클라이언트 연결 구성

StorageGRID software

NetApp
July 23, 2026

목차

클라이언트 연결 구성

StorageGRID에 대한 S3 클라이언트 연결을 구성합니다

그리드 관리자는 S3 클라이언트 애플리케이션이 데이터를 저장하고 검색하기 위해 StorageGRID 시스템에 연결하는 방식을 제어하는 구성 옵션을 관리합니다.

Swift 관련 세부 정보는 이 버전의 문서 사이트에서 삭제되었습니다. 을 참조하십시오 "StorageGRID 11.8: S3 및 Swift 클라이언트 연결 구성".

구성 작업

1. 클라이언트 애플리케이션이 StorageGRID에 연결하는 방법에 따라 StorageGRID에서 사전 요구 사항 작업을 수행합니다.

필수 작업

다음 사항을 확보해야 합니다.

- IP 주소
- 도메인 이름
- SSL 인증서

선택적 작업

선택적으로 구성합니다.

- ID 페더레이션
- SSO

1. StorageGRID를 사용하여 애플리케이션이 그리드에 연결하는 데 필요한 값을 가져오세요. S3 설정 마법사를 사용하거나 각 StorageGRID 엔티티를 수동으로 구성할 수 있습니다.

S3 설정 마법사 사용

S3 설정 마법사의 단계를 따르십시오.

수동으로 구성

1. 고가용성 그룹 생성
2. 로드 밸런서 엔드포인트 생성
3. 테넌트 계정 생성
4. 버킷 및 액세스 키 생성
5. ILM 규칙 및 정책 구성

1. S3 애플리케이션을 사용하여 StorageGRID에 대한 연결을 완료합니다. 사용할 도메인 이름에 IP 주소를 연결하려면 DNS 항목을 생성하십시오.

   필요에 따라 추가적인 애플리케이션 설정을 수행하십시오.

2. 애플리케이션 및 StorageGRID에서 지속적인 작업을 수행하여 시간 경과에 따라 오브젝트 스토리지를 관리하고 모니터링합니다.

클라이언트 애플리케이션에 **StorageGRID**를 연결하는 데 필요한 정보

StorageGRID를 S3 클라이언트 애플리케이션에 연결하기 전에 StorageGRID에서 구성 단계를 수행하고 특정 값을 얻어야 합니다.

어떤 값이 필요합니까**?**

다음 표는 StorageGRID에서 구성해야 하는 값과 해당 값이 S3 애플리케이션 및 DNS 서버에서 사용되는 위치를 보여줍니다.

가치	값이 구성된 위치	값이 사용되는 곳
가상 IP(VIP) 주소	StorageGRID > HA 그룹	DNS 항목
포트	StorageGRID > 로드 밸런서 엔드포인트	클라이언트 애플리케이션
SSL 인증서	StorageGRID > 로드 밸런서 엔드포인트	클라이언트 애플리케이션
서버 이름(FQDN)	StorageGRID > 로드 밸런서 엔드포인트	• 클라이언트 애플리케이션 • DNS 항목
S3 액세스 키 ID 및 비밀 액세스 키	StorageGRID > 테넌트 및 버킷	클라이언트 애플리케이션
버킷/컨테이너 이름	StorageGRID > 테넌트 및 버킷	클라이언트 애플리케이션

이 값을 어떻게 얻을 수 있습니까**?**

필요에 따라 다음 두 가지 방법 중 하나를 사용하여 필요한 정보를 얻을 수 있습니다.

- **"S3** 설정 마법사**"**를 사용하세요**.** S3 설정 마법사는 StorageGRID에서 필요한 값을 빠르게 구성하는 데 도움을 주며, S3 애플리케이션을 구성할 때 사용할 수 있는 하나 또는 두 개의 파일을 출력합니다. 마법사는 필요한 단계를 안내하고 설정이 StorageGRID 모범 사례를 준수하는지 확인하는 데 도움을 줍니다.

  S3 애플리케이션을 구성하는 경우, 특별한 요구 사항이 있거나 구현에 상당한 사용자 지정이 필요한 경우가 아니라면 S3 설정 마법사를 사용하는 것이 좋습니다.

- **"FabricPool** 설정 마법사**"**를 사용하세요**.** S3 설정 마법사와 마찬가지로, FabricPool 설정 마법사는 필요한 값을 신속하게 구성하는 데 도움이 되며, ONTAP에서 FabricPool 클라우드 계층을 구성할 때 사용할 수 있는 파일을

출력합니다.

> StorageGRID를 FabricPool 클라우드 계층의 객체 스토리지 시스템으로 사용하려는 경우, 특별한 요구 사항이 있거나 구현에 상당한 사용자 지정이 필요한 경우가 아니라면 FabricPool 설정 마법사를 사용하는 것이 좋습니다.

- 항목을 수동으로 구성합니다. S3 애플리케이션에 연결하고 S3 설정 마법사를 사용하지 않으려는 경우 구성을 수동으로 수행하여 필요한 값을 얻을 수 있습니다. 다음 단계를 따르십시오.
  a. S3 애플리케이션에 사용할 고가용성(HA) 그룹을 구성하십시오. "고가용성 그룹 구성"을 참조하십시오.
  b. S3 애플리케이션에서 사용할 로드 밸런서 엔드포인트를 생성합니다. "로드 밸런서 엔드포인트 구성"을 참조하십시오.
  c. S3 애플리케이션에서 사용할 테넌트 계정을 생성합니다. "테넌트 계정 생성"을 참조하십시오.
  d. S3 테넌트의 경우 테넌트 계정에 로그인하여 애플리케이션에 액세스할 각 사용자에 대한 액세스 키 ID와 비밀 액세스 키를 생성합니다. "액세스 키 생성"을 참조하십시오.
  e. 테넌트 계정 내에 하나 이상의 S3 버킷을 생성합니다. S3에 대한 자세한 내용은 "S3 버킷 생성"을 참조하십시오.
  f. 새 테넌트 또는 버킷/컨테이너에 속하는 객체에 대한 특정 배치 지침을 추가하려면 새 ILM 규칙을 생성하고 해당 규칙을 사용하도록 새 ILM 정책을 활성화하십시오. 자세한 내용은 "ILM 규칙 생성" 및 "ILM 정책 생성"을 참조하십시오.

StorageGRID의 S3 클라이언트 보안

StorageGRID 테넌트 계정은 S3 클라이언트 애플리케이션을 사용하여 객체 데이터를 StorageGRID에 저장합니다. 클라이언트 애플리케이션에 구현된 보안 조치를 검토해야 합니다.

요약

다음 목록은 S3 REST API에 대한 보안 구현 방식을 요약한 것입니다.

연결 보안
: TLS

서버 인증
: 시스템 CA에서 서명한 X.509 서버 인증서 또는 관리자가 제공한 사용자 지정 서버 인증서

클라이언트 인증
: S3 계정 액세스 키 ID 및 비밀 액세스 키

클라이언트 승인
: 버킷 소유권 및 모든 관련 액세스 제어 정책

StorageGRID가 클라이언트 애플리케이션에 보안을 제공하는 방법

S3 클라이언트 애플리케이션은 게이트웨이 노드 또는 관리 노드의 로드 밸런서 서비스에 연결하거나 스토리지 노드에 직접 연결할 수 있습니다.

- 로드 밸런서 서비스에 연결하는 클라이언트는 사용자의 설정에 따라 HTTPS 또는 HTTP를 사용할 수 있습니다 "로드 밸런서 엔드포인트 구성".

  HTTPS는 안전한 TLS 암호화 통신을 제공하며 권장됩니다. 엔드포인트에 보안 인증서를 연결해야 합니다.

  HTTP는 보안 수준이 낮고 암호화되지 않은 통신을 제공하므로 비운영 환경 또는 테스트 그리드에서만 사용해야 합니다.

- 스토리지 노드에 연결하는 클라이언트는 HTTPS 또는 HTTP를 사용할 수 있습니다.

  HTTPS가 기본 프로토콜이며 권장됩니다.

  HTTP는 암호화되지 않은 통신으로 보안성이 떨어지지만, 비운영 환경이나 테스트 환경에서 선택적으로 "활성화됨" 사용할 수 있습니다.

- StorageGRID와 클라이언트 간의 통신은 TLS를 사용하여 암호화됩니다.
- 로드 밸런서 서비스와 그리드 내 스토리지 노드 간의 통신은 로드 밸런서 엔드포인트가 HTTP 또는 HTTPS 연결을 허용하도록 구성되어 있는지 여부와 관계없이 암호화됩니다.
- 클라이언트는 REST API 작업을 수행하기 위해 "HTTP 인증 헤더"을 StorageGRID에 제공해야 합니다.

보안 인증서 및 클라이언트 애플리케이션

모든 경우에 클라이언트 애플리케이션은 그리드 관리자가 업로드한 사용자 지정 서버 인증서 또는 StorageGRID 시스템에서 생성한 인증서를 사용하여 TLS 연결을 설정할 수 있습니다.

- 클라이언트 애플리케이션이 로드 밸런서 서비스에 연결할 때 로드 밸런서 엔드포인트에 대해 구성된 인증서를 사용합니다. 각 로드 밸런서 엔드포인트에는 고유한 인증서가 있습니다—그리드 관리자가 업로드한 사용자 지정 서버 인증서이거나 엔드포인트를 구성할 때 그리드 관리자가 StorageGRID에서 생성한 인증서입니다.

  "로드 밸런싱 고려 사항"을 참조하십시오.

- 클라이언트 애플리케이션이 스토리지 노드에 직접 연결할 때, StorageGRID 시스템 설치 시 스토리지 노드용으로 생성된 시스템 생성 서버 인증서(시스템 인증 기관에서 서명함) 또는 그리드 관리자가 그리드에 제공한 단일 사용자 지정 서버 인증서를 사용합니다. "사용자 지정 S3 API 인증서 추가"을 참조하십시오.

클라이언트는 TLS 연결을 설정하는 데 사용하는 인증서를 서명한 인증 기관을 신뢰하도록 구성해야 합니다.

TLS 라이브러리에서 지원하는 해싱 및 암호화 알고리즘

StorageGRID 시스템은 클라이언트 애플리케이션이 TLS 세션을 설정할 때 사용할 수 있는 암호화 스위트 세트를 지원합니다. 암호화를 구성하려면 구성 > 보안 > *보안 설정*으로 이동하여 *TLS 및 SSH 정책*을 선택하십시오.

지원되는 **TLS** 버전

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.

SSLv3 및 TLS 1.1(또는 이전 버전)은 더 이상 지원되지 않습니다.

S3 설정 마법사 사용

StorageGRID S3 setup wizard 고려 사항 및 요구 사항

S3 설정 마법사를 사용하여 StorageGRID를 S3 애플리케이션의 객체 스토리지 시스템으로 구성할 수 있습니다.

S3 설정 마법사를 사용하는 경우

S3 설정 마법사는 S3 애플리케이션과 함께 사용하도록 StorageGRID를 구성하는 각 단계를 안내합니다. 마법사를 완료하는 과정에서 S3 애플리케이션에 값을 입력하는 데 사용할 파일을 다운로드하게 됩니다. 마법사를 사용하여 시스템을 더 빠르게 구성하고 설정이 StorageGRID 모범 사례를 준수하는지 확인하십시오.

"루트 액세스 권한"가 있는 경우 StorageGRID Grid Manager를 처음 사용할 때 S3 설정 마법사를 완료하거나, 나중에 언제든지 마법사에 액세스하여 완료할 수 있습니다. 필요에 따라 일부 또는 모든 필수 항목을 수동으로 구성한 다음 마법사를 사용하여 S3 애플리케이션에 필요한 값을 조합할 수도 있습니다.

마법사를 사용하기 전에

마법사를 사용하기 전에 다음 필수 조건을 모두 충족했는지 확인하십시오.

IP 주소를 확보하고 **VLAN** 인터페이스를 설정합니다**.**

고가용성(HA) 그룹을 구성하려면 S3 애플리케이션이 연결될 노드와 사용할 StorageGRID 네트워크를 알아야 합니다. 또한 서브넷 CIDR, 게이트웨이 IP 주소 및 가상 IP(VIP) 주소에 입력해야 하는 값도 알아야 합니다.

S3 애플리케이션의 트래픽을 분리하기 위해 가상 LAN을 사용할 계획이라면 이미 VLAN 인터페이스를 구성한 상태입니다. "VLAN 인터페이스 구성"을 참조하십시오.

ID 페더레이션 및 **SSO** 구성

StorageGRID 시스템에 ID 페더레이션 또는 싱글 사인온(SSO)을 사용하려면 이러한 기능을 활성화해야 합니다. 또한 S3 애플리케이션에서 사용할 테넌트 계정에 루트 액세스 권한을 부여해야 하는 페더레이션 그룹도 알고 있어야 합니다. "ID 페더레이션 사용" 및 "싱글 사인온(SSO) 구성"을 참조하십시오.

도메인 이름 획득 및 구성

StorageGRID에 사용할 정규화된 도메인 이름(FQDN)을 알고 있습니다. 도메인 네임 서버(DNS) 항목은 이 FQDN을 마법사를 사용하여 생성하는 HA 그룹의 가상 IP(VIP) 주소에 매핑합니다.

S3 가상 호스팅 방식 요청을 사용하려는 경우 "구성된 S3 엔드포인트 도메인 이름"이(가) 있어야 합니다. 가상 호스팅 방식 요청 사용을 권장합니다.

로드 밸런서 및 보안 인증서 요구 사항 검토

StorageGRID 로드 밸런서를 사용할 계획이라면 로드 밸런싱에 대한 일반적인 고려 사항을 검토했을 것입니다. 업로드할 인증서 또는 인증서 생성에 필요한 값을 준비했을 것입니다.

외부(타사) 로드 밸런싱 엔드포인트를 사용할 계획이라면 해당 로드 밸런서의 정규화된 도메인 이름(FQDN), 포트 및 인증서를 확보해야 합니다.

그리드 페더레이션 연결 구성

S3 테넌트가 그리드 페더레이션 연결을 사용하여 계정 데이터를 복제하고 버킷 객체를 다른 그리드로 복제할 수 있도록 허용하려면 마법사를 시작하기 전에 다음 사항을 확인하십시오.

- "그리드 페더레이션 연결을 구성했습니다."이(가) 있습니다.
- 연결 상태는 *연결됨*입니다.
- 루트 액세스 권한이 있습니다.

StorageGRID에서 S3 설정 마법사에 액세스하여 완료합니다

S3 설정 마법사를 사용하여 S3 애플리케이션에서 StorageGRID를 사용할 수 있도록 구성할 수 있습니다. 설정 마법사는 애플리케이션이 StorageGRID 버킷에 액세스하고 객체를 저장하는 데 필요한 값을 제공합니다.

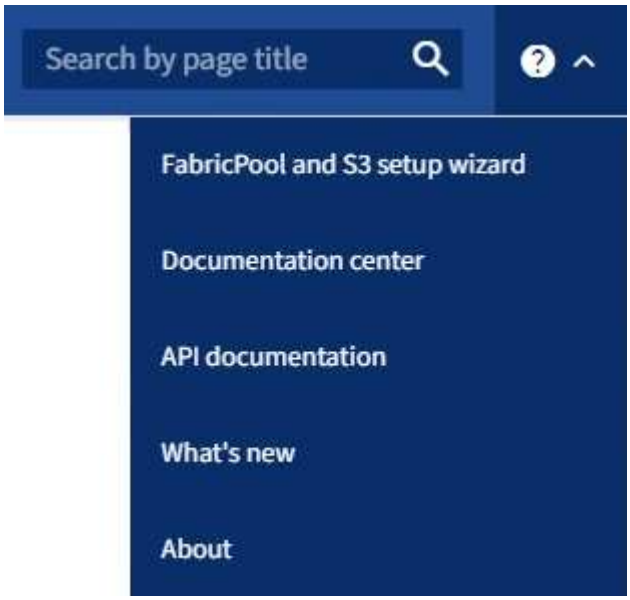
시작하기 전에

- 다음이 있습니다. "루트 액세스 권한"
- 마법사 사용을 위한 "고려사항 및 요구사항"을 검토했습니다.

마법사에 액세스합니다

단계

1. "지원되는 웹 브라우저"을(를) 사용하여 Grid Manager에 로그인합니다.
2. * FabricPool 및 S3 설정 마법사* 배너가 대시보드에 나타나면 배너의 링크를 선택하십시오. 배너가 더 이상 표시되지 않으면 그리드 관리자 헤더 바에서 도움말 아이콘을 선택하고 * FabricPool 및 S3 설정 마법사*를 선택하십시오.



3. FabricPool 및 S3 설정 마법사 페이지의 S3 애플리케이션 섹션에서 *지금 구성*을 선택합니다.

6단계 중 **1**단계**: HA** 그룹 구성

HA 그룹은 StorageGRID 로드 밸런서 서비스를 각각 포함하는 노드들의 모음입니다. HA 그룹에는 게이트웨이 노드, 관리 노드 또는 둘 다 포함될 수 있습니다.

HA 그룹을 사용하면 S3 데이터 연결 가용성을 유지하는 데 도움이 됩니다. HA 그룹의 활성 인터페이스에 장애가 발생하면 백업 인터페이스가 워크로드를 관리하여 S3 운영에 미치는 영향을 최소화할 수 있습니다.

이 작업에 대한 자세한 내용은 "고가용성 그룹 관리"을 참조하십시오.

단계

1. 외부 로드 밸런서를 사용할 계획이라면 HA 그룹을 생성할 필요가 없습니다. *이 단계 건너뛰기*를 선택하고 6단계 중 2단계: 로드 밸런싱 엔드포인트 구성로 이동합니다.
2. StorageGRID 로드 밸런서를 사용하려면 새 HA 그룹을 생성하거나 기존 HA 그룹을 사용할 수 있습니다.

HA 그룹 생성

a. 새 HA 그룹을 생성하려면 *HA 그룹 생성*을 선택하십시오.

b. 세부 정보 입력 단계에서 다음 필드를 입력합니다.

필드	설명
HA 그룹 이름	이 HA 그룹에 대한 고유한 표시 이름입니다.
설명 (선택 사항)	이 HA 그룹에 대한 설명입니다.

c. 인터페이스 추가 단계에서는 이 HA 그룹에서 사용할 노드 인터페이스를 선택합니다.

열 머리글을 사용하여 행을 정렬하거나 검색어를 입력하여 인터페이스를 더 빠르게 찾을 수 있습니다.

노드를 하나 이상 선택할 수 있지만, 각 노드에 대해 인터페이스는 하나만 선택할 수 있습니다.

d. 인터페이스 우선순위 지정 단계에서는 이 HA 그룹의 기본 인터페이스와 백업 인터페이스를 결정합니다.

행을 드래그하여 우선순위 순서 열의 값을 변경합니다.

목록의 첫 번째 인터페이스가 기본 인터페이스입니다. 기본 인터페이스는 오류가 발생하지 않는 한 활성 인터페이스입니다.

고가용성(HA) 그룹에 인터페이스가 두 개 이상 포함되어 있고 활성 인터페이스에 장애가 발생하면 가상 IP(VIP) 주소는 우선순위에 따라 첫 번째 백업 인터페이스로 이동합니다. 해당 인터페이스에도 장애가 발생하면 VIP 주소는 다음 백업 인터페이스로 이동하고, 이러한 과정이 반복됩니다. 장애가 해결되면 VIP 주소는 사용 가능한 가장 높은 우선순위의 인터페이스로 다시 이동합니다.

e. **IP** 주소 입력 단계에서 다음 필드를 입력합니다.

필드	설명
서브넷 CIDR	CIDR 표기법의 VIP 서브넷 주소 — IPv4 주소 뒤에 슬래시(/)와 서브넷 길이(0~32)가 붙습니다. 네트워크 주소에는 호스트 비트가 설정되어 있으면 안 됩니다. 예를 들어, `192.16.0.0/22`.
게이트웨이 IP 주소(선택 사항)	StorageGRID에 액세스하는 데 사용되는 S3 IP 주소가 StorageGRID VIP 주소와 동일한 서브넷에 없는 경우 StorageGRID VIP 로컬 게이트웨이 IP 주소를 입력합니다. 로컬 게이트웨이 IP 주소는 VIP 서브넷 내에 있어야 합니다.

필드	설명
가상 IP 주소	HA 그룹의 활성 인터페이스에 대해 최소 1개, 최대 10개의 VIP 주소를 입력하십시오. 모든 VIP 주소는 VIP 서브넷 내에 있어야 합니다. 최소 하나의 주소는 IPv4여야 합니다. 선택적으로 추가적인 IPv4 및 IPv6 주소를 지정할 수 있습니다.

f. *HA 그룹 생성*을 선택한 다음 *완료*를 선택하여 S3 설정 마법사로 돌아갑니다.

g. 로드 밸런싱 단계로 이동하려면 *계속*을 선택하십시오.

기존 **HA** 그룹 사용

a. 기존 HA 그룹을 사용하려면 *HA 그룹 선택*에서 HA 그룹 이름을 선택하십시오.

b. 로드 밸런싱 단계로 이동하려면 *계속*을 선택하십시오.

6단계 중 **2**단계**:** 로드 밸런싱 엔드포인트 구성

StorageGRID는 로드 밸런서를 사용하여 클라이언트 애플리케이션의 워크로드를 관리합니다. 로드 밸런싱은 여러 스토리지 노드에서 속도와 연결 용량을 극대화합니다.

모든 게이트웨이 및 관리 노드에 있는 StorageGRID 로드 밸런서 서비스를 사용하거나 외부(타사) 로드 밸런서에 연결할 수 있습니다. StorageGRID 로드 밸런서를 사용하는 것이 좋습니다.

이 작업에 대한 자세한 내용은 "로드 밸런싱 고려 사항"을 참조하십시오.

StorageGRID 로드 밸런서 서비스를 사용하려면 **StorageGRID** 로드 밸런서 탭을 선택한 다음 사용할 로드 밸런서 엔드포인트를 생성하거나 선택하십시오. 외부 로드 밸런서를 사용하려면 외부 로드 밸런서 탭을 선택하고 이미 구성한 시스템에 대한 세부 정보를 제공하십시오.

엔드포인트 생성

단계

1. 로드 밸런서 엔드포인트를 생성하려면 *엔드포인트 생성*을 선택합니다.
2. 엔드포인트 세부 정보 입력 단계에서 다음 필드를 입력합니다.

필드	설명
이름	엔드포인트에 대한 설명적인 이름입니다.
포트	로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드는 처음 생성하는 엔드포인트의 경우 기본값인 10433으로 설정되지만, 사용하지 않는 외부 포트를 입력할 수 있습니다. 80 또는 443을 입력하면 해당 포트는 관리 노드에서 예약되어 있으므로 게이트웨이 노드에만 엔드포인트가 구성됩니다. 참고**:** 다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. "StorageGRID 내부 포트"을 참조하십시오.
클라이언트 유형	*S3*이어야 합니다.
네트워크 프로토콜	*HTTPS*를 선택합니다. 참고: TLS 암호화 없이 StorageGRID와 통신하는 것은 지원되지만 권장하지 않습니다.

3. 바인딩 모드 선택 단계에서는 바인딩 모드를 지정합니다. 바인딩 모드는 엔드포인트에 모든 IP 주소를 사용하거나 특정 IP 주소 및 네트워크 인터페이스를 사용하여 액세스하는 방식을 제어합니다.

모드	설명
전역(기본값)	클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크상의 HA 그룹의 가상 IP(VIP) 주소, 또는 해당 FQDN을 사용하여 엔드포인트에 액세스할 수 있습니다. 이 엔드포인트의 접근성을 제한해야 하는 경우가 아니라면 전역 설정(기본값)을 사용하십시오.
HA 그룹의 가상 IP	클라이언트는 이 엔드포인트에 액세스하기 위해 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용해야 합니다. 이 바인딩 모드를 사용하는 엔드포인트는 선택한 HA 그룹이 서로 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.
노드 인터페이스	클라이언트는 이 엔드포인트에 액세스하기 위해 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.

모드	설명
노드 유형	선택한 노드 유형에 따라 클라이언트는 이 엔드포인트에 액세스하기 위해 관리 노드의 IP 주소(또는 해당 FQDN) 또는 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.

4. 테넌트 액세스 단계에서는 다음 중 하나를 선택하십시오.

필드	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 버킷에 액세스할 수 있습니다.
선택한 테넌트 허용	선택된 테넌트 계정만 이 엔드포인트를 사용하여 자신의 버킷에 액세스할 수 있습니다.
선택한 테넌트 차단	선택된 테넌트 계정은 이 엔드포인트를 사용하여 버킷에 액세스할 수 없습니다. 다른 모든 테넌트는 이 엔드포인트를 사용할 수 있습니다.

5. 인증서 첨부 단계에서는 다음 중 하나를 선택하십시오.

필드	설명
인증서 업로드(권장)	이 옵션을 사용하여 CA에서 서명한 서버 인증서, 인증서 개인 키 및 선택적 CA 번들을 업로드할 수 있습니다.
인증서 생성	이 옵션을 사용하여 자체 서명 인증서를 생성할 수 있습니다. "로드 밸런서 엔드포인트 구성"입력해야 할 내용에 대한 자세한 내용은 해당 문서를 참조하십시오.
StorageGRID S3 인증서 사용	StorageGRID 글로벌 인증서를 이미 업로드했거나 사용자 지정 버전을 생성한 경우에만 이 옵션을 사용하십시오. 자세한 내용은 "S3 API 인증서 구성"을 참조하십시오.

6. S3 설정 마법사로 돌아가려면 **Finish** 를 선택합니다.
7. *계속*을 선택하여 테넌트 및 버킷 단계로 이동합니다.

엔드포인트 인증서 변경 사항이 모든 노드에 적용되는 데 최대 15분이 소요될 수 있습니다.

기존 로드 밸런서 엔드포인트 사용

단계

1. 기존 엔드포인트를 사용하려면 *로드 밸런서 엔드포인트 선택*에서 해당 이름을 선택하십시오.
2. *계속*을 선택하여 테넌트 및 버킷 단계로 이동합니다.

외부 로드 밸런서 사용

단계

1. 외부 로드 밸런서를 사용하려면 다음 필드를 작성하십시오.

필드	설명
FQDN	외부 로드 밸런서의 정규화된 도메인 이름(FQDN)입니다.
포트	S3 애플리케이션이 외부 로드 밸런서에 연결하는 데 사용할 포트 번호입니다.
인증서	외부 로드 밸런서의 서버 인증서를 복사하여 이 필드에 붙여넣으십시오.

2. *계속*을 선택하여 테넌트 및 버킷 단계로 이동합니다.

6단계 중 **3**단계**:** 테넌트 및 버킷 생성

테넌트는 S3 애플리케이션을 사용하여 StorageGRID에 객체를 저장하고 검색할 수 있는 엔터티입니다. 각 테넌트는 고유한 사용자, 액세스 키, 버킷, 객체 및 특정 기능 집합을 갖습니다.

버킷은 테넌트의 객체와 객체 메타데이터를 저장하는 데 사용되는 컨테이너입니다. 테넌트는 여러 개의 버킷을 가질 수 있지만, 설정 마법사를 사용하면 가장 빠르고 쉽게 테넌트와 버킷을 생성할 수 있습니다. 나중에 버킷을 추가하거나 옵션을 설정해야 하는 경우 Tenant Manager를 사용할 수 있습니다.

이 작업에 대한 자세한 내용은 "테넌트 계정 생성" 및 "S3 버킷 생성"을 참조하십시오.

단계

1. 테넌트 계정의 이름을 입력합니다.

   테넌트 이름은 고유할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID가 부여됩니다.

2. StorageGRID 시스템에서 "ID 페더레이션", "싱글 사인온(SSO)" 또는 둘 다를 사용하는지에 따라 테넌트 계정에 대한 루트 액세스를 정의하십시오.

옵션	이렇게 하세요
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	a. 기존 페더레이션 그룹을 선택하여 테넌트에 대한 "루트 액세스 권한"을(를) 부여합니다. b. 선택적으로, 로컬 루트 사용자로 테넌트에 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션과 싱글 사인온(SSO)이 모두 활성화된 경우	테넌트에 대해 "루트 액세스 권한"을(를) 갖도록 기존 페더레이션 그룹을 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

3. 마법사가 루트 사용자의 액세스 키 ID와 비밀 액세스 키를 생성하도록 하려면 *루트 사용자 S3 액세스 키 자동 생성*을 선택하십시오.

테넌트의 유일한 사용자가 루트 사용자인 경우 이 옵션을 선택합니다. 다른 사용자가 이 테넌트를 사용할 경우 "테넌트 관리자 사용" 키 및 권한을 구성합니다.

4. 지금 이 테넌트용 버킷을 생성하려면 *이 테넌트용 버킷 생성*을 선택합니다.

> 그리드에 S3 객체 잠금이 활성화된 경우, 이 단계에서 생성되는 버킷에는 S3 객체 잠금이 활성화되지 않습니다. 이 S3 애플리케이션에 S3 객체 잠금이 활성화된 버킷을 사용해야 하는 경우, 지금 버킷을 생성하지 마십시오. 대신 Tenant Manager를 사용하여 "버킷을 생성합니다" 나중에 생성하십시오.

   a. S3 애플리케이션에서 사용할 버킷 이름을 입력하세요. 예를 들어, `s3-bucket`.

      버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

   b. 이 버킷에 대한 *지역*을 선택합니다.

      향후 ILM을 사용하여 버킷의 지역을 기준으로 객체를 필터링할 계획이 없다면 기본 지역(`us-east-1`)을 사용하십시오.

5. *생성하고 계속하기*를 선택합니다.

6단계 중 **4**단계**:** 데이터 다운로드

데이터 다운로드 단계에서는 방금 설정한 세부 정보를 저장하기 위해 하나 또는 두 개의 파일을 다운로드할 수 있습니다.

단계

1. *루트 사용자 S3 액세스 키 자동 생성*을 선택한 경우 다음 중 하나 또는 둘 다를 수행하십시오.
   - 테넌트 계정 이름, 액세스 키 ID 및 비밀 액세스 키가 포함된 `.csv` 파일을 다운로드하려면 *액세스 키 다운로드*를 선택하십시오.
   - 액세스 키 ID와 비밀 액세스 키를 클립보드에 복사하려면 복사 아이콘( )을 선택하십시오.
2. *구성 값 다운로드*를 선택하여 로드 밸런서 엔드포인트, 테넌트, 버킷 및 루트 사용자에 대한 설정이 포함된 `.txt` 파일을 다운로드합니다.
3. 이 정보를 안전한 위치에 저장하십시오.

> 액세스 키를 모두 복사하기 전까지는 이 페이지를 닫지 마십시오. 페이지를 닫으면 키를 더 이상 사용할 수 없습니다. 이 정보는 StorageGRID 시스템에서 데이터를 가져오는 데 사용될 수 있으므로 안전한 곳에 저장해 두십시오.

4. 메시지가 표시되면 확인란을 선택하여 키를 다운로드했거나 복사했음을 확인하십시오.
5. ILM 규칙 및 정책 단계로 이동하려면 *계속*을 선택하십시오.

6단계 중 **5**단계**: S3**에 대한 **ILM** 규칙 및 **ILM** 정책 검토

정보 수명주기 관리(ILM) 규칙은 StorageGRID 시스템의 모든 객체의 배치, 유지 기간 및 수집 동작을 제어합니다. StorageGRID에 포함된 ILM 정책은 모든 객체의 복제본을 두 개 생성합니다. 이 정책은 새 정책을 하나 이상 활성화할 때까지 유효합니다.

단계

1. 해당 페이지에 제공된 정보를 검토하십시오.
2. 새 테넌트 또는 버킷에 속하는 객체에 대한 특정 지침을 추가하려면 새 규칙과 새 정책을 생성하십시오. "ILM 규칙 생성" 및 "ILM 정책 사용"을 참조하십시오.
3. *이 단계들을 검토했으며 제가 해야 할 일을 이해했습니다.*를 선택하세요.
4. 다음 단계에 대해 이해하셨다면 확인란을 선택하십시오.
5. 요약 페이지로 이동하려면 *계속*을 선택합니다.

6단계 중 **6**단계**:** 요약 검토

단계

1. 요약을 검토하세요.
2. 다음 단계에서 세부 정보를 기록해 두십시오. S3 클라이언트에 연결하기 전에 필요한 추가 구성에 대해 설명합니다. 예를 들어, *루트로 로그인*을 선택하면 테넌트 관리자로 이동하여 테넌트 사용자를 추가하고, 추가 버킷을 생성하고, 버킷 설정을 업데이트할 수 있습니다.
3. *완료*를 선택합니다.
4. StorageGRID에서 다운로드한 파일 또는 수동으로 얻은 값을 사용하여 애플리케이션을 구성하십시오.

HA 그룹 관리

StorageGRID 고가용성 그룹에 대해 알아보세요

고가용성(HA) 그룹은 S3 클라이언트에 고가용성 데이터 연결을 제공하고 Grid Manager 및 Tenant Manager에 고가용성 연결을 제공합니다.

여러 관리 노드와 게이트웨이 노드의 네트워크 인터페이스를 고가용성(HA) 그룹으로 묶을 수 있습니다. HA 그룹의 활성 인터페이스에 장애가 발생하면 백업 인터페이스가 워크로드를 관리할 수 있습니다.

각 HA 그룹은 선택된 노드의 공유 서비스에 대한 액세스를 제공합니다.

- 게이트웨이 노드, 관리 노드 또는 둘 다를 포함하는 HA 그룹은 S3 클라이언트에 고가용성 데이터 연결을 제공합니다.
- 관리자 노드만 포함하는 HA 그룹은 그리드 관리자 및 테넌트 관리자에 고가용성 연결을 제공합니다.
- 서비스 어플라이언스와 VMware 기반 소프트웨어 노드만 포함하는 HA 그룹은 "S3 Select를 사용하는 S3 테넌트 "에 대한 고가용성 연결을 제공할 수 있습니다. S3 Select를 사용할 때는 HA 그룹을 사용하는 것이 좋지만 필수 사항은 아닙니다.

HA 그룹은 어떻게 생성하나요**?**

1. 하나 이상의 관리 노드 또는 게이트웨이 노드에 사용할 네트워크 인터페이스를 선택합니다. 그리드 네트워크(eth0) 인터페이스, 클라이언트 네트워크(eth2) 인터페이스, VLAN 인터페이스 또는 노드에 추가한 액세스 인터페이스를 사용할 수 있습니다.

   DHCP로 할당된 IP 주소가 있는 경우 인터페이스를 HA 그룹에 추가할 수 없습니다.

2. 기본 인터페이스로 사용할 인터페이스를 하나 지정합니다. 기본 인터페이스는 오류가 발생하지 않는 한 활성

인터페이스입니다.

3. 백업 인터페이스의 우선순위 순서는 사용자가 결정합니다.
4. 그룹에 1개에서 10개까지의 가상 IP(VIP) 주소를 할당할 수 있습니다. 클라이언트 애플리케이션은 이러한 VIP 주소 중 하나를 사용하여 StorageGRID에 연결할 수 있습니다.

지침은 "고가용성 그룹 구성"을 참조하십시오.

활성 인터페이스란 무엇입니까?

정상 작동 시, HA 그룹의 모든 VIP 주소는 우선순위 순서상 첫 번째 인터페이스인 기본 인터페이스에 추가됩니다. 기본 인터페이스를 사용할 수 있는 한, 클라이언트가 그룹의 VIP 주소에 연결할 때 기본 인터페이스가 사용됩니다. 즉, 정상 작동 시 기본 인터페이스는 해당 그룹의 "활성" 인터페이스입니다.

마찬가지로, 정상 작동 중에는 HA 그룹의 우선순위가 낮은 인터페이스는 "백업" 인터페이스 역할을 합니다. 이러한 백업 인터페이스는 기본(현재 활성) 인터페이스를 사용할 수 없게 되는 경우에만 사용됩니다.

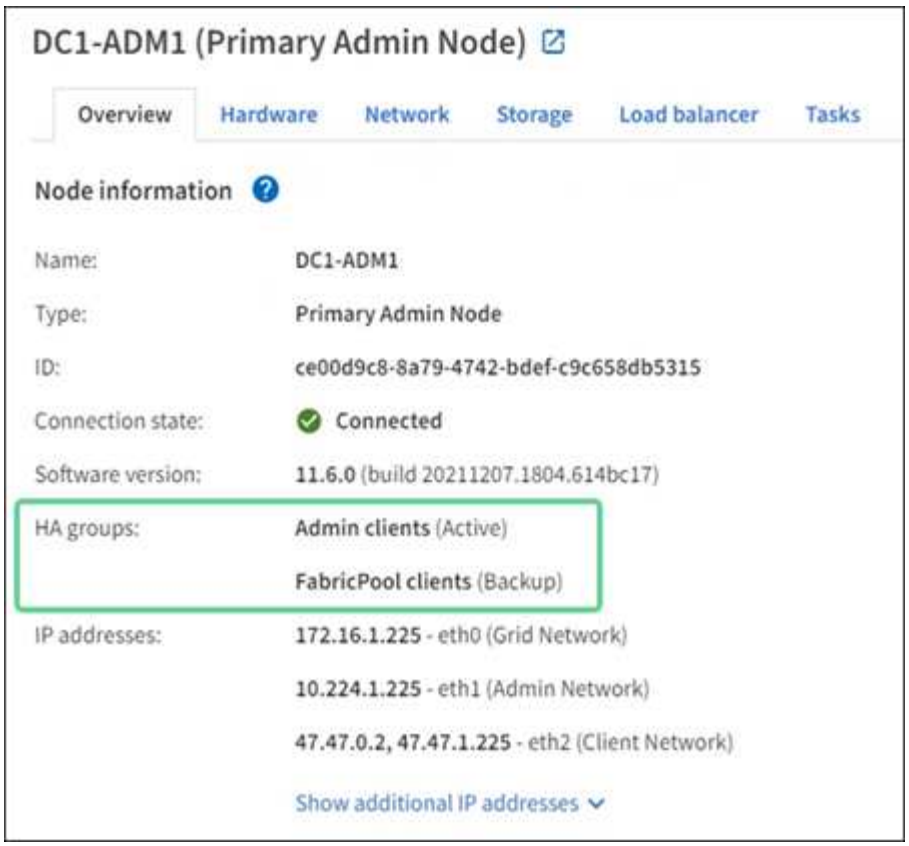
노드의 현재 **HA** 그룹 상태 보기

노드가 HA 그룹에 할당되었는지 여부와 현재 상태를 확인하려면 **Nodes** > *_node_*를 선택하십시오.

개요 탭에 **HA** 그룹 항목이 포함되어 있으면 해당 노드는 나열된 HA 그룹에 할당됩니다. 그룹 이름 뒤의 값은 해당 HA 그룹에서 노드의 현재 상태입니다.

- 활성: HA 그룹은 현재 이 노드에서 호스팅되고 있습니다.
- 백업: HA 그룹은 현재 이 노드를 사용하고 있지 않습니다. 이 인터페이스는 백업용입니다.
- 중지됨: 고가용성(keepalived) 서비스가 수동으로 중지되었기 때문에 이 노드에서 HA 그룹을 호스팅할 수 없습니다.
- **Fault**: 다음 중 하나 이상의 이유로 이 노드에서 HA 그룹을 호스팅할 수 없습니다.
  - 로드 밸런서(nginx-gw) 서비스가 노드에서 실행 중이 아닙니다.
  - 노드의 eth0 또는 VIP 인터페이스가 다운되었습니다.
  - 해당 노드가 다운되었습니다.

이 예시에서는 기본 관리 노드가 두 개의 HA 그룹에 추가되었습니다. 이 노드는 현재 관리 클라이언트 그룹의 활성 인터페이스이며, FabricPool 클라이언트 그룹의 백업 인터페이스입니다.



활성 인터페이스에 오류가 발생하면 어떻게 됩니까**?**

현재 VIP 주소를 호스팅하는 인터페이스가 활성 인터페이스입니다. HA 그룹에 둘 이상의 인터페이스가 포함되어 있고 활성 인터페이스에 장애가 발생하면 VIP 주소는 우선순위에 따라 사용 가능한 첫 번째 백업 인터페이스로 이동합니다. 해당 인터페이스에 장애가 발생하면 VIP 주소는 다음으로 사용 가능한 백업 인터페이스로 이동하는 식으로 진행됩니다.

장애 조치는 다음과 같은 이유로 발생할 수 있습니다.

- 인터페이스가 구성된 노드가 다운됩니다.
- 인터페이스가 구성된 노드가 최소 2분 동안 다른 모든 노드와의 연결이 끊어집니다.
- 활성 인터페이스가 다운됩니다.
- 로드 밸런서 서비스가 중지됩니다.
- 고가용성 서비스가 중지됩니다.

> 활성 인터페이스를 호스팅하는 노드 외부의 네트워크 장애로 인해 페일오버가 발생하지 않을 수 있습니다. 마찬가지로, Grid Manager 또는 Tenant Manager 서비스로 인해 페일오버가 발생하지도 않습니다.

장애 조치 프로세스는 일반적으로 몇 초밖에 걸리지 않으며 매우 빠르기 때문에 클라이언트 애플리케이션은 거의 영향을 받지 않고 정상적인 재시도 동작을 통해 계속 작동할 수 있습니다.

장애가 해결되고 우선순위가 더 높은 인터페이스를 다시 사용할 수 있게 되면 VIP 주소는 자동으로 사용 가능한 가장 높은 우선순위 인터페이스로 이동됩니다.

StorageGRID HA 그룹이 고가용성을 제공하는 방법

고가용성(HA) 그룹을 사용하면 오브젝트 데이터 및 관리 용도로 StorageGRID에 대한 고가용성 연결을 제공할 수 있습니다.

- HA 그룹은 그리드 관리자 또는 테넌트 관리자에 고가용성 관리 연결을 제공할 수 있습니다.
- HA 그룹은 S3 클라이언트에 고가용성 데이터 연결을 제공할 수 있습니다.
- 인터페이스가 하나만 포함된 HA 그룹을 사용하면 여러 VIP 주소를 제공하고 IPv6 주소를 명시적으로 설정할 수 있습니다.

HA 그룹은 그룹에 포함된 모든 노드가 동일한 서비스를 제공하는 경우에만 고가용성을 제공할 수 있습니다. HA 그룹을 생성할 때는 필요한 서비스를 제공하는 노드 유형의 인터페이스를 추가해야 합니다.

- 관리자 노드: 로드 밸런서 서비스를 포함하고 Grid Manager 또는 Tenant Manager에 대한 액세스를 활성화합니다.
- 게이트웨이 노드: 로드 밸런서 서비스를 포함합니다.

HA 그룹의 목적	이 유형의 노드를 **HA** 그룹에 추가합니다**.**
Grid Manager 액세스	• 기본 관리자 노드 (**Primary**) • 비기본 관리 노드 참고**:** 기본 관리 노드는 기본 인터페이스여야 합니다. 일부 유지 관리 절차는 기본 관리 노드에서만 수행할 수 있습니다.
테넌트 관리자에 대한 액세스만 허용	• 기본 또는 비기본 관리 노드
S3 클라이언트 액세스 - 로드 밸런서 서비스	• 관리자 노드 • 게이트웨이 노드
S3 클라이언트 액세스("S3 Select"	• 서비스 어플라이언스 • VMware 기반 소프트웨어 노드 참고: S3 Select를 사용할 때는 HA 그룹을 사용하는 것이 좋지만 필수 사항은 아닙니다.

Grid Manager 또는 Tenant Manager에서 HA 그룹을 사용할 때의 제한 사항

그리드 관리자 또는 테넌트 관리자 서비스에 장애가 발생하면 HA 그룹 페일오버가 트리거되지 않습니다.

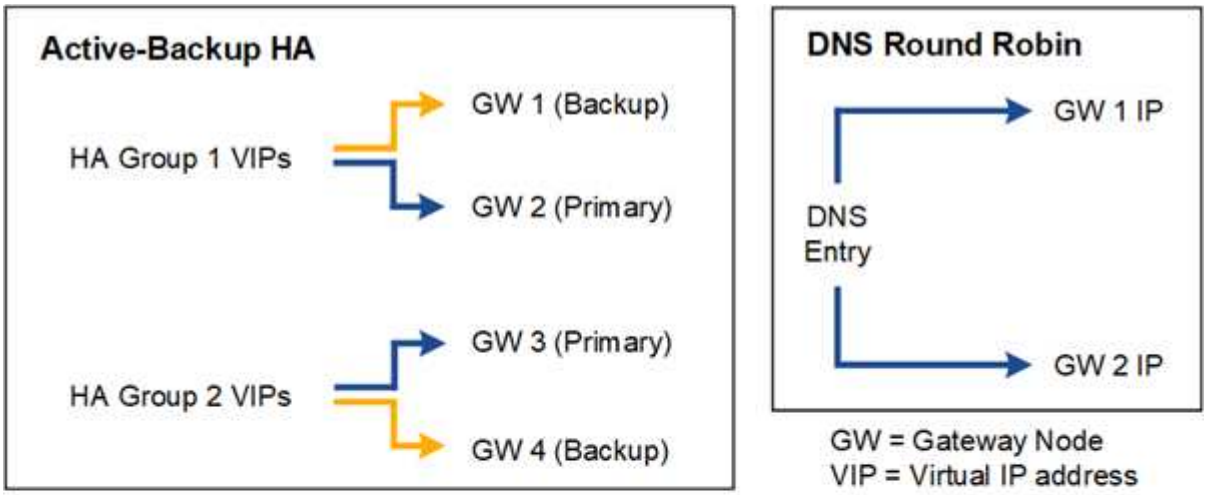
장애 조치가 발생할 때 Grid Manager 또는 테넌트 관리자에 로그인되어 있는 경우 로그아웃되므로 작업을 재개하려면 다시 로그인해야 합니다.

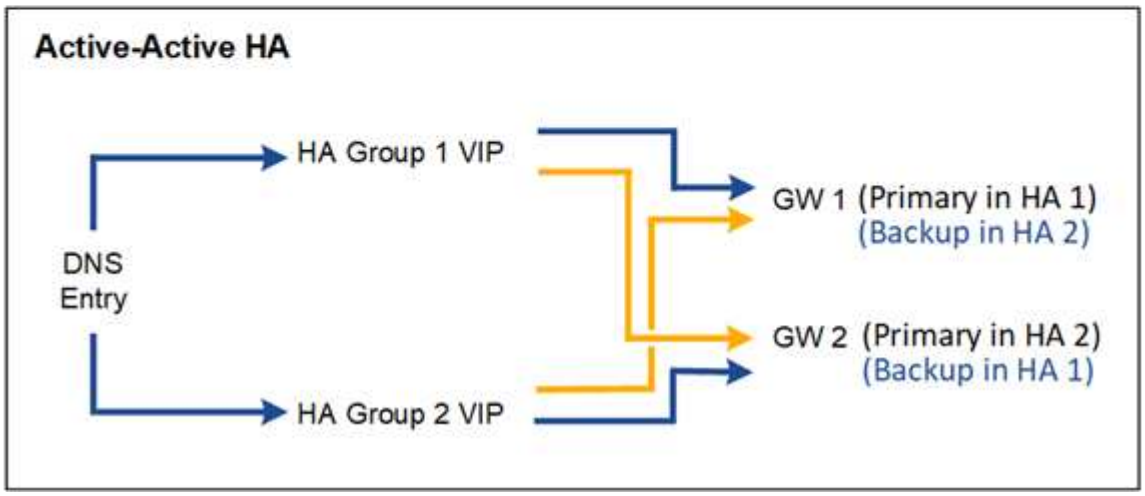
기본 관리 노드를 사용할 수 없는 경우 일부 유지 관리 절차를 수행할 수 없습니다. 장애 조치 중에는 Grid Manager를 사용하여 StorageGRID 시스템을 모니터링할 수 있습니다.

StorageGRID 고가용성 그룹의 구성 옵션

다음 다이어그램은 고가용성(HA) 그룹을 구성하는 다양한 방법을 보여주는 예시입니다. 각 옵션에는 장점과 단점이 있습니다.

다이어그램에서 파란색은 HA 그룹의 기본 인터페이스를 나타내고 노란색은 HA 그룹의 백업 인터페이스를 나타냅니다.





이 표는 다이어그램에 표시된 각 HA 구성의 이점을 요약합니다.

구성	장점	단점
액티브-백업 HA	• 외부 종속성 없이 StorageGRID에서 관리됩니다. • 빠른 장애 조치.	• HA 그룹에서는 하나의 노드만 활성화됩니다. 각 HA 그룹에는 최소 하나의 노드가 유휴 상태로 유지됩니다.

구성	장점	단점
DNS 라운드 로빈	• 전체 처리량 증가. • 유휴 호스트가 없습니다.	• 클라이언트 동작에 따라 달라질 수 있는 느린 페일오버. • StorageGRID 외부의 하드웨어 구성이 필요합니다. • 고객이 직접 수행하는 상태 점검이 필요합니다.
액티브-액티브 HA	• 트래픽은 여러 HA 그룹에 분산됩니다. • HA 그룹 수에 따라 확장되는 높은 총 처리량. • 빠른 장애 조치.	• 구성이 더 복잡합니다. • StorageGRID 외부의 하드웨어 구성이 필요합니다. • 고객이 직접 수행하는 상태 점검이 필요합니다.

StorageGRID에서 고가용성 그룹 구성

고가용성(HA) 그룹을 구성하여 관리 노드 또는 게이트웨이 노드의 서비스에 고가용성 액세스를 제공할 수 있습니다.

StorageGRID 시스템은 최대 255개의 HA 그룹을 가질 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"
- HA 그룹에서 VLAN 인터페이스를 사용하려면 VLAN 인터페이스를 생성해야 합니다. "VLAN 인터페이스 구성"을 참조하십시오.
- HA 그룹의 노드에 액세스 인터페이스를 사용하려면 인터페이스를 생성해야 합니다.
  - **Linux** (노드 설치 전): "노드 구성 파일 생성"
  - **Linux** (노드 설치 후): "노드에 트렁크 또는 액세스 인터페이스 추가"
  - **VMware** (노드 설치 후): "노드에 트렁크 또는 액세스 인터페이스 추가"

"Linux"는 RHEL, Ubuntu 또는 Debian 배포판을 의미합니다. 지원되는 버전 목록은 "NetApp 상호 운용성 매트릭스 툴(IMT)"을 참조하십시오.

고가용성 그룹 생성

고가용성 그룹을 생성할 때 하나 이상의 인터페이스를 선택하고 우선순위 순으로 정렬합니다. 그런 다음 그룹에 하나 이상의 VIP 주소를 할당합니다.

HA 그룹에 포함되려면 인터페이스는 게이트웨이 노드 또는 관리 노드용이어야 합니다. HA 그룹은 특정 노드에 대해 하나의 인터페이스만 사용할 수 있지만, 동일한 노드의 다른 인터페이스는 다른 HA 그룹에서 사용할 수 있습니다.

마법사에 액세스합니다

단계

1. 구성 > 네트워크 > *고가용성 그룹*을 선택하십시오.
2. *생성*을 선택합니다.

HA 그룹에 대한 세부 정보를 입력합니다.

단계

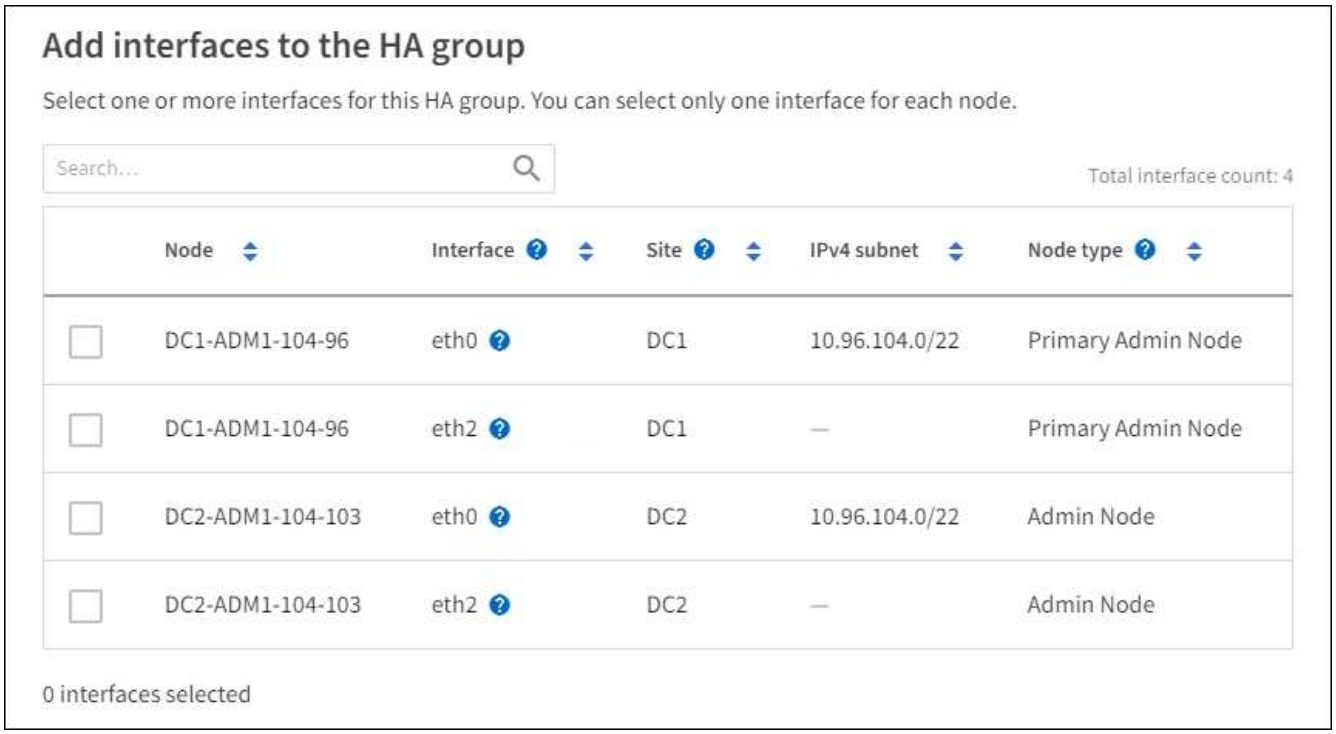
1. HA 그룹에 고유한 이름을 제공하십시오.
2. 선택적으로 HA 그룹에 대한 설명을 입력할 수 있습니다.
3. *Continue*를 선택합니다.

HA 그룹에 인터페이스 추가

단계

1. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

   열 머리글을 사용하여 행을 정렬하거나 검색어를 입력하여 인터페이스를 더 빠르게 찾을 수 있습니다.



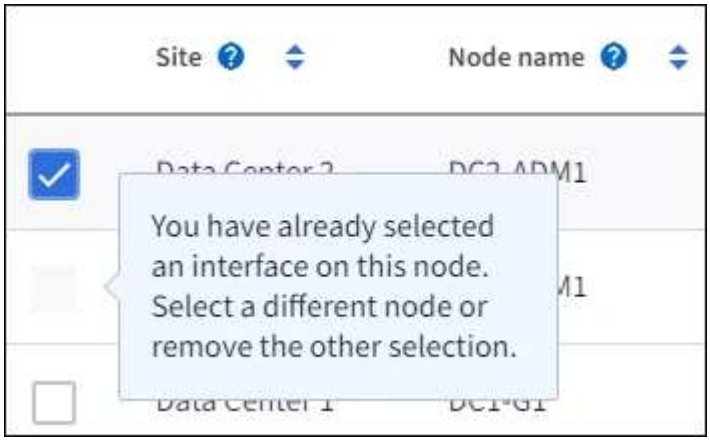
VLAN 인터페이스를 생성한 후 새 인터페이스가 테이블에 나타날 때까지 최대 5분 정도 기다리십시오.

인터페이스 선택 가이드라인

- 최소한 하나의 인터페이스를 선택해야 합니다.
- 노드당 하나의 인터페이스만 선택할 수 있습니다.
- HA 그룹이 Grid Manager 및 Tenant Manager를 포함한 관리 노드 서비스의 HA 보호를 위한 것이라면 관리

노드에서만 인터페이스를 선택하십시오.

- HA 그룹이 S3 클라이언트 트래픽의 HA 보호를 위한 것이라면 관리 노드, 게이트웨이 노드 또는 둘 다에서 인터페이스를 선택하십시오.
- 노드 유형이 다른 인터페이스를 선택하면 안내 메시지가 표시됩니다. 장애 조치가 발생할 경우 이전에 활성화된 노드에서 제공하던 서비스가 새로 활성화된 노드에서 사용 불가능할 수 있음을 알려줍니다. 예를 들어, 백업 게이트웨이 노드는 관리 노드 서비스에 대한 HA 보호 기능을 제공할 수 없습니다. 마찬가지로, 백업 관리 노드는 기본 관리 노드가 수행할 수 있는 모든 유지 관리 절차를 수행할 수 없습니다.
- 인터페이스를 선택할 수 없는 경우 해당 확인란이 비활성화된 것입니다. 도구 설명에서 자세한 정보를 확인할 수 있습니다.



- 서브넷 값이나 게이트웨이가 이미 선택된 다른 인터페이스와 충돌하는 경우 해당 인터페이스를 선택할 수 없습니다.
- 고정 IP 주소가 없는 경우 구성된 인터페이스를 선택할 수 없습니다.

2. *Continue*를 선택합니다.

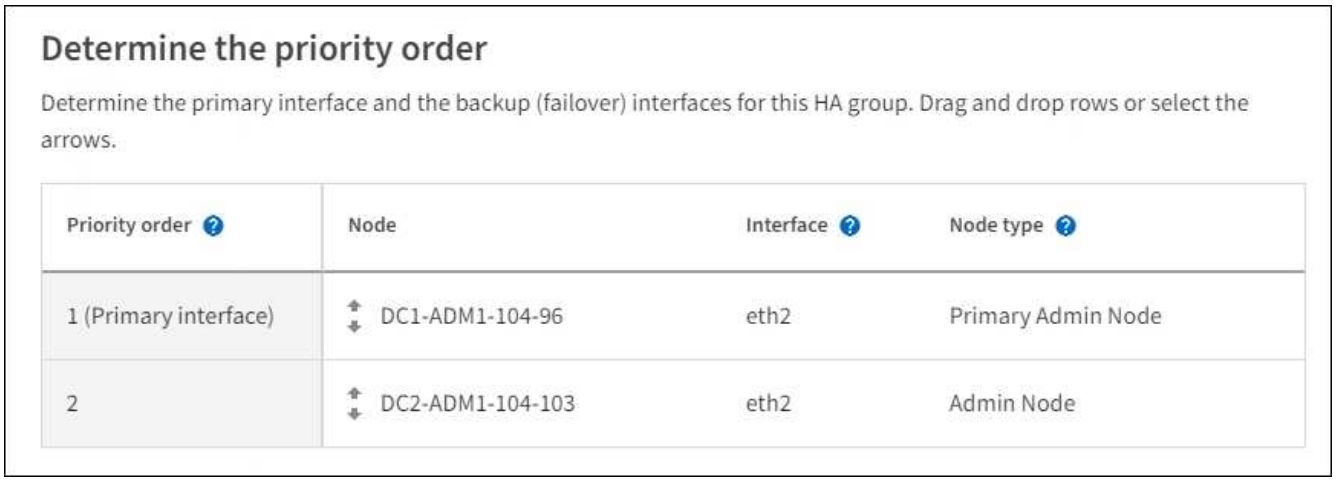
우선순위 결정

HA 그룹에 인터페이스가 두 개 이상 포함된 경우, 기본 인터페이스와 백업(장애 조치) 인터페이스를 지정할 수 있습니다. 기본 인터페이스에 장애가 발생하면 VIP 주소는 사용 가능한 가장 높은 우선순위의 인터페이스로 이동합니다. 해당 인터페이스에 장애가 발생하면 VIP 주소는 사용 가능한 다음으로 높은 우선순위의 인터페이스로 이동하는 식으로 진행됩니다.

단계

1. 우선순위 순서 열의 행을 드래그하여 기본 인터페이스와 백업 인터페이스를 지정하십시오.

   목록의 첫 번째 인터페이스가 기본 인터페이스입니다. 기본 인터페이스는 오류가 발생하지 않는 한 활성 인터페이스입니다.



HA 그룹이 Grid Manager에 대한 액세스 권한을 제공하는 경우, 기본 관리 노드에서 기본 인터페이스로 사용할 인터페이스를 선택해야 합니다. 일부 유지 관리 절차는 기본 관리 노드에서만 수행할 수 있습니다.

2. *Continue*를 선택합니다.

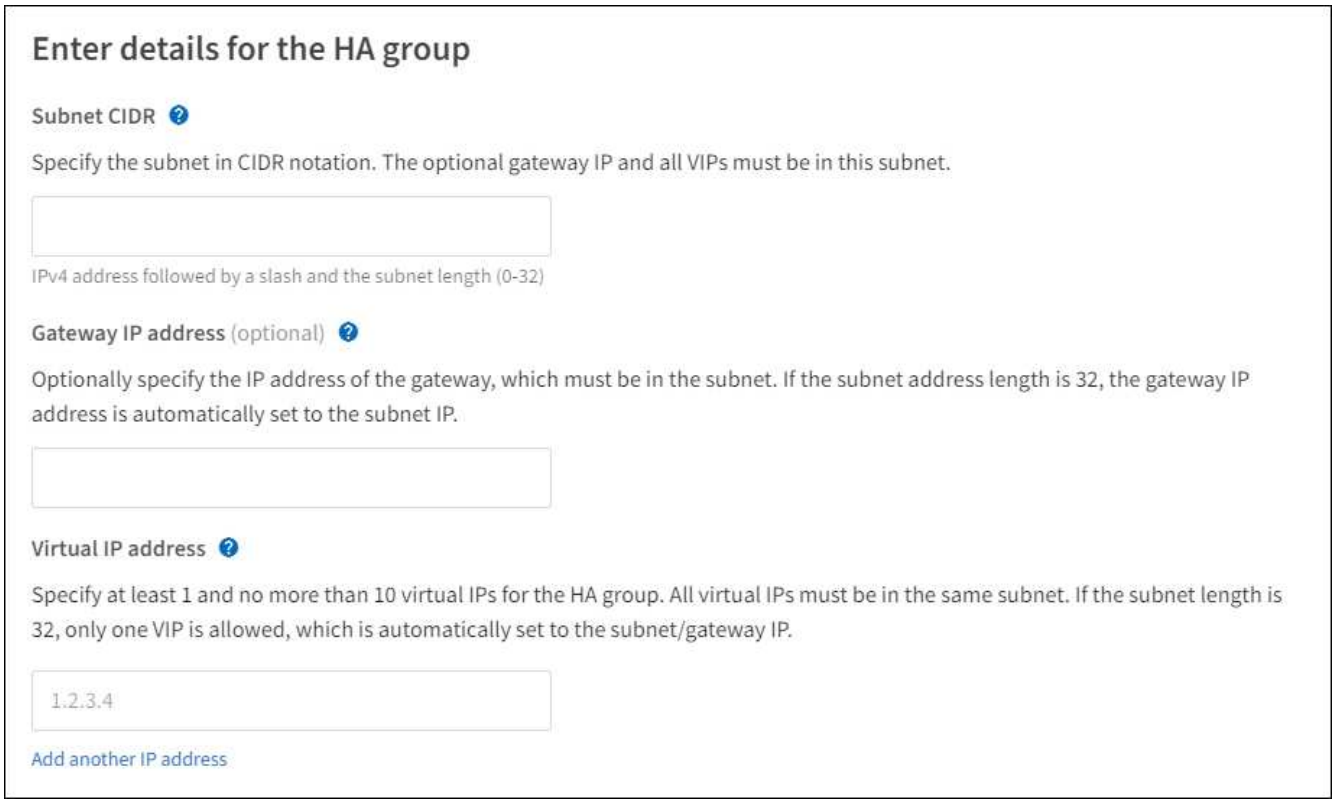
IP 주소를 입력합니다

단계

1. **Subnet CIDR** 필드에 VIP 서브넷을 CIDR 표기법(IPv4 주소 뒤에 슬래시와 서브넷 길이(0-32)를 입력)으로 지정합니다.

   네트워크 주소에는 호스트 비트가 설정되어 있으면 안 됩니다. 예를 들어, `192.16.0.0/22`.

   32비트 접두사를 사용하는 경우 VIP 네트워크 주소는 게이트웨이 주소 및 VIP 주소 역할도 겸합니다.



2. 선택적으로, S3 관리자 또는 테넌트 클라이언트가 다른 서브넷에서 이러한 VIP 주소에 액세스하는 경우 *게이트웨이 IP 주소*를 입력하십시오. 게이트웨이 주소는 VIP 서브넷 내에 있어야 합니다.

   클라이언트 및 관리자 사용자는 이 게이트웨이를 사용하여 가상 IP 주소에 액세스합니다.

3. HA 그룹의 활성 인터페이스에 대해 최소 1개, 최대 10개의 VIP 주소를 입력하십시오. 모든 VIP 주소는 VIP 서브넷 내에 있어야 하며, 활성 인터페이스에서 모든 VIP 주소가 동시에 활성화됩니다.

   최소 하나의 IPv4 주소를 제공해야 합니다. 선택적으로 추가적인 IPv4 및 IPv6 주소를 지정할 수 있습니다.

4. *HA 그룹 생성*을 선택하고 *완료*를 선택합니다.

   HA 그룹이 생성되었으며, 이제 구성된 가상 IP 주소를 사용할 수 있습니다.

다음 단계

이 HA 그룹을 로드 밸런싱에 사용할 경우, 포트와 네트워크 프로토콜을 결정하고 필요한 인증서를 첨부하기 위해 로드 밸런서 엔드포인트를 생성하십시오. "로드 밸런서 엔드포인트 구성"을 참조하십시오.

고가용성 그룹 편집

고가용성(HA) 그룹을 편집하여 이름과 설명을 변경하고, 인터페이스를 추가 또는 제거하고, 우선순위 순서를 변경하거나, 가상 IP 주소를 추가 또는 업데이트할 수 있습니다.

예를 들어, 사이트 또는 노드 폐기 절차에서 선택한 인터페이스와 연결된 노드를 제거하려면 HA 그룹을 편집해야 할 수 있습니다.

단계

1. 구성 > 네트워크 > *고가용성 그룹*을 선택하십시오.

   고가용성 그룹 페이지에는 기존의 모든 HA 그룹이 표시됩니다.

2. 편집하려는 HA 그룹의 확인란을 선택합니다.
3. 업데이트하려는 내용에 따라 다음 중 하나를 수행하세요.
   - VIP 주소를 추가하거나 제거하려면 작업 > *가상 IP 주소 편집*을 선택하십시오.
   - 그룹 이름이나 설명을 업데이트하거나, 인터페이스를 추가 또는 제거하거나, 우선순위 순서를 변경하거나, VIP 주소를 추가 또는 제거하려면 **Actions** > *Edit HA group*을 선택하십시오.
4. *가상 IP 주소 편집*을 선택한 경우:
   a. HA 그룹의 가상 IP 주소를 업데이트합니다.
   b. *저장*을 선택하세요.
   c. *완료*를 선택합니다.
5. *HA 그룹 편집*을 선택한 경우:
   a. 필요에 따라 그룹 이름이나 설명을 업데이트합니다.
   b. 선택적으로 체크박스를 선택하거나 선택 해제하여 인터페이스를 추가하거나 제거할 수 있습니다.

      HA 그룹이 Grid Manager에 대한 액세스 권한을 제공하는 경우, 기본 관리 노드에서 기본 인터페이스로 사용할 인터페이스를 선택해야 합니다. 일부 유지 관리 절차는 기본 관리 노드에서만 수행할 수 있습니다.

   c. 선택적으로 행을 드래그하여 이 HA 그룹의 기본 인터페이스와 백업 인터페이스의 우선 순위 순서를 변경할 수 있습니다.
   d. 필요에 따라 가상 IP 주소를 업데이트할 수 있습니다.
   e. *저장*을 선택한 다음 *완료*를 선택합니다.

고가용성 그룹 제거

한 번에 하나 이상의 고가용성(HA) 그룹을 제거할 수 있습니다.

HA 그룹이 로드 밸런서 엔드포인트에 바인딩된 경우 해당 그룹을 제거할 수 없습니다. HA 그룹을 삭제하려면 해당 그룹을 사용하는 모든 로드 밸런서 엔드포인트에서 그룹을 제거해야 합니다.

클라이언트 중단을 방지하려면 HA 그룹을 제거하기 전에 영향을 받는 S3 클라이언트 애플리케이션을 모두 업데이트하십시오. 각 클라이언트가 다른 IP 주소(예: 다른 HA 그룹의 가상 IP 주소 또는 설치 중에 인터페이스에 구성된 IP 주소)를 사용하여 연결하도록 업데이트하십시오.

단계

1. 구성 > 네트워크 > *고가용성 그룹*을 선택하십시오.
2. 제거하려는 각 HA 그룹의 로드 밸런서 엔드포인트 열을 검토하십시오. 로드 밸런서 엔드포인트가 나열되어 있는 경우:
   a. 구성 > 네트워크 > *로드 밸런서 엔드포인트*로 이동하세요.
   b. 엔드포인트의 확인란을 선택합니다.

c. 작업 > *엔드포인트 바인딩 모드 편집*을 선택합니다.

d. HA 그룹을 제거하도록 바인딩 모드를 업데이트합니다.

e. *변경 사항 저장*을 선택합니다.

3. 로드 밸런서 엔드포인트가 표시되지 않으면 제거하려는 각 HA 그룹에 대한 확인란을 선택하십시오.

4. 작업 > *HA 그룹 제거*를 선택합니다.

5. 메시지를 검토하고 *HA 그룹 삭제*를 선택하여 선택을 확인합니다.

선택한 모든 HA 그룹이 제거됩니다. 고가용성 그룹 페이지에 녹색 성공 배너가 나타납니다.

${post_edited_translations.segment}

StorageGRID 로드 밸런싱에 대해 알아보십시오

로드 밸런싱을 사용하여 S3 클라이언트의 데이터 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 워크로드를 여러 스토리지 노드에 분산시켜 속도와 연결 용량을 극대화합니다.

StorageGRID 로드 밸런싱 서비스는 모든 관리 노드와 모든 게이트웨이 노드에 설치되어 레이어 7 로드 밸런싱을 제공합니다. 이 서비스는 클라이언트 요청에 대한 전송 계층 보안(TLS) 종료를 수행하고, 요청을 검사하며, 스토리지 노드와의 새로운 보안 연결을 설정합니다.

각 노드의 로드 밸런싱 서비스는 클라이언트 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런싱 서비스는 가중치 부여 과정을 통해 CPU 가용성이 높은 스토리지 노드로 더 많은 요청을 라우팅합니다.

> StorageGRID Load Balancer 서비스가 권장되는 로드 밸런싱 메커니즘이지만, 타사 로드 밸런서를 통합할 수도 있습니다. 자세한 내용은 NetApp 계정 담당자에게 문의하거나 "StorageGRID에서 타사 로드 밸런서 사용"를 참조하십시오.

로드 밸런싱 노드는 몇 개가 필요합니까?

일반적으로 StorageGRID 시스템의 각 사이트에는 Load Balancer 서비스를 사용하는 노드가 두 개 이상 포함되어야 합니다. 예를 들어, 한 사이트에 게이트웨이 노드가 두 개 있거나 관리 노드와 게이트웨이 노드가 모두 포함될 수 있습니다. 서비스 어플라이언스, 베어메탈 노드 또는 가상 머신(VM) 기반 노드를 사용하는 경우, 각 로드 밸런싱 노드에 적합한 네트워킹, 하드웨어 또는 가상화 인프라가 갖춰져 있는지 확인하십시오.

로드 밸런서 엔드포인트란 무엇인가요?

로드 밸런서 엔드포인트는 클라이언트 애플리케이션의 수신 및 발신 요청이 로드 밸런서 서비스가 포함된 노드에 액세스하는 데 사용할 포트와 네트워크 프로토콜(HTTPS 또는 HTTP)을 정의합니다. 또한 엔드포인트는 클라이언트 유형(S3), 바인딩 모드, 그리고 선택적으로 허용 또는 차단된 테넌트 목록을 정의합니다.

로드 밸런서 엔드포인트를 생성하려면 Grid Manager를 사용하거나 S3 설정 및 FabricPool 마법사를 완료하십시오.

- "로드 밸런서 엔드포인트 구성"
- "S3 설정 마법사 사용"
- "FabricPool 설정 마법사 사용"

로드 밸런서 캐싱에 대한 고려 사항

캐싱은 워크로드가 데이터의 일부를 처리하고 객체에 여러 번 액세스할 때 성능을 크게 향상시킵니다. 또한 캐싱을 통해 전체 그리드 배포 없이도 객체 스토리지에 원격으로 액세스할 수 있습니다. 로드 밸런서 캐싱은 게이트웨이 노드에서만 사용할 수 있습니다.

로드 밸런서 엔드포인트를 생성할 때 다음 사항을 고려하세요.

- 캐시 가능한 워크로드에 대해서만 캐싱을 활성화하십시오. 캐시된 데이터보다 캐시되지 않은 데이터에 더 자주 액세스하는 워크로드는 캐시를 사용하지 않을 때보다 성능이 저하될 수 있습니다. 경우에 따라 덮어쓰기 및 삭제 빈도가 높은 워크로드는 드라이브의 보증된 쓰기 내구성을 초과할 수도 있습니다.
- 캐싱에 적합한 개별 워크로드를 캐싱하기 위해 추가 엔드포인트 또는 노드를 추가하는 것을 고려하십시오.
- 캐시 가능한 워크로드와 캐시 불가능한 워크로드에 대해 서로 다른 엔드포인트를 사용하십시오. 이러한 분리를 통해 캐싱 메커니즘이 적절하게 적용되고 캐시 불가능한 데이터 처리와 충돌하지 않도록 할 수 있습니다.
- 캐시가 활성화된 엔드포인트로 워크로드를 전송하여 캐시 가능 여부를 평가합니다. 캐시 적중률을 모니터링하고 검증하여 워크로드의 캐싱 적합성을 판단합니다. 이러한 평가를 통해 성능을 최적화하고 캐시 리소스를 효율적으로 활용할 수 있습니다.
- "감사 로그 검토"기존 워크로드가 캐싱에 적합한지 판단합니다. 특정 기간 동안 GET 요청 중 고유 객체에 대한 요청의 비율을 확인합니다. 캐싱에 적합하려면 이 값이 50% 미만이어야 합니다.

캐싱에 적합한 워크로드의 예시

- 데이터 레이크
- 고성능 컴퓨팅(HPC)
- AI/ML 교육
- 콘텐츠 전송 네트워크(CDN)
- 미디어 자산 관리
- 영상 제작

- 여러 객체 버전을 캐시할 수 있습니다.
- 범위 읽기 작업이 지원됩니다.

캐싱에 적합하지 않은 워크로드의 예

- FabricPool
- 백업 애플리케이션
- 스토리지 계층화

캐시에서 제공될 콘텐츠 중 저장 시 암호화가 필요한 콘텐츠가 있는 경우, "노드 또는 드라이브 암호화 활성화" 캐시 노드에서.

캐시되지 않는 객체 및 요청 유형

- The `response-content-encoding` 쿼리 매개변수
- The `partNumber` 쿼리 매개변수
- 조건부 헤더
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- 다음과 같은 방법으로 저장 시 암호화된 요청:
  - SSE(StorageGRID 관리 키를 사용하는 서버 측 암호화)
  - SSE-C(고객이 제공한 키를 사용하는 서버 측 암호화)
  - 저장된 객체 암호화

캐시되지 않은 요청은 캐시가 활성화되지 않은 것처럼 상위 LDR로 전달됩니다.

관련 정보

- "로드 밸런서 캐싱 문제 해결"
- 로드 밸런서 캐싱에 대한 자세한 내용은 기술 지원 부서에 문의하십시오.

포트에 대한 고려 사항

로드 밸런서 엔드포인트의 기본 포트는 처음 생성하는 경우 10433으로 설정되지만, 1에서 65535 사이의 사용되지 않는 외부 포트를 지정할 수 있습니다. 포트 80 또는 443을 사용하는 경우 해당 엔드포인트는 게이트웨이 노드의 로드 밸런서 서비스만 사용하게 됩니다. 이러한 포트는 관리 노드에서 예약되어 있습니다. 둘 이상의 엔드포인트에 동일한 포트를 사용하는 경우 각 엔드포인트에 대해 서로 다른 바인딩 모드를 지정해야 합니다.

다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. "StorageGRID 내부 포트"을 참조하십시오.

네트워크 프로토콜 고려 사항

대부분의 경우 클라이언트 애플리케이션과 StorageGRID 간의 연결에는 TLS(전송 계층 보안) 암호화를 사용해야 합니다. TLS 암호화 없이 StorageGRID에 연결하는 것은 지원되지만, 특히 운영 환경에서는 권장하지 않습니다. StorageGRID 로드 밸런서 엔드포인트에 사용할 네트워크 프로토콜을 선택할 때는 *HTTPS*를 선택하십시오.

로드 밸런서 엔드포인트 인증서에 대한 고려 사항

로드 밸런서 엔드포인트의 네트워크 프로토콜로 *HTTPS*를 선택하는 경우 보안 인증서를 제공해야 합니다. 로드 밸런서 엔드포인트를 생성할 때 다음 세 가지 옵션 중 하나를 사용할 수 있습니다.

- 서명된 인증서를 업로드하세요(권장). 이 인증서는 공개적으로 신뢰할 수 있는 CA 또는 사설 인증 기관(CA)에서 서명할 수 있습니다. 연결 보안을 위해 공개적으로 신뢰할 수 있는 CA 서버 인증서를 사용하는 것이 가장 좋습니다. 생성된 인증서와 달리 CA에서 서명한 인증서는 서비스 중단 없이 갱신할 수 있으므로 만료 문제를 방지하는 데 도움이 됩니다.

  로드 밸런서 엔드포인트를 생성하기 전에 다음 파일들을 확보해야 합니다.

- 사용자 지정 서버 인증서 파일입니다.
- 사용자 지정 서버 인증서 개인 키 파일입니다.
- 선택적으로, 각 중간 발급 인증 기관의 인증서를 묶은 CA 번들을 제공할 수 있습니다.

- 자체 서명 인증서를 생성합니다.
- 글로벌 **StorageGRID S3** 인증서를 사용하십시오. 로드 밸런서 엔드포인트에 이 인증서를 선택하려면 먼저 이 인증서의 사용자 지정 버전을 업로드하거나 생성해야 합니다. 을 참조하십시오. "S3 API 인증서 구성"

어떤 값이 필요합니까?

인증서를 생성하려면 S3 클라이언트 애플리케이션이 엔드포인트에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소를 알고 있어야 합니다.

인증서의 주체 **DN**(고유 이름) 항목에는 클라이언트 애플리케이션이 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 들어, `.storagegrid.example.com` 와일드카드를 사용하여 `adm1.storagegrid.example.com` 및 `gn1.storagegrid.example.com`을 나타냅니다.

S3 가상 호스팅 스타일 요청을 사용할 계획이라면, 인증서에는 구성한 각 "S3 엔드포인트 도메인 이름"에 대한 대체 이름 항목(와일드카드 이름 포함)도 포함되어야 합니다. 예를 들면 다음과 같습니다.

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

도메인 이름에 와일드카드를 사용하는 경우 "서버 인증서 보안 강화 지침"을(를) 검토하십시오.

보안 인증서에 있는 각 이름에 대해 DNS 항목을 정의해야 합니다.

만료 예정인 인증서는 어떻게 관리하나요?

S3 애플리케이션과 StorageGRID 간의 연결을 보호하는 데 사용된 인증서가 만료되면 애플리케이션이 일시적으로 StorageGRID에 대한 액세스를 잃을 수 있습니다.

인증서 만료 문제를 방지하려면 다음 모범 사례를 따르십시오.

- 로드 밸런서 엔드포인트 인증서 만료 및 **S3 API**용 글로벌 서버 인증서 만료 알림과 같이 인증서 만료일이 임박했음을 경고하는 모든 알림을 주의 깊게 모니터링하십시오.
- StorageGRID 와 S3 애플리케이션의 인증서 버전을 항상 동기화 상태로 유지하십시오. 로드 밸런서 엔드포인트에 사용되는 인증서를 교체하거나 갱신하는 경우, S3 애플리케이션에서 사용하는 해당 인증서도 교체하거나 갱신해야 합니다.
- 공개적으로 서명된 CA 인증서를 사용하십시오. CA가 서명한 인증서를 사용하면 만료가 임박한 인증서를 서비스 중단 없이 교체할 수 있습니다.

- 자체 서명된 StorageGRID 인증서를 생성했고 해당 인증서의 만료일이 임박한 경우, 기존 인증서가 만료되기 전에 StorageGRID와 S3 애플리케이션 모두에서 수동으로 인증서를 교체해야 합니다.

결합 모드에 대한 고려 사항

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

다음 바인딩 모드 중 하나를 지정할 수 있습니다.

- 전역(기본값): 클라이언트 애플리케이션은 모든 게이트웨이 노드 또는 관리 노드의 IP 주소, 모든 네트워크의 모든 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 엔드포인트에 액세스할 수 있습니다. 엔드포인트의 액세스를 제한해야 하는 경우가 아니면 이 설정을 사용하십시오.
- **HA** 그룹의 가상 **IP** 주소. 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
- 노드 인터페이스. 클라이언트는 선택된 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
- 노드 유형. 선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN) 또는 게이트웨이 노드의 IP 주소(또는 해당 FQDN) 중 하나를 사용해야 합니다.

테넌트 액세스 관련 고려 사항

테넌트 액세스는 StorageGRID 테넌트 계정 중 어떤 계정이 로드 밸런서 엔드포인트를 사용하여 버킷에 액세스할 수 있는지 제어할 수 있는 선택적 보안 기능입니다. 모든 테넌트가 엔드포인트에 액세스할 수 있도록 허용(기본값)하거나, 각 엔드포인트에 대해 허용 또는 차단할 테넌트 목록을 지정할 수 있습니다.

이 기능을 사용하면 테넌트와 해당 엔드포인트 간의 보안 격리를 강화할 수 있습니다. 예를 들어, 이 기능을 사용하여 한 테넌트가 소유한 일급 비밀 또는 고도로 기밀인 자료가 다른 테넌트에게 완전히 액세스되지 않도록 할 수 있습니다.

> 액세스 제어를 위해 테넌트는 클라이언트 요청에 사용된 액세스 키를 기준으로 결정됩니다. 요청의 일부로 액세스 키가 제공되지 않은 경우(익명 액세스와 같이) 버킷 소유자를 사용하여 테넌트를 결정합니다.

테넌트 액세스 예시

이 보안 기능이 어떻게 작동하는지 이해하려면 다음 예를 살펴보십시오.

1. 다음과 같이 두 개의 로드 밸런싱 엔드포인트를 생성했습니다.
   - **Public** 엔드포인트: 포트 10443을 사용하며 모든 테넌트에 대한 액세스를 허용합니다.
   - 극비 엔드포인트: 포트 10444를 사용하며 극비 테넌트만 액세스할 수 있습니다. 다른 모든 테넌트는 이 엔드포인트에 액세스할 수 없습니다.
2. The `top-secret.pdf`은(는) 극비 테넌트가 소유한 버킷에 있습니다.

`top-secret.pdf`에 액세스하기 위해 *극비* 테넌트의 사용자는 `\https://w.x.y.z:10444/top-secret.pdf`에 GET 요청을 보낼 수 있습니다. 이 테넌트는 10444 엔드포인트를 사용할 수 있도록 허용되어 있으므로 사용자는 해당 객체에 액세스할 수 있습니다. 그러나 다른 테넌트에 속한 사용자가 동일한 URL로 동일한 요청을 보내면 즉시 액세스 거부 메시지가 표시됩니다. 자격 증명과 서명이 유효한 경우에도 액세스가 거부됩니다.

CPU 가용성

각 관리 노드와 게이트웨이 노드의 로드 밸런서 서비스는 스토리지 노드로 S3 트래픽을 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중치 부여 과정을 통해 CPU 가용성이 높은 스토리지 노드로 더 많은 요청을 라우팅합니다. 노드 CPU 부하 정보는 몇 분마다 업데이트되지만, 가중치는 더 자주 업데이트될 수 있습니다. 모든 스토리지 노드에는 최소 기본 가중치 값이 할당되며, 노드의 사용률이 100%이거나 사용률을 보고하지 않는 경우에도 마찬가지입니다.

경우에 따라 CPU 가용성에 대한 정보는 로드 밸런서 서비스가 위치한 사이트로 제한될 수 있습니다.

StorageGRID 로드 밸런서 엔드포인트를 구성합니다

로드 밸런서 엔드포인트는 S3 클라이언트가 게이트웨이 및 관리 노드의 StorageGRID 로드 밸런서에 연결할 때 사용할 수 있는 포트와 네트워크 프로토콜을 결정합니다. 엔드포인트를 사용하여 Grid Manager, Tenant Manager 또는 둘 다에 액세스할 수도 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"
- "로드 밸런싱 고려 사항"를 검토했습니다.
- 이전에 로드 밸런서 엔드포인트에 사용할 포트를 다시 매핑한 경우, "포트 리맵핑을 제거했습니다.".
- 사용할 고가용성(HA) 그룹을 생성했습니다. HA 그룹은 권장 사항이지만 필수 사항은 아닙니다. "고가용성 그룹 관리"을 참조하십시오.
- 로드 밸런서 엔드포인트를 "S3 Select용 S3 테넌트"에서 사용할 경우, 베어메탈 노드의 IP 주소 또는 FQDN을 사용해서는 안 됩니다. S3 Select에 사용되는 로드 밸런서 엔드포인트에는 서비스 어플라이언스 및 VMware 기반 소프트웨어 노드만 허용됩니다.
- 사용할 VLAN 인터페이스를 모두 구성했습니다. "VLAN 인터페이스 구성"을 참조하십시오.
- HTTPS 엔드포인트를 생성하는 경우(권장), 서버 인증서에 대한 정보가 있어야 합니다.

  엔드포인트 인증서 변경 사항이 모든 노드에 적용되는 데 최대 15분이 소요될 수 있습니다.

  - 인증서를 업로드하려면 서버 인증서, 인증서 개인 키, 그리고 선택적으로 CA 번들이 필요합니다.
  - 인증서를 생성하려면 S3 클라이언트가 엔드포인트에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소가 필요합니다. 또한 주체(고유 이름)도 알아야 합니다.
  - StorageGRID S3 API 인증서(스토리지 노드에 직접 연결하는 데에도 사용 가능)를 사용하려면 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 이미 교체해야 합니다. "S3 API 인증서 구성"을

참조하십시오.

로드 밸런서 엔드포인트 생성

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

마법사에 액세스합니다

단계

1. 구성 > 네트워크 > *로드 밸런서 엔드포인트*를 선택합니다.
2. S3 클라이언트용 엔드포인트를 생성하려면 **S3** 클라이언트 탭을 선택합니다.
3. Grid Manager, Tenant Manager 또는 둘 다에 액세스할 수 있는 엔드포인트를 생성하려면 관리 인터페이스 탭을 선택하십시오.
4. *생성*을 선택합니다.

엔드포인트 세부 정보를 입력합니다

단계

1. 생성하려는 엔드포인트 유형에 대한 세부 정보를 입력하려면 적절한 지침을 선택하십시오.

S3 클라이언트

필드	설명
이름	로드 밸런서 엔드포인트 페이지의 표에 표시될 엔드포인트에 대한 설명적인 이름입니다.
포트	로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드는 처음 생성하는 엔드포인트의 경우 기본값으로 10433이 설정되지만, 1에서 65535 사이의 사용되지 않는 외부 포트를 입력할 수 있습니다. **80** 또는 *8443*을 입력하면, 포트 8443을 사용 가능한 상태로 확보하지 않은 경우 게이트웨이 노드에만 엔드포인트가 구성됩니다. 그러면 포트 8443을 S3 엔드포인트로 사용할 수 있으며, 해당 포트는 게이트웨이 노드와 관리 노드 모두에 구성됩니다.
클라이언트 유형	*S3*이어야 합니다.
네트워크 프로토콜	클라이언트가 이 엔드포인트에 연결할 때 사용할 네트워크 프로토콜입니다. • 안전한 TLS 암호화 통신을 위해서는 *HTTPS*를 선택하십시오(권장). 엔드포인트를 저장하기 전에 보안 인증서를 연결해야 합니다. • 덜 안전한 암호화되지 않은 통신을 위해 *HTTP*를 선택하십시오. HTTP는 운영 환경이 아닌 그리드에서만 사용하십시오.
캐싱 활성화	이 로드 밸런서 엔드포인트에 대해 "게이트웨이 노드에서의 캐싱"을(를) 활성화 또는 비활성화합니다. 캐싱 관련 문제가 발생하는 경우, "로드 밸런서 캐싱 문제 해결"을 참조하십시오.

관리 인터페이스

필드	설명
이름	로드 밸런서 엔드포인트 페이지의 표에 표시될 엔드포인트에 대한 설명적인 이름입니다.
포트	Grid Manager, 테넌트 Manager 또는 둘 다에 액세스하는 데 사용할 StorageGRID 포트입니다. • Grid Manager: **8443** • 테넌트 관리자: **9443** • Grid Manager 및 Tenant Manager 모두: **443** 참고: 이러한 사전 설정 포트 또는 사용 가능한 다른 포트를 사용할 수 있습니다.
인터페이스 유형	이 엔드포인트를 사용하여 액세스할 StorageGRID 인터페이스에 해당하는 라디오 버튼을 선택하십시오.

필드	설명
신뢰할 수 없는 클라이언트 네트워크	이 엔드포인트를 신뢰할 수 없는 클라이언트 네트워크에서 액세스할 수 있도록 하려면 *예*를 선택하십시오. 그렇지 않으면 *아니요*를 선택하십시오. '예'를 선택하면 신뢰할 수 없는 모든 클라이언트 네트워크에서 해당 포트가 열립니다. 참고: 로드 밸런서 엔드포인트를 생성할 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 방식을 제어할 수 있습니다.

   클라이언트 엔드포인트 또는 관리 인터페이스 엔드포인트에 대해 몇 가지 바인딩 모드를 사용할 수 있습니다. 두 엔드포인트 유형에 대한 모든 모드는 여기에 나열되어 있습니다.

모드	설명
전역(클라이언트 엔드포인트의 기본값)	클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크상의 HA 그룹의 가상 IP(VIP) 주소, 또는 해당 FQDN을 사용하여 엔드포인트에 액세스할 수 있습니다. 이 엔드포인트의 접근성을 제한해야 하는 경우가 아니라면 전역 설정을 사용하십시오.
HA 그룹의 가상 IP	클라이언트는 이 엔드포인트에 액세스하기 위해 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용해야 합니다. 이 바인딩 모드를 사용하는 엔드포인트는 선택한 HA 그룹이 서로 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.
노드 인터페이스	클라이언트는 이 엔드포인트에 액세스하기 위해 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
노드 유형(클라이언트 엔드포인트만 해당)	선택한 노드 유형에 따라 클라이언트는 이 엔드포인트에 액세스하기 위해 관리 노드의 IP 주소(또는 해당 FQDN) 또는 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
모든 관리 노드(관리 인터페이스 엔드포인트의 기본값)	클라이언트는 이 엔드포인트에 액세스하기 위해 관리 노드의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.

   둘 이상의 엔드포인트가 동일한 포트를 사용하는 경우 StorageGRID는 다음 우선순위 순서를 사용하여 사용할

엔드포인트를 결정합니다. **HA** 그룹의 가상 **IP** > 노드 인터페이스 > 노드 유형 > 전역.

관리 인터페이스 엔드포인트를 생성하는 경우 관리자 노드만 허용됩니다.

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

   관리 인터페이스 엔드포인트를 생성하는 경우, 관리자 노드에만 연결된 VIP를 선택하십시오.

3. *노드 인터페이스*를 선택한 경우, 이 엔드포인트와 연결할 각 관리 노드 또는 게이트웨이 노드에 대해 하나 이상의 노드 인터페이스를 선택하십시오.
4. *노드 유형*을 선택한 경우, 기본 관리 노드와 모든 비기본 관리 노드를 포함하는 관리 노드 또는 게이트웨이 노드를 선택하십시오.

테넌트 액세스 제어

관리 인터페이스 엔드포인트는 해당 엔드포인트에 테넌트 관리자의 인터페이스 유형이(가) 있는 경우에만 테넌트 액세스를 제어할 수 있습니다.

단계

1. 테넌트 액세스 단계에서는 다음 중 하나를 선택하십시오.

필드	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 버킷에 액세스할 수 있습니다. 아직 테넌트 계정을 생성하지 않은 경우 이 옵션을 선택해야 합니다. 테넌트 계정을 추가한 후에는 로드 밸런서 엔드포인트를 편집하여 특정 계정을 허용하거나 차단할 수 있습니다.
선택한 테넌트 허용	선택된 테넌트 계정만 이 엔드포인트를 사용하여 자신의 버킷에 액세스할 수 있습니다.
선택한 테넌트 차단	선택된 테넌트 계정은 이 엔드포인트를 사용하여 버킷에 액세스할 수 없습니다. 다른 모든 테넌트는 이 엔드포인트를 사용할 수 있습니다.

2. HTTP 엔드포인트를 생성하는 경우 인증서를 연결할 필요가 없습니다. 새 로드 밸런서 엔드포인트를 추가하려면 *생성*을 선택합니다. 그런 다음 완료한 후으로 이동합니다. 그렇지 않으면 인증서를 연결하려면 *계속*을 선택합니다.

인증서 첨부

단계

1. HTTPS 엔드포인트를 생성하는 경우, 엔드포인트에 연결할 보안 인증서 유형을 선택하십시오.

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

   - 인증서 업로드. 사용자 지정 인증서를 업로드하려면 이 옵션을 선택하십시오.
   - 인증서 생성. 사용자 지정 인증서를 생성하는 데 필요한 값이 있는 경우 이 옵션을 선택하십시오.

- **StorageGRID S3** 인증서 사용. 이 옵션을 선택하면 스토리지 노드에 직접 연결하는 데에도 사용할 수 있는 글로벌 S3 API 인증서를 사용할 수 있습니다.

  그리드 CA에서 서명한 기본 S3 API 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체하지 않은 경우 이 옵션을 선택할 수 없습니다. "S3 API 인증서 구성"을 참조하십시오.

- 관리 인터페이스 인증서 사용. 전역 관리 인터페이스 인증서를 사용하려면 이 옵션을 선택하십시오. 이 인증서는 관리 노드에 직접 연결하는 데에도 사용할 수 있습니다.

2. StorageGRID S3 인증서를 사용하지 않는 경우 인증서를 업로드하거나 생성하십시오.

인증서 업로드

a. *인증서 업로드*를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

- 서버 인증서: PEM 인코딩 형식의 사용자 지정 서버 인증서 파일입니다.
- 인증서 개인 키: 사용자 지정 서버 인증서 개인 키 파일 (`.key`).

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

- **CA** 번들: 각 중간 발급 인증 기관(CA)의 인증서가 포함된 단일 선택적 파일입니다. 이 파일에는 각 CA 인증서 파일이 PEM 형식으로 인코딩되어 인증서 체인 순서대로 연결되어 있어야 합니다.

c. *인증서 세부 정보*를 펼치면 업로드한 각 인증서의 메타데이터를 볼 수 있습니다. 선택적으로 CA 번들을 업로드한 경우 각 인증서가 별도의 탭에 표시됩니다.

- 인증서 파일을 저장하려면 *인증서 다운로드*를 선택하고, 인증서 번들을 저장하려면 *CA 번들 다운로드*를 선택하십시오.

  인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

  예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

- 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 인증서 **PEM** 복사 또는 *CA 번들 PEM 복사*를 선택하십시오.

d. *생성*을 선택합니다. + 로드 밸런서 엔드포인트가 생성됩니다. 사용자 지정 인증서는 S3 클라이언트 또는 관리 인터페이스와 엔드포인트 간의 모든 후속 새 연결에 사용됩니다.

인증서 생성

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

필드	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내려면 와일드카드 문자 *를 사용하십시오.
IP	인증서에 포함할 IP 주소를 하나 이상 입력하십시오.
제목 (선택 사항)	X.509 인증서 소유자의 주체 또는 고유명칭(DN). 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 주체 공통 이름(CN)으로 사용합니다.
유효 기간	인증서 발급일로부터 만료일까지의 일수입니다.

필드	설명
키 사용 확장 추가	선택된 경우(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다. 이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다. 참고: 인증서에 이러한 확장이 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택한 상태로 두십시오.

c. *생성*을 선택합니다.

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

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

     인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.

e. *생성*을 선택합니다.

   로드 밸런서 엔드포인트가 생성되었습니다. 사용자 지정 인증서는 S3 클라이언트 또는 관리 인터페이스와 이 엔드포인트 간의 모든 후속 새 연결에 사용됩니다.

완료한 후

단계

1. DNS를 사용하는 경우 클라이언트가 연결할 때 사용할 각 IP 주소에 StorageGRID의 정규화된 도메인 이름(FQDN)을 연결하는 레코드가 DNS에 포함되어 있는지 확인하십시오.

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

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

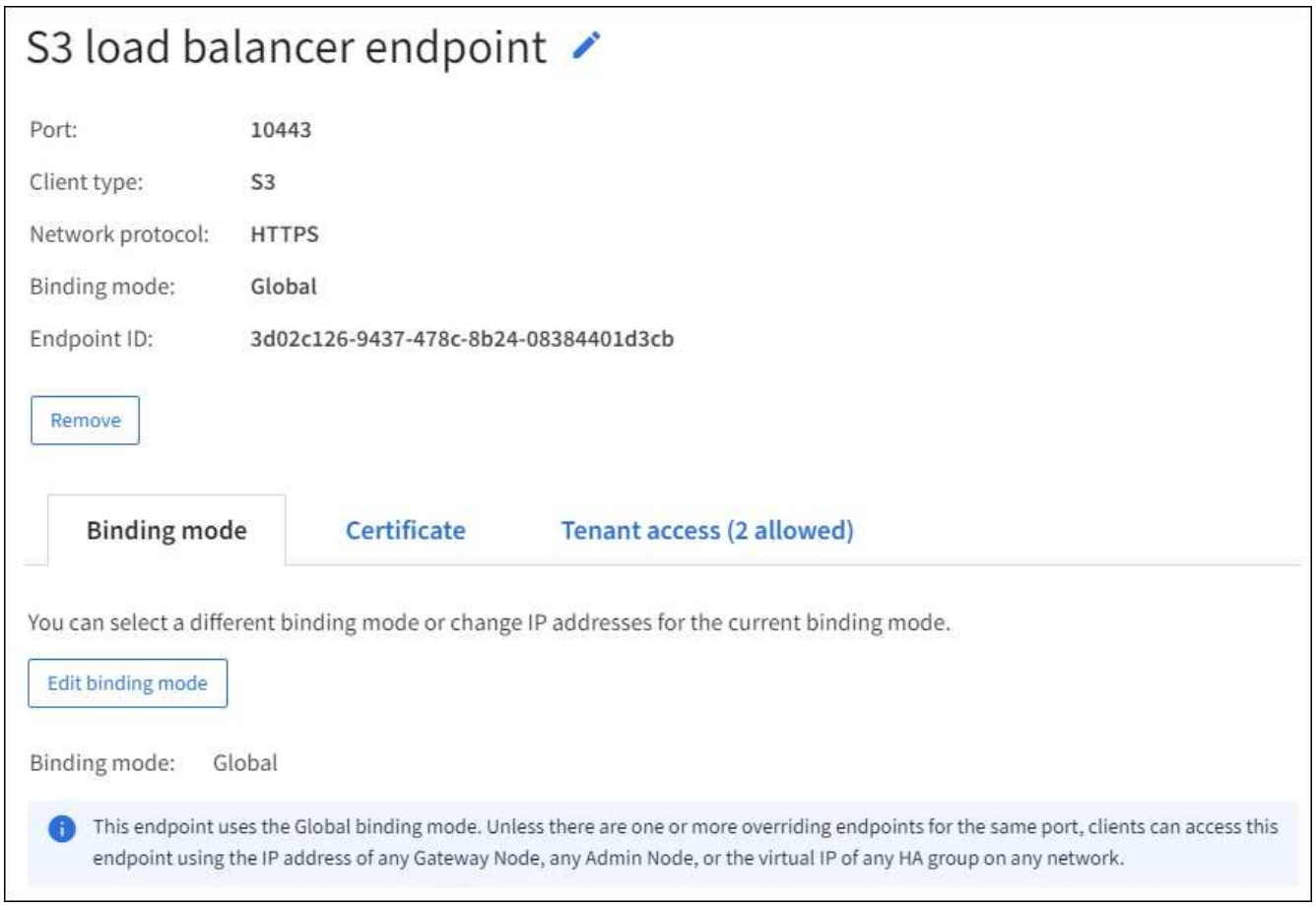
     또한 DNS 레코드에 와일드카드 이름을 포함하여 필요한 모든 엔드포인트 도메인 이름이 참조되어 있는지 확인해야 합니다.

2. S3 클라이언트가 엔드포인트에 연결하는 데 필요한 정보를 제공합니다.
   - 포트 번호
   - 정규화된 도메인 이름 또는 IP 주소
   - 필요한 인증서 세부 정보

로드 밸런서 엔드포인트 보기 및 편집

기존 로드 밸런서 엔드포인트에 대한 세부 정보를 볼 수 있으며, 여기에는 보안 엔드포인트의 인증서 메타데이터도 포함됩니다. 엔드포인트의 특정 설정을 변경할 수도 있습니다.

- 모든 로드 밸런서 엔드포인트에 대한 기본 정보를 보려면 로드 밸런서 엔드포인트 페이지의 표를 참조하십시오.
- 인증서 메타데이터를 포함하여 특정 엔드포인트에 대한 모든 세부 정보를 보려면 표에서 해당 엔드포인트 이름을 선택하십시오. 표시되는 정보는 엔드포인트 유형 및 구성 방식에 따라 다릅니다.



- 엔드포인트를 편집하려면 로드 밸런서 엔드포인트 페이지의 작업 메뉴를 사용하십시오.

관리 인터페이스 엔드포인트의 포트를 편집하는 동안 Grid Manager에 대한 액세스 권한을 잃은 경우, URL과 포트를 업데이트하여 액세스 권한을 다시 확보하십시오.

엔드포인트를 편집한 후 변경 사항이 모든 노드에 적용되는 데 최대 15분이 소요될 수 있습니다.

작업	작업 메뉴	상세 정보 페이지
엔드포인트 이름 편집	a. 엔드포인트의 확인란을 선택합니다. b. 작업 > *엔드포인트 이름 편집*을 선택합니다. c. 새 이름을 입력합니다. d. *저장*을 선택하세요.	a. 세부 정보를 표시하려면 엔드포인트 이름을 선택하세요. b. 편집 아이콘 을 선택합니다. c. 새 이름을 입력합니다. d. *저장*을 선택하세요.
엔드포인트 포트 편집	a. 엔드포인트의 확인란을 선택합니다. b. 작업 > *엔드포인트 포트 편집*을 선택합니다. c. 유효한 포트 번호를 입력하세요. d. *저장*을 선택하세요.	해당 없음
엔드포인트 바인딩 모드 편집	a. 엔드포인트의 확인란을 선택합니다. b. 작업 > *엔드포인트 바인딩 모드 편집*을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트하십시오. d. *변경 사항 저장*을 선택합니다.	a. 세부 정보를 표시하려면 엔드포인트 이름을 선택하세요. b. *바인딩 모드 편집*을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트하십시오. d. *변경 사항 저장*을 선택합니다.
엔드포인트 인증서 편집	a. 엔드포인트의 확인란을 선택합니다. b. 작업 > *엔드포인트 인증서 편집*을 선택합니다. c. 필요에 따라 새 사용자 지정 인증서를 업로드하거나 생성하거나, 글로벌 S3 인증서를 사용하기 시작합니다. d. *변경 사항 저장*을 선택합니다.	a. 세부 정보를 표시하려면 엔드포인트 이름을 선택하세요. b. 인증서 탭을 선택합니다. c. *인증서 편집*을 선택합니다. d. 필요에 따라 새 사용자 지정 인증서를 업로드하거나 생성하거나, 글로벌 S3 인증서를 사용하기 시작합니다. e. *변경 사항 저장*을 선택합니다.
테넌트 액세스 편집	a. 엔드포인트의 확인란을 선택합니다. b. 작업 > *테넌트 액세스 편집*을 선택합니다. c. 다른 액세스 옵션을 선택하거나, 목록에서 테넌트를 선택 또는 제거하거나, 둘 다 수행할 수 있습니다. d. *변경 사항 저장*을 선택합니다.	a. 세부 정보를 표시하려면 엔드포인트 이름을 선택하세요. b. 테넌트 액세스 탭을 선택합니다. c. *테넌트 액세스 편집*을 선택합니다. d. 다른 액세스 옵션을 선택하거나, 목록에서 테넌트를 선택 또는 제거하거나, 둘 다 수행할 수 있습니다. e. *변경 사항 저장*을 선택합니다.

로드 밸런서 엔드포인트 제거

작업 메뉴를 사용하여 하나 이상의 엔드포인트를 제거하거나, 세부 정보 페이지에서 단일 엔드포인트를 제거할 수 있습니다.

> 클라이언트 서비스 중단을 방지하려면 로드 밸런서 엔드포인트를 제거하기 전에 영향을 받는 S3 클라이언트 애플리케이션을 모두 업데이트하십시오. 각 클라이언트가 다른 로드 밸런서 엔드포인트에 할당된 포트를 사용하여 연결하도록 업데이트해야 합니다. 필요한 인증서 정보도 반드시 업데이트하십시오.

> 관리 인터페이스 엔드포인트를 제거하는 동안 Grid Manager에 대한 액세스 권한을 잃게 되면 URL을 업데이트하십시오.

- 하나 이상의 엔드포인트를 제거하려면:
  a. 로드 밸런싱 페이지에서 제거하려는 각 엔드포인트의 확인란을 선택합니다.
  b. * 작업 * > * 제거 * 를 선택합니다.
  c. *확인*을 선택합니다.
- 세부 정보 페이지에서 엔드포인트 하나를 제거하려면:
  a. 로드 밸런서 페이지에서 엔드포인트 이름을 선택합니다.
  b. 세부 정보 페이지에서 *제거*를 선택합니다.
  c. *확인*을 선택합니다.

StorageGRID에서 S3 엔드포인트 도메인 이름 구성

S3 가상 호스팅 스타일 요청을 지원하려면 Grid Manager를 사용하여 S3 클라이언트가 연결하는 S3 엔드포인트 도메인 이름 목록을 구성해야 합니다.

> 엔드포인트 도메인 이름에 IP 주소를 사용하는 것은 지원되지 않습니다. 향후 릴리스에서는 이러한 구성이 방지됩니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 그리드 업그레이드가 진행 중이 아님을 확인했습니다.

> 그리드 업그레이드가 진행 중일 때는 도메인 이름 구성을 변경하지 마십시오.

이 작업 정보

클라이언트가 S3 엔드포인트 도메인 이름을 사용할 수 있도록 하려면 다음 모든 단계를 수행해야 합니다.

- Grid Manager를 사용하여 S3 엔드포인트 도메인 이름을 StorageGRID 시스템에 추가하십시오.
- "클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서"이(가) 클라이언트가 필요로 하는 모든 도메인 이름에 대해 서명되어 있는지 확인하십시오.

예를 들어 엔드포인트가 `s3.company.com`인 경우 HTTPS 연결에 사용되는 인증서에 `s3.company.com` 엔드포인트와 엔드포인트의 와일드카드 주체 대체 이름(SAN): `*.s3.company.com`이 포함되어 있는지 확인해야 합니다.

- 클라이언트가 사용하는 DNS 서버를 구성합니다. 클라이언트가 연결에 사용하는 IP 주소에 대한 DNS 레코드를 포함하고, 필요한 모든 S3 엔드포인트 도메인 이름(와일드카드 이름 포함)이 레코드에 참조되어 있는지 확인합니다.

> 클라이언트는 게이트웨이 노드, 관리 노드 또는 스토리지 노드의 IP 주소를 사용하거나 고가용성 그룹의 가상 IP 주소에 연결하여 StorageGRID에 연결할 수 있습니다. 클라이언트 애플리케이션이 그리드에 연결하는 방식을 이해하고 DNS 레코드에 올바른 IP 주소를 포함해야 합니다.

HTTPS 연결(권장)을 사용하여 그리드에 접속하는 클라이언트는 다음 인증서 중 하나를 사용할 수 있습니다.

- 로드 밸런서 엔드포인트에 연결하는 클라이언트는 해당 엔드포인트에 대한 사용자 지정 인증서를 사용할 수 있습니다. 각 로드 밸런서 엔드포인트는 서로 다른 S3 엔드포인트 도메인 이름을 인식하도록 구성할 수 있습니다.
- 로드 밸런서 엔드포인트 또는 스토리지 노드에 직접 연결하는 클라이언트는 필요한 모든 S3 엔드포인트 도메인 이름을 포함하도록 글로벌 S3 API 인증서를 사용자 지정할 수 있습니다.

> S3 엔드포인트 도메인 이름을 추가하지 않고 목록이 비어 있는 경우, S3 가상 호스팅 스타일 요청에 대한 지원이 비활성화됩니다.

S3 엔드포인트 도메인 이름 추가

단계

1. 구성 > 네트워크 > *S3 엔드포인트 도메인 이름*을 선택합니다.
2. 도메인 이름 **1** 필드에 도메인 이름을 입력합니다. 도메인 이름을 추가하려면 *다른 도메인 이름 추가*를 선택합니다.
3. *저장*을 선택하세요.
4. 클라이언트가 사용하는 서버 인증서가 필요한 S3 엔드포인트 도메인 이름과 일치하는지 확인하십시오.
   - 클라이언트가 자체 인증서를 사용하는 로드 밸런서 엔드포인트에 연결하는 경우, "엔드포인트와 연결된 인증서를 업데이트합니다.".
   - 클라이언트가 글로벌 S3 API 인증서를 사용하는 로드 밸런서 엔드포인트에 연결하거나 스토리지 노드에 직접 연결하는 경우, "글로벌 S3 API 인증서를 업데이트합니다.".
5. 엔드포인트 도메인 이름 요청을 확인할 수 있도록 필요한 DNS 레코드를 추가하십시오.

결과

이제 클라이언트가 엔드포인트 `*bucket.s3.company.com*`를 사용하면 DNS 서버가 올바른 엔드포인트로 확인되고 인증서는 예상대로 엔드포인트를 인증합니다.

S3 엔드포인트 도메인 이름 변경

S3 애플리케이션에서 사용하는 이름을 변경하면 가상 호스팅 방식 요청이 실패합니다.

단계

1. 구성 > 네트워크 > *S3 엔드포인트 도메인 이름*을 선택합니다.
2. 수정하려는 도메인 이름 필드를 선택하고 필요한 변경 사항을 적용하십시오.

3. *저장*을 선택하세요.
4. 변경 사항을 확인하려면 *예*를 선택하십시오.

S3 엔드포인트 도메인 이름 삭제

S3 애플리케이션에서 사용하는 이름을 제거하면 가상 호스팅 방식 요청이 실패합니다.

단계

1. 구성 > 네트워크 > *S3 엔드포인트 도메인 이름*을 선택합니다.
2. 도메인 이름 옆에 있는 삭제 아이콘 ✕을 선택하세요.
3. 삭제를 확인하려면 *예*를 선택하세요.

관련 정보

- "S3 REST API 사용"
- "IP 주소 보기"
- "고가용성 그룹 구성"

StorageGRID 클라이언트 연결을 위한 IP 주소 및 포트

객체를 저장하거나 검색하기 위해 S3 클라이언트 애플리케이션은 모든 관리 노드와 게이트웨이 노드에 포함된 Load Balancer 서비스 또는 모든 스토리지 노드에 포함된 LDR(Local Distribution Router) 서비스에 연결합니다.

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드의 서비스 포트 번호를 사용하여 StorageGRID에 연결할 수 있습니다. 필요에 따라 로드 밸런싱 노드로 구성된 고가용성(HA) 그룹을 생성하여 가상 IP(VIP) 주소를 사용하는 고가용성 연결을 제공할 수 있습니다. IP 주소나 VIP 주소 대신 정규화된 도메인 이름(FQDN)을 사용하여 StorageGRID에 연결하려면 DNS 항목을 구성하면 됩니다.

이 표는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트를 요약한 것입니다. 로드 밸런서 엔드포인트와 고가용성(HA) 그룹을 이미 생성한 경우, IP 주소를 찾는 방법을 참조하여 Grid Manager에서 이러한 값을 찾으십시오.

연결이 이루어지는 곳	클라이언트가 연결하는 서비스	IP 주소	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소	로드 밸런서 엔드포인트에 할당된 포트
관리자 노드	로드 밸런서	관리 노드의 IP 주소	로드 밸런서 엔드포인트에 할당된 포트
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소	로드 밸런서 엔드포인트에 할당된 포트

연결이 이루어지는 곳	클라이언트가 연결하는 서비스	**IP** 주소	포트
스토리지 노드	LDR	스토리지 노드의 IP 주소	기본 S3 포트: • HTTPS: 18082 • HTTP: 18084

예시 **URL**

고가용성(HA) 게이트웨이 노드 그룹의 로드 밸런서 엔드포인트에 클라이언트 애플리케이션을 연결하려면 아래와 같은 구조의 URL을 사용하십시오.

`https://VIP-of-HA-group:LB-endpoint-port`

예를 들어, HA 그룹의 가상 IP 주소가 192.0.2.5이고 로드 밸런서 엔드포인트의 포트 번호가 10443인 경우 애플리케이션은 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

`https://192.0.2.5:10443`

IP 주소를 찾는 방법

1. "지원되는 웹 브라우저"을(를) 사용하여 Grid Manager에 로그인합니다.
2. 그리드 노드의 IP 주소를 찾으려면:
   a. *노드*를 선택합니다.
   b. 연결할 관리 노드, 게이트웨이 노드 또는 스토리지 노드를 선택하십시오.
   c. 개요 탭을 선택합니다.
   d. 노드 정보 섹션에서 해당 노드의 IP 주소를 확인하십시오.
   e. IPv6 주소 및 인터페이스 매핑을 보려면 *더 보기*를 선택하십시오.

      클라이언트 애플리케이션에서 목록에 있는 모든 IP 주소로 연결을 설정할 수 있습니다.

      - **eth0:** 그리드 네트워크
      - **eth1:** 관리 네트워크 (선택 사항)
      - **eth2:** 클라이언트 네트워크 (선택 사항)

      관리 노드 또는 게이트웨이 노드를 보고 있고 해당 노드가 고가용성 그룹에서 활성 노드인 경우, HA 그룹의 가상 IP 주소가 eth2에 표시됩니다.

3. 고가용성 그룹의 가상 IP 주소를 찾으려면:
   a. 구성 > 네트워크 > *고가용성 그룹*을 선택하십시오.
   b. 표에서 HA 그룹의 가상 IP 주소를 확인하십시오.
4. 로드 밸런서 엔드포인트의 포트 번호를 찾으려면:
   a. 구성 > 네트워크 > *로드 밸런서 엔드포인트*를 선택합니다.

b. 사용하려는 엔드포인트의 포트 번호를 기록해 두십시오.

> 포트 번호가 80 또는 443인 경우, 해당 포트는 관리 노드에서 예약되어 있으므로 게이트웨이 노드에만 엔드포인트가 구성됩니다. 나머지 포트는 게이트웨이 노드와 관리 노드 모두에 구성됩니다.

c. 표에서 엔드포인트 이름을 선택합니다.

d. 클라이언트 유형(S3)이 엔드포인트를 사용할 클라이언트 애플리케이션과 일치하는지 확인하십시오.