	利点	デメリット
アクティブバックアップ HA	• 外部依存なしでStorageGRIDによって管理されます。 • 高速フェイルオーバー。	• HA グループ内の 1 つのノードのみがアクティブになります。 HA グループごとに少なくとも 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	• 総スループットの向上。 • アイドル状態のホストはありません。	• フェイルオーバーが遅く、クライアントの動作に依存する可能性があります。 • StorageGRID外部のハードウェアの構成が必要です。 • 顧客が実装するヘルスチェックが必要です。

構成	利点	デメリット
アクティブ-アクティブ HA	• トラフィックは複数の HA グループに分散されます。 • HA グループの数に応じて拡張される高い集約スループット。 • 高速フェイルオーバー。	• 設定がより複雑になります。 • StorageGRID外部のハードウェアの構成が必要です。 • 顧客が実装するヘルスチェックが必要です。

高可用性グループを構成する

高可用性 (HA) グループを構成して、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高可用性アクセスを提供できます。

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"。
- HA グループで VLAN インターフェイスを使用する予定の場合は、VLAN インターフェイスを作成しておきます。見る"VLANインターフェースを構成する" 。
- HA グループ内のノードにアクセス インターフェイスを使用する予定の場合は、インターフェイスを作成しておく必要があります。
  - **Red Hat Enterprise Linux** (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する"
  - **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する"
  - **Linux** (ノードのインストール後):"Linux: ノードにトランクまたはアクセスインターフェースを追加する"
  - **VMware** (ノードのインストール後):"VMware: ノードにトランクまたはアクセス インターフェースを追加する"

高可用性グループを作成する

高可用性グループを作成するときは、1 つ以上のインターフェースを選択し、優先順位に従って整理します。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 グループに含めるには、ゲートウェイ ノードまたは管理ノード用のインターフェイスが必要です。 HA グループは、特定のノードに対して 1 つのインターフェイスのみを使用できます。ただし、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する

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。
2. *作成*を選択します。

HAグループの詳細を入力します

手順

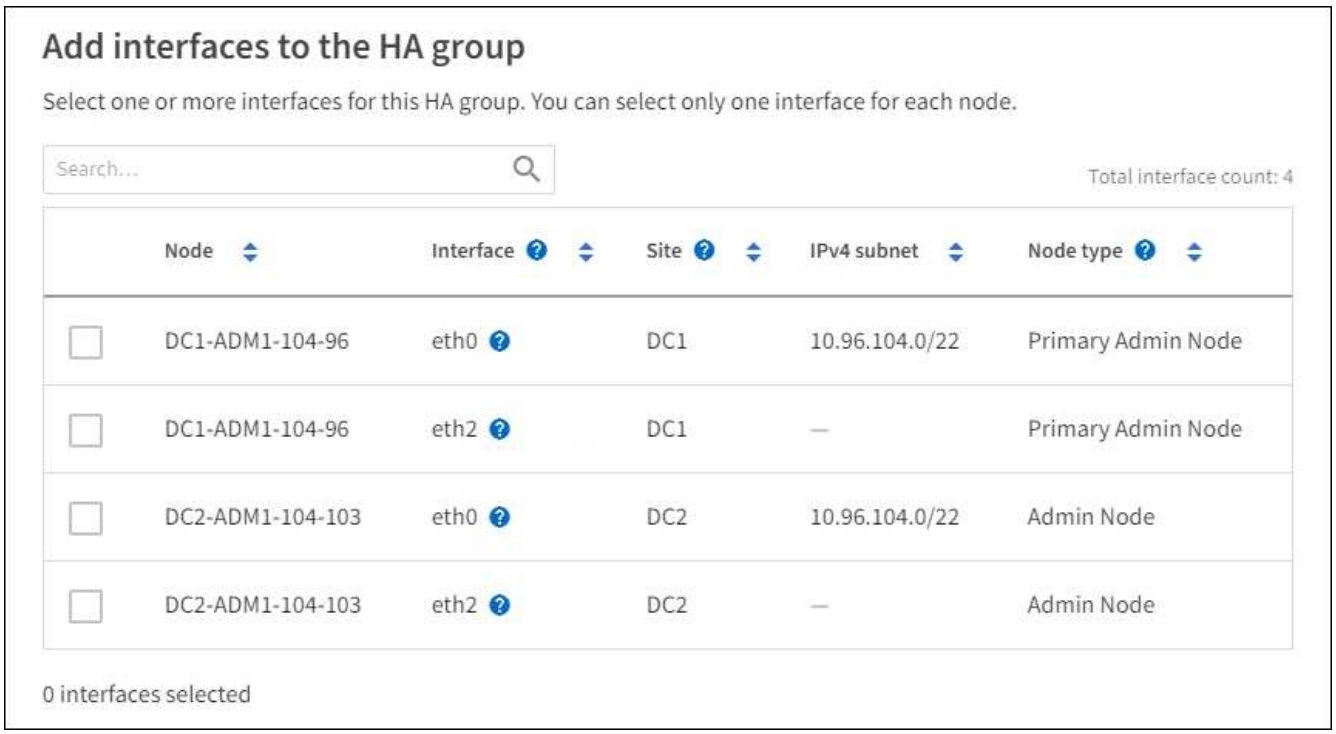
1. HA グループに一意の名前を付けます。
2. 必要に応じて、HA グループの説明を入力します。
3. *続行*を選択します。

HAグループにインターフェースを追加する

手順

1. この HA グループに追加する 1 つ以上のインターフェースを選択します。

   列ヘッダーを使用して行を並べ替えるか、検索語を入力してインターフェイスをより速く見つけます。

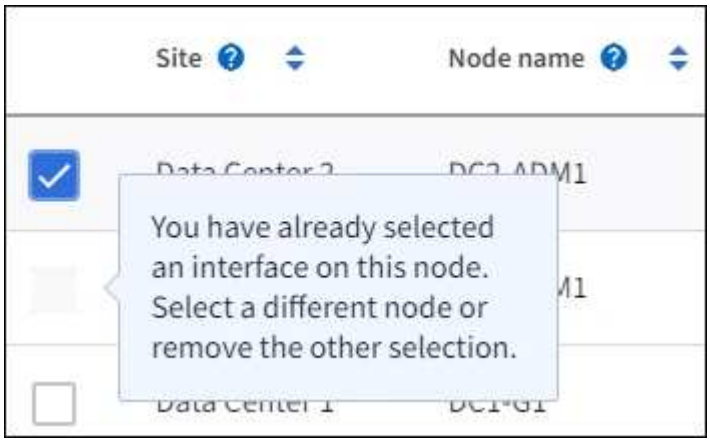


   VLAN インターフェイスを作成した後、新しいインターフェイスがテーブルに表示されるまで最大 5 分間待ちます。

インターフェース選択のガイドライン

- 少なくとも 1 つのインターフェースを選択する必要があります。
- ノードに対して選択できるインターフェースは 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 クライアント トラフィックの HA 保護用である場合は、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。
- 異なるタイプのノード上のインターフェースを選択すると、情報メモが表示されます。フェイルオーバーが発生した場合、以前アクティブだったノードによって提供されていたサービスは、新しくアクティブになったノードでは利用できなくなる可能性があることに注意してください。たとえば、バックアップ ゲートウェイ ノードは、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。

- インターフェースを選択できない場合は、そのチェックボックスは無効になります。ツールヒントにはさらに詳しい情報が表示されます。



- 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ースと競合する場合は、そのインターフェースを選択できません。
- 静的 IP アドレスがない場合、構成されたインターフェースを選択することはできません。

2. *続行*を選択します。

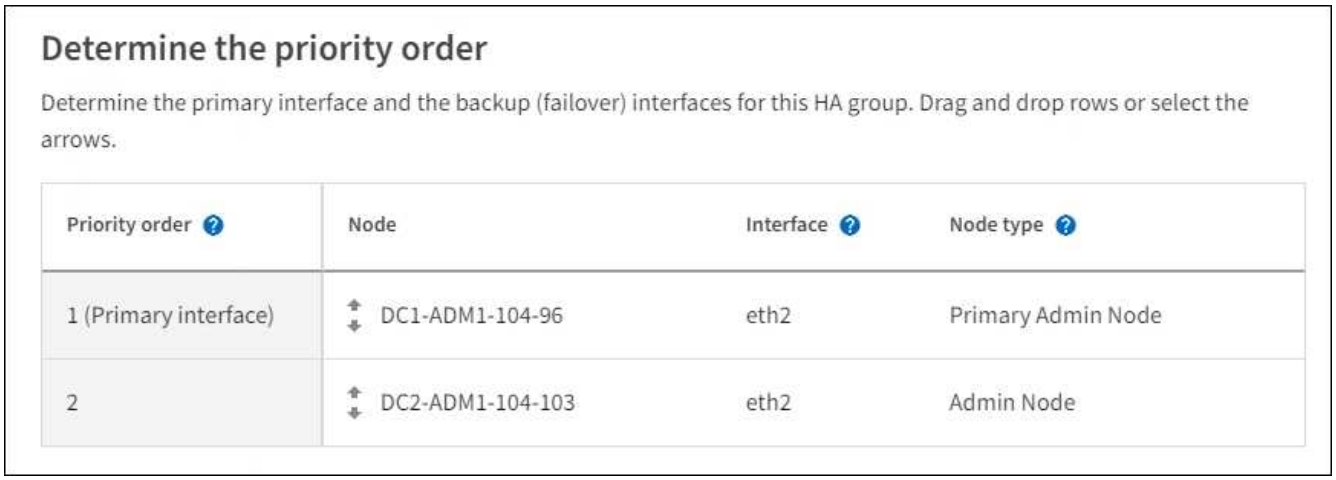
優先順位を決定する

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は、どのインターフェイスがプライマリ インターフェイスで、どのインターフェイスがバックアップ (フェイルオーバー) インターフェイスであるかを決定できます。プライマリ インターフェイスに障害が発生した場合、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。そのインターフェースに障害が発生した場合、VIP アドレスは利用可能な次の最も優先度の高いインターフェースに移動し、これを繰り返します。

手順

1. *優先順位*列の行をドラッグして、プライマリ インターフェイスとバックアップ インターフェイスを決定します。

   リストの最初のインターフェースはプライマリ インターフェースです。障害が発生しない限り、プライマリ インターフェイスはアクティブ インターフェイスになります。



HA グループがグリッド マネージャ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プライマリ インターフェイス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からのみ実行できます。

2. *続行*を選択します。

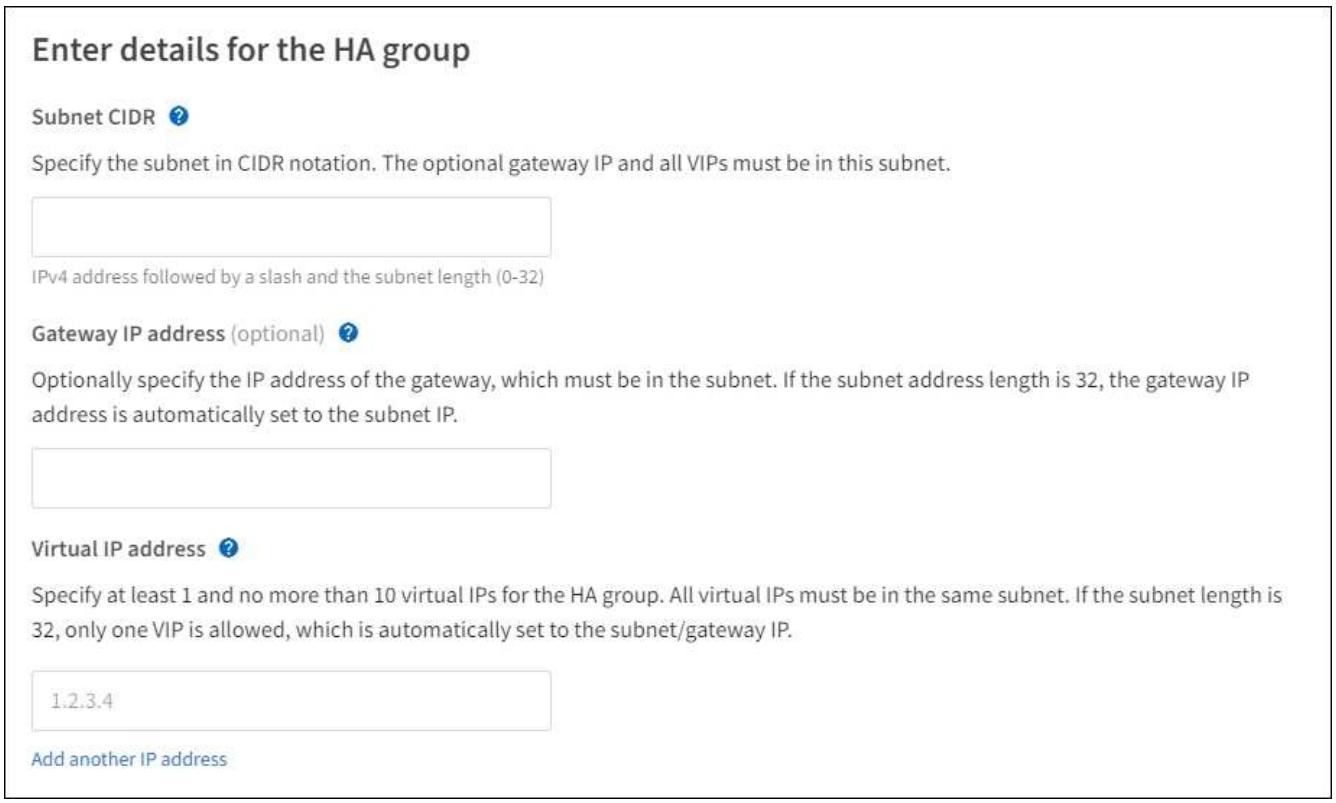
IPアドレスを入力してください

手順

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

   ネットワーク アドレスにはホスト ビットを設定しないでください。例： `192.16.0.0/22` 。

   32 ビットの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. オプションとして、S3 管理クライアントまたはテナント 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 サブネット内にある必要があります。

   クライアントおよび管理者ユーザーは、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 グループ内のアクティブ インターフェイスに、少なくとも 1 個、最大 10 個の VIP アドレスを入力します。すべての VIP アドレスは VIP サブネット内にある必要があり、アクティブ インターフェイス上ですべてが同時にアクティブになります。

少なくとも 1 つの IPv4 アドレスを指定する必要があります。必要に応じて、追加の IPv4 および 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、構成された仮想 IP アドレスを使用できるようになります。

次の手順

この HA グループを負荷分散に使用する場合は、ロード バランサー 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、必要な証明書を添付します。見る"ロードバランサのエンドポイントを構成する" 。

高可用性グループを編集する

高可用性 (HA) グループを編集して、名前や説明を変更したり、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廃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は、HA グループを編集する必要がある場合があります。

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。

   高可用性グループ ページには、既存の HA グループがすべて表示されます。

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. 更新する内容に応じて、次のいずれかを実行します。
   - VIP アドレスを追加または削除するには、[アクション] > [仮想 IP アドレスの編集] を選択します。
   - グループの名前または説明を更新したり、インターフェー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するには、[アクション] > [HA グループの編集] を選択します。
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*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説明を更新します。
   b. 必要に応じて、チェックボックスを選択または選択解除して、インターフェースを追加または削除します。

      HA グループがグリッド マネージャ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プライマリ インターフェイス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からのみ実行できます

   c. 必要に応じて、行をドラッグして、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*を選択し、*完了*を選択します。

高可用性グループを削除する

一度に 1 つ以上の高可用性 (HA) グループを削除できます。

HA グループがロードバランサーエンドポイントにバインドされている場合、その HA グループを削除することはできません。 HA グループを削除するには、そのグループを使用しているすべてのロードバランサーエンドポイントからそのグループを削除する必要があります。

クライアントの中断を防ぐには、HA グループを削除する前に、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 IP アドレス (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構成された IP アドレスなど) 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。

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。
2. 削除する各 HA グループの ロード バランサ エンドポイント 列を確認します。ロード バランサのエンドポイントがリストされている場合:
   a. 構成 > ネットワーク > ロードバランサーエンドポイント に移動します。
   b. エンドポイントのチェックボックスを選択します。
   c. 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。
   d. バインディング モードを更新して HA グループを削除します。
   e. *変更を保存*を選択します。
3. ロード バランサ エンドポイントがリストされていない場合は、削除する各 HA グループのチェックボックスをオンにします。
4. アクション > **HA** グループの削除 を選択します。
5. メッセージを確認し、「**HA** グループの削除」を選択して選択を確定します。

   選択したすべての HA グループが削除されます。高可用性グループ ページに緑色の成功バナーが表示されます。

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。

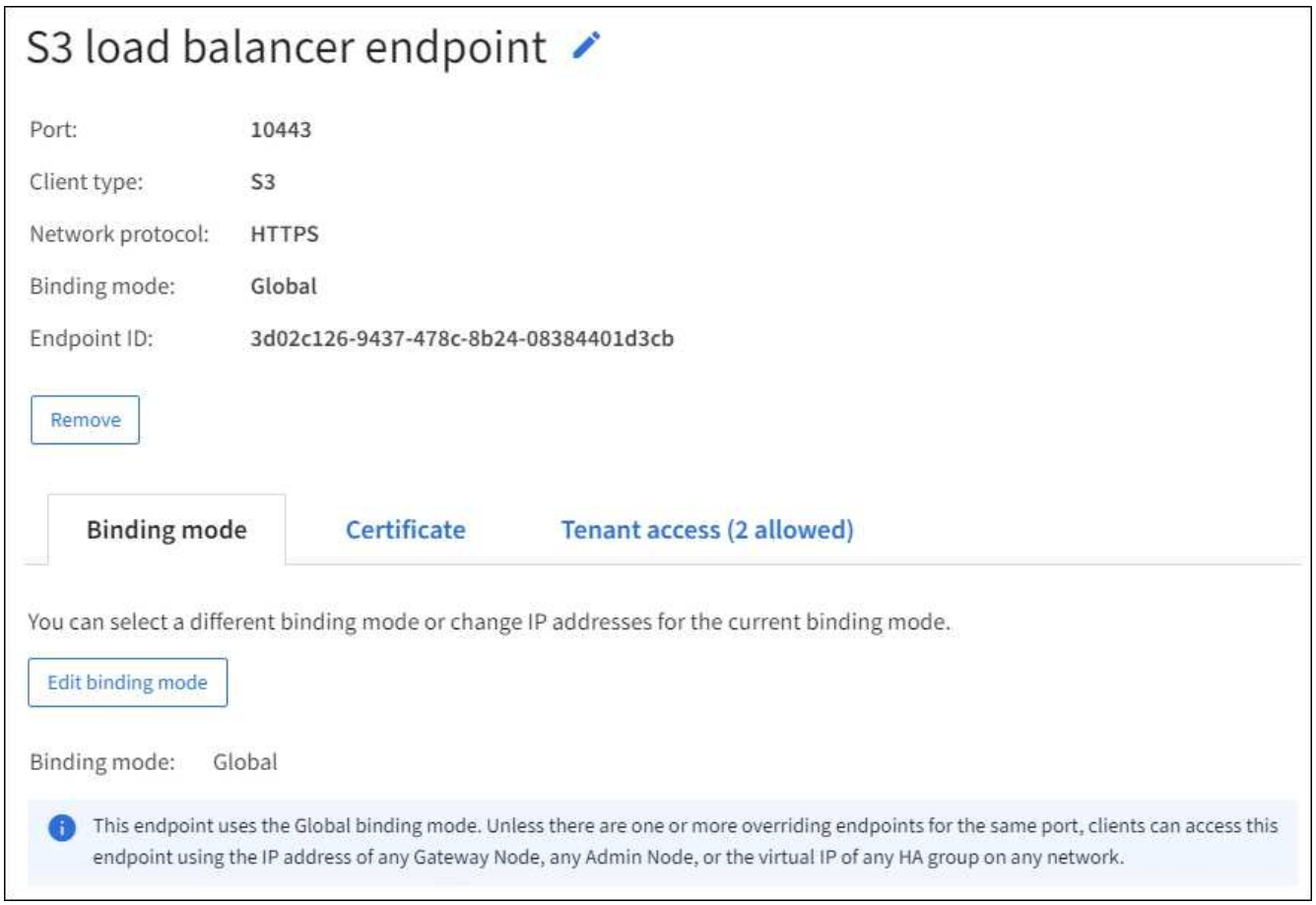
2. エンドポイントに接続するために必要な情報を S3 クライアントに提供します。

- 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。

S3エンドポイントのドメイン名を設定する

S3 仮想ホスト スタイルのリクエストをサポートするには、グリッド マネージャーを使用して、S3 クライアントが接続する S3 エンドポイント ドメイン名のリストを設定する必要があります。

エンドポイント ドメイン名に IP アドレスを使用することはサポートされていません。将来のリリースではこの構成は禁止されます。

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" 。
- あなたが持っている"特定のアクセス権限"。
- グリッドのアップグレードが進行中ではないことを確認しました。

グリッドのアップグレードが進行中の場合は、ドメイン名の構成を変更しないでください。

タスク概要

クライアントが S3 エンドポイント ドメイン名を使用できるようにするには、次のすべてを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 ドメイン名をStorageGRIDシステムに追加します。
- 確実に"クライアントがStorageGRIDへのHTTPS接続に使用する証明書"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ます。

  たとえば、エンドポイントが `s3.company.com`、HTTPS接続に使用する証明書に次の内容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 サブジェクト別名 (SAN)： `*.s3.company.com` 。

- クライアントが使用する DNS サーバーを構成します。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、レコードがワイルドカード名を含むすべての必要な S3 エンドポイント ドメイン名を参照していることを確認します。

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、高可用性グループの仮想 IP アドレスに接続することで、 StorageGRID に接続できます。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、DNS レコードに正しい IP アドレスを含める必要があります。

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

- ロード バランサー 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のカスタム証明書を使用できます。各ロードバランサーエンドポイントは、異なる S3 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。
- ロードバランサーエンドポイントに接続するクライアント、またはストレージノードに直接接続するクライアントは、必要なすべての S3 エンドポイントドメイン名を含めるようにグローバル S3 API 証明書をカスタマイズできます。

S3 エンドポイント ドメイン名を追加せず、リストが空の場合、S3 仮想ホスト スタイルのリクエストのサポートは無効になります。

S3エンドポイントドメイン名を追加する

手順

1. 構成 > ネットワーク > **S3** エンドポイント ドメイン名 を選択します。
2. ドメイン名 **1** フィールドにドメイン名を入力します。さらにドメイン名を追加するには、「別のドメイン名を追加」を選択します。
3. *保存*を選択します。
4. クライアントが使用するサーバー証明書が、必要な S3 エンドポイント 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、"エンドポイントに関連付けられた証明書を更新する" 。
   - クライアントがグローバルS3 API証明書を使用するロードバランサーエンドポイントに接続するか、直接ストレージノードに接続する場合、"グローバルS3 API証明書を更新する" 。
5. エンドポイント ドメイン名要求を解決できるようにするために必要な DNS レコードを追加します。

結果

さて、クライアントがエンドポイントを使用すると `*bucket.s3.company.com*`DNS サーバーは正しいエンドポイントに解決し、証明書は期待どおりにエンドポイントを認証します。

S3エンドポイントのドメイン名を変更する

S3 アプリケーションで使用される名前を変更すると、仮想ホスト形式のリクエストは失敗します。

手順

1. 構成 > ネットワーク > **S3** エンドポイント ドメイン名 を選択します。
2. 編集するドメイン名フィールドを選択し、必要な変更を加えます。
3. *保存*を選択します。
4. 変更を確認するには、[はい] を選択します。

S3エンドポイントドメイン名を削除する

S3 アプリケーションで使用される名前を削除すると、仮想ホスト形式のリクエストは失敗します。

手順

1. 構成 > ネットワーク > **S3** エンドポイント ドメイン名 を選択します。
2. 削除アイコンを選択します  ドメイン名の横にあります。
3. 削除を確認するには、[はい] を選択します。

関連情報

- "S3 REST APIを使用する"
- "IPアドレスを表示"
- "高可用性グループを構成する"

概要: クライアント接続の IP アドレスとポート

オブジェクトを保存または取得するために、S3 クライアント アプリケーションは、すべての管理ノードとゲートウェイ ノードに含まれるロード バランサ サービス、またはすべてのストレージ ノードに含まれるローカル ディストリビューション ルータ (LDR) サービスに接続します。

クライアント アプリケーションは、グリッド ノードの IP アドレスと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。オプションで、負荷分散ノードの高可用性 (HA) グループを作成して、仮想 IP (VIP) アドレスを使用する高可用性接続を提供することもできます。 IP アドレスまたは VIP アドレスではなく完全修飾ドメイン名 (FQDN) を使用してStorageGRIDに接続する場合は、DNS エントリを設定できます。

この表は、クライアントがStorageGRIDに接続できるさまざまな方法と、各接続タイプで使用される IP アドレスとポートをまとめたものです。ロードバランサエンドポイントと高可用性（HA）グループをすでに作成している場合は、IPアドレスを見つける場所グリッド マネージャーでこれらの値を見つけます。

接続が行われる場所	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	ロードバランサのエンドポイントに割り当てられたポート
管理ノード	ロード バランサ	管理ノードのIPアドレス	ロードバランサのエンドポイントに割り当てられたポート
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	ロードバランサのエンドポイントに割り当てられたポート
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

URLの例

クライアント アプリケーションをゲートウェイ 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、次に示すような構造の 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、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、アプリケーションは次の URL を使用してStorageGRIDに接続できます。

`https://192.0.2.5:10443`

IPアドレスを見つける場所

1. グリッドマネージャーにSign inには、"サポートされているウェブブラウザ" 。
2. グリッド ノードの IP アドレスを見つけるには:
   a. 「NODES」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. *概要*タブを選択します。
   d. ノード情報セクションで、ノードの IP アドレスをメモします。
   e. IPv6 アドレスとインターフェース マッピングを表示するには、[詳細を表示] 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）

      管理ノードまたはゲートウェイ ノードを表示していて、それが高可用性グループ内のアクティブ ノードである場合、HA グループの仮想 IP アドレスが eth2 に表示されます。

3. 高可用性グループの仮想 IP アドレスを見つけるには:
   a. 構成 > ネットワーク > *高可用性グループ*を選択します。
   b. 表で、HA グループの仮想 IP アドレスを書き留めます。
4. ロード バランサ エンドポイントのポート番号を見つけるには:
   a. 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。
   b. 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、これらのポート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 ノードでのみ構成されます。他のすべてのポートは、ゲートウェイ ノードと管理ノードの両方で構成されます。

   c. テーブルからエンドポイントの名前を選択します。
   d. クライアント タイプ (S3) がエンドポイントを使用するクライアント アプリケーションと一致していることを確認します。

著作権に関する情報

商標に関する情報