클라이언트 연결을 구성합니다

StorageGRID 11.8

NetApp
March 19, 2024

목차

클라이언트 연결을 구성합니다

S3 및 Swift 클라이언트 연결 구성: 개요

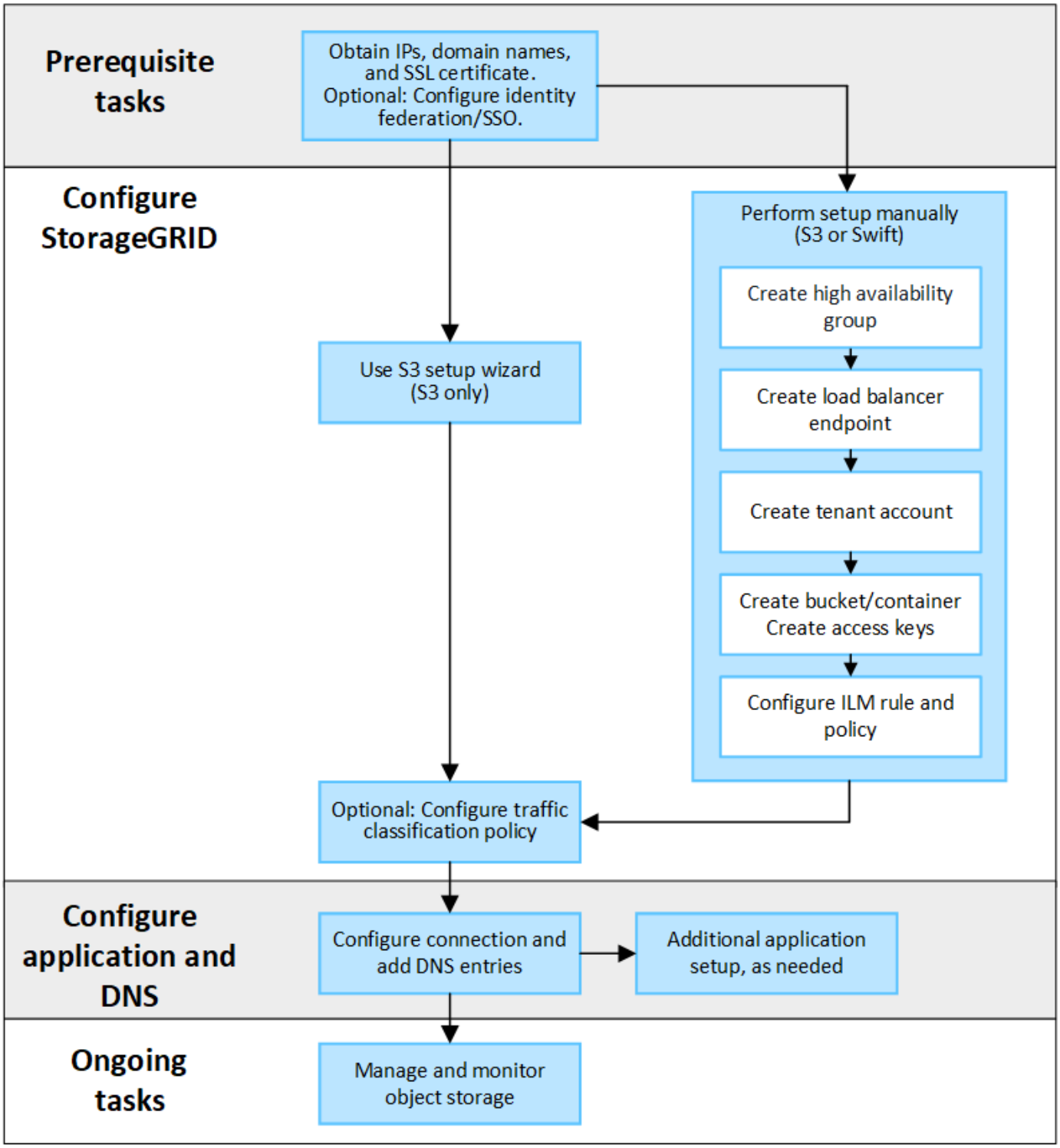
그리드 관리자는 S3 및 Swift 클라이언트 애플리케이션이 StorageGRID 시스템에 연결되어 데이터를 저장 및 검색하는 방법을 제어하는 구성 옵션을 관리합니다.

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

구성 워크플로우

워크플로우 다이어그램에 표시된 것처럼 StorageGRID를 S3 또는 Swift 애플리케이션에 연결하는 기본 단계는 4가지입니다.

1. 클라이언트 응용 프로그램이 StorageGRID에 연결되는 방법에 따라 StorageGRID에서 필수 작업을 수행합니다.
2. StorageGRID를 사용하여 응용 프로그램이 그리드에 연결하는 데 필요한 값을 얻습니다. S3 설정 마법사를 사용하거나 각 StorageGRID 엔터티를 수동으로 구성할 수 있습니다.
3. S3 또는 Swift 애플리케이션을 사용하여 StorageGRID에 대한 연결을 완료합니다. DNS 항목을 만들어 사용하려는 도메인 이름에 IP 주소를 연결합니다.
4. 애플리케이션 및 StorageGRID에서 지속적인 작업을 수행하여 시간에 따라 오브젝트 스토리지를 관리하고 모니터링합니다.



StorageGRID를 클라이언트 애플리케이션에 연결하는 데 필요한 정보입니다

StorageGRID를 S3 또는 Swift 클라이언트 애플리케이션에 연결하려면 먼저 StorageGRID에서 구성 단계를 수행하고 특정 값을 얻어야 합니다.

어떤 가치가 필요합니까?

다음 표에는 StorageGRID에서 구성해야 하는 값과 S3 또는 Swift 애플리케이션 및 DNS 서버에서 해당 값을 사용하는 값이 나와 있습니다.

값	값이 구성된 위치	값이 사용되는 위치
가상 IP(VIP) 주소입니다	StorageGRID > HA 그룹 을 선택합니다	DNS 항목
포트	StorageGRID > 부하 분산 장치 끝점	클라이언트 응용 프로그램
SSL 인증서	StorageGRID > 부하 분산 장치 끝점	클라이언트 응용 프로그램
서버 이름(FQDN)	StorageGRID > 부하 분산 장치 끝점	• 클라이언트 응용 프로그램 • DNS 항목
S3 액세스 키 ID 및 비밀 액세스 키	StorageGRID > 테넌트 및 버킷	클라이언트 응용 프로그램
버킷/컨테이너 이름입니다	StorageGRID > 테넌트 및 버킷	클라이언트 응용 프로그램

이러한 값을 얻으려면 어떻게 해야 합니까**?**

요구 사항에 따라 다음 중 하나를 수행하여 필요한 정보를 얻을 수 있습니다.

- * 를 사용합니다 "S3 설정 마법사"*. S3 설정 마법사를 사용하면 StorageGRID에서 필요한 값을 빠르게 구성하고 S3 애플리케이션을 구성할 때 사용할 수 있는 하나 또는 두 개의 파일을 출력할 수 있습니다. 마법사는 필요한 단계를 안내하고 설정이 StorageGRID 모범 사례를 준수하는지 확인하는 데 도움이 됩니다.

  S3 애플리케이션을 구성할 경우 특별한 요구 사항이 있거나 구현이 상당한 사용자 지정이 필요한 경우가 아니라면 S3 설정 마법사를 사용하는 것이 좋습니다.

- * 를 사용합니다 "FabricPool 설정 마법사"*. S3 설정 마법사와 마찬가지로 FabricPool 설정 마법사를 사용하면 필요한 값을 빠르게 구성하고 ONTAP에서 FabricPool 클라우드 계층을 구성할 때 사용할 수 있는 파일을 출력할 수 있습니다.

  StorageGRID를 FabricPool 클라우드 계층의 오브젝트 스토리지 시스템으로 사용하려는 경우 특별한 요구사항이 있는지 또는 구현을 위해 상당한 양의 사용자 지정이 필요한 경우가 아니라면 FabricPool 설정 마법사를 사용하는 것이 좋습니다.

- * 항목을 수동으로 구성 *. Swift 애플리케이션에 연결하거나 S3 애플리케이션에 연결하고 S3 설정 마법사를 사용하지 않으려는 경우 구성을 수동으로 수행하여 필요한 값을 얻을 수 있습니다. 다음 단계를 수행하십시오.

  a. S3 또는 Swift 애플리케이션에 사용할 고가용성(HA) 그룹을 구성합니다. 을 참조하십시오 "고가용성 그룹을 구성합니다".

  b. S3 또는 Swift 애플리케이션이 사용할 로드 밸런서 엔드포인트를 생성합니다. 을 참조하십시오 "로드 밸런서 엔드포인트를 구성합니다".

  c. S3 또는 Swift 애플리케이션이 사용할 테넌트 계정을 생성합니다. 을 참조하십시오 "테넌트 계정을 생성합니다".

  d. S3 테넌트의 경우 테넌트 계정에 로그인하고 응용 프로그램에 액세스할 각 사용자에 대한 액세스 키 ID 및 비밀 액세스 키를 생성합니다. 을 참조하십시오 "사용자 고유의 액세스 키를 생성합니다".

e. 테넌트 계정 내에 하나 이상의 S3 버킷 또는 Swift 컨테이너를 생성합니다. S3의 경우 를 참조하십시오 "S3 버킷을 생성합니다". Swift의 경우 를 사용합니다 "컨테이너 요청을 넣습니다".

f. 새 테넌트 또는 버킷/컨테이너에 속한 개체에 대한 특정 배치 지침을 추가하려면 새 ILM 규칙을 생성하고 해당 규칙을 사용하도록 새 ILM 정책을 활성화합니다. 을 참조하십시오 "ILM 규칙을 생성합니다" 및 "ILM 정책을 생성합니다".

S3 또는 Swift 클라이언트에 대한 보안

StorageGRID 테넌트 계정은 S3 또는 Swift 클라이언트 애플리케이션을 사용하여 오브젝트 데이터를 StorageGRID에 저장합니다. 클라이언트 응용 프로그램에 대해 구현된 보안 조치를 검토해야 합니다.

요약

다음 표에는 S3 및 Swift REST API에 대해 보안이 구현되는 방식이 요약되어 있습니다.

보안 문제	**REST API** 구현
연결 보안	TLS
서버 인증	시스템 CA에서 서명한 X.509 서버 인증서 또는 관리자가 제공한 사용자 지정 서버 인증서입니다
클라이언트 인증	**S3** S3 계정(액세스 키 ID 및 비밀 액세스 키) 스위프트 SWIFT 계정(사용자 이름 및 암호)
클라이언트 인증	**S3** 버킷 소유권 및 모든 적용 가능한 액세스 제어 정책 스위프트 관리자 역할 액세스

StorageGRID가 클라이언트 응용 프로그램에 보안을 제공하는 방법

S3 및 Swift 클라이언트 애플리케이션을 게이트웨이 노드 또는 관리 노드에서 로드 밸런서 서비스에 연결하거나 스토리지 노드에 직접 연결할 수 있습니다.

- 부하 분산 서비스에 연결하는 클라이언트는 사용자의 방식에 따라 HTTPS 또는 HTTP를 사용할 수 있습니다 "부하 분산 장치 끝점을 구성합니다".

  HTTPS는 TLS로 암호화된 안전한 통신을 제공하며 권장됩니다. 보안 인증서를 끝점에 연결해야 합니다.

  HTTP는 보안이 약하고 암호화되지 않은 통신을 제공하므로 비운영 또는 테스트 그리드에만 사용해야 합니다.

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

  HTTPS가 기본값이며 권장됩니다.

  HTTP는 보안이 약하고 암호화되지 않은 통신을 제공하지만 선택적으로 사용할 수 있습니다 "활성화됨" 비운영 또는 테스트 그리드에 사용

- StorageGRID와 클라이언트 간의 통신은 TLS를 사용하여 암호화됩니다.
- 로드 밸런서 끝점이 HTTP 또는 HTTPS 연결을 허용하도록 구성되었는지 여부에 관계없이 그리드 내의 로드 밸런서 서비스와 스토리지 노드 간의 통신이 암호화됩니다.
- 클라이언트는 REST API 작업을 수행하기 위해 StorageGRID에 HTTP 인증 헤더를 제공해야 합니다. 을 참조하십시오 "요청을 인증합니다" 및 "지원되는 Swift API 엔드포인트".

보안 인증서 및 클라이언트 응용 프로그램

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

- 클라이언트 응용 프로그램은 부하 분산 서비스에 연결할 때 부하 분산 장치 끝점에 대해 구성된 인증서를 사용합니다. 각 로드 밸런서 끝점에는 고유한 인증서 &#8212(그리드 관리자가 업로드한 사용자 지정 서버 인증서 또는 끝점 구성 시 그리드 관리자가 StorageGRID에서 생성한 인증서)가 있습니다.

  을 참조하십시오 "로드 균형 조정에 대한 고려 사항".

- 클라이언트 애플리케이션이 스토리지 노드에 직접 접속하면 시스템 인증 기관에서 서명한 StorageGRID 시스템을 설치할 때 스토리지 노드에 대해 생성된 시스템 생성 서버 인증서를 사용합니다. 또는 그리드 관리자가 그리드에 제공하는 단일 사용자 정의 서버 인증서입니다. 을 참조하십시오 "사용자 지정 S3 또는 Swift API 인증서를 추가합니다".

클라이언트가 TLS 연결을 설정하는 데 사용하는 인증서를 신뢰하도록 구성해야 합니다.

TLS 라이브러리에 대해 지원되는 해시 및 암호화 알고리즘

StorageGRID 시스템은 클라이언트 응용 프로그램이 TLS 세션을 설정할 때 사용할 수 있는 암호 그룹 집합을 지원합니다. 암호를 구성하려면 * 구성 * > * 보안 * > * 보안 설정 * 으로 이동하여 * TLS 및 SSH 정책 * 을 선택합니다.

지원되는 **TLS** 버전입니다

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.

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

S3 설정 마법사를 사용합니다

S3 설정 마법사 고려 사항 및 요구 사항을 사용합니다

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

S3 설정 마법사를 사용하는 경우

S3 설정 마법사는 S3 애플리케이션에서 사용할 StorageGRID를 구성하는 각 단계를 안내합니다. 마법사 완료 시 S3 애플리케이션에 값을 입력하는 데 사용할 수 있는 파일을 다운로드합니다. 마법사를 사용하여 시스템을 보다 빠르게 구성하고 설정이 StorageGRID 모범 사례에 맞는지 확인합니다.

를 가지고 있는 경우 "루트 액세스 권한", StorageGRID 그리드 관리자를 사용하여 시작할 때 S3 설정 마법사를 완료할 수 있으며, 나중에 마법사를 액세스하여 완료할 수 있습니다. 요구 사항에 따라 필요한 항목의 일부 또는 전체를 수동으로 구성한 다음 마법사를 사용하여 S3 애플리케이션에 필요한 값을 조합할 수도 있습니다.

마법사를 사용하기 전에

마법사를 사용하기 전에 이러한 사전 요구 사항을 완료했는지 확인합니다.

IP 주소를 얻고 **VLAN** 인터페이스를 설정합니다

고가용성(HA) 그룹을 구성할 경우 S3 애플리케이션이 연결할 노드와 사용할 StorageGRID 네트워크를 알게 됩니다. 서브넷 CIDR, 게이트웨이 IP 주소 및 가상 IP(VIP) 주소에 대해 입력할 값도 알고 있습니다.

가상 LAN을 사용하여 S3 애플리케이션의 트래픽을 분리할 계획이라면 이미 VLAN 인터페이스를 구성한 것입니다. 을 참조하십시오 "VLAN 인터페이스를 구성합니다".

ID 페더레이션 및 **SSO**를 구성합니다

StorageGRID 시스템에 대해 ID 페더레이션 또는 SSO(Single Sign-On)를 사용하려는 경우 이러한 기능을 활성화했습니다. 또한 S3 애플리케이션에서 사용할 테넌트 계정에 대한 루트 액세스 권한이 있어야 하는 통합 그룹도 알고 있습니다. 을 참조하십시오 "ID 페더레이션을 사용합니다" 및 "Single Sign-On 구성".

도메인 이름 가져오기 및 구성

StorageGRID에 사용할 FQDN(정규화된 도메인 이름)을 알고 있습니다. DNS(Domain Name Server) 항목은 이 FQDN을 마법사를 사용하여 생성한 HA 그룹의 가상 IP(VIP) 주소에 매핑합니다.

S3 가상 호스팅 스타일 요청을 사용하려는 경우 이 있어야 합니다 "S3 끝점 도메인 이름을 구성했습니다". 가상 호스팅 방식의 요청을 사용하는 것이 좋습니다.

로드 밸런서 및 보안 인증서 요구 사항을 검토합니다

StorageGRID 부하 분산 장치를 사용할 계획이라면 로드 밸런싱에 대한 일반적인 고려 사항을 검토했습니다. 업로드할 인증서 또는 인증서를 생성하는 데 필요한 값이 있습니다.

외부(타사) 로드 밸런서 끝점을 사용하려는 경우 해당 로드 밸런서에 대한 FQDN(정규화된 도메인 이름), 포트 및 인증서가 있어야 합니다.

모든 그리드 페더레이션 연결을 구성합니다

S3 테넌트가 계정 데이터를 복제하고 그리드 통합 연결을 사용하여 버킷 오브젝트를 다른 그리드에 복제하도록 허용하려면 마법사를 시작하기 전에 다음을 확인하십시오.

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

S3 설정 마법사를 액세스하고 완료합니다

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

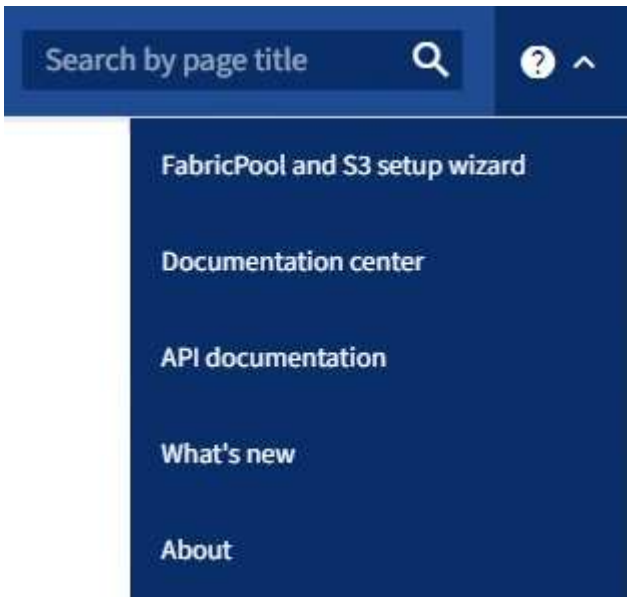
시작하기 전에

- 을(를) 보유하고 있습니다 "루트 액세스 권한".
- 을(를) 검토했습니다 "고려 사항 및 요구 사항" 마법사를 사용합니다.

마법사에 액세스합니다

단계

1. 를 사용하여 Grid Manager에 로그인합니다 "지원되는 웹 브라우저".
2. 대시보드에 * FabricPool and S3 setup wizard * 배너가 나타나면 배너에서 링크를 선택합니다. 배너가 더 이상 나타나지 않으면 그리드 관리자의 머리글 표시줄에서 도움말 아이콘을 선택하고 * FabricPool and S3 setup wizard * 를 선택합니다.



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

단계 **1/6: HA** 그룹 구성

HA 그룹은 각 노드에 StorageGRID 로드 밸런서 서비스가 포함된 노드 모음입니다. HA 그룹에는 게이트웨이 노드, 관리자 노드 또는 둘 다 포함될 수 있습니다.

HA 그룹을 사용하면 S3 데이터 연결을 계속 사용할 수 있습니다. HA 그룹의 액티브 인터페이스에 장애가 발생하면 백업 인터페이스에서 S3 작업에 거의 영향을 주지 않고 워크로드를 관리할 수 있습니다.

이 작업에 대한 자세한 내용은 을 참조하십시오 "고가용성 그룹을 관리합니다".

단계

1. 외부 로드 밸런서를 사용할 계획이라면 HA 그룹을 생성할 필요가 없습니다. Skip this step * 을 선택하고 로

이동합니다 6단계 중 2단계: 로드 밸런서 끝점을 구성합니다.

2. StorageGRID 로드 밸런서를 사용하려면 새 HA 그룹을 생성하거나 기존 HA 그룹을 사용할 수 있습니다.

HA 그룹을 생성합니다

a. 새 HA 그룹을 생성하려면 * Create HA group * 을 선택합니다.

b. Enter details * (세부 정보 입력) 단계에 대해 다음 필드를 작성합니다.

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

c. Add interfaces * 단계에서 이 HA 그룹에 사용할 노드 인터페이스를 선택합니다.

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

하나 이상의 노드를 선택할 수 있지만 각 노드에 대해 하나의 인터페이스만 선택할 수 있습니다.

d. 인터페이스 * 우선 순위 지정 단계의 경우 이 HA 그룹에 대한 기본 인터페이스와 백업 인터페이스를 결정합니다.

행을 드래그하여 * Priority order * 열의 값을 변경합니다.

목록의 첫 번째 인터페이스는 기본 인터페이스입니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active 인터페이스입니다.

HA 그룹에 둘 이상의 인터페이스가 포함되어 있고 활성 인터페이스에 장애가 발생하면 VIP(가상 IP) 주소가 우선 순위 순서대로 첫 번째 백업 인터페이스로 이동합니다. 이 인터페이스에 장애가 발생하면 VIP 주소가 다음 백업 인터페이스로 이동합니다. 장애가 해결되면 VIP 주소가 사용 가능한 우선 순위가 가장 높은 인터페이스로 다시 이동됩니다.

e. IP 주소 입력 * 단계에 대해 다음 필드를 입력합니다.

필드에 입력합니다	설명
서브넷 CIDR	CIDR 표기법 &#8212의 VIP 서브넷 주소, IPv4 주소, 슬래시 및 서브넷 길이(0-32). 네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. 예를 들면, 다음과 같습니다. `192.16.0.0/22`.
게이트웨이 IP 주소(선택 사항)	StorageGRID 액세스에 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.

필드에 입력합니다	설명
가상 IP 주소입니다	HA 그룹에 액티브 인터페이스에 대한 VIP 주소는 하나 이상, 10개 이하로 입력하십시오. 모든 VIP 주소는 VIP 서브넷 내에 있어야 합니다. 하나 이상의 주소는 IPv4여야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

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

g. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

기존 **HA** 그룹 사용

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

b. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

6단계 중 **2**단계**:** 로드 밸런서 끝점을 구성합니다

StorageGRID는 로드 밸런서를 사용하여 클라이언트 애플리케이션에서 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 을 참조하십시오 "로드 균형 조정에 대한 고려 사항".

StorageGRID 로드 밸런서 서비스를 사용하려면 * StorageGRID 로드 밸런서 * 탭을 선택한 다음 사용할 로드 밸런서 끝점을 만들거나 선택합니다. 외부 로드 밸런서를 사용하려면 * 외부 로드 밸런서 * 탭을 선택하고 이미 구성한 시스템에 대한 세부 정보를 제공합니다.

끝점 작성

단계

1. 로드 밸런서 끝점을 만들려면 * 끝점 만들기 * 를 선택합니다.
2. Enter endpoint details * 단계에서 다음 필드를 입력합니다.

필드에 입력합니다	설명
이름	끝점에 대한 설명 이름입니다.
포트	로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드는 처음 생성한 엔드포인트에 대해 기본적으로 10433으로 설정되지만 사용하지 않는 외부 포트는 입력할 수 있습니다. 80 또는 443을 입력하면 해당 포트가 관리 노드에 예약되기 때문에 끝점이 게이트웨이 노드에서만 구성됩니다. • 참고: * 다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 를 참조하십시오 "네트워크 포트 참조".
클라이언트 유형입니다	S3 * 여야 합니다.
네트워크 프로토콜	HTTPS * 를 선택합니다. • 참고 *: TLS 암호화 없이 StorageGRID와 통신하는 것은 지원되지만 권장되지 않습니다.

3. Select binding mode * 단계에서 binding 모드를 지정합니다. 바인딩 모드는 임의의 IP 주소를 사용하거나 특정 IP 주소 및 네트워크 인터페이스를 사용하여 끝점에 액세스하는 방법을 제어합니다.

모드를 선택합니다	설명
글로벌(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 * Global * (글로벌 *) 설정(기본값)을 사용합니다.
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.

모드를 선택합니다	설명
노드 유형입니다	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.

4. 테넌트 액세스 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 해당 버킷에 액세스할 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.

5. 인증서 연결 * 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
인증서 업로드(권장)	CA 서명 서버 인증서, 인증서 개인 키 및 선택적 CA 번들을 업로드하려면 이 옵션을 사용합니다.
인증서를 생성합니다	자체 서명된 인증서를 생성하려면 이 옵션을 사용합니다. 을 참조하십시오 "로드 밸런서 엔드포인트를 구성합니다" 를 참조하십시오.
StorageGRID S3 및 Swift 인증서를 사용합니다	StorageGRID 글로벌 인증서의 사용자 지정 버전을 이미 업로드했거나 생성한 경우에만 이 옵션을 사용합니다. 을 참조하십시오 "S3 및 Swift API 인증서를 구성합니다" 를 참조하십시오.

6. S3 설정 마법사로 돌아가려면 * 마침 * 을 선택합니다.
7. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

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

기존 로드 밸런서 끝점을 사용합니다

단계

1. 기존 끝점을 사용하려면 * 로드 밸런서 끝점 선택 * 에서 해당 이름을 선택합니다.
2. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

외부 로드 밸런서를 사용합니다

단계

1. 외부 로드 밸런서를 사용하려면 다음 필드를 완료합니다.

필드에 입력합니다	설명
FQDN	외부 로드 밸런싱 장치의 FQDN(정규화된 도메인 이름)입니다.
포트	S3 애플리케이션이 외부 로드 밸런서에 연결하는 데 사용할 포트 번호입니다.
인증서	외부 로드 밸런싱 장치의 서버 인증서를 복사하여 이 필드에 붙여 넣습니다.

2. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

6단계 중 **3**단계**:** 테넌트 및 버킷을 생성합니다

테넌트는 S3 애플리케이션을 사용하여 StorageGRID에 오브젝트를 저장하고 검색할 수 있는 엔터티입니다. 각 테넌트에는 자체 사용자, 액세스 키, 버킷, 오브젝트 및 특정 기능 세트가 있습니다. S3 애플리케이션에서 오브젝트를 저장하는 데 사용할 버킷을 생성하려면 먼저 테넌트를 생성해야 합니다.

버킷은 테넌트의 오브젝트 및 오브젝트 메타데이터를 저장하는 데 사용되는 컨테이너입니다. 일부 테넌트에는 버킷이 여러 개 있을 수 있지만 마법사를 사용하면 가장 빠르고 쉬운 방법으로 테넌트와 버킷을 만들 수 있습니다. 나중에 테넌트 관리자를 사용하여 필요한 추가 버킷을 추가할 수 있습니다.

이 S3 애플리케이션에서 사용할 새 테넌트를 생성할 수 있습니다. 필요에 따라 새 테넌트의 버킷을 생성할 수도 있습니다. 마지막으로 마법사에서 테넌트의 루트 사용자에 대한 S3 액세스 키를 생성하도록 허용할 수 있습니다.

이 작업에 대한 자세한 내용은 을 참조하십시오 "테넌트 계정을 생성합니다" 및 "S3 버킷을 생성합니다".

단계

1. 테넌트 생성 * 을 선택합니다.
2. 세부 정보 입력 단계에 대해 다음 정보를 입력합니다.

필드에 입력합니다	설명
이름	테넌트 계정의 이름입니다. 테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.
설명(선택 사항)	테넌트를 식별하는 데 도움이 되는 설명입니다.
클라이언트 유형입니다	이 테넌트가 사용할 클라이언트 프로토콜의 유형입니다. S3 설정 마법사의 경우 * S3 * 가 선택되고 필드가 비활성화됩니다.
스토리지 할당량(선택 사항)	이 테넌트에 스토리지 할당량을 사용하려면 할당량과 유닛에 대한 숫자 값입니다.

3. Continue * 를 선택합니다.

4. 필요에 따라 이 테넌트에게 부여할 권한을 선택합니다.

   이러한 권한 중 일부는 추가 요구 사항이 있습니다. 자세한 내용을 보려면 각 권한에 대한 도움말 아이콘을 선택합니다.

권한	선택한 경우...
플랫폼 서비스를 허용합니다	테넌트는 CloudMirror와 같은 S3 플랫폼 서비스를 사용할 수 있습니다. 을 참조하십시오 "S3 테넌트 계정에 대한 플랫폼 서비스 관리".
고유 ID 소스를 사용합니다	테넌트는 통합 그룹 및 사용자에 대한 자체 ID 소스를 구성하고 관리할 수 있습니다. 이 옵션은 가 있는 경우 사용할 수 없습니다 "SSO를 구성했습니다" StorageGRID 시스템을 위한 것입니다.
S3 선택 허용	테넌트는 오브젝트 데이터를 필터링하고 검색하기 위해 S3 SelectObjectContent API 요청을 실행할 수 있습니다. 을 참조하십시오 "관리 S3 테넌트 계정에 대해 선택 ". • 중요 *: SelectObjectContent 요청은 모든 S3 클라이언트 및 모든 테넌트의 로드 밸런서 성능을 감소시킬 수 있습니다. 신뢰할 수 있는 테넌트에만 필요한 경우에만 이 기능을 사용하도록 설정합니다.
그리드 페더레이션 연결을 사용합니다	테넌트는 그리드 페더레이션 연결을 사용할 수 있습니다. 이 옵션 선택: • 이 테넌트 및 계정에 추가된 모든 테넌트 그룹 및 사용자가 이 그리드(*source grid*)에서 선택한 연결의 다른 그리드(*destination grid*)로 복제되도록 합니다. • 이 테넌트가 각 그리드의 해당 버킷 간에 교차 그리드 복제를 구성할 수 있도록 허용합니다. 을 참조하십시오 "그리드 페더레이션을 위해 허용된 테넌트를 관리합니다".

5. 그리드 페더레이션 연결 사용 * 을 선택한 경우 사용 가능한 그리드 페더레이션 연결 중 하나를 선택합니다.
6. StorageGRID 시스템에서 를 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스를 정의합니다 "ID 제휴", "SSO(Single Sign-On)"또는 둘 다 가능합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	a. 테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. b. 필요에 따라 테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션 및 SSO(Single Sign-On)가 모두 활성화된 경우	테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

7. 마법사에서 루트 사용자에 대한 액세스 키 ID 및 비밀 액세스 키를 생성하려면 * 루트 사용자 S3 액세스 키 자동 생성 * 을 선택합니다.

   테넌트의 유일한 사용자가 루트 사용자인 경우 이 옵션을 선택합니다. 다른 사용자가 이 테넌트를 사용할 경우 테넌트 관리자를 사용하여 키와 권한을 구성합니다.

8. Continue * 를 선택합니다.
9. Create bucket 단계에서 필요에 따라 테넌트의 객체에 대한 버킷을 생성합니다. 그렇지 않으면 * Create tenant without bucket * 을 선택하여 로 이동합니다 데이터 단계를 다운로드합니다.

   그리드에 S3 오브젝트 잠금이 활성화된 경우 이 단계에서 생성한 버킷에 S3 오브젝트 잠금이 활성화되지 않습니다. 이 S3 애플리케이션에 S3 오브젝트 잠금 버킷을 사용해야 하는 경우 * 버킷 없이 테넌트 생성 * 을 선택합니다. 그런 다음 테넌트 관리자를 사용하여 "버킷을 생성합니다" 대신

   a. S3 애플리케이션에서 사용할 버킷의 이름을 입력합니다. 예를 들면, 다음과 같습니다. `S3-bucket`.

      버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

   b. 이 버킷의 * 지역 * 을 선택합니다.

      기본 영역을 사용합니다 (`us-east-1`) 앞으로 ILM을 사용하여 버킷 영역을 기준으로 오브젝트를 필터링하지 않을 것입니다.

   c. 이 버킷에 각 오브젝트 버전을 저장하려면 * 개체 버전 관리 활성화 * 를 선택합니다.

   d. Create tenant and bucket * 을 선택하고 데이터 다운로드 단계로 이동합니다.

단계 **4 / 6:** 데이터 다운로드

데이터 다운로드 단계에서는 하나 또는 두 개의 파일을 다운로드하여 방금 구성한 파일의 세부 정보를 저장할 수 있습니다.

단계

1. 루트 사용자 S3 액세스 키 자동 생성 * 을 선택한 경우 다음 중 하나 또는 모두를 수행합니다.
   - 다운로드 액세스 키 * 를 선택하여 를 다운로드합니다 `.csv` 테넌트 계정 이름, 액세스 키 ID 및 비밀 액세스 키가 포함된 파일입니다.
   - 복사 아이콘( )을 클릭하여 액세스 키 ID 및 비밀 액세스 키를 클립보드에 복사합니다.
2. 를 다운로드하려면 * 구성 값 다운로드 * 를 선택합니다 `.txt` 로드 밸런서 엔드포인트, 테넌트, 버킷 및 루트 사용자에 대한 설정이 포함된 파일입니다.
3. 이 정보를 안전한 위치에 저장합니다.

두 액세스 키를 모두 복사할 때까지 이 페이지를 닫지 마십시오. 이 페이지를 닫으면 키를 사용할 수 없습니다. 이 정보는 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있으므로 안전한 위치에 저장해야 합니다.

4. 메시지가 나타나면 확인란을 선택하여 키를 다운로드하거나 복사했는지 확인합니다.
5. ILM 규칙 및 정책 단계로 이동하려면 * 계속 * 을 선택합니다.

단계 **6** 중 **5: S3**에 대한 **ILM** 규칙 및 **ILM** 정책을 검토합니다

ILM(정보 라이프사이클 관리) 규칙은 StorageGRID 시스템에 있는 모든 개체의 배치, 기간 및 수집 동작을 제어합니다. StorageGRID에 포함된 ILM 정책은 모든 개체의 복제된 복사본 두 개를 만듭니다. 이 정책은 하나 이상의 새 정책을 활성화할 때까지 적용됩니다.

단계

1. 페이지에 제공된 정보를 검토합니다.
2. 새 테넌트 또는 버킷에 속한 객체에 대한 특정 지침을 추가하려면 새 규칙과 새 정책을 생성합니다. 을 참조하십시오 "ILM 규칙을 생성합니다" 및 "ILM 정책: 개요".
3. 선택 * 이 단계를 검토했으며 무엇을 해야 하는지 이해했습니다 *.
4. 다음에 수행할 작업을 이해했음을 나타내려면 확인란을 선택합니다.
5. 요약 * 으로 이동하려면 * 계속 * 을 선택합니다.

6단계 중 **6**단계**:** 요약 검토

단계

1. 요약 내용을 검토합니다.
2. S3 클라이언트에 연결하기 전에 필요할 수 있는 추가 구성을 설명하는 다음 단계의 세부 정보를 기록해 둡니다. 예를 들어 * root로 로그인 * 을 선택하면 테넌트 관리자로 이동합니다. 여기서 테넌트 사용자를 추가하고, 추가 버킷을 생성하고, 버킷 설정을 업데이트할 수 있습니다.
3. 마침 * 을 선택합니다.
4. StorageGRID에서 다운로드한 파일 또는 수동으로 얻은 값을 사용하여 응용 프로그램을 구성합니다.

HA 그룹 관리

고가용성**(HA)** 그룹 관리**:** 개요

여러 관리 및 게이트웨이 노드의 네트워크 인터페이스를 고가용성(HA) 그룹으로 그룹화할 수 있습니다. HA 그룹의 액티브 인터페이스에 장애가 발생하면 백업 인터페이스에서 워크로드를 관리할 수 있습니다.

HA 그룹이란 무엇입니까**?**

고가용성(HA) 그룹을 사용하여 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공하거나 그리드 관리자 및 테넌트 관리자에 고가용성 연결을 제공할 수 있습니다.

각 HA 그룹은 선택한 노드의 공유 서비스에 대한 액세스를 제공합니다.

- 게이트웨이 노드, 관리 노드 또는 둘 다 포함된 HA 그룹은 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공합니다.
- 관리 노드만 포함하는 HA 그룹은 Grid Manager 및 테넌트 관리자에 대한 고가용성 연결을 제공합니다.
- SG100 또는 SG1000 어플라이언스와 VMware 기반 소프트웨어 노드를 포함하는 HA 그룹은 에 고가용성 연결을 제공할 수 있습니다 "S3 Select를 사용하는 S3 테넌트". S3 Select를 사용할 때는 HA 그룹을 사용하는 것이 좋지만 반드시 필요한 것은 아닙니다.

HA 그룹을 어떻게 생성합니까**?**

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

   DHCP 할당 IP 주소가 있는 HA 그룹에는 인터페이스를 추가할 수 없습니다.

2. 하나의 인터페이스를 기본 인터페이스로 지정합니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active 인터페이스입니다.
3. 모든 백업 인터페이스의 우선 순위 순서를 결정합니다.
4. 그룹에 가상 IP(VIP) 주소를 10개까지 할당할 수 있습니다. 클라이언트 응용 프로그램은 이러한 VIP 주소를 사용하여 StorageGRID에 연결할 수 있습니다.

자세한 내용은 을 참조하십시오 "고가용성 그룹을 구성합니다".

액티브 인터페이스란 무엇입니까**?**

정상 작동 중에 HA 그룹의 모든 VIP 주소가 우선 순위 순서대로 첫 번째 인터페이스인 기본 인터페이스에 추가됩니다. 기본 인터페이스를 계속 사용할 수 있는 경우 클라이언트가 그룹의 VIP 주소에 연결할 때 사용됩니다. 즉, 정상 작동 중에 주 인터페이스는 그룹의 "활성" 인터페이스입니다.

마찬가지로 정상 작동 중에 HA 그룹에 대한 우선순위가 낮은 인터페이스는 "백업" 인터페이스로 작동합니다. 이러한 백업 인터페이스는 운영(현재 활성) 인터페이스를 사용할 수 없는 경우가 아니면 사용되지 않습니다.

노드의 현재 **HA** 그룹 상태를 봅니다

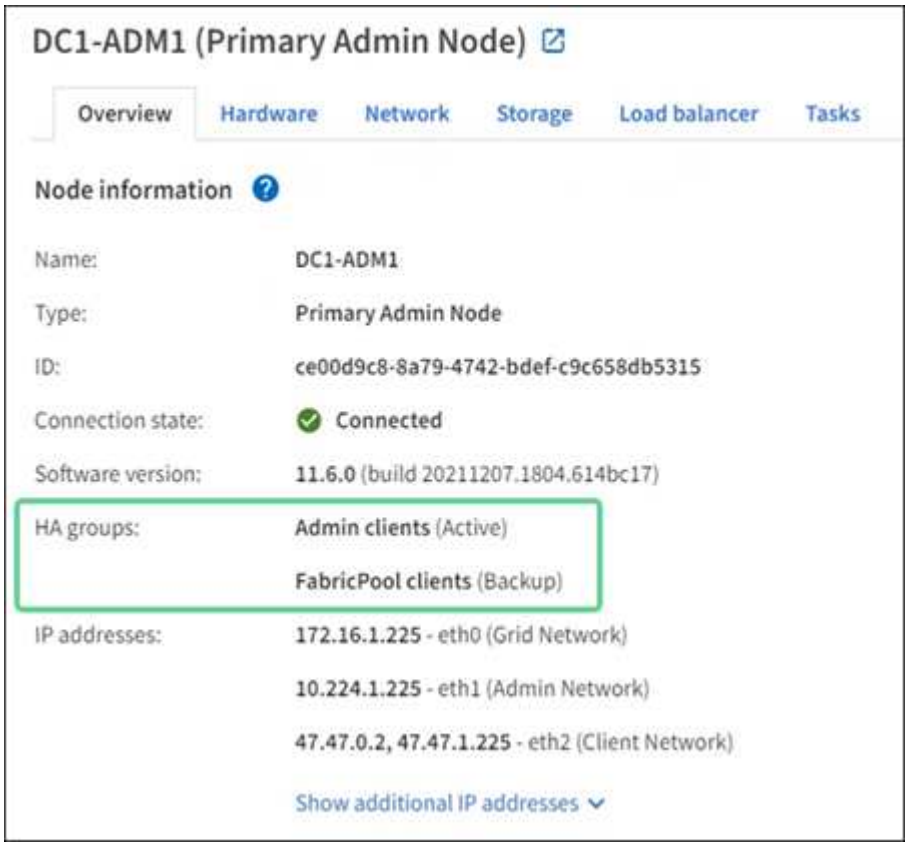
노드가 HA 그룹에 할당되어 있는지 확인하고 현재 상태를 확인하려면 * nodes * > **node* * 를 선택합니다.

Overview * 탭에 * HA 그룹 * 항목이 포함된 경우 나열된 HA 그룹에 노드가 할당됩니다. 그룹 이름 뒤의 값은 HA 그룹에 있는 노드의 현재 상태입니다.

- * 활성 *: HA 그룹이 현재 이 노드에서 호스팅 중입니다.
- * 백업 *: HA 그룹이 현재 이 노드를 사용하고 있지 않습니다. 이것은 백업 인터페이스입니다.
- * 중지됨 *: 고가용성(keepalived) 서비스를 수동으로 중지했기 때문에 이 노드에서 HA 그룹을 호스팅할 수 없습니다.
- * 장애 *: 다음 중 하나 이상의 이유로 이 노드에서 HA 그룹을 호스팅할 수 없습니다.
  - 로드 밸런서(nginx-GW) 서비스가 노드에서 실행되고 있지 않습니다.
  - 노드의 eth0 또는 VIP 인터페이스가 다운되었습니다.

◦ 노드가 다운되었습니다.

이 예에서는 운영 관리 노드가 두 개의 HA 그룹에 추가되었습니다. 이 노드는 현재 관리 클라이언트 그룹의 활성 인터페이스이며 FabricPool 클라이언트 그룹의 백업 인터페이스입니다.



활성 인터페이스가 실패하면 어떻게 됩니까**?**

현재 VIP 주소를 호스트하는 인터페이스는 활성 인터페이스입니다. HA 그룹에 둘 이상의 인터페이스가 포함되어 있고 활성 인터페이스에 장애가 발생하면 VIP 주소가 우선 순위 순서대로 사용 가능한 첫 번째 백업 인터페이스로 이동합니다. 해당 인터페이스에 장애가 발생하면 VIP 주소가 사용 가능한 다음 백업 인터페이스로 이동합니다.

페일오버는 다음과 같은 이유로 트리거될 수 있습니다.

- 인터페이스가 구성된 노드가 다운됩니다.
- 인터페이스가 구성된 노드는 다른 모든 노드와의 연결이 2분 이상 끊어집니다.
- 활성 인터페이스가 다운됩니다.
- 로드 밸런서 서비스가 중지됩니다.
- High Availability 서비스가 중지됩니다.

> 활성 인터페이스를 호스팅하는 노드 외부의 네트워크 장애로 인해 페일오버가 트리거되지 않을 수 있습니다. 마찬가지로, 페일오버는 Grid Manager 또는 테넌트 관리자에 대한 서비스에 의해 트리거되지 않습니다.

장애 조치 프로세스는 일반적으로 몇 초밖에 걸리지 않으며 클라이언트 응용 프로그램에 거의 영향을 주지 않고 정상적인 재시도 동작에 의존하여 작업을 계속할 수 있을 정도로 빠릅니다.

장애가 해결되고 더 높은 우선 순위 인터페이스를 다시 사용할 수 있게 되면 VIP 주소가 사용 가능한 가장 높은 우선 순위 인터페이스로 자동 이동됩니다.

HA 그룹은 어떻게 사용됩니까?

고가용성(HA) 그룹을 사용하여 오브젝트 데이터 및 관리용으로 StorageGRID에 대한 고가용성 연결을 제공할 수 있습니다.

- HA 그룹은 Grid Manager 또는 Tenant Manager에 대한 고가용성 관리 연결을 제공할 수 있습니다.
- HA 그룹은 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공할 수 있습니다.
- 인터페이스가 하나만 포함된 HA 그룹을 사용하면 많은 VIP 주소를 제공하고 IPv6 주소를 명시적으로 설정할 수 있습니다.

그룹에 포함된 모든 노드가 동일한 서비스를 제공하는 경우에만 HA 그룹이 고가용성을 제공할 수 있습니다. HA 그룹을 생성할 때 필요한 서비스를 제공하는 노드 유형의 인터페이스를 추가합니다.

- * 관리 노드 *: 로드 밸런서 서비스를 포함하고 그리드 관리자 또는 테넌트 관리자에 대한 액세스를 활성화합니다.
- * 게이트웨이 노드 *: 로드 밸런서 서비스를 포함합니다.

HA 그룹의 용도	이 유형의 노드를 **HA** 그룹에 추가합니다
Grid Manager에 액세스합니다	• 기본 관리 노드(* 기본 *) • 운영 관리자 노드가 아닌 노드 • 참고: * 기본 관리 노드는 기본 인터페이스여야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.
테넌트 관리자에 대한 액세스만 가능합니다	• 운영 또는 비운영 관리 노드
S3 또는 Swift 클라이언트 액세스 — 로드 밸런서 서비스	• 관리자 노드 • 게이트웨이 노드
에 대한 S3 클라이언트 액세스 "S3 를 선택합니다"	• SG100 또는 SG1000 어플라이언스 • VMware 기반 소프트웨어 노드입니다 • 참고 *: S3 Select를 사용할 때는 HA 그룹을 사용하는 것이 좋지만 반드시 필요한 것은 아닙니다.

Grid Manager 또는 **Tenant Manager**에 **HA** 그룹을 사용할 때의 제한 사항

Grid Manager 또는 Tenant Manager 서비스에 장애가 발생하면 HA 그룹 페일오버가 트리거되지 않습니다.

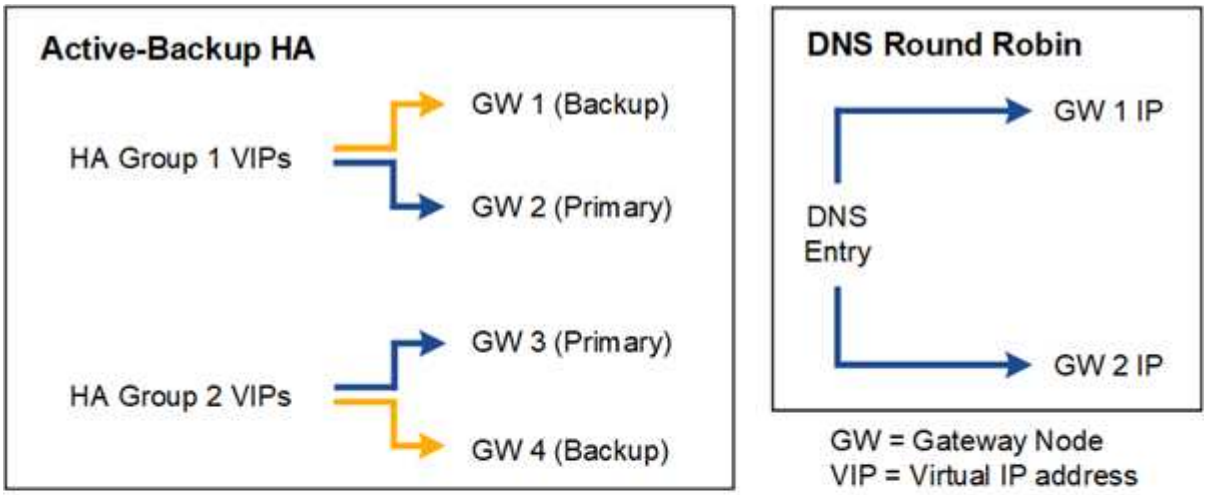
페일오버가 발생했을 때 Grid Manager 또는 Tenant Manager에 로그인한 경우, 로그아웃되며 작업을 재개하려면 다시 로그인해야 합니다.

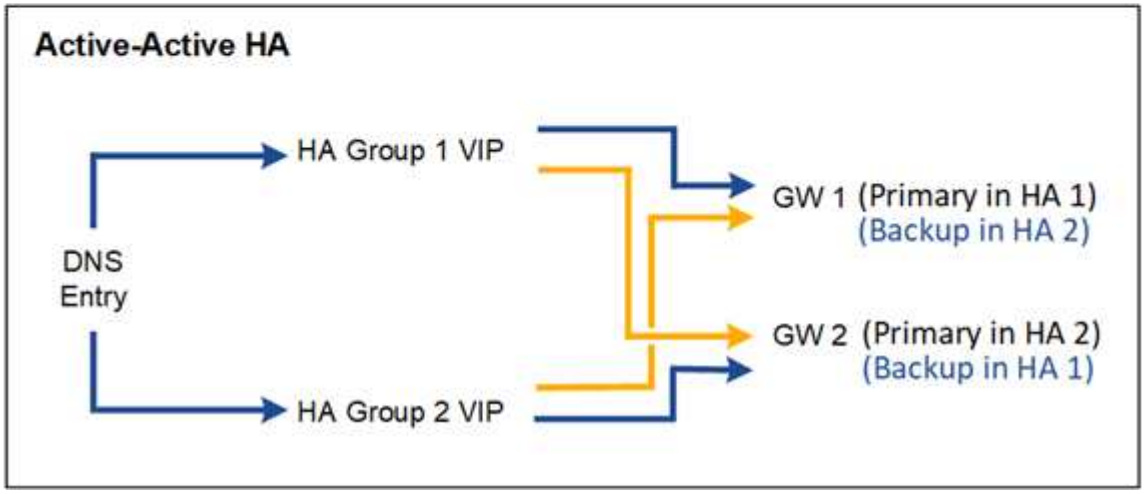
기본 관리 노드를 사용할 수 없는 경우 일부 유지 관리 절차를 수행할 수 없습니다. 장애 조치 중에 그리드 관리자를 사용하여 StorageGRID 시스템을 모니터링할 수 있습니다.

HA 그룹에 대한 구성 옵션

다음 다이어그램에서는 HA 그룹을 구성할 수 있는 다양한 방법의 예를 제공합니다. 각 옵션에는 장단점이 있습니다.

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





이 표에는 다이어그램에 표시된 각 HA 구성의 이점이 요약되어 있습니다.

구성	장점	단점
Active-Backup HA를 참조하십시오	• 외부 종속성 없이 StorageGRID에서 관리 • 빠른 페일오버.	• HA 그룹에서 하나의 노드만 활성화됩니다. HA 그룹당 최소 하나의 노드가 유휴 상태가 됩니다.
DNS 라운드 로빈	• 총 처리량 향상: • 유휴 호스트가 없습니다.	• 느린 페일오버 - 클라이언트 동작에 따라 달라질 수 있습니다. • StorageGRID 외부에서 하드웨어를 구성해야 합니다. • 고객이 구현한 상태 점검이 필요합니다.

구성	장점	단점
액티브-액티브 HA	• 트래픽이 여러 HA 그룹에 분산됩니다. • HA 그룹 수에 따라 확장 가능한 높은 애그리게이트 처리량입니다. • 빠른 페일오버.	• 구성이 더 복잡합니다. • StorageGRID 외부에서 하드웨어를 구성해야 합니다. • 고객이 구현한 상태 점검이 필요합니다.

고가용성 그룹을 구성합니다

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

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 있습니다 "루트 액세스 권한".
- HA 그룹에서 VLAN 인터페이스를 사용하려는 경우 VLAN 인터페이스를 만들었습니다. 을 참조하십시오 "VLAN 인터페이스를 구성합니다".
- HA 그룹의 노드에 액세스 인터페이스를 사용하려는 경우 인터페이스를 생성했습니다.
  - * Red Hat Enterprise Linux(노드 설치 전) *: "노드 구성 파일을 생성합니다"
  - * Ubuntu 또는 Debian(노드 설치 전) *: "노드 구성 파일을 생성합니다"
  - * Linux(노드 설치 후) *: "Linux: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다"
  - * VMware(노드 설치 후) *: "VMware: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다"

고가용성 그룹을 생성합니다

고가용성 그룹을 만들 때 하나 이상의 인터페이스를 선택하고 우선 순위에 따라 구성합니다. 그런 다음 그룹에 하나 이상의 VIP 주소를 할당합니다.

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

마법사에 액세스합니다

단계

1. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.
2. Create * 를 선택합니다.

HA 그룹에 대한 세부 정보를 입력합니다

단계

1. HA 그룹에 고유한 이름을 제공하십시오.
2. 필요에 따라 HA 그룹에 대한 설명을 입력합니다.

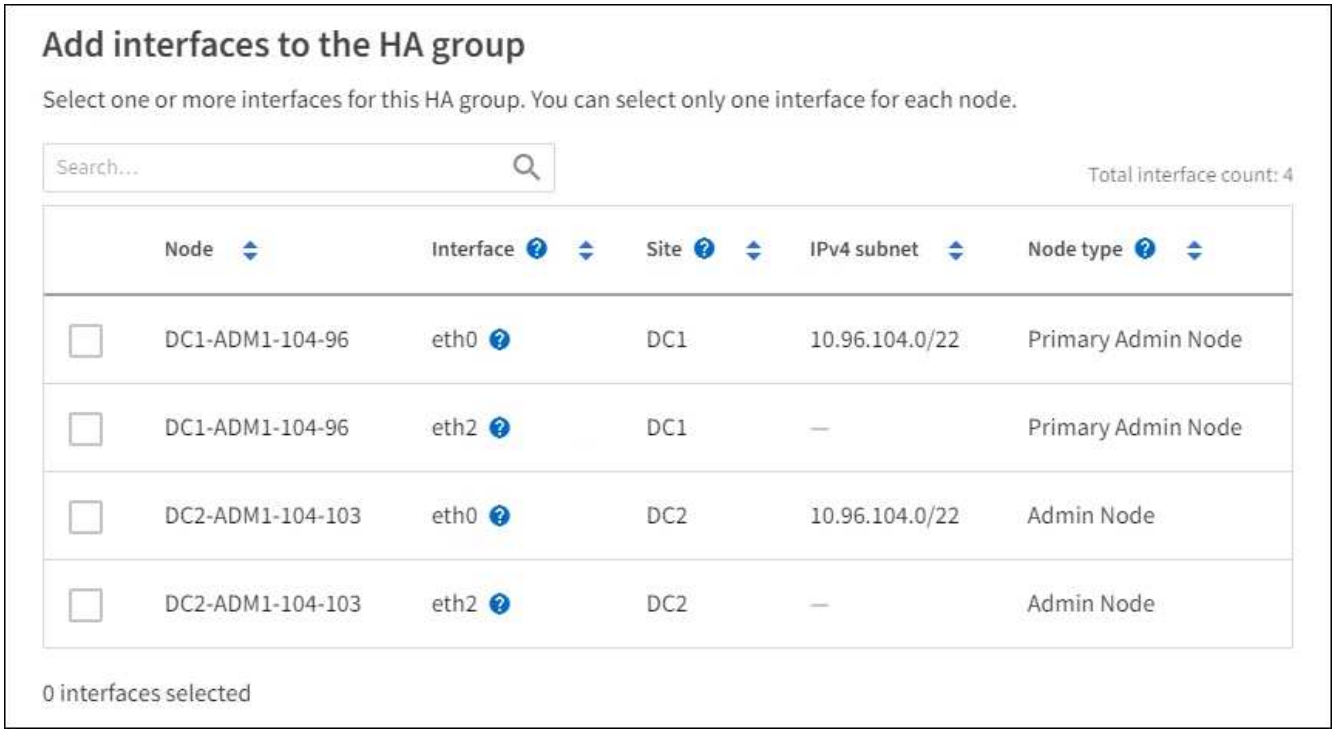
3. Continue * 를 선택합니다.

HA 그룹에 인터페이스를 추가합니다

단계

1. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

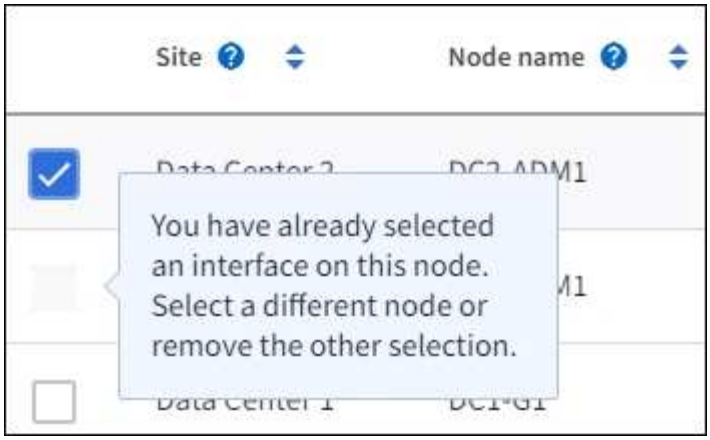
   열 머리글을 사용하여 행을 정렬하거나 검색어를 입력하여 인터페이스를 보다 빠르게 찾을 수 있습니다.



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

   인터페이스 선택을 위한 지침

   - 인터페이스를 하나 이상 선택해야 합니다.
   - 한 노드에 대해 하나의 인터페이스만 선택할 수 있습니다.
   - HA 그룹이 그리드 관리자 및 테넌트 관리자를 포함하는 관리 노드 서비스의 HA 보호를 위한 경우 관리 노드에서만 인터페이스를 선택합니다.
   - HA 그룹이 S3 또는 Swift 클라이언트 트래픽의 HA 보호를 지원하는 경우 관리 노드의 인터페이스, 게이트웨이 노드 또는 둘 다를 선택합니다.
   - 다른 유형의 노드에서 인터페이스를 선택하면 정보 참고 사항이 나타납니다. 페일오버가 발생하면 이전에 활성 노드에서 제공하는 서비스를 새로 활성 노드에서 사용하지 못할 수 있습니다. 예를 들어 백업 게이트웨이 노드는 관리 노드 서비스의 HA 보호를 제공할 수 없습니다. 마찬가지로 백업 관리 노드는 기본 관리 노드가 제공할 수 있는 모든 유지 관리 절차를 수행할 수 없습니다.
   - 인터페이스를 선택할 수 없는 경우 해당 확인란이 비활성화됩니다. 자세한 내용은 툴 팁을 참조하십시오.



- 서브넷 값 또는 게이트웨이가 선택한 다른 인터페이스와 충돌하는 경우 인터페이스를 선택할 수 없습니다.
- 정적 IP 주소가 없는 경우 구성된 인터페이스를 선택할 수 없습니다.

2. Continue * 를 선택합니다.

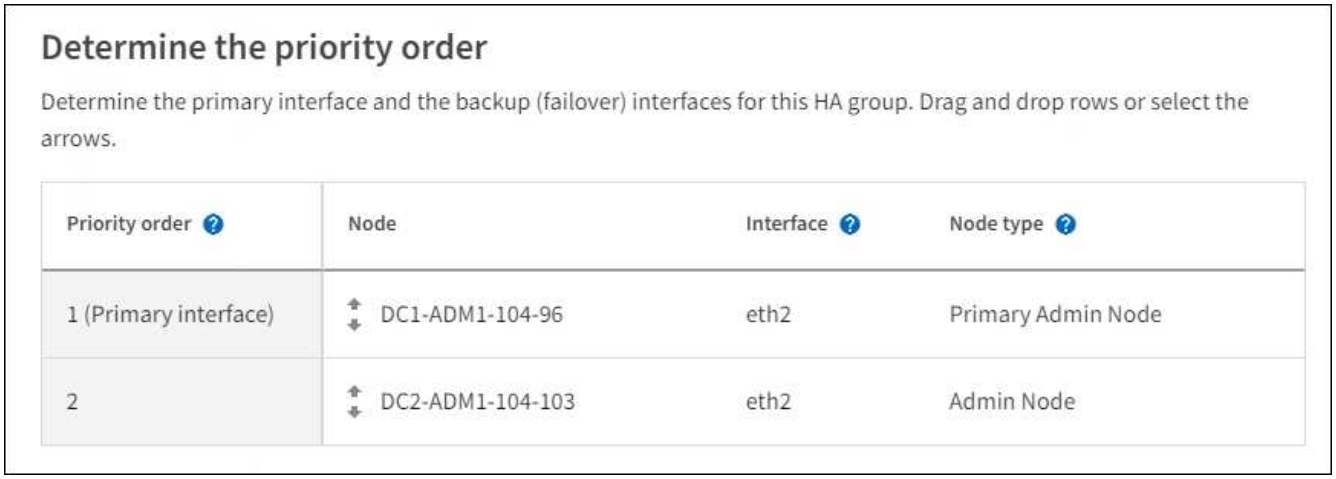
우선 순위 순서를 결정합니다

HA 그룹에 둘 이상의 인터페이스가 포함된 경우 운영 인터페이스인지, 백업(페일오버) 인터페이스인지 확인할 수 있습니다. 기본 인터페이스에 장애가 발생하면 VIP 주소가 사용 가능한 가장 높은 우선 순위 인터페이스로 이동합니다. 이 인터페이스에 장애가 발생하면 VIP 주소는 사용 가능한 다음 우선 순위 인터페이스로 이동합니다.

단계

1. Priority order* 열의 행을 끌어서 기본 인터페이스와 백업 인터페이스를 결정합니다.

   목록의 첫 번째 인터페이스는 기본 인터페이스입니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active 인터페이스입니다.



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

2. Continue * 를 선택합니다.

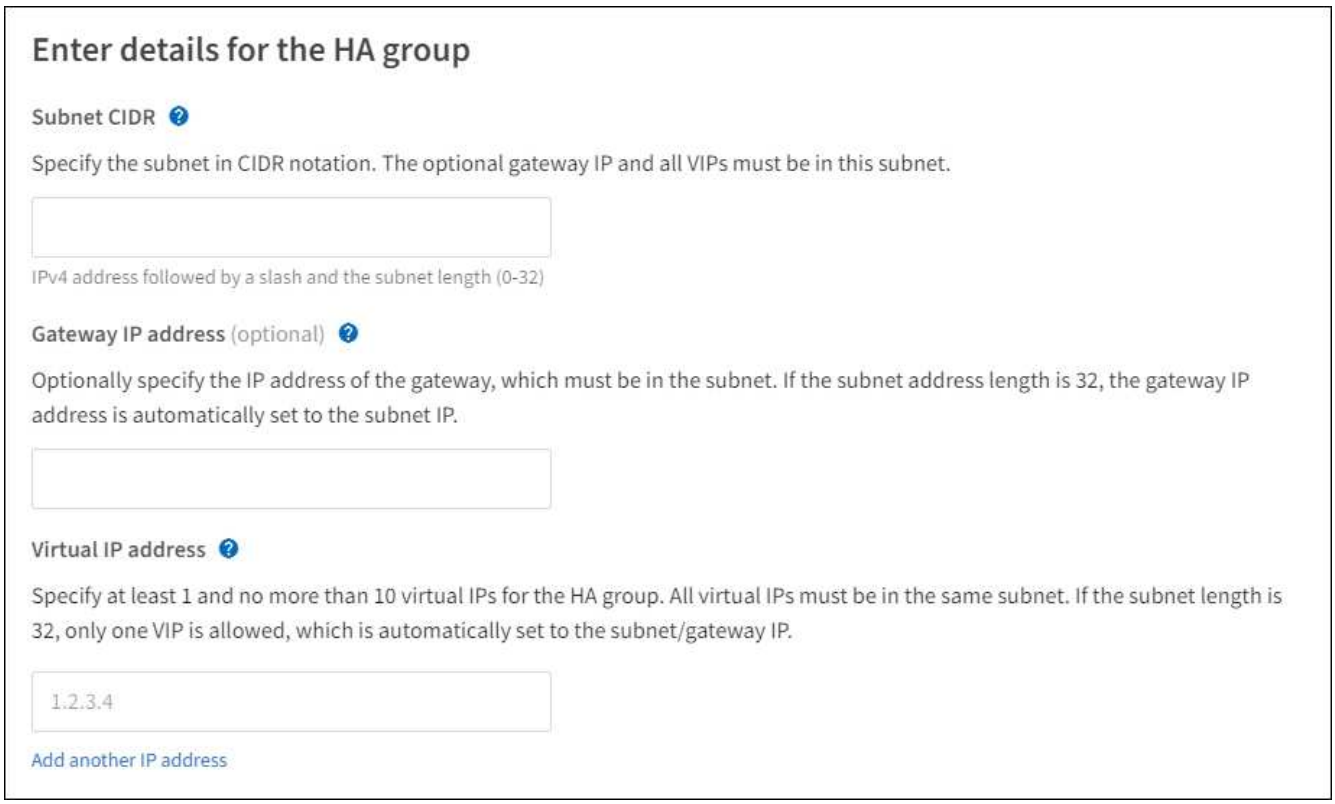
IP 주소를 입력합니다

단계

1. 서브넷 CIDR* 필드에서 CIDR 표시법으로 VIP 서브넷을 지정합니다. IPv4 주소 다음에 슬래시와 서브넷 길이(0-32)를 입력합니다.

   네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. 예를 들면, 다음과 같습니다. `192.16.0.0/22`.

   32비트 접두사를 사용하는 경우 VIP 네트워크 주소는 게이트웨이 주소 및 VIP 주소로도 사용됩니다.



2. 선택적으로 S3, Swift, 관리 또는 테넌트 클라이언트가 다른 서브넷에서 이러한 VIP 주소에 액세스할 경우 * 게이트웨이 IP 주소 * 를 입력합니다. 게이트웨이 주소는 VIP 서브넷 내에 있어야 합니다.

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

3. HA 그룹에 액티브 인터페이스에 대한 VIP 주소는 하나 이상, 10개 이하로 입력하십시오. 모든 VIP 주소는 VIP 서브넷 내에 있어야 하며 모든 주소는 활성 인터페이스에서 동시에 활성화됩니다.

   IPv4 주소를 하나 이상 입력해야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

4. HA 그룹 생성 * 을 선택하고 * 마침 * 을 선택합니다.

   HA 그룹이 생성되고 이제 구성된 가상 IP 주소를 사용할 수 있습니다.

다음 단계

이 HA 그룹을 로드 밸런싱에 사용하려면 로드 밸런서 엔드포인트를 생성하여 포트 및 네트워크 프로토콜을 결정하고 필요한 인증서를 연결합니다. 을 참조하십시오 "로드 밸런서 엔드포인트를 구성합니다".

High Availability 그룹을 편집합니다

HA(고가용성) 그룹을 편집하여 이름과 설명을 변경하거나, 인터페이스를 추가 또는 제거하거나, 우선 순위 순서를 변경하거나, 가상 IP 주소를 추가 또는 업데이트할 수 있습니다.

예를 들어, 사이트 또는 노드 사용 중단 절차에서 선택한 인터페이스에 연결된 노드를 제거하려면 HA 그룹을 편집해야 할 수 있습니다.

단계

1. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.

   고가용성 그룹 페이지에는 기존의 모든 HA 그룹이 표시됩니다.

2. 편집할 HA 그룹의 확인란을 선택합니다.
3. 업데이트할 항목을 기준으로 다음 중 하나를 실행합니다.
   - VIP 주소를 추가하거나 제거하려면 * Actions * > * Edit virtual IP address * 를 선택합니다.
   - 작업 * > * HA 그룹 편집 * 을 선택하여 그룹의 이름 또는 설명을 업데이트하거나, 인터페이스를 추가 또는 제거하거나, 우선 순위 순서를 변경하거나, VIP 주소를 추가 또는 제거합니다.
4. Edit virtual IP address * 를 선택한 경우:
   a. HA 그룹의 가상 IP 주소를 업데이트합니다.
   b. 저장 * 을 선택합니다.
   c. 마침 * 을 선택합니다.
5. HA 그룹 편집 * 을 선택한 경우:
   a. 필요에 따라 그룹의 이름 또는 설명을 업데이트합니다.
   b. 선택적으로 확인란을 선택하거나 선택 취소하여 인터페이스를 추가하거나 제거합니다.

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

   c. 필요에 따라 행을 끌어서 운영 인터페이스 및 이 HA 그룹에 대한 백업 인터페이스의 우선 순위를 변경합니다.
   d. 필요에 따라 가상 IP 주소를 업데이트합니다.
   e. Save * 를 선택한 다음 * Finish * 를 선택합니다.

High Availability 그룹을 제거합니다

HA(고가용성) 그룹을 한 번에 하나 이상 제거할 수 있습니다.

HA 그룹이 로드 밸런서 끝점에 바인딩되어 있으면 제거할 수 없습니다. HA 그룹을 삭제하려면 해당 그룹을 사용하는 모든 로드 밸런싱 장치 끝점에서 HA 그룹을 제거해야 합니다.

클라이언트 중단을 방지하려면 HA 그룹을 삭제하기 전에 영향을 받는 S3 또는 Swift 클라이언트 애플리케이션을 업데이트하십시오. 다른 IP 주소(예: 다른 HA 그룹의 가상 IP 주소 또는 설치 중 인터페이스에 대해 구성된 IP 주소)를 사용하여 연결할 각 클라이언트를 업데이트합니다.

단계

1. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.
2. 제거하려는 각 HA 그룹에 대해 * 로드 밸런서 엔드포인트 * 열을 검토합니다. 로드 밸런서 끝점이 나열되어 있는 경우:
   a. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 로 이동합니다.
   b. 끝점의 확인란을 선택합니다.
   c. 작업 * > * 끝점 바인딩 모드 편집 * 을 선택합니다.
   d. 바인딩 모드를 업데이트하여 HA 그룹을 제거합니다.
   e. 변경 내용 저장 * 을 선택합니다.
3. 로드 밸런싱 장치 엔드포인트가 나열되지 않은 경우 제거할 각 HA 그룹에 대한 확인란을 선택합니다.
4. Actions * > * Remove HA group * 을 선택합니다.
5. 메시지를 검토하고 * Delete HA group * 을 선택하여 선택 사항을 확인합니다.

   선택한 모든 HA 그룹이 제거됩니다. High Availability Groups 페이지에 녹색 성공 배너가 나타납니다.

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

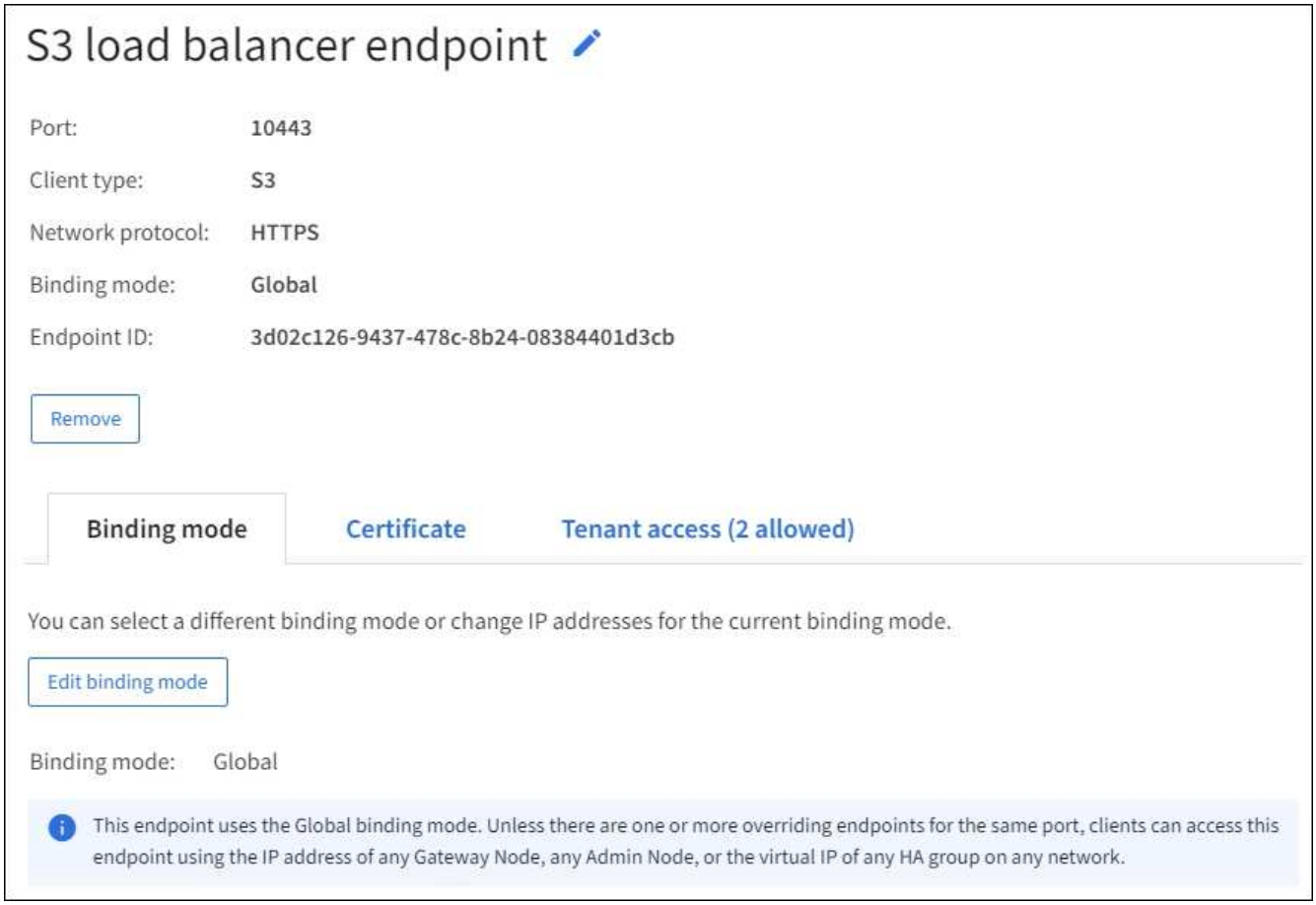
   ◦ 정규화된 도메인 이름 또는 IP 주소입니다

   ◦ 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.

S3 끝점 도메인 이름을 구성합니다

S3 가상 호스팅 스타일 요청을 지원하려면 그리드 관리자를 사용하여 S3 클라이언트가 연결하는 S3 엔드 포인트 도메인 이름 목록을 구성해야 합니다.

끝점 도메인 이름에 IP 주소를 사용하는 것은 지원되지 않습니다. 향후 릴리즈에서는 이 구성을 사용할 수 없습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 있습니다 "특정 액세스 권한".
- 그리드 업그레이드가 진행 중이 아닌 것을 확인했습니다.

그리드 업그레이드가 진행 중일 때는 도메인 이름 구성을 변경하지 마십시오.

이 작업에 대해

클라이언트가 S3 엔드포인트 도메인 이름을 사용하도록 설정하려면 다음 작업을 모두 수행해야 합니다.

- 그리드 관리자를 사용하여 StorageGRID 시스템에 S3 끝점 도메인 이름을 추가합니다.
- 를 확인합니다 "클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서입니다" 클라이언트가 필요로 하는 모든 도메인 이름에 대해 서명됩니다.

  예를 들어, 끝점이 인 경우 `s3.company.com`HTTPS 연결에 사용되는 인증서에 가 포함되어 있는지 확인해야 합니다 `s3.company.com` 끝점 및 끝점의 와일드카드 주체 대체 이름(SAN): `*.s3.company.com`.

- 클라이언트가 사용하는 DNS 서버를 구성합니다. 클라이언트가 연결하는 데 사용하는 IP 주소에 대한 DNS 레코드를 포함하고 와일드카드 이름을 포함하여 필요한 모든 S3 끝점 도메인 이름을 레코드가 참조하는지 확인합니다.

> 클라이언트는 게이트웨이 노드, 관리 노드 또는 스토리지 노드의 IP 주소를 사용하거나 고가용성 그룹의 가상 IP 주소에 연결하여 StorageGRID에 연결할 수 있습니다. DNS 레코드에 올바른 IP 주소를 포함하도록 클라이언트 응용 프로그램이 그리드에 연결하는 방법을 이해해야 합니다.

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

- 로드 밸런서 끝점에 연결하는 클라이언트는 해당 끝점에 대해 사용자 지정 인증서를 사용할 수 있습니다. 각 로드 밸런서 끝점은 서로 다른 S3 끝점 도메인 이름을 인식하도록 구성할 수 있습니다.
- 로드 밸런서 끝점에 연결하거나 스토리지 노드에 직접 연결하는 클라이언트는 글로벌 S3 및 Swift API 인증서를 사용자 정의하여 필요한 모든 S3 엔드포인트 도메인 이름을 포함할 수 있습니다.

> S3 끝점 도메인 이름을 추가하지 않고 목록이 비어 있으면 S3 가상 호스팅 스타일 요청에 대한 지원이 비활성화됩니다.

S3 엔드포인트 도메인 이름을 추가합니다

단계

1. 구성 * > * 네트워크 * > * S3 엔드포인트 도메인 이름 * 을 선택합니다.
2. 도메인 이름 1 * 필드에 도메인 이름을 입력합니다. 도메인 이름을 더 추가하려면 * 다른 도메인 이름 추가 * 를 선택합니다.
3. 저장 * 을 선택합니다.
4. 클라이언트가 사용하는 서버 인증서가 필요한 S3 엔드포인트 도메인 이름과 일치하는지 확인합니다.
   - 클라이언트가 자체 인증서를 사용하는 로드 밸런서 끝점에 연결하는 경우 "끝점과 연결된 인증서를 업데이트합니다".
   - 클라이언트가 글로벌 S3 및 Swift API 인증서를 사용하는 로드 밸런서 끝점에 연결하거나 스토리지 노드에 직접 연결하는 경우 "글로벌 S3 및 Swift API 인증서를 업데이트합니다".
5. 엔드포인트 도메인 이름 요청을 확인하는 데 필요한 DNS 레코드를 추가합니다.

결과

이제 클라이언트가 끝점을 사용할 때 `*bucket.s3.company.com*`DNS 서버가 올바른 끝점으로 확인되고 인증서는 끝점을 예상대로 인증합니다.

S3 끝점 도메인 이름 바꾸기

S3 애플리케이션에서 사용하는 이름을 변경하면 가상 호스팅 스타일 요청이 실패합니다.

단계

1. 구성 * > * 네트워크 * > * S3 엔드포인트 도메인 이름 * 을 선택합니다.
2. 편집할 도메인 이름 필드를 선택하고 필요한 내용을 변경합니다.
3. 저장 * 을 선택합니다.

4. 예 * 를 선택하여 변경 사항을 확인합니다.

S3 끝점 도메인 이름을 삭제합니다

S3 애플리케이션에서 사용하는 이름을 제거하면 가상 호스팅 스타일 요청이 실패합니다.

단계

1. 구성 * > * 네트워크 * > * S3 엔드포인트 도메인 이름 * 을 선택합니다.
2. 삭제 아이콘을 선택합니다 ✕ 도메인 이름 옆에 있습니다.
3. 예 * 를 선택하여 삭제를 확인합니다.

관련 정보

- "S3 REST API 사용"
- "IP 주소를 봅니다"
- "고가용성 그룹을 구성합니다"

요약: 클라이언트 연결을 위한 IP 주소 및 포트

오브젝트를 저장하거나 검색하기 위해 S3 및 Swift 클라이언트 애플리케이션은 모든 관리 노드 및 게이트웨이 노드에 포함된 로드 밸런서 서비스 또는 모든 스토리지 노드에 포함된 LDR(Local Distribution Router) 서비스에 연결됩니다.

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드의 서비스 포트 번호를 사용하여 StorageGRID에 연결할 수 있습니다. 선택적으로, 로드 밸런싱 노드의 고가용성(HA) 그룹을 생성하여 가상 IP(VIP) 주소를 사용하는 고가용성 연결을 제공할 수 있습니다. IP 또는 VIP 주소 대신 FQDN(정규화된 도메인 이름)을 사용하여 StorageGRID에 연결하려는 경우 DNS 항목을 구성할 수 있습니다.

이 표에는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트가 요약되어 있습니다. 로드 밸런서 엔드포인트 및 고가용성(HA) 그룹을 이미 생성한 경우 를 참조하십시오 IP 주소를 찾을 위치 그리드 관리자에서 이러한 값을 찾습니다.

연결 위치	클라이언트가 연결하는 서비스입니다	IP 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다

연결 위치	클라이언트가 연결하는 서비스입니다	**IP** 주소입니다	포트
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: • HTTPS: 18082 • HTTP: 18084 기본 Swift 포트: • HTTPS: 18083 • HTTP: 18085

URL의 예

클라이언트 응용 프로그램을 게이트웨이 노드의 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

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

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

`https://192.0.2.5:10443`

IP 주소를 찾을 위치

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

      클라이언트 응용 프로그램에서 목록의 IP 주소로의 연결을 설정할 수 있습니다.

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

      관리 노드 또는 게이트웨이 노드를 보고 있고 고가용성 그룹의 활성 노드인 경우 HA 그룹의 가상 IP 주소가 eth2에 표시됩니다.
3. 고가용성 그룹의 가상 IP 주소를 찾으려면 다음을 수행합니다.

a. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.

b. 표에서 HA 그룹의 가상 IP 주소를 확인합니다.

4. 로드 밸런서 끝점의 포트 번호를 찾으려면 다음을 수행합니다.

a. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.

b. 사용할 끝점의 포트 번호를 확인합니다.

> 포트 번호가 80 또는 443인 경우 엔드포인트는 게이트웨이 노드에서만 구성됩니다. 이러한 포트는 관리 노드에 예약되기 때문입니다. 다른 모든 포트는 게이트웨이 노드와 관리 노드 모두에서 구성됩니다.

c. 테이블에서 끝점 이름을 선택합니다.

d. 클라이언트 유형 * (S3 또는 Swift)이 끝점을 사용할 클라이언트 응용 프로그램과 일치하는지 확인합니다.