로드 밸런싱 관리

StorageGRID 11.8

NetApp
March 19, 2024

목차

로드 밸런싱 관리

로드 균형 조정에 대한 고려 사항

로드 밸런싱을 사용하여 S3 및 Swift 클라이언트에서 수집 및 검색 워크로드를 처리할 수 있습니다.

로드 밸런싱이란 무엇입니까?

클라이언트 애플리케이션이 StorageGRID 시스템에서 데이터를 저장하거나 검색할 때 StorageGRID는 로드 밸런서를 사용하여 수집 및 검색 워크로드를 관리합니다. 로드 밸런싱은 여러 스토리지 노드에 워크로드를 분산하여 속도와 연결 용량을 극대화합니다.

StorageGRID 로드 밸런서 서비스는 모든 관리 노드 및 모든 게이트웨이 노드에 설치되며 계층 7 로드 밸런싱을 제공합니다. 클라이언트 요청에 대한 TLS(Transport Layer Security) 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다.

각 노드의 로드 밸런서 서비스는 클라이언트 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 가용성이 높은 스토리지 노드로 라우팅합니다.

> StorageGRID 로드 밸런서 서비스가 권장되는 로드 밸런싱 메커니즘이지만 타사 로드 밸런서를 대신 통합할 수도 있습니다. 자세한 내용은 NetApp 어카운트 담당자에게 문의하거나 를 참조하십시오 "TR-4626: StorageGRID 타사 및 글로벌 로드 밸런서".

몇 개의 로드 밸런싱 노드가 필요합니까?

일반적으로 StorageGRID 시스템의 각 사이트에는 부하 분산 서비스가 있는 두 개 이상의 노드가 포함되어야 합니다. 예를 들어 사이트에는 두 개의 게이트웨이 노드 또는 관리 노드와 게이트웨이 노드가 모두 포함될 수 있습니다. SG100 또는 SG1000 서비스 어플라이언스, 베어 메탈 노드 또는 가상 머신(VM) 기반 노드를 사용 중이든, 각 로드 밸런싱 노드에 적절한 네트워킹, 하드웨어 또는 가상화 인프라가 있는지 확인하십시오.

로드 밸런서 엔드포인트란 무엇입니까?

로드 밸런서 끝점은 들어오는 클라이언트 응용 프로그램 요청과 나가는 클라이언트 응용 프로그램이 로드 밸런서 서비스를 포함하는 노드에 액세스하는 데 사용할 포트 및 네트워크 프로토콜(HTTPS 또는 HTTP)을 정의합니다. 또한 끝점은 클라이언트 유형(S3 또는 Swift), 바인딩 모드 및 허용 또는 차단된 테넌트 목록을 정의합니다.

로드 밸런서 끝점을 만들려면 * 구성 * > * 네트워크 * > * 로드 밸런서 끝점 * 을 선택하거나 FabricPool 및 S3 설정 마법사를 완료합니다. 지침:

- "로드 밸런서 엔드포인트를 구성합니다"
- "S3 설정 마법사를 사용합니다"
- "FabricPool 설정 마법사를 사용합니다"

포트에 대한 고려 사항

로드 밸런서 끝점의 포트는 사용자가 만든 첫 번째 끝점의 경우 기본적으로 10433으로 설정되지만 사용하지 않는 외부 포트는 1에서 65535 사이로 지정할 수 있습니다. 포트 80 또는 443을 사용하는 경우 엔드포인트는 게이트웨이

노드에서만 로드 밸런서 서비스를 사용합니다. 이러한 포트는 관리 노드에 예약되어 있습니다. 두 개 이상의 끝점에 동일한 포트를 사용하는 경우 각 끝점에 대해 다른 바인딩 모드를 지정해야 합니다.

다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 를 참조하십시오 "네트워크 포트 참조".

네트워크 프로토콜에 대한 고려 사항

대부분의 경우 클라이언트 응용 프로그램과 StorageGRID 간의 연결은 TLS(전송 계층 보안) 암호화를 사용해야 합니다. TLS 암호화 없이 StorageGRID에 연결하는 것은 지원되지만 특히 프로덕션 환경에서는 권장되지 않습니다. StorageGRID 로드 밸런서 끝점에 대한 네트워크 프로토콜을 선택할 때 * HTTPS * 를 선택해야 합니다.

로드 밸런서 끝점 인증서에 대한 고려 사항

로드 밸런서 끝점의 네트워크 프로토콜로 * HTTPS * 를 선택한 경우 보안 인증서를 제공해야 합니다. 로드 밸런서 끝점을 만들 때 다음 세 가지 옵션 중 하나를 사용할 수 있습니다.

- * 서명된 인증서 업로드(권장) *. 이 인증서는 공개적으로 신뢰할 수 있거나 개인 인증 기관(CA)에서 서명할 수 있습니다. 공개적으로 신뢰할 수 있는 CA 서버 인증서를 사용하여 연결을 보호하는 것이 가장 좋습니다. 생성된 인증서와 달리 CA에서 서명한 인증서는 중단 없이 회전할 수 있으므로 만료 문제를 방지하는 데 도움이 됩니다.

  로드 밸런서 끝점을 만들기 전에 다음 파일을 얻어야 합니다.

  - 사용자 지정 서버 인증서 파일입니다.
  - 사용자 지정 서버 인증서 개인 키 파일입니다.
  - 선택적으로 각 중간 발급 인증 기관의 인증서 CA 번들.
- * 자체 서명된 인증서 생성 *.
- * 글로벌 StorageGRID S3 및 Swift 인증서 사용 *. 로드 밸런서 끝점에 대해 인증서를 선택하려면 먼저 이 인증서의 사용자 지정 버전을 업로드하거나 생성해야 합니다. 을 참조하십시오 "S3 및 Swift API 인증서를 구성합니다".

어떤 가치가 필요합니까?

인증서를 생성하려면 S3 또는 Swift 클라이언트 응용 프로그램이 끝점에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소를 알아야 합니다.

인증서의 * 주체 DN * (고유 이름) 항목에는 클라이언트 응용 프로그램이 StorageGRID에 사용할 정규화된 도메인 이름이 포함되어야 합니다. 예를 들면 다음과 같습니다.

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

필요에 따라 인증서는 와일드카드를 사용하여 로드 밸런서 서비스를 실행하는 모든 관리 노드 및 게이트웨이 노드의 정규화된 도메인 이름을 나타낼 수 있습니다. 예를 들면, 다음과 같습니다. `*.storagegrid.example.com` 와일드카드를 사용하여 나타냅니다 `adm1.storagegrid.example.com` 및 `gn1.storagegrid.example.com`.

S3 가상 호스팅 스타일 요청을 사용하려는 경우 인증서에는 각 요청에 대해 * 대체 이름 * 항목도 포함되어야 합니다 "S3 끝점 도메인 이름입니다" 와일드카드 이름을 포함하여 을 구성했습니다. 예를 들면 다음과 같습니다.

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

도메인 이름에 와일드카드를 사용하는 경우 을 검토하십시오 "서버 인증서에 대한 강화 지침".

보안 인증서의 각 이름에 대한 DNS 항목도 정의해야 합니다.

만료 예정인 인증서를 관리하려면 어떻게 해야 합니까?

S3 응용 프로그램과 StorageGRID 간의 연결을 보호하는 데 사용되는 인증서가 만료되면 응용 프로그램이 StorageGRID에 대한 액세스를 일시적으로 상실할 수 있습니다.

인증서 만료 문제를 방지하려면 다음 모범 사례를 따르십시오.

- 로드 밸런서 끝점 인증서 만료 * 및 * S3 및 Swift API * 알림에 대한 글로벌 서버 인증서 만료 등과 같이 인증서 만료 날짜에 근접했다는 경고를 신중하게 모니터링하십시오.
- 항상 StorageGRID 및 S3 애플리케이션 버전의 인증서를 동기화된 상태로 유지합니다. 로드 밸런서 끝점에 사용되는 인증서를 교체하거나 갱신하는 경우 S3 애플리케이션에서 사용하는 동등한 인증서를 교체하거나 갱신해야 합니다.
- 공개적으로 서명된 CA 인증서를 사용합니다. CA에서 서명한 인증서를 사용하는 경우 만료 예정 인증서를 중단 없이 교체할 수 있습니다.
- 자체 서명된 StorageGRID 인증서를 생성했으며 인증서가 곧 만료될 경우 기존 인증서가 만료되기 전에 StorageGRID 및 S3 응용 프로그램 모두에서 수동으로 인증서를 교체해야 합니다.

바인딩 모드에 대한 고려 사항

바인딩 모드를 사용하면 로드 밸런서 끝점에 액세스하는 데 사용할 수 있는 IP 주소를 제어할 수 있습니다. 끝점에서 바인딩 모드를 사용하는 경우 클라이언트 응용 프로그램은 허용된 IP 주소 또는 해당 FQDN(정규화된 도메인 이름)을 사용하는 경우에만 끝점에 액세스할 수 있습니다. 다른 IP 주소 또는 FQDN을 사용하는 클라이언트 응용 프로그램은 끝점에 액세스할 수 없습니다.

다음 바인딩 모드 중 하나를 지정할 수 있습니다.

- * 글로벌 * (기본값): 클라이언트 응용 프로그램은 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크의 모든 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 끝점에 액세스할 수 있습니다. 끝점의 접근성을 제한할 필요가 없는 경우 이 설정을 사용합니다.
- * HA 그룹의 가상 IP *. 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
- * 노드 인터페이스 *. 클라이언트는 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
- * 노드 유형 *. 선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN)나 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.

테넌트 액세스에 대한 고려 사항

테넌트 액세스는 어떤 StorageGRID 테넌트 계정에서 로드 밸런서 끝점을 사용하여 해당 버킷을 액세스할 수 있는지 제어할 수 있는 선택적 보안 기능입니다. 모든 테넌트가 끝점(기본값)에 액세스하도록 허용하거나 각 끝점에 대해 허용 또는 차단된 테넌트 목록을 지정할 수 있습니다.

이 기능을 사용하여 테넌트와 해당 끝점 간의 보안 격리를 향상시킬 수 있습니다. 예를 들어, 이 기능을 사용하여 한

테넌트가 소유한 기밀 자료 또는 기밀 자료를 다른 테넌트에서 완전히 액세스할 수 없도록 할 수 있습니다.

액세스 제어를 위해 테넌트는 클라이언트 요청에 사용된 액세스 키로 결정되며, 요청의 일부로 액세스 키가 제공되지 않은 경우(예: 익명 액세스) 버킷 소유자가 테넌트를 결정하는 데 사용됩니다.

테넌트 액세스 예

이 보안 기능의 작동 방식을 이해하려면 다음 예제를 고려해 보십시오.

1. 다음과 같이 두 개의 로드 밸런서 엔드포인트를 생성했습니다.
   - * 공개 * 엔드포인트: 포트 10443을 사용하고 모든 테넌트에 대한 액세스를 허용합니다.
   - * 상위 비밀 * 엔드포인트: 포트 10444를 사용하며 * 상위 비밀 * 테넌트에만 액세스할 수 있습니다. 다른 모든 테넌트는 이 끝점에 액세스할 수 없습니다.
2. 를 클릭합니다 `top-secret.pdf` 은(는) * Top Secret * 테넌트가 소유한 버킷에 있습니다.

를 눌러 에 액세스합니다 `top-secret.pdf`, * Top secret * 테넌트에 있는 사용자는 에 GET 요청을 보낼 수 있습니다 `https://w.x.y.z:10444/top-secret.pdf`. 이 테넌트는 10444 엔드포인트를 사용할 수 있으므로 사용자가 개체에 액세스할 수 있습니다. 그러나 다른 테넌트에 속한 사용자가 동일한 URL에 동일한 요청을 보내면 즉시 액세스 거부 메시지가 표시됩니다. 자격 증명과 서명이 유효하더라도 액세스가 거부됩니다.

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. 끝점을 사용하여 그리드 관리자, 테넌트 관리자 또는 둘 다에 액세스할 수도 있습니다.

Swift 클라이언트 응용 프로그램에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 있습니다 "루트 액세스 권한".
- 을(를) 검토했습니다 "로드 균형 조정에 대한 고려 사항".
- 로드 밸런서 끝점에 사용할 포트를 이전에 다시 매핑한 경우 "포트 재맵을 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".

로드 밸런서 끝점을 만듭니다

각 S3 또는 Swift 클라이언트 로드 밸런서 엔드포인트는 포트, 클라이언트 유형(S3 또는 Swift) 및 네트워크 프로토콜(HTTP 또는 HTTPS)을 지정합니다. 관리 인터페이스 부하 분산 장치 끝점은 포트, 인터페이스 유형 및 신뢰할 수 없는 클라이언트 네트워크를 지정합니다.

마법사에 액세스합니다

단계

1. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.
2. S3 또는 Swift 클라이언트의 끝점을 만들려면 * S3 또는 Swift 클라이언트 * 탭을 선택합니다.
3. Grid Manager, Tenant Manager 또는 둘 다에 액세스하기 위한 끝점을 만들려면 * Management interface * 탭을 선택합니다.
4. Create * 를 선택합니다.

끝점 세부 정보를 입력합니다

단계

1. 만들려는 끝점 유형에 대한 세부 정보를 입력하려면 적절한 지침을 선택합니다.

S3 또는 **Swift** 클라이언트

필드에 입력합니다	설명
이름	Load Balancer Endpoints(분산 장치 끝점 로드) 페이지의 테이블에 표시되는 끝점에 대한 설명 이름입니다.
포트	로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드의 기본값은 첫 번째 끝점에서 10433이지만 사용하지 않는 외부 포트는 1에서 65535까지 입력할 수 있습니다. 80 * 또는 * 8443 * 을 입력하면 포트 8443을 해제하지 않는 한 엔드포인트는 게이트웨이 노드에서만 구성됩니다. 그런 다음 포트 8443을 S3 엔드포인트로 사용할 수 있으며 포트가 게이트웨이 및 관리 노드 모두에서 구성됩니다.
클라이언트 유형입니다	이 끝점을 사용할 클라이언트 응용 프로그램 유형, * S3 * 또는 * Swift *.
네트워크 프로토콜	클라이언트가 이 끝점에 연결할 때 사용할 네트워크 프로토콜입니다. • 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. 비프로덕션 그리드에만 HTTP를 사용합니다.

관리 인터페이스

필드에 입력합니다	설명
이름	Load Balancer Endpoints(분산 장치 끝점 로드) 페이지의 테이블에 표시되는 끝점에 대한 설명 이름입니다.
포트	그리드 관리자, 테넌트 관리자 또는 둘 모두에 액세스하는 데 사용할 StorageGRID 포트입니다. • 그리드 관리자: * 8443 * • 테넌트 관리자: * 9443 * • 그리드 관리자와 테넌트 관리자 모두: * 443 * 참고: 이 사전 설정 포트나 기타 사용 가능한 포트를 사용할 수 있습니다.
인터페이스 유형입니다	이 엔드포인트를 사용하여 액세스할 StorageGRID 인터페이스의 라디오 버튼을 선택합니다.

필드에 입력합니다	설명
신뢰할 수 없는 클라이언트 네트워크	신뢰할 수 없는 클라이언트 네트워크에서 이 끝점에 액세스할 수 있어야 하는 경우 * 예 * 를 선택합니다. 그렇지 않으면 * 아니요 * 를 선택합니다. 예 * 를 선택하면 포트가 모든 신뢰할 수 없는 클라이언트 네트워크에서 열립니다. 참고: 로드 밸런서 끝점을 만들 때만 신뢰할 수 없는 클라이언트 네트워크에 대해 포트를 열거나 닫도록 구성할 수 있습니다.

1. Continue * 를 선택합니다.

바인딩 모드를 선택합니다

단계

1. 엔드포인트에 대한 바인딩 모드를 선택하여 모든 IP 주소를 사용하거나 특정 IP 주소 및 네트워크 인터페이스를 사용하여 엔드포인트에 액세스하는 방법을 제어합니다.

   일부 바인딩 모드는 클라이언트 끝점 또는 관리 인터페이스 끝점에 사용할 수 있습니다. 두 끝점 유형의 모든 모드가 여기에 나열됩니다.

모드를 선택합니다	설명
글로벌(클라이언트 끝점의 기본값)	클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크에 있는 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 끝점에 액세스할 수 있습니다. 이 끝점의 접근성을 제한할 필요가 없는 경우 * 글로벌 * 설정을 사용하십시오.
HA 그룹의 가상 IP입니다	클라이언트는 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다. 이 바인딩 모드의 엔드포인트는 엔드포인트에 대해 선택한 HA 그룹이 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.
노드 인터페이스	클라이언트는 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.
노드 유형(클라이언트 엔드포인트만 해당)	선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN)나 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.
모든 관리 노드(관리 인터페이스 엔드포인트의 기본값)	클라이언트는 이 끝점에 액세스하려면 관리자 노드의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.

   둘 이상의 끝점에서 동일한 포트를 사용하는 경우 StorageGRID는 이 우선 순위 순서를 사용하여 사용할 끝점을 결정합니다. * HA 그룹의 가상 IP * > * 노드 인터페이스 * > * 노드 유형 * > * 글로벌 *.

관리 인터페이스 엔드포인트를 생성하는 경우 관리 노드만 허용됩니다.

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

   관리 인터페이스 끝점을 생성하는 경우 관리 노드에만 연결된 VIP를 선택합니다.

3. 노드 인터페이스 * 를 선택한 경우 이 끝점과 연결할 각 관리 노드 또는 게이트웨이 노드에 대해 하나 이상의 노드 인터페이스를 선택합니다.
4. 노드 유형 * 을 선택한 경우 기본 관리 노드와 비기본 관리 노드 또는 게이트웨이 노드를 모두 포함하는 관리자 노드 중 하나를 선택합니다.

테넌트 액세스를 제어합니다

관리 인터페이스 끝점은 끝점에 가 있는 경우에만 테넌트 액세스를 제어할 수 있습니다 Tenant Manager의 인터페이스 유형입니다.

단계

1. Tenant access * 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 해당 버킷에 액세스할 수 있습니다. 테넌트 계정을 아직 생성하지 않은 경우 이 옵션을 선택해야 합니다. 테넌트 계정을 추가한 후 로드 밸런서 끝점을 편집하여 특정 계정을 허용하거나 차단할 수 있습니다.
선택한 테넌트 허용	선택한 테넌트 계정만 이 끝점을 사용하여 해당 버킷을 액세스할 수 있습니다.
선택한 테넌트 차단	선택한 테넌트 계정은 이 끝점을 사용하여 해당 버킷을 액세스할 수 없습니다. 다른 모든 테넌트는 이 끝점을 사용할 수 있습니다.

2. 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

단계

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".

- * 관리 인터페이스 인증서 사용 *. 관리 노드에 대한 직접 연결에도 사용할 수 있는 글로벌 관리 인터페이스 인증서를 사용하려면 이 옵션을 선택합니다.

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 파일입니다 (`.key`)를 클릭합니다.

> 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. 파일을 확장자로 저장합니다 `.pem`.

  예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

d. Create * 를 선택합니다. 를 누릅니다 로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3와 Swift 클라이언트 또는 관리 인터페이스와 엔드포인트 간의 모든 후속 새 연결에 사용됩니다.

인증서를 생성합니다

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.

필드에 입력합니다	설명
키 사용 확장을 추가합니다	이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다. 이러한 확장은 인증서에 포함된 키의 용도를 정의합니다. • 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

c. Generate * 를 선택합니다.

d. 생성된 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 선택하십시오.

   ▪ 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 파일을 확장자로 저장합니다 `.pem`.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

e. Create * 를 선택합니다.

   로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3와 Swift 클라이언트 또는 관리 인터페이스와 이 끝점 간의 모든 후속 새 연결에 사용됩니다.

작업을 마친 후

단계

1. DNS를 사용하는 경우 DNS에 StorageGRID FQDN(정규화된 도메인 이름)을 클라이언트가 연결에 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

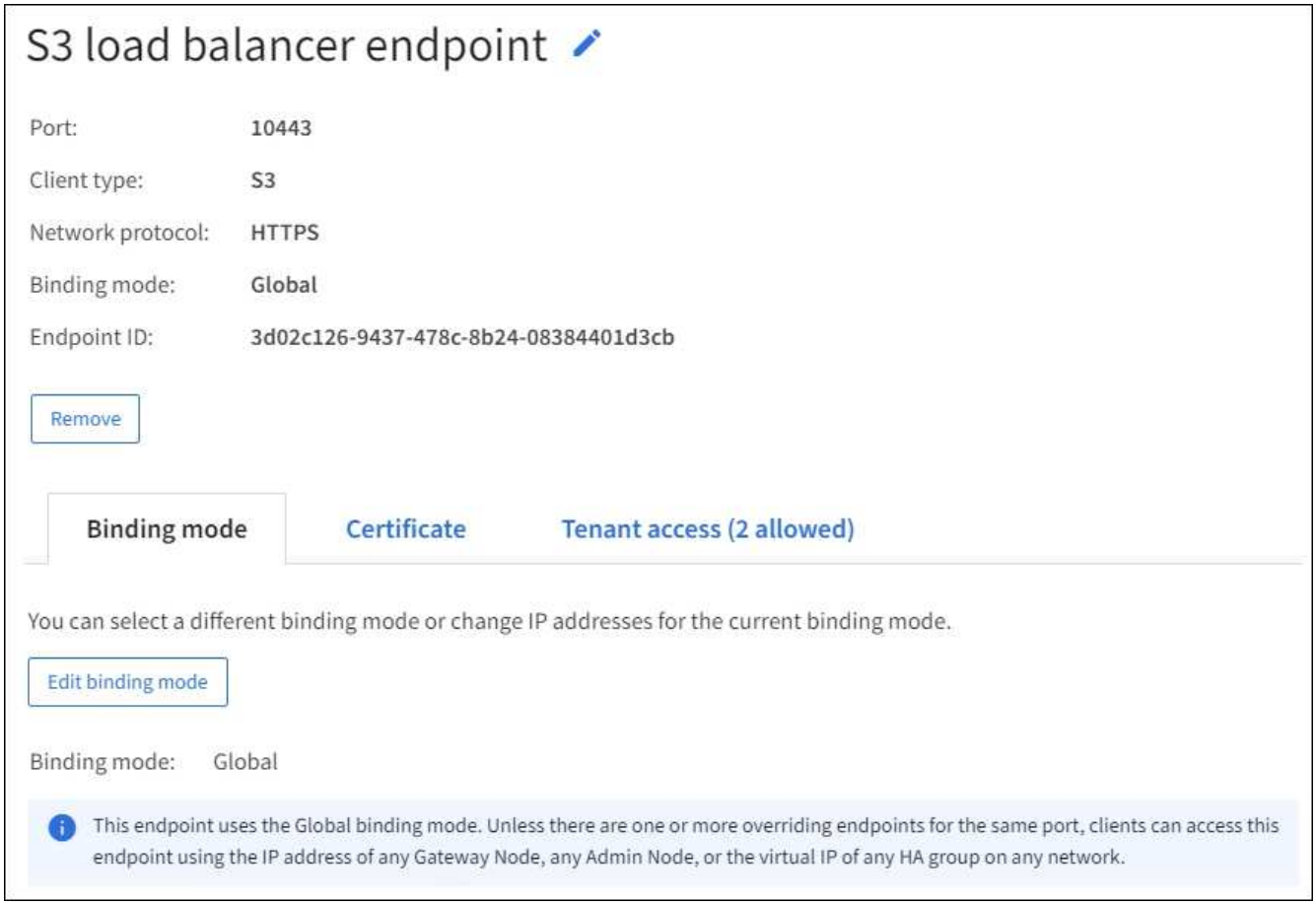
   ◦ 정규화된 도메인 이름 또는 IP 주소입니다

   ◦ 필요한 인증서 세부 정보입니다

로드 밸런서 끝점을 보고 편집합니다

보안 끝점의 인증서 메타데이터를 포함하여 기존 로드 밸런서 끝점에 대한 세부 정보를 볼 수 있습니다. 끝점의 특정 설정을 변경할 수 있습니다.

- 모든 로드 밸런서 끝점에 대한 기본 정보를 보려면 부하 분산 끝점 페이지의 표를 검토하십시오.
- 인증서 메타데이터를 포함하여 특정 끝점에 대한 모든 세부 정보를 보려면 테이블에서 끝점 이름을 선택합니다. 표시되는 정보는 엔드포인트 유형 및 구성 방법에 따라 다릅니다.



- 끝점을 편집하려면 로드 밸런서 끝점 페이지의 * 작업 * 메뉴를 사용하십시오.

관리 인터페이스 끝점의 포트를 편집하는 동안 Grid Manager에 액세스할 수 없는 경우 URL 및 포트를 업데이트하여 다시 액세스합니다.

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.
엔드포인트 포트를 편집합니다	a. 끝점의 확인란을 선택합니다. b. Actions * > * Edit Endpoint port * 를 선택합니다 c. 유효한 포트 번호를 입력하십시오. d. 저장 * 을 선택합니다.	*n/a*
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.
끝점 인증서를 편집합니다	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.	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.
테넌트 액세스를 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 테넌트 액세스 편집 * 을 선택합니다. c. 다른 액세스 옵션을 선택하거나 목록에서 테넌트를 선택하거나 제거하거나 둘 모두를 수행합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. Tenant access * 탭을 선택합니다. c. Edit tenant access * 를 선택합니다. d. 다른 액세스 옵션을 선택하거나 목록에서 테넌트를 선택하거나 제거하거나 둘 모두를 수행합니다. 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.

관리 인터페이스 끝점을 제거하는 동안 그리드 관리자에 액세스할 수 없는 경우 URL을 업데이트합니다.

- 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.