TR-4626: 로드 밸런서

How to enable StorageGRID in your environment

NetApp
July 05, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/storagegrid-enable/technical-reports/load-balancer/index.html on July 05, 2024. Always check docs.netapp.com for the latest.

목차

TR-4626: 로드 밸런서

StorageGRID과 함께 타사 로드 밸런서를 사용하십시오

StorageGRID 같은 오브젝트 스토리지 시스템에서 타사 및 글로벌 로드 밸런서의 역할에 대해 알아보십시오.

타사 로드 밸런서와 함께 NetApp ® StorageGRID ® 를 구현하기 위한 일반 지침입니다.

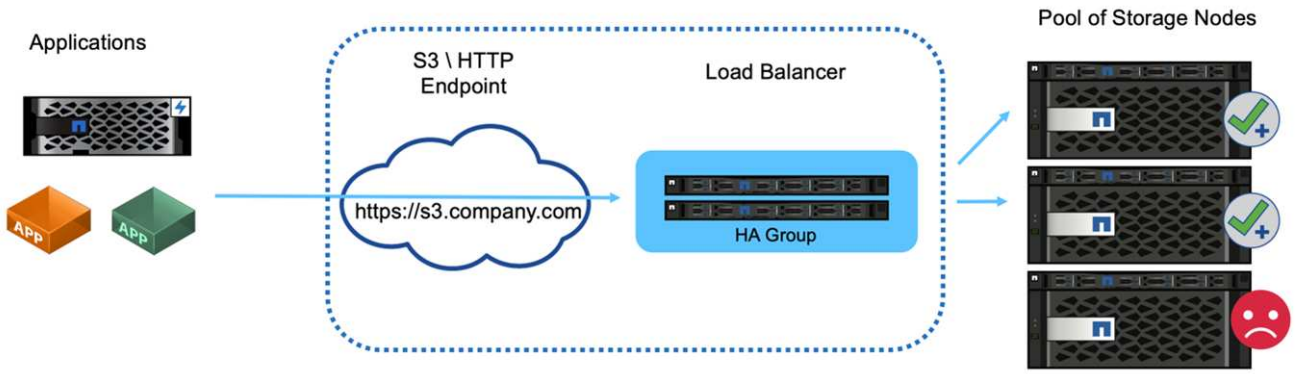
오브젝트 스토리지는 클라우드 스토리지라는 용어와 동의하며, 클라우드 스토리지를 활용하는 애플리케이션은 URL을 통해 해당 스토리지를 처리합니다. 단순한 URL 뒤단에 있는 StorageGRID는 단일 사이트 또는 지리적으로 분산된 사이트에서 용량, 성능 및 내구성을 확장할 수 있습니다. 이러한 단순성을 가능하게 하는 구성 요소는 로드 밸런서입니다.

이 문서의 목적은 StorageGRID 고객에게 로드 밸런서 옵션에 대해 설명하고 타사 로드 밸런서 구성에 대한 일반적인 지침을 제공하는 것입니다.

로드 밸런서 기본 사항

로드 밸런서는 StorageGRID와 같은 엔터프라이즈급 오브젝트 스토리지 시스템의 필수 구성 요소입니다. StorageGRID는 여러 스토리지 노드로 구성되며, 각 스토리지 노드는 특정 StorageGRID 인스턴스에 대해 전체 S3(Simple Storage Service) 이름 공간을 제공할 수 있습니다. 로드 밸런서는 StorageGRID 노드를 배치할 수 있는 고가용성 엔드포인트를 생성합니다. StorageGRID는 자체 로드 밸런서를 제공한다는 점에서 S3 호환 오브젝트 스토리지 시스템 간에는 고유하지만 F5, Citrix NetScaler, HA Proxy, NGINX 등과 같은 타사 또는 범용 로드 밸런서도 지원합니다.

다음 그림에서는 예제 URL/FQDN(정규화된 도메인 이름) “s3.company.com” 사용합니다. 로드 밸런서는 DNS를 통해 FQDN으로 확인되는 가상 IP(VIP)를 생성한 다음, 애플리케이션의 요청을 StorageGRID 노드 풀로 보냅니다. 로드 밸런서는 각 노드에서 상태 점검을 수행하고 정상 노드에 대한 연결만 설정합니다.



이 그림에는 StorageGRID가 제공하는 로드 밸런서가 나와 있지만 타사 로드 밸런서의 개념은 같습니다. 애플리케이션은 로드 밸런서의 VIP를 사용하여 HTTP 세션을 설정하고 트래픽이 로드 밸런서를 통해 스토리지 노드로 전달됩니다. 기본적으로 애플리케이션에서 로드 밸런서까지, 로드 밸런서에서 스토리지 노드까지 모든 트래픽은 HTTPS를 통해 암호화됩니다. HTTP는 지원되는 옵션입니다.

로컬 및 글로벌 로드 밸런서

로드 밸런서에는 두 가지 유형이 있습니다.

- * 로컬 트래픽 관리자(LTM) *. 단일 사이트의 노드 풀에 연결을 분산합니다.
- * 글로벌 서비스 로드 밸런서(GSLB) *. 여러 사이트에 연결을 분산하여 LTM 로드 밸런서를 효과적으로 로드 밸런싱합니다. GSLB는 지능형 DNS 서버라고 생각하면 됩니다. 클라이언트가 StorageGRID 엔드포인트 URL을 요청하면 GSLB는 가용성 또는 기타 요인(예: 애플리케이션의 지연 시간을 줄일 수 있는 사이트)을 기반으로 LTM의 VIP로 이를 확인합니다. LTM은 항상 필요하지만 StorageGRID 사이트의 수와 애플리케이션 요구 사항에 따라 GSLB는 선택 사항입니다.

StorageGRID 게이트웨이 노드 로드 밸런서 대 타사 로드 밸런서

StorageGRID는 S3 호환 오브젝트 스토리지 공급업체에서는 특별 제작된 어플라이언스, VM 또는 컨테이너로 제공되는 네이티브 로드 밸런서를 제공한다는 점에서 차별화됩니다. StorageGRID에서 제공하는 로드 밸런서를 게이트웨이 노드라고도 합니다.

F5, Citrix 등과 같은 로드 밸런서를 아직 소유하고 있지 않은 고객의 경우 타사 로드 밸런서를 구현하는 것이 매우 복잡할 수 있습니다. StorageGRID 로드 밸런서는 로드 밸런서 운영을 크게 단순화합니다.

게이트웨이 노드는 고가용성 및 고성능 로드 밸런서입니다. 고객은 게이트웨이 노드, 타사 로드 밸런서 또는 둘 다를 동일한 그리드에 구현할 수 있습니다. 게이트웨이 노드는 GSLB와 로컬 트래픽 관리자입니다.

StorageGRID 로드 밸런서는 다음과 같은 이점을 제공합니다.

- * 단순성 *. 리소스 풀 자동 구성, 상태 점검, 패치 적용 및 유지 관리 기능이 모두 StorageGRID에서 관리됩니다.
- * 성능 *. StorageGRID 로드 밸런서는 StorageGRID 전용이므로 대역폭을 위해 다른 애플리케이션과 경쟁하지 않습니다.
- * 비용 *. 추가 비용 없이 가상 머신(VM) 및 컨테이너 버전이 제공됩니다.
- * 트래픽 분류 *. 고급 트래픽 분류 기능을 사용하면 워크로드 분석과 함께 StorageGRID 관련 QoS 규칙을 사용할 수 있습니다.
- * 미래의 StorageGRID 전용 기능 *. StorageGRID는 향후 릴리스에 걸쳐 로드 밸런서에 혁신적인 기능을 지속적으로 최적화하고 추가할 예정입니다.

StorageGRID 게이트웨이 노드 배포에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 설명서".

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- NetApp StorageGRID 문서 센터 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 지원 https://docs.netapp.com/us-en/storagegrid-enable/
- StorageGRID F5 로드 밸런서 설계 고려 사항 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load NetApp StorageGRID 밸런싱 https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp - 로드 밸런싱 NetApp StorageGRID https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

StorageGRID에서 HTTPS용 SSL 인증서를 구현하는 방법에 대해 알아봅니다

StorageGRID에서 SSL 인증서를 구현하는 것의 중요성과 단계를 이해합니다.

HTTPS를 사용하는 경우 SSL(Secure Sockets Layer) 인증서가 있어야 합니다. SSL 프로토콜은 클라이언트와 엔드포인트를 식별하여 신뢰할 수 있는 것으로 검증합니다. SSL은 또한 트래픽의 암호화를 제공합니다. SSL 인증서를 클라이언트에서 신뢰할 수 있어야 합니다. 이를 위해 SSL 인증서는 DigiCert, 인프라에서 실행되는 사설 CA 또는 호스트에서 생성한 자체 서명된 인증서와 같은 전역 신뢰 받는 CA(인증 기관)에서 발급받을 수 있습니다.

클라이언트 측 추가 작업이 필요하지 않으므로 전역적으로 신뢰할 수 있는 CA 인증서를 사용하는 것이 좋습니다. 인증서가 로드 밸런서 또는 StorageGRID에 로드되고 클라이언트가 끝점을 신뢰하고 연결합니다.

개인 CA를 사용하려면 루트 및 모든 하위 인증서를 클라이언트에 추가해야 합니다. 개인 CA 인증서를 신뢰하는 프로세스는 클라이언트 운영 체제 및 응용 프로그램에 따라 다를 수 있습니다. 예를 들어 ONTAP for FabricPool에서 체인의 각 인증서(루트 인증서, 하위 인증서, 끝점 인증서)를 ONTAP 클러스터에 개별적으로 업로드해야 합니다.

자체 서명된 인증서를 사용하려면 클라이언트가 CA 없이 제공된 인증서를 신뢰하여 인증을 확인해야 합니다. 일부 응용 프로그램에서는 자체 서명된 인증서를 허용하지 않으며 확인을 무시할 수 없습니다.

클라이언트 부하 분산 장치 StorageGRID 경로에 SSL 인증서 배치는 SSL 종료가 필요한 위치에 따라 달라집니다. 로드 밸런서를 클라이언트의 종료 끝점으로 구성한 다음 로드 밸런서에 대한 StorageGRID 연결을 위한 새 SSL 인증서를 사용하여 다시 암호화하거나 핫 암호화할 수 있습니다. 또는 트래픽을 통과하여 StorageGRID가 SSL 종료 엔드포인트가 되도록 할 수 있습니다. 로드 밸런서가 SSL 종료 엔드포인트인 경우 인증서가 로드 밸런서에 설치되며 DNS 이름/URL의 주체 이름과 클라이언트가 로드 밸런서를 통해 StorageGRID 대상에 연결하도록 구성된 대체 URL/DNS 이름을 포함합니다. 와일드카드 이름을 포함합니다. 로드 밸런서가 패스스루로 구성된 경우 SSL 인증서를 StorageGRID에 설치해야 합니다. 또한 인증서에는 DNS 이름/URL의 주체 이름과 와일드카드 이름을 포함하여 로드 밸런서를 통해 StorageGRID 대상에 연결하도록 클라이언트가 구성된 대체 URL/DNS 이름이 포함되어야 합니다. 인증서에 개별 스토리지 노드 이름을 포함할 필요는 없으며 끝점 URL만 포함할 수 있습니다.

StorageGRID에서 신뢰할 수 있는 타사 로드 밸런서를 구성합니다

StorageGRID에서 신뢰할 수 있는 타사 로드 밸런서를 구성하는 방법을 알아보십시오.

하나 이상의 외부 계층 7 로드 밸런서와 IP 기반의 S3 버킷 또는 그룹 정책을 사용 중인 경우 StorageGRID는 실제 보낸 사람의 IP 주소를 결정해야 합니다. 로드 밸런서에 의해 요청에 삽입된 X-Forwarded-For(XFF) 헤더를 보면 이 작업을 수행할 수 있습니다. XFF 헤더는 스토리지 노드로 직접 전송된 요청에서 쉽게 스푸핑될 수 있으므로 StorageGRID는 각 요청이 신뢰할 수 있는 계층 7 로드 밸런서에 의해 라우팅되고 있는지 확인해야 합니다. StorageGRID에서 요청의 소스를 신뢰할 수 없는 경우 XFF 헤더를 무시합니다. 신뢰할 수 있는 외부 레이어 7 로드 밸런서 목록을 구성할 수 있는

그리드 관리 API가 있습니다. 이 새로운 API는 비공개이며 향후 StorageGRID 릴리스에서 변경될 수 있습니다. 최신 정보는 KB 문서, 를 참조하십시오 "타사 레이어 7 로드 밸런서와 함께 작동하도록 StorageGRID를 구성하는 방법".

로컬 트래픽 매니저 로드 밸런서에 대해 알아보십시오

로컬 트래픽 관리자 로드 밸런서에 대한 지침을 살펴보고 최적의 구성을 결정합니다.

다음은 타사 로드 밸런서 구성에 대한 일반적인 지침입니다. 로드 밸런서 관리자와 협력하여 사용자 환경에 가장 적합한 구성을 결정합니다.

스토리지 노드의 리소스 그룹을 생성합니다

StorageGRID 스토리지 노드를 리소스 풀 또는 서비스 그룹으로 그룹화합니다(용어는 특정 로드 밸런서에 따라 다를 수 있음). StorageGRID 스토리지 노드는 다음 포트에 S3 API를 제공합니다.

- S3 HTTPS: 18082
- S3 HTTP: 18084

대부분의 고객은 표준 HTTPS 및 HTTP 포트(443 및 80)를 통해 가상 서버에서 API를 제공하도록 선택합니다.

각 StorageGRID 사이트에는 3개의 스토리지 노드가 기본적으로 필요하고 2개는 정상 상태여야 합니다.

상태 점검

타사 로드 밸런서를 사용하려면 각 노드의 상태와 해당 노드의 트래픽 수신 자격을 확인하는 방법이 필요합니다. NetApp에서는 상태 점검을 수행할 것을 HTTP `OPTIONS` 메소드를 권장합니다. 로드 밸런서는 각 개별 스토리지 노드에 HTTP `OPTIONS` 요청을 전송하고 상태 응답을 예상합니다. `200`

스토리지 노드가 응답을 제공하지 않으면 `200` 해당 노드에서 스토리지 요청을 처리할 수 없습니다. 애플리케이션 및 비즈니스 요구 사항에 따라 이러한 확인 시간 초과 및 로드 밸런서가 수행하는 작업이 결정됩니다.

예를 들어, 데이터 센터 1에 있는 4개의 스토리지 노드 중 3개가 중단된 경우 모든 트래픽을 데이터 센터 2로 전달할 수 있습니다.

권장되는 폴링 간격은 초당 1회이며, 세 번의 검사가 실패한 후 노드가 오프라인 상태로 표시됩니다.

S3 상태 점검의 예

다음 예에서는 `OPTIONS` 를 보내고 `200 OK`확인합니다. `OPTIONS`Amazon S3)가 승인되지 않은 요청을 지원하지 않기 때문에 사용합니다.

```
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
```

파일 또는 콘텐츠 기반의 상태 점검

일반적으로 NetApp은 파일 기반 상태 점검을 권장하지 않습니다. 예를 들어, 일반적으로 작은 파일이 —`healthcheck.htm`읽기 전용 정책으로 버킷에서 생성됩니다. 그런 다음 로드 밸런서에 의해 이 파일을 가져와 평가합니다. 이 접근 방식에는 몇 가지 단점이 있습니다.

- 단일 계정에 따라 다릅니다**.** 파일을 소유한 계정이 비활성화되면 상태 점검이 실패하고 스토리지 요청이 처리되지 않습니다.
- * 데이터 보호 규칙. * 기본 데이터 보호 체계는 두 가지 복사본 접근 방식입니다. 이 시나리오에서는 상태 점검 파일을 호스팅하는 두 스토리지 노드를 사용할 수 없는 경우 상태 점검이 실패하고 스토리지 요청이 정상적인 스토리지 노드로 전송되지 않아 그리드가 오프라인으로 렌더링됩니다.
- * 감사 로그 블로트. * 로드 밸런서는 매 X 분마다 모든 스토리지 노드에서 파일을 가져와 감사 로그 항목을 많이 생성합니다.
- * 리소스 집약적 * 몇 초마다 모든 노드에서 상태 점검 파일을 가져오면 그리드 및 네트워크 리소스가 사용됩니다.

콘텐츠 기반의 상태 점검이 필요한 경우 전용 S3 버킷이 있는 전용 테넌트를 사용하십시오.

세션 지속성

세션 지속성 또는 고정성은 지정된 HTTP 세션이 지속될 수 있는 시간을 나타냅니다. 기본적으로 세션은 10분 후에 스토리지 노드에 의해 삭제됩니다. 지속성 시간이 길어지면 애플리케이션이 모든 작업에 대해 세션을 다시 설정할 필요가 없으므로 성능이 향상될 수 있지만 이러한 세션을 열어 두면 리소스가 소모됩니다. 작업 부하가 유용하다고 판단되면 타사 로드 밸런서의 세션 지속성을 줄일 수 있습니다.

가상 호스팅 방식의 주소 지정

이제 가상 호스팅 방식이 AWS S3의 기본 방법이며 StorageGRID와 많은 애플리케이션이 경로 스타일을 지원하는 반면, 호스팅된 가상 지원을 구축하는 것이 모범 사례입니다. 가상 호스팅 방식의 요청에는 호스트 이름의 일부분으로 버켓이 있습니다.

가상 호스팅 스타일을 지원하려면 다음을 수행합니다.

- 와일드카드 DNS 조회 지원: * .s3.company.com
- 와일드카드를 지원하려면 제목 대체 이름이 있는 SSL 인증서를 사용하십시오. *.s3.company.com 일부 고객은 와일드카드 인증서 사용과 관련하여 보안 문제를 제기했습니다. StorageGRID는 FabricPool와 같은 주요 애플리케이션과 마찬가지로 경로 스타일 액세스를 계속 지원합니다. 하지만 가상 호스팅 지원 없이는 특정 S3 API 호출이 실패하거나 제대로 작동하지 않습니다.

SSL 종료

타사 로드 밸런서의 SSL 종료에는 보안상의 이점이 있습니다. 로드 밸런서가 손상되면 그리드가 분리됩니다.

지원되는 구성은 세 가지입니다.

- * SSL 패스스루. * SSL 인증서는 StorageGRID에 사용자 지정 서버 인증서로 설치됩니다.
- * SSL 종료 및 재암호화(권장). * StorageGRID에 SSL 인증서를 설치하지 않고 로드 밸런서에서 SSL 인증서 관리를 이미 수행하고 있는 경우 이 방법이 도움이 될 수 있습니다. 이 구성은 공격 대상을 로드 밸런서까지 제한하는 추가적인 보안 이점을 제공합니다.
- * HTTP로 SSL 종료. * 이 구성에서 SSL은 타사 로드 밸런서에서 종료되며 로드 밸런서에서 StorageGRID로의 통신은 SSL 오프로드를 활용하기 위해 암호화되지 않습니다(최신 프로세서에 내장된 SSL 라이브러리 사용).

패스스루 구성

패스스루에 대해 로드 밸런서를 구성하려면 StorageGRID에 인증서를 설치해야 합니다. 메뉴: 구성 [서버 인증서 > 개체 스토리지 API 서비스 끝점 서버 인증서]로 이동합니다.

소스 클라이언트 IP 가시성

StorageGRID 11.4에는 신뢰할 수 있는 타사 로드 밸런서라는 개념이 도입되었습니다. 클라이언트 응용 프로그램 IP를 StorageGRID로 전달하려면 이 기능을 구성해야 합니다. 자세한 내용은 을 참조하십시오 "타사 레이어 7 로드 밸런서와 함께 작동하도록 StorageGRID를 구성하는 방법"

클라이언트 응용 프로그램의 IP를 보는 데 XFF 헤더를 사용하도록 설정하려면 다음 단계를 수행하십시오.

단계

1. 감사 로그에 클라이언트 IP를 기록합니다.
2. `aws:SourceIp`S3 버킷 또는 그룹 정책을 사용합니다.

로드 밸런싱 전략

대부분의 로드 밸런싱 솔루션은 로드 밸런싱을 위한 여러 전략을 제공합니다. 다음은 일반적인 전략입니다.

- * 라운드 로빈. * 보편적인 적합하지만 소수의 노드와 대규모 전송으로 인해 단일 노드가 어려움을 겪고 있습니다.

- * 최소 연결. * 소형 및 혼합 오브젝트 워크로드에 적합하며, 모든 노드에 대한 연결의 균등한 분산을 제공합니다.

알고리즘 선택은 선택할 스토리지 노드의 수가 늘어날수록 더 중요해집니다.

데이터 경로

모든 데이터는 로컬 트래픽 관리자 로드 밸런서를 통해 흐릅니다. StorageGRID는 DSR(Direct Server Routing)을 지원하지 않습니다.

연결 배포를 확인하는 중입니다

메서드가 스토리지 노드 전체에 로드를 균등하게 분산하는지 확인하려면 지정된 사이트의 각 노드에서 설정된 세션을 확인합니다.

- * UI 방법. * 메뉴로 이동: 지원 [메트릭 > S3 개요 > LDR HTTP 세션]
- * 메트릭 API. * 사용 `storagegrid_http_sessions_incoming_currently_established`

StorageGRID 구성의 몇 가지 사용 사례에 대해 알아보십시오

고객과 NetApp IT가 구현한 StorageGRID 구성에 대한 몇 가지 사용 사례를 살펴보십시오.

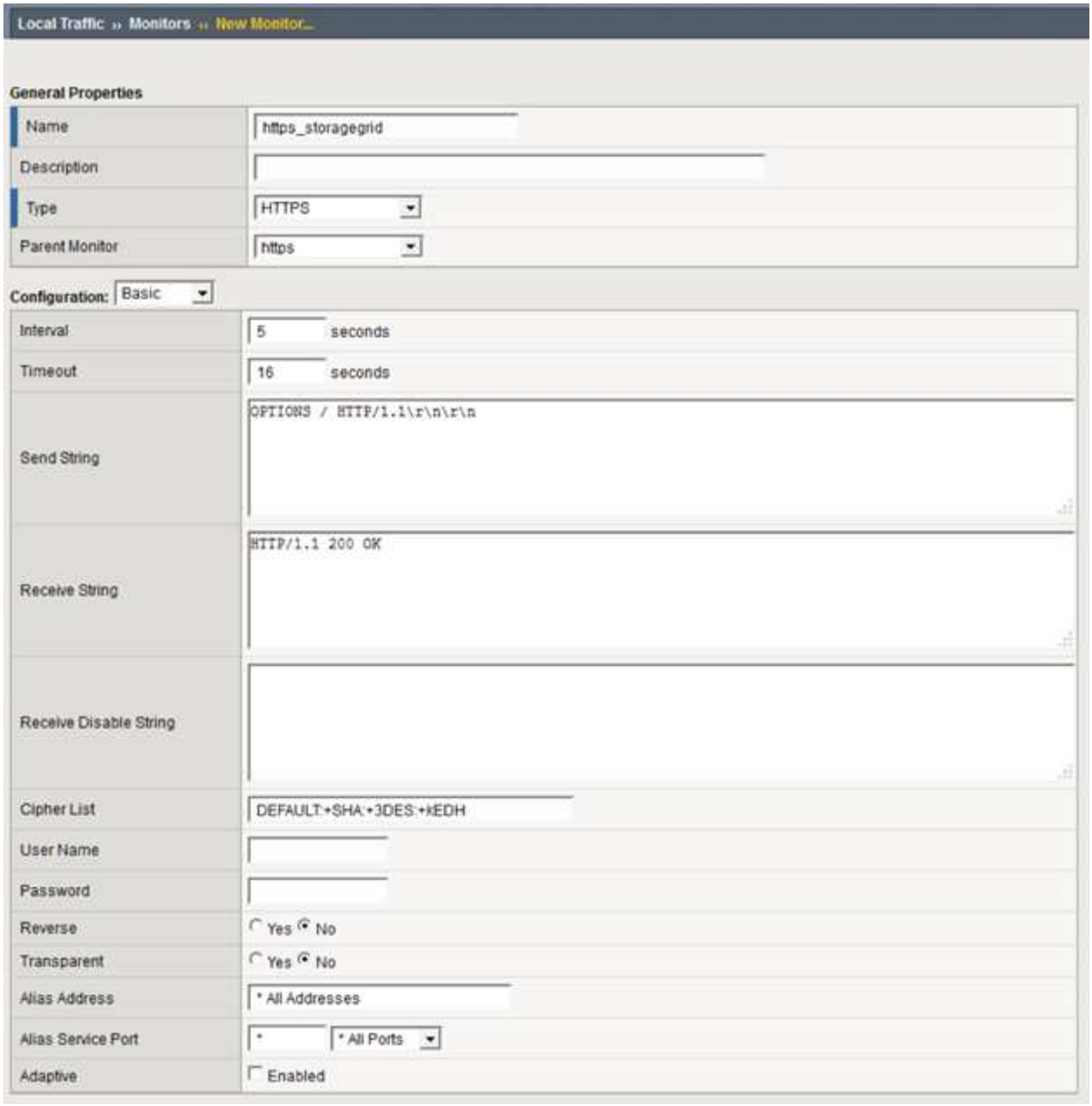
다음 예에서는 NetApp IT를 포함하여 StorageGRID 고객이 구현한 구성을 보여 줍니다.

S3 버킷에 대한 F5 BIG-IP 로컬 트래픽 관리자 상태 점검 모니터

F5 BIG-IP 로컬 트래픽 관리자 상태 점검 모니터를 구성하려면 다음 단계를 수행하십시오.

단계

1. 새 모니터를 만듭니다.
   a. 유형 필드에 을 `HTTPS`입력합니다.
   b. 간격 및 시간 초과를 원하는 대로 구성합니다.
   c. Send String(문자열 보내기) 필드에 \r\n을 `OPTIONS / HTTP/1.1\r\n\r\n.` 입력하십시오. BIG-IP 소프트웨어의 버전이 다르면 0개, 1개 또는 2개의 시퀀스 세트가 필요합니다. 자세한 내용은 을 https://support.f5.com/csp/article/K10655참조하십시오.
   d. 수신 문자열 필드에 다음을 입력합니다 `HTTP/1.1 200 OK`.



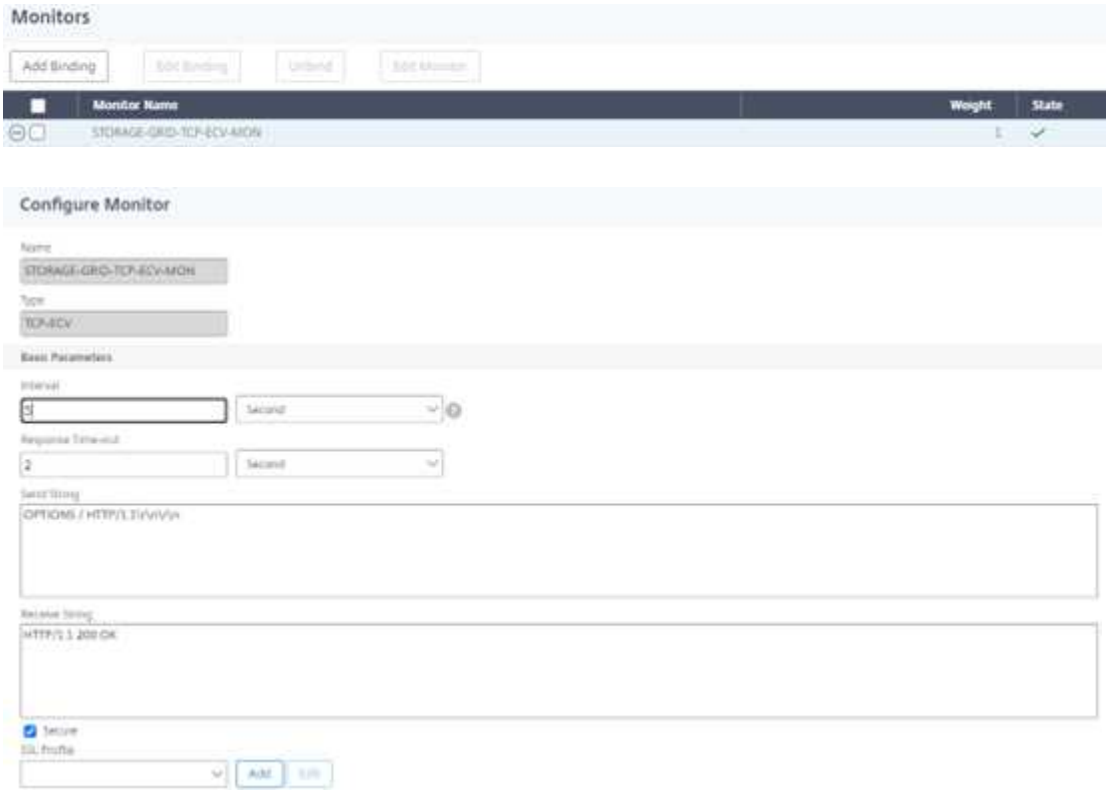
2. Create Pool에서 필요한 각 포트에 대해 하나의 풀을 생성합니다.
   a. 이전 단계에서 만든 상태 모니터를 할당합니다.
   b. 부하 분산 방법을 선택합니다.
   c. 서비스 포트 18082(S3)를 선택합니다.
   d. 노드 추가

Citrix NetScaler를 선택합니다

Citrix NetScaler는 스토리지 엔드포인트에 대한 가상 서버를 생성하고 StorageGRID 스토리지 노드를 애플리케이션 서버로 참조한 다음 서비스 로 그룹화합니다.

HTTPS-ECV 상태 점검 모니터를 사용하여 옵션 요청 및 수신을 사용하여 권장 상태 점검을 수행할 사용자 지정 모니터를 만듭니다 `200`. HTTP-ECV는 송신 문자열로 구성되어 있고 수신 문자열의 유효성을 검사합니다.

자세한 내용은 Citrix 설명서를 참조하십시오 "HTTP-ECV 상태 점검 모니터의 샘플 구성".



Loadbalancer.org

Loadbalancer.org 에서는 StorageGRID를 사용한 자체 통합 테스트를 수행했으며 다음과 같은 포괄적인 구성 가이드를 보유하고 있습니다. https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf

케이이엠피주식회사

Kemp는 StorageGRID와의 자체 통합 테스트를 수행했으며 광범위한 구성 가이드를 보유하고 있습니다 https://kemptechnologies.com/solutions/netapp/.

HAProxy

옵션 요청을 사용하도록 HAProxy를 구성하고 hafroxy.cfg의 상태 검사에 대한 200개의 상태 응답을 확인합니다. 프런트 엔드의 바인딩 포트를 443과 같은 다른 포트로 변경할 수 있습니다.

다음은 HAProxy에서 SSL 종료의 예입니다.

```
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
```

다음은 SSL pass-through의 예입니다.

```
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 구성에 대한 전체 예는 GitHub의 를 "HAProxy 구성의 예" 참조하십시오.

StorageGRID에서 SSL 연결을 검증합니다

StorageGRID에서 SSL 연결의 유효성을 검사하는 방법에 대해 알아봅니다.

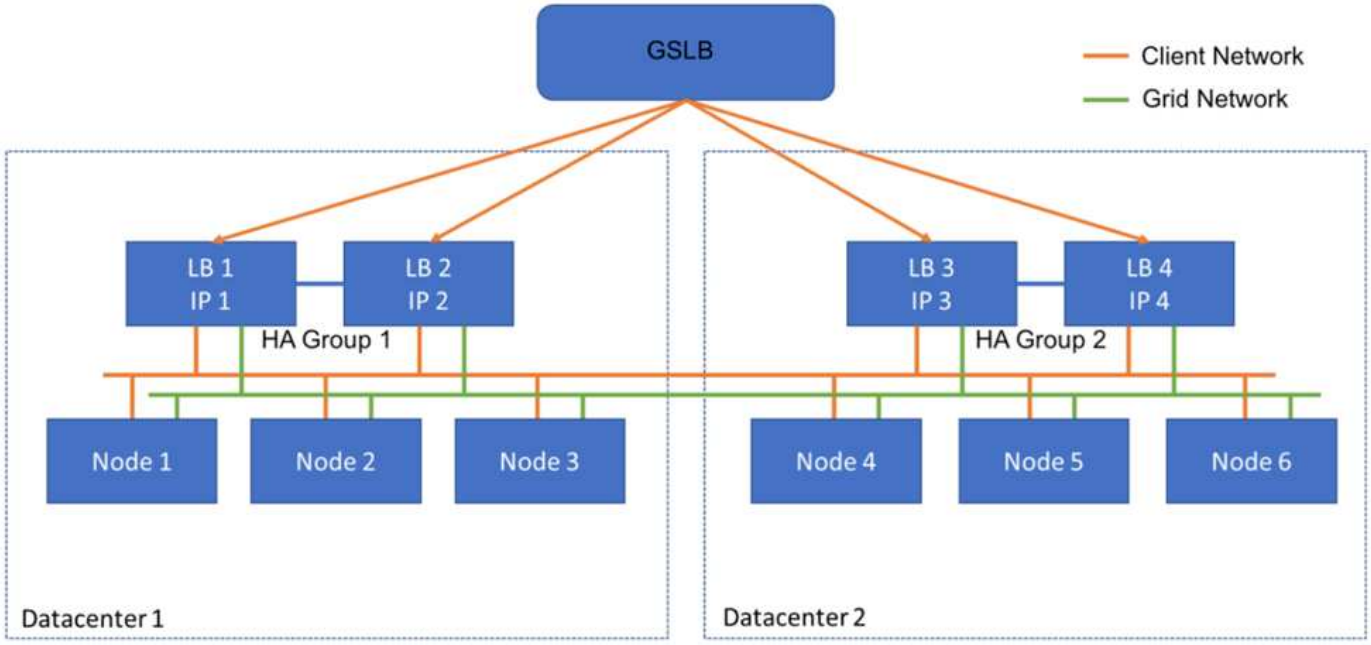
로드 밸런서를 구성한 후에는 OpenSSL 및 AWS CLI와 같은 툴을 사용하여 연결의 유효성을 확인해야 합니다. S3 브라우저와 같은 다른 응용 프로그램은 SSL 구성 오류를 무시할 수 있습니다.

StorageGRID의 글로벌 로드 밸런싱 요구 사항을 이해합니다

StorageGRID의 글로벌 부하 분산에 대한 설계 고려 사항 및 요구 사항을 살펴보십시오.

글로벌 로드 밸런싱을 위해서는 DNS와 통합하여 여러 StorageGRID 사이트에 걸친 지능형 라우팅을 제공해야 합니다. 이 기능은 StorageGRID 도메인 외부에 있으며 앞에서 설명한 로드 밸런서 제품 또는 Infoblox와 같은 DNS 트래픽 제어 솔루션과 같은 타사 솔루션을 통해 제공되어야 합니다. 이 최상위 수준의 부하 분산은 네임스페이스에서 가장 가까운 대상 사이트로 스마트 라우팅을 제공하고, 중단 감지 및 네임스페이스의 다음 사이트로 리디렉션합니다. 일반적인 GSLB 구현은 사이트-로컬 로드 밸런서가 포함된 사이트 풀이 있는 최상위 GSLB로 구성됩니다. 사이트 로드

밸런서에는 로컬 사이트 스토리지 노드의 풀이 포함됩니다. 여기에는 GSLB 기능을 위한 타사 로드 밸런서와 사이트 로컬 로드 밸런싱을 제공하는 StorageGRID의 조합 또는 타사 조합 또는 앞에서 논의된 많은 타사가 GSLB와 사이트 로컬 로드 밸런싱을 모두 제공할 수 있습니다.



저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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