



負荷分散の管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

負荷分散の管理	1
ロードバランシングの仕組み - ロードバランササービス	1
ロードバランサエンドポイントの設定	2
ロードバランシングの仕組み - CLB サービス	10

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。

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

Changes to endpoints can take up to 15 minutes to be applied to all nodes.

[+ Add endpoint port](#) [Edit endpoint](#) [Remove endpoint port](#)

Display name	Port	Using HTTPS
--------------	------	-------------

No endpoints configured.

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。

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Cancel

Save

- 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。
- 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。

- 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。
- 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。

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

i This endpoint is currently bound globally. All nodes will use this endpoint unless an endpoint with an overriding binding mode exists for a specific port.

Cancel Save

- * 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。

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Name	Description	Virtual IP Addresses	Interfaces
<input type="checkbox"/> Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
<input type="checkbox"/> Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

Displaying 2 HA groups.

⚠ No HA groups selected. You must select one or more HA Groups; otherwise, this endpoint will act as a globally bound endpoint.

Cancel Save

- 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。

Create Endpoint


Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Node	Interface
<input type="checkbox"/> CO-REF-DC1-ADM1	eth0
<input type="checkbox"/> CO-REF-DC1-ADM1	eth1
<input type="checkbox"/> CO-REF-DC1-ADM1	eth2
<input type="checkbox"/> CO-REF-DC1-GW1	eth0
<input type="checkbox"/> CO-REF-DC2-ADM1	eth0
<input type="checkbox"/> CO-REF-DC2-GW1	eth0

 No node interfaces selected. You must select one or more node interfaces; otherwise, this endpoint will act as a globally bound endpoint.

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。

Edit Endpoint Unsecured Port A (port 10449)

Endpoint Service Configuration

Endpoint service type S3 Swift

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。

Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate

Certificate Private Key

CA Bundle

Cancel

Save

- 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。

Generate Certificate

Domain 1 +

IP 1 +

Subject

Days valid

Cancel

Generate

- 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*

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。

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

- 編集するエンドポイントを選択します。
- *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。

Endpoint Service Configuration

Endpoint service type S3 Swift

Certificates

Upload Certificate

Generate Certificate

Server CA

Certificate metadata

```
Subject DN: /C=CA/ST=British Columbia/O=NetApp, Inc./OU=SGQA/CN=*.mraymond-grid-a.sgqa.eng.netapp.com
Serial Number: 1C:FD:27:8B:E6:A5:BA:30:45:A9:16:4F:DC:77:3E:C6:80:7D:AF:E9
Issuer DN: /C=CA/ST=British Columbia/O=EqualSign, Inc./OU=IT/CN=EqualSign Issuing CA
Issued On: 2000-01-01T00:00:00.000Z
Expires On: 3000-01-01T00:00:00.000Z
SHA-1 Fingerprint: 60:3D:5A:8C:62:C5:B8:49:DC:9A:B3:F7:B9:0B:5B:0E:D2:A2:7E:C7
SHA-256 Fingerprint: AF:75:7F:44:C6:86:A4:84:B2:7D:11:DE:9F:49:D3:F6:2A:7E:D9:4D:2A:1B:8A:0B:B3:7E:23:0F:B3:CB:84:8
9
Alternative Names: DNS:*.mraymond-grid-a.sgqa.eng.netapp.com
DNS:*.99-140-dc1-g1.mraymond-grid-a.sgqa.eng.netapp.com
DNS:*.99-142-dc1-s1.mraymond-grid-a.sgqa.eng.netapp.com
```

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIIEFDCCBWSgAwIBAgIUHP0ni+alujBFgRZP3Hc+xoB9r+kwDQYJKoZIhvcNAQEL
BQAwbjELMAkGA1UEBhMCQ0ExGTAXBgNVBAGMEEJyaXRpc2ggQ29sdWliaWExGDAW
BgNVBAoMD0VxdWFeU2lnbiwgSW5jLjELMAkGA1UECwwCSVQxHTAbBgNVBAMFEVx
dWFeU2lnbiBjc3N1aW5nIENBMCAXDTEwMDEwMDAwMDAwMDEwMDAwMDAwMDAw
MDAwWjB+MQswCQYDVQQGEwJDTEZMBcGAlUECAwQnJpdG1zaCBDb2x1bWpYTEV
MEMGA1UECgwMTmV0QXBwLmV0QXBwLmV0QXBwLmV0QXBwLmV0QXBwLmV0QXBw
Lm1yYX10b25kLWdyYWQtYS5zZ3FhLmV0Zy5uZXRhcHAuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEaonUkwkFg/B1U1Y+bIR80MaVJSC+R7Sfz102v
Hz4rSnrYCh/WJRCT+fznmxzaGs2RRUDinNlnX1Yk+QUPAdIFZ+Sldr6HirYTF/NK
-----
```

- 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。

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

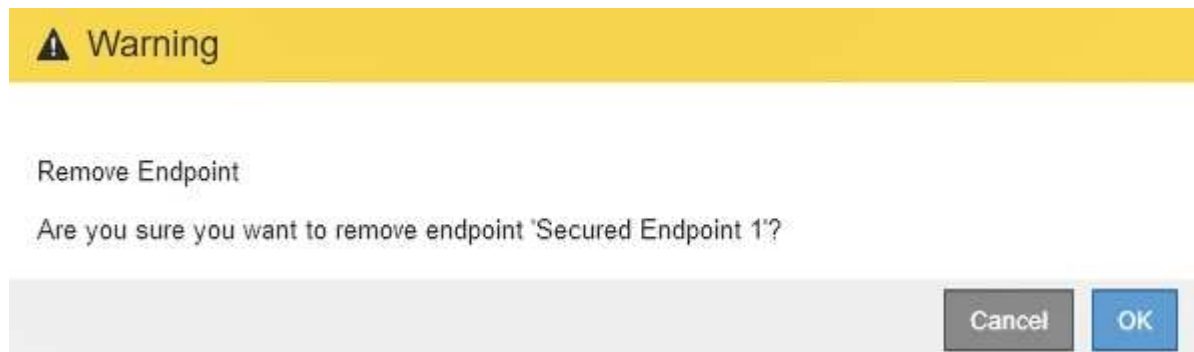
<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

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。

The screenshot shows the StorageGRID Webconsole interface. On the left, the "Grid Topology" tree is visible, with "DC1-G1-98-161" selected and highlighted with a blue box. The main content area shows the "Overview" tab for "DC1-G1-98-161", updated on 2015-10-27 16:23:33 PDT. Below this, there is a "Storage Capacity" section with a table of metrics.

Storage Capacity	
Storage Nodes Installed:	N/A
Storage Nodes Readable:	N/A
Storage Nodes Writable:	N/A
Installed Storage Capacity:	N/A
Used Storage Capacity:	N/A
Used Storage Capacity for Data:	N/A
Used Storage Capacity for Metadata:	N/A
Usable Storage Capacity:	N/A

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せん"

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。