StorageGRID ネットワークと接続の管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

StorageGRID ネットワークと接続の管理

グリッドマネージャを使用して、 StorageGRID のネットワークと接続を設定および管理できます。

を参照してください "S3およびSwiftクライアント接続の設定" を参照して、 S3 または Swift クライアントを接続する方法を確認してください。

- "StorageGRID ネットワークのガイドライン"
- "IPアドレスを表示しています"
- "発信 TLS 接続でサポートされる暗号"
- "ネットワーク転送の暗号化の変更"
- "サーバ証明書の設定"
- "ストレージプロキシを設定しています"
- "管理プロキシの設定"
- "トラフィック分類ポリシーの管理"
- "リンクコストとは"

StorageGRID ネットワークのガイドライン

StorageGRID では、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

> グリッドノードのネットワークを変更または追加するには、リカバリとメンテナンスの手順を参照してください。ネットワークトポロジの詳細については、ネットワークの手順を参照してください。

Grid ネットワーク

必須グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。

管理ネットワーク

任意。通常、管理ネットワークはシステムの管理とメンテナンスに使用されます。クライアントプロトコルアクセスにも使用できます。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。

クライアントネットワーク

任意。クライアントネットワークはオープンネットワークで、主に S3 および Swift クライアントアプリケーションへのアクセスに使用されます。そのため、グリッドネットワークを分離してセキュリティを確保できま

す。クライアントネットワークは、ローカルゲートウェイ経由でアクセス可能なすべてのサブネットと通信できます。

ガイドライン

- 各 StorageGRID グリッドノードには、割り当て先のネットワークごとに専用のネットワークインターフェイス、 IP アドレス、サブネットマスク、およびゲートウェイが必要です。
- 1 つのグリッドノードに複数のインターフェイスを設定することはできません。
- 各ネットワークのグリッドノードごとに、単一のゲートウェイがサポートされます。このゲートウェイはノードと同じサブネット上に配置する必要があります。必要に応じて、より複雑なルーティングをゲートウェイに実装できます。
- 各ノードでは、各ネットワークが特定のネットワークインターフェイスにマッピングされます。

ネットワーク	インターフェイス名
グリッド（ Grid ）	eth0
管理（オプション）	Eth1
クライアント（オプション）	eth2

- ノードが StorageGRID アプライアンスに接続されている場合は、ネットワークごとに特定のポートが使用されます。詳細については、使用しているアプライアンスのインストール手順を参照してください。
- デフォルトルートはノードごとに自動的に生成されます。eth2 が有効な場合、 0.0.0.0/0 は eth2 のクライアントネットワークを使用します。eth2 が無効な場合、 0.0.0.0/0 は eth0 のグリッドネットワークを使用します。
- クライアントネットワークは、グリッドノードがグリッドに参加するまで動作状態になりません
- グリッドが完全にインストールされる前にインストールユーザインターフェイスにアクセスできるように、グリッドノード導入時に管理ネットワークを設定できます。

関連情報

""

"ネットワークガイドライン"

IPアドレスを表示しています

StorageGRID システムの各グリッドノードの IP アドレスを表示できます。コマンドラインでこの IP アドレスを使用してグリッドノードにログインし、さまざまなメンテナンス手順を実行できます。

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。

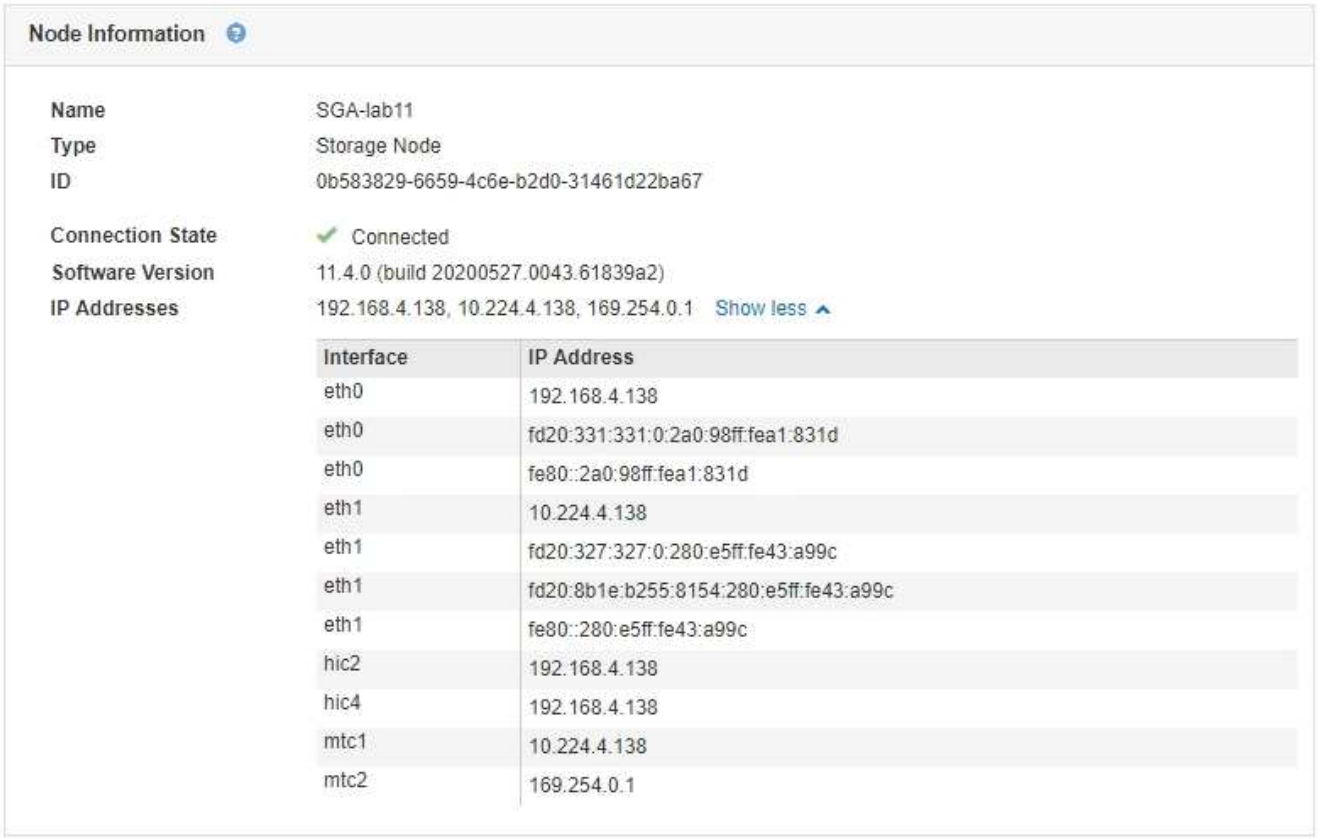
このタスクについて

IPアドレス変更の詳細については、リカバリおよびメンテナンスの手順を参照してください。

手順

1. ノード*>**grid node**>* Overview *を選択します。
2. [IP Addresses]のタイトルの右にある[**Show More**]をクリックします。

   このグリッドノードの IP アドレスがテーブルに表示されます。



関連情報

""

発信 **TLS** 接続でサポートされる暗号

StorageGRID システムでは、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの Transport Layer Security （ TLS ）接続でサポートされる暗号スイートに制限があります。

サポートされる **TLS** のバージョン

StorageGRID では、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの接続で TLS 1.2 と TLS 1.3 がサポートされます。

外部システムとの互換性を確保するために、外部システムとの使用がサポートされている TLS 暗号が選択されています。S3 または Swift クライアントアプリケーションで使用できる暗号のリストは、このリストよりも大容量です。

プロトコルのバージョン、暗号、鍵交換アルゴリズム、 MAC アルゴリズムなどの TLS 設定オプションは、 StorageGRID では設定できません。これらの設定について具体的なご要望がある場合は、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。

サポートされている **TLS 1.2** 暗号スイート

次の TLS 1.2 暗号スイートがサポートされています。

- TLS_ECDHE_RSA_With _AES_128_GCM_SHA256
- TLS_ECDHE_RSA_with _AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_With _AES_128_GG_SHA256
- TLS_ECDHE_ECDSA_With _AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_With _AES_128_GCM _SHA256
- TLS_RSA_With _AES_256_GCM_SHA384

サポートされている **TLS 1.3** 暗号スイート

次の TLS 1.3 暗号スイートがサポートされています。

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM _SHA256

ネットワーク転送の暗号化の変更

StorageGRID システムでは、 Transport Layer Security （ TLS ）を使用して、グリッドノード間の内部制御トラフィックを保護します。Network Transfer Encryption オプションは、グリッドノード間の制御トラフィックを暗号化するために TLS で使用されるアルゴリズムを設定します。この設定はデータ暗号化には影響しません。

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

デフォルトでは、ネットワーク転送の暗号化には AES256-SHA アルゴリズムが使用されます。AES128-SHA アルゴリズムを使用して暗号化することもできます。

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、ネットワーク転送の暗号化を * AES128-SHA * または * AES256-SHA * （デフォルト）に変更します。

3. [保存（ Save ）] をクリックします。

サーバ証明書の設定

StorageGRID システムで使用されるサーバ証明書をカスタマイズできます。

StorageGRID システムは、用途が異なる複数のセキュリティ証明書を使用します。

- 管理インターフェイスのサーバ証明書：Grid Manager、Tenant Manager、Grid管理API、およびテナント管理APIへのアクセスを保護するために使用します。
- ストレージAPIのサーバ証明書：ストレージノードおよびゲートウェイノードへのアクセスを保護するために使用します。これらのノードは、APIクライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

インストール時に作成されたデフォルトの証明書を使用できるほか、デフォルトの証明書のいずれか、または両方を独自のカスタム証明書に置き換えることもできます。

サポートされているカスタムサーバ証明書のタイプ

StorageGRID システムでは、RSAまたはECDSA（Elliptic Curve Digital Signature Algorithm）で暗号化されたカスタムサーバ証明書がサポートされます。

StorageGRID でREST APIのクライアント接続を保護する方法の詳細については、S3またはSwiftの実装ガイドを参照してください。

ロードバランサエンドポイントの証明書

StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、ロードバランサエンドポイントの設定手順を参照してください。

関連情報

"S3 を使用する"

"Swift を使用します"

"ロードバランサエンドポイントの設定"

Grid Managerおよび**Tenant Manager**用のカスタムサーバ証明書を設定する

デフォルトの StorageGRID サーバ証明書を単一のカスタムサーバ証明書に置き換える

と、ユーザがグリッドマネージャとテナントマネージャにアクセスする際にセキュリティの警告が表示されなくなります。

このタスクについて

デフォルトでは、管理ノードごとに、グリッド CA によって署名された証明書が 1 つずつ発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1つのカスタムサーバ証明書がすべての管理ノードに対して使用されるため、Grid ManagerおよびTenant Managerへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードに一致するカスタム証明書を定義してください。

設定はサーバ上で行う必要があります。また、使用しているルート認証局（CA）によっては、ユーザがGrid ManagerおよびTenant Managerへのアクセスに使用するWebブラウザにルートCA証明書をインストールすることも必要になります。

サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと、Expiration of server certificate for Management Interface アラートと**Legacy Management Interface Certificate Expiry**（**MCEP**）アラームの両方がトリガーされます。必要に応じて、 Support **>** Tools **>** Grid Topology を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「***_ primary Admin Node_**>* CMN **>** Resources *」を選択します。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイスサーバ証明書の有効期限が切れます。
- カスタムの管理インターフェイスサーバ証明書をデフォルトのサーバ証明書に戻した場合。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Management Interface Server Certificateセクションで、* Install Custom Certificate *をクリックします。
3. 必要なサーバ証明書ファイルをアップロードします。
   - サーバー証明書：カスタムサーバー証明書ファイル（`.crt`）。
   - * Server 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。
4. [保存（ Save ）] をクリックします。

以降すべての新しいクライアント接続には、カスタムサーバ証明書が使用されます。

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。

新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

Grid ManagerおよびTenant Manager用のデフォルトのサーバ証明書のリストア

Grid ManagerおよびTenant Managerでデフォルトのサーバ証明書を使用するように戻すことができます。

手順

1. [* Configuration]>[Network Settings]>[Server Certificates*]を選択します。
2. Manage Interface Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

   デフォルトのサーバ証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいクライアント接続には、デフォルトのサーバ証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

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

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（廃止）へのS3またはSwiftクライアント接続に使用するサーバ証明書は、置き換えることができます。置き換え用のカスタムサーバ証明書は組織に固有のものです。

このタスクについて

デフォルトでは、すべてのストレージノードに、グリッド CA によって署名された X.509 サーバ証明書が発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1 つのカスタムサーバ証明書がすべてのストレージノードに対して使用されるため、ストレージエンドポイントへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージノードに一致するカスタム証明書を定義してください。

サーバでの設定が完了したら、使用しているルート認証局（CA）によっては、ユーザがシステムへのアクセスに使用するS3またはSwift APIクライアントにルートCA証明書をインストールすることも必要になる場合があります。

サーバ証明書の問題によって処理が中断されないようにするために、Expiration of server certificate for Storage API Endpoints アラートと、ルートサーバ証明書の有効期限が近づくと従来の**Storage API Service Endpoints Certificate Expiry**（**SCEP**）アラームの両方がトリガーされます。必要に応じて、「 Support **Tools * Grid Topology *** 」を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「**_ primary Admin Node_** CMN * Resources *」を選択します。

カスタム証明書は、クライアントがゲートウェイノード上の廃止されたCLBサービスを使用してStorageGRIDに接続する場合、またはクライアントがストレージノードに直接接続する場合にのみ使用されます。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を使用してStorageGRID に接続するS3またはSwiftクライアントは、ロードバランサエンドポイント用に設定された証明書を使用します。

*ロードバランサエンドポイント証明書の有効期限*アラートは、まもなく期限切れになるロードバランサエンドポイントに対してトリガーされます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Install Custom Certificate *をクリックします。
3. 必要なサーバ証明書ファイルをアップロードします。
   - サーバー証明書：カスタムサーバー証明書ファイル（`.crt`）。
   - * Server 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。
4. [保存（ Save ）] をクリックします。

   以降すべての新しいAPIクライアント接続には、カスタムサーバ証明書が使用されます。

   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。

   新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

関連情報

"S3 を使用する"

"Swift を使用します"

"S3 APIエンドポイントのドメイン名を設定しています"

S3およびSwiftのREST APIエンドポイント用のデフォルトサーバ証明書のリストア

S3およびSwiftのREST APIエンドポイント用のデフォルトサーバ証明書を使用する設定に戻すことができます。

手順

1. [* Configuration]>[Network Settings]>[Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

   オブジェクトストレージAPIエンドポイント用のデフォルトサーバ証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいAPIクライアント接続には、デフォルトのサーバ証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

StorageGRID システムのCA証明書をコピーしています

StorageGRID は、内部の認証局（CA）を使用して内部トラフィックを保護します。独自の証明書をアップロードしても、この証明書は変更されません。

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。

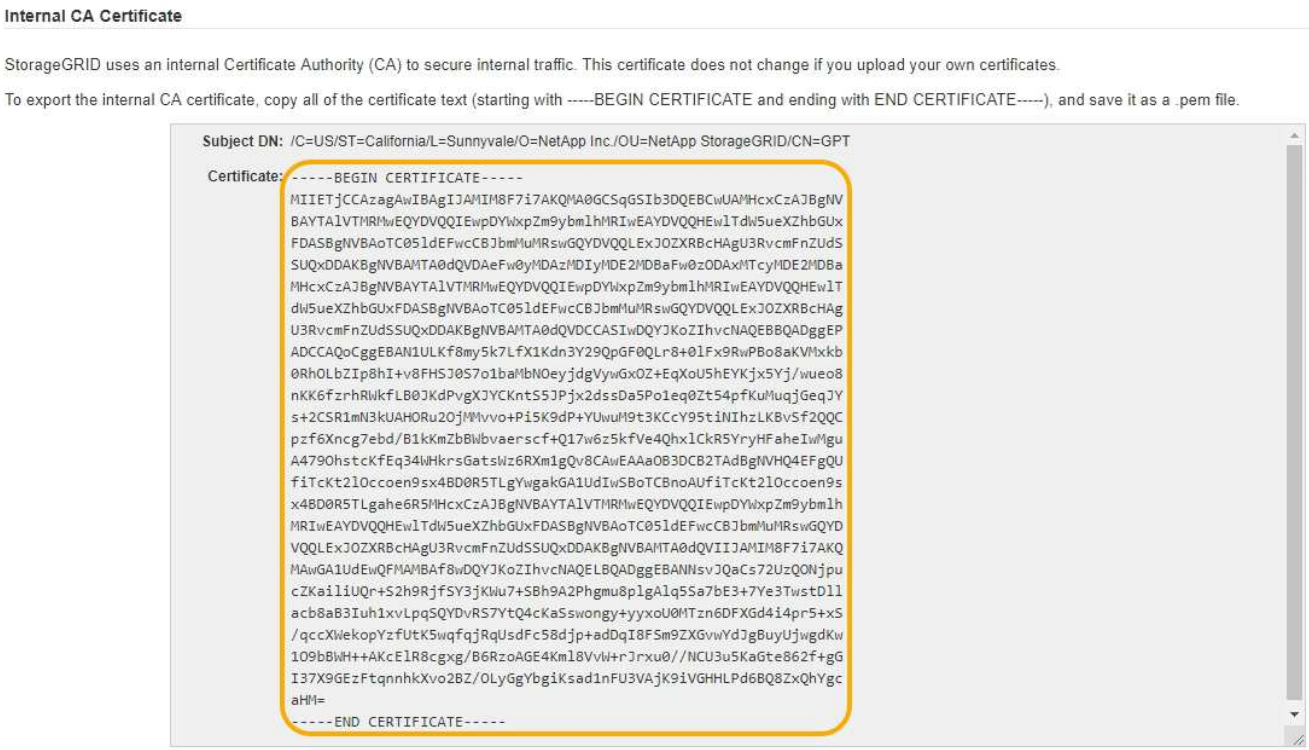
このタスクについて

カスタムサーバ証明書が設定されている場合、クライアントアプリケーションはカスタムサーバ証明書を使用してサーバを検証する必要があります。StorageGRID システムから CA 証明書をコピーしない。

手順

1. [* Configuration]>[Network Settings]>[Server Certificates*]を選択します。
2. [内部CA証明書（* Internal CA Certificate *）]セクションで、すべての証明書テキストを選択します。

   を含める必要があります `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` を選択します。



3. 選択したテキストを右クリックし、*コピー*を選択します。
4. コピーした証明書をテキストエディタに貼り付けます。
5. 拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

FabricPool 用のStorageGRID 証明書を設定しています

厳密なホスト名検証を実行する S3 クライアントでは、 FabricPool を使用する ONTAP クライアントなどの厳密なホスト名検証の無効化をサポートしていない場合は、ロードバランサエンドポイントの設定時にサーバ証明書を生成またはアップロードできます。

必要なもの

- 特定のアクセス権限が必要です。
- 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。

このタスクについて

ロードバランサエンドポイントを作成する際には、自己署名サーバ証明書を生成するか、既知の認証局（CA）によって署名された証明書をアップロードできます。本番環境では、既知の CA によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

次の手順は、 FabricPool を使用する S3 クライアントを対象とした一般的なガイドラインです。詳細な情報と手順については、StorageGRID for FabricPool の設定手順を参照してください。

ゲートウェイノード上の別の Connection Load Balancer （ CLB ）サービスは廃止され、FabricPool での使用は推奨されなくなりました。

手順

1. 必要に応じて、 FabricPool で使用するハイアベイラビリティ（ HA ）グループを設定します。
2. FabricPool で使用する S3 ロードバランサエンドポイントを作成します。

   HTTPSロードバランサエンドポイントを作成する際に、サーバ証明書、証明書の秘密鍵、およびCAバンドルのアップロードを求めるプロンプトが表示されます。

3. ONTAP でクラウド階層として StorageGRID を接続します。

   ロードバランサエンドポイントのポートと、アップロードした CA 証明書で使用する完全修飾ドメイン名を指定します。次に、 CA 証明書を指定します。

   中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。

関連情報

"StorageGRID for FabricPool を設定します"

管理インターフェイス用の自己署名サーバ証明書の生成

スクリプトを使用して、ホスト名の厳密な検証が必要な管理APIクライアント用の自己署名サーバ証明書を生成できます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

本番環境では、既知の認証局（CA）によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

手順

1. 各管理ノードの完全修飾ドメイン名（ FQDN ）を取得します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

3. 新しい自己署名証明書を使用して StorageGRID を設定します。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - の場合 `--domains`、ワイルドカードを使用して、すべての管理ノードの完全修飾ドメイン名を表します。例： `*.ui.storagegrid.example.com` ワイルドカード*を使用して表します `admin1.ui.storagegrid.example.com` および `admin2.ui.storagegrid.example.com`。
   - 設定 `--type` 終了： `management` Grid ManagerおよびTenant Managerで使用される証明書を設定するため。
   - デフォルトでは、生成された証明書の有効期間は 1 年間（ 365 日）です。この期間を過ぎる前に証明書を再作成する必要があります。を使用できます `--days` デフォルトの有効期間を上書きする引数。

     > 証明書の有効期間は、で始まります `make-certificate` を実行します。管理APIクライアントがStorageGRID と同じ時間ソースと同期されるようにしてください。同期されていないと、クライアントが証明書を拒否する可能性があります。

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 365
     ```

     出力には、管理 API クライアントで必要なパブリック証明書が含まれています。

4. 証明書を選択してコピーします。

   BEGIN タグと END タグも含めて選択してください。

5. コマンドシェルからログアウトします。 `$ exit`
6. 証明書が設定されたことを確認します。
   a. Grid Manager にアクセスします。
   b. 「* Configuration * Server Certificates * Management Interface Server Certificate *」を選択します。
7. コピーしたパブリック証明書を使用するように管理APIクライアントを設定します。BEGIN タグと END タグを含めてください。

ストレージプロキシを設定しています

プラットフォームサービスまたはクラウドストレージプールを使用している場合は、ストレージノードと外部の S3 エンドポイントの間に非透過型プロキシを設定できます。たとえば、インターネット上のエンドポイントなどの外部エンドポイントへプラットフォームサービスメッセージを送信する場合などには、非透過型プロキシが必要です。

必要なもの

- 特定のアクセス権限が必要です。
- 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。

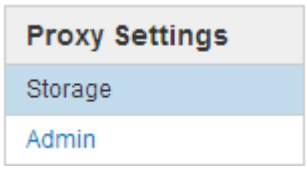
このタスクについて

設定できるストレージプロキシは 1 つです。

手順

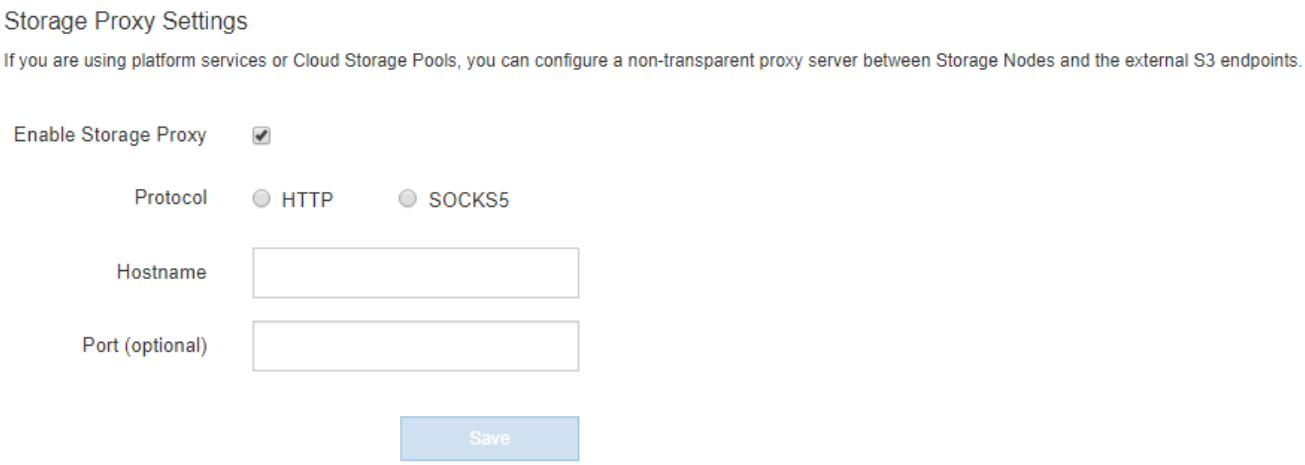
1. [環境設定*ネットワーク設定*プロキシ設定]を選択します。

   ストレージプロキシの設定ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。



2. Enable Storage Proxy （ストレージプロキシの有効化）チェックボックスを選択します。

   ストレージプロキシを設定するためのフィールドが表示されます。



3. 非透過型ストレージプロキシのプロトコルを選択します。
4. プロキシサーバのホスト名または IP アドレスを入力します。
5. 必要に応じて、プロキシサーバへの接続に使用するポートを入力します。

   プロトコルにデフォルトのポート 80 を使用する場合は、このフィールドを空白のままにできます。 HTTP の場合は 80 、 SOCKS5 の場合は 1080 です。

6. [保存（ Save ）] をクリックします。

   ストレージプロキシが保存されたら、プラットフォームサービスまたはクラウドストレージプールの新しいエンドポイントを設定してテストできます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

7. プロキシサーバの設定をチェックして、 StorageGRID からのプラットフォームサービス関連メッセージがブロックされないようにします。

完了後

ストレージプロキシを無効にする必要がある場合は、*ストレージプロキシを有効にする*チェックボックスの

選択を解除し、*保存*をクリックします。

関連情報

"プラットフォームサービス用のネットワークとポート"

"ILM を使用してオブジェクトを管理する"

管理プロキシの設定

HTTPまたはHTTPSを使用してAutoSupport メッセージを送信する場合は、管理ノードとテクニカルサポート（AutoSupport ）の間に非透過型プロキシサーバを設定できます。

必要なもの

- 特定のアクセス権限が必要です。
- 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。

このタスクについて

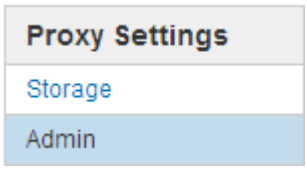
設定できる管理プロキシは 1 つです。

手順

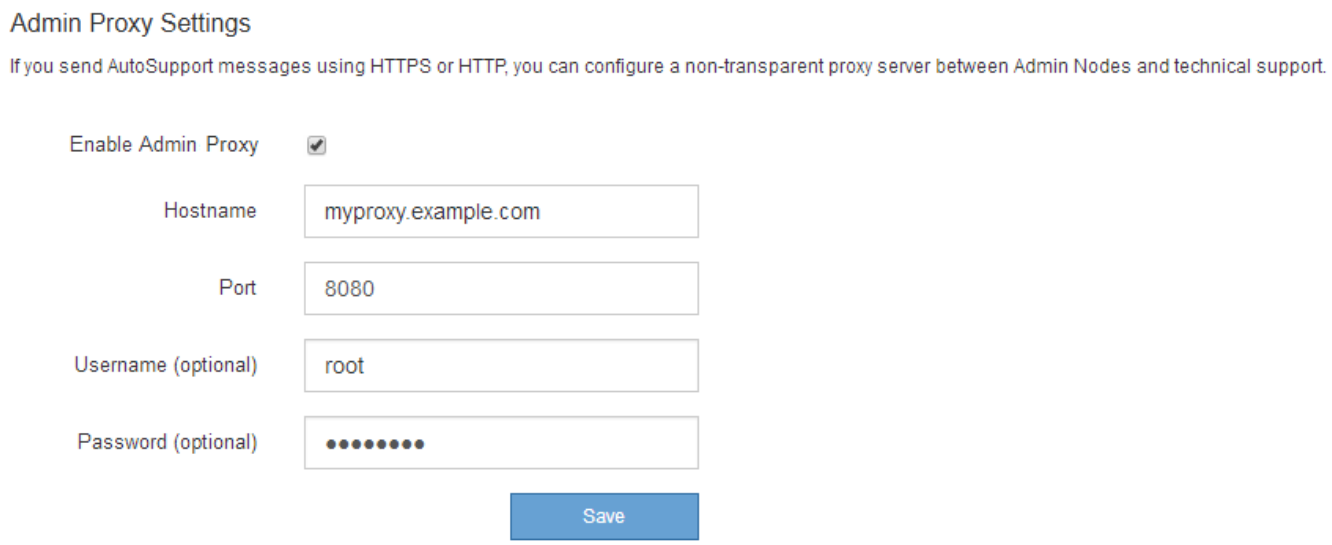
1. [環境設定*ネットワーク設定*プロキシ設定]を選択します。

   Admin Proxy Settings ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。

2. サイドバーのメニューから、 **Admin** を選択します。



3. [管理プロキシを有効にする *] チェックボックスをオンにします。



4. プロキシサーバのホスト名または IP アドレスを入力します。
5. プロキシサーバへの接続に使用するポートを入力します。
6. 必要に応じて、プロキシユーザ名を入力します。

   プロキシサーバでユーザ名が不要な場合は、このフィールドを空白のままにします。

7. 必要に応じて、プロキシパスワードを入力します。

   プロキシサーバでパスワードが不要な場合は、このフィールドを空白のままにします。

8. [保存（ Save ）] をクリックします。

   管理プロキシが保存されると、管理ノードとテクニカルサポートの間にプロキシサーバが設定されます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

9. プロキシを無効にする必要がある場合は、*管理者プロキシを有効にする*チェックボックスの選択を解除し、*保存*をクリックします。

関連情報

"AutoSupport メッセージのプロトコルの指定"

トラフィック分類ポリシーの管理

サービス品質（ QoS ）サービスを強化するために、トラフィック分類ポリシーを作成して、さまざまなタイプのネットワークトラフィックを識別および監視できます。これらのポリシーは、トラフィックの制限と監視に役立ちます。

トラフィック分類ポリシーは、ゲートウェイノードおよび管理ノードの StorageGRID ロードバランササービス上のエンドポイントに適用されます。トラフィック分類ポリシーを作成するには、ロードバランサエンドポイントを作成しておく必要があります。

ルールとオプションの制限を一致させる

各トラフィック分類ポリシーには、次のエンティティに関連するネットワークトラフィックを識別する 1 つ以上の一致ルールが含まれています。

- バケット
- テナント
- サブネット（クライアントを含む IPv4 サブネット）
- エンドポイント（ロードバランサエンドポイント）

StorageGRID は、ルールの目的に応じて、ポリシー内のルールに一致するトラフィックを監視します。ポリシーのルールに一致するトラフィックは、そのポリシーによって処理されます。逆に、指定されたエンティティを除くすべてのトラフィックを照合するルールを設定できます。

必要に応じて、次のパラメータに基づいてポリシーの制限を設定できます。

- 総帯域幅
- 総帯域幅アウト
- 同時読み取り要求
- 同時書き込み要求
- での要求ごとの帯域幅
- 要求ごとの帯域幅アウト
- 読み取り要求レート
- 書き込み要求の速度

> ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、 StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。

トラフィック制限

トラフィック分類ポリシーを作成した場合、トラフィックは設定したルールおよび制限のタイプに応じて制限されます。集約または要求ごとの帯域幅制限の場合、要求は、設定したレートでストリームインまたはアウトされます。StorageGRID では 1 つの速度しか適用できないため、最も特定のポリシーがマッチするのはマッチャーのタイプです。それ以外のすべての制限タイプでは、クライアント要求は 250 ミリ秒遅延し、一致するポリシー制限を超える要求に対しては 503 スローダウン応答を受信します。

Grid Manager では、トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

SLAでのトラフィック分類ポリシーの使用

トラフィック分類ポリシーを容量制限およびデータ保護とともに使用して、容量、データ保護、およびパフォーマンスに固有のサービスレベル契約（ SLA ）を適用できます。

トラフィック分類の制限は、ロードバランサごとに実装されます。複数のロードバランサに同時にトラフィックが分散されている場合、合計最大速度は指定した速度制限の倍数になります。

次の例は、 SLA の 3 つの階層を示しています。トラフィック分類ポリシーを作成して、各 SLA 層のパフォーマンス目標を達成できます。

サービスレベル階層	容量	データ保護	パフォーマンス	コスト
ゴールド	1 PB のストレージを使用できます	3 コピーの ILM ルール	25 、 000 要求 / 秒 5 GB/ 秒（ 40 Gbps ）の帯域幅	$$/ 月
シルバー	250 TB のストレージを使用できます	2 コピーの ILM ルール	10 K 要求 / 秒 1.25 GB/ 秒（ 10 Gbps ）の帯域幅	$/ 月
ブロンズ	100TB のストレージを使用できます	2 コピーの ILM ルール	5 、 000 要求 / 秒 1 GB/ 秒（ 8 Gbps ）の帯域幅	月あたりのコスト

トラフィック分類ポリシーの作成

バケット、テナント、 IP サブネット、またはロードバランサエンドポイントごとにネットワークトラフィックを監視し、必要に応じて制限する場合は、トラフィック分類ポリシーを作成します。必要に応じて、帯域幅、同時要求数、または要求速度に基づいてポリシーの制限を設定できます。

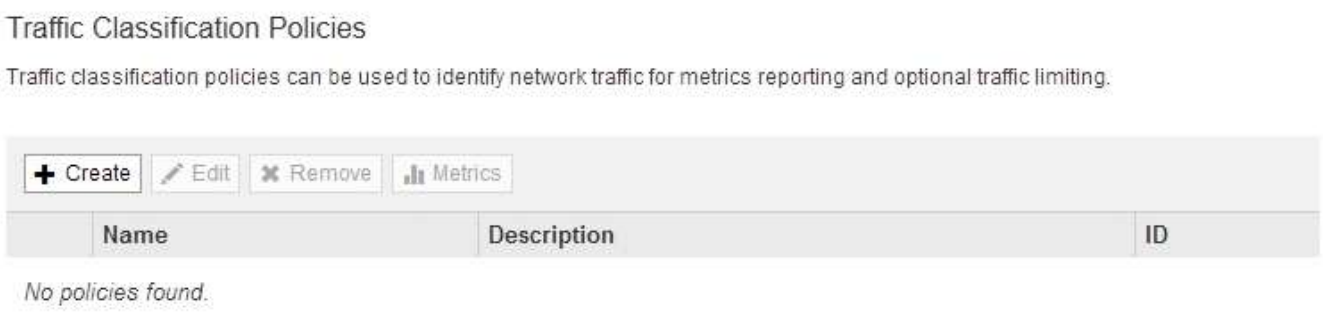
必要なもの

- 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。
- 照合するロードバランサエンドポイントを作成しておく必要があります。
- 該当するテナントを作成しておく必要があります。

手順

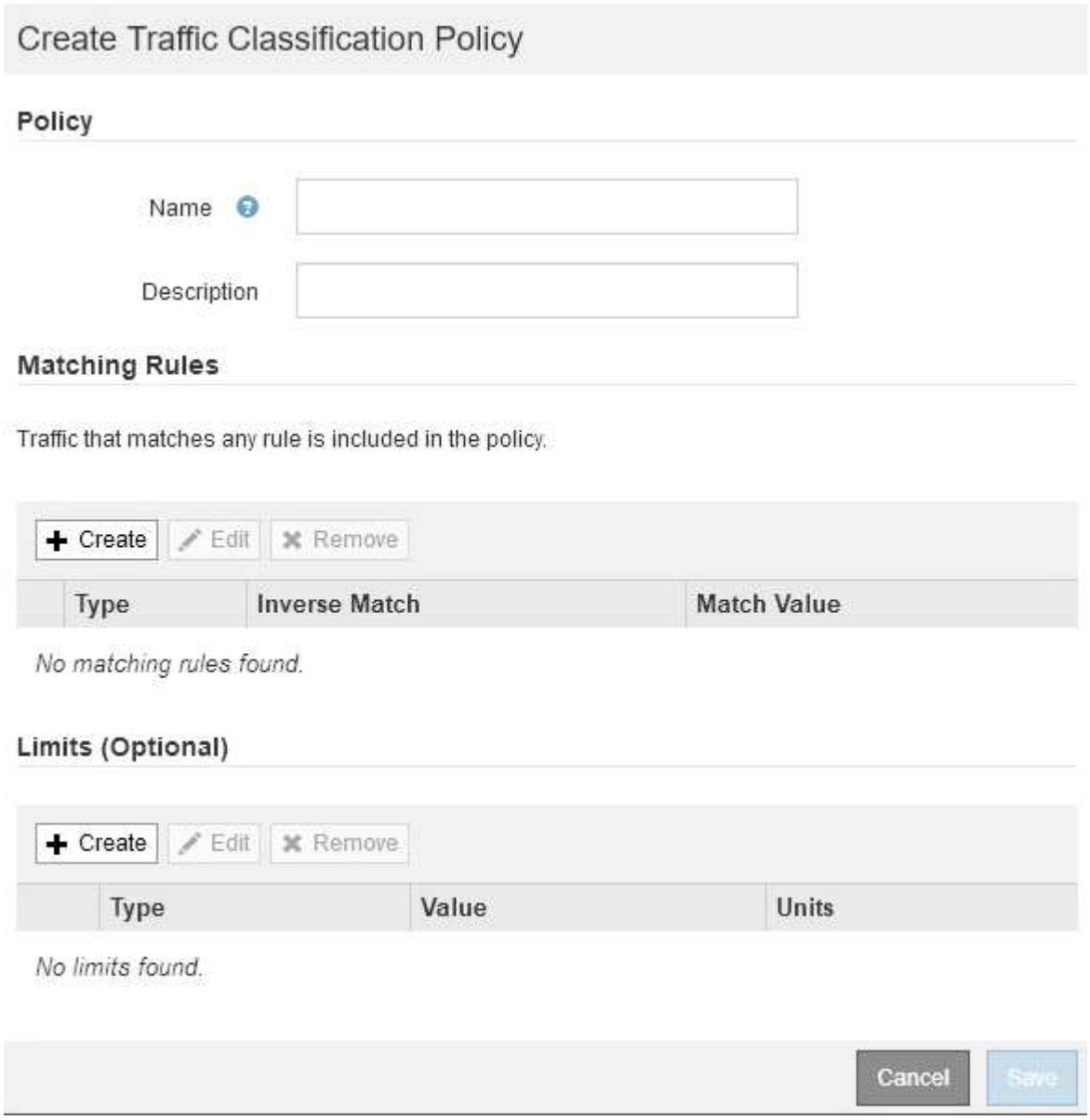
1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示されます。



2. [作成（ Create ）] をクリックします。

Create Traffic Classification Policy ダイアログボックスが表示されます。



3. [* 名前 *] フィールドに、ポリシーの名前を入力します。

ポリシーを識別できるように、わかりやすい名前を入力します。

4. 必要に応じて、 * 概要 * フィールドにポリシーの概要 を追加します。

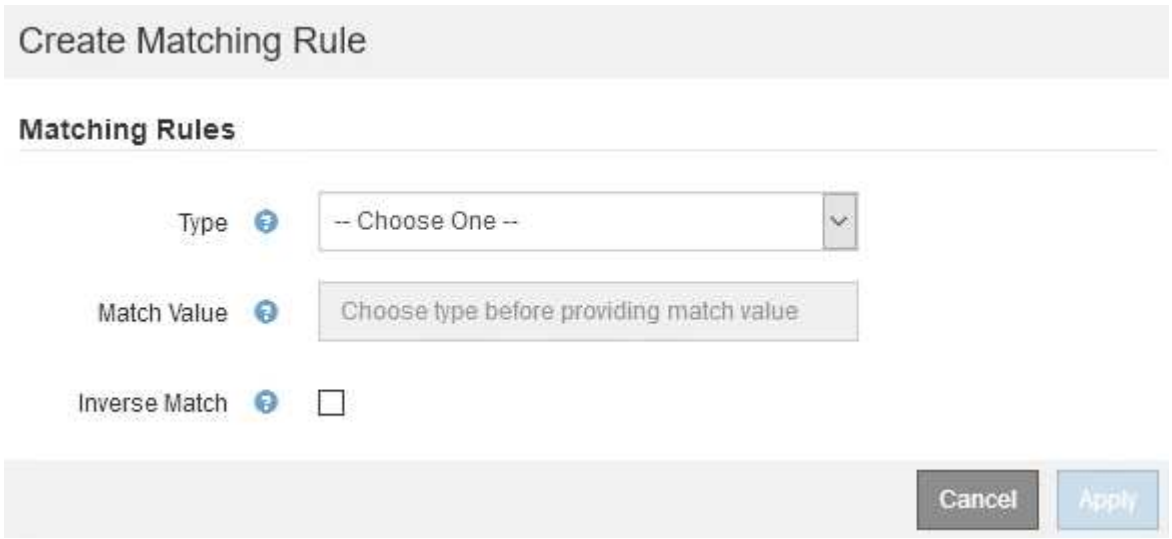
   たとえば、このトラフィック分類ポリシー環境 の内容と制限する内容を説明します。

5. ポリシーに一致するルールを 1 つ以上作成します。

   一致ルールは、このトラフィック分類ポリシーの影響を受けるエンティティを制御します。たとえば、このポリシーを特定のテナントのネットワークトラフィックに適用する場合は、テナントを選択します。または、このポリシーを特定のロードバランサエンドポイントのネットワークトラフィックに適用する場合は、 [Endpoint] を選択します。

   a. [マッチングルール（Matching Rules *）]セクションで[*作成（Create *）]をクリックし

      [Create Matching Rule] ダイアログボックスが表示されます。



   b. [* タイプ *] ドロップダウンから、一致するルールに含めるエンティティのタイプを選択します。

   c. [**match value**] フィールドに、選択したエンティティのタイプに基づいて照合値を入力します。

      - Bucket ：バケット名を入力します。
      - Bucket Regex ：一連のバケット名と一致するために使用される正規表現を入力します。

        正規表現は固定されていません。バケット名の先頭にある ｛キャレット｝ アンカーを使用し、名前の末尾に $ アンカーを使用します。

      - CIDR ： IPv4 サブネットを CIDR 表記で入力し、目的のサブネットと一致させます。
      - Endpoint ：既存のエンドポイントのリストからエンドポイントを選択します。これは、ロードバランサエンドポイントのページで定義したロードバランサエンドポイントです。
      - テナント：既存のテナントのリストからテナントを選択します。テナントの一致は、アクセス対象のバケットの所有権に基づきます。バケットへの匿名アクセスは、バケットを所有するテナントと一致します。

   d. 定義した Type および Match 値と一致するすべての TRAFFER_EXCEPT _Traffic を照合する場合は、* Inverse * チェックボックスをオンにします。それ以外の場合は、このチェックボックスをオフのままにします。

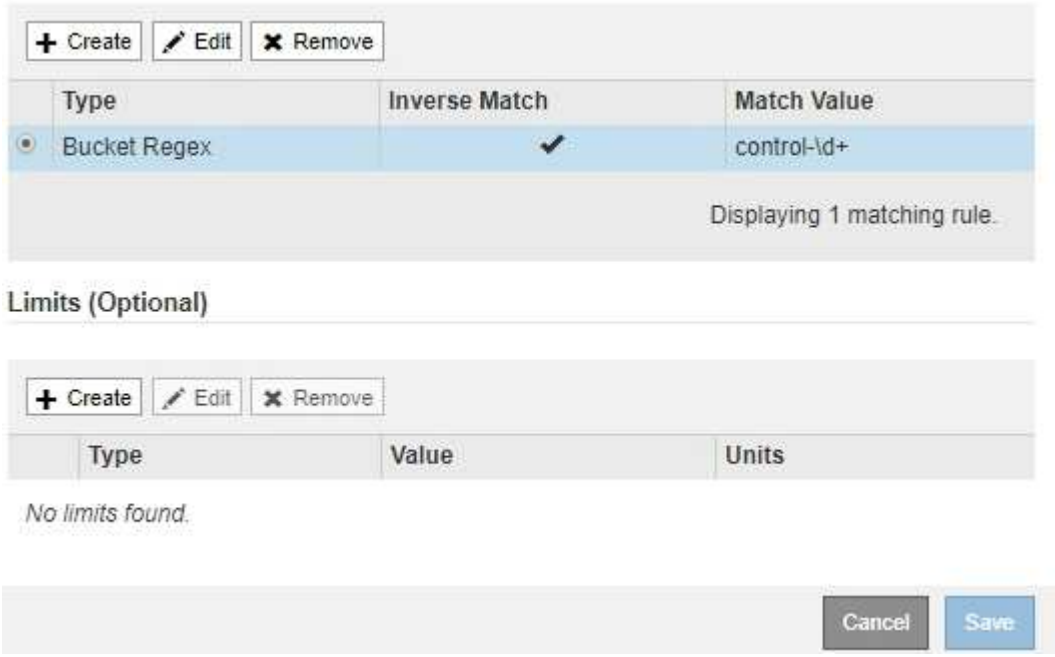
      たとえば、このポリシーをいずれかのロードバランサエンドポイントを除くすべてのエンドポイント

に適用する場合は、除外するロードバランサエンドポイントを指定し、 * Inverse * を選択します。

> 少なくとも 1 つが逆マッチャーである複数のマッチャーを含むポリシーの場合、すべてのリクエストに一致するポリシーを作成しないように注意してください。

e. [適用（ Apply ）] をクリックします。

ルールが作成され、 [Matching Rules] テーブルに表示されます。



a. ポリシーに対して作成するルールごとに上記の手順を繰り返します。

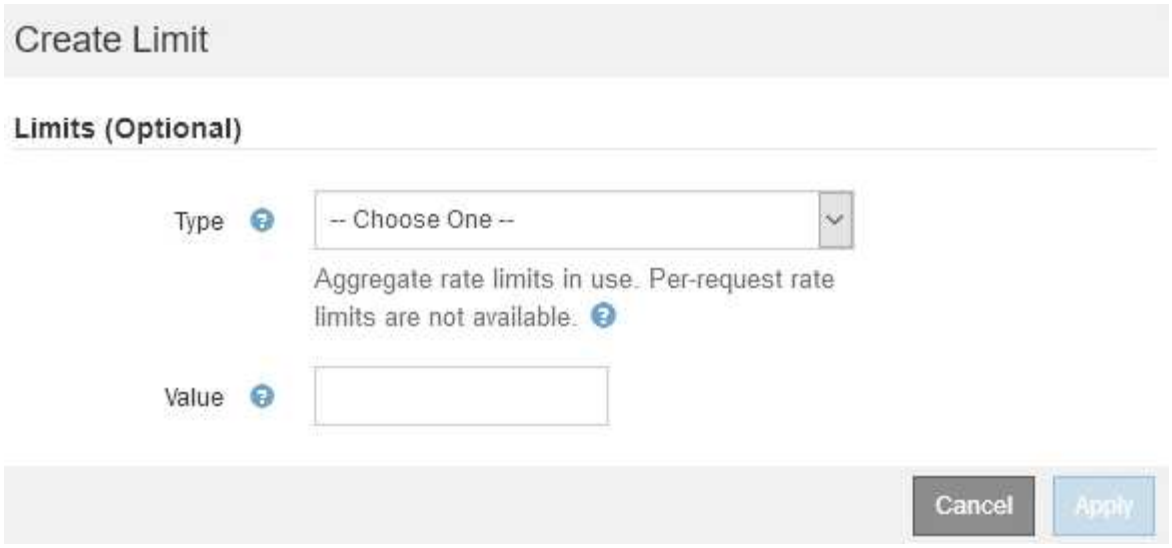
> ルールに一致するトラフィックは、ポリシーによって処理されます。

6. 必要に応じて、ポリシーの制限を作成します。

> 制限を作成しない場合でも、ポリシーに一致するネットワークトラフィックを監視できるように StorageGRID で指標が収集されます。

a. 「制限」セクションで「*作成」をクリックします。

境界を作成（ Create Limit ）ダイアログボックスが表示されます。



b. [* タイプ *] ドロップダウンから、ポリシーに適用する制限のタイプを選択します。

次のリストの * in * は S3 または Swift クライアントから StorageGRID ロードバランサへのトラフィックを表し、 * out * はロードバランサから S3 または Swift クライアントへのトラフィックを表しています。

- 総帯域幅
- 総帯域幅アウト
- 同時読み取り要求
- 同時書き込み要求
- での要求ごとの帯域幅
- 要求ごとの帯域幅アウト
- 読み取り要求レート
- 書き込み要求の速度

ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、 StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。

帯域幅の制限については、設定された制限のタイプに最も一致するポリシーが StorageGRID によって適用されます。たとえば、トラフィックを一方向のみに制限するポリシーがある場合、帯域幅制限が設定されている他のポリシーと一致するトラフィックがあっても、反対方向のトラフィックは無制限になります。StorageGRID は、帯域幅制限の「ベスト」マッチを次の順序で実装します。

- 正確な IP アドレス（ /32 マスク）
- 正確なバケット名
- バケットの正規表現
- テナント

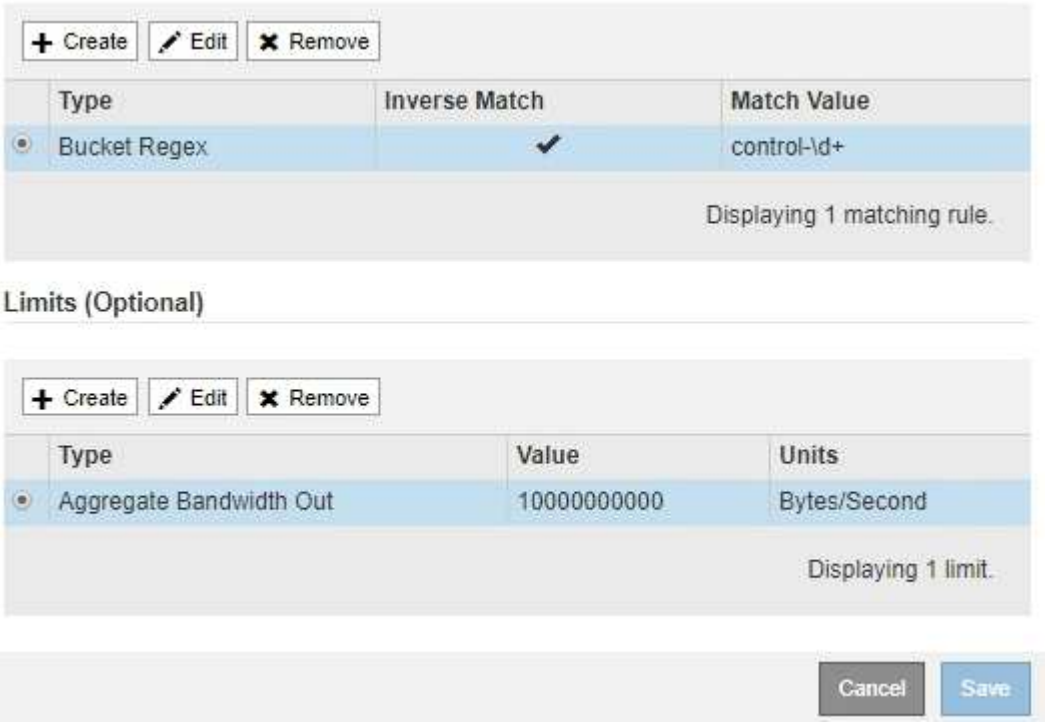
- エンドポイント
- 正確でない CIDR の一致（ /32 ではない）
- 逆一致

c. [* 値 *] フィールドに、選択した制限のタイプの数値を入力します。

制限を選択すると、想定される単位が表示されます。

d. [適用（ Apply ）] をクリックします。

境界が作成され、 [境界（ Limits ）] テーブルにリストされます。



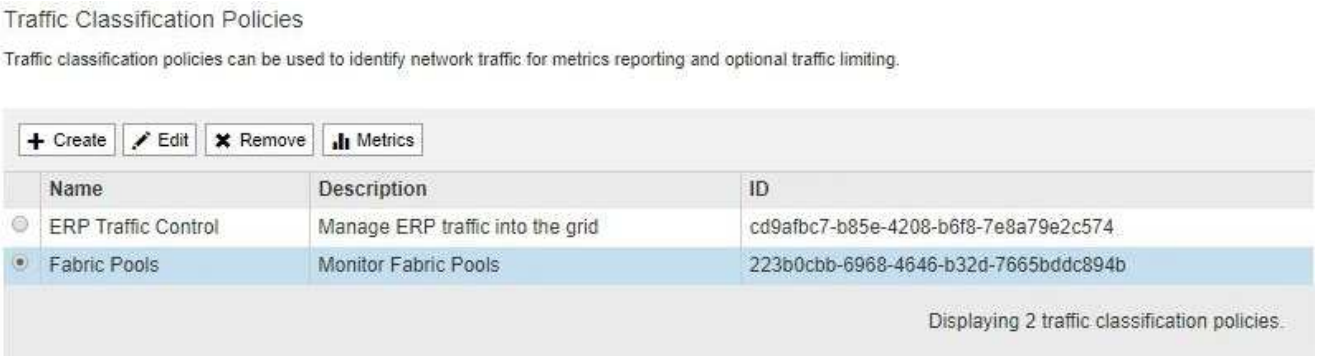
e. ポリシーに追加する上限ごとに、上記の手順を繰り返します。

たとえば、 SLA 階層に 40Gbps の帯域幅制限を作成する場合は、制限されたアグリゲート帯域幅と合計帯域幅の制限を作成し、各帯域幅を 40Gbps に設定します。

1 秒あたりのメガバイト数をギガビット / 秒に変換するには、 8 倍にします。たとえば、 125 MB/ 秒は 1 、 000 Mbps または 1 Gbps に相当します。

7. ルールと制限の作成が完了したら、*保存*をクリックします。

ポリシーが保存され、 Traffic Classification Policies テーブルにリストされます。



S3 および Swift クライアントトラフィックがトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

関連情報

"負荷分散の管理"

"ネットワークトラフィックメトリックの表示"

トラフィック分類ポリシーを編集する

トラフィック分類ポリシーを編集して、その名前または概要 を変更したり、ポリシーのルールや制限を作成、編集、削除したりできます。

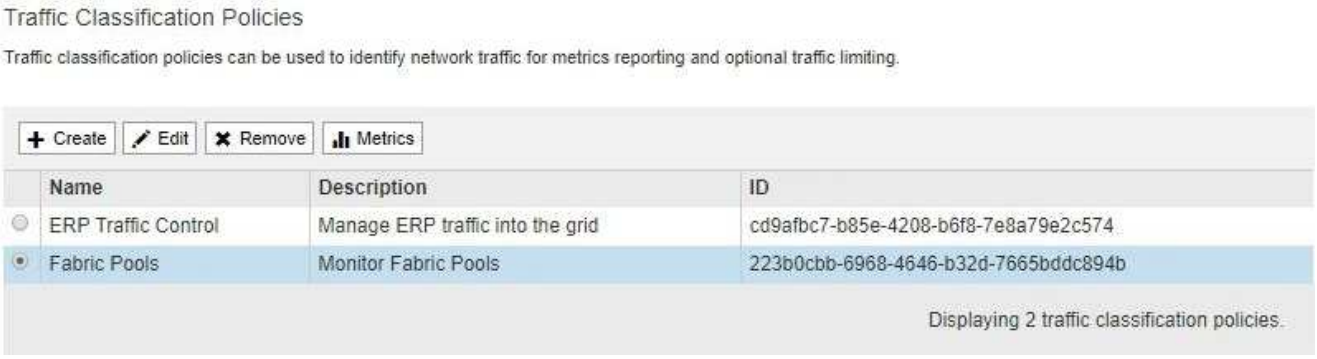
必要なもの

- 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。

手順

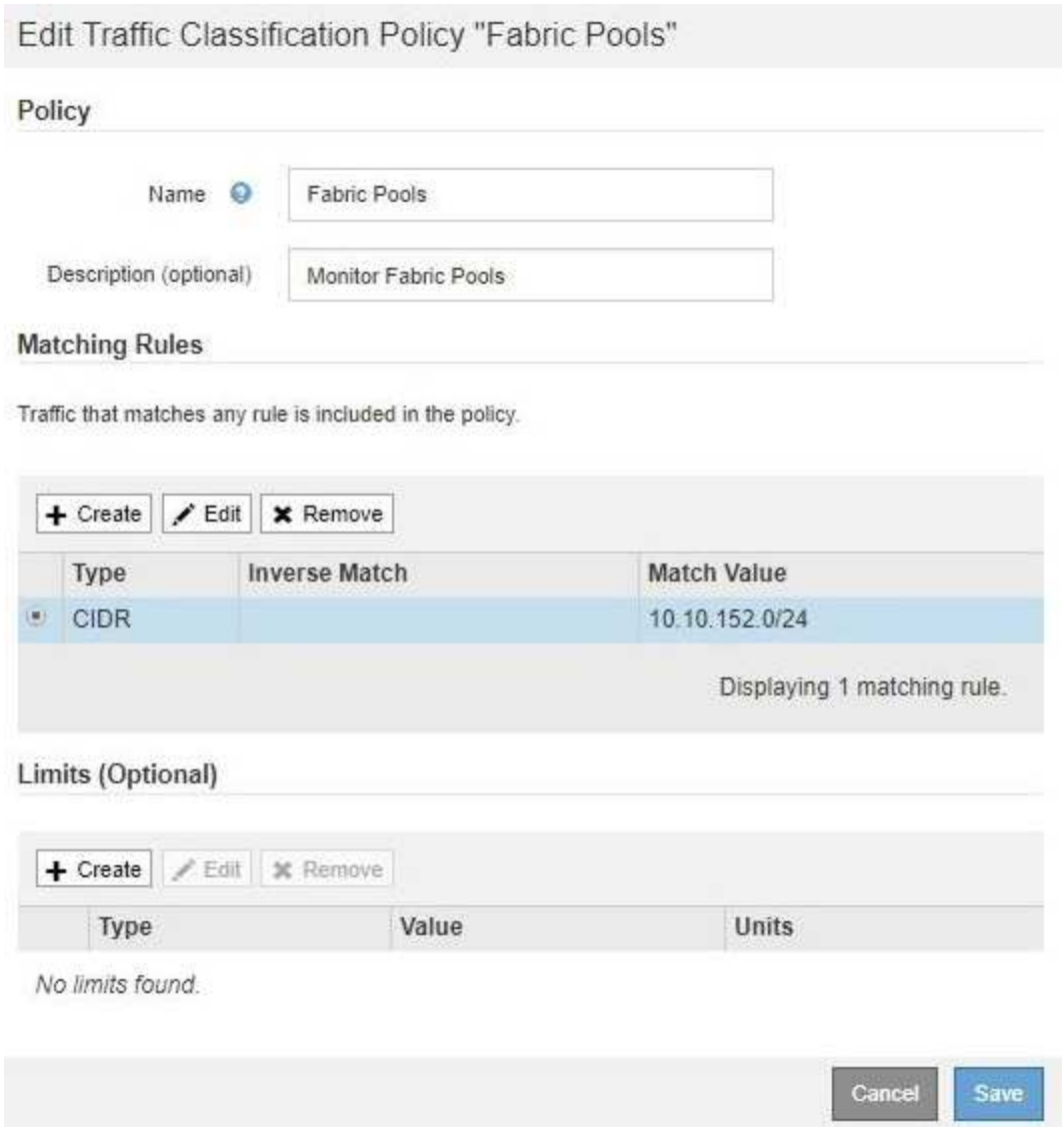
1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。



2. 編集するポリシーの左側にあるオプションボタンを選択します。
3. [編集（ Edit ）] をクリックします。

   Edit Traffic Classification Policy ダイアログボックスが表示されます。



4. 必要に応じて、一致するルールと制限を作成、編集、または削除します。
   a. 一致するルールまたは制限を作成するには、*作成*をクリックし、ルールの作成または制限の作成の手順に従います。
   b. 一致するルールまたは制限を編集するには、ルールまたは制限のラジオボタンを選択し、[一致するルール*]セクションまたは[制限]セクションで[編集]をクリックして、ルールの作成または制限の作成の手順に従います。
   c. 一致するルールまたは制限を削除するには、ルールまたは制限のラジオボタンを選択し、*削除*をクリックします。次に、[OK]をクリックして、ルールまたは制限を削除することを確認します。
5. ルールまたは制限の作成または編集が終了したら、*適用*をクリックします。
6. ポリシーの編集が完了したら、*保存*をクリックします。

   ポリシーに加えた変更が保存され、ネットワークトラフィックはトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

トラフィック分類ポリシーを削除する

トラフィック分類ポリシーが不要になった場合は、削除できます。

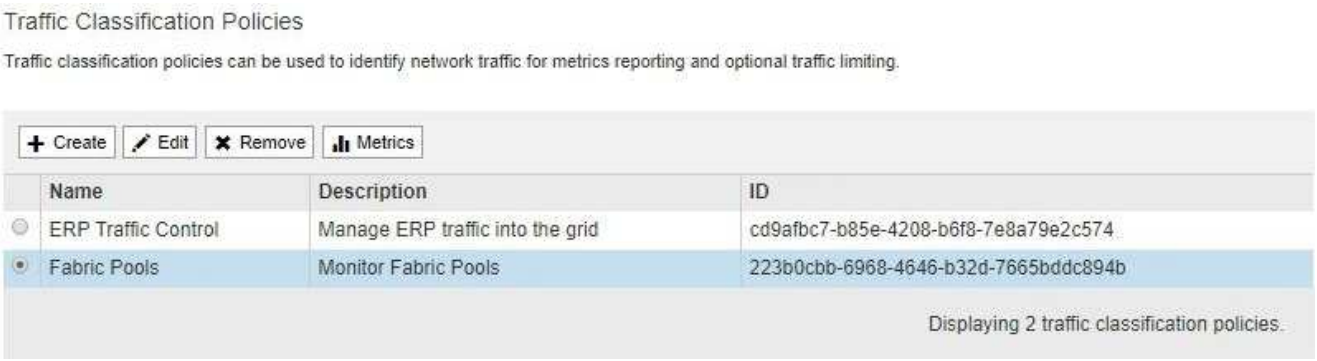
必要なもの

- 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。

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。



2. 削除するポリシーの左側にあるオプションボタンを選択します。
3. [削除（ Remove ）] をクリックします。

   警告ダイアログボックスが表示されます。

4. [OK]をクリックして、ポリシーを削除することを確認します。

   ポリシーが削除されます。

ネットワークトラフィックメトリックの表示

Traffic Classification Policies ページから使用可能なグラフを表示することで、ネットワークトラフィックを監視できます。

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

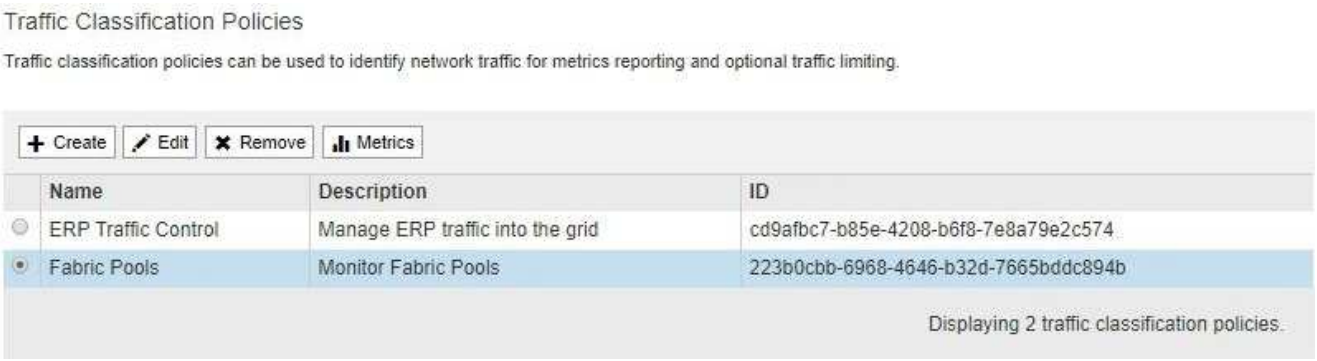
既存のトラフィック分類ポリシーでは、ロードバランササービスのメトリックを表示して、ポリシーがネットワーク全体のトラフィックを正常に制限しているかどうかを判断できます。グラフ内のデータは、ポリシーの調整が必要かどうかを判断するのに役立ちます。

トラフィック分類ポリシーに制限が設定されていない場合でも、メトリックが収集され、グラフにはトラフィックの傾向を把握するのに役立つ情報が表示されます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。



2. 指標を表示するポリシーの左側にあるラジオボタンを選択します。
3. [メトリクス]をクリックします。

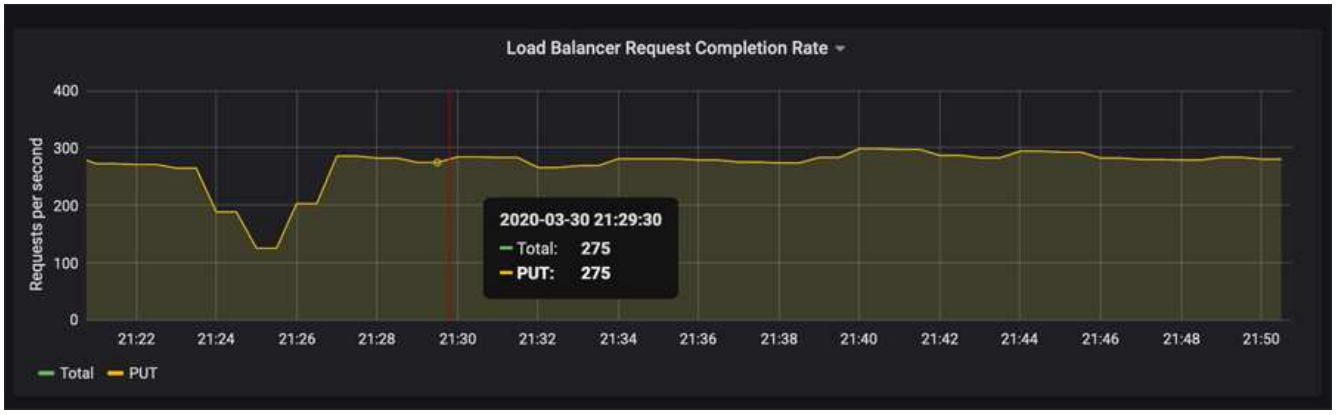
   新しいブラウザウィンドウが開き、 Traffic Classification Policy グラフが表示されます。このグラフには、選択したポリシーに一致するトラフィックのメトリックだけが表示されます。

   その他のポリシーを選択して表示するには、 * policy * プルダウンを使用します。

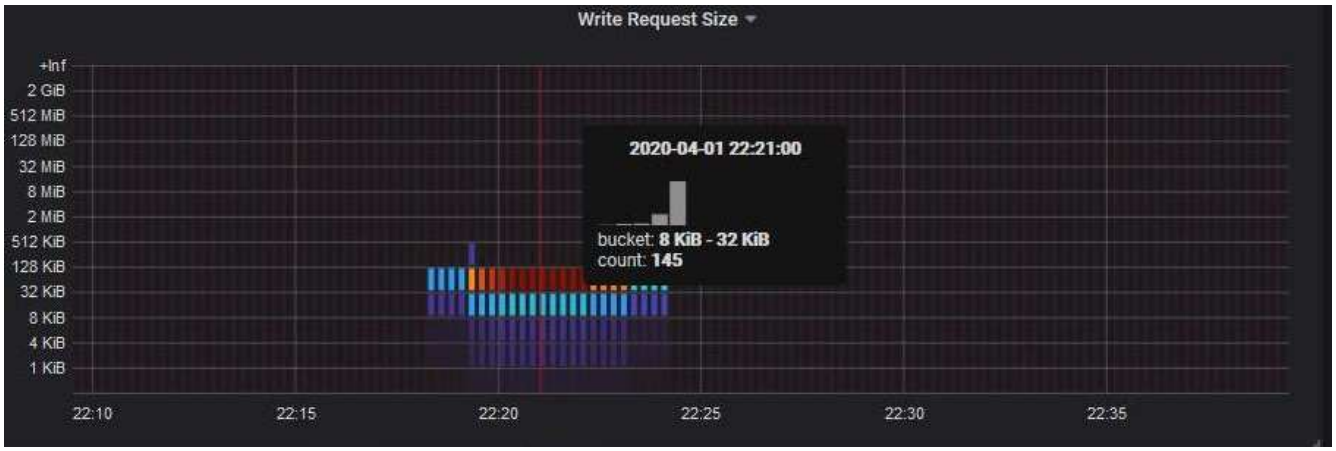
Web ページには次のグラフが表示されます。

- ロードバランサ要求トラフィック：このグラフは、ロードバランサエンドポイントと要求を送信しているクライアントの間で伝送されるデータのスループットを、 1 秒あたりのビット数で 3 分間の移動平均を提供します。
- ロードバランサの要求完了率：このグラフには、 1 秒あたりの完了済み要求数の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。この値は、新しい要求のヘッダーが検証されると更新されます。
- Error Response Rate ：このグラフには、 1 秒あたりにクライアントに返されたエラー応答数の 3 分間の移動平均が、エラー応答コード別に示されます。
- Average Request Duration （ Non-Error ）：このグラフには、要求期間の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。要求期間は、要求ヘッダーがロードバランササービスによって解析された時点から始まり、完全な応答本文がクライアントに返された時点で終了します。
- オブジェクトサイズ別の書き込み要求速度：このヒートマップは、オブジェクトサイズに基づいて書き込み要求が完了した時点での 3 分間の移動平均を提供します。この場合、書き込み要求は PUT 要求のみを参照します。
- オブジェクトサイズ別の読み取り要求速度：このヒートマップでは、オブジェクトサイズに基づいて読み取り要求が完了した時点での 3 分間の移動平均が提供されます。この場合、読み取り要求は GET 要求のみを参照します。ヒートマップの色は、個々のグラフ内のオブジェクトサイズの相対的な頻度を示します。クーラの色（紫や青など）は相対レートが低いことを示し、暖色の色（オレンジや赤など）は相対レートが高いことを示します。

4. 折れ線グラフにカーソルを合わせると、グラフの特定の部分の値がポップアップで表示されます。



5. ヒートマップにカーソルを合わせると、サンプルの日時、カウントに集約されたオブジェクトサイズ、およびその期間の 1 秒あたりのリクエスト数を示すポップアップが表示されます。



6. 左上の * Policy * プルダウンを使用して、別のポリシーを選択します。

   選択したポリシーのグラフが表示されます。

7. または、* Support *メニューからグラフにアクセスします。
   a. [* Support*]>[* Tools]>[* Metrics]を選択します。
   b. ページの * Grafana * セクションで、 * Traffic Classification Policy * を選択します。
   c. ページ左上のプルダウンからポリシーを選択します。

      トラフィック分類ポリシーは、その ID によって識別されます。ポリシー ID は、 Traffic Classification Policies ページにリストされます。

8. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要があるかどうかを判断します。

関連情報

"トラブルシューティングを監視します"

リンクコストとは

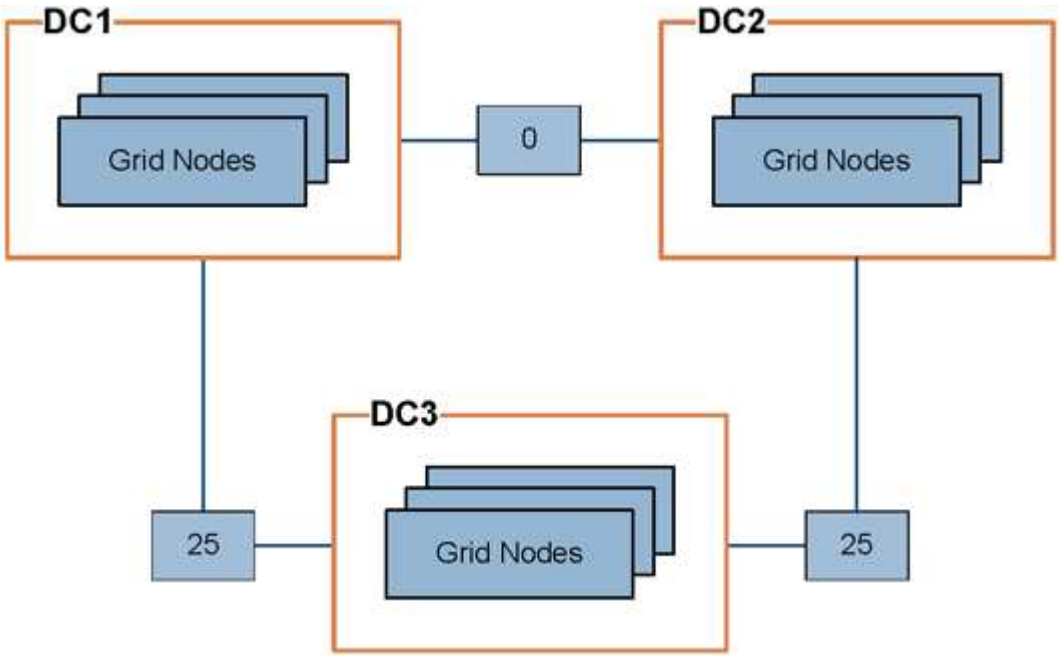
リンクコストを使用すると、複数のデータセンターサイトが存在する場合に、要求され

たサービスを提供するデータセンターサイトの優先順位を決定できます。サイト間のレイテンシに合わせてリンクコストを調整できます。

- リンクコストは、オブジェクトの読み出しにどのオブジェクトコピーを使用するかを優先的に処理するために使用されます。
- リンクコストは、グリッド管理 API およびテナント管理 API で、使用する内部 StorageGRID サービスを決定するために使用されます。
- リンクコストは、ゲートウェイノード上のCLBサービスがクライアント接続を転送するために使用します。

> CLB サービスは廃止されました。

次の図は、サイト間でリンクコストが設定されている 3 つのサイトグリッドを示しています。



- ゲートウェイノード上の CLB サービスは、同じデータセンターサイトにあるすべてのストレージノード、およびリンクコストが 0 のデータセンターサイトにクライアント接続を均等に分散します。

  この例で、データセンターサイト 1 （ DC1 ）にあるゲートウェイノードは、 DC1 にあるストレージノードと DC2 にあるストレージノードにクライアント接続を均等に分散します。DC3 にあるゲートウェイノードは、 DC3 にあるストレージノードにのみクライアント接続を送信します。

- 複数のレプリケートコピーが存在するオブジェクトを読み出す場合、 StorageGRID はリンクコストが最も低いデータセンターにあるコピーを読み出します。

  この例で、 DC2 にあるクライアントアプリケーションが DC1 と DC3 の両方に格納されているオブジェクトを読み出す場合、 DC1 から DC2 へのリンクコストは 0 で、 DC3 から DC2 へのリンクコスト（ 25 ）よりも低いため、オブジェクトは DC1 から読み出されます。

リンクコストは、測定単位を伴わない任意の相対的な数値です。たとえば、使用にあたってリンクコスト 50 の優先度はリンクコスト 25 よりも低くなります。次の表に、よく使用されるリンクコストを示します。

リンク	リンクコスト	注：
物理データセンターサイト間	25 （デフォルト）	WAN リンクで接続されたデータセンター。
同じ物理的な場所にある論理データセンターサイト間	0	同じ物理ビルディングまたはキャンパスにある論理データセンターを LAN で接続します。

関連情報

"ロードバランシングの仕組み - CLB サービス"

リンクコストを更新しています

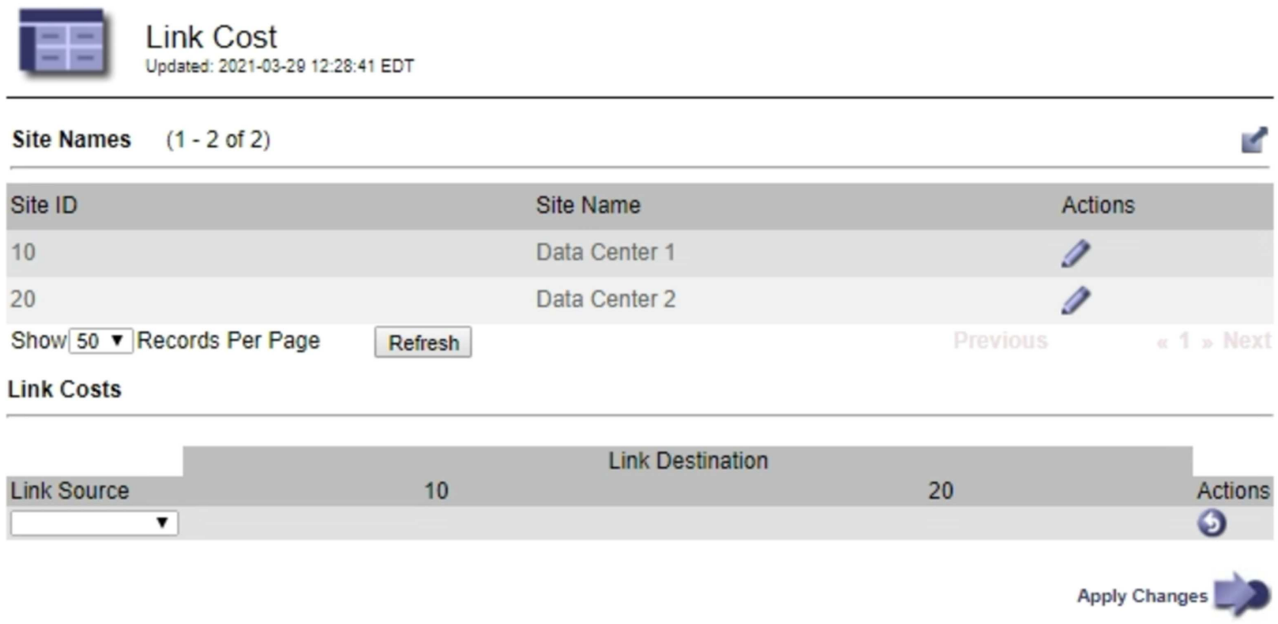
データセンターサイト間のリンクコストを更新して、サイト間のレイテンシを反映させることができます。

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。
- Grid Topology Page Configuration権限が必要です。

手順

1. [環境設定]>[ネットワーク設定]>[リンクコスト]を選択します。



2. [リンク先 *] でサイトを選択し、 [リンク先 *] に 0 ～ 100 のコスト値を入力します。

   リンク元がリンク先と同じ場合は、リンクコストを変更できません。

   変更をキャンセルするには、をクリックします * 復帰 * 。

3. [変更の適用 *] をクリックします。

著作権に関する情報

商標に関する情報