



로드 밸런싱 관리 StorageGRID

NetApp
April 10, 2024

목차

로드 밸런싱 관리	1
부하 분산 관리: 개요	1
로드 밸런싱 작동 방식 - 로드 밸런서 서비스	1
로드 밸런서 엔드포인트를 구성합니다	2
로드 밸런싱 작동 방식 - CLB 서비스(더 이상 사용되지 않음)	10

로드 밸런싱 관리

부하 분산 관리: 개요

StorageGRID 로드 밸런싱 기능을 사용하여 S3 및 Swift 클라이언트에서 수집 및 검색 워크로드를 처리할 수 있습니다. 로드 밸런싱은 여러 스토리지 노드에 워크로드와 연결을 분산하여 속도와 연결 용량을 극대화합니다.

다음과 같은 방법으로 클라이언트 워크로드의 로드 밸런싱을 수행할 수 있습니다.

- 관리 노드 및 게이트웨이 노드에 설치된 로드 밸런서 서비스를 사용합니다. 로드 밸런서 서비스는 계층 7 로드 밸런싱을 제공하고 클라이언트 요청에 대한 TLS 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다. 이것은 권장되는 로드 밸런싱 메커니즘입니다.

을 참조하십시오 [로드 밸런싱 작동 방식 - 로드 밸런서 서비스](#).

- 게이트웨이 노드에만 설치된 더 이상 사용되지 않는 CLB(연결 로드 밸런서) 서비스를 사용합니다. CLB 서비스는 계층 4 로드 밸런싱을 제공하고 링크 비용을 지원합니다.

을 참조하십시오 [로드 밸런싱 작동 방식 - CLB 서비스\(더 이상 사용되지 않음\)](#).

- 타사 로드 밸런서를 통합합니다. 자세한 내용은 NetApp 어카운트 담당자에게 문의하십시오.

로드 밸런싱 작동 방식 - 로드 밸런서 서비스

로드 밸런서 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 배포합니다. 로드 밸런싱을 사용하려면 Grid Manager를 사용하여 부하 분산 엔드포인트를 구성해야 합니다.

이러한 노드 유형에는 로드 밸런서 서비스가 포함되어 있으므로 관리 노드 또는 게이트웨이 노드에 대해서만 로드 밸런서 끝점을 구성할 수 있습니다. 스토리지 노드 또는 아카이브 노드의 끝점은 구성할 수 없습니다.

각 로드 밸런서 끝점은 포트, 네트워크 프로토콜(HTTP 또는 HTTPS), 클라이언트 유형(S3 또는 Swift) 및 바인딩 모드를 지정합니다. HTTPS 엔드포인트에는 서버 인증서가 필요합니다. 바인딩 모드를 사용하면 엔드포인트 포트의 액세스를 다음과 같이 제한할 수 있습니다.

- 특정 HA(고가용성) 그룹의 가상 IP 주소(VIP)
- 특정 관리 및 게이트웨이 노드의 특정 네트워크 인터페이스

포트 고려 사항

클라이언트는 로드 밸런서 서비스를 실행하는 노드에서 구성한 모든 끝점에 액세스할 수 있습니다. 단, 포트 80과 443은 관리 노드에 예약되므로 이러한 포트에 구성된 끝점은 게이트웨이 노드에서만 로드 밸런싱 작업을 지원합니다.

포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 의 단계를 따릅니다 [포트 재매핑 제거합니다](#).



CLB 서비스는 더 이상 사용되지 않습니다.

CPU 가용성

각 관리 노드와 게이트웨이 노드의 로드 밸런서 서비스는 S3 또는 Swift 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 가용성이 높은 스토리지 노드로 라우팅합니다. 노드 CPU 로드 정보는 몇 분마다 업데이트되지만 가중치는 더 자주 업데이트될 수 있습니다. 모든 스토리지 노드에는 최소 기본 가중치 값이 할당됩니다. 이는 노드에서 100% 사용률을 보고하거나 사용률을 보고하지 않는 경우에도 마찬가지입니다.

경우에 따라 CPU 가용성에 대한 정보는 로드 밸런서 서비스가 있는 사이트로 제한됩니다.

로드 밸런서 엔드포인트를 구성합니다

로드 밸런서 끝점은 게이트웨이 및 관리 노드의 StorageGRID 로드 밸런서에 연결할 때 사용할 수 있는 포트 및 네트워크 프로토콜 S3 및 Swift 클라이언트를 결정합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 [지원되는 웹 브라우저](#).
- 루트 액세스 권한이 있습니다.
- 로드 밸런서 끝점에 사용할 포트를 이전에 다시 매핑한 경우 [포트 재매핑을 제거했습니다](#).
- 사용할 고가용성(HA) 그룹을 만들었습니다. HA 그룹이 권장되지만 필수는 아닙니다. 을 참조하십시오 [고가용성 그룹을 관리합니다](#).
- 에서 로드 밸런서 끝점을 사용하는 경우 [S3 테넌트를 선택합니다](#), Bare-Metal 노드의 IP 주소 또는 FQDN을 사용해서는 안 됩니다. S3 Select에 사용되는 로드 밸런싱 장치 엔드포인트에는 SG100 또는 SG1000 어플라이언스 및 VMware 기반 소프트웨어 노드만 허용됩니다.
- 사용할 VLAN 인터페이스를 구성했습니다. 을 참조하십시오 [VLAN 인터페이스를 구성합니다](#).
- HTTPS 끝점을 만드는 경우(권장) 서버 인증서에 대한 정보가 있습니다.



끝점 인증서 변경 내용을 모든 노드에 적용하는 데 최대 15분이 걸릴 수 있습니다.

- 인증서를 업로드하려면 서버 인증서, 인증서 개인 키 및 선택적으로 CA 번들이 필요합니다.
- 인증서를 생성하려면 S3 또는 Swift 클라이언트가 끝점에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소가 필요합니다. 제목(고유 이름)도 알아야 합니다.
- StorageGRID S3 및 Swift API 인증서(스토리지 노드에 직접 연결하는 데에도 사용 가능)를 사용하려면 이미 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체했습니다. 을 참조하십시오 [S3 및 Swift API 인증서를 구성합니다](#).

이 인증서는 와일드카드를 사용하여 로드 밸런서 서비스를 실행하는 모든 관리 노드 및 게이트웨이 노드의 정규화된 도메인 이름을 나타낼 수 있습니다. 예를 들어, '* .storagegrid.example.com'은 'adm1.storagegrid.example.com' 및 'gn1.storagegrid.example.com'을 나타내는 * 와일드카드를 사용합니다. 을 참조하십시오 [S3 API 엔드포인트 도메인 이름을 구성합니다](#).

로드 밸런서 끝점을 만듭니다

각 로드 밸런서 끝점은 포트, 클라이언트 유형(S3 또는 Swift) 및 네트워크 프로토콜(HTTP 또는 HTTPS)을 지정합니다.

마법사에 액세스합니다

1. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.
2. Create * 를 선택합니다.

끝점 세부 정보를 입력합니다

1. 끝점의 세부 정보를 입력합니다.

Create a load balancer endpoint

1 Enter endpoint details

2 Select binding mode

3 Attach certificate

Endpoint details

Name

Port

Enter an unused port or accept the suggested port.

Client type

Select the type of client application that will use this endpoint.

☒ S3 ☐ Swift

Network protocol

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

☐ HTTPS (recommended) ☒ HTTP

Cancel

Continue

필드에 입력합니다	설명
이름	Load Balancer Endpoints(분산 장치 끝점 로드) 페이지의 테이블에 표시되는 끝점에 대한 설명 이름입니다.

필드에 입력합니다	설명
포트	<p>포트 클라이언트는 를 사용하여 관리 노드 및 게이트웨이 노드의 로드 밸런서 서비스에 연결합니다.</p> <p>제안된 포트 번호를 수락하거나 다른 그리드 서비스에서 사용되지 않는 외부 포트를 입력합니다. 1에서 65535 사이의 값을 입력합니다.</p> <p>80 * 또는 * 443 * 을 입력하면 끝점이 게이트웨이 노드에서만 구성됩니다. 이러한 포트는 관리 노드에 예약되어 있습니다.</p> <p>를 참조하십시오 네트워킹 지침 외부 포트에 대한 자세한 내용은 를 참조하십시오.</p>
클라이언트 유형입니다	이 끝점을 사용할 클라이언트 응용 프로그램 유형, * S3 * 또는 * Swift *.
네트워크 프로토콜	<p>클라이언트가 이 끝점에 연결할 때 사용할 네트워크 프로토콜입니다.</p> <ul style="list-style-type: none"> • TLS 암호화 보안 통신을 위해 * HTTPS * 를 선택합니다(권장). 끝점을 저장하려면 먼저 보안 인증서를 연결해야 합니다. • 보안이 취약한 암호화되지 않은 통신을 위해 * HTTP * 를 선택합니다. 비 프로덕션 그리드에만 HTTP를 사용합니다.

2. Continue * 를 선택합니다.

바인딩 모드를 선택합니다

1. 끝점에 대한 바인딩 모드를 선택하여 끝점에 액세스하는 방법을 제어합니다.

옵션을 선택합니다	설명
글로벌(기본값)	<p>클라이언트는 FQDN(정규화된 도메인 이름), 게이트웨이 노드 또는 관리 노드의 IP 주소 또는 네트워크에 있는 HA 그룹의 가상 IP 주소를 사용하여 끝점에 액세스할 수 있습니다.</p> <p>이 끝점의 접근성을 제한할 필요가 없는 경우 * Global * (글로벌 *) 설정(기본값)을 사용합니다.</p>
노드 인터페이스	클라이언트는 선택한 노드와 네트워크 인터페이스의 IP 주소를 사용하여 이 끝점에 액세스해야 합니다.
HA 그룹의 가상 IP입니다	<p>클라이언트는 이 끝점에 액세스하기 위해 HA 그룹의 가상 IP 주소를 사용해야 합니다.</p> <p>이 바인딩 모드의 엔드포인트는 엔드포인트에 대해 선택한 HA 그룹이 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.</p> <p>이 모드를 사용하는 끝점은 끝점에 대해 선택한 인터페이스가 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.</p>



두 개 이상의 끝점에 대해 동일한 포트를 사용하는 경우 * HA 그룹의 가상 IP * 모드를 사용하는 끝점은 * 글로벌 * 모드를 사용하여 끝점을 재정의하는 * 노드 인터페이스 * 모드를 사용하는 끝점에 우선합니다.

2. 노드 인터페이스 * 를 선택한 경우 이 끝점과 연결할 각 관리 노드 또는 게이트웨이 노드에 대해 하나 이상의 노드 인터페이스를 선택합니다.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☒ Node interfaces ☐ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Total interface count: 3

<input type="checkbox"/>	Node	Node interface ?	Site ?	IP address ?	Node type ?
<input type="checkbox"/>	DC1-ADM1	eth0 ?	Data Center 1	172.16.3.246 and 2 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth1 ?	Data Center 1	10.224.3.246 and 5 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth2 ?	Data Center 1	47.47.3.246 and 3 more	Primary Admin Node

3. HA 그룹의 가상 IP * 를 선택한 경우 하나 이상의 HA 그룹을 선택합니다.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☐ Node interfaces ☒ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search...				Total interface count: 2
<input type="checkbox"/>	Name ?	Description ?	Virtual IP address ?	Interfaces (in priority order) ?
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

4. HTTP* 끝점을 만드는 경우에는 인증서를 첨부할 필요가 없습니다. 새 로드 밸런서 끝점을 추가하려면 * Create * 를 선택합니다. 그런 다음 로 이동합니다 [작업을 마친 후](#). 그렇지 않으면 * 계속 * 을 선택하여 인증서를 첨부하십시오.

인증서를 첨부합니다

1. HTTPS* 끝점을 만드는 경우 끝점에 연결할 보안 인증서 유형을 선택합니다.

인증서는 S3 및 Swift 클라이언트와 관리 노드 또는 게이트웨이 노드의 로드 밸런서 서비스 간의 연결을 보호합니다.

- * 인증서 업로드 *. 업로드할 사용자 지정 인증서가 있는 경우 이 옵션을 선택합니다.
- * 인증서 생성 *. 사용자 지정 인증서를 생성하는 데 필요한 값이 있는 경우 이 옵션을 선택합니다.
- * StorageGRID S3 및 Swift 인증서 사용 *. 글로벌 S3 및 Swift API 인증서를 사용하려면 이 옵션을 선택합니다. 스토리지 노드에 직접 연결하는 데에도 이 인증서를 사용할 수 있습니다.

GRID CA에서 서명한 기본 S3 및 Swift API 인증서를 외부 인증 기관이 서명한 사용자 지정 인증서로 대체하지 않으면 이 옵션을 선택할 수 없습니다. [을 참조하십시오 S3 및 Swift API 인증서를 구성합니다](#).

2. StorageGRID S3 및 Swift 인증서를 사용하지 않는 경우 인증서를 업로드하거나 생성합니다.

인증서를 업로드합니다

- a. 인증서 업로드 * 를 선택합니다.
- b. 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: PEM 인코딩의 사용자 정의 서버 인증서 파일.
 - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일('.key')입니다.



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.
- c. 업로드한 각 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 확장합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.
 - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택하고 인증서 번들을 저장하려면 * CA 번들 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

예를 들어, 'toragegrid_certificate.pem'

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 또는 * CA 번들 PEM * 복사 를 선택합니다.
- d. Create * 를 선택합니다. + 로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 및 Swift 클라이언트와 끝점 간의 이후의 모든 새 연결에 사용됩니다.

인증서를 생성합니다

- a. 인증서 생성 * 을 선택합니다.
- b. 인증서 정보를 지정합니다.
 - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
 - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
 - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
 - * 일 유효 *: 인증서 만료 후 일 수입니다.
- c. Generate * 를 선택합니다.
- d. 생성된 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 선택합니다.

- 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

예를 들어, 'toragegrid_certificate.pem'

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

e. Create * 를 선택합니다.

로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 및 Swift 클라이언트와 이 엔드포인트 간의 이후의 모든 새 연결에 사용됩니다.

를 클릭합니다

1. DNS(도메인 이름 시스템)를 사용하는 경우 DNS에 StorageGRID 정규화된 도메인 이름을 클라이언트가 연결하는 데 사용할 각 IP 주소에 연결하는 레코드가 포함되어 있는지 확인합니다.

DNS 레코드에 입력하는 IP 주소는 로드 밸런싱 노드의 HA 그룹을 사용하는지 여부에 따라 달라집니다.

- HA 그룹을 구성한 경우 클라이언트는 해당 HA 그룹의 가상 IP 주소에 연결됩니다.
- HA 그룹을 사용하지 않는 경우 클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소를 사용하여 StorageGRID 로드 밸런서 서비스에 연결됩니다.

또한 DNS 레코드가 와일드카드 이름을 포함하여 필요한 모든 끝점 도메인 이름을 참조하는지 확인해야 합니다.

2. S3 및 Swift 클라이언트에 엔드포인트에 연결하는 데 필요한 정보 제공:

- 포트 번호입니다
- 정규화된 도메인 이름 또는 IP 주소입니다
- 필요한 인증서 세부 정보입니다

로드 밸런서 끝점을 보고 편집합니다

보안 끝점의 인증서 메타데이터를 포함하여 기존 로드 밸런서 끝점에 대한 세부 정보를 볼 수 있습니다. 또한 끝점의 이름 또는 바인딩 모드를 변경하고 연결된 인증서를 업데이트할 수 있습니다.

서비스 유형(S3 또는 Swift), 포트 또는 프로토콜(HTTP 또는 HTTPS)은 변경할 수 없습니다.

- 모든 로드 밸런서 끝점에 대한 기본 정보를 보려면 부하 분산 장치 끝점 페이지의 표를 검토하십시오.

Create Actions Search...						Total endpoints count: 1
<input type="checkbox"/>	Name ?	Port ?	Network protocol ?	Binding mode ?	Certificate expiration ?	
<input type="checkbox"/>	FabricPool endpoint	10443	HTTPS	Global	Oct 19th, 2022	

- 인증서 메타데이터를 포함하여 특정 끝점에 대한 모든 세부 정보를 보려면 테이블에서 끝점 이름을 선택합니다.

FabricPool endpoint

Port: 10443

Client type: S3

Network protocol: HTTPS

Binding mode: Global

Endpoint ID: c2b6feb3-c567-449d-b717-4fed98c4a411

Remove


Binding Mode

Certificate

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode


Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- 끝점을 편집하려면 부하 분산 끝점 페이지의 * 작업 * 메뉴 또는 특정 끝점의 세부 정보 페이지를 사용합니다.



끝점을 편집한 후 변경 내용이 모든 노드에 적용될 때까지 최대 15분 정도 기다려야 할 수 있습니다.

작업	작업 메뉴	세부 정보 페이지
끝점 이름을 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 이름 편집 * 을 선택합니다. c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 편집 아이콘을 선택합니다  . c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다.
끝점 바인딩 모드를 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다.

작업	작업 메뉴	세부 정보 페이지
끝점 인증서를 편집합니다	<ul style="list-style-type: none"> a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 인증서 편집 * 을 선택합니다. c. 필요에 따라 새 사용자 지정 인증서를 업로드하거나 생성하거나 글로벌 S3 및 Swift 인증서를 사용하기 시작합니다. d. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. Certificate * 탭을 선택합니다. c. 인증서 편집 * 을 선택합니다. d. 필요에 따라 새 사용자 지정 인증서를 업로드하거나 생성하거나 글로벌 S3 및 Swift 인증서를 사용하기 시작합니다. e. 변경 내용 저장 * 을 선택합니다.

로드 밸런서 끝점을 제거합니다

Actions * 메뉴를 사용하여 하나 이상의 끝점을 제거하거나 세부 정보 페이지에서 단일 끝점을 제거할 수 있습니다.



클라이언트 중단을 방지하려면 로드 밸런서 엔드포인트를 제거하기 전에 영향을 받는 S3 또는 Swift 클라이언트 애플리케이션을 모두 업데이트하십시오. 다른 로드 밸런서 끝점에 할당된 포트를 사용하여 연결할 각 클라이언트를 업데이트합니다. 필요한 인증서 정보도 업데이트해야 합니다.

- 하나 이상의 끝점을 제거하려면:
 - a. 부하 분산 장치 페이지에서 제거할 각 끝점에 대한 확인란을 선택합니다.
 - b. Actions * > * Remove * 를 선택합니다.
 - c. OK * 를 선택합니다.
- 세부 정보 페이지에서 끝점 하나를 제거하려면 다음을 수행합니다.
 - a. 로드 밸런서 페이지에서 끝점 이름을 선택합니다.
 - b. 세부 정보 페이지에서 * 제거 * 를 선택합니다.
 - c. OK * 를 선택합니다.

로드 밸런싱 작동 방식 - CLB 서비스(더 이상 사용되지 않음)

게이트웨이 노드의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않습니다. 이제 로드 밸런서 서비스가 권장되는 로드 밸런싱 메커니즘입니다.

CLB 서비스는 Layer 4 로드 밸런싱을 사용하여 클라이언트 응용 프로그램에서 들어오는 TCP 네트워크 연결을 가용성, 시스템 로드 및 관리자 구성 링크 비용에 따라 최적의 스토리지 노드로 배포합니다. 최적의 스토리지 노드를 선택하면 CLB 서비스는 양방향 네트워크 연결을 설정하고 선택한 노드로 트래픽을 전달합니다. CLB는 들어오는 네트워크 연결을 연결할 때 그리드 네트워크 구성을 고려하지 않습니다.


CLB 서비스에 대한 정보를 보려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택한 다음 * CLB * 와 그 아래 옵션을 선택할 때까지 게이트웨이 노드를 확장합니다.

Grid Topology
StorageGRID Webscale Deployment

Data Center 1
DC1-ADM1-98-160
DC1-G1-98-161
SSM
CLB
HTTP
Events
Resources
DC1-G1-98-162
DC1-S2-98-163
DC1-S3-98-164
DC1-ARC1-98-165
Data Center 2
Data Center 3

Overview
Alarms
Reports
Configuration







Main



Overview: Summary - DC1-G1-98-161

Updated: 2015-10-27 16:23:33 PDT

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 서비스를 사용하도록 선택한 경우 StorageGRID 시스템에 대한 링크 비용을 구성하는 것이 좋습니다.

- 링크 비용은 얼마입니까
- 링크 비용을 업데이트합니다

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.