TR-4626：ロードバランサ

How to enable StorageGRID in your environment

NetApp

July 05, 2024

目次

TR-4626：ロードバランサ

StorageGRIDで他社製ロードバランサを使用する

StorageGRIDなどのオブジェクトストレージシステムにおける、サードパーティおよびグローバルロードバランサの役割について説明します。

サードパーティ製ロードバランサを使用してNetApp®StorageGRID®を実装するための一般的なガイダンス。

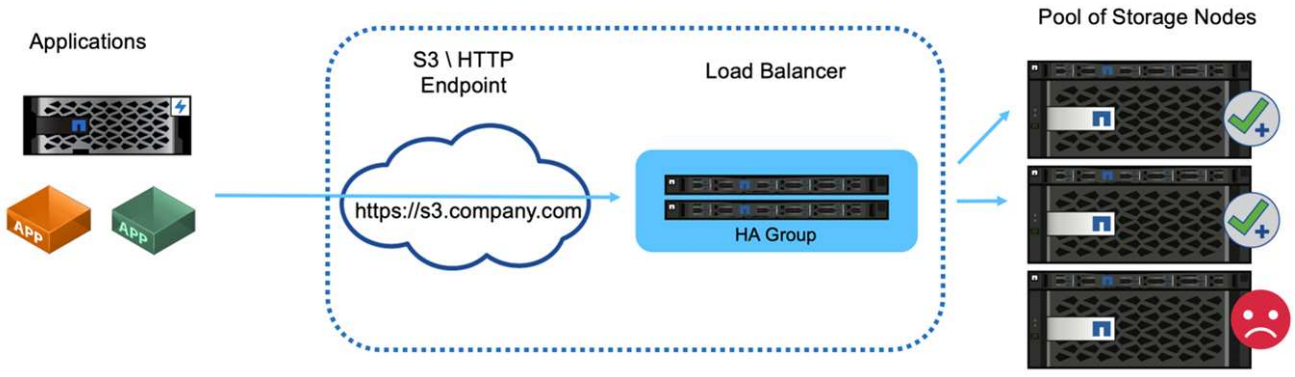
オブジェクトストレージはクラウドストレージと同義です。クラウドストレージを利用するアプリケーションは、予想どおりURLを介してストレージに対応します。StorageGRIDは、このシンプルなURLを使用して、単一サイトまたは地理的に分散したサイト全体で容量、パフォーマンス、データ保持性を拡張できます。この簡易性を実現するコンポーネントは、ロードバランサです。

このドキュメントの目的は、StorageGRIDのお客様にロードバランサのオプションについて説明し、サードパーティ製ロードバランサの設定に関する一般的なガイダンスを提供することです。

ロードバランサの基本

ロードバランサは、StorageGRIDなどのエンタープライズクラスのオブジェクトストレージシステムに欠かせないコンポーネントです。StorageGRIDは複数のストレージノードで構成され、各ストレージノードは特定のStorageGRIDインスタンスのSimple Storage Service（S3）ネームスペース全体を提供できます。ロードバランサは可用性の高いエンドポイントを作成し、その背後にStorageGRIDノードを配置します。StorageGRIDは、S3互換オブジェクトストレージシステムの中で独自のロードバランサを提供するだけでなく、F5、Citrix NetScaler、HAプロキシ、NGINXなどのサードパーティまたは汎用のロードバランサもサポートしています。

次の図では、例としてURL/完全修飾ドメイン名（FQDN）「s3.company.com”」を使用しています。ロードバランサは、DNSを介してFQDNに解決される仮想IP（VIP）を作成し、アプリケーションからの要求をすべてStorageGRIDノードのプールに転送します。ロードバランサは各ノードで健全性チェックを実行し、正常なノードへの接続のみを確立します。



次の図はStorageGRIDが提供するロードバランサを示していますが、概念はサードパーティのロードバランサでも同じです。アプリケーションはロードバランサのVIPを使用してHTTPセッションを確立し、トラフィックはロードバランサを経由してストレージノードに送信されます。デフォルトでは、アプリケーションからロードバランサ、およびロードバランサからストレージノードへのすべてのトラフィックがHTTPSを介して暗号化されます。HTTPはサポートされているオプションです。

ローカルおよびグローバルのロードバランサ

ロードバランサには次の2種類があります。

- ローカルトラフィックマネージャ（**LTM**）。単一サイト内のノードのプール全体に接続を分散します。
- グローバルサービスロードバランサ（**GSLB**）。複数のサイトに接続を分散し、LTMロードバランサを効果的にロードバランシングします。GSLBは、インテリジェントDNSサーバと考えてください。クライアントがStorageGRIDエンドポイントURLを要求すると、GSLBは可用性またはその他の要因（アプリケーションの遅延を低減できるサイトなど）に基づいて、そのURLをLTMのVIPに解決します。LTMは常に必要ですが、StorageGRIDサイトの数とアプリケーションの要件に応じて、GSLBはオプションです。

StorageGRIDゲートウェイノードロードバランサと他社製ロードバランサの比較

StorageGRIDは、S3と互換性のあるオブジェクトストレージベンダーの中で唯一、専用のアプライアンス、VM、コンテナとして使用できる標準のロードバランサを提供します。StorageGRIDが提供するロードバランサは、ゲートウェイノードとも呼ばれます。

F5やCitrixなどのロードバランサをまだ所有していないお客様の場合、サードパーティのロードバランサの実装は非常に複雑になる可能性があります。StorageGRIDロードバランサは、ロードバランサの処理を大幅に簡易化します。

ゲートウェイノードは、可用性とパフォーマンスに優れたエンタープライズクラスのロードバランサです。ゲートウェイノード、サードパーティ製ロードバランサ、またはその両方を同じグリッドに実装することもできます。ゲートウェイノードはローカルトラフィックマネージャであり、GSLBではありません。

StorageGRIDロードバランサには、次の利点があります。

- 簡易性。リソースプール、健全性チェック、パッチ適用、メンテナンスの自動構成をすべてStorageGRIDで管理
- パフォーマンス。StorageGRIDロードバランサはStorageGRID専用です。帯域幅に関して他のアプリケーションと競合することはありません。
- コスト。仮想マシン（VM）とコンテナのバージョンは追加コストなしで提供されます。
- トラフィック分類。高度なトラフィック分類機能を使用すると、StorageGRID固有のQoSルールとワークロード分析を実行できます。
- 今後の**StorageGRID**固有の機能。StorageGRIDは、今後のリリースで引き続き最適化を行い、ロードバランサに革新的な機能を追加していきます。

StorageGRIDゲートウェイノードの導入の詳細については、を参照して "StorageGRID のドキュメント"ください。

追加情報の参照先

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- NetApp StorageGRIDドキュメントセンター https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRIDイネーブルメント https://docs.netapp.com/us-en/storagegrid-enable/
- StorageGRID F5ロードバランサの設計に関する考慮事項 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/

- Loadbalancer.org—Load Balancing NetApp StorageGRID https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp：ロードバランシングNetApp StorageGRID https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

HTTPS用のSSL証明書をStorageGRIDに実装する方法

StorageGRIDにSSL証明書を実装するための重要性と手順を理解します。

HTTPSを使用する場合は、Secure Sockets Layer（SSL）証明書が必要です。SSLプロトコルはクライアントとエンドポイントを識別し、信頼できるものとして検証します。SSLは、トラフィックの暗号化も提供します。SSL証明書はクライアントから信頼されている必要があります。これを実現するには、DigiCertなどのグローバルに信頼された認証局（CA）からのSSL証明書、インフラストラクチャで実行されているプライベートCA、またはホストによって生成された自己署名証明書を使用します。

クライアント側での追加のアクションが不要なため、グローバルに信頼されたCA証明書の使用が推奨されます。証明書がロードバランサまたはStorageGRIDにロードされ、クライアントはエンドポイントを信頼して接続します。

プライベートCAを使用するには、ルート証明書とすべての下位証明書をクライアントに追加する必要があります。プライベートCA証明書を信頼するプロセスは、クライアントのオペレーティングシステムとアプリケーションによって異なります。たとえば、ONTAP for FabricPoolでは、チェーン内の各証明書（ルート証明書、下位証明書、エンドポイント証明書）をONTAPクラスタに個別にアップロードする必要があります。

自己署名証明書を使用するには、クライアントがCAなしで提供された証明書を信頼して信頼性を検証する必要があります。一部のアプリケーションでは、自己署名証明書が受け入れられず、検証を無視できない場合があります。

クライアントロードバランサのStorageGRIDパスへのSSL証明書の配置は、SSLターミネーションが必要な場所によって異なります。ロードバランサをクライアントの終端エンドポイントとして設定し、ロードバランサからStorageGRIDへの接続用の新しいSSL証明書を使用して再暗号化またはホット暗号化することができます。または、トラフィックを通過させ、StorageGRIDをSSL終端エンドポイントにすることもできます。ロードバランサがSSLターミネーションエンドポイントの場合、証明書はロードバランサにインストールされ、DNS名/URLのサブジェクト名、およびロードバランサを介してStorageGRIDターゲットに接続するようにクライアントが設定されている代替URL/DNS名が含まれています。 ワイルドカード名を含む。ロードバランサがパススルー用に設定されている場合は、StorageGRIDにSSL証明書をインストールする必要があります。証明書には、DNS名/URLのサブジェクト名と、ロードバランサを介してStorageGRIDターゲットに接続するようにクライアントが設定されている代替URL/DNS名（ワイルドカード名を含む）が含まれている必要があります。個 々 のストレージノード名を証明書に含める必要はなく、エンドポイントのURLのみを含める必要があります。

StorageGRIDでの信頼できるサードパーティ製ロードバランサの設定

StorageGRIDで信頼できるサードパーティ製ロードバランサを設定する方法について説明します。

1つ以上の外部レイヤ7ロードバランサと、IPベースのS3バケットまたはグループポリシーを使用している場合、StorageGRIDは実際の送信者のIPアドレスを特定する必要があります。これは、ロードバランサによって要求に挿入されるX-Forwarded-For（XFF）ヘッダーを調べることによって行われます。ストレージノードに直接送信された要求でXFFヘッダーが簡単にスプーフィングされる可能性があるため、StorageGRIDでは、各要求が信頼されたレイヤ7ロードバランサによってルーティングされていることを確認する必要があります。StorageGRIDがリクエストの送信元を信頼できない場合は、XFFヘッダを無視します。グリッド管理APIを使用して、信頼された外部レイヤ7ロードバランサのリストを設定できます。この新しいAPIはプライベートAPIであり、今後のStorageGRIDリリースで変更される可能性があります。最新の情報については、技術情報アーティクルを参照してください "サードパーティのレイヤ7ロードバランサと連携するようにStorageGRIDを設定する方法"。

ローカルトラフィックマネージャロードバランサの詳細

ローカルトラフィックマネージャロードバランサのガイダンスを確認し、最適な設定を決定します。

以下は、サードパーティ製ロードバランサの設定に関する一般的なガイダンスです。お使いの環境に最適な構成を決定するには、ロードバランサ管理者にお問い合わせください。

ストレージノードのリソースグループを作成

StorageGRIDストレージノードをリソースプールまたはサービスグループにグループ化します（用語は特定のロードバランサによって異なる場合があります）。StorageGRIDストレージノードは次のポートにS3 APIを提供します。

- S3 HTTPS：18082
- S3 HTTP：18084

ほとんどのお客様は、標準のHTTPSポートとHTTPポート（443および80）を使用してAPIを仮想サーバに提供することを選択しています。

> 各StorageGRIDサイトにはデフォルトで3つのストレージノードが必要で、そのうち2つは正常な状態である必要があります。

健全性チェック

サードパーティのロードバランサには、各ノードの健常性とトラフィックを受信できるかどうかを確認する方法が必要です。NetAppでは、健全性チェックの実行にHTTP方式を使用することを推奨しています `OPTIONS` 。ロードバランサは個 々 のストレージノードにHTTP要求を発行し `OPTIONS` 、ステータス応答を期待します。 `200`

応答を返さないストレージノードがあると `200` 、そのノードはストレージ要求を処理できません。アプリケ

ーションとビジネスの要件によって、これらのチェックのタイムアウトと、ロードバランサが実行するアクションを決定する必要があります。

たとえば、データセンター1の4つのストレージノードのうち3つが停止している場合は、すべてのトラフィックをデータセンター2に転送できます。

推奨されるポーリング間隔は1秒に1回で、チェックに3回失敗したあとにノードをオフラインにします。

S3の健全性チェックの例

次の例では、を送信し `OPTIONS` て確認し `200 OK`ます。`Amazon S3`が許可されていない要求をサポートしていないため、を使用して `OPTIONS` います。

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

ファイルベースまたはコンテンツベースの健全性チェック

一般に、NetAppではファイルベースの健全性チェックは推奨されません。通常、読み取り専用ポリシーが設定されたバケットには、たとえば小さなファイル —`healthcheck.htm`が作成されます。このファイルがフェッチされ、ロードバランサによって評価されます。この方法にはいくつかの欠点があります。

- * 1つのアカウントに依存します。*ファイルを所有するアカウントが無効になると、健全性チェックは失敗し、ストレージ要求は処理されません。
- *データ保護ルール。*デフォルトのデータ保護方式は2コピー方式です。このシナリオでは、健全性チェックファイルをホストしている2つのストレージノードを使用できない場合、健全性チェックは失敗し、ストレージ要求が正常なストレージノードに送信されず、グリッドがオフラインになります。
- *監査ログの肥大化。*ロードバランサは各ストレージノードからファイルをX分ごとにフェッチし、多数の監査ログエントリを作成します。
- *大量のリソースを必要とします。*健全性チェックファイルをすべてのノードから数秒おきにフェッチす

ると、グリッドリソースとネットワークリソースが消費されます。

コンテンツベースの健全性チェックが必要な場合は、専用のS3バケットで専用テナントを使用します。

セッションの永続性

セッションの持続性（スティッキ性）とは、特定のHTTPセッションの持続が許可される時間のことです。デフォルトでは、ストレージノードは10分後にセッションを破棄します。持続性が長くなると、すべてのアクションでアプリケーションがセッションを再確立する必要がなくなるため、パフォーマンスが向上しますが、セッションを開いたままにするとリソースが消費されます。ワークロードにメリットがあると判断した場合は、サードパーティのロードバランサでのセッションの永続性を減らすことができます。

仮想ホスト形式のアドレス指定

AWS S3のデフォルトの方法が仮想ホスト形式になりました。StorageGRIDや多くのアプリケーションでは引き続きパス形式がサポートされますが、仮想ホスト形式のサポートを実装することを推奨します。仮想ホスト形式の要求では、ホスト名の一部にバケットが含まれます。

仮想ホスト形式をサポートするには、次の手順を実行します。

- サポートされるワイルドカードDNSルックアップ：*.s3.company.com
- ワイルドカードをサポートするには、サブジェクトalt名を含むSSL証明書を使用してください。*.s3.company.com一部のお客様から、ワイルドカード証明書の使用に関するセキュリティ上の懸念が表明されています。StorageGRIDは、FabricPoolなどの主要なアプリケーションと同様に、パス形式のアクセスを引き続きサポートします。とはいえ、仮想ホストがサポートされていないと、一部のS3 API呼び出しが失敗したり、正常に動作しなくなったりします。

SSLターミネーション

サードパーティのロードバランサでのSSLターミネーションには、セキュリティ上の利点があります。ロードバランサが危険にさらされると、グリッドは分離されます。

サポートされる構成は次の3つです。

- * SSLパススルー*SSL証明書は、カスタムサーバ証明書としてStorageGRIDにインストールされます。
- * SSLターミネーションと再暗号化（推奨）*これは、SSL証明書をStorageGRIDにインストールするのではなく、ロードバランサでSSL証明書管理をすでに実行している場合に便利です。この構成では、攻撃対象をロードバランサに限定することで、セキュリティ上のメリットが追加されます。
- * HTTPによるSSL終了*この構成では、SSLはサードパーティのロードバランサで終端され、ロードバランサからStorageGRIDへの通信はSSLオフロードを利用するために非暗号化されます（最新のプロセッサに組み込まれたSSLライブラリを使用すると、メリットは限られています）。

パススルー構成

ロードバランサをパススルー用に設定する場合は、StorageGRIDに証明書をインストールする必要があります。メニューの[Configuration][Server Certificates]>[Object Storage API Service Endpoints Server Certificate]に移動します。

ソースクライアントのIP可視性

StorageGRID 11.4では、信頼できるサードパーティ製ロードバランサの概念が導入されました。クライアントアプリケーションIPをStorageGRIDに転送するには、この機能を設定する必要があります。詳細については、を参照してください。 "サードパーティのレイヤ7ロードバランサと連携するようにStorageGRIDを設定する方法。"

XFFヘッダーを使用してクライアントアプリケーションのIPを表示できるようにするには、次の手順を実行します。

手順

1. 監査ログにクライアントIPを記録します。
2. S3バケットまたはグループポリシーを使用する `aws:SourceIp` 。

ロードバランシング戦略

ほとんどのロードバランシングソリューションには、ロードバランシングに関する複数の戦略が用意されています。一般的な戦略は次のとおりです。

- *ラウンドロビン*ユニバーサルフィットですが、少数のノードと大規模な転送で単一のノードを詰まらせることに苦しんでいます。
- *最小接続。*すべてのノードへの接続が均等に分散される、小規模なオブジェクトワークロードや混在オブジェクトワークロードに適しています。

選択するストレージノードの数が増えるにつれて、アルゴリズムの選択はそれほど重要ではありません。

データパス

すべてのデータは、ローカルトラフィックマネージャロードバランサを経由します。StorageGRIDは、Direct Server Routing（DSR；直接サーバールーティング）をサポートしていません。

セツソクノフンサンノカクニン

負荷を複数のストレージノードに均等に分散していることを確認するには、特定のサイトの各ノードで確立されたセッションを確認します。

- * UIメソッド。*メニューの[Support][Metrics]>[S3][Overview]>[LDR HTTP Sessions]に移動します。
- *メトリクスAPI。*使用 `storagegrid_http_sessions_incoming_currently_established`

StorageGRID構成のユースケースをご紹介します

お客様とNetApp ITによって実装されたStorageGRID構成のユースケースをご紹介します。

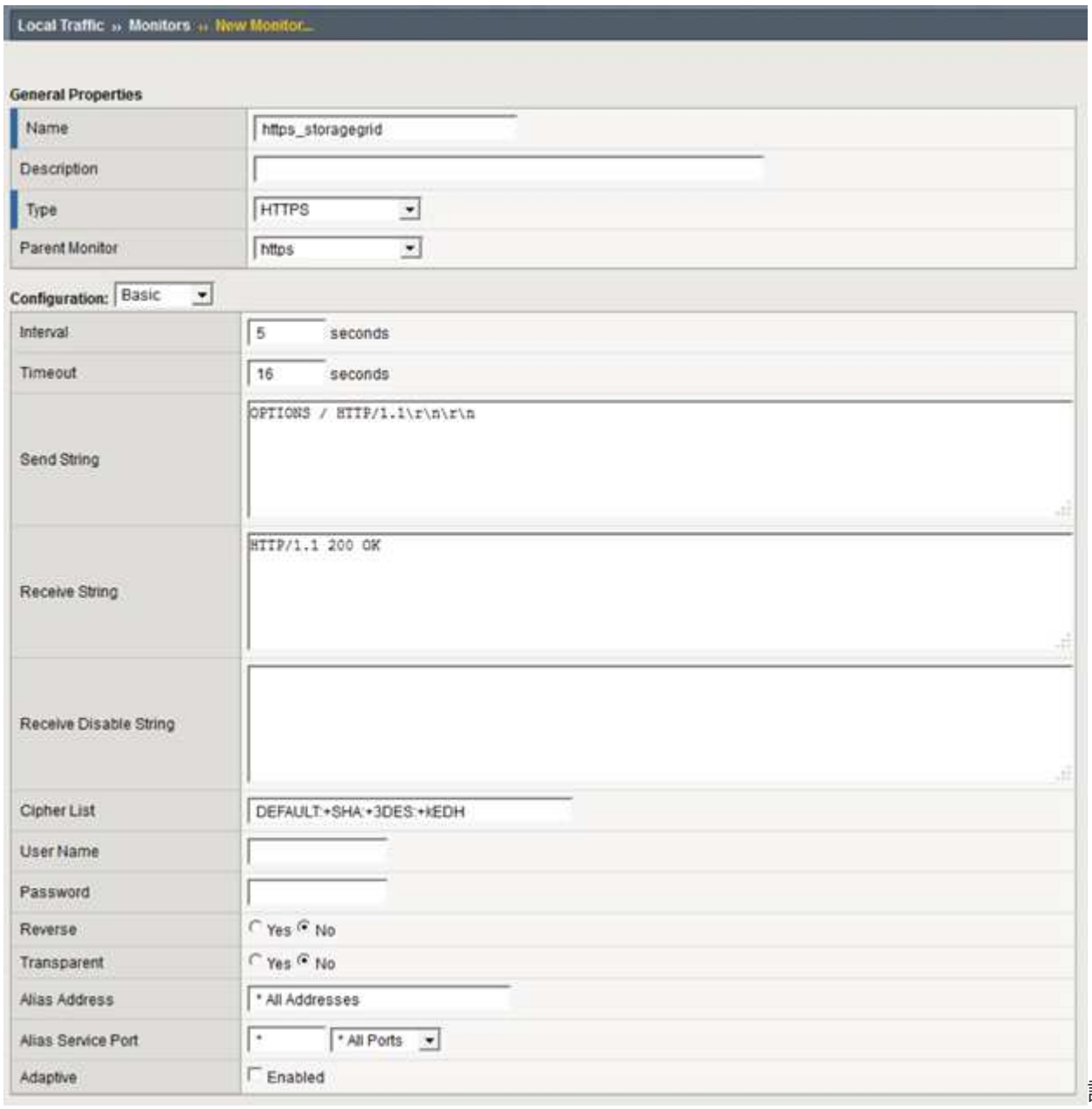
次の例は、StorageGRIDのお客様（NetApp ITを含む）が実装した構成を示しています。

S3バケット用のF5 BIG-IP Local Traffic Manager健全性チェックモニタ

F5 BIG-IPローカルトラフィックマネージャヘルスチェックモニタを設定する手順は、次のとおりです。

手順

1. 新しいモニタを作成します。
   a. [Type]フィールドにと入力します `HTTPS`。
   b. 必要に応じて、間隔とタイムアウトを設定します。
   c. Send Stringフィールドに、 `OPTIONS / HTTP/1.1\r\n\r\n`. \r\nはキャリッジリターンです。異なるバージョンのBIG-IPソフトウェアでは、0、1、または2セットの\r\nシーケンスが必要です。詳細については、を参照してください https://support.f5.com/csp/article/K10655。
   d. [Receive String]フィールドに、次のように入力します。 `HTTP/1.1 200 OK`



設定ページ"]

2. [Create Pool]で、必要なポートごとにプールを1つ作成します。
   a. 前の手順で作成したヘルスモニタを割り当てます。

b. ロードバランシング方式を選択します。

c. サービスポート18082（S3）を選択します。

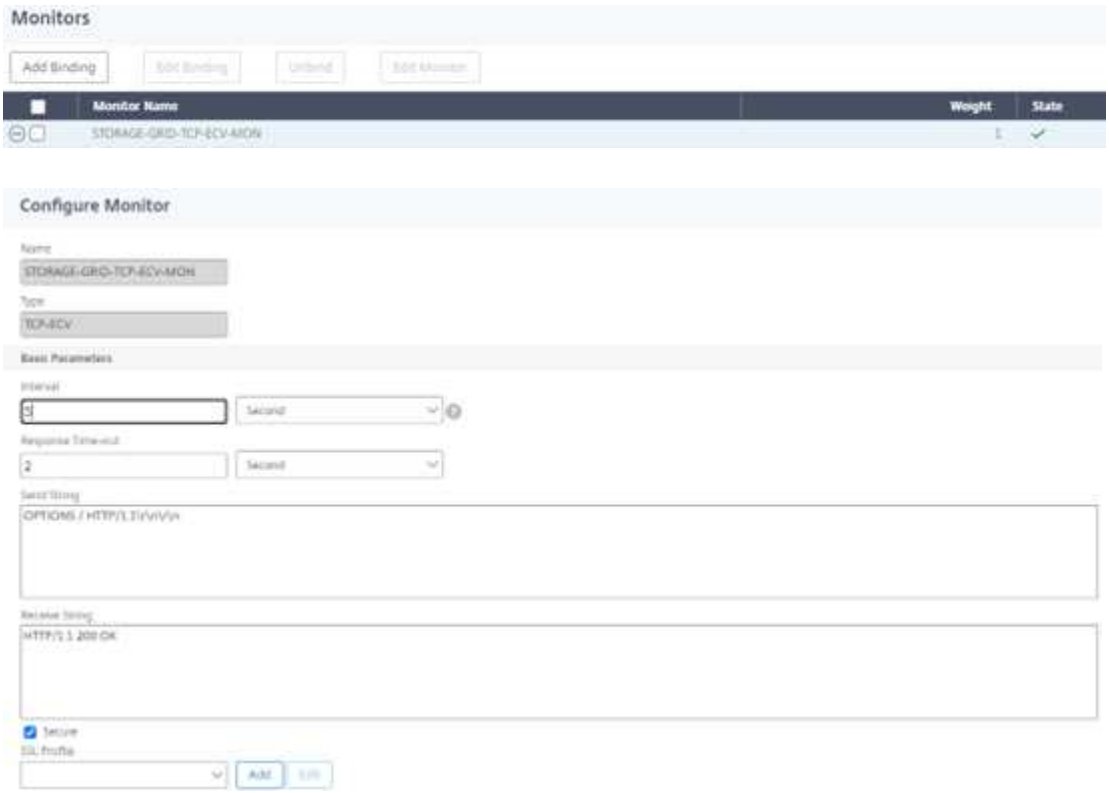
d. ノードを追加します。

Citrix NetScaler

Citrix NetScalerは、ストレージエンドポイント用の仮想サーバーを作成し、StorageGRIDストレージノードをアプリケーションサーバーとして参照してから、サービスにグループ化します。

HTTPS-ECV健全性チェックモニタを使用してカスタムモニタを作成し、OPTIONS要求と受信を使用して推奨される健全性チェックを実行し `200`ます。HTTP-ECVは送信文字列を使用して設定され、受信文字列を検証します。

詳細については、Citrixのドキュメントを参照してください "HTTP-ECVヘルスチェックモニタの設定例"。



Loadbalancer.org

Loadbalancer.orgは、独自のStorageGRIDとの統合テストを実施し、広範な構成ガイドを用意しています。
https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf

ケンプ

KempはStorageGRIDとの統合テストを独自に実施し、広範な構成ガイドを用意しています。
https://kemptechnologies.com/solutions/netapp/

HAProxy

OPTIONS要求を使用するようにHAProxyを設定し、haproxy.cfgでヘルスチェックの200ステータス応答を確認します。フロントエンドのバインドポートを別のポート（443など）に変更できます。

次に、HAProxyでのSSL終端の例を示します。

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

次に、SSLパススルーの例を示します。

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

StorageGRIDの設定の完全な例については、GitHubのを参照してください "HAProxy設定の例" 。

StorageGRIDでのSSL接続の検証

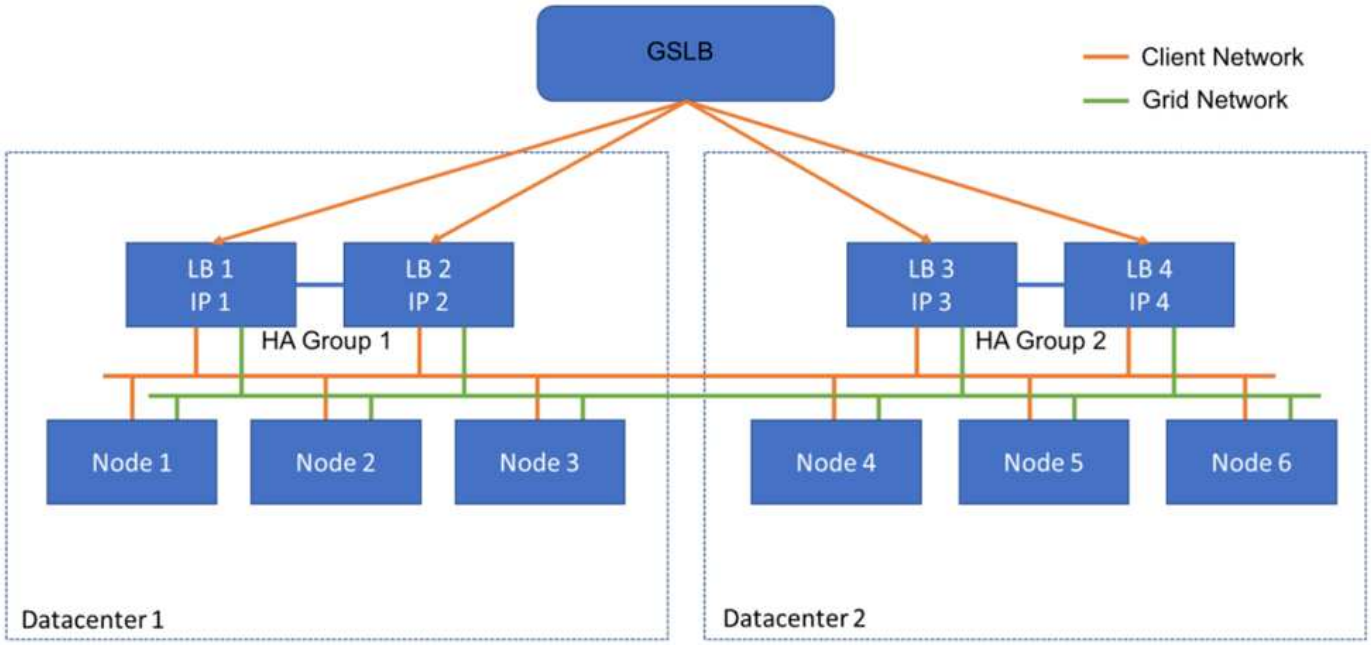
StorageGRIDでSSL接続を検証する方法について説明します。

ロードバランサを設定したら、OpenSSLやAWS CLIなどのツールを使用して接続を検証する必要があります。S3 Browserなどの他のアプリケーションでは、SSLの設定ミスが無視される可能性があります。

StorageGRIDのグローバルロードバランシング要件を理解する

StorageGRIDでのグローバルロードバランシングの設計上の考慮事項と要件を確認します。

グローバルなロードバランシングでは、複数のStorageGRIDサイトにインテリジェントなルーティングを提供するために、DNSと統合する必要があります。この機能はStorageGRIDドメインの外部にあり、前述のロードバランサ製品などのサードパーティのソリューションや、InfobloxなどのDNSトラフィック制御ソリューションによって提供される必要があります。このトップレベルのロードバランシングは、ネームスペース内の最も近い宛先サイトへのスマートルーティング、および停止の検出とネームスペース内の次のサイトへのリダイレクションを提供します。一般的なGSLBの実装は、サイトローカルのロードバランサを含むサイトプールを含むトップレベルのGSLBで構成されます。サイトロードバランサには、ローカルサイトのストレージノードのプールが含まれています。これには、GSLB機能用のサードパーティ製ロードバランサとサイトローカルロードバランシングを提供するStorageGRIDの組み合わせ、またはサードパーティの組み合わせが含まれます。または、前述したサードパーティの多くが、GSLBとサイトローカルロードバランシングの両方を提供できます。



著作権に関する情報

商標に関する情報