StorageGRID 솔루션 및 리소스

StorageGRID solutions and resources

NetApp
December 12, 2025

목차

StorageGRID 솔루션 및 리소스

StorageGRID 평가판 소프트웨어에 액세스하는 단계

이 지침은 NetApp과 협력하는 NetApp 세일즈, 파트너 및 잠재 고객을 위한 것입니다.

계정을 등록하십시오

1. 회사 이메일을 사용하여 에 계정을 "NetApp Support 사이트" 등록합니다.
   a. 새로 생성된 계정으로 로그인하지 않았는지 확인합니다.
   b. 이미 계정이 있는 경우 로그인되어 있지 않은지 확인하고 다음 단계를 진행합니다.
2. 비기술적 지원 케이스를 생성하여 액세스 수준을 "잠재 고객"으로 높입니다. 이렇게 하려면 ""문제를 보고하십시오 "웹 사이트의 바닥글에서 " 링크를 클릭하십시오.
3. 피드백 범주로 "등록 문제"를 선택합니다.
4. 설명 섹션에 "내 계정 이메일 주소는 _ 귀하의 - 이메일 - 주소 _ 입니다. 잠재 고객이 StorageGRID 평가판 소프트웨어를 다운로드할 수 있도록 액세스하려고 합니다."
   a. 잠재 고객 액세스 요청을 제안한 NetApp 내부 담당자의 이름을 언급하십시오.

StorageGRID를 다운로드합니다

1. 지원 케이스를 검토 및 승인하면 NetApp 지원 팀에서 이메일을 통해 귀하의 계정에 잠재 고객 액세스 권한이 부여되었음을 알려드립니다.
2. 를 "StorageGRID 평가판 소프트웨어"다운로드하십시오.

ⓘ 평가판 라이센스 파일은 zip 파일 내에 있습니다. 일단 압축이 풀리면 StorageGRID-Webscale-<version>\vSphere\NLF000000.txt 입니다.

ⓘ 소프트웨어 다운로드는 법적 요구 사항을 준수하기 위한 무역 규정 준수 조치와 관련된 프로세스입니다. 규정 준수를 보장하기 위해 사용자는 액세스 권한을 얻기 전에 계정을 생성하고 지원 케이스를 개설해야 합니다. 이 프로세스를 통해 잠재 고객에게 필요한 즉시 운영 가능한 소프트웨어를 제공하는 동시에 적절한 제어 및 문서화를 유지할 수 있습니다.

StorageGRID는 오픈 소스 또는 대체 버전이 아닌 "프로덕션 준비" 버전을 제공합니다. 잠재 고객이 프로덕션 라이센스로 업그레이드하지 않는 한 * 지원은 제공되지 않습니다 *.

위 단계에 문제가 있는 경우 StorageGRID.Feedback@netapp.com 으로 문의하십시오.

검증된 타사 솔루션

검증된 타사 솔루션: 개요

NetApp은 파트너와 협력하여 이러한 솔루션을 StorageGRID와 함께 사용할 수 있도록 검증했습니다. 이 섹션의 정보를 검토하여 검증된 솔루션을 확인하고 해당하는 경우 추가 지침을 얻습니다.

NetApp과 함께 업계 최고의 검증된 NetApp 솔루션을 구축하여 포트폴리오 혁신을 가속하고 시장 인지도를 높이며 매출을 늘리십시오. "지금 바로 제휴 파트너가 되십시오".

StorageGRID 12.0 검증된 타사 솔루션

다음 타사 솔루션은 StorageGRID 12.0과 함께 사용하기 위해 검증되었습니다. + 찾고 있는 솔루션이 목록에 없는 경우 NetApp 계정 담당자에게 문의하세요.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 알럭시오
- 아파치 카프카
- AWS 마운트 지점
- 브리지스톤
- 캔템오
- Citrix 콘텐츠 협업
- Collibra(최소 Collibra 데이터 품질 버전 2024.02)
- Commvault 11
- 카우치베이스 엔터프라이즈 애널리틱스 2.0
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 디스크 오버 데이터
- 드리미오
- Elasticsearch 스냅샷(동결된 계층 포함)
- eMAM
- Fujifilm 개체 아카이브

- GitHub 엔터프라이즈 서버
- IBM Filenet
- IBM 스토리지 프로텍트
- 인터카
- 고마프라이즈
- Microsoft SQL Server 빅 데이터 클러스터
- 모델9
- Modzy
- 문워크 유니버설
- 멋져
- 나스니
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- PixitMedia ngenea 를 참조하십시오
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 빌드 220706 이상
- Rubrik CDM
- s3a 를 참조하십시오
- 용감합니다
- 스노우플레이크
- Spectra Logic On-Premise Glacier의 약어입니다
- Splunk 스마트스토어
- 별 모양
- 간편한 보관
- 트리노
- Varnish Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1 이상

- Vertica 10.x
- 비딘
- Virtalica StorageFabric
- Weka v3.10 이상

StorageGRID에서 오브젝트 잠금을 통해 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- CommVault 11 기능 릴리스 26
- IBM Filenet
- IBM 스토리지 프로텍트
- OpenText Documentum 21.4
- Rubrik으로 이동합니다
- Veeam 12
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1 이상

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신
- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 기트랩주식회사
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS
- 품질

- 벨라시아

StorageGRID에서 지원되는 주요 관리자

이러한 솔루션은 테스트를 거쳤습니다.

- Entrust 암호화 보안 플랫폼 v10.4.5
- Entrust KeyControl 10.2
- 하시코프 볼트 1.20.2
- Thales CipherTrust Manager 2.20

StorageGRID 11.9은 타사 솔루션으로 검증되었습니다

다음 타사 솔루션은 StorageGRID 11.9과 함께 사용할 수 있도록 검증되었습니다. + 찾으려는 솔루션이 목록에 없는 경우 NetApp 고객 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 알럭시오
- 아파치 카프카
- AWS 마운트 지점
- 브리지스톤
- 캔템오
- Citrix 콘텐츠 협업
- Collibra(최소 Collibra 데이터 품질 버전 2024.02)
- Commvault 11
- 카우치베이스 엔터프라이즈 애널리틱스 2.0
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 디스크 오버 데이터
- 드리미오
- Elasticsearch 스냅샷(동결된 계층 포함)
- eMAM

- Fujifilm 개체 아카이브
- GitHub 엔터프라이즈 서버
- IBM Filenet
- IBM 스토리지 프로텍트
- 인터카
- 고마프라이즈
- Microsoft SQL Server 빅 데이터 클러스터
- 모델9
- Modzy
- 문워크 유니버설
- 멋져
- 나스니
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- PixitMedia ngenea 를 참조하십시오
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 빌드 220706 이상
- Rubrik CDM
- s3a 를 참조하십시오
- 용감합니다
- 스노우플레이크
- Spectra Logic On-Premise Glacier의 약어입니다
- Splunk 스마트스토어
- 별 모양
- 간편한 보관
- 트리노
- Varnish Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15.1

- Veritas NetBackup 10.1.1 이상
- Vertica 10.x
- 비딘
- Virtalica StorageFabric
- Weka v3.10 이상

StorageGRID에서 오브젝트 잠금을 통해 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- CommVault 11 기능 릴리스 26
- IBM Filenet
- IBM 스토리지 프로텍트
- OpenText Documentum 21.4
- Rubrik으로 이동합니다
- Veeam 12
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1 이상

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신
- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 기트랩주식회사
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS

- 품질
- 벨라시아

StorageGRID에서 지원되는 주요 관리자

이러한 솔루션은 테스트를 거쳤습니다.

- Entrust 암호화 보안 플랫폼 v10.4.5
- Entrust KeyControl 10.2
- Hashicorp 볼트 1.15.0
- Thales CipherTrust Manager 2.0 을 참조하십시오
- Thales CipherTrust 관리자 2.1
- Thales CipherTrust 관리자 2.2
- Thales CipherTrust Manager 2.3
- Thales CipherTrust 관리자 2.4
- Thales CipherTrust Manager 2.8
- Thales CipherTrust 관리자 2.9
- Thales CipherTrust 관리자 2.10
- Thales CipherTrust 관리자 2.11
- Thales CipherTrust 관리자 2.12
- Thales CipherTrust 관리자 2.13
- Thales CipherTrust 관리자 2.14
- Thales CipherTrust Manager 2.15
- Thales CipherTrust Manager 2.16
- Thales CipherTrust Manager 2.20

StorageGRID 11.8은 타사 솔루션으로 검증되었습니다

다음 타사 솔루션은 StorageGRID 11.8과 함께 사용할 수 있도록 검증되었습니다. 를 누릅니다 찾고 있는 솔루션이 목록에 없으면 NetApp 계정 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 알럭시오
- 아파치 카프카
- AWS 마운트 지점

- 브리지스톤
- 캔템오
- Citrix 콘텐츠 협업
- Collibra(최소 Collibra 데이터 품질 버전 2024.02)
- Commvault 11
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 디스크 오버 데이터
- 드리미오
- Elasticsearch 스냅샷(동결된 계층 포함)
- eMAM
- Fujifilm 개체 아카이브
- GitHub 엔터프라이즈 서버
- IBM Filenet
- IBM 스토리지 프로텍트
- 인터카
- 고마프라이즈
- Microsoft SQL Server 빅 데이터 클러스터
- 모델9
- Modzy
- 문워크 유니버설
- 멋져
- 나스니
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- PixitMedia ngenea 를 참조하십시오
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream

- Quantum StorNext 5.4.0.1
- Reveille v10 빌드 220706 이상
- Rubrik CDM
- s3a 를 참조하십시오
- 용감합니다
- 스노우플레이크
- Spectra Logic On-Premise Glacier의 약어입니다
- Splunk 스마트스토어
- 별 모양
- 간편한 보관
- 트리노
- Varnish Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1 이상
- Vertica 10.x
- 비딘
- Virtalica StorageFabric
- Weka v3.10 이상

StorageGRID에서 오브젝트 잠금을 통해 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- CommVault 11 기능 릴리스 26
- IBM Filenet
- IBM 스토리지 프로텍트
- OpenText Documentum 21.4
- Rubrik으로 이동합니다
- Veeam 12
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1 이상

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신

- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 기트랩주식회사
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS
- 품질
- 벨라시아

StorageGRID에서 지원되는 주요 관리자

이러한 솔루션은 테스트를 거쳤습니다.

- Entrust KeyControl 10.2
- Hashicorp 볼트 1.15.0
- Thales CipherTrust Manager 2.0 을 참조하십시오
- Thales CipherTrust 관리자 2.1
- Thales CipherTrust 관리자 2.2
- Thales CipherTrust Manager 2.3
- Thales CipherTrust 관리자 2.4
- Thales CipherTrust Manager 2.8
- Thales CipherTrust 관리자 2.9
- Thales CipherTrust 관리자 2.10
- Thales CipherTrust 관리자 2.11
- Thales CipherTrust 관리자 2.12
- Thales CipherTrust 관리자 2.13
- Thales CipherTrust 관리자 2.14

StorageGRID 11.7 검증된 타사 솔루션

다음 타사 솔루션은 StorageGRID 11.7에서 사용하도록 검증되었습니다. + 찾으려는 솔루션이 목록에 없는 경우 NetApp 고객 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 알럭시오
- 아파치 카프카
- AWS 마운트 지점
- 브리지스톤
- 캔템오
- Citrix 콘텐츠 협업
- Collibra(최소 Collibra 데이터 품질 버전 2024.02)
- Commvault 11
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 디스크 오버 데이터
- 드리미오
- Elasticsearch 스냅샷(동결된 계층 포함)
- eMAM
- Fujifilm 개체 아카이브
- GitHub 엔터프라이즈 서버
- IBM Filenet
- IBM Spectrum Protect Plus
- IBM 스토리지 프로텍트
- 인터카
- 고마프라이즈
- Microsoft SQL Server 빅 데이터 클러스터
- 모델9
- Modzy

- 문워크 유니버설
- 멋져
- 나스니
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- PixitMedia ngenea 를 참조하십시오
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 빌드 220706 이상
- Rubrik CDM
- s3a 를 참조하십시오
- 용감합니다
- 스노우플레이크
- Spectra Logic On-Premise Glacier의 약어입니다
- Splunk 스마트스토어
- 간편한 보관
- 트리노
- Varnish Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 10.1.1 이상
- Vertica 10.x
- 비딘
- Virtalica StorageFabric
- Weka v3.10 이상

StorageGRID에서 오브젝트 잠금을 통해 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- CommVault 11 기능 릴리스 26
- IBM Filenet

- IBM 스토리지 프로텍트
- OpenText Documentum 21.4
- Rubrik으로 이동합니다
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 이상

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신
- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 기트랩주식회사
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS
- 품질
- 벨라시아

StorageGRID에서 지원되는 주요 관리자

이러한 솔루션은 테스트를 거쳤습니다.

- Thales CipherTrust Manager 2.0 을 참조하십시오
- Thales CipherTrust 관리자 2.1
- Thales CipherTrust 관리자 2.2
- Thales CipherTrust Manager 2.3
- Thales CipherTrust 관리자 2.4

- Thales CipherTrust Manager 2.8
- Thales CipherTrust 관리자 2.9

StorageGRID 11.6 검증된 타사 솔루션

다음 타사 솔루션은 StorageGRID 11.6에서 사용하도록 검증되었습니다. + 찾으려는 솔루션이 목록에 없는 경우 NetApp 고객 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 알럭시오
- 아파치 카프카
- 브리지스톤
- 캔템오
- Citrix 콘텐츠 협업
- Commvault 11
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 디스크 오버 데이터
- 드리미오
- eMAM
- Fujifilm 개체 아카이브
- GitHub 엔터프라이즈 서버
- IBM Filenet
- IBM Spectrum Protect Plus
- 인터카
- 고마프라이즈
- Microsoft SQL Server 빅 데이터 클러스터
- 모델9
- Modzy
- 문워크 유니버설
- 멋져

- 나스니
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- PixitMedia ngenea 를 참조하십시오
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10 빌드 220706 이상
- Rubrik CDM
- s3a 를 참조하십시오
- 용감합니다
- 스노우플레이크
- Spectra Logic On-Premise Glacier의 약어입니다
- Splunk 스마트스토어
- 간편한 보관
- 트리노
- Varnish Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Vertica 10.x
- 비딘
- Virtalica StorageFabric
- Weka v3.10 이상

StorageGRID에서 오브젝트 잠금을 통해 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- CommVault 11 기능 릴리스 26
- IBM Filenet
- OpenText Documentum 21.4
- Veeam 12

- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 이상

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신
- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 기트랩주식회사
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS
- 품질
- 벨라시아

StorageGRID 11.5는 타사 솔루션을 검증했습니다

다음 타사 솔루션은 StorageGRID 11.5에서 사용하도록 검증되었습니다. + 찾으려는 솔루션이 목록에 없는 경우 NetApp 고객 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 알럭시오
- 브리지스톤
- 캔템오

- Citrix 콘텐츠 협업
- Commvault 11
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 인터카
- 고마프라이즈
- 문워크 유니버설
- 멋져
- 나스니
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM
- s3a 를 참조하십시오
- 용감합니다
- Splunk 스마트스토어
- 트리노
- Varnish Enterprise 6.0.4
- Veeam 11
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- 비딘
- Virtalica StorageFabric

StorageGRID에서 오브젝트 잠금을 통해 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- OpenText Documentum 21.4
- Veeam 11

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신
- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 기트랩주식회사
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS
- 품질
- 벨라시아

StorageGRID 11.4는 타사 솔루션의 유효성을 검증했습니다

다음 타사 솔루션은 StorageGRID 11.4에서 사용하도록 검증되었습니다. + 찾으려는 솔루션이 목록에 없는 경우 NetApp 고객 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 브리지스톤

- 캔템오
- Citrix 콘텐츠 협업
- Commvault 11
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 인터카
- 고마프라이즈
- 멋져
- 나스니
- OpenText Documentum 16.4
- OpenText InfoArchive 16 EP7
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM
- 용감합니다
- Splunk 스마트스토어
- Varnish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- 비딘

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신

- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS
- 품질
- 벨라시아

StorageGRID 11.3은 타사 솔루션의 유효성을 검증했습니다

다음 타사 솔루션은 StorageGRID 11.3에서 사용하도록 검증되었습니다. + 찾으려는 솔루션이 목록에 없는 경우 NetApp 고객 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 브리지스톤
- 캔템오
- Citrix 콘텐츠 협업
- Commvault 11
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 인터카
- 고마프라이즈
- 멋져

- 나스니
- OpenText Documentum 16.4
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 P1-1342
- 용감합니다
- Splunk 스마트스토어
- Varnish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- 비딘

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신
- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS

- 품질
- 벨라시아

StorageGRID 11.2는 타사 솔루션을 검증했습니다

다음 타사 솔루션은 StorageGRID 11.2에서 사용하도록 검증되었습니다. + 찾으려는 솔루션이 목록에 없는 경우 NetApp 고객 담당자에게 문의하십시오.

StorageGRID에서 검증된 타사 솔루션

이러한 솔루션은 해당 파트너와 협력하여 테스트를 거쳤습니다.

- Actifio(활성)
- 브리지스톤
- 캔템오
- Citrix 콘텐츠 협업
- Commvault 11
- Ctera 포털 6
- 다레트
- 다타도비
- Data Dynamics StorageX를 나타냅니다
- DefendX
- 인터카
- 고마프라이즈
- 멋져
- 나스니
- OpenText Documentum 16.4
- CyanGate Cloud를 사용한 OpenText Media Management 16.5
- 판주라
- 포인트 아카이브 게이트웨이 2.0
- 포인트 스토리지 관리자 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 P1-1342
- 용감합니다
- Splunk 스마트스토어
- Varnish Enterprise 6.0.4
- Veeam 9.5.4

- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- 비딘

StorageGRID에서 지원되는 타사 솔루션

이러한 솔루션은 테스트를 거쳤습니다.

- Archiware를 참조하십시오
- Axis 통신
- 코너 360
- DataFrameworks
- EcoDigital DIVA 플랫폼
- Encoding.com
- Fujifilm 개체 아카이브
- GE Centricity Enterprise Archive
- 하이랜드 아쿠오
- IBM Aspera
- 마일스톤 시스템
- ONSSI
- 리치 엔진
- SilverTrak
- 소프트NAS
- 품질
- 벨라시아

제품 기능 가이드

StorageGRID로 제로 RPO 달성 - 멀티 사이트 복제에 대한 포괄적인 가이드

이 기술 보고서는 사이트 장애 발생 시 복구 지점 목표(RPO)를 0으로 달성하기 위해 StorageGRID 복제 전략을 구현하는 방법에 대한 포괄적인 가이드를 제공합니다. 이 문서에서는 다중 사이트 동기 복제 및 다중 그리드 비동기 복제를 포함하여 StorageGRID 에 대한 다양한 배포 옵션에 대해 자세히 설명합니다. 여기서는 StorageGRID 정보 수명 주기 관리(ILM) 정책을 구성하여 여러 위치에서 데이터 내구성과 가용성을 보장하는 방법을 설명합니다. 또한 이 보고서는 중단 없는 클라이언트 운영을 유지하기 위한 성능 고려 사항, 실패 시나리오 및 복구 프로세스도 다룹니다. 이 문서의 목적은 동기 및 비동기 복제 기술을 모두 활용하여 사이트 전체에 장애가 발생한 경우에도 데이터에 대한 접근 가능성과 일관성을 유지하는 데 필요한 정보를 제공하는 것입니다.

StorageGRID 개요

NetApp StorageGRID는 업계 표준 Amazon S3(Amazon Simple Storage Service) API를 지원하는 오브젝트 기반 스토리지 시스템입니다.

StorageGRID는 정보 라이프사이클 관리 정책(ILM)에 따라 다양한 서비스 수준의 단일 네임스페이스를 여러 위치에서 제공합니다. 이러한 수명 주기 정책을 사용하면 수명 주기 전반에 걸쳐 데이터가 저장되는 위치를 최적화할 수 있습니다.

StorageGRID은 로컬 및 지리적으로 분산된 솔루션에서 구성 가능한 내구성과 데이터 가용성을 지원합니다. 데이터가 온프레미스에 있든 퍼블릭 클라우드에 있든, 통합 하이브리드 클라우드 워크플로를 통해 기업은 Amazon Simple Notification Service(Amazon SNS), Google Cloud, Microsoft Azure Blob, Amazon S3 Glacier, Elasticsearch 등의 클라우드 서비스를 활용할 수 있습니다.

StorageGRID 확장

최소 StorageGRID 배포는 단일 사이트의 관리 노드와 3개의 스토리지 노드로 구성됩니다. 단일 그리드는 최대 220개 노드까지 확장될 수 있습니다. StorageGRID 단일 사이트로 배포하거나 16개 사이트로 확장할 수 있습니다.

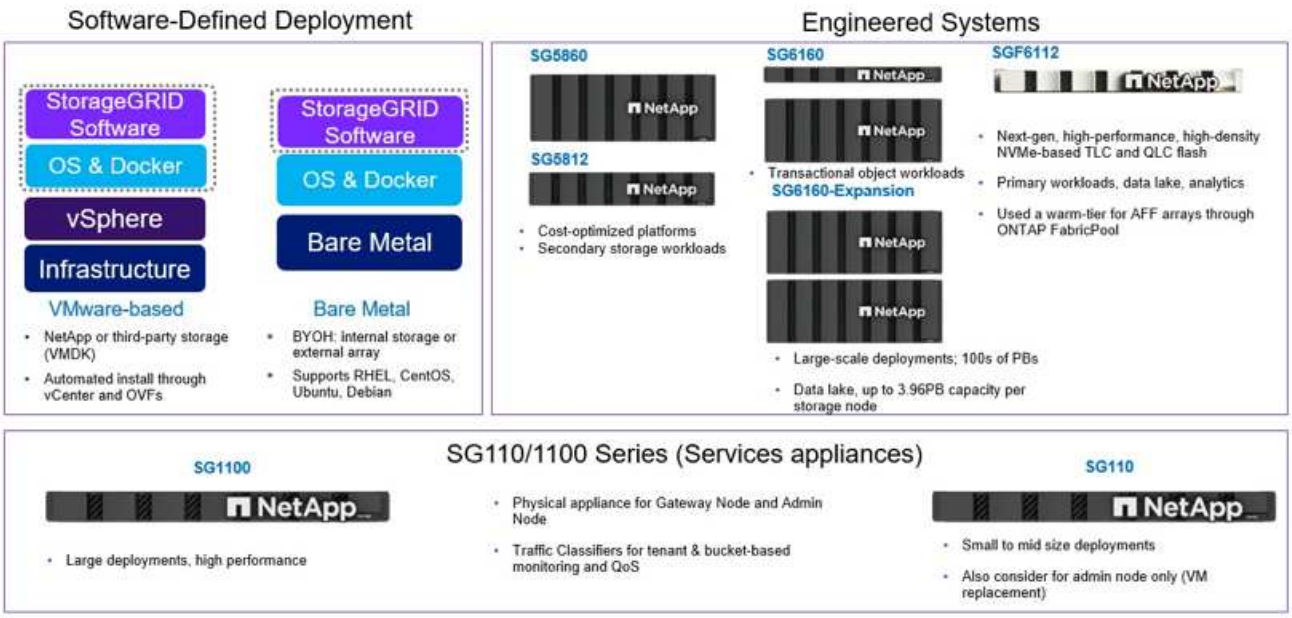
관리 노드에는 측정 항목과 로깅을 위한 중앙 지점인 관리 인터페이스가 포함되어 있으며 StorageGRID 구성 요소의 구성을 유지 관리합니다. 관리자 노드에는 S3 API 액세스를 위한 통합 로드 밸런서도 포함되어 있습니다.

StorageGRID 소프트웨어 전용, VMware 가상 머신 어플라이언스 또는 특수 목적 어플라이언스로 배포할 수 있습니다.

스토리지 노드는 다음과 같이 배포될 수 있습니다.

- 객체 수를 최대화하는 메타데이터 전용 노드
- 객체 공간을 극대화하는 객체 스토리지 전용 노드
- 객체 수와 객체 공간을 모두 추가하는 결합된 메타데이터 및 객체 스토리지 노드

각 스토리지 노드는 수백 페타바이트 규모의 단일 네임스페이스를 허용하는 객체 스토리지의 멀티 페타바이트 용량으로 확장될 수 있습니다. StorageGRID 게이트웨이 노드라고 하는 S3 API 작업을 위한 통합 로드 밸런서도 제공합니다.



StorageGRID 사이트 토폴로지에 배치된 노드 컬렉션으로 구성됩니다. StorageGRID 의 사이트는 고유한 물리적 위치일 수도 있고, 논리적 구조로 그리드의 다른 사이트와 공유되는 물리적 위치에 상주할 수도 있습니다. StorageGRID 사이트는 여러 물리적 위치에 걸쳐 있어서는 안 됩니다. 사이트는 공유된 LAN(Local Area Network) 인프라와 장애 도메인을 나타냅니다.

StorageGRID 및 장애 도메인

StorageGRID에는 장애 위험을 완화하기 위해 솔루션 설계 방법, 데이터 저장 방법 및 데이터 저장 위치를 결정할 때 고려해야 할 여러 계층의 장애 도메인이 포함되어 있습니다.

- 그리드 수준 - 여러 사이트로 구성된 그리드는 사이트 장애 또는 격리를 가질 수 있으며 액세스 가능한 사이트는 그리드로 계속 작동할 수 있습니다.
- 사이트 수준 - 사이트 내의 장애가 발생하면 해당 사이트의 운영에 영향을 줄 수 있지만 나머지 그리드에는 영향을 주지 않습니다.
- 노드 레벨 - 노드 장애는 사이트 운영에 영향을 미치지 않습니다.
- 디스크 레벨 - 디스크 장애는 노드 작동에 영향을 주지 않습니다.

오브젝트 데이터 및 메타데이터

오브젝트 스토리지의 경우, 스토리지 단위는 파일 또는 블록이 아닌 오브젝트입니다. 파일 시스템 또는 블록 스토리지의 트리와 같은 계층구조와 달리 오브젝트 스토리지는 데이터를 구조화되지 않은 단순 레이아웃으로 구성합니다. 오브젝트 스토리지는 데이터의 물리적 위치를 해당 데이터를 저장하고 검색하는 데 사용되는 메서드에서 분리합니다.

오브젝트 기반 스토리지 시스템의 각 오브젝트에는 오브젝트 데이터와 오브젝트 메타데이터의 두 부분이 있습니다.

- 객체 데이터는 실제 기본 데이터를 나타냅니다. 예를 들어 사진, 영화, 의료 기록 등이 있습니다.
- 개체 메타데이터는 개체를 설명하는 정보입니다.

StorageGRID는 오브젝트 메타데이터를 사용하여 그리드 전체의 모든 오브젝트의 위치를 추적하고 각 오브젝트의 라이프사이클 관리를 제공합니다.

오브젝트 메타데이터에는 다음과 같은 정보가 포함됩니다.

- 각 개체의 고유 ID, 개체 이름, S3 버킷 이름, 테넌트 계정 이름 또는 ID, 개체의 논리적 크기, 개체가 처음 생성된 날짜 및 시간, 개체가 마지막으로 수정된 날짜 및 시간을 포함한 시스템 메타데이터입니다.
- 각 객체의 복제본 사본이나 삭제 코드화된 조각의 현재 저장 위치입니다.
- 객체와 연결된 모든 사용자 메타데이터 키 값 쌍입니다.
- S3 오브젝트의 경우 오브젝트와 연결된 모든 오브젝트 태그 키-값 쌍입니다
- 세그먼트화된 객체와 다중 파트 객체의 경우 세그먼트 식별자와 데이터 크기입니다.

개체 메타데이터는 사용자 지정이 가능하며 확장이 가능하므로 응용 프로그램에서 유연하게 사용할 수 있습니다. StorageGRID에서 오브젝트 메타데이터를 저장하는 방법과 위치에 대한 자세한 내용은 를 참조하십시오 "오브젝트 메타데이터 스토리지 관리".

StorageGRID의 ILM(정보 라이프사이클 관리) 시스템은 StorageGRID 시스템의 모든 오브젝트 데이터에 대한 배치, 기간 및 수집 동작을 조정하는 데 사용됩니다. ILM 규칙은 StorageGRID에서 오브젝트의 복제본을 사용하거나 노드 및 사이트 간에 오브젝트를 삭제 코딩하여 시간에 따라 저장하는 방식을 결정합니다. 이 ILM 시스템은 그리드 내의 객체 데이터 일관성을 담당합니다.

삭제 코딩

StorageGRID 노드 수준과 드라이브 수준에서 코드 데이터를 지우는 기능을 제공합니다. StorageGRID 어플라이언스를 사용하면 노드 내의 모든 드라이브에 저장된 데이터의 삭제 코드를 작성하여 여러 디스크 장애로 인한 데이터 손실이나 중단으로부터 로컬 보호를 제공합니다. 드라이브 장애로 인한 재구축은 노드에 국한되므로 네트워크를 통해 데이터를 복제할 필요가 없습니다.

또한 StorageGRID 어플라이언스는 StorageGRID의 ILM 규칙을 통해 노드 장애로부터 보호하면서, 삭제 코딩 방식을 사용하여 사이트 내의 노드 전체 또는 StorageGRID 시스템의 3개 이상의 사이트에 걸쳐 개체 데이터를 저장합니다.

삭제 코딩은 복제보다 오버헤드가 낮으면서 노드 및 사이트 장애에 대한 복원력이 뛰어난 스토리지 레이아웃을 제공합니다. 모든 StorageGRID 삭제 코딩 체계는 데이터 청크를 저장하는 데 필요한 최소 노드 수가 충족되는 경우 단일 사이트에 배포할 수 있습니다. 즉, 4+2의 EC 체계에서는 데이터를 수신할 수 있는 노드가 최소 6개 있어야 합니다.

Erasure-coding scheme (*k+m*)	Minimum number of deployed sites	Recommended number of Storage Nodes at each site	Total recommended number of Storage Nodes	Site loss protection?	Storage overhead
4+2	3	3	9	Yes	50%
6+2	4	3	12	Yes	33%
8+2	5	3	15	Yes	25%
6+3	3	4	12	Yes	50%
9+3	4	4	16	Yes	33%
2+1	3	3	9	Yes	50%
4+1	5	3	15	Yes	25%
6+1	7	3	21	Yes	17%
7+5	3	5	15	Yes	71%

메타데이터 정합성

StorageGRID에서 메타데이터는 일반적으로 사이트당 3개의 복제본으로 저장되므로 정합성 보장 및 가용성이 보장됩니다. 이러한 중복성은 장애가 발생한 경우에도 데이터 무결성과 접근성을 유지할 수 있도록 도와줍니다.

기본 일관성은 그리드 전체에서 정의됩니다. 사용자는 언제든지 버킷 수준에서 일관성을 변경할 수 있습니다.

StorageGRID에서 사용할 수 있는 버킷 일관성 옵션은 다음과 같습니다.

- * 모두 *: 최고 수준의 일관성을 제공합니다. 그리드의 모든 노드가 즉시 데이터를 수신하면 요청이 실패합니다.
- 강력한 글로벌:
  - 레거시 스트롱 글로벌: 모든 사이트의 모든 클라이언트 요청에 대해 읽기-쓰기 일관성을 보장합니다.
    - 이는 새로운 Quorum Strong Global로 수동으로 변경하지 않고도 11.9 이하 버전에서 12.0으로 업그레이드한 모든 시스템에 적용되는 기본 동작입니다.
  - **Quorum Strong-global**: 모든 사이트의 모든 클라이언트 요청에 대해 읽기-쓰기 일관성을 보장합니다. 메타데이터 복제본 쿼럼을 달성할 수 있는 경우 여러 노드 또는 사이트 장애에도 일관성을 제공합니다.
    - 이는 12.0 이상으로 새로 설치된 모든 시스템에 대한 기본 동작입니다.
    - QUORUM 일관성은 각 사이트에 3개의 메타데이터 복제본이 있는 스토리지 노드 메타데이터 복제본의 쿼럼으로 정의됩니다. 다음과 같이 계산할 수 있습니다. 1+((N*3)/2) 여기서 N은 총 사이트 수입니다.
    - 예를 들어, 3개 사이트 그리드에서 최소 5개의 복제본을 만들어야 하며, 사이트 내에는 최대 3개의 복제본이 있어야 합니다.
- * 강력한 사이트 *: 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
- * Read-after-new-write * (기본값): 새 개체에 대해 읽기-쓰기 후 일관성을 제공하고 개체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 대부분의 경우에 권장됩니다.

- * 사용 가능 *: 새 객체 및 객체 업데이트 모두에 대한 최종 일관성을 제공합니다. S3 버킷의 경우 필요한 경우에만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷의 경우 또는 존재하지 않는 키의 헤드 또는 GET 작업의 경우). S3 FabricPool 버킷은 지원되지 않습니다.

오브젝트 데이터 정합성

사이트 내부 및 사이트 간에 메타데이터가 자동으로 복제되지만, 오브젝트 데이터 스토리지를 배치할 결정은 사용자의 몫입니다. 오브젝트 데이터는 사이트 내부 및 사이트 간 복제본에 저장되거나, 사이트 내부 또는 사이트 간 삭제 코딩되거나, 복제 및 삭제 코딩 스토리지 스키마의 조합에 저장될 수 있습니다. ILM 규칙은 모든 오브젝트에 적용되거나 특정 오브젝트, 버킷 또는 테넌트에만 적용되도록 필터링될 수 있습니다. ILM 규칙은 객체의 저장 방식, 복제본 및/또는 삭제 코딩 방식, 해당 위치에 객체가 저장되는 기간, 복제본 또는 삭제 코딩 체계 수가 변경되거나 위치가 시간에 따라 변경될 경우 정의합니다.

각 ILM 규칙은 오브젝트 보호를 위한 세 가지 수집 동작 중 하나인 이중 커밋, 균등 또는 엄격 으로 구성됩니다.

듀얼 커밋 옵션은 그리드 내의 두 개의 서로 다른 스토리지 노드에 두 개의 사본을 즉시 만들고 클라이언트에게 요청이 성공했다는 것을 반환합니다. 노드 선택은 요청 사이트 내에서 시도되지만 어떤 상황에서는 다른 사이트의 노드를 사용할 수도 있습니다. 해당 객체는 ILM 대기열에 추가되어 ILM 규칙에 따라 평가되고 배치됩니다.

균형 잡힌 옵션은 ILM 정책에 대해 객체를 즉시 평가하고 클라이언트에게 요청을 성공적으로 반환하기 전에 객체를 동기적으로 배치합니다. 중단이나 배치 요구 사항을 충족할 만큼의 저장 공간이 부족하여 ILM 규칙을 즉시 충족할 수 없는 경우 대신 이중 커밋이 사용됩니다. 문제가 해결되면 ILM은 정의된 규칙에 따라 객체를 자동으로 배치합니다.

엄격한 옵션은 ILM 정책에 대해 객체를 즉시 평가하고 클라이언트에게 요청을 성공적으로 반환하기 전에 객체를 동기적으로 배치합니다. 중단이나 배치 요구 사항을 충족할 만큼의 저장 공간이 부족하여 ILM 규칙을 즉시 충족할 수 없는 경우 요청은 실패하고 클라이언트는 다시 시도해야 합니다.

로드 밸런싱

StorageGRID는 통합 게이트웨이 노드, 외부 타사 로드 밸런서, DNS 라운드 로빈 또는 스토리지 노드에 대한 직접 클라이언트 액세스를 통해 배포할 수 있습니다. 한 사이트에 여러 게이트웨이 노드를 구축하고 고가용성 그룹으로 구성하여 게이트웨이 노드가 중단될 경우 자동 페일오버 및 장애 복구를 제공할 수 있습니다. 솔루션에 로드 밸런싱 방법을 결합하여 솔루션의 모든 사이트에 대한 단일 액세스 지점을 제공할 수 있습니다.

게이트웨이 노드는 기본적으로 게이트웨이 노드가 있는 사이트의 스토리지 노드 간에 부하를 분산합니다. StorageGRID 구성하면 게이트웨이 노드가 여러 사이트의 노드를 사용하여 부하를 분산할 수 있습니다. 이 구성을 사용하면 클라이언트 요청에 대한 응답 지연에 해당 사이트 간의 지연이 추가됩니다. 이는 전체 지연 시간이 클라이언트에게 허용되는 경우에만 구성해야 합니다.

로컬 및 글로벌 부하 분산을 결합하면 RTO를 0으로 보장할 수 있습니다. 중단 없는 클라이언트 액세스를 보장하려면 클라이언트 요청의 부하 분산이 필요합니다. StorageGRID 솔루션은 각 사이트에 여러 개의 게이트웨이 노드와 고가용성 그룹을 포함할 수 있습니다. 사이트 장애 발생 시에도 모든 사이트의 클라이언트에 중단 없는 액세스를 제공하려면 StorageGRID Gateway 노드와 함께 외부 부하 분산 솔루션을 구성해야 합니다. 각 사이트 내의 부하를 관리하는 Gateway 노드 고가용성 그룹을 구성하고 외부 부하 분산 장치를 사용하여 고가용성 그룹 전체에서 부하를 분산합니다. 외부 로드 밸런서는 요청이 운영 사이트에만 전송되는지 확인하기 위해 상태 검사를 수행하도록 구성되어야 합니다. StorageGRID 사용한 부하 분산에 대한 자세한 내용은 다음을 참조하세요. "StorageGRID 로드 밸런서 기술 보고서".

StorageGRID 사용한 Zero RPO 요구 사항

오브젝트 스토리지 시스템에서 RPO(복구 시점 목표)를 0으로 달성하려면 장애 발생 시 다음 사항이 중요합니다.

- 메타데이터와 개체 콘텐츠 모두 동기화되며 정합성이 보장되는 것으로 간주됩니다

- 오류가 발생해도 개체 콘텐츠에 액세스할 수 있습니다.

다중 사이트 배포의 경우 Quorum Strong Global은 모든 사이트에서 메타데이터가 동기화되도록 보장하는 기본 일관성 모델로, 0 RPO 요구 사항을 충족하는 데 필수적입니다.

저장 시스템의 객체는 정보 수명 주기 관리(ILM) 규칙에 따라 저장됩니다. 이 규칙은 데이터가 수명 주기 전반에 걸쳐 어떻게, 어디에 저장되는지를 결정합니다. 동기 복제의 경우 엄격한 실행과 균형 실행을 고려할 수 있습니다.

- 이러한 ILM 규칙을 엄격하게 실행해야 제로 RPO에 대해 엄격한 실행이 필요합니다. 왜냐하면 지연 또는 폴백 없이 정의된 위치에 오브젝트를 배치하고 데이터 가용성과 일관성을 유지할 수 있기 때문입니다.
- StorageGRID의 ILM 밸런스 수집 동작은 고가용성과 복구 성능 간의 균형을 유지하여 사이트 장애 시에도 사용자가 데이터를 계속 수집할 수 있도록 합니다.

여러 사이트에 동기 배포

다중 사이트 솔루션**:** StorageGRID 사용하면 그리드 내의 여러 사이트에 걸쳐 객체를 동기적으로 복제할 수 있습니다. 균형이나 엄격한 동작을 포함하는 정보 수명 주기 관리(ILM) 규칙을 설정하면 객체가 지정된 위치에 즉시 배치됩니다. 버킷 일관성 수준을 Quorum Strong Global로 구성하면 동기식 메타데이터 복제도 보장됩니다. StorageGRID 단일 글로벌 네임스페이스를 사용하여 객체 배치 위치를 메타데이터로 저장하므로 모든 노드가 모든 복사본이나 삭제 코드 조각의 위치를 알 수 있습니다. 요청이 이루어진 사이트에서 객체를 검색할 수 없는 경우 장애 조치 절차가 필요 없이 원격 사이트에서 자동으로 객체를 검색합니다.

장애가 해결되면 수동으로 페일백을 수행할 필요가 없습니다. 복제 성능은 네트워크 처리량이 가장 낮고 지연 시간이 가장 짧으며 성능이 가장 낮은 사이트에 따라 달라집니다. 사이트의 성능은 노드 수, CPU 코어 수 및 속도, 메모리, 드라이브 수 및 드라이브 유형에 따라 달라집니다.

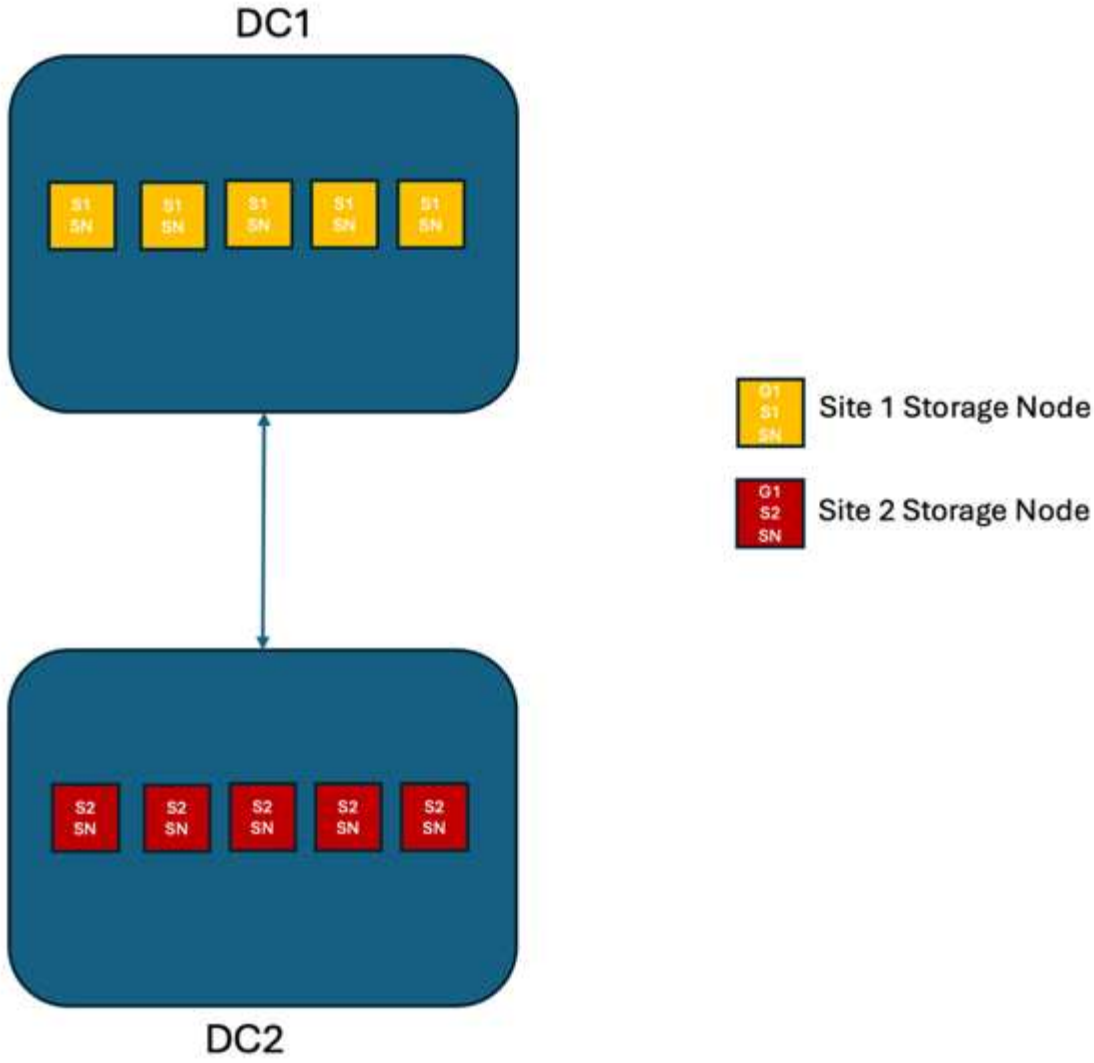
- 다중 그리드 솔루션: * StorageGRID는 교차 그리드 복제(CGR)를 사용하여 여러 StorageGRID 시스템 간에 테넌트, 사용자 및 버킷을 복제할 수 있습니다. CGR은 선택한 데이터를 16개 이상의 사이트로 확장하고, 오브젝트 저장소의 사용 가능 용량을 늘리며, 재해 복구를 제공할 수 있습니다. CGR을 이용한 버킷 복제에는 객체, 객체 버전 및 메타데이터가 포함되며 양방향 또는 단방향 복제일 수 있습니다. RPO(복구 지점 목표)는 각 StorageGRID 시스템의 성능과 이러한 시스템 간의 네트워크 연결에 따라 달라집니다.
- 요약 : *
- 그리드 내 복제에는 동기식 및 비동기식 복제가 포함되며, ILM 수집 동작 및 메타데이터 정합성 제어를 사용하여 구성 가능합니다.
- 그리드 간 복제는 비동기식만 가능합니다.

단일 그리드 다중 사이트 배포

다음 시나리오에서 StorageGRID 솔루션은 통합 로드 밸런서 고가용성 그룹에 대한 요청을 관리하는 선택적 외부 로드 밸런서로 구성됩니다. 이를 통해 RPO가 0인 것 외에도 RTO도 0이 됩니다. ILM은 동기식 배치를 위한 균형 잡힌 수집 보호 기능으로 구성됩니다. 각 버킷은 3개 이상의 사이트 그리드의 경우 강력한 글로벌 일관성 모델의 Quorum 버전으로 구성되고, 2개 사이트의 경우 강력한 글로벌 일관성의 레거시 버전으로 구성됩니다.

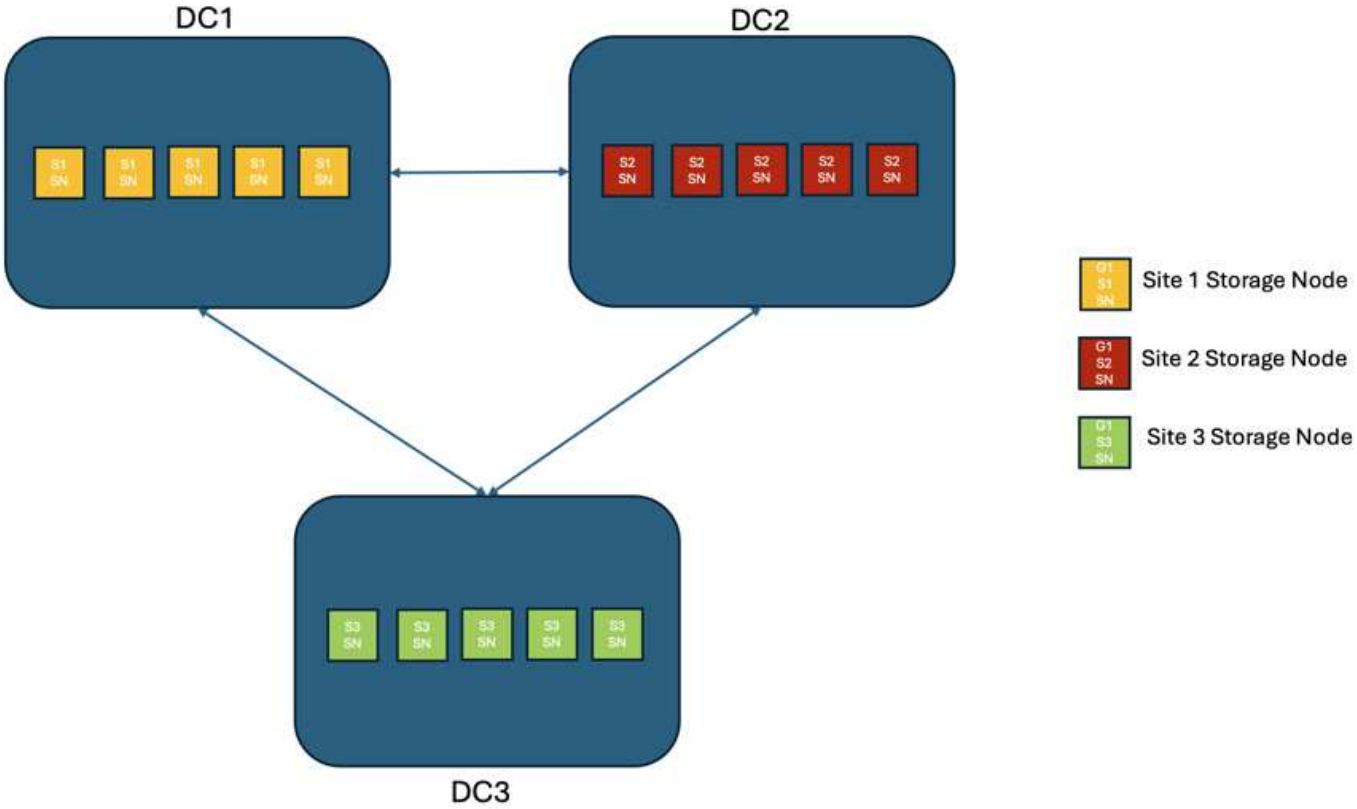
시나리오 **1:**

2개 사이트 StorageGRID 솔루션에는 모든 객체의 복제본이 최소 2개 있고 모든 메타데이터의 복제본이 6개 있습니다. 장애 복구 시, 장애로 인한 업데이트는 복구된 사이트/노드에 자동으로 동기화됩니다. 사이트가 2개뿐이므로 전체 사이트가 손실되는 상황을 넘어 장애 발생 시 RPO를 0으로 유지하는 것은 불가능합니다.



시나리오 **2:**

3개 이상의 사이트로 구성된 StorageGRID 솔루션에는 모든 객체의 복제본 또는 EC 청크가 최소 3개 있고 모든 메타데이터의 복제본은 9개 있습니다. 장애 복구 시, 장애로 인한 업데이트는 복구된 사이트/노드에 자동으로 동기화됩니다. 사이트가 3개 이상인 경우 RPO를 0으로 설정하는 것이 가능합니다.



다중 사이트 장애 시나리오

실패	**2**개 사이트 결과 **+** 강력한 글로벌 레거시	**3**개 이상의 사이트 결과 **+ Quorum Strong Global**
단일 노드 드라이브에 장애	각 어플라이언스는 여러 디스크 그룹을 사용하며 중단이나 데이터 손실 없이 그룹당 최소 1개의 드라이브를 유지할 수 있습니다.	각 어플라이언스는 여러 디스크 그룹을 사용하며 중단이나 데이터 손실 없이 그룹당 최소 1개의 드라이브를 유지할 수 있습니다.
단일 사이트에 단일 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.	운영 중단 또는 데이터 손실이 없습니다.
단일 사이트에 다중 노드 장애 발생	이 사이트로 리디렉션된 클라이언트 작업이 중단되지만 데이터는 손실되지 않습니다. 다른 사이트로 리디렉션된 작업은 중단 없이 지속되며 데이터 손실이 없습니다.	작업은 다른 모든 사이트로 전송되며 중단 없이 데이터 손실이 없습니다.

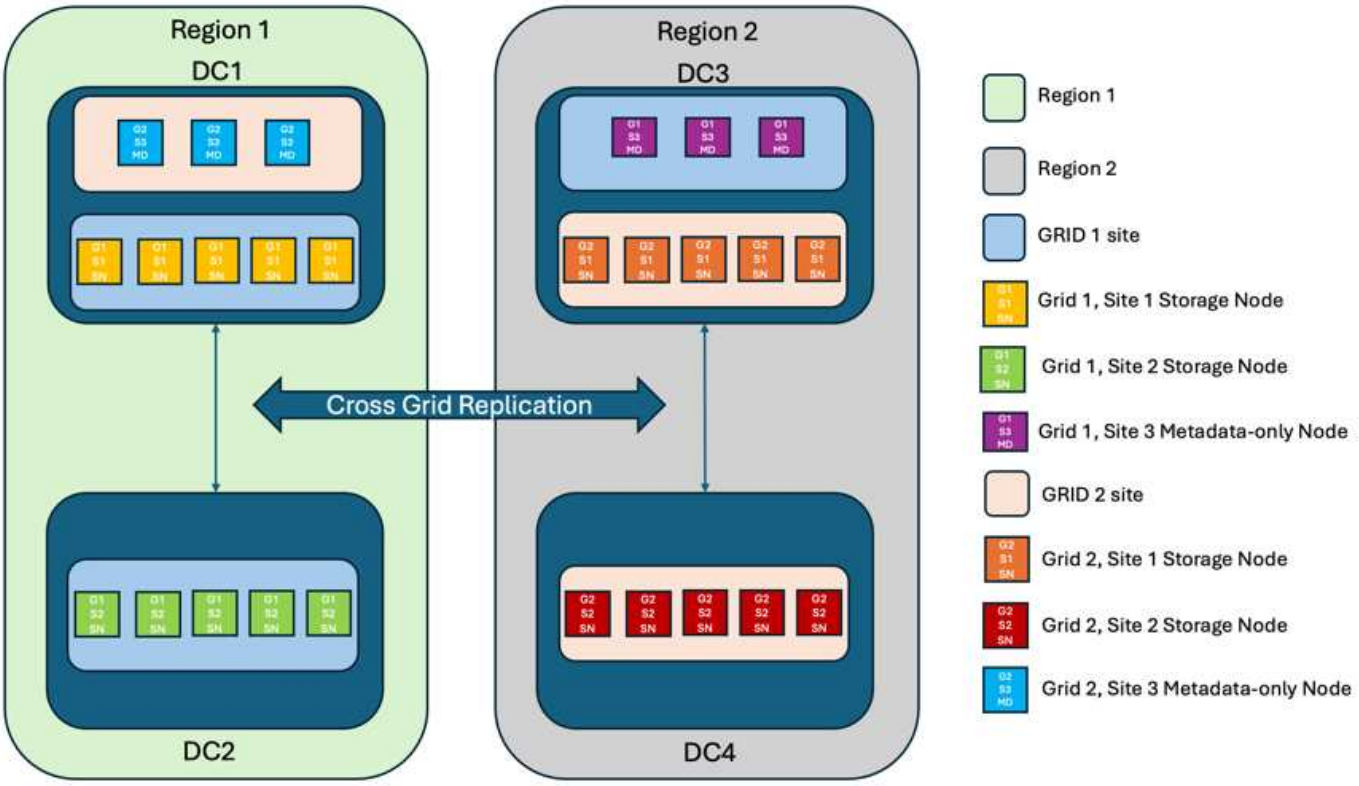
실패	**2**개 사이트 결과 **+** 강력한 글로벌 레거시	**3**개 이상의 사이트 결과 **+ Quorum Strong Global**
여러 사이트에서 단일 노드 장애 발생	다음과 같은 경우 중단 또는 데이터 손실 없음: • 그리드에 최소 하나의 복제본이 존재합니다. • 그리드에 충분한 EC 청크가 있습니다 작업이 중단되고 다음과 같은 경우 데이터 손실 위험이 있습니다. • 복제본이 존재하지 않습니다 • EC 척이 부족합니다	다음과 같은 경우 중단 또는 데이터 손실 없음: • 그리드에 최소한 하나의 복제본이 존재합니다. • 그리드에 충분한 EC 청크가 있습니다 작업이 중단되고 다음과 같은 경우 데이터 손실 위험이 있습니다. • 복제본이 존재하지 않습니다 • 개체를 검색할 EC 척이 부족합니다
단일 사이트 장애	일부 클라이언트 작업은 장애가 해결될 때까지 중단됩니다. GET 및 HEAD 작업은 중단 없이 계속 진행됩니다. 이 실패 상태에서도 중단 없이 작업을 계속하려면 버킷 일관성을 읽기-새로 쓰기로 줄이거나 낮추세요.	운영 중단 또는 데이터 손실이 없습니다.
단일 사이트 및 단일 노드 장애	일부 클라이언트 작업은 장애가 해결될 때까지 중단됩니다. HEAD 운영은 중단 없이 계속됩니다. 복제본이나 충분한 EC 청크가 있는 경우 GET 작업은 중단 없이 계속됩니다. 이 실패 상태에서도 중단 없이 작업을 계속하려면 버킷 일관성을 읽기-새로 쓰기로 줄이거나 낮추세요.	운영이 중단되거나 데이터가 손실되지 않습니다. 복제본 수에 따라 데이터 손실이 발생할 수 있습니다. 로컬 삭제 코딩을 통해 데이터 손실을 방지할 수 있습니다.
단일 사이트 + 나머지 각 사이트의 노드 1개	두 개의 사이트만 존재합니다. 참조: 단일 사이트와 단일 노드.	메타데이터 복제본 쿼럼을 충족하지 못하면 작업이 중단됩니다. 이 실패 상태에서도 중단 없이 작업을 계속하려면 버킷 일관성을 읽기-새로 쓰기로 줄이거나 낮추세요. 복제본 수에 따라 영구적인 실패로 인한 데이터 손실이 발생할 수 있습니다. 로컬 삭제 코딩을 통해 데이터 손실을 방지할 수 있습니다.

실패	**2**개 사이트 결과 **+** 강력한 글로벌 레거시	**3**개 이상의 사이트 결과 **+ Quorum Strong Global**
다중 사이트 장애	운영 중인 사이트는 더 이상 남아 있지 않습니다. 적어도 하나의 사이트를 전체적으로 복구할 수 없는 경우 데이터가 손실됩니다.	메타데이터 복제본 쿼럼을 충족하지 못하면 작업이 중단됩니다. 이 실패 상태에서도 중단 없이 작업을 계속하려면 버킷 일관성을 읽기-새로 쓰기로 줄이거나 낮추세요. 충분한 삭제 코드 청크가 남아 있지 않으면 영구적인 오류로 인해 데이터가 손실될 가능성이 있습니다. 로컬 삭제 코딩이나 복제 사본을 사용하면 데이터 손실을 방지할 수 있습니다.
사이트의 네트워크 격리	오류가 해결될 때까지 클라이언트 작업이 중단됩니다. 이 실패 상태에서도 중단 없이 작업을 계속하려면 버킷 일관성을 읽기-새로 쓰기로 줄이거나 낮추세요. 데이터 손실 없음	격리된 사이트의 운영은 중단되지만 데이터 손실은 발생하지 않습니다. 이 실패 상태에서도 중단 없이 작업을 계속하려면 버킷 일관성을 읽기-새로 쓰기로 줄이거나 낮추세요. 나머지 사이트에서는 운영이 중단되지 않으며 데이터 손실도 없습니다.

다중 사이트 다중 그리드 배포

중복성을 한층 더 강화하기 위해 이 시나리오에서는 두 개의 StorageGRID 클러스터를 사용하고 그리드 간 복제를 사용하여 동기화를 유지합니다. 이 솔루션의 경우 각 StorageGRID 클러스터에는 3개의 사이트가 있습니다. 두 사이트는 객체 스토리지와 메타데이터에 사용되고, 세 번째 사이트는 메타데이터에만 사용됩니다. 두 시스템 모두 두 데이터 사이트 각각에서 삭제 코딩을 사용하여 객체를 동기적으로 저장하기 위한 균형 잡힌 ILM 규칙으로 구성됩니다. 버킷은 Quorum Strong Global 일관성 모델로 구성됩니다. 각 그리드는 모든 버킷에서 양방향 크로스 그리드 복제를 구성합니다. 이는 지역 간 비동기 복제를 제공합니다. 선택적으로 글로벌 로드 밸런서를 구현하여 두 StorageGRID 시스템의 통합 로드 밸런서 고가용성 그룹에 대한 요청을 관리하여 RPO를 0으로 설정할 수 있습니다.

이 솔루션은 두 지역으로 균등하게 분할된 4개의 위치를 사용합니다. 영역 1은 그리드 1의 스토리지 사이트 2개를 영역의 기본 그리드로 포함하고 그리드 2의 메타데이터 사이트를 포함합니다. 영역 2는 그리드 2의 스토리지 사이트 2개를 영역의 기본 그리드로 포함하고 그리드 1의 메타데이터 사이트를 포함합니다. 각 영역에서 동일한 위치에 다른 영역 그리드의 메타데이터 전용 사이트와 해당 영역의 기본 그리드의 스토리지 사이트가 포함될 수 있습니다. 메타데이터만 세 번째 사이트로 사용하면 메타데이터에 필요한 일관성을 제공할 수 있고 해당 위치에 있는 객체의 저장소를 복제할 수 없습니다.



이 솔루션은 4개의 별도 위치를 통해 RPO를 0으로 유지하는 2개의 개별 StorageGRID 시스템을 완벽하게 이중화하고 멀티 사이트 동기식 복제와 멀티 그리드 비동기식 복제를 모두 활용합니다. 두 StorageGRID 시스템에서 아무런 중단 없는 클라이언트 작업을 유지하면서 단일 사이트에 장애가 발생할 수 있습니다.

이 솔루션에는 모든 오브젝트에 대해 삭제 코딩 4개의 복사본과 모든 메타데이터에 대한 복제본 18개가 있습니다. 따라서 클라이언트 작업에 영향을 주지 않고 여러 가지 장애 시나리오가 발생할 수 있습니다. 장애 발생 시 중단 시 복구 업데이트가 자동으로 장애가 발생한 사이트/노드에 동기화됩니다.

다중 사이트, 다중 그리드 장애 시나리오

실패	결과
단일 노드 드라이브에 장애	각 어플라이언스는 여러 디스크 그룹을 사용하며 중단이나 데이터 손실 없이 그룹당 최소 1개의 드라이브를 유지할 수 있습니다.
그리드에서 한 사이트에 단일 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
각 그리드에서 한 사이트에 단일 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
그리드에서 한 사이트에 다중 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
각 그리드에서 한 사이트에 여러 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
그리드의 여러 사이트에서 단일 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
각 그리드의 여러 사이트에서 단일 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
그리드에서 단일 사이트 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
각 그리드에서 단일 사이트 장애 발생	운영 중단 또는 데이터 손실이 없습니다.
그리드에서 단일 사이트와 단일 노드 장애 발생	운영 중단 또는 데이터 손실이 없습니다.

실패	결과
단일 사이트 + 나머지 각 사이트의 노드 1개가 단일 그리드에 포함됩니다	운영 중단 또는 데이터 손실이 없습니다.
단일 위치 장애	운영 중단 또는 데이터 손실이 없습니다.
각 그리드 DC1 및 DC3의 단일 위치 오류	장애가 해결되거나 버킷 일관성이 낮아질 때까지 작업이 중단됩니다. 각 그리드에서 2개의 사이트가 손실됩니다 모든 데이터는 여전히 2개 위치에 있습니다
각 그리드 DC1 및 DC4 또는 DC2 및 DC3의 단일 위치 오류	운영 중단 또는 데이터 손실이 없습니다.
각 그리드 DC2 및 DC4의 단일 위치 오류	운영 중단 또는 데이터 손실이 없습니다.
사이트의 네트워크 격리	격리된 사이트의 작업은 중단되지만 데이터는 손실되지 않습니다 나머지 사이트에서 작업을 중단하거나 데이터가 손실되지 않습니다.

결론

StorageGRID로 복구 시점 목표(RPO)를 0으로 달성하는 것은 사이트 장애 발생 시 데이터 내구성과 가용성을 보장하는 데 있어 매우 중요한 목표입니다. 다중 사이트 동기식 복제 및 다중 그리드 비동기식 복제를 비롯한 StorageGRID의 강력한 복제 전략을 활용하여 조직은 클라이언트 작업을 중단 없이 유지하고 여러 위치에서 데이터 일관성을 유지할 수 있습니다. ILM(정보 수명 주기 관리) 정책을 구현하고 메타데이터 전용 노드를 사용하면 시스템의 복원력과 성능이 더욱 향상됩니다. StorageGRID을 사용하면 복잡한 장애 시나리오에서도 데이터에 액세스하고 일관되게 유지할 수 있으므로 데이터를 자신 있게 관리할 수 있습니다. 이러한 포괄적인 데이터 관리 및 복제 접근 방식은 제로 RPO를 달성하고 소중한 정보를 보호하는 데 있어 세심한 계획과 실행의 중요성을 강조합니다.

AWS 또는 Google Cloud용 클라우드 스토리지 풀을 생성합니다

StorageGRID 오브젝트를 외부 S3 버킷으로 이동하려는 경우 클라우드 스토리지 풀을 사용할 수 있습니다. 외부 버킷은 Amazon S3(AWS) 또는 Google Cloud에 속할 수 있습니다.

필요한 것

- StorageGRID 11.6이 구성되었습니다.
- AWS 또는 Google Cloud에서 외부 S3 버킷을 이미 설정했습니다.

단계

1. Grid Manager에서 * ILM * > * 스토리지 풀 * 으로 이동합니다.
2. 페이지의 클라우드 스토리지 풀 섹션에서 * 생성 * 을 선택합니다.

   Create Cloud Storage Pool 팝업이 나타납니다.

3. 표시 이름을 입력합니다.

4. 공급자 유형 드롭다운 목록에서 * Amazon S3 * 를 선택합니다.

   이 공급자 유형은 AWS S3 또는 Google Cloud에서 작동합니다.

5. 클라우드 스토리지 풀에 사용할 S3 버킷의 URI를 입력합니다.

   다음 두 가지 형식이 허용됩니다.

   "https://host:port`

   "http://host:port`

6. S3 버킷 이름을 입력합니다.

   지정하는 이름은 S3 버킷의 이름과 정확히 일치해야 합니다. 그렇지 않으면 클라우드 스토리지 풀을 생성하지 못합니다. 클라우드 스토리지 풀을 저장한 후에는 이 값을 변경할 수 없습니다.

7. 선택적으로 액세스 키 ID와 비밀 액세스 키를 입력합니다.
8. 드롭다운에서 * 인증서 확인 안 함 * 을 선택합니다.
9. 저장 * 을 클릭합니다.

예상 결과

Amazon S3 또는 Google Cloud에 대한 클라우드 스토리지 풀이 생성되었는지 확인합니다.

Jonathan Wong이 _

Azure Blob Storage용 클라우드 스토리지 풀 생성

StorageGRID 오브젝트를 외부 Azure 컨테이너로 이동하려는 경우 클라우드 스토리지 풀을 사용할 수 있습니다.

필요한 것

- StorageGRID 11.6이 구성되었습니다.
- 외부 Azure 컨테이너를 이미 설정했습니다.

단계

1. Grid Manager에서 * ILM * > * 스토리지 풀 * 으로 이동합니다.
2. 페이지의 클라우드 스토리지 풀 섹션에서 * 생성 * 을 선택합니다.

   Create Cloud Storage Pool 팝업이 나타납니다.

3. 표시 이름을 입력합니다.
4. 공급자 유형 드롭다운 목록에서 * Azure Blob Storage * 를 선택합니다.
5. 클라우드 스토리지 풀에 사용할 S3 버킷의 URI를 입력합니다.

   다음 두 가지 형식이 허용됩니다.

   "https://host:port`

"http://host:port`

6. Azure 컨테이너 이름을 입력합니다.

   지정하는 이름은 Azure 컨테이너 이름과 정확히 일치해야 합니다. 그렇지 않으면 클라우드 스토리지 풀을 생성하지 못합니다. 클라우드 스토리지 풀을 저장한 후에는 이 값을 변경할 수 없습니다.

7. 필요한 경우 인증을 위해 Azure 컨테이너의 관련 계정 이름 및 계정 키를 입력합니다.
8. 드롭다운에서 * 인증서 확인 안 함 * 을 선택합니다.
9. 저장 * 을 클릭합니다.

예상 결과

Azure Blob Storage용 Cloud Storage Pool이 생성되었는지 확인합니다.

Jonathan Wong이 _

백업에 클라우드 스토리지 풀 사용

ILM 규칙을 생성하여 백업을 위해 오브젝트를 클라우드 스토리지 풀로 이동할 수 있습니다.

필요한 것

- StorageGRID 11.6이 구성되었습니다.
- 외부 Azure 컨테이너를 이미 설정했습니다.

단계

1. Grid Manager에서 * ILM * > * 규칙 * > * 생성 * 으로 이동합니다.
2. 설명을 입력합니다.
3. 규칙을 트리거할 기준을 입력합니다.
4. 다음 * 을 클릭합니다.
5. 오브젝트를 스토리지 노드로 복제합니다.
6. 배치 규칙을 추가합니다.
7. 객체를 클라우드 스토리지 풀에 복제합니다
8. 다음 * 을 클릭합니다.
9. 저장 * 을 클릭합니다.

예상 결과

보존 다이어그램에 백업용 StorageGRID 및 클라우드 스토리지 풀에 로컬로 저장된 객체가 표시되는지 확인합니다.

ILM 규칙이 트리거되면 클라우드 스토리지 풀에 복사본이 존재하므로 오브젝트 복원을 수행하지 않고 로컬에서 개체를 검색할 수 있는지 확인합니다.

Jonathan Wong이 _

StorageGRID 검색 통합 서비스를 구성합니다

이 가이드는 아마존 OpenSearch 서비스 또는 온-프레미스 Elasticsearch를 사용하여 NetApp StorageGRID 검색 통합 서비스를 구성하는 방법에 대한 자세한 지침을 제공합니다.

소개

StorageGRID는 세 가지 유형의 플랫폼 서비스를 지원합니다.

- * StorageGRID CloudMirror 복제 *. StorageGRID 버킷에서 지정된 외부 대상으로 특정 객체를 미러링합니다.
- * 알림 *. 객체에서 수행한 특정 작업에 대한 알림을 지정된 외부 Amazon SNS(Amazon Simple Notification Service)로 보내는 버킷당 이벤트 알림입니다.
- * 통합 서비스 검색 *. S3(Simple Storage Service) 개체 메타데이터를 지정된 Elasticsearch 인덱스에 전송하여 외부 서비스를 사용하여 메타데이터를 검색하거나 분석할 수 있습니다.

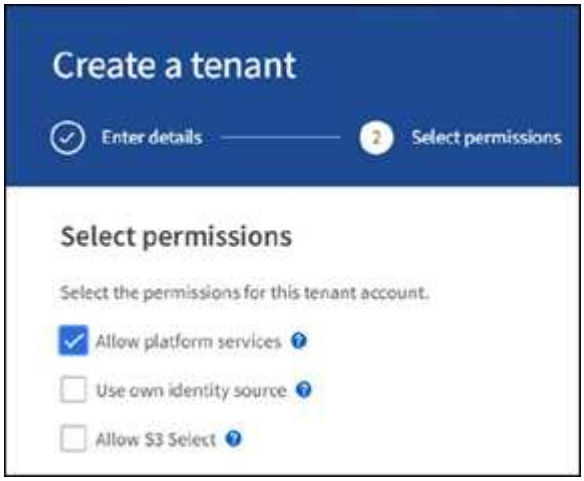
플랫폼 서비스는 테넌트 관리자 UI를 통해 S3 테넌트에서 구성합니다. 자세한 내용은 을 참조하십시오 "플랫폼 서비스 사용에 대한 고려 사항".

이 문서는 에 대한 보충 자료로 사용됩니다 "StorageGRID 11.6 테넌트 가이드" 및 에서는 검색 통합 서비스를 위한 엔드포인트 및 버킷 구성에 대한 단계별 지침과 예제를 제공합니다. 여기에 포함된 AWS(Amazon Web Services) 또는 온프레미스 Elasticsearch 설정 지침은 기본 테스트 또는 데모 전용입니다.

대상 고객은 그리드 관리자, 테넌트 관리자에 익숙해야 하며, StorageGRID 검색 통합 테스트를 위한 기본 업로드(PUT) 및 다운로드(GET) 작업을 수행하기 위해 S3 브라우저에 액세스할 수 있어야 합니다.

테넌트 생성 및 플랫폼 서비스 활성화

1. Grid Manager를 사용하여 S3 테넌트를 생성하고 표시 이름을 입력한 다음 S3 프로토콜을 선택합니다.
2. 사용 권한 페이지에서 플랫폼 서비스 허용 옵션을 선택합니다. 필요한 경우 다른 사용 권한을 선택합니다.



3. 테넌트 루트 사용자 초기 암호를 설정하거나, 격자에서 페더레이션 식별 이 설정된 경우 테넌트 계정을 구성할 루트 액세스 권한이 있는 통합 그룹을 선택합니다.
4. 루트로 로그인 을 클릭하고 버킷:버킷 생성 및 관리 를 선택합니다.

   그러면 Tenant Manager 페이지로 이동합니다.

5. Tenant Manager에서 내 액세스 키를 선택하여 나중에 테스트할 S3 액세스 키를 생성하고 다운로드합니다.

Amazon OpenSearch로 통합 서비스를 검색합니다

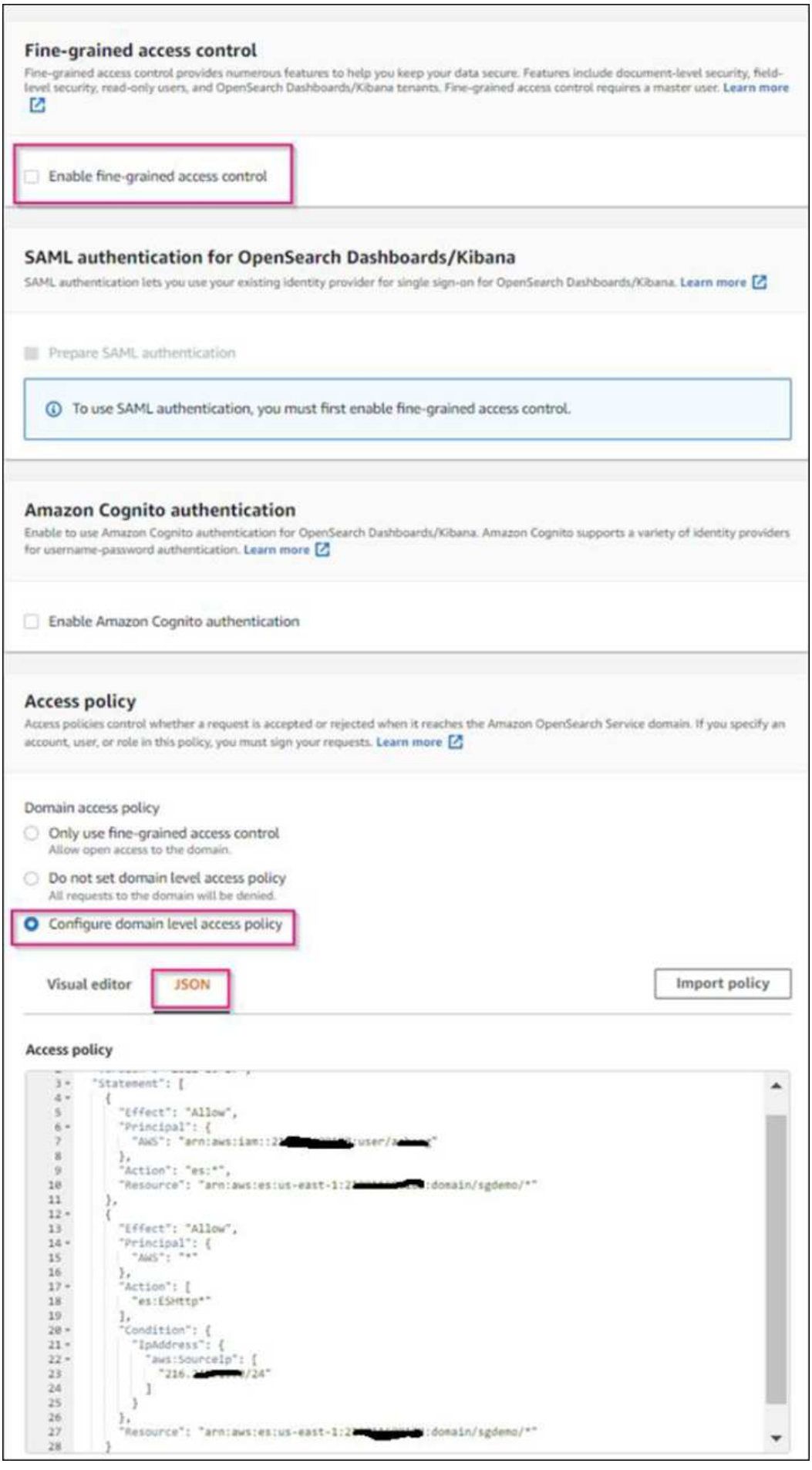
Amazon OpenSearch(이전의 Elasticsearch) 서비스 설정

테스트/데모용으로만 OpenSearch 서비스를 빠르고 간편하게 설정하려면 이 절차를 사용하십시오. 온-프레미스 Elasticsearch를 사용하여 검색 통합 서비스를 사용하는 경우 섹션을 참조하십시오 온-프레미스 Elasticsearch와 통합 서비스를 검색합니다.

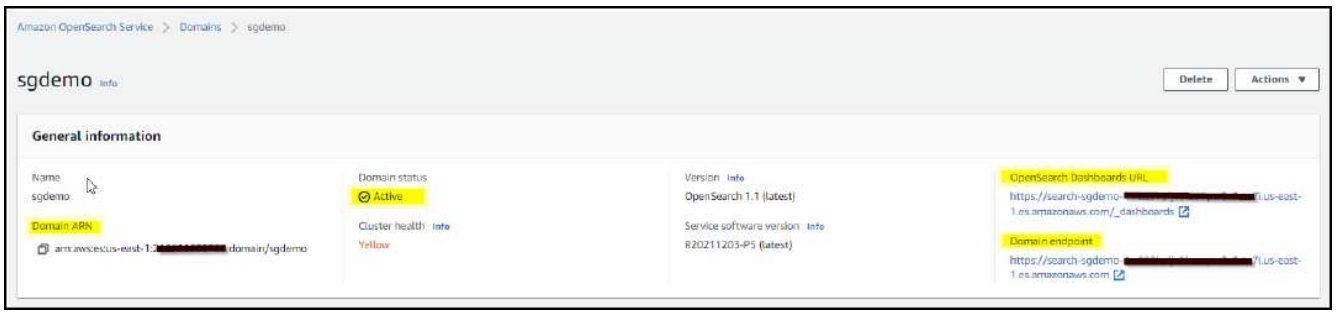
> OpenSearch 서비스에 가입하려면 유효한 AWS 콘솔 로그인, 액세스 키, 비밀 액세스 키 및 권한이 있어야 합니다.

1. 의 지침에 따라 새 도메인을 만듭니다 "AWS OpenSearch 서비스 시작"다음 사항을 제외한 경우:
   - 4단계. 도메인 이름: sgdemo
   - 10단계. 세분화된 액세스 제어: 세분화된 액세스 제어 사용 옵션을 선택 취소합니다.
   - 12단계. 액세스 정책: 레벨 액세스 정책 구성을 선택하고 JSON 탭을 선택하여 다음 예를 사용하여 액세스 정책을 수정합니다.
     - 강조 표시된 텍스트를 사용자 고유의 AWS ID 및 액세스 관리(IAM) ID 및 사용자 이름으로 바꿉니다.
     - 강조 표시된 텍스트(IP 주소)를 AWS 콘솔에 액세스하는 데 사용한 로컬 컴퓨터의 공용 IP 주소로 바꿉니다.
     - 브라우저 탭을 에 엽니다 "https://checkip.amazonaws.com" 공용 IP를 찾습니다.

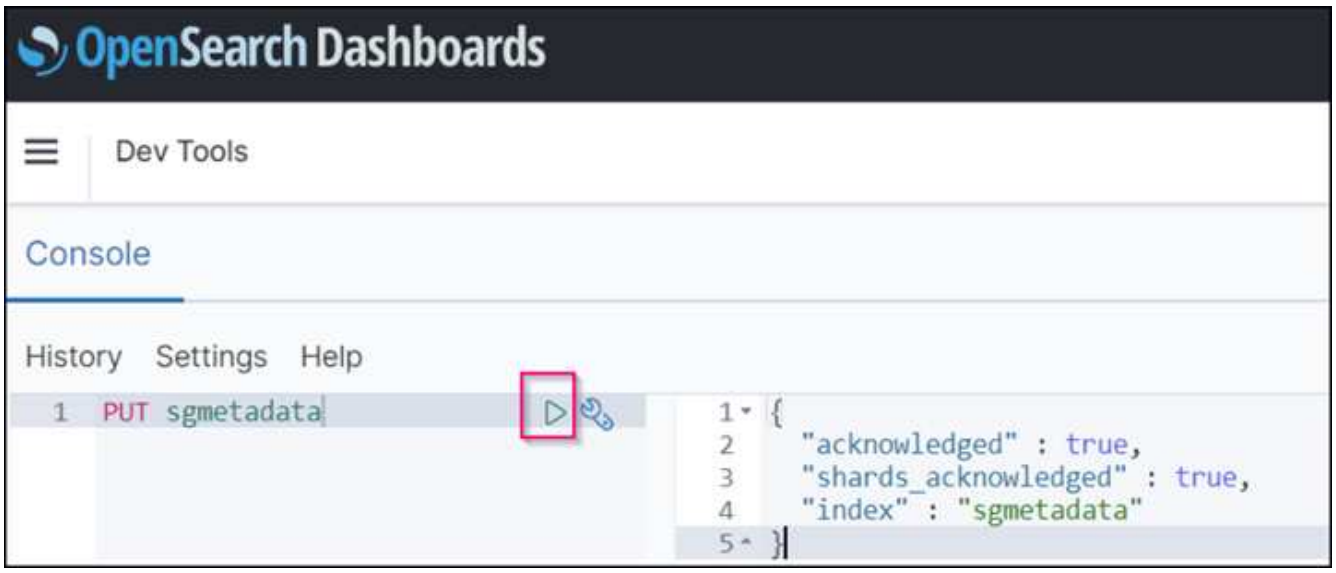
```
{

    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal":
        {"AWS": "arn:aws:iam:: nnnnnn:user/xyzabc"},
        "Action": "es:*",
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        },
        {
        "Effect": "Allow",
        "Principal": {"AWS": "*"},
        "Action": [
        "es:ESHttp*"
                ],
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": [ "nnn.nnn.nn.n/nn"
                    ]
                }
        },
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        }
    ]
}
```


Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
Enable fine-grained access control
SAML authentication for OpenSearch Dashboards/Kibana
SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. Learn more
Prepare SAML authentication
To use SAML authentication, you must first enable fine-grained access control.
Amazon Cognito authentication
Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more
Enable Amazon Cognito authentication
Access policy
Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. Learn more
Domain access policy
Only use fine-grained access control
Allow open access to the domain.
Do not set domain level access policy
All requests to the domain will be denied.
Configure domain level access policy
Visual editor
JSON
Import policy
Access policy
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::2[redacted]:user/A[redacted]"
},
"Action": "es:*",
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
},
{
"Effect": "Allow",
"Principal": {
"AWS": "*"
},
"Action": [
"es:ESHttp*"
],
"Condition": {
"IpAddress": {
"aws:SourceIp": [
"216.[redacted]/24"
]
}
},
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
}

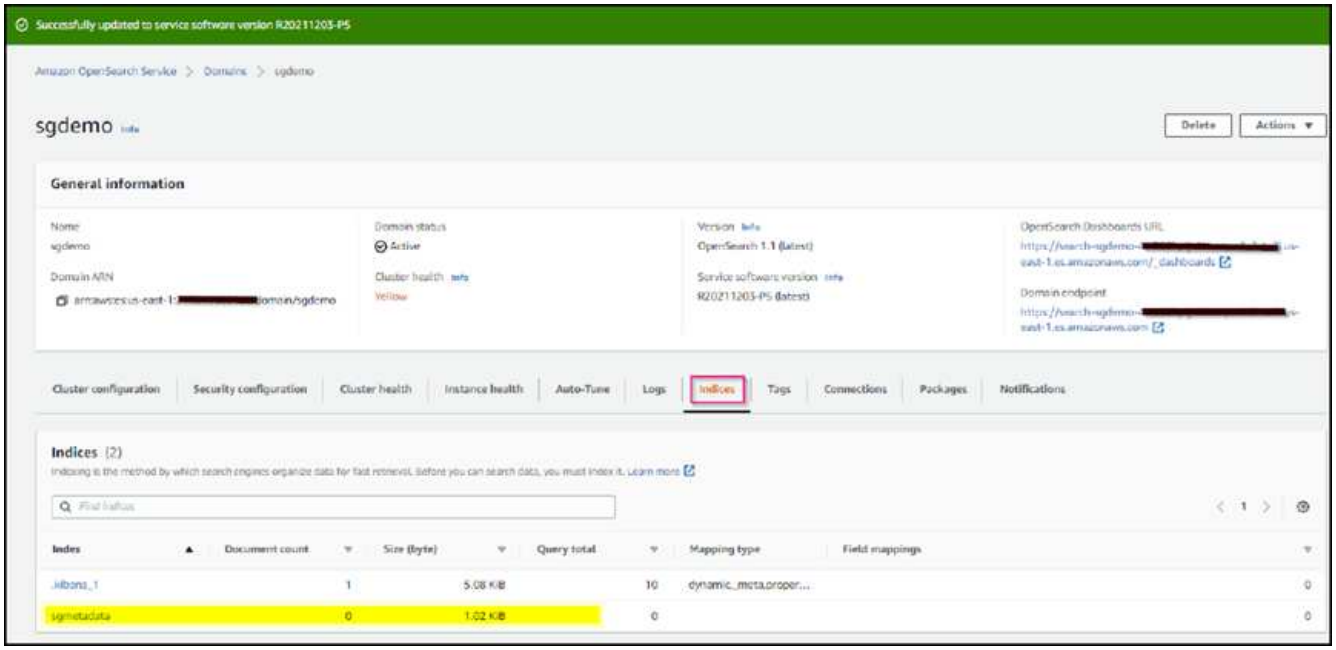
2. 도메인이 활성화될 때까지 15-20분 정도 기다립니다.



3. OpenSearch Dashboards URL 을 클릭하여 새 탭에서 도메인을 열고 대시보드에 액세스합니다. 액세스 거부 오류가 발생하면 도메인 대시보드에 액세스할 수 있도록 액세스 정책 원본 IP 주소가 컴퓨터 공용 IP로 올바르게 설정되어 있는지 확인합니다.
4. 대시보드 시작 페이지에서 직접 탐색 을 선택합니다. 메뉴에서 관리 → 개발 도구 로 이동합니다
5. 개발 도구 → 콘솔에서 StorageGRID 개체 메타데이터를 저장하기 위해 인덱스를 사용하는 'Put <index>'를 입력합니다. 다음 예에서는 인덱스 이름 'gmetadata'를 사용합니다. 작은 삼각형 기호를 클릭하여 PUT 명령을 실행합니다. 다음 예제 스크린샷과 같이 오른쪽 패널에 예상 결과가 표시됩니다.



6. 색인이 sgdomain > Indices 아래의 Amazon OpenSearch UI에서 표시되는지 확인합니다.

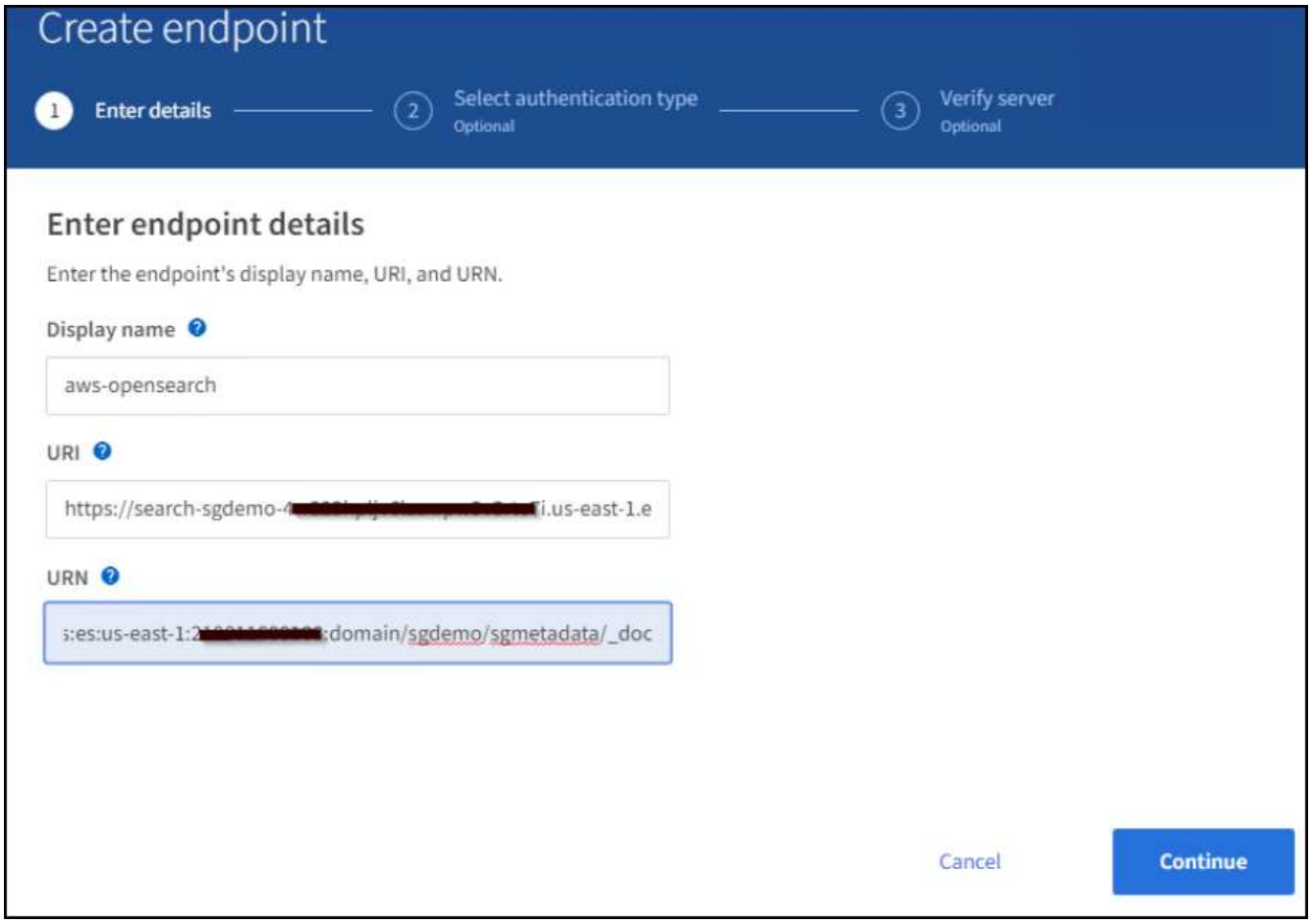


플랫폼 서비스 엔드포인트 구성

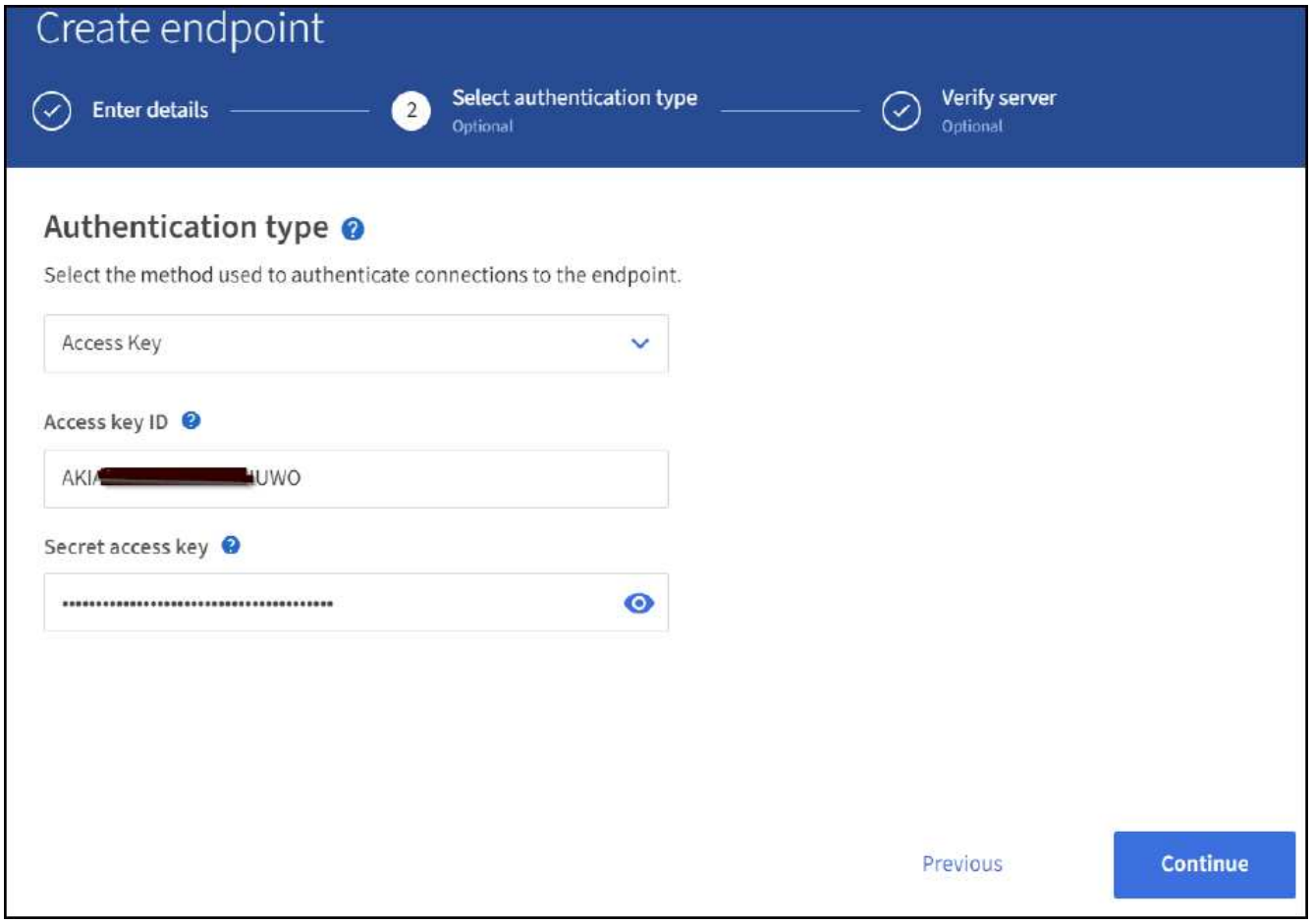
플랫폼 서비스 끝점을 구성하려면 다음 단계를 수행하십시오.

1. 테넌트 관리자 에서 스토리지(S3) > 플랫폼 서비스 엔드포인트 로 이동합니다.
2. 끝점 만들기 를 클릭하고 다음을 입력한 다음 계속 을 클릭합니다.
   - 표시 이름 예 AWS-OpenSearch
   - 예제 스크린샷의 도메인 끝점은 URI 필드의 이전 절차의 2단계 아래에 있습니다.
   - URN 필드의 이전 절차 2단계에서 사용한 ARN 도메인을 ARN의 끝에 추가하는 /<index>/_doc'를 추가한다.

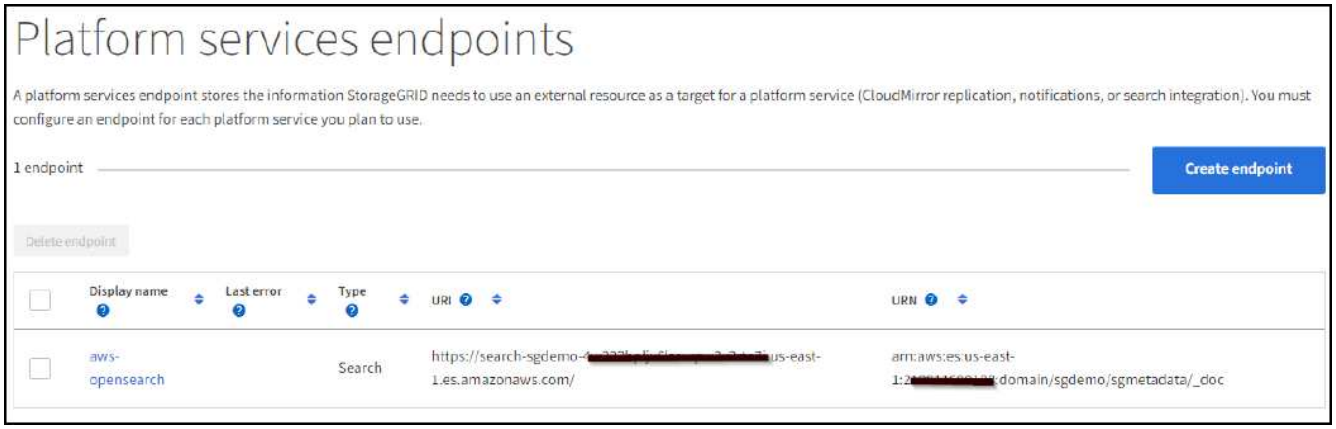
     이 예에서 URN은 'arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc'가 됩니다.



3. Amazon OpenSearch sgdomain에 액세스하려면 인증 유형으로 Access Key를 선택한 다음 Amazon S3 액세스 키와 암호 키를 입력합니다. 다음 페이지로 이동하려면 계속 을 클릭합니다.



4. 끝점을 확인하려면 운영 체제 CA 인증서 사용 및 끝점 테스트 및 만들기 를 선택합니다. 확인이 성공하면 다음 그림과 유사한 엔드포인트 화면이 표시됩니다. 확인이 실패하면 경로 끝에 URN에 "/<index>/_doc"가 포함되어 있고 AWS 액세스 키와 비밀 키가 올바른지 확인합니다.



온-프레미스 **Elasticsearch**와 통합 서비스를 검색합니다

온-프레미스 **Elasticsearch** 설정

이 절차는 테스트 목적으로만 Docker를 사용하여 사내 Elasticsearch 및 Kibana를 빠르게 설정하기 위한 것입니다. Elasticsearch 및 Kibana 서버가 이미 있는 경우 5단계로 이동합니다.

1. 다음 단계를 따르십시오 "Docker 설치 절차" Docker를 설치합니다. 을 사용합니다 "CentOS Docker 설치 절차" 를

클릭합니다.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io
sudo systemctl start docker
```

- 재부팅 후 Docker를 시작하려면 다음을 입력합니다.

```
sudo systemctl enable docker
```

- VM.max_map_count 값을 262144로 설정한다.

```
sysctl -w vm.max_map_count=262144
```

- 재부팅 후 설정을 유지하려면 다음을 입력합니다.

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

2. 를 따릅니다 "Elasticsearch 빠른 시작 가이드" Elasticsearch 및 Kibana Docker를 설치하고 실행하기 위한 자가 관리 섹션입니다. 이 예에서는 버전 8.1을 설치했습니다.

참고 Elasticsearch에서 만든 사용자 이름/암호 및 토큰을 아래로 하여 Kibana UI 및 StorageGRID 플랫폼 엔드포인트 인증을 시작해야 합니다.

Elasticsearch Service | Self-managed

Install and run Elasticsearch

1. Install and start Docker Desktop.
2. Run:

```
docker network create elastic
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.0
docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -it
```

When you start Elasticsearch for the first time, the following security configuration occurs automatically:

- Certificates and keys are generated for the transport and HTTP layers.
- The Transport Layer Security (TLS) configuration settings are written to `elasticsearch.yml`.
- A password is generated for the `elastic` user.
- An enrollment token is generated for Kibana.

NOTE You might need to scroll back a bit in the terminal to view the password and enrollment token.

3. Copy the generated password and enrollment token and save them in a secure location. These values are shown only when you start Elasticsearch for the first time. You'll use these to enroll Kibana with your Elasticsearch cluster and log in.

NOTE If you need to reset the password for the `elastic` user or other built-in users, run the `elasticsearch-reset-password` tool. To generate new enrollment tokens for Kibana or Elasticsearch nodes, run the `elasticsearch-create-enrollment-token` tool. These tools are available in the Elasticsearch `bin` directory.

Install and run Kibana

To analyze, visualize, and manage Elasticsearch data using an intuitive UI, install Kibana.

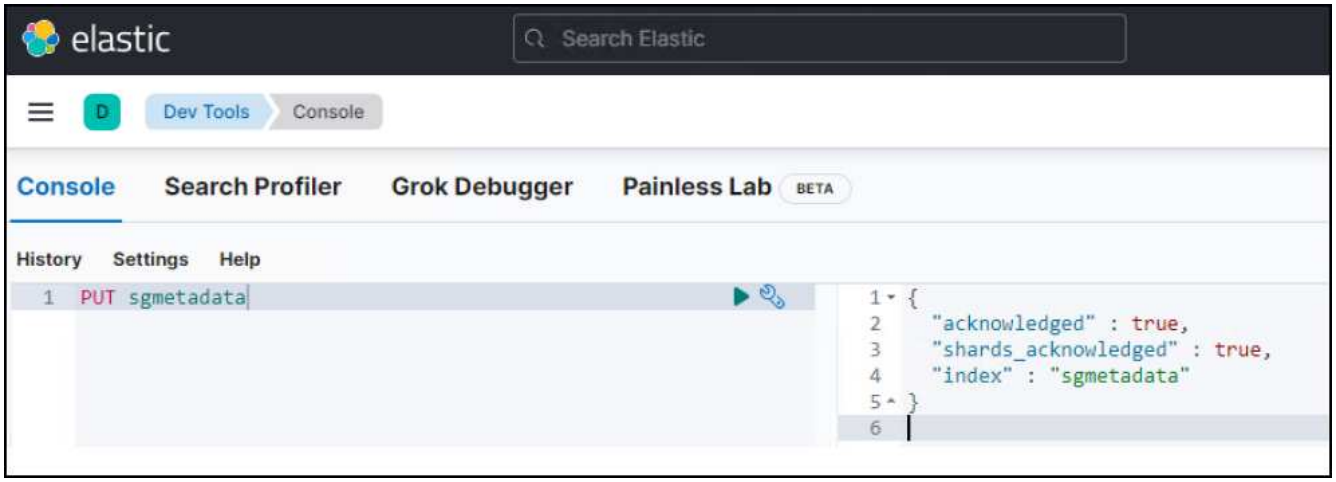
1. In a new terminal session, run:

```
docker pull docker.elastic.co/kibana/kibana:8.1.0
docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/ki
```

When you start Kibana, a unique link is output to your terminal.

2. To access Kibana, click the generated link in your terminal.
   a. In your browser, paste the enrollment token that you copied and click the button to connect your Kibana instance with Elasticsearch.
   b. Log in to Kibana as the `elastic` user with the password that was generated when you started Elasticsearch.

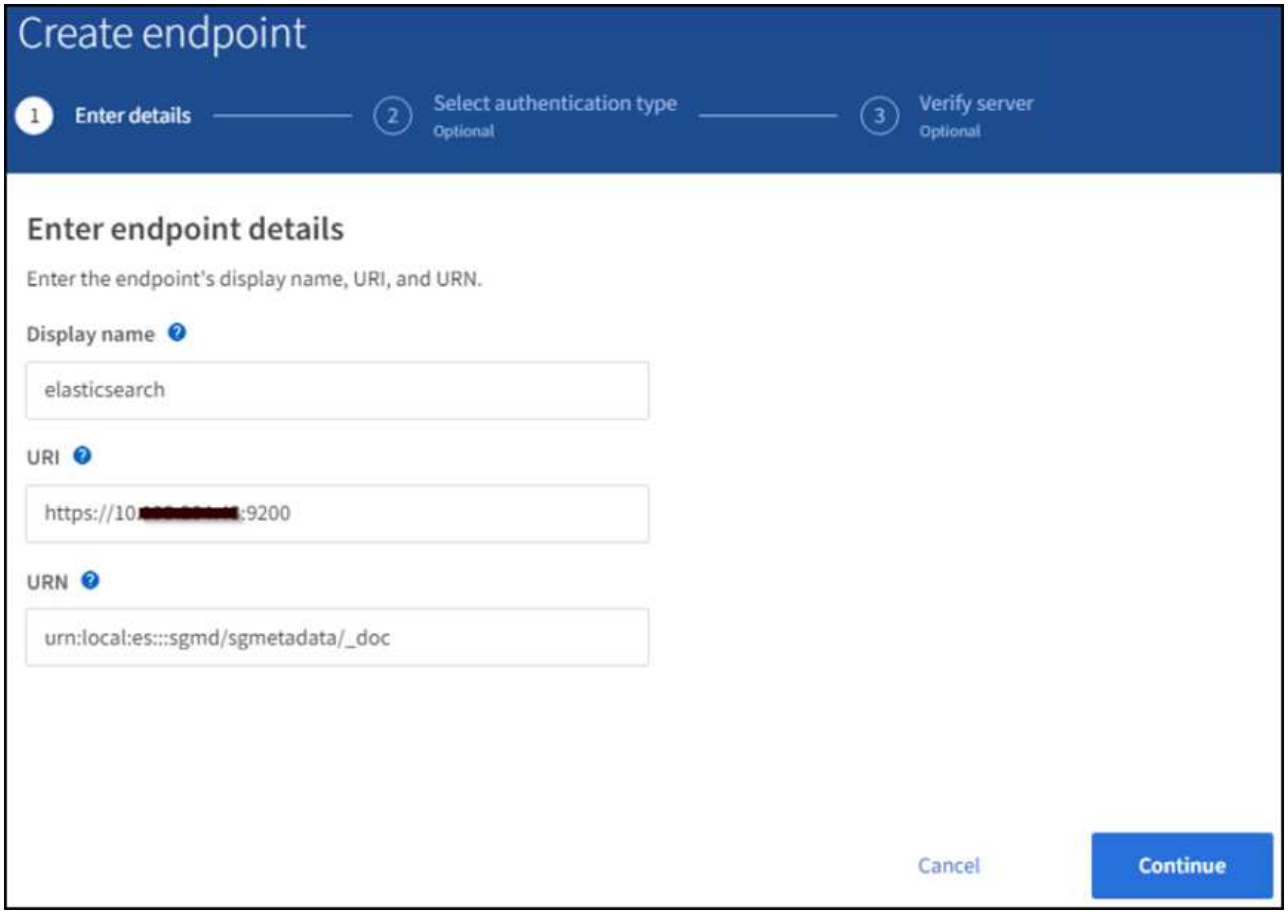
3. Kibana Docker 컨테이너가 시작되면 URL 링크 'https://0.0.0.0:5601` 가 콘솔에 표시됩니다. 0.0.0.0을 URL의 서버 IP 주소로 바꿉니다.
4. 사용자 이름 탄력성과 이전 단계에서 Elastic에 의해 생성된 암호를 사용하여 Kibana UI에 로그인합니다.
5. 처음 로그인하는 경우 대시보드 시작 페이지에서 직접 탐색 을 선택합니다. 메뉴에서 관리 > 개발 도구 를 선택합니다.
6. 개발 도구 콘솔 화면에서 StorageGRID 개체 메타데이터를 저장하기 위해 이 인덱스를 사용하는 "Put <index>"를 입력합니다. 이 예에서는 인덱스 이름 'gmetadata'를 사용합니다. 작은 삼각형 기호를 클릭하여 PUT 명령을 실행합니다. 다음 예제 스크린샷과 같이 오른쪽 패널에 예상 결과가 표시됩니다.



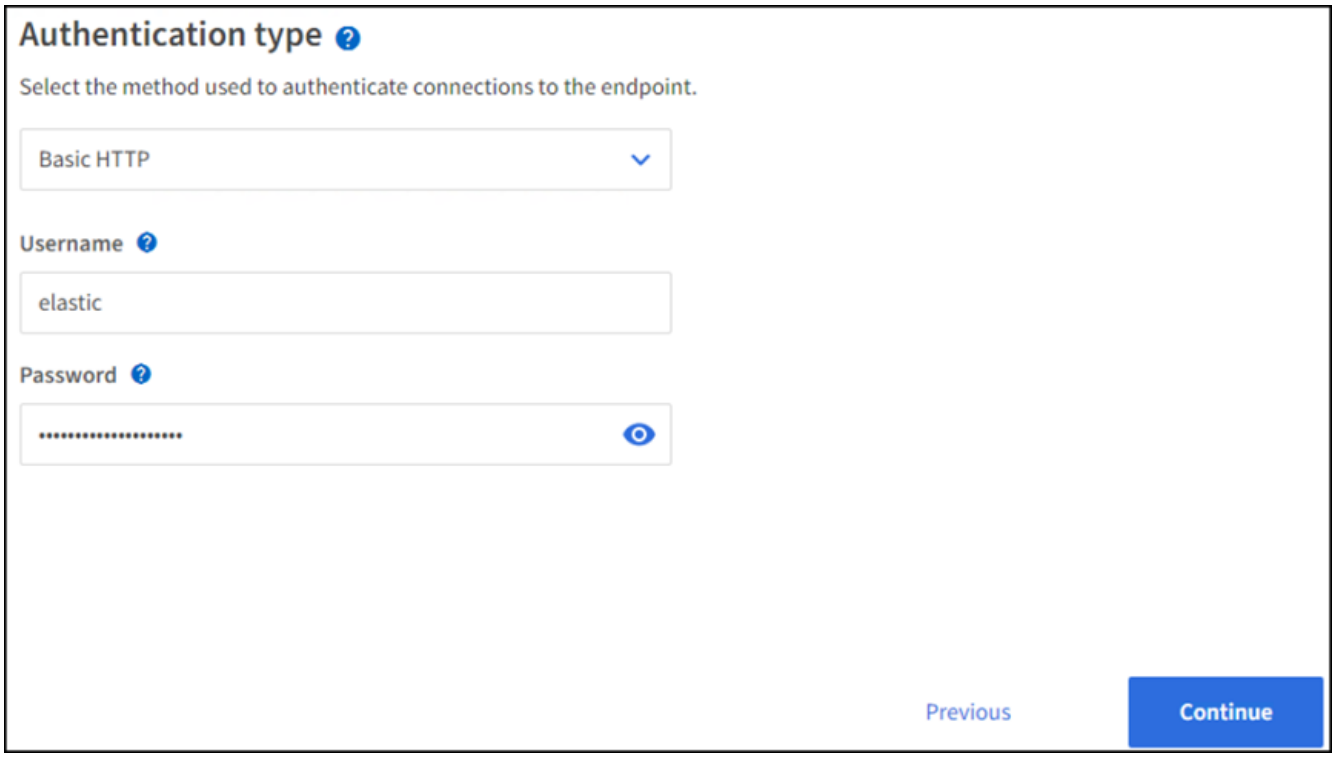
플랫폼 서비스 엔드포인트 구성

플랫폼 서비스에 대한 끝점을 구성하려면 다음 단계를 수행하십시오.

1. 테넌트 관리자에서 스토리지(S3) > 플랫폼 서비스 엔드포인트로 이동합니다
2. 끝점 만들기 를 클릭하고 다음을 입력한 다음 계속 을 클릭합니다.
   - 이름 표시 예: 탄력적인 검색
   - Uri:'https://<elasticsearch-server-ip or hostname>:9200'입니다
   - urn:'urn:<something>:es:::<some-unique-text>/<index-name>/_doc' 여기서 index-name은 Kibana 콘솔에서 사용한 이름입니다. 예: 'urn:local:es::::sgmd/sgmetadata/_doc'

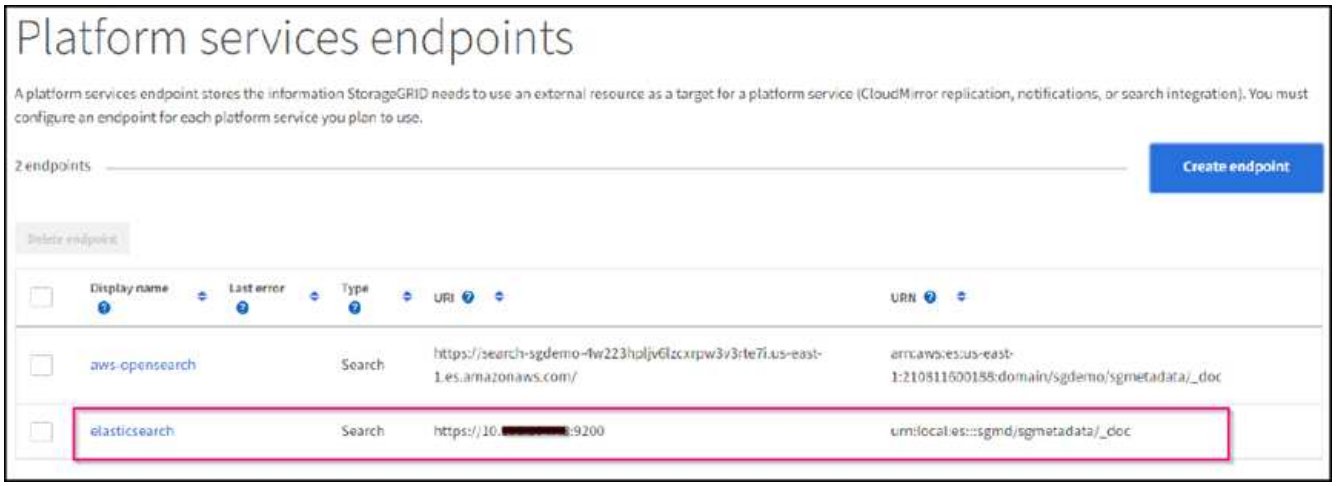


3. 인증 유형으로 기본 HTTP 를 선택하고 Elasticsearch 설치 프로세스에서 생성된 사용자 이름 'elastic'과 암호를 입력합니다. 다음 페이지로 이동하려면 계속 을 클릭합니다.



4. 인증서 확인 안 함 및 테스트 및 끝점 만들기 를 선택하여 끝점을 확인합니다. 확인이 성공하면 다음 스크린샷과

유사한 엔드포인트 화면이 표시됩니다. 확인에 실패하면 URN, URI 및 사용자 이름/암호 항목이 올바른지 확인합니다.



버킷 검색 통합 서비스 구성

플랫폼 서비스 끝점을 만든 후 다음 단계는 개체가 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 개체 메타데이터를 정의된 끝점으로 보내도록 버킷 수준에서 이 서비스를 구성하는 것입니다.

다음과 같이 테넌트 관리자를 사용하여 사용자 지정 StorageGRID 구성 XML을 버킷에 적용하여 검색 통합을 구성할 수 있습니다.

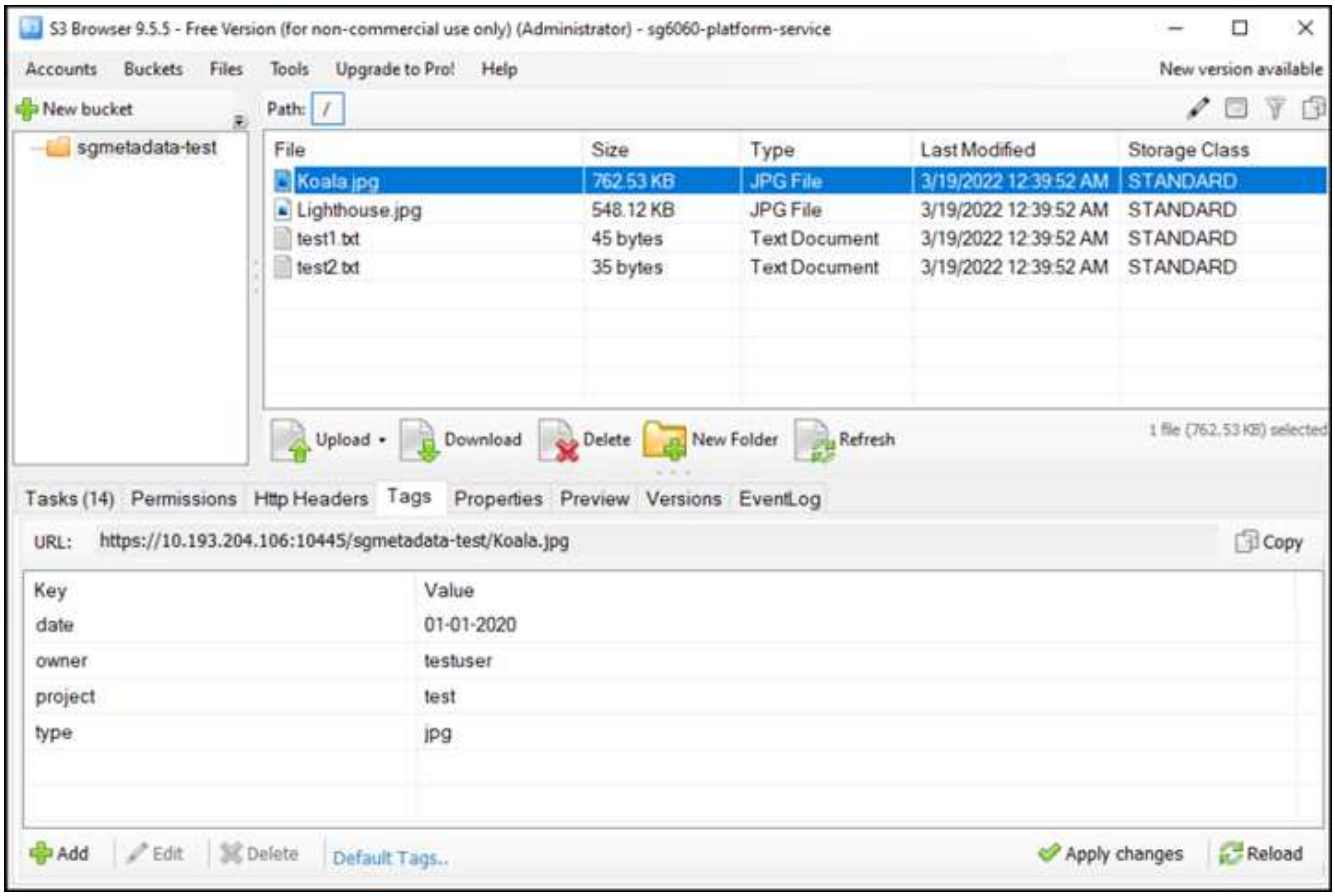
1. 테넌트 관리자 에서 스토리지(S3) > 버킷 으로 이동합니다
2. Create Bucket을 클릭하고 bucket 이름(예: 'gmetadata-test')을 입력한 후 기본 us-east-1 영역을 그대로 사용합니다.
3. 계속 > 버킷 생성 을 클릭합니다.
4. 버킷 개요 페이지를 표시하려면 버킷 이름을 클릭한 다음 플랫폼 서비스를 선택합니다.
5. 검색 통합 활성화 대화 상자를 선택합니다. 제공된 XML 상자에 이 구문을 사용하여 구성 XML을 입력합니다.

   강조 표시된 URN은 사용자가 정의한 플랫폼 서비스 끝점과 일치해야 합니다. 다른 브라우저 탭을 열어 테넌트 관리자에 액세스하고 정의된 플랫폼 서비스 끝점에서 URN을 복사할 수 있습니다.

   이 예에서는 접두어를 사용하지 않았습니다. 즉, 이 버킷의 모든 객체에 대한 메타데이터가 이전에 정의된 Elasticsearch 끝점으로 전송됩니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Urn> urn:local:es:::sgmd/sgmetadata/_doc</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

6. S3 브라우저를 사용하여 테넌트 액세스/암호 키를 사용하여 StorageGRID에 연결하고, 테스트 객체를 '메타데이터 테스트' 버킷에 업로드하고, 태그나 사용자 지정 메타데이터를 객체에 추가합니다.



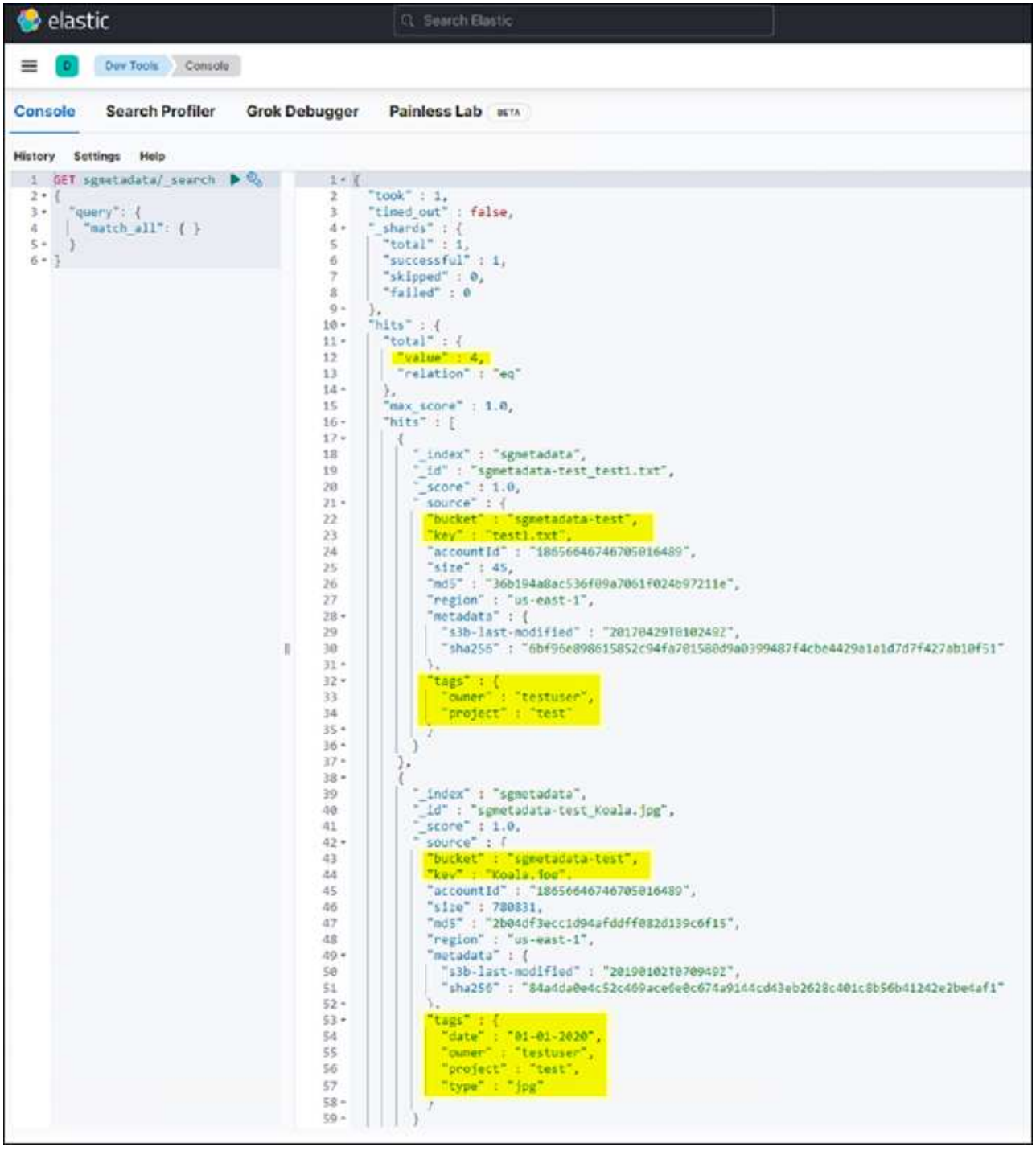
7. Kibana UI를 사용하여 오브젝트 메타데이터가 sgmetadata의 인덱스에 로드되었는지 확인합니다.

   a. 메뉴에서 관리 > 개발 도구 를 선택합니다.

   b. 왼쪽의 콘솔 패널에 샘플 쿼리를 붙여넣고 삼각형 기호를 클릭하여 실행합니다.

      다음 예제 스크린샷의 쿼리 1 예제 결과는 네 개의 레코드를 보여 줍니다. 이는 버킷의 오브젝트 수와 일치합니다.

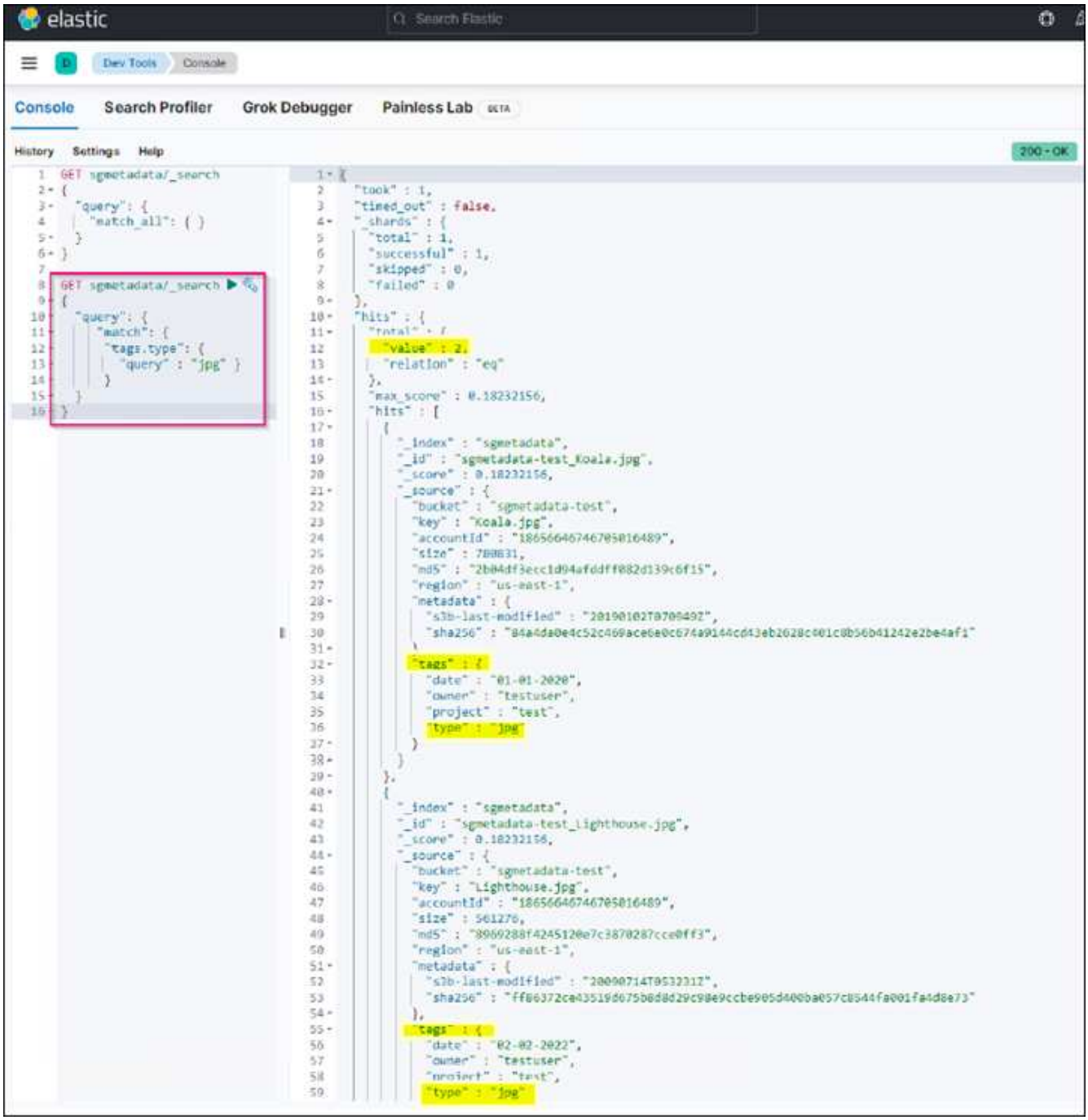
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



다음 스크린샷의 쿼리 2 샘플 결과는 태그 유형 jpg의 두 레코드를 보여 줍니다.

```
GET sgmetadata/_search
{
    "query": {
        "match": {
            "tags.type": {
                "query" : "jpg" }
                }
            }
}
```

+



추가 정보를 찾을 수 있는 위치

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

- "플랫폼 서비스란 무엇입니까"
- "StorageGRID 11.6 문서"

안젤라 청 _ 에 의해

노드 클론

노드 클론 고려 사항 및 성능

노드 클론 고려 사항

노드 클론은 기술 업데이트, 용량 증가 또는 StorageGRID 시스템 성능 향상을 위해 기존 어플라이언스 노드를 빠르게 교체할 수 있는 방법이 될 수 있습니다. 노드 클론은 KMS를 사용하여 노드 암호화로 변환하거나 스토리지 노드를 DDP8에서 DDP16으로 변경하는 경우에도 유용합니다.

- 소스 노드의 사용된 용량은 클론 프로세스를 완료하는 데 필요한 시간과 관련이 없습니다. 노드 클론은 노드의 여유 공간을 포함하는 노드의 전체 복사본입니다.
- 소스 및 대상 장비는 동일한 PGE 버전이어야 합니다
- 대상 노드의 용량은 항상 소스보다 커야 합니다
  - 새 대상 어플라이언스의 드라이브 크기가 소스보다 큰지 확인하십시오
  - 대상 어플라이언스의 크기가 동일한 드라이브가 DDP8에 대해 구성된 경우 DDP16의 대상을 구성할 수 있습니다. 소스가 DDP16에 대해 이미 구성되어 있으면 노드 클론을 사용할 수 없습니다.
  - SG5660 또는 SG5760 어플라이언스에서 SG6060 어플라이언스로 이동하는 경우 SG5x60은 60개의 대용량 드라이브를 지원하며 SG6060은 58만 지원합니다.
- 노드 클론 프로세스를 수행하려면 클론 생성 프로세스 동안 소스 노드가 그리드에 대해 오프라인 상태여야 합니다. 이 시간 동안 추가 노드가 오프라인이 되면 클라이언트 서비스에 영향을 줄 수 있습니다.
- 11.8 이하: 스토리지 노드는 15일 동안만 오프라인 상태가 될 수 있습니다. 복제 프로세스 추정치가 15일에 가깝거나 15일을 초과할 경우 확장 및 서비스 해제 절차를 사용하십시오.
  - 11.9 : 15일 제한이 제거되었습니다.
- 확장 쉘프가 포함된 SG6060 또는 SG6160의 경우, 전체 클론 기간을 얻기 위해 올바른 쉘프 드라이브 크기에 대한 시간을 기본 어플라이언스 시간의 시간과 추가해야 합니다.
- 타겟 스토리지 어플라이언스의 볼륨 수는 소스 노드의 볼륨 수보다 크거나 같아야 합니다. 오브젝트 저장소 볼륨(rangedb)이 16개인 소스 노드를 12개의 오브젝트 저장소 볼륨이 있는 타겟 스토리지 어플라이언스에 클론 복제할 수 없습니다. 타겟 어플라이언스에 소스 노드보다 용량이 더 큰 경우에도 마찬가지입니다. 오브젝트 저장소 볼륨이 12개뿐인 SGF6112 스토리지 어플라이언스를 제외하고 대부분의 스토리지 어플라이언스에는 16개의 오브젝트 저장소 볼륨이 있습니다. 예를 들어, SG5760에서 SGF6112로 클론을 생성할 수 없습니다.

노드 클론 성능 추정치

다음 표에는 노드 클론 기간에 대해 계산된 추정치가 나와 있습니다. 조건이 다양하므로 * BOLD * 의 항목은 노드 다운에 대해 15일 제한을 초과할 위험이 있습니다.

DDP8

SG5612/SG5712/SG5812 → 모두

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	1일	2일	2.5일	3일	4일	4.5일	5.5일
25GB	1일	2일	2.5일	3일	4일	4.5일	5.5일

SG5660 → **SG5760/SG5860**

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	3.5일	7일	8.5일	10.5일	• 13.5일 *	• 15.5일 *	• 18.5일 *
25GB	3.5일	7일	8.5일	10.5일	• 13.5일 *	• 15.5일 *	• 18.5일 *

SG5660 → **SG6060/SG6160**

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	2.5일	4.5일	5.5일	6.5일	9일	10일	• 12일 *
25GB	2일	4일	5일	6일	8일	9일	10일

SG5760/SG5860 → **SG5760/SG5860**

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	3.5일	7일	8.5일	10.5일	• 13.5일 *	• 15.5일 *	• 18.5일 *
25GB	3.5일	7일	8.5일	10.5일	• 13.5일 *	• 15.5일 *	• 18.5일 *

SG5760/SG5860 → **SG6060/SG6160**

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	2.5일	4.5일	5.5일	6.5일	9일	10일	• 12일 *
25GB	2일	3.5일	4.5일	5.5일	7일	8일	9.5일

SG6060/SG6160 → SG6060/SG6160

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	2.5일	4.5일	5.5일	6.5일	8.5일	9.5일	11.5일
25GB	2일	3일	4일	4.5일	6일	7일	8.5일

DDP16을 참조하십시오

SG5760/SG5860 → SG5760/SG5860

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	3.5일	6.5일	8일	9.5일	• 12.5일 *	• 14일 *	• 17일 *
25GB	3.5일	6.5일	8일	9.5일	• 12.5일 *	• 14일 *	• 17일 *

SG5760/SG5860 → SG6060/SG6160

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	2.5일	5일	6일	7.5일	10일	11일	• 13일 *
25GB	2일	3.5일	4일	5일	6.5일	7일	8.5일

SG6060/SG6160 → SG6060/SG6160

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	3일	5일	6일	7일	9.5일	10.5일	• 13일 *
25GB	2일	3.5일	4.5일	5일	7일	7.5일	9일

확장 쉘프(소스 어플라이언스의 각 쉘프마다 **SG6060/SG6160** 위에 추가)

네트워크 인터페이스 속도	**4TB** 드라이브 크기	**8TB** 드라이브 크기	**10TB** 드라이브 크기	**12TB** 드라이브 크기	**16TB** 드라이브 크기	**18TB** 드라이브 크기	**22TB** 드라이브 크기
10GB	3.5일	5일	6일	7일	9.5일	10.5일	• 12일 *
25GB	2일	3일	4일	4.5일	6일	7일	8.5일

_ 아론 클라인 _

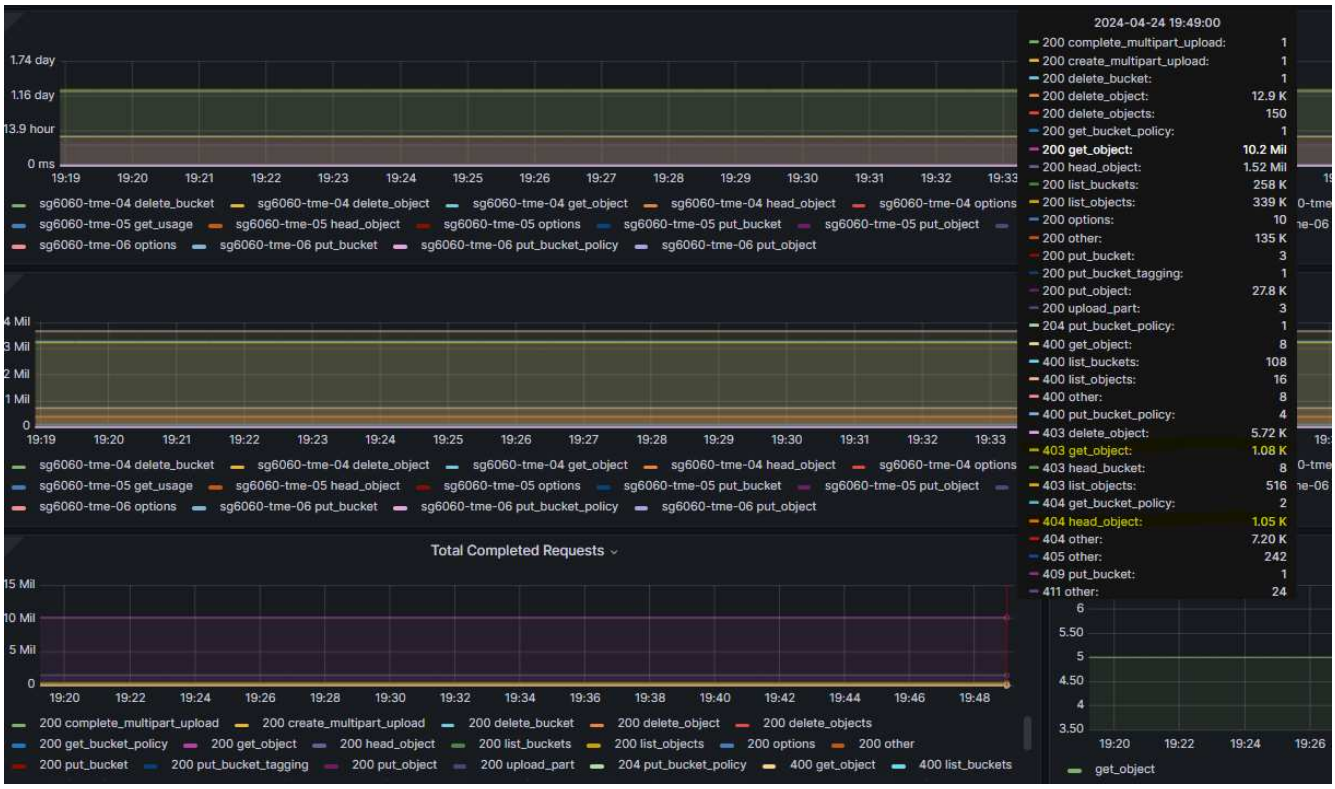
그리드 사이트 재배치 및 사이트 전체 네트워크 변경 절차

이 가이드에서는 다중 사이트 그리드에서 StorageGRID 사이트 재배치를 위한 준비 및 절차에 대해 설명합니다. 이 절차를 완전히 이해하고 원활한 프로세스를 보장하고 고객의 중단을 최소화할 수 있도록 미리 계획해야 합니다.

전체 그리드의 그리드 네트워크를 변경해야 하는 경우 을 참조하십시오
"그리드의 모든 노드에 대한 IP 주소를 변경합니다".

사이트 재배치 전 고려 사항

- 사이트 이동을 완료하고 모든 노드를 15일 이내에 온라인으로 전환하여 Cassandra 데이터베이스가 재구축되지 않도록 합니다.
"스토리지 노드를 15일 이상 복구합니다"
- 활성 정책의 ILM 규칙이 엄격한 수집 동작을 사용하고 있는 경우, 고객이 사이트 재배치 중에 그리드에 개체를 계속 넣으려는 경우 이를 밸런스 또는 이중 커밋으로 변경하는 것이 좋습니다.
- 60개 이상의 드라이브가 있는 스토리지 어플라이언스의 경우 디스크 드라이브가 설치된 상태로 쉘프를 이동하지 마십시오. 포장/이동 전에 각 디스크 드라이브에 레이블을 지정하고 스토리지 인클로저에서 분리하십시오.
- StorageGRID 어플라이언스 변경 그리드 네트워크 VLAN은 관리 네트워크 또는 클라이언트 네트워크를 통해 원격으로 수행할 수 있습니다. 또는 재배치 이전 또는 이후에 변경을 수행하기 위해 현장에 있을 계획입니다.
- 고객 응용 프로그램이 HEAD를 사용하고 있는지 또는 넣기 전에 존재하지 않는 개체를 가져오는지 확인합니다. 그렇다면 HTTP 500 오류를 방지하기 위해 버킷 일관성을 강력한 사이트로 변경합니다. 확실하지 않은 경우, S3 개요 Grafana Charts * 그리드 매니저 > 지원 > 메트릭 * 에서 '총 완료된 요청' 차트 위에 마우스를 올려 놓습니다. 404 Get Object 또는 404 head object의 개수가 매우 많으면 하나 이상의 응용 프로그램이 head 또는 get nonexistance object를 사용하고 있을 가능성이 높습니다. 카운트가 누적됩니다. 다른 타임라인에 마우스를 갖다 대면 차이를 확인할 수 있습니다.



사이트 재배치 전 그리드 **IP** 주소를 변경하는 절차

단계

1. 새 그리드 네트워크 서브넷을 새 위치에서 사용할 경우
   "그리드 네트워크 서브넷 목록에 서브넷을 추가합니다"
2. 기본 관리자 노드에 로그인하고 change-IP를 사용하여 그리드 IP를 변경합니다. 변경을 위해 노드를 종료하기 전에 * 단계 * 해야 합니다.
   a. 그리드 IP 변경에 대해 2와 1을 차례로 선택합니다

```
Editing: Node IP/subnet and gateway

Use up arrow to recall a previously typed value, which you can then edit
Use d or 0.0.0.0/0 as the IP/mask to delete the network from the node
Use q to complete the editing session early and return to the previous menu
Press <enter> to use the value shown in square brackets

================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP/mask [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP/mask [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP/mask [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP/mask [     10.45.74.18/26 ]: 10.45.74.28/26
================================================================================
LONDON-ADM1 Grid    Gateway [         10.45.74.1 ]:
LONDON-S1   Grid    Gateway [         10.45.74.1 ]:
LONDON-S2   Grid    Gateway [         10.45.74.1 ]:
LONDON-S3   Grid    Gateway [         10.45.74.1 ]:
================================================================================
================================================================================
Site: OXFORD
================================================================================
OXFORD-ADM1 Grid    IP/mask [     10.45.75.14/26 ]:
OXFORD-S1   Grid    IP/mask [     10.45.75.16/26 ]:
OXFORD-S2   Grid    IP/mask [     10.45.75.17/26 ]:
OXFORD-S3   Grid    IP/mask [     10.45.75.18/26 ]:
================================================================================
OXFORD-ADM1 Grid    Gateway [         10.45.75.1 ]:
OXFORD-S1   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S2   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S3   Grid    Gateway [         10.45.75.1 ]:
================================================================================
Finished editing. Press Enter to return to menu.
```

b. 5를 선택하여 변경 사항을 표시합니다

```
================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP      [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP      [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP      [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP      [     10.45.74.18/26 ]: 10.45.74.28/26
Press Enter to continue
```

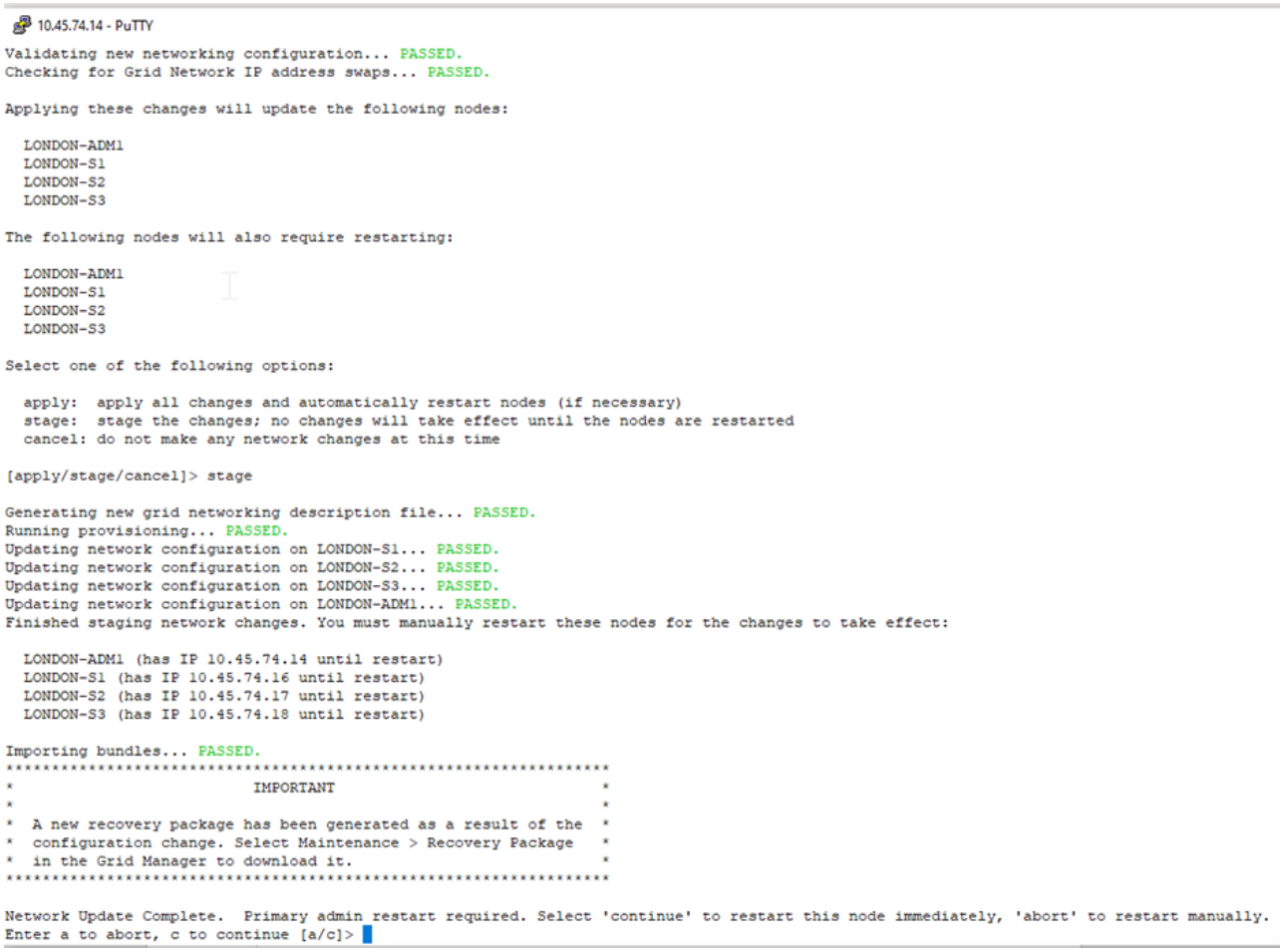
c. 10을 선택하여 변경 사항을 확인하고 적용합니다.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask and gateway
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection: 10
```

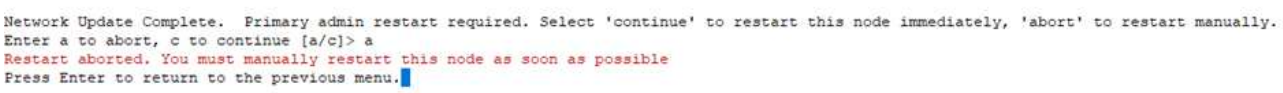
d. 이 단계에서 * stage * 를 선택해야 합니다.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

The following nodes will also require restarting:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

Select one of the following options:

  apply:  apply all changes and automatically restart nodes (if necessary)
  stage:  stage the changes; no changes will take effect until the nodes are restarted
  cancel: do not make any network changes at this time

[apply/stage/cancel]> stage
```

e. 위 변경에 기본 관리 노드가 포함되어 있는 경우 * 'a'를 입력하여 운영 관리 노드를 수동으로 다시 시작합니다 *



f. 이전 메뉴로 돌아가고 change-IP 인터페이스에서 나가려면 Enter 키를 누릅니다.



3. Grid Manager에서 새 복구 패키지를 다운로드합니다. * 그리드 관리자 * > * 유지 관리 * > * 복구 패키지 *
4. StorageGRID 어플라이언스에서 VLAN 변경이 필요한 경우 섹션을 참조하십시오 어플라이언스 VLAN 변경.
5. 사이트의 모든 노드 및/또는 어플라이언스를 종료하고, 필요한 경우 디스크 드라이브에 레이블을 붙이거나 제거하고, 랙을 해제하고, 포장하고, 이동합니다.
6. 관리자 네트워크 IP 및/또는 클라이언트 VLAN 및 IP 주소를 변경하려는 경우 재배치 후 변경 작업을 수행할 수 있습니다.

어플라이언스 **VLAN** 변경

아래 절차에서는 StorageGRID 어플라이언스의 관리자 또는 클라이언트 네트워크에 원격으로 액세스하여 원격으로 변경을 수행하는 것으로 가정합니다.

단계

1. 제품을 종료하기 전에 "제품을 유지보수 모드로 두십시오".
2. 브라우저를 사용하여 를 사용하여 StorageGRID 어플라이언스 설치 프로그램 GUI에 액세스합니다

https://<admin-or-client-network-ip>:8443. 어플라이언스가 유지보수 모드로 부팅된 후 새 그리드 IP가 이미 있으므로 그리드 IP를 사용할 수 없습니다.

3. 그리드 네트워크의 VLAN을 변경합니다. 클라이언트 네트워크를 통해 어플라이언스에 액세스하는 경우 지금은 클라이언트 VLAN을 변경할 수 없으며 이동 후 변경할 수 있습니다.
4. 어플라이언스에 SSH로 연결하고 'shutdoown -h now'를 사용하여 노드를 종료합니다.
5. 어플라이언스가 새 사이트에서 준비되면 를 사용하여 StorageGRID 어플라이언스 설치 프로그램 GUI에 액세스합니다 https://<grid-network-ip>:8443. GUI에서 ping/nmap 툴을 사용하여 스토리지가 최적의 상태이고 다른 그리드 노드에 대한 네트워크 연결인지 확인합니다.
6. 클라이언트 네트워크 IP를 변경하려는 경우 이 단계에서 클라이언트 VLAN을 변경할 수 있습니다. 클라이언트 네트워크는 이후 단계에서 change-IP 도구를 사용하여 클라이언트 네트워크 IP를 업데이트할 때까지 준비되지 않습니다.
7. 유지보수 모드를 종료합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.
8. 모든 노드가 가동되고 그리드에 연결 문제가 표시되지 않으면 필요에 따라 change-IP를 사용하여 어플라이언스 관리 네트워크와 클라이언트 네트워크를 업데이트합니다.

오브젝트 기반 스토리지를 **ONTAP S3**에서 **StorageGRID**로 마이그레이션

ONTAP S3에서 **StorageGRID**로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 **S3**를 지원합니다

ONTAP S3에서 StorageGRID로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 S3를 지원합니다

마이그레이션 데모

이 데모는 사용자 및 버킷을 ONTAP S3에서 StorageGRID로 마이그레이션하는 데 사용됩니다.

ONTAP S3에서 **StorageGRID**로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 **S3**를 지원합니다

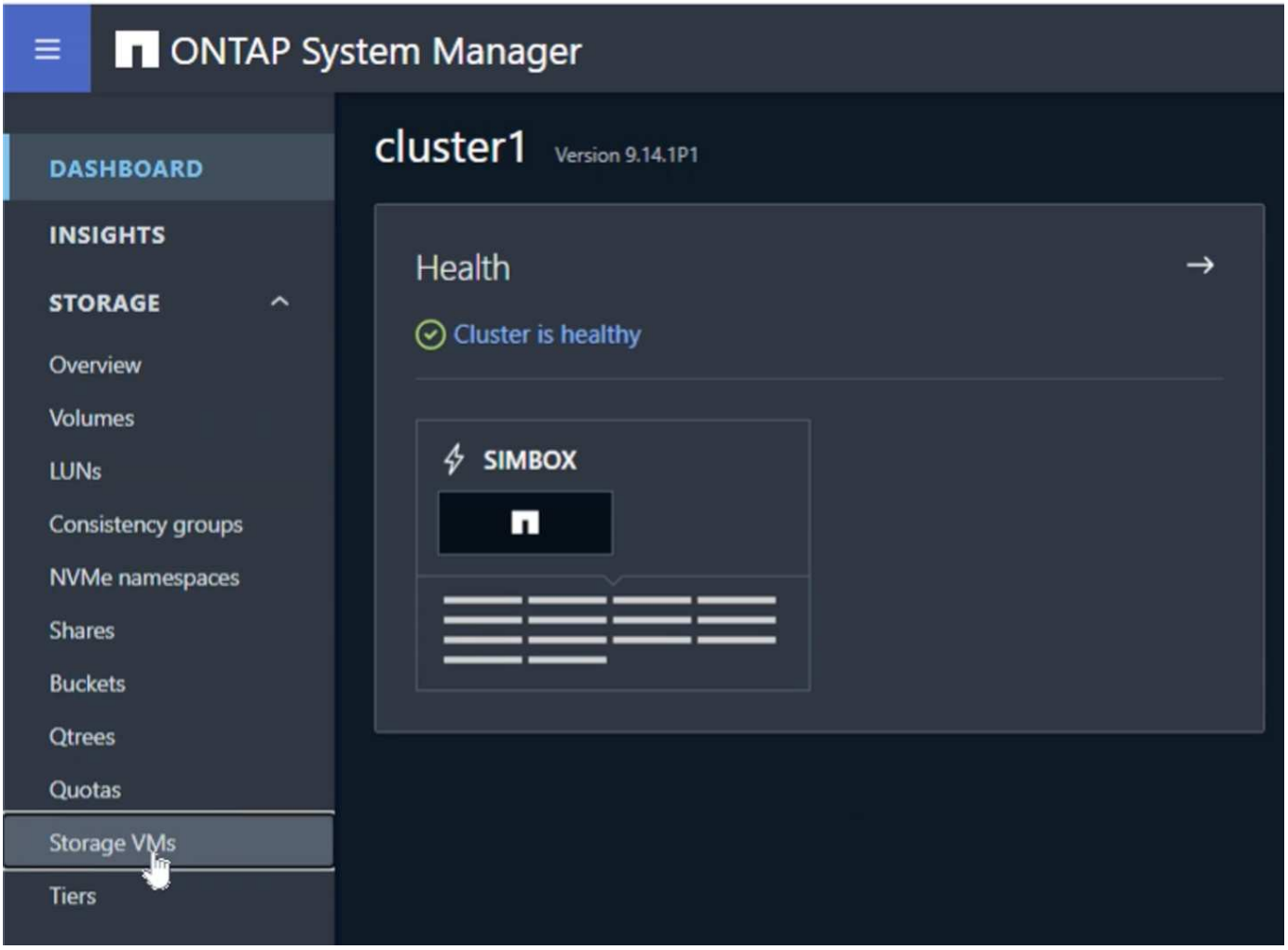
ONTAP S3에서 StorageGRID로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 S3를 지원합니다

ONTAP 준비 중

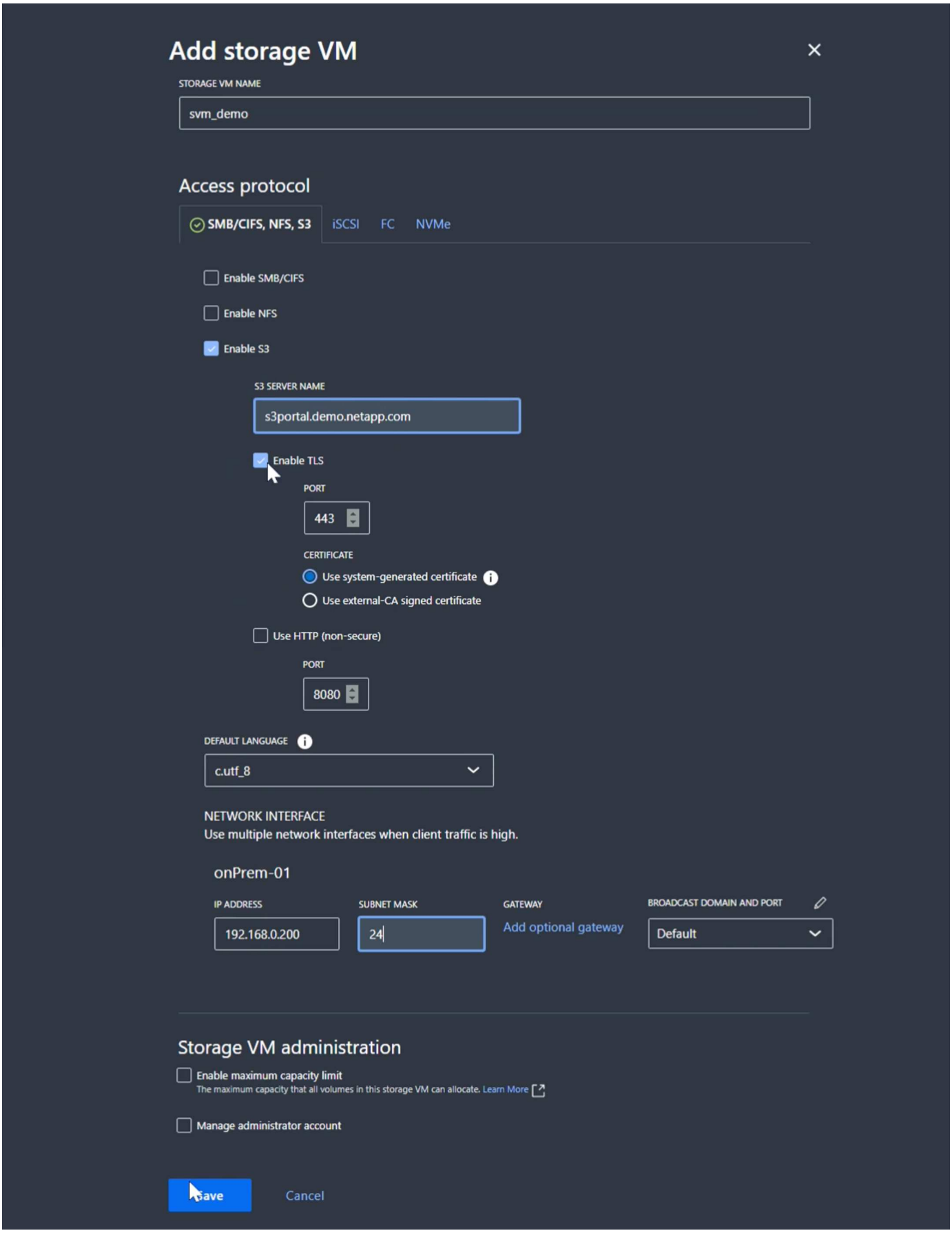
데모를 위해 SVM 오브젝트 저장소 서버, 사용자, 그룹, 그룹 정책 및 버킷을 생성합니다.

스토리지 가상 시스템을 생성합니다

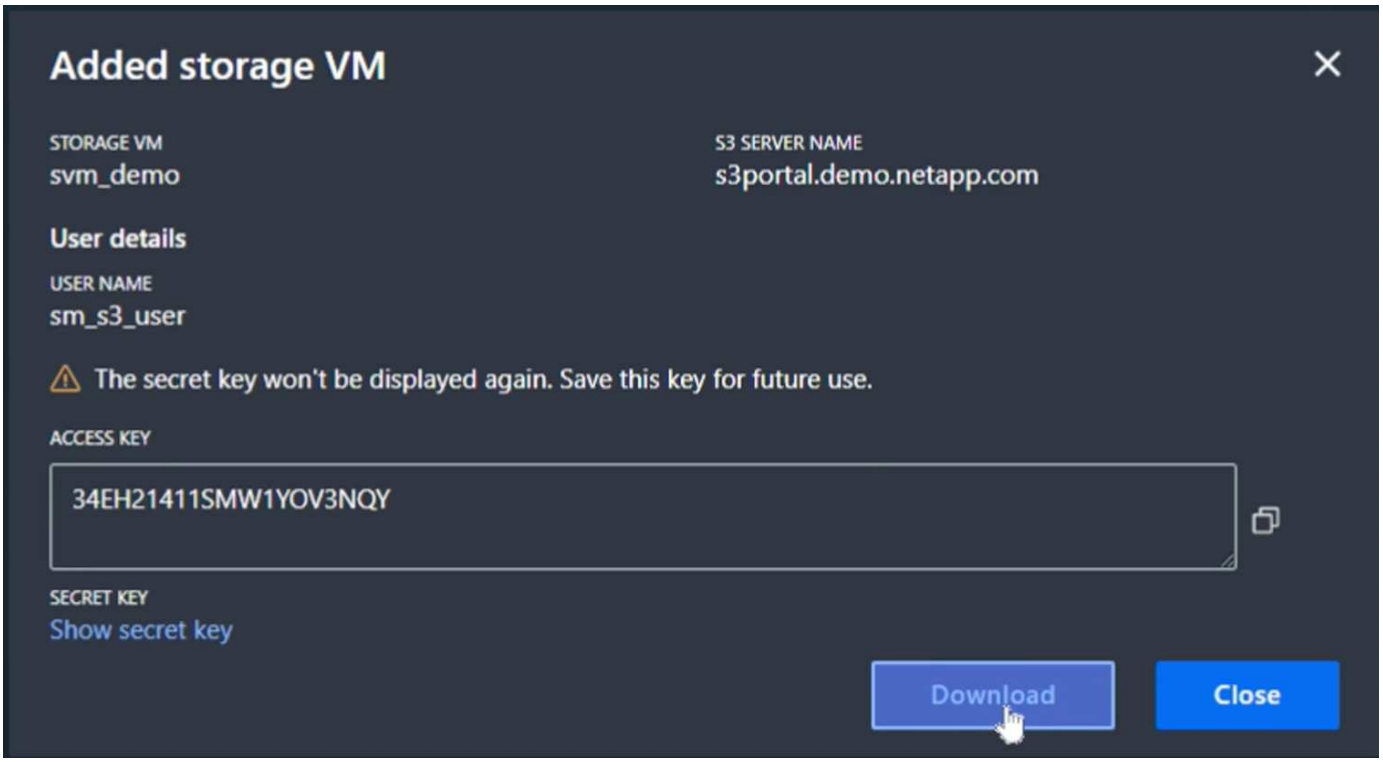
ONTAP 시스템 관리자에서 스토리지 VM으로 이동하여 새 스토리지 VM을 추가합니다.



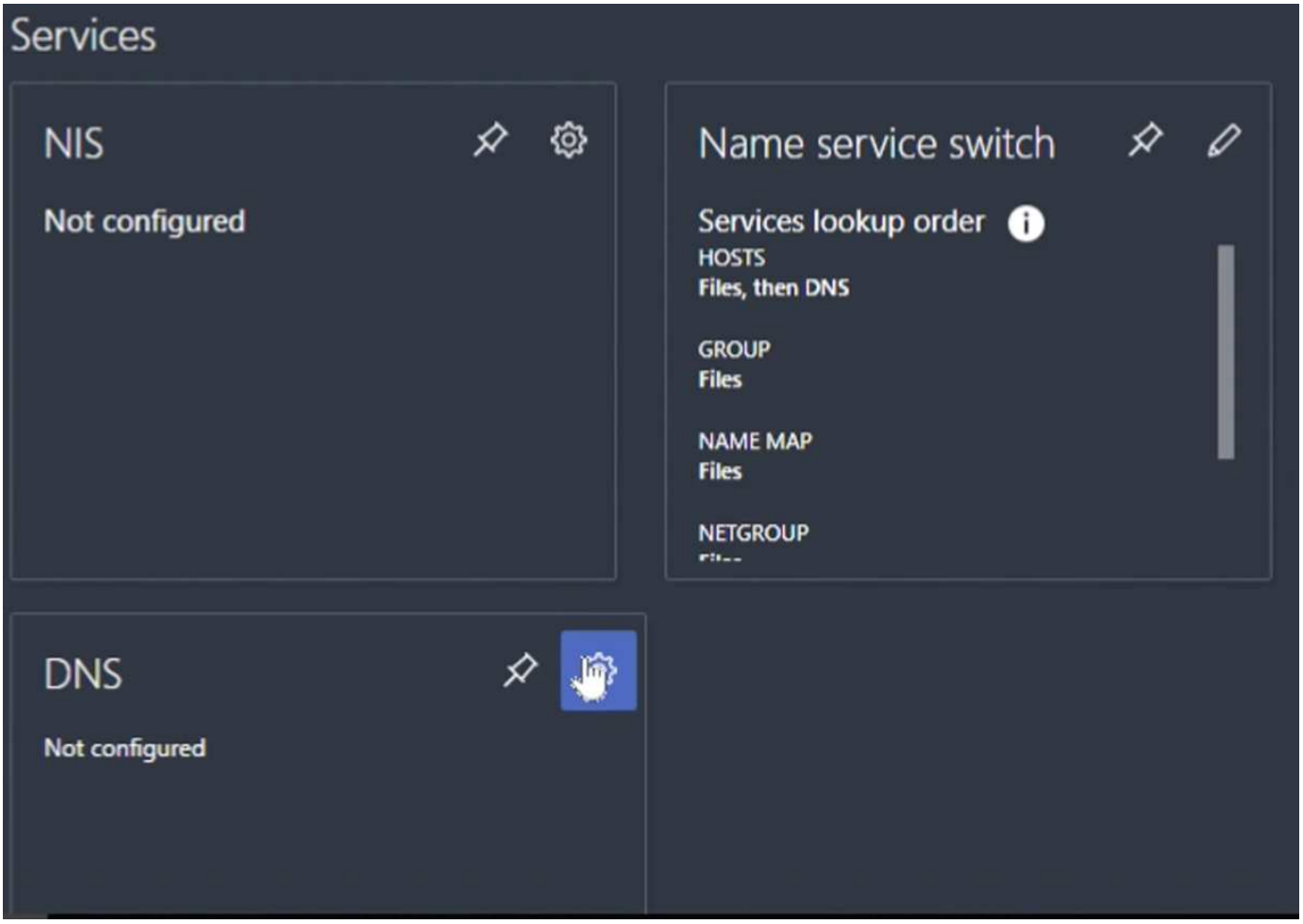
"S3 활성화" 및 "TLS 활성화" 확인란을 선택하고 HTTP(S) 포트를 구성합니다. IP, 서브넷 마스크를 정의하고 게이트웨이 및 브로드캐스트 도메인을 정의하십시오(기본 또는 필수).



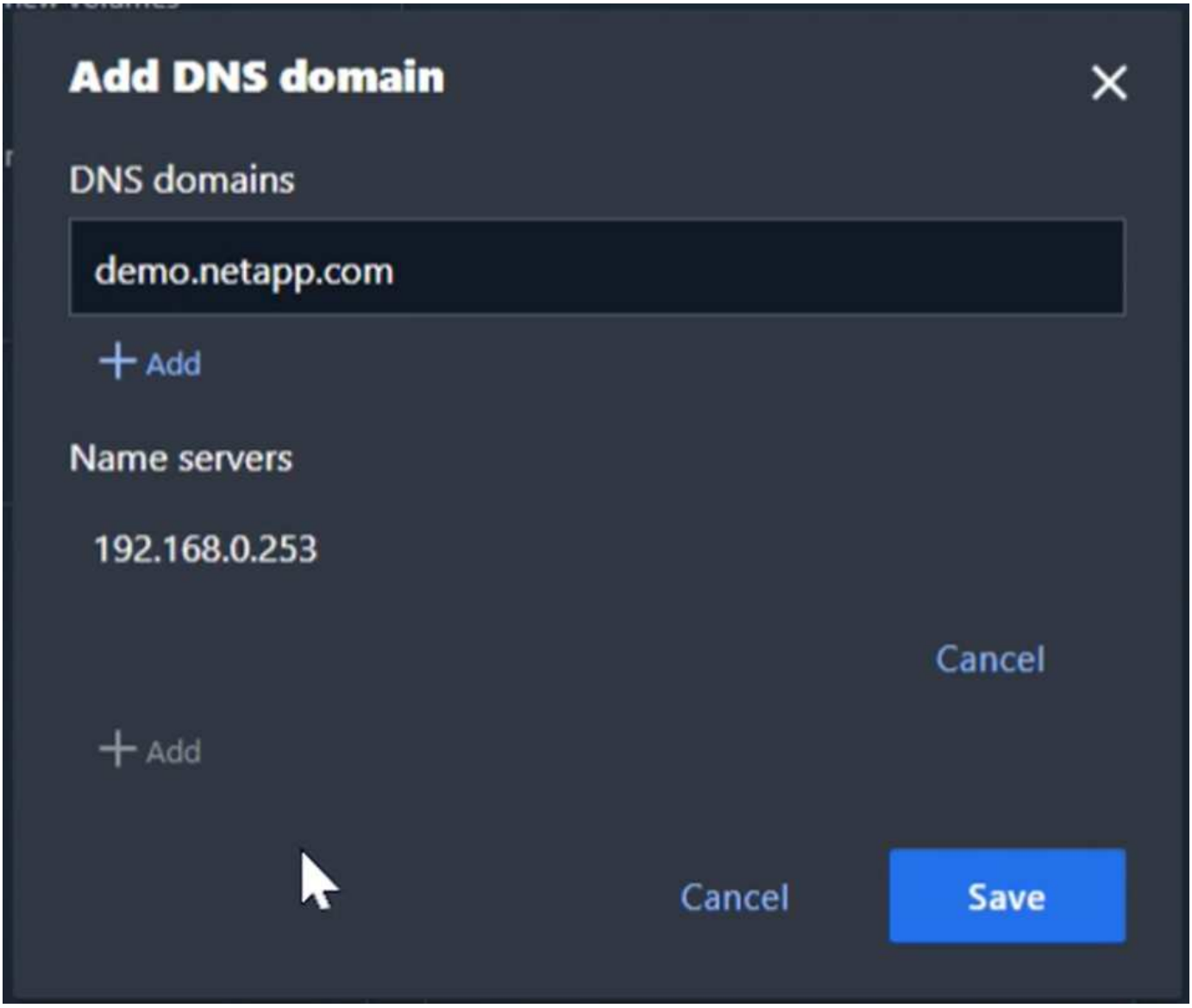
SVM을 생성할 때 사용자가 생성됩니다. 이 사용자의 S3 키를 다운로드하고 창을 닫습니다.



SVM이 생성되면 SVM을 편집하고 DNS 설정을 추가합니다.

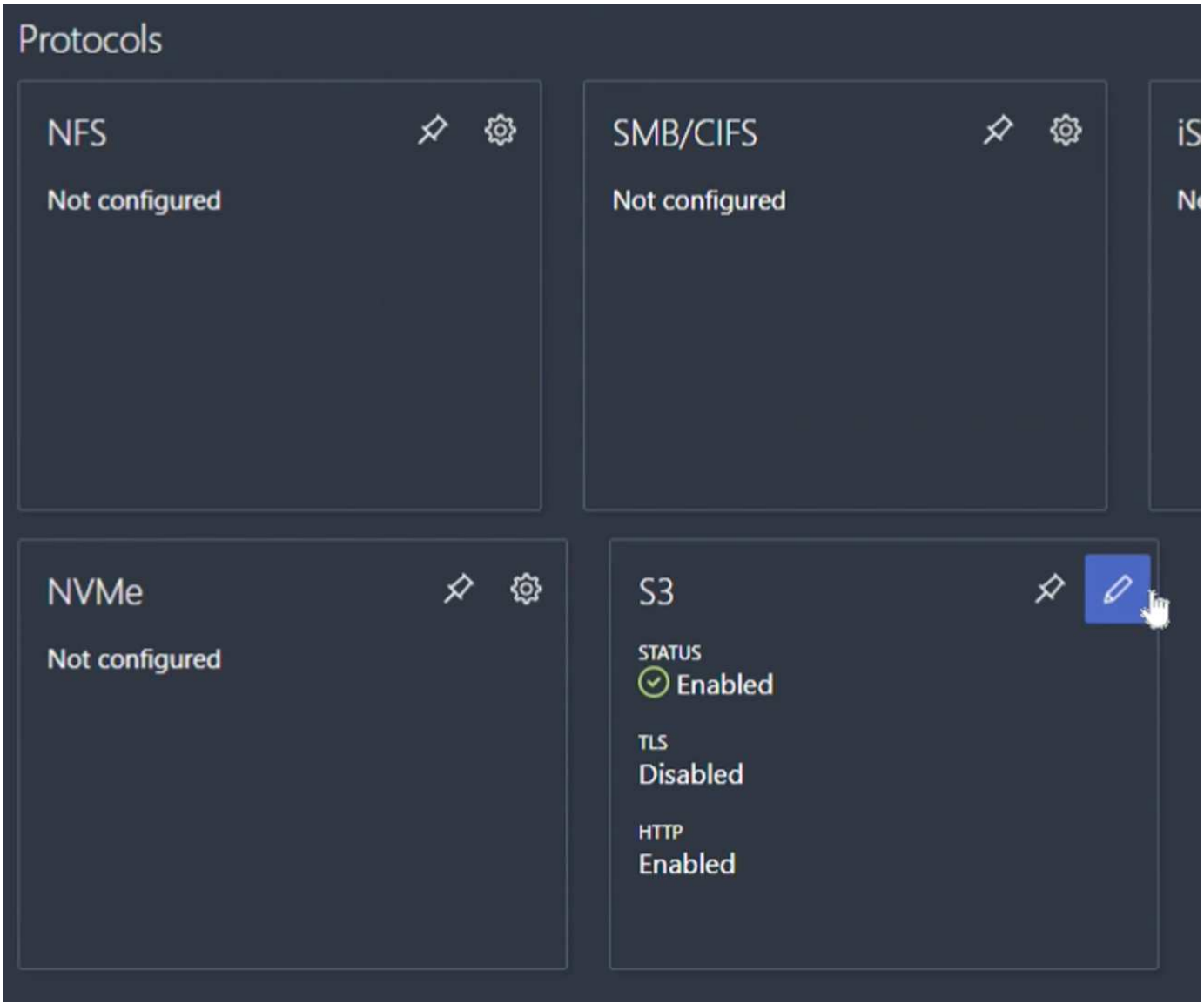


DNS 이름 및 IP를 정의합니다.

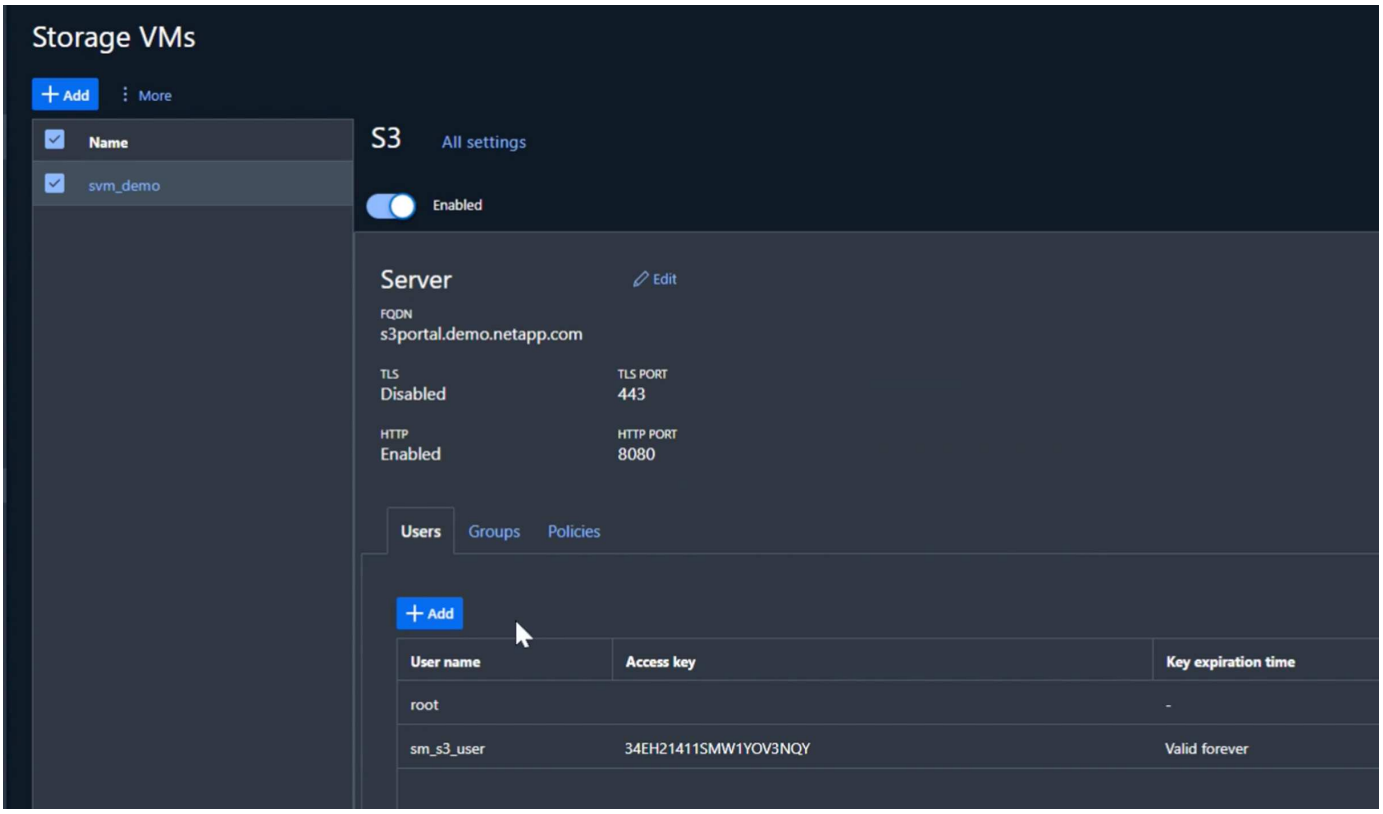


SVM S3 사용자를 생성합니다

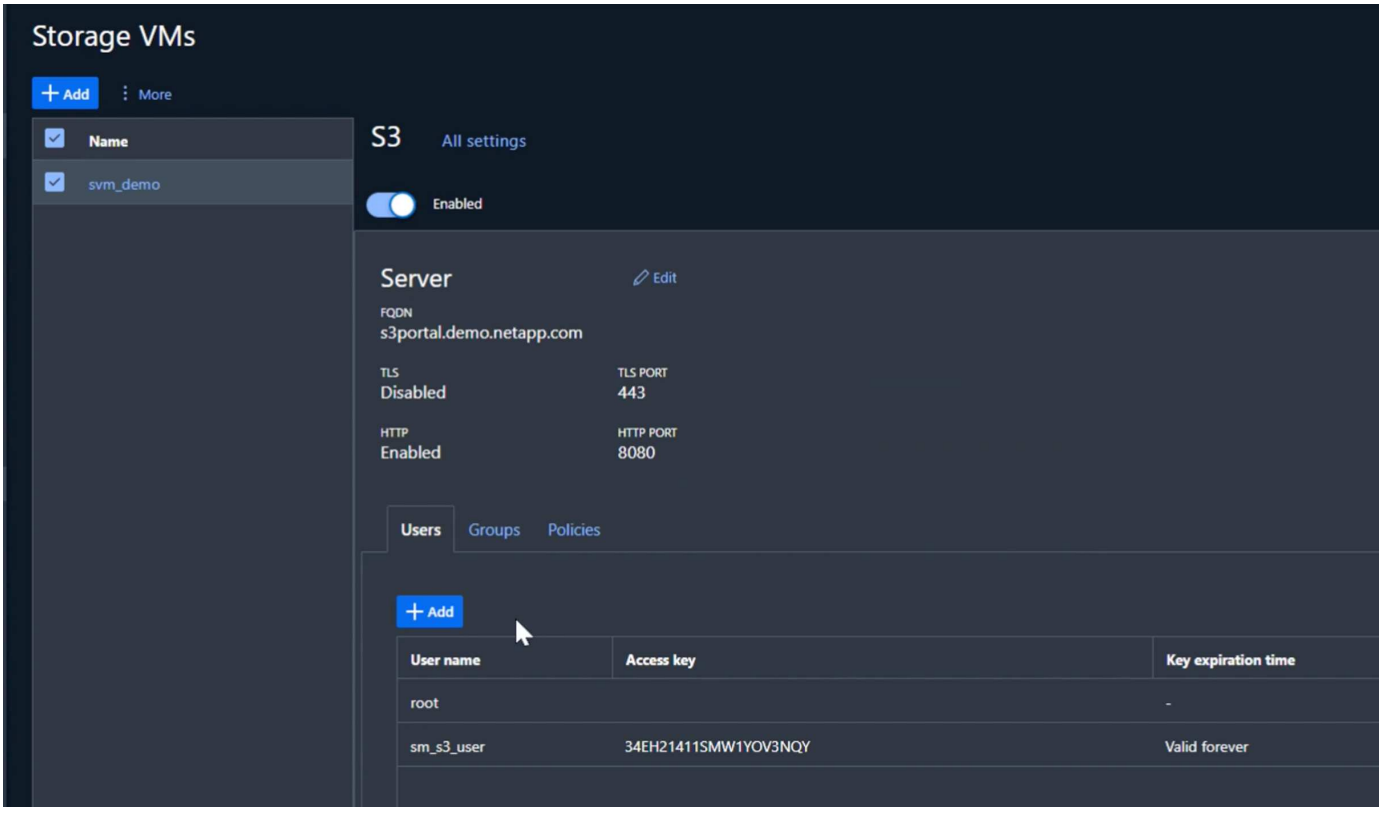
이제 S3 사용자 및 그룹을 구성할 수 있습니다. S3 설정을 편집합니다.


Protocols
NFS
Not configured
SMB/CIFS
Not configured
NVMe
Not configured
S3
STATUS
Enabled
TLS
Disabled
HTTP
Enabled

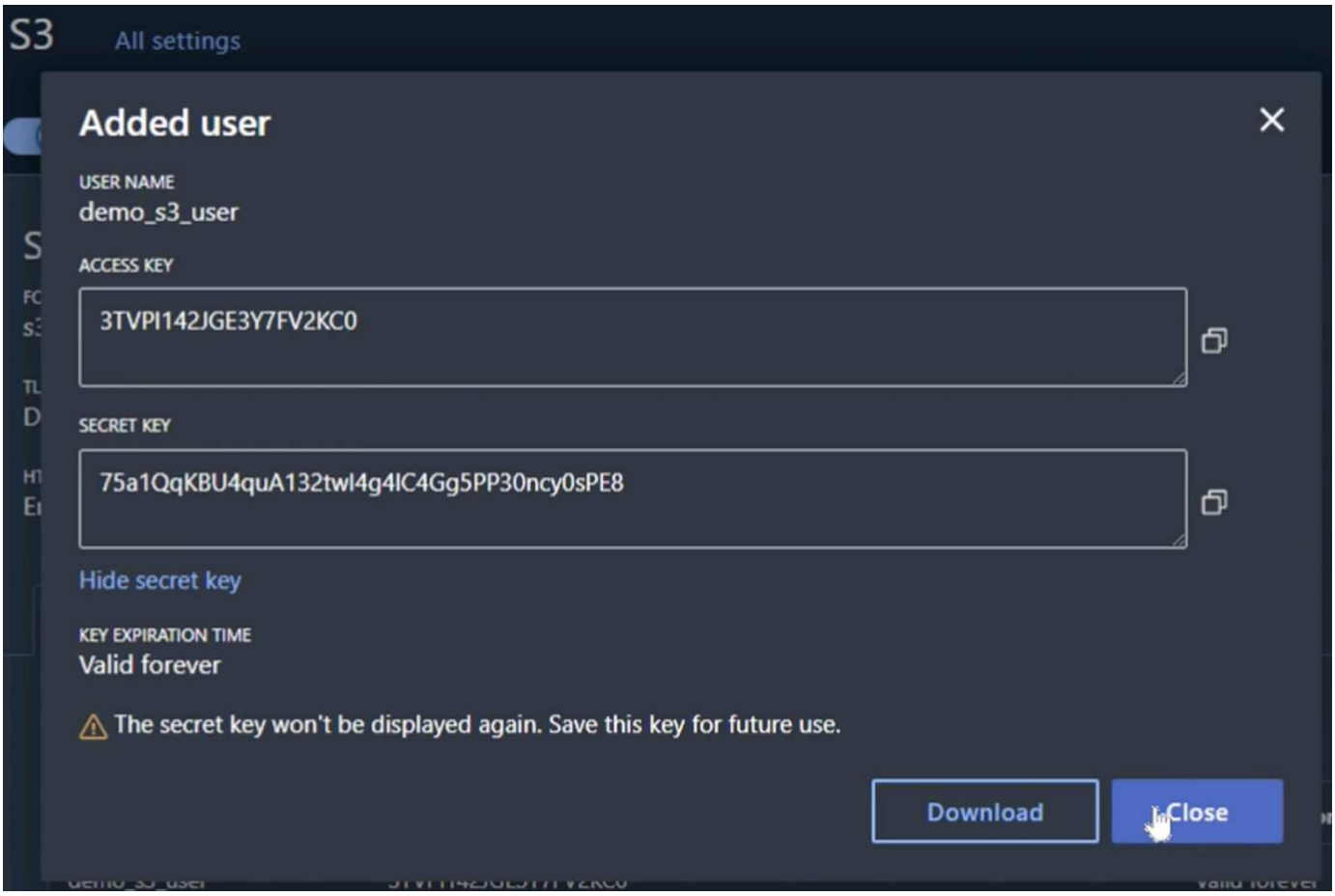
새 사용자를 추가합니다.



사용자 이름과 키 만료 날짜를 입력합니다.

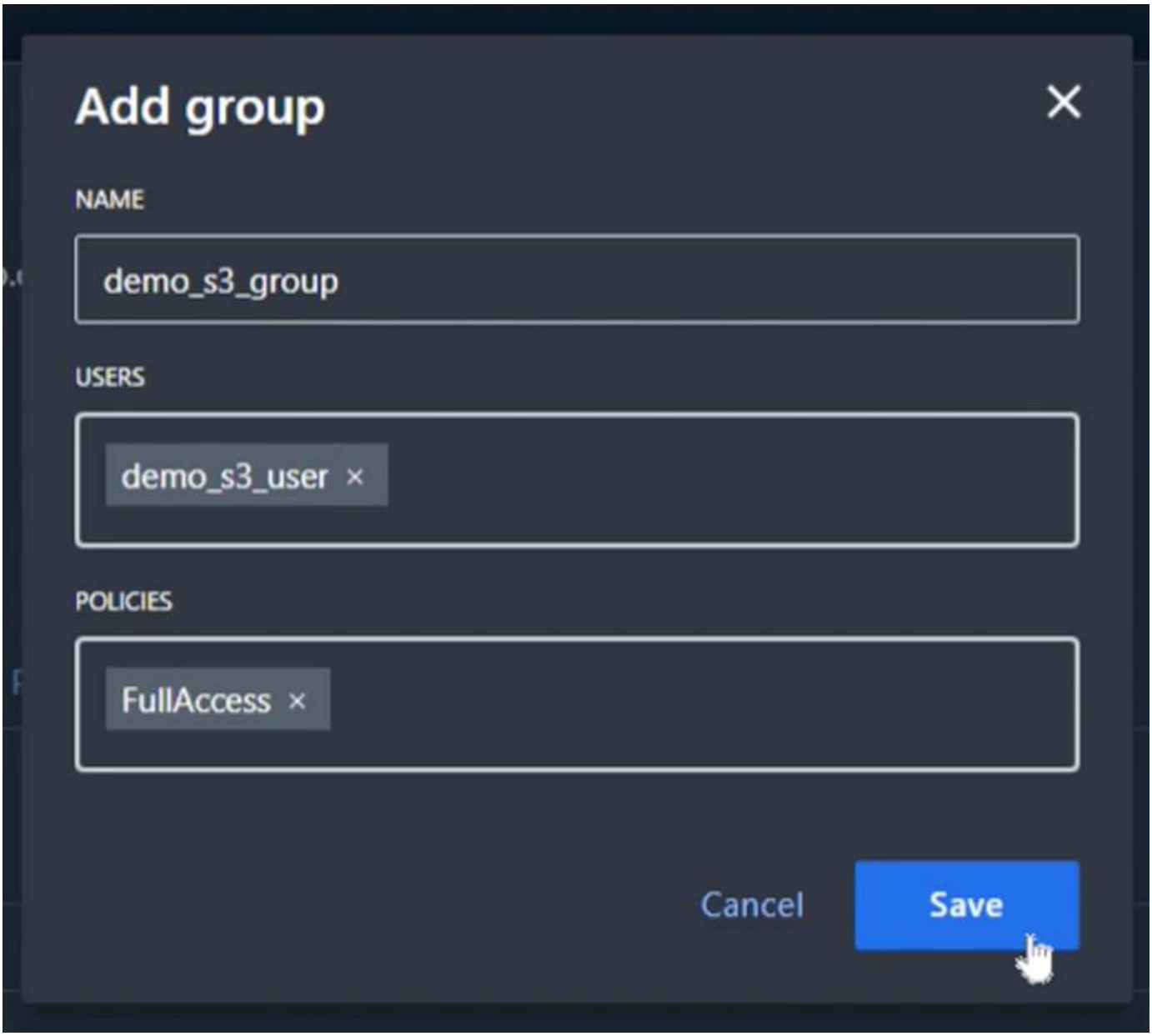


새 사용자의 S3 키를 다운로드합니다.



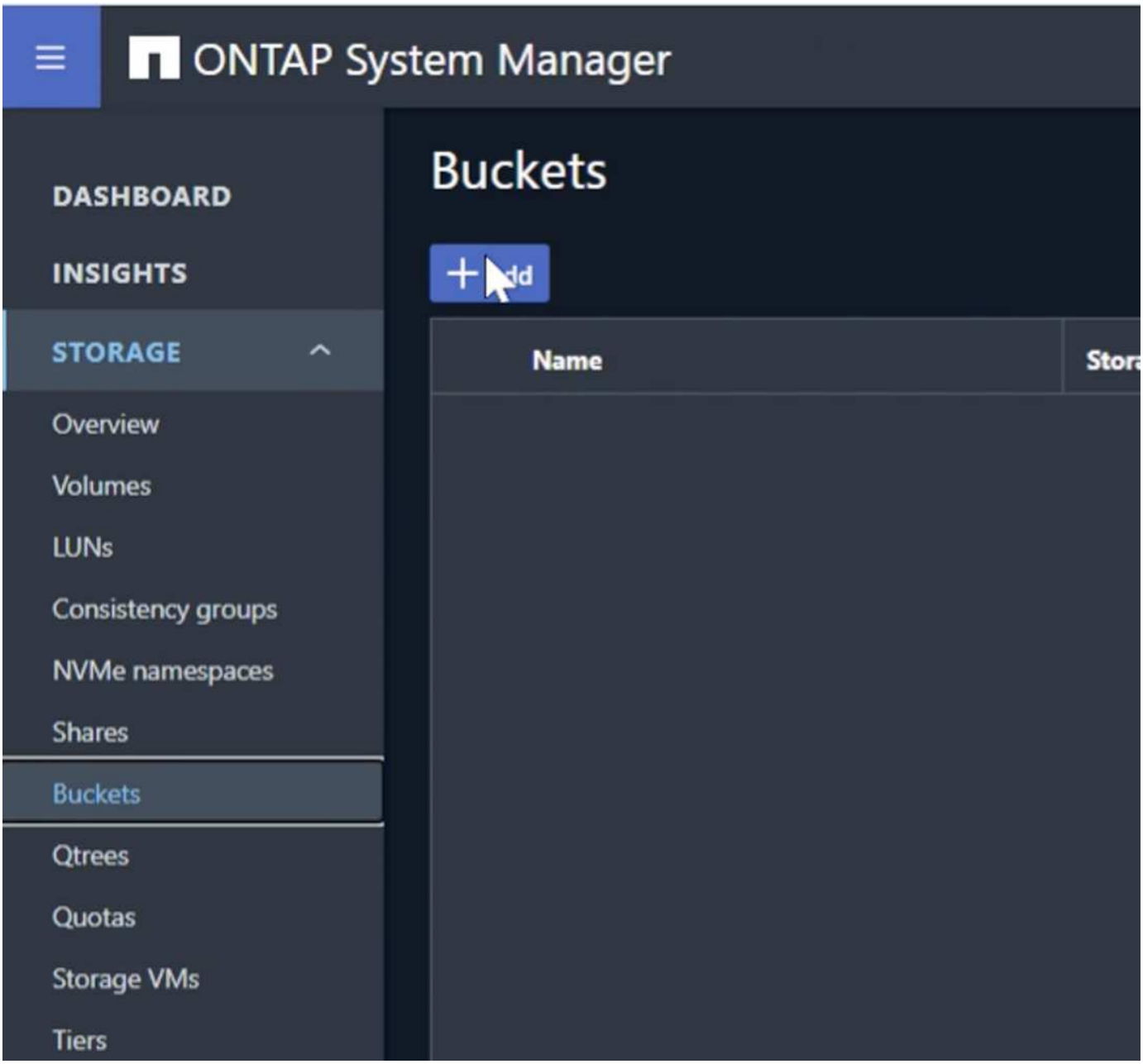
SVM S3 그룹 생성

SVM S3 설정의 그룹 탭에서 위에서 생성한 사용자 및 FullAccess 권한이 있는 새 그룹을 추가합니다.

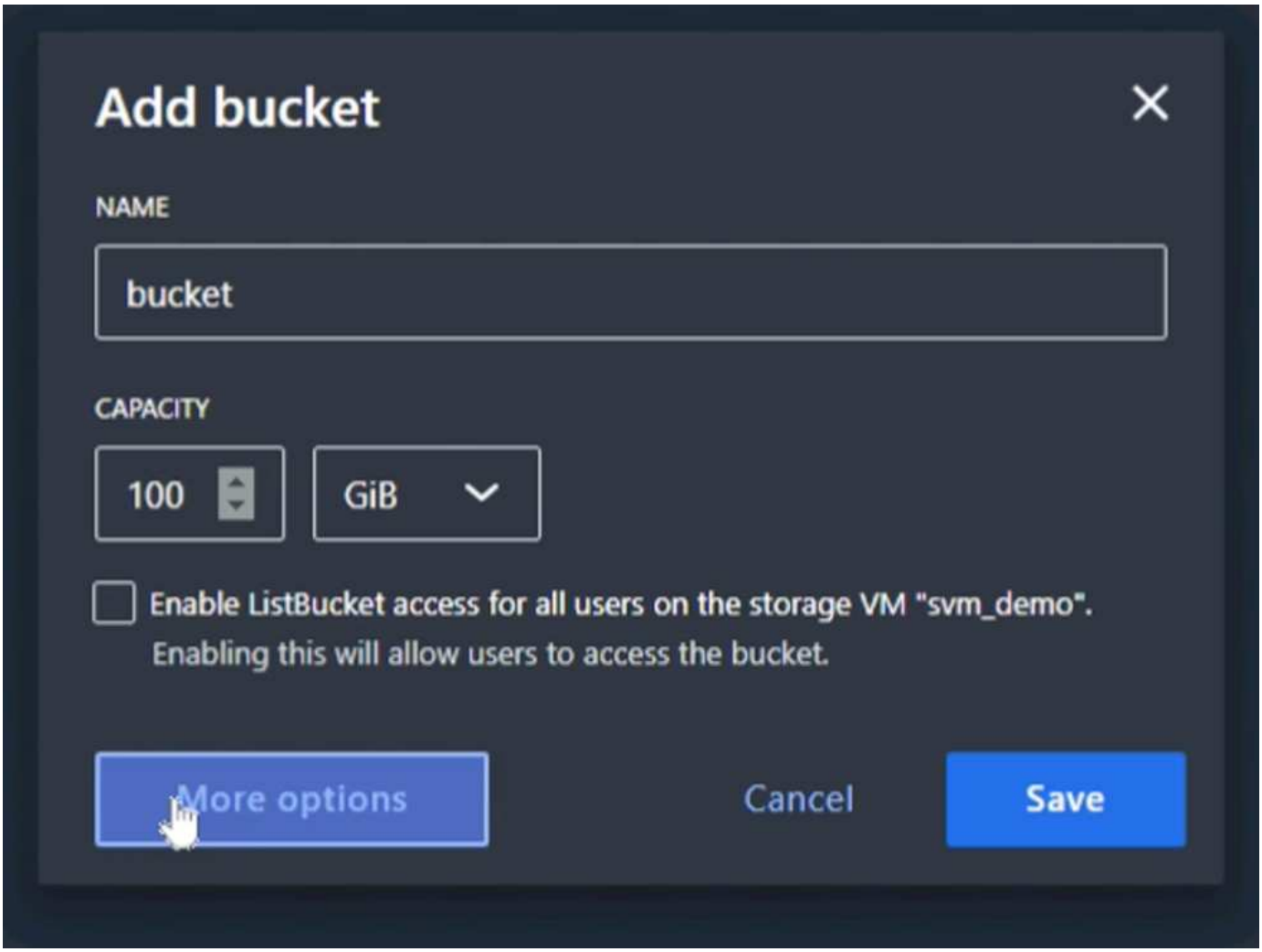


SVM S3 버킷을 생성합니다

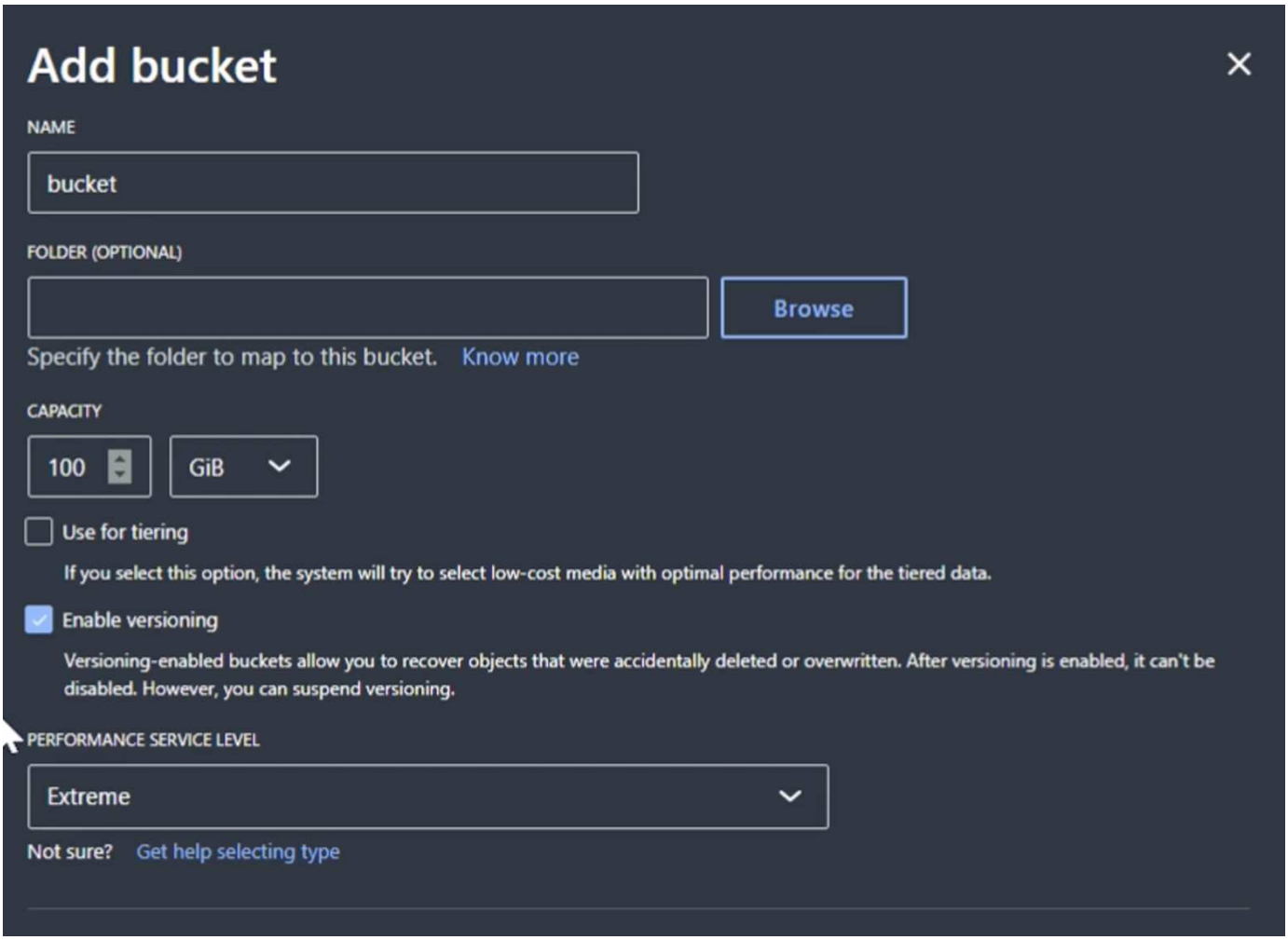
Bucket 섹션으로 이동하여 "+Add" 버튼을 클릭합니다.



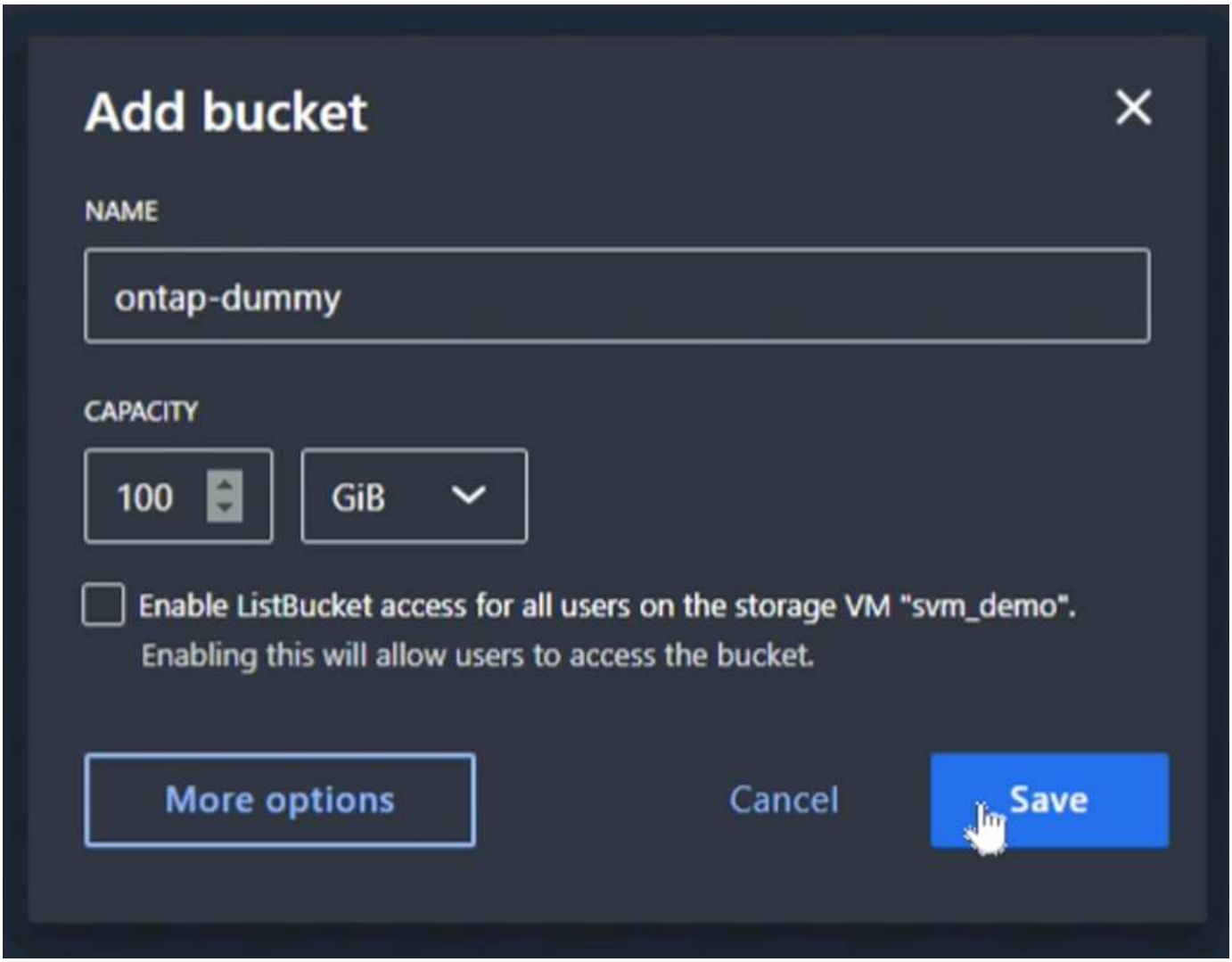
이름, 용량을 입력하고 "ListBucket 액세스 사용…" 확인란의 선택을 취소하고 "추가 옵션" 버튼을 클릭합니다.



"추가 옵션" 섹션에서 버전 관리 활성화 확인란을 선택하고 "저장" 단추를 클릭합니다.



이 프로세스를 반복하고 버전 관리를 사용하지 않고 두 번째 버킷을 만듭니다. 버킷 1과 동일한 용량의 이름을 입력하고 "ListBucket 액세스 사용…" 확인란의 선택을 취소하고 "저장" 버튼을 클릭합니다.



라파엘 게데스, 아론 클라인

ONTAP S3에서 **StorageGRID**로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 **S3**를 지원합니다

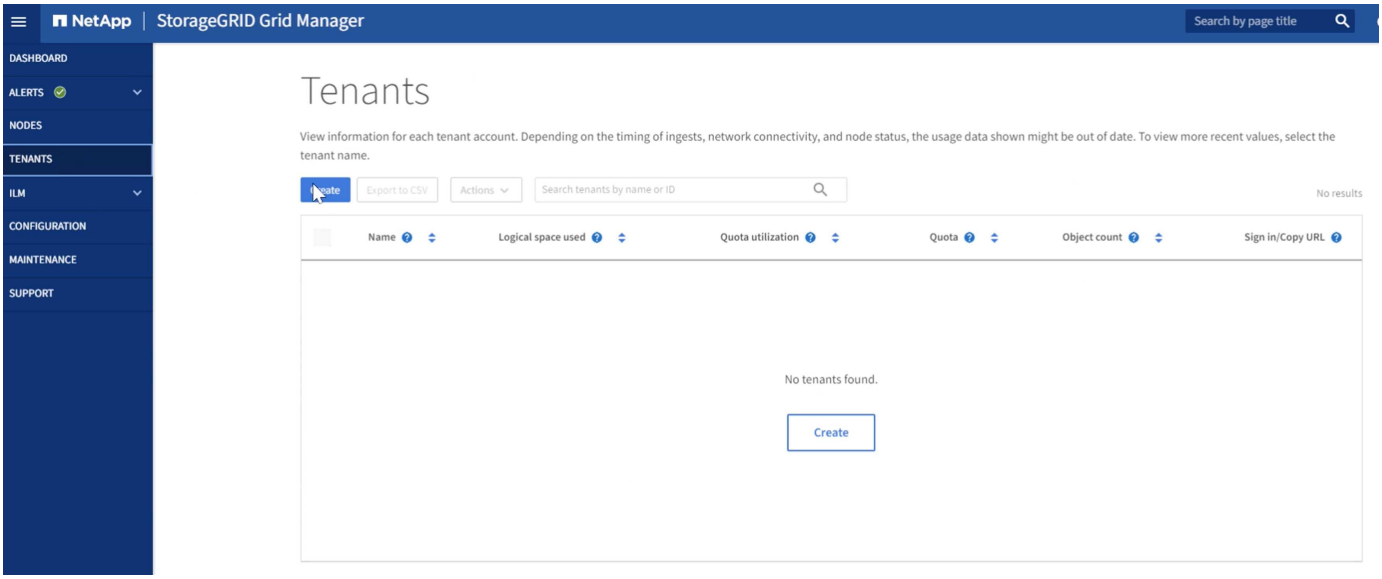
ONTAP S3에서 StorageGRID로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 S3를 지원합니다

StorageGRID 준비 중

이 데모의 구성을 계속하면 테넌트, 사용자, 보안 그룹, 그룹 정책 및 버킷을 생성합니다.

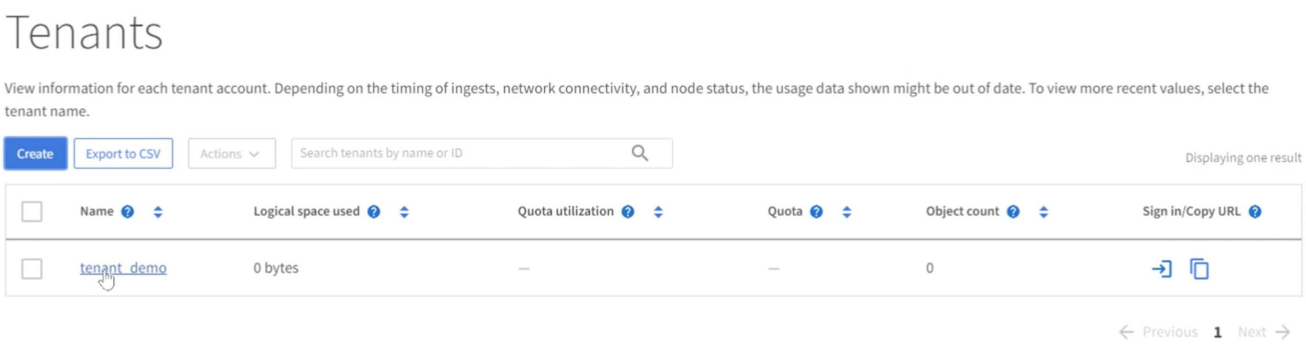
테넌트를 만듭니다

"Tenants" 탭으로 이동하고 "Create" 버튼을 클릭합니다

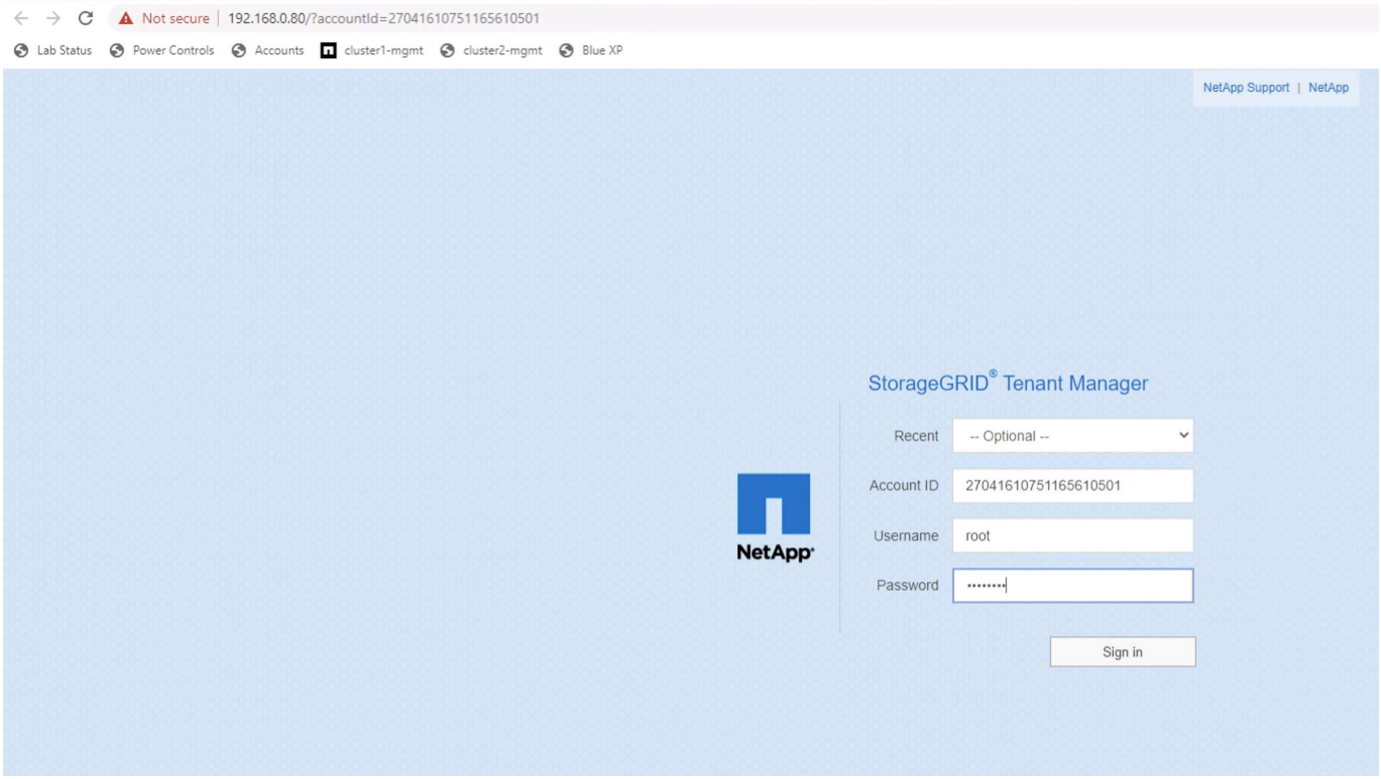


테넌트 이름을 제공하는 테넌트에 대한 세부 정보를 입력하고 클라이언트 유형으로 S3를 선택하면 할당량이 필요하지 않습니다. 플랫폼 서비스를 선택하거나 S3 선택을 허용하지 않아도 됩니다. 원하는 경우 고유한 ID 소스를 사용하도록 선택할 수 있습니다. 루트 암호를 설정하고 마침 단추를 클릭합니다.

테넌트 세부 정보를 보려면 테넌트 이름을 클릭합니다. * 나중에 테넌트 ID가 필요하므로 이를 복사하십시오. *. 로그인 버튼을 클릭합니다. 그러면 테넌트 포털 로그인이 나타납니다. 나중에 사용할 수 있도록 URL을 저장합니다.

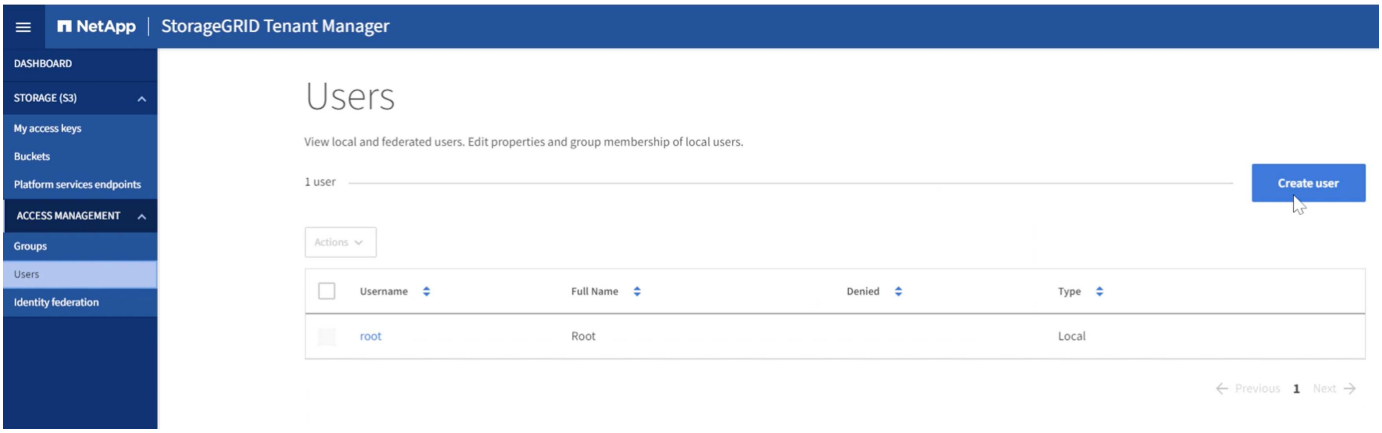


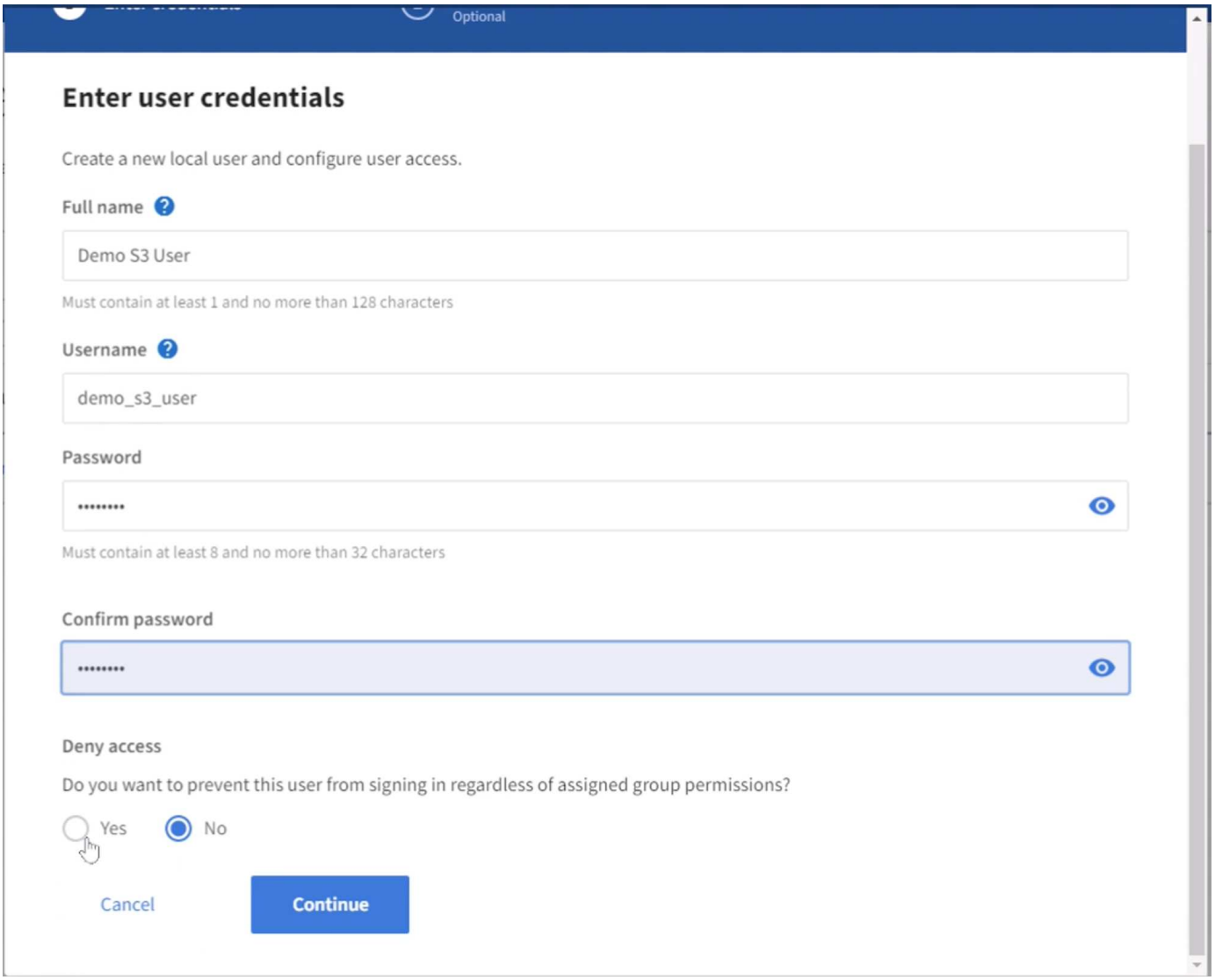
그러면 테넌트 포털 로그인이 나타납니다. 나중에 사용할 수 있도록 URL을 저장하고 루트 사용자 자격 증명을 입력합니다.



사용자를 생성합니다

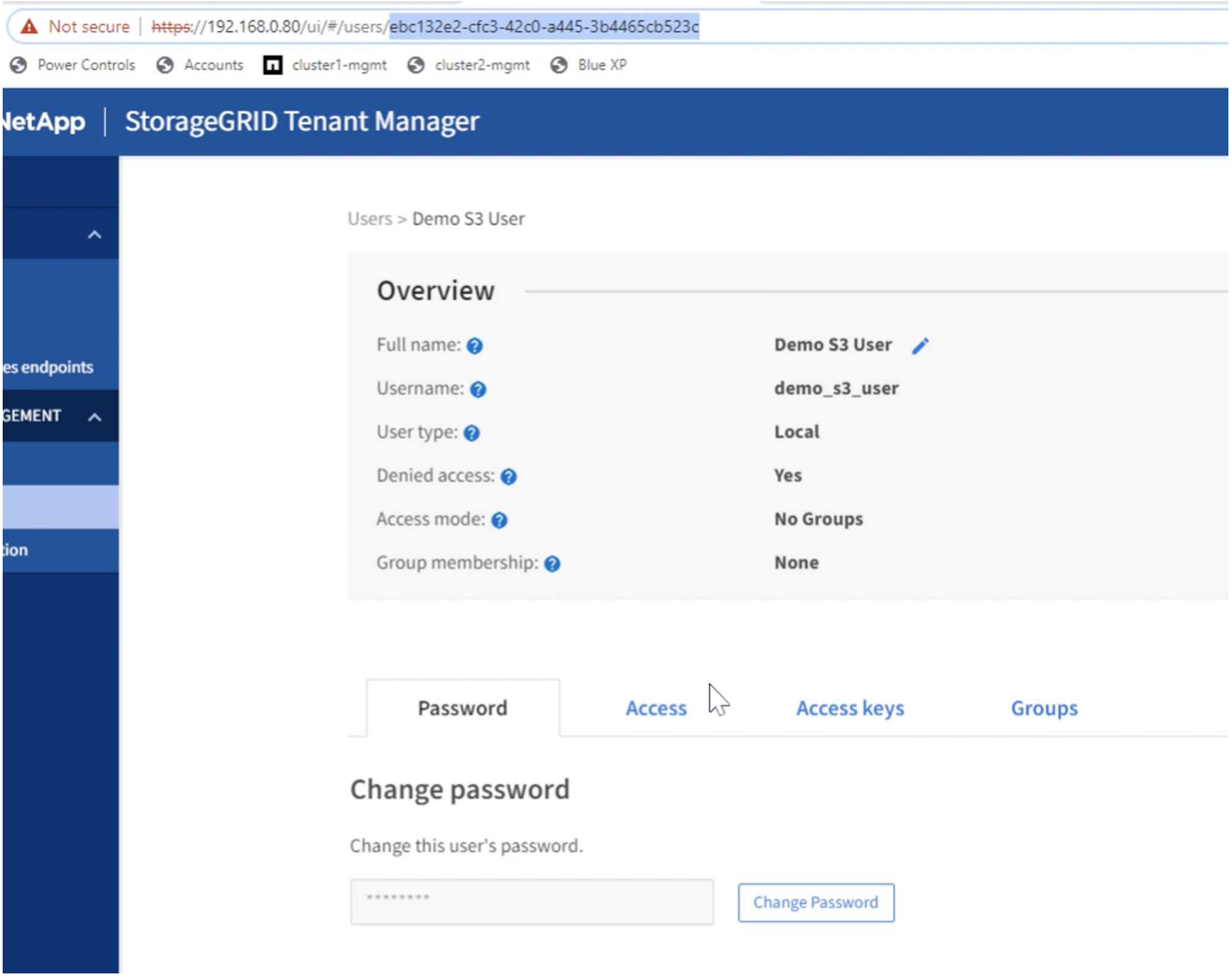
사용자 탭으로 이동하여 새 사용자를 생성합니다.



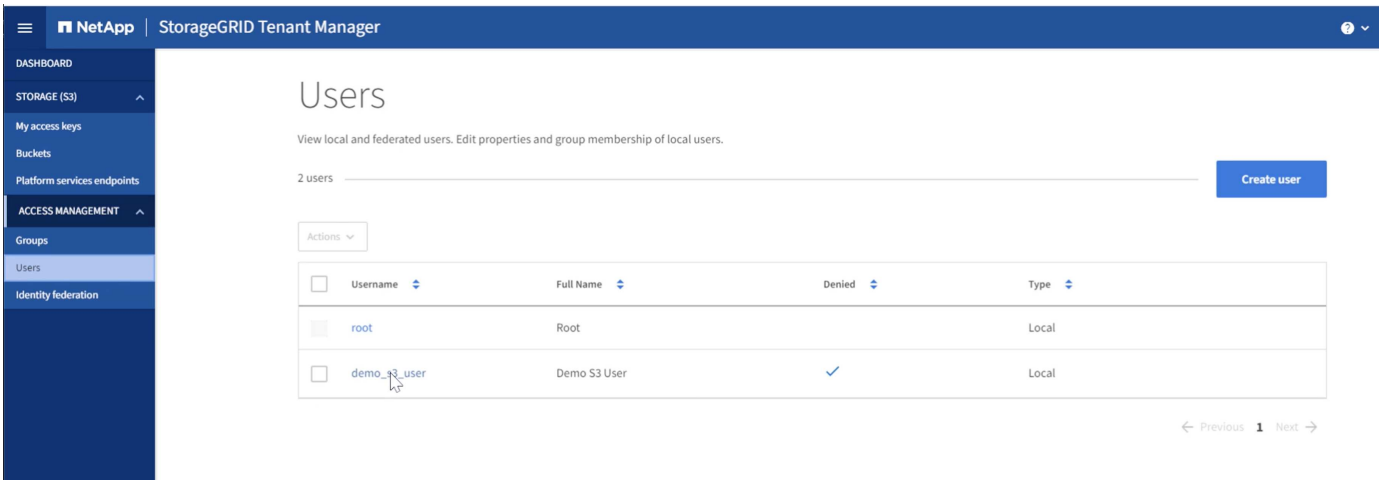


이제 새 사용자가 생성되었으므로 사용자 이름을 클릭하여 사용자 세부 정보를 엽니다.

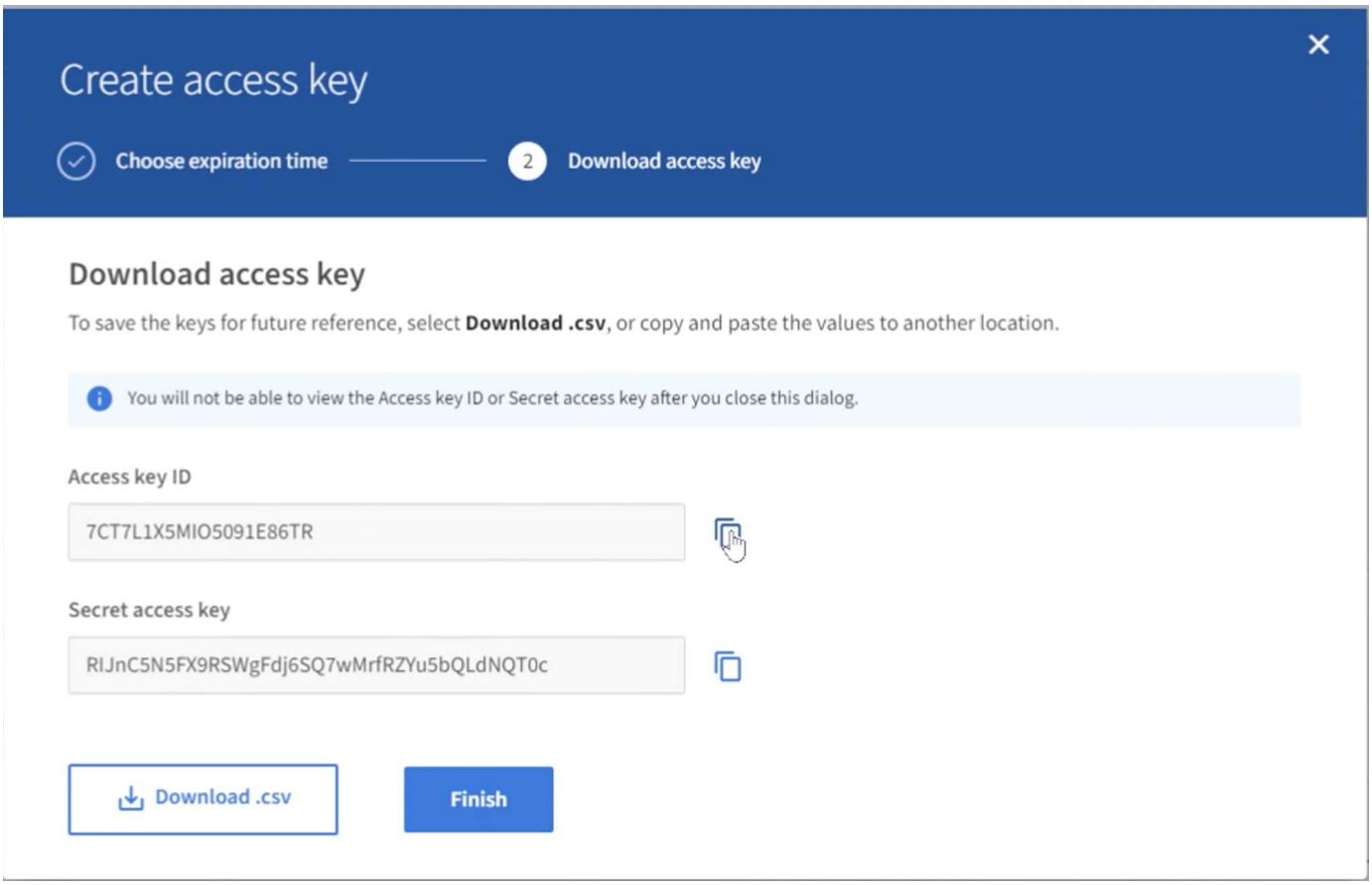
나중에 사용할 URL에서 사용자 ID를 복사합니다.



S3 키를 생성하려면 사용자 이름을 클릭합니다.

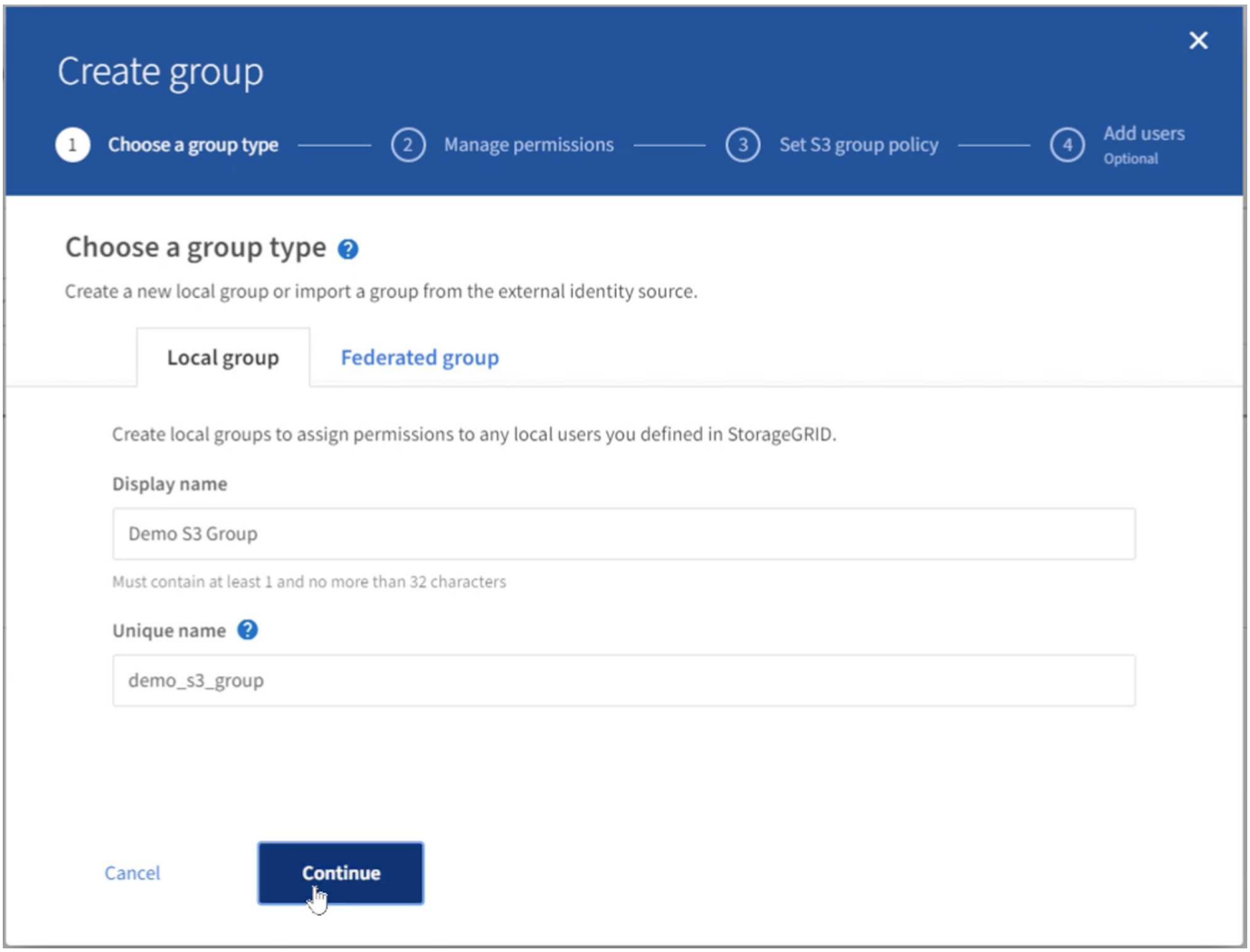


"액세스 키" 탭을 선택하고 "키 만들기" 버튼을 클릭합니다. 만료 시간을 설정할 필요가 없습니다. 창이 닫히면 다시 검색할 수 없으므로 S3 키를 다운로드합니다.

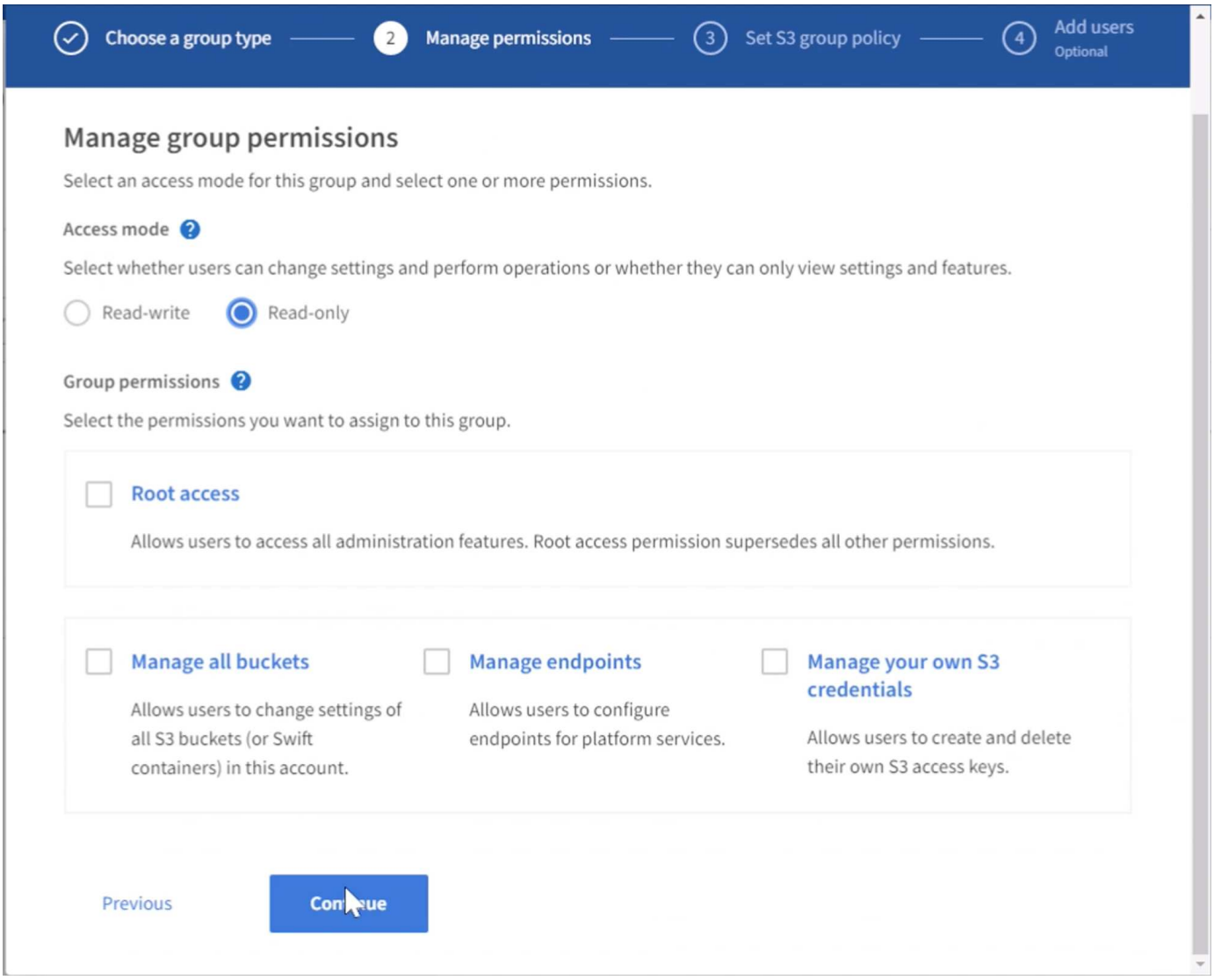


보안 그룹을 만듭니다

이제 그룹 페이지로 이동하여 새 그룹을 만듭니다.

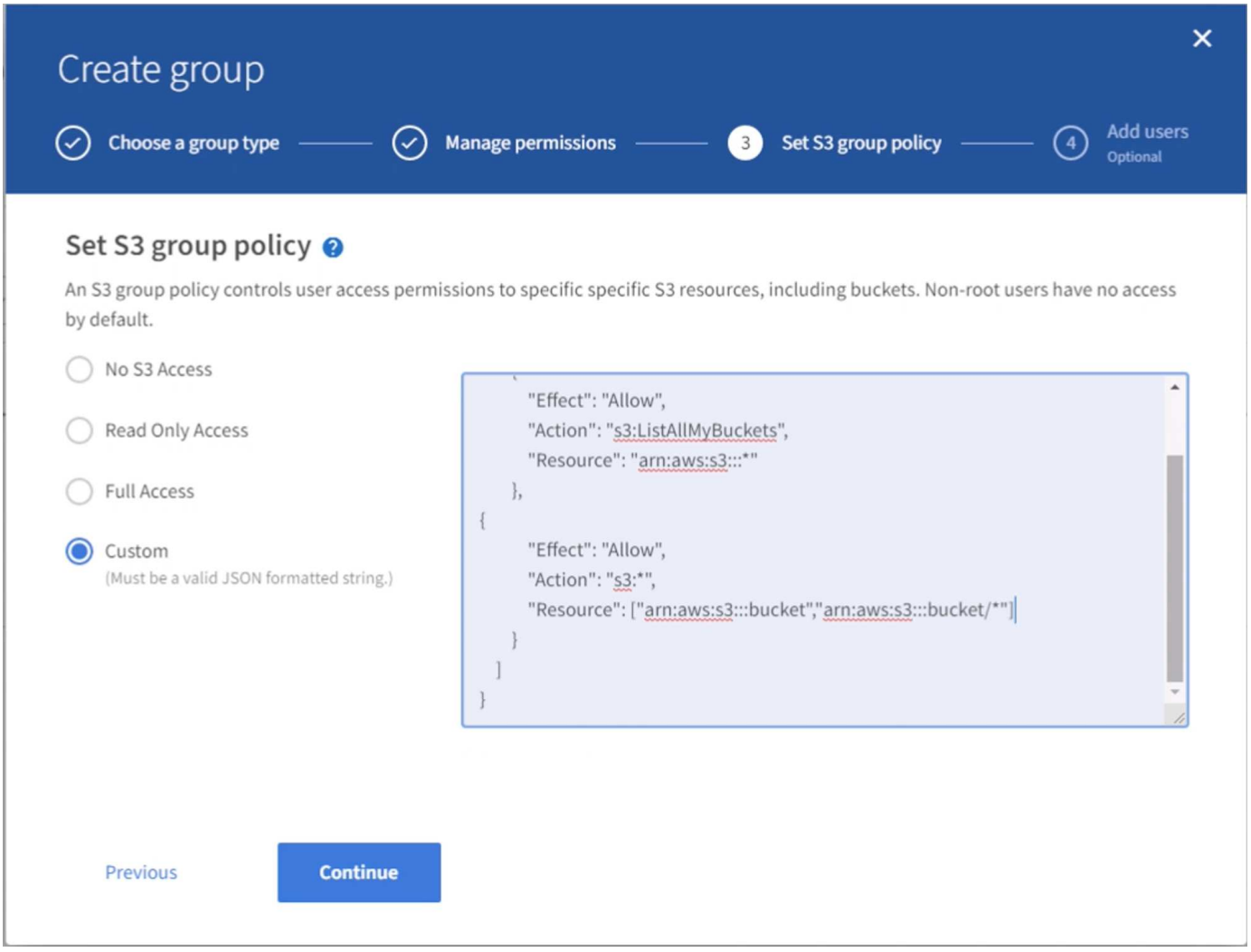


그룹 권한을 읽기 전용으로 설정합니다. S3 사용 권한이 아닌 테넌트 UI 사용 권한입니다.

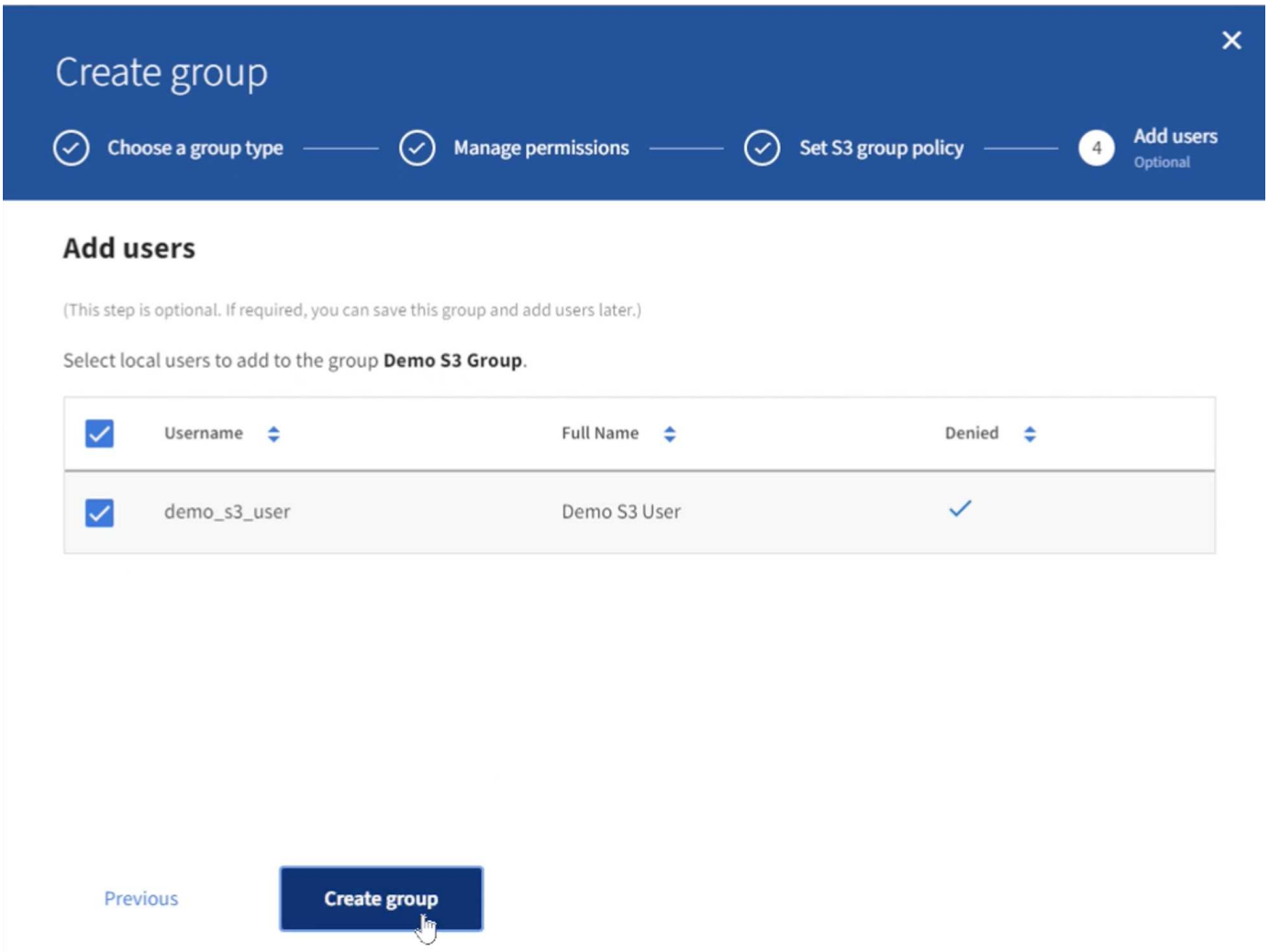


S3 권한은 그룹 정책(IAM 정책)을 통해 제어됩니다. 그룹 정책을 사용자 정의로 설정하고 상자에 json 정책을 붙여 넣습니다. 이 정책을 통해 이 그룹의 사용자는 테넌트의 버킷을 나열하고 버킷에서 "bucket"이라는 이름의 S3 작업 또는 "bucket"이라는 이름의 하위 폴더를 수행할 수 있습니다.

```
{
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
        "Action": "s3:*",
        "Resource": ["arn:aws:s3:::bucket","arn:aws:s3:::bucket/*"]
      }
    ]
}
```

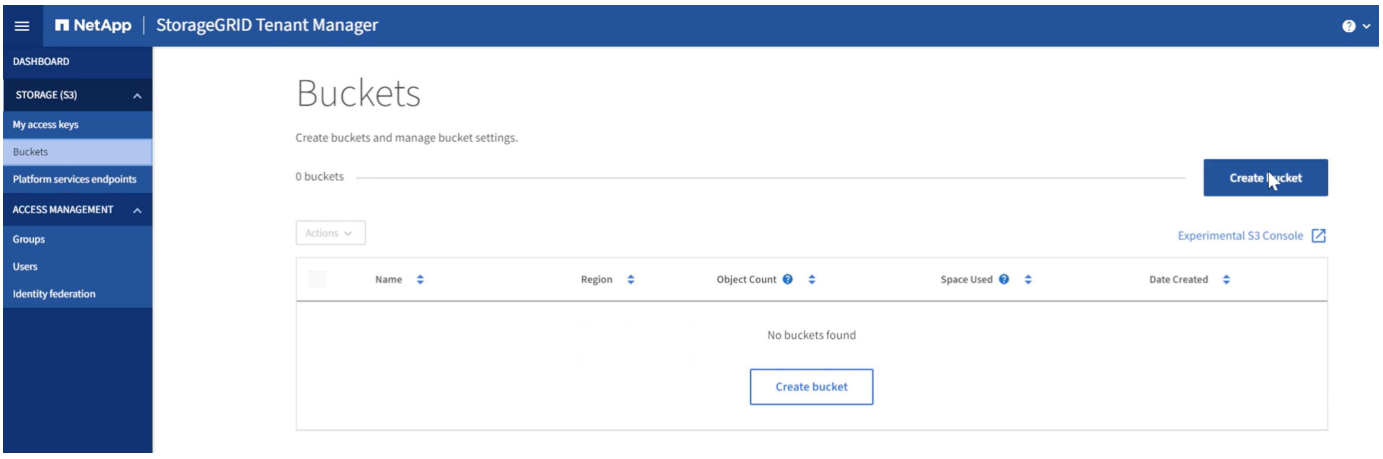


마지막으로 사용자를 그룹에 추가하고 완료합니다.

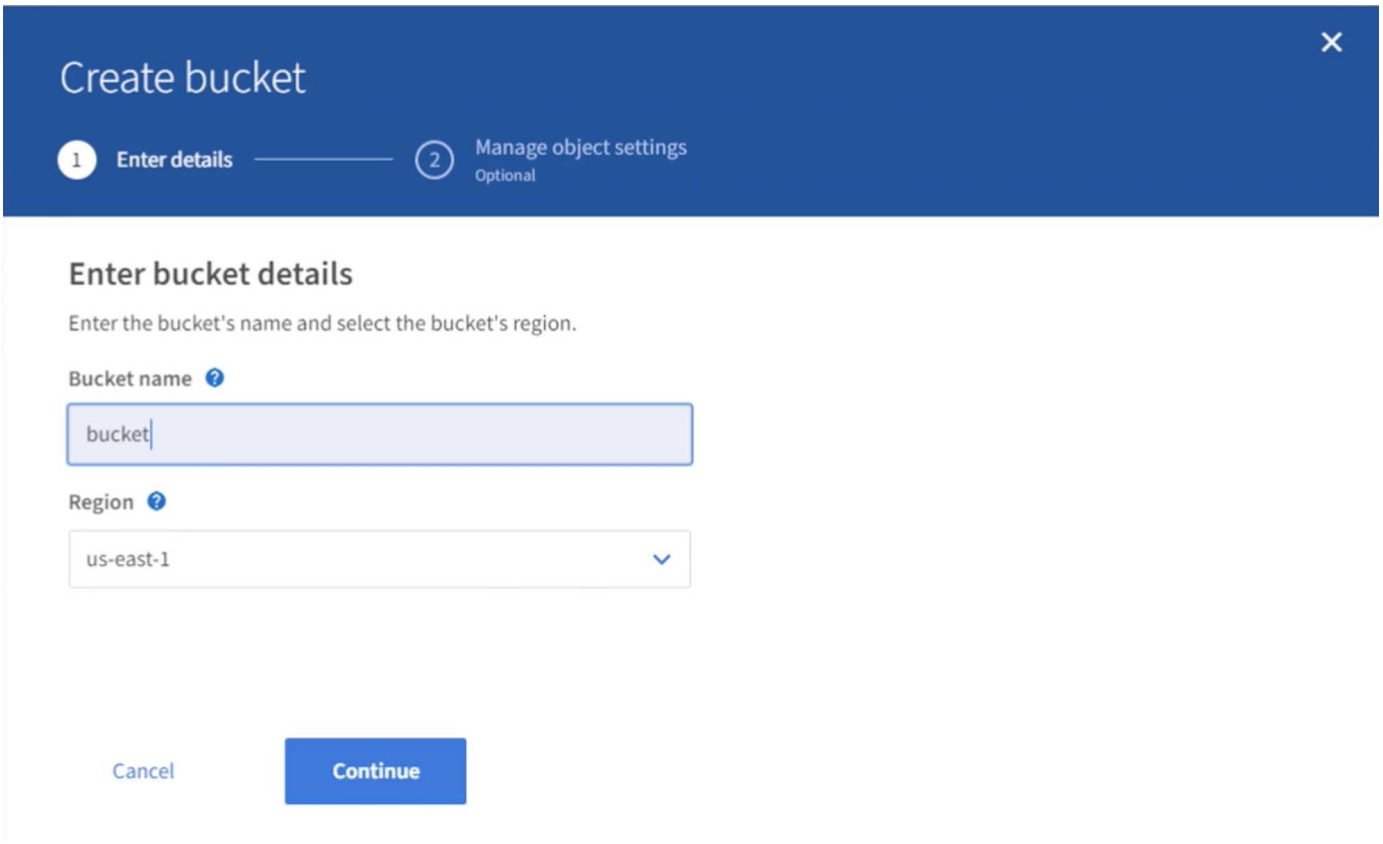


버킷 **2**개를 만듭니다

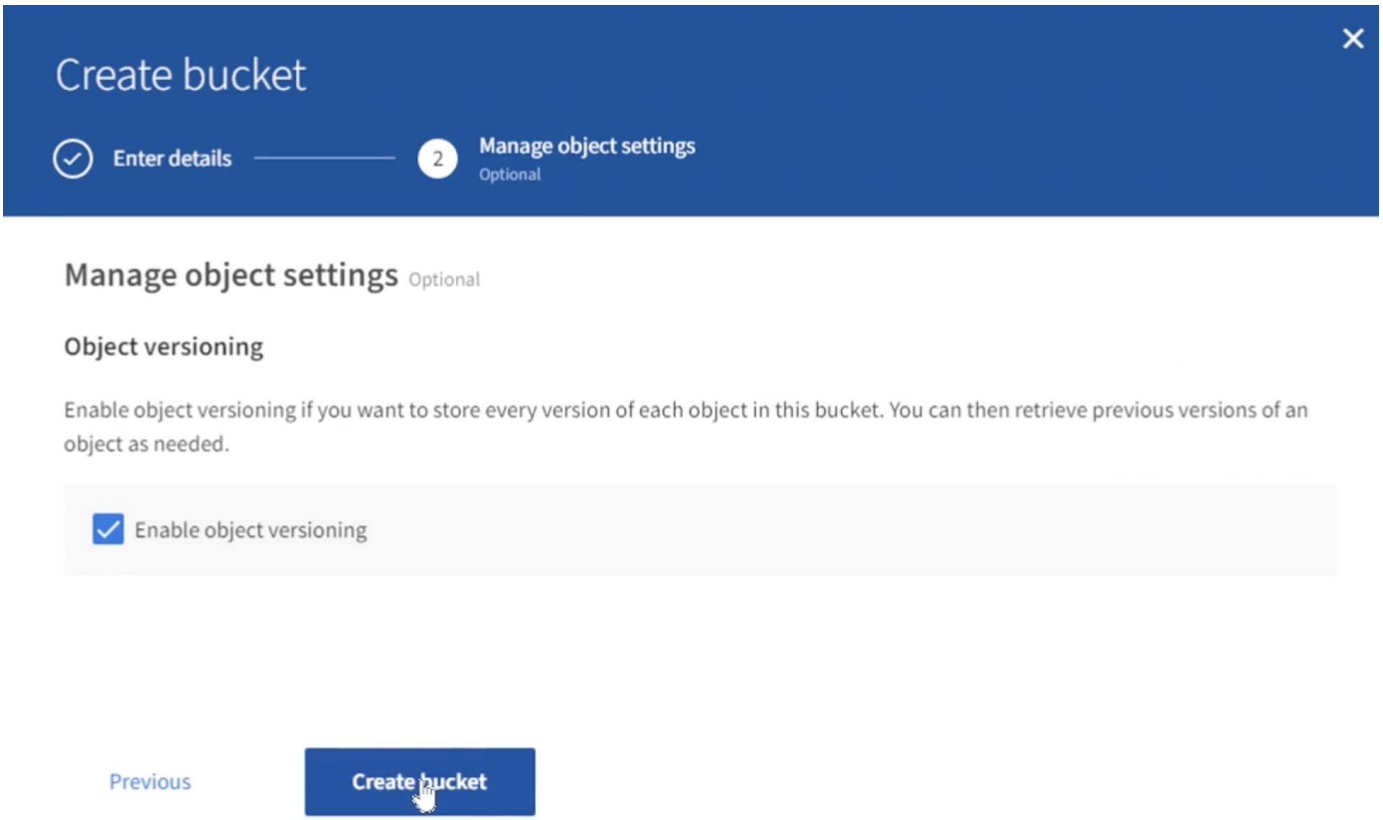
Bucket 탭으로 이동하고 Create Bucket(버킷 생성) 버튼을 클릭합니다.



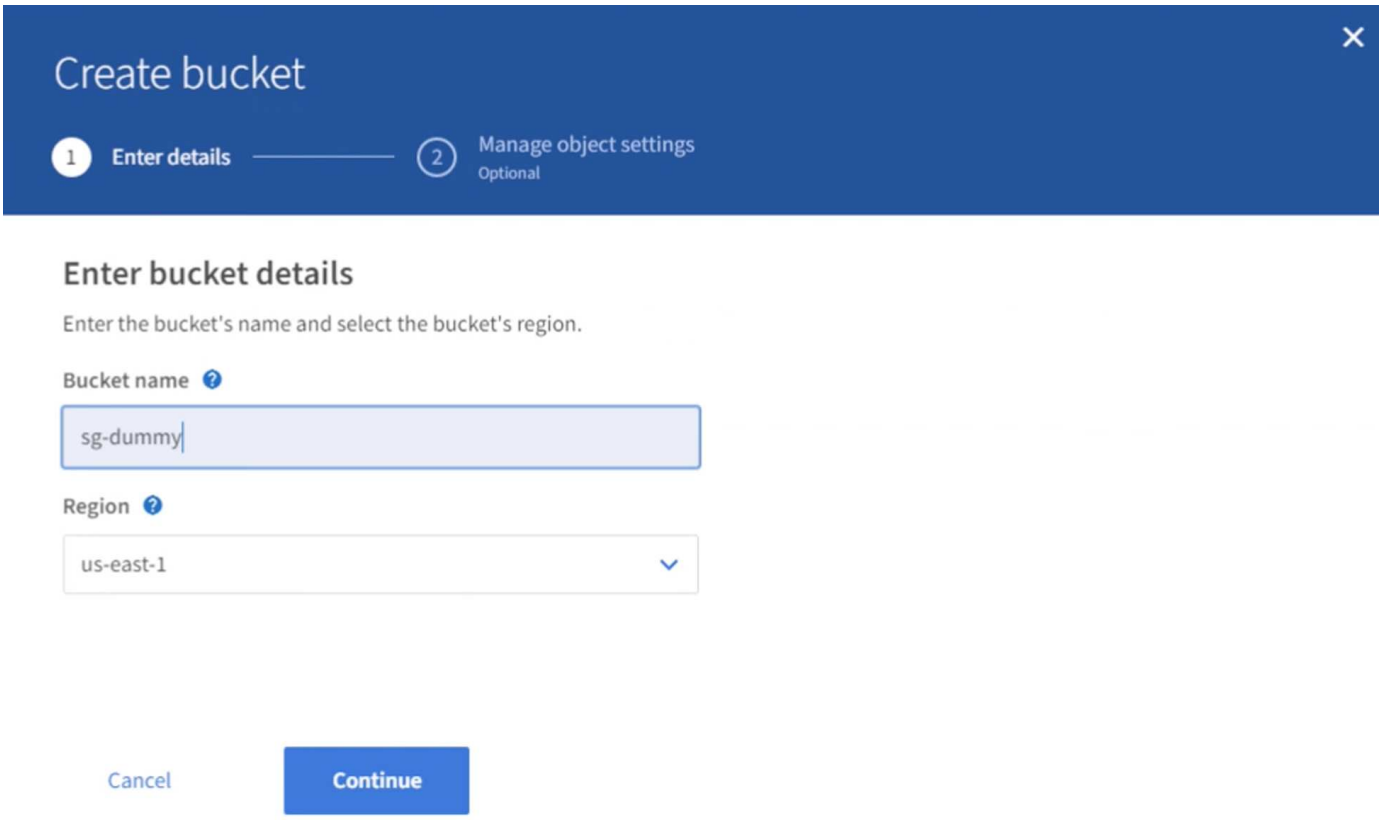
버킷 이름 및 지역을 정의합니다.



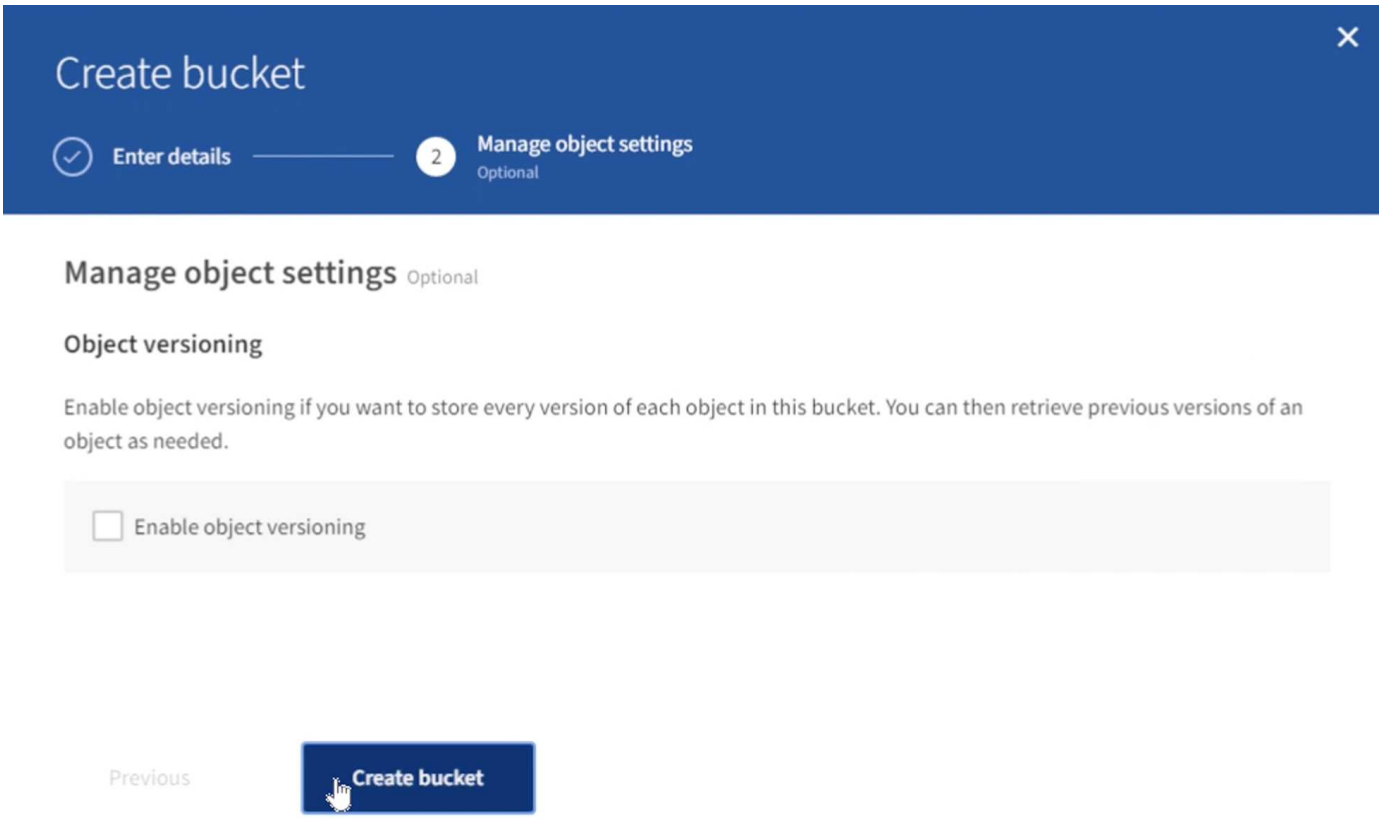
이 첫 번째 버킷에서 버전 관리를 활성화합니다.



이제 버전 관리를 사용하지 않고 두 번째 버킷을 만듭니다.



이 두 번째 버킷에서 버전 관리를 활성화하지 마십시오.



라파엘 게데스, 아론 클라인

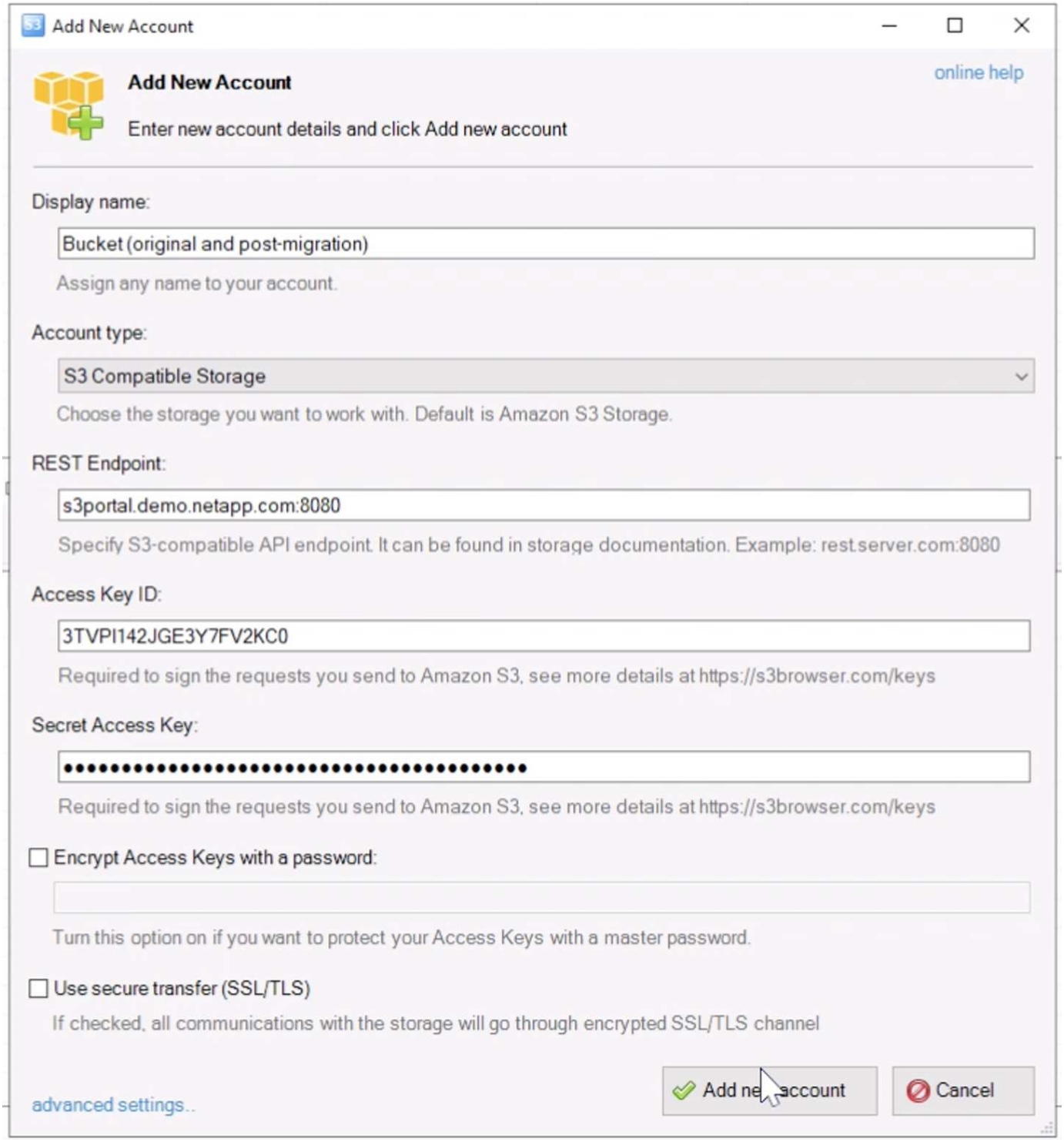
ONTAP S3에서 **StorageGRID**로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 **S3**를 지원합니다

ONTAP S3에서 StorageGRID로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 S3를 지원합니다

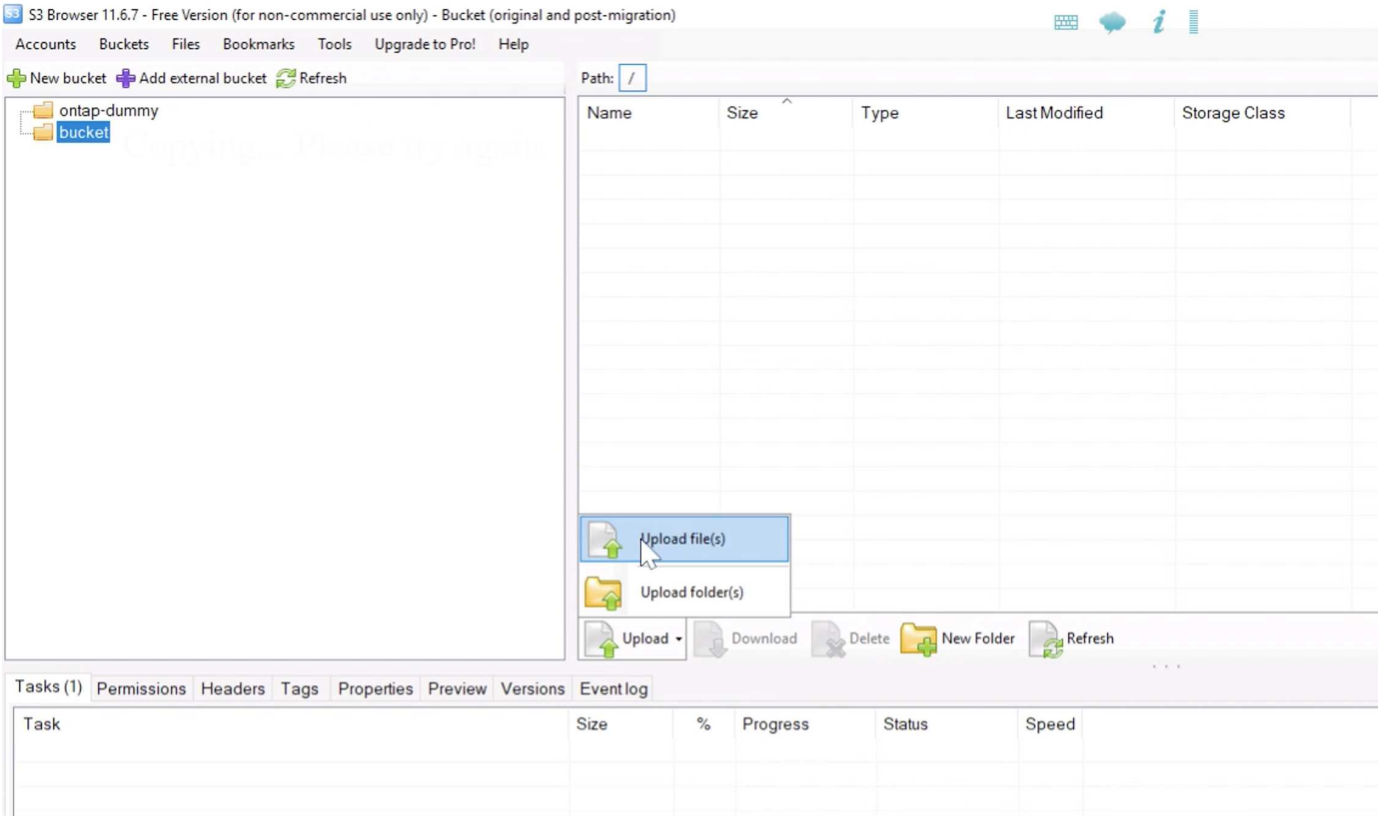
소스 버킷을 채웁니다

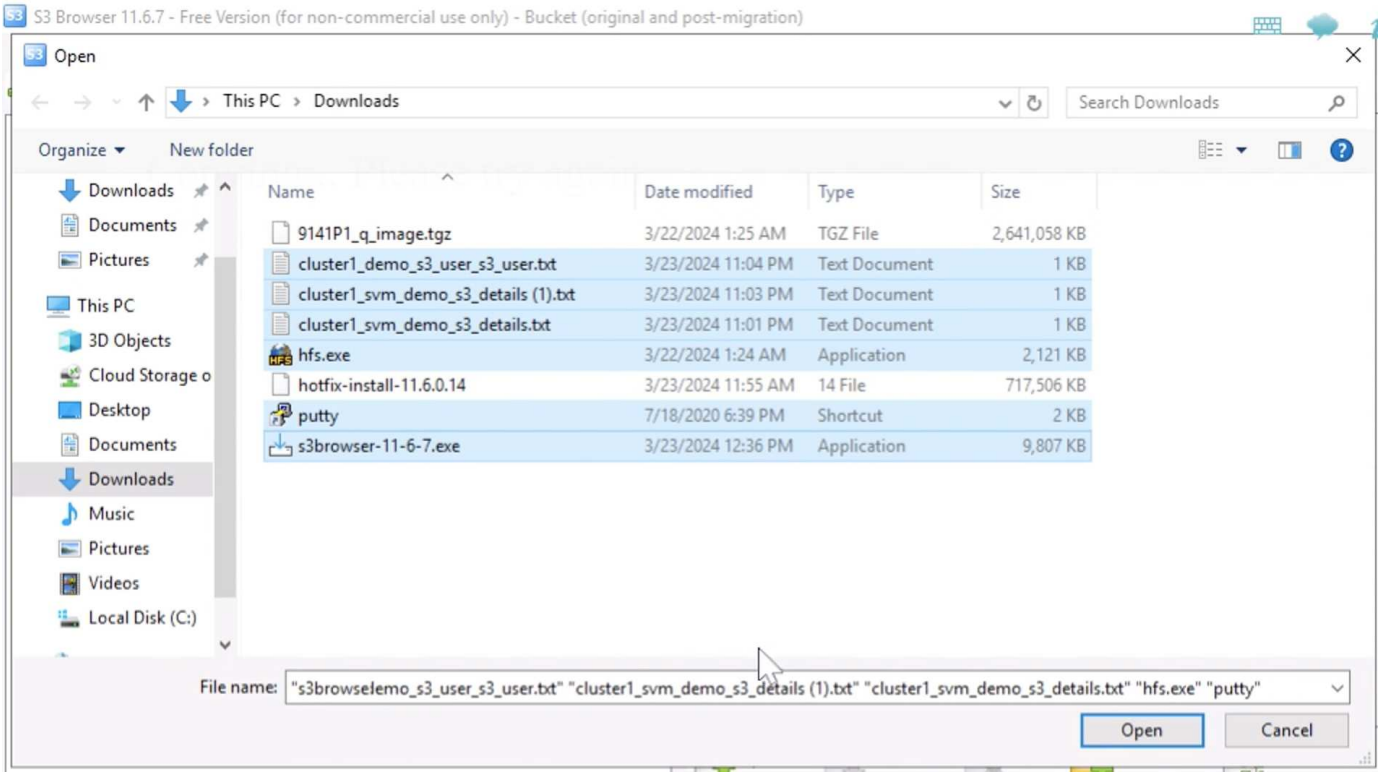
소스 ONTAP 버킷에 일부 오브젝트를 배치하도록 한다. 이 데모에서는 S3Browser를 사용할 예정이지만 편안한 도구를 사용할 수 있습니다.

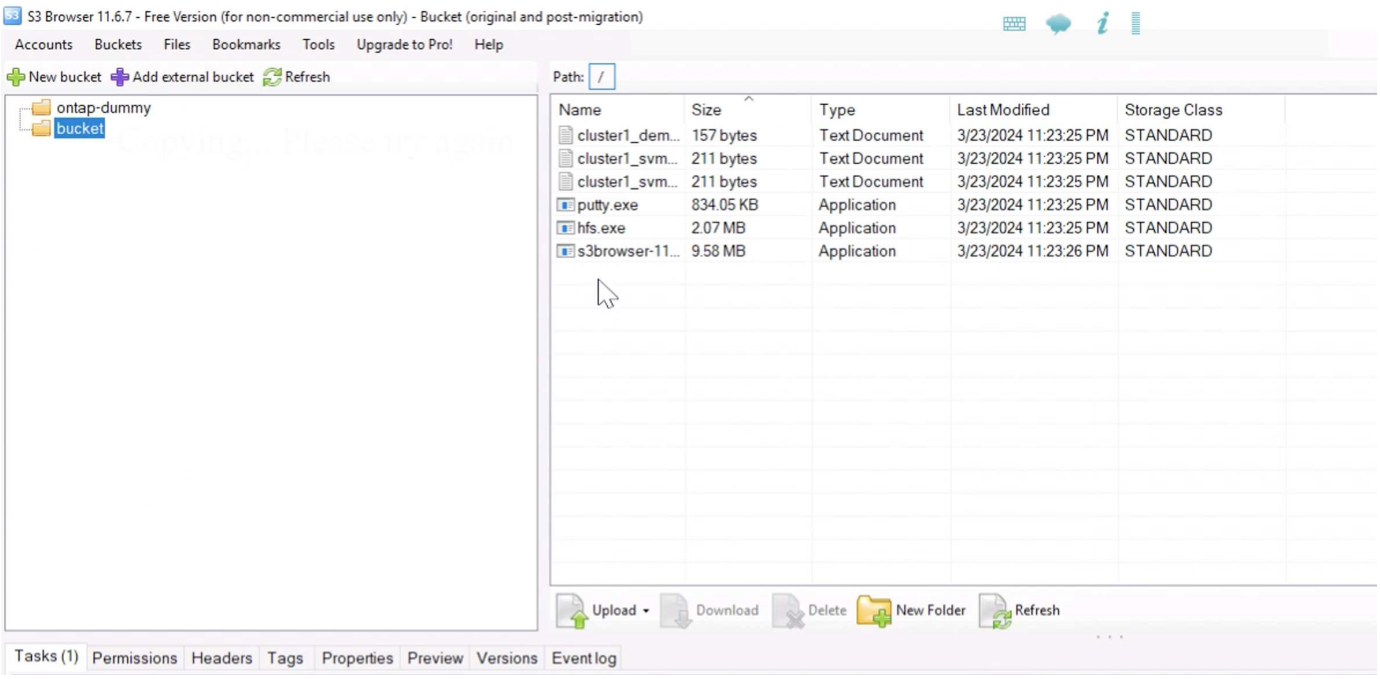
위에서 생성한 ONTAP 사용자 S3 키를 사용하여 S3Browser를 ONTAP 시스템에 연결하도록 구성합니다.



이제 일부 파일을 버전 관리가 활성화된 버킷에 업로드할 수 있습니다.

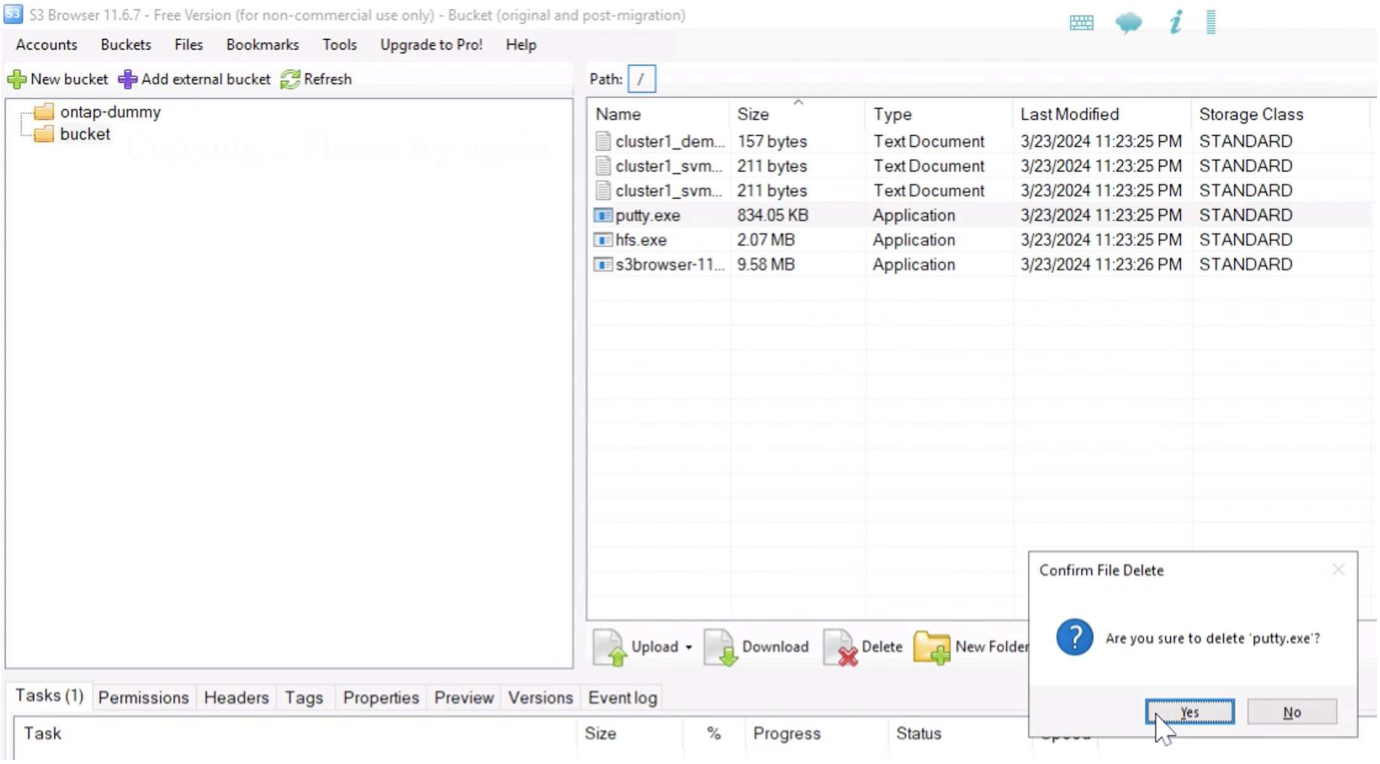

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)
Upload
Download
Delete
New Folder
Refresh
Tasks (1)
Permissions
Headers
Tags
Properties
Preview
Versions
Event log
Task
Size
%
Progress
Status
Speed


S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Open
This PC
Downloads
Search Downloads
Organize
New folder
Downloads
Documents
Pictures
This PC
3D Objects
Cloud Storage o
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
9141P1_q_image.tgz
3/22/2024 1:25 AM
TGZ File
2,641,058 KB
cluster1_demo_s3_user_s3_user.txt
3/23/2024 11:04 PM
Text Document
1 KB
cluster1_svm_demo_s3_details (1).txt
3/23/2024 11:03 PM
Text Document
1 KB
cluster1_svm_demo_s3_details.txt
3/23/2024 11:01 PM
Text Document
1 KB
hfs.exe
3/22/2024 1:24 AM
Application
2,121 KB
hotfix-install-11.6.0.14
3/23/2024 11:55 AM
14 File
717,506 KB
putty
7/18/2020 6:39 PM
Shortcut
2 KB
s3browser-11-6-7.exe
3/23/2024 12:36 PM
Application
9,807 KB
File name:
"s3browselemo_s3_user_s3_user.txt" "cluster1_svm_demo_s3_details (1).txt" "cluster1_svm_demo_s3_details.txt" "hfs.exe" "putty"
Open
Cancel

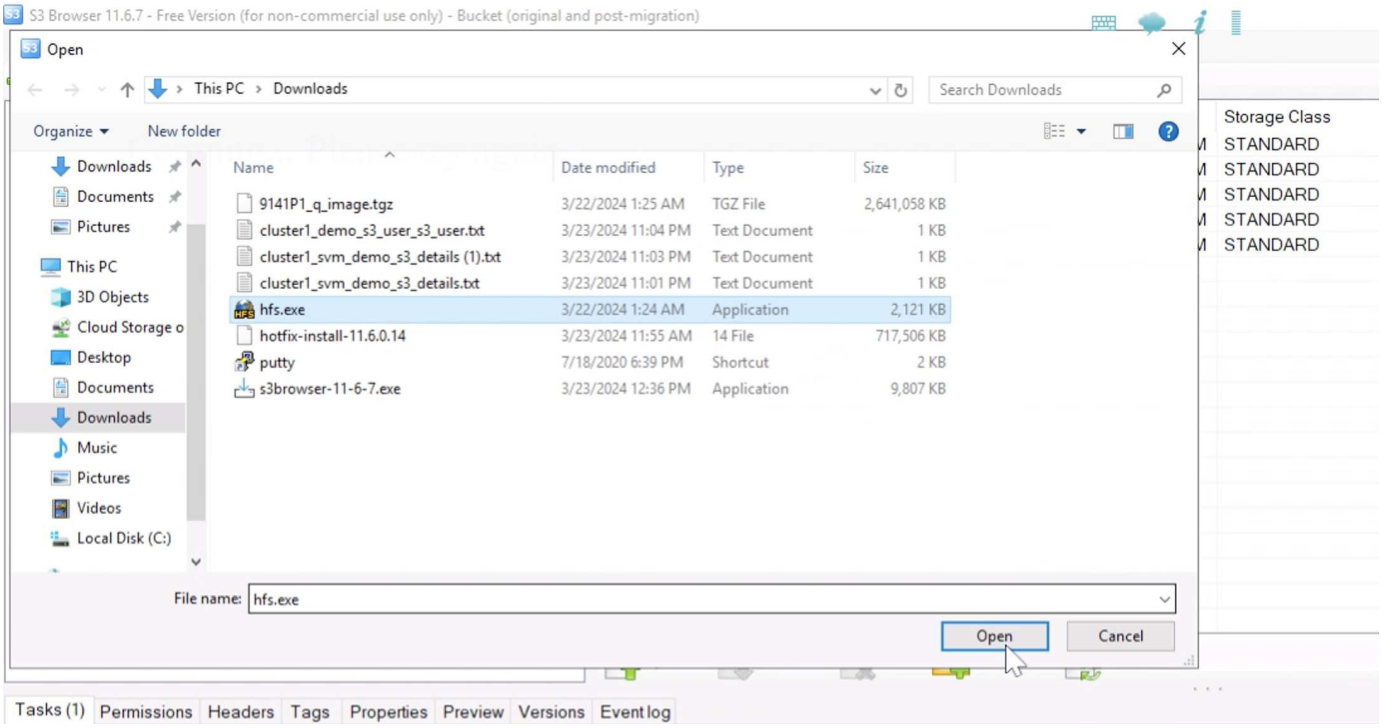


이제 버킷에 몇 가지 오브젝트 버전을 만들어 보겠습니다.

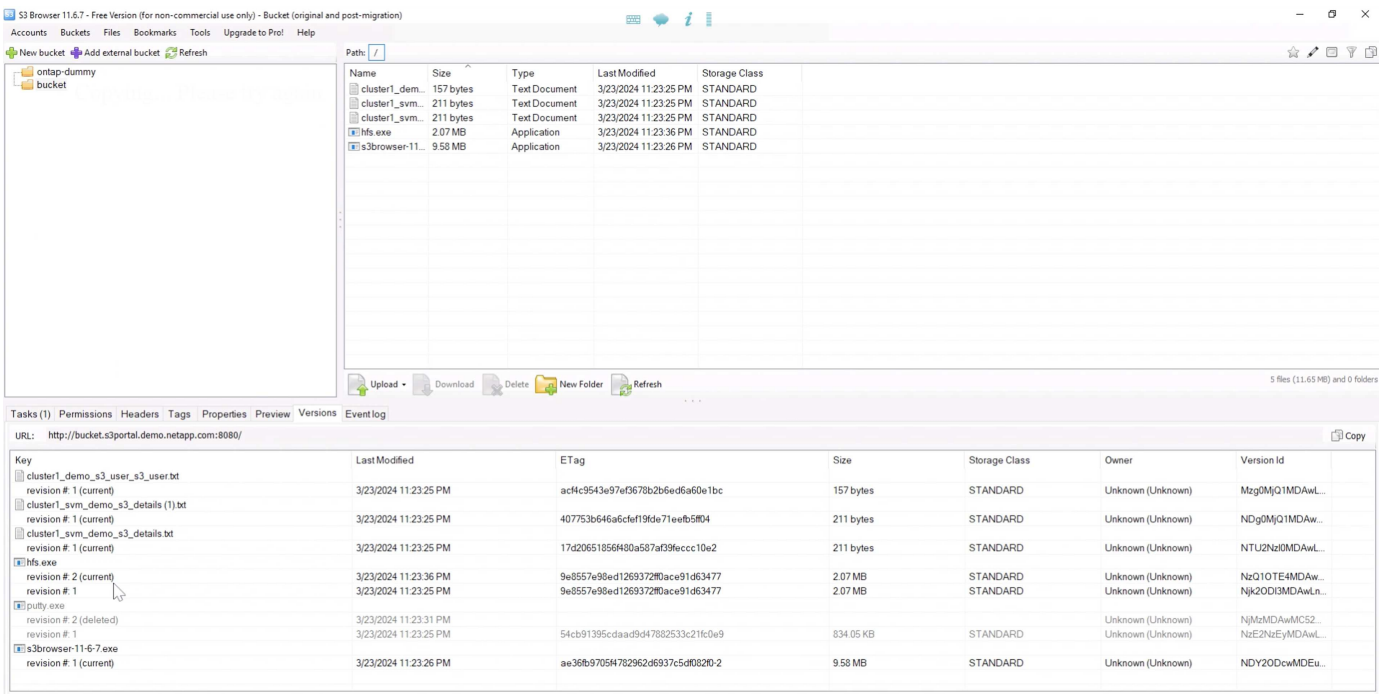
파일을 삭제합니다.



버킷에 이미 있는 파일을 업로드하여 파일 자체를 복사하고 새 버전을 만듭니다.



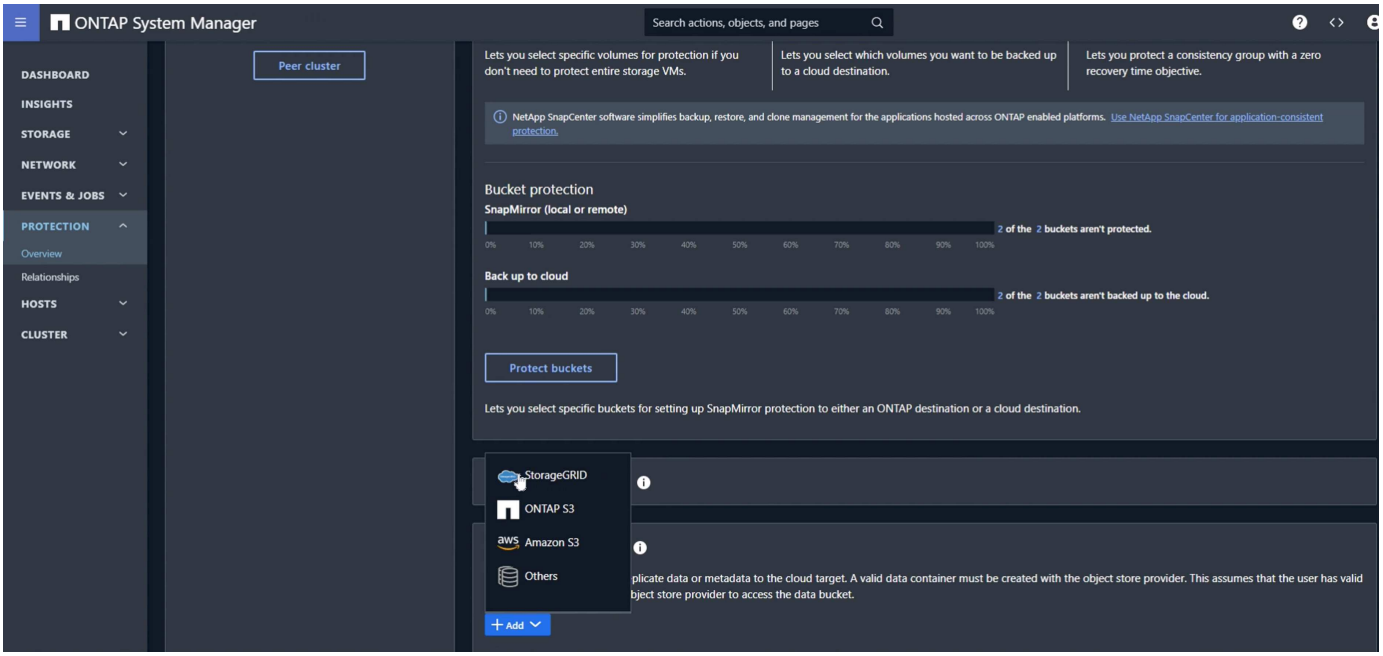
S3Browser에서는 방금 만든 개체의 버전을 볼 수 있습니다.



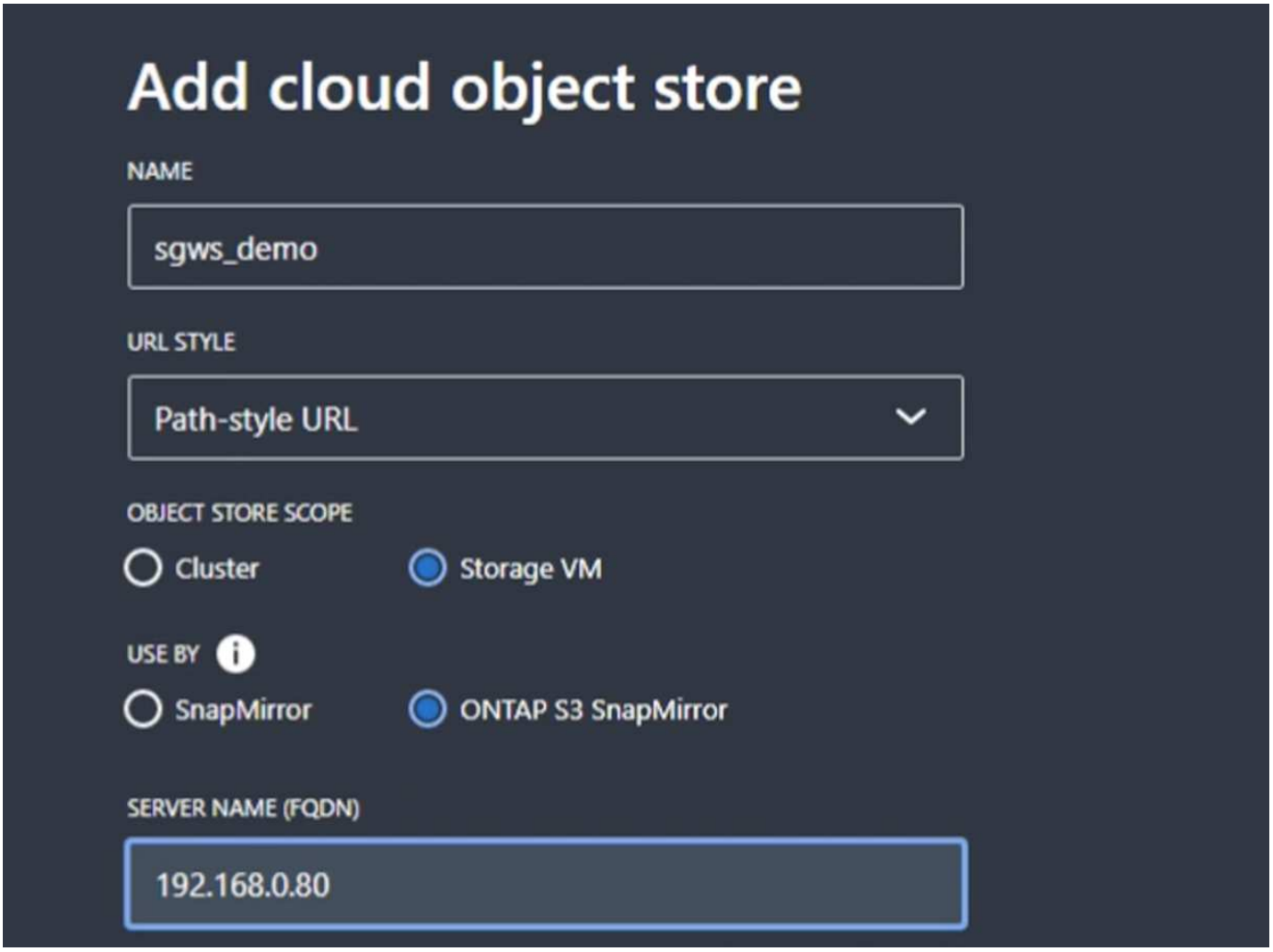
복제 관계를 설정합니다

ONTAP에서 StorageGRID로 데이터 전송을 시작합니다.

ONTAP 시스템 관리자에서 "보호/개요"로 이동합니다. 아래로 스크롤하여 "클라우드 개체 저장소"를 찾은 다음 "추가" 버튼을 클릭하고 "StorageGRID"를 선택합니다.



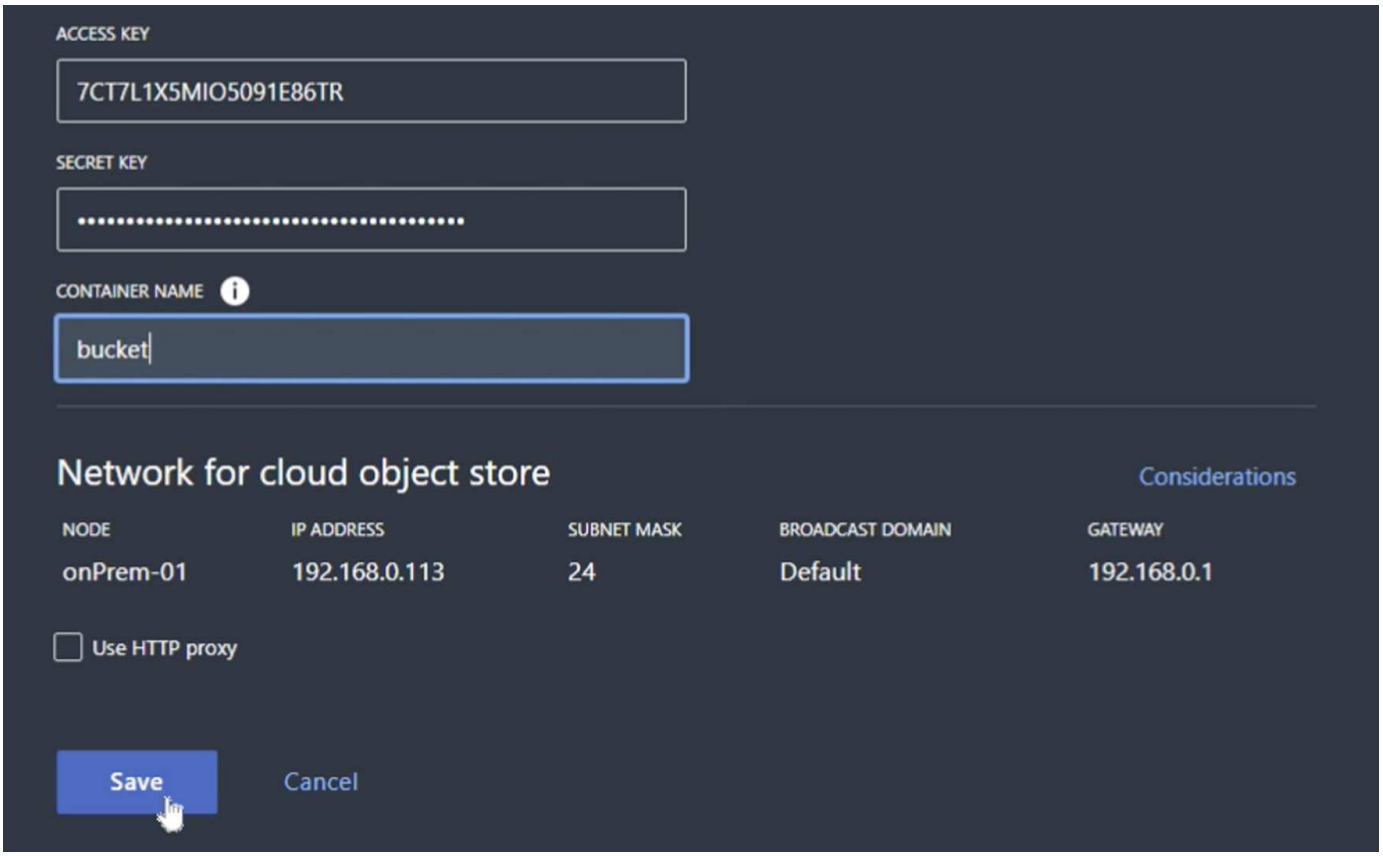
이름, URL 스타일을 제공하여 StorageGRID 정보를 입력합니다(이 데모에서는 Path-styl URL 사용). 객체 저장소 범위를 "스토리지 VM"으로 설정합니다.



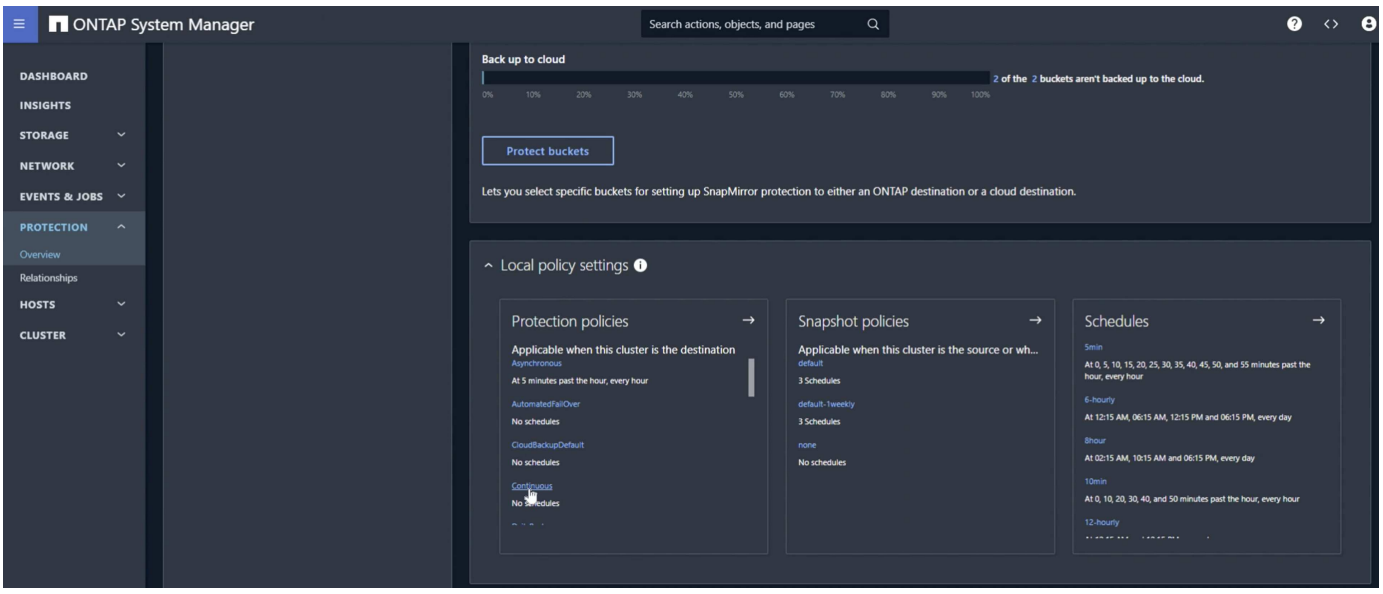
SSL을 사용하는 경우 부하 분산 엔드포인트 포트를 설정하고 여기에 StorageGRID 엔드포인트 인증서를 복사합니다.

그렇지 않으면 SSL 상자의 선택을 취소하고 여기에 HTTP 엔드포인트 포트를 입력합니다.

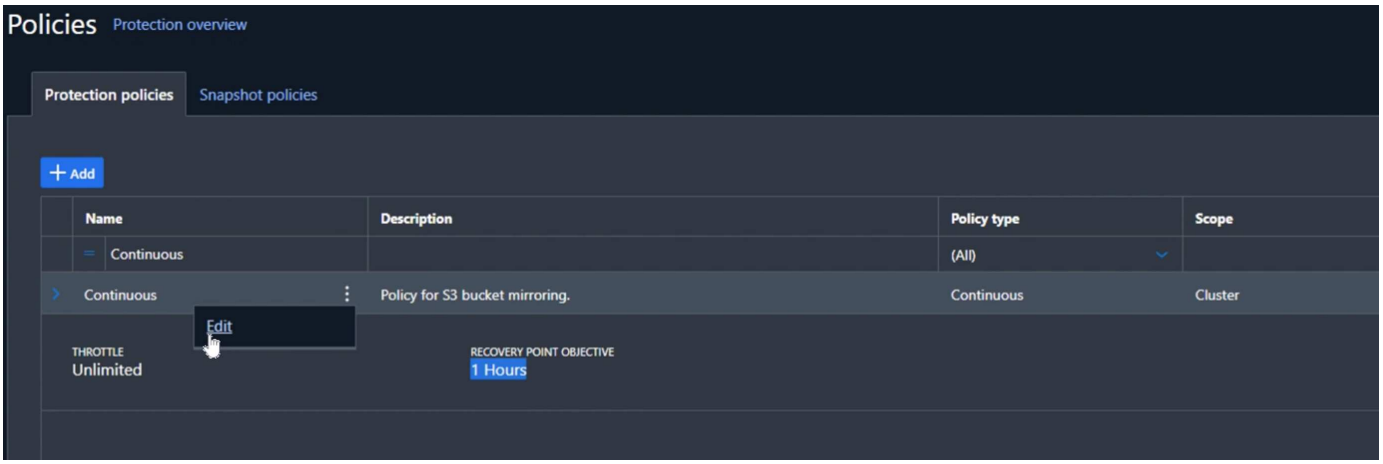
위의 StorageGRID 구성에서 대상에 대해 StorageGRID 사용자 S3 키 및 버킷 이름을 입력합니다.



이제 대상 대상이 구성되었으므로 대상에 대한 정책 설정을 구성할 수 있습니다. "로컬 정책 설정"을 확장하고 "연속"을 선택합니다.



연속 정책을 편집하고 "복구 시점 목표"를 "1시간"에서 "3초"로 변경합니다.

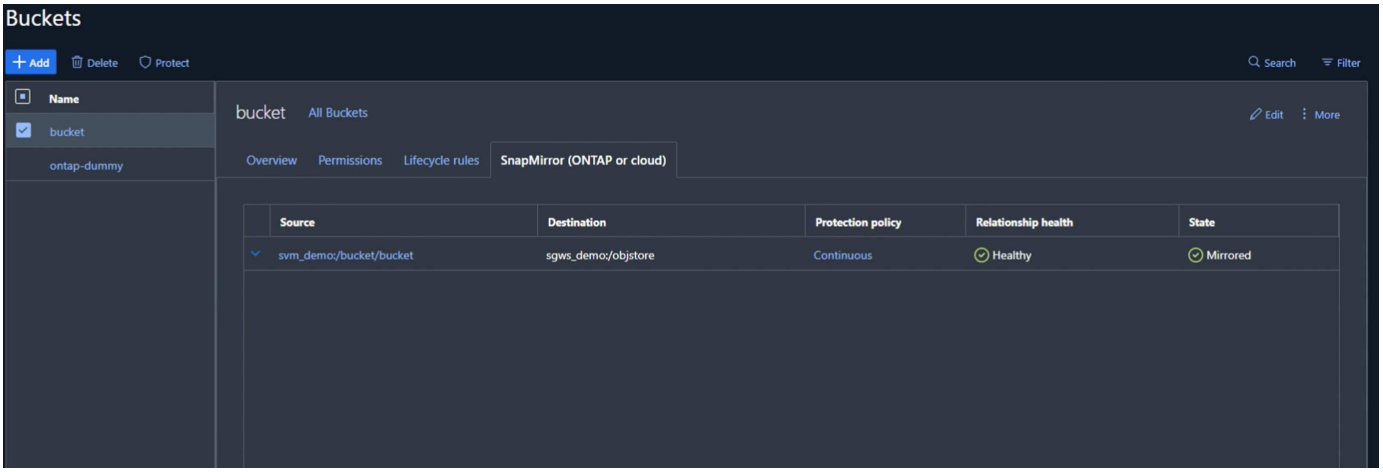


이제 버킷을 복제하도록 SnapMirror를 구성할 수 있습니다.

```
SnapMirror create-source-path sv_demo:/bucket/bucket-destination-path sgws_demo:/objstore-policy Continuous
```

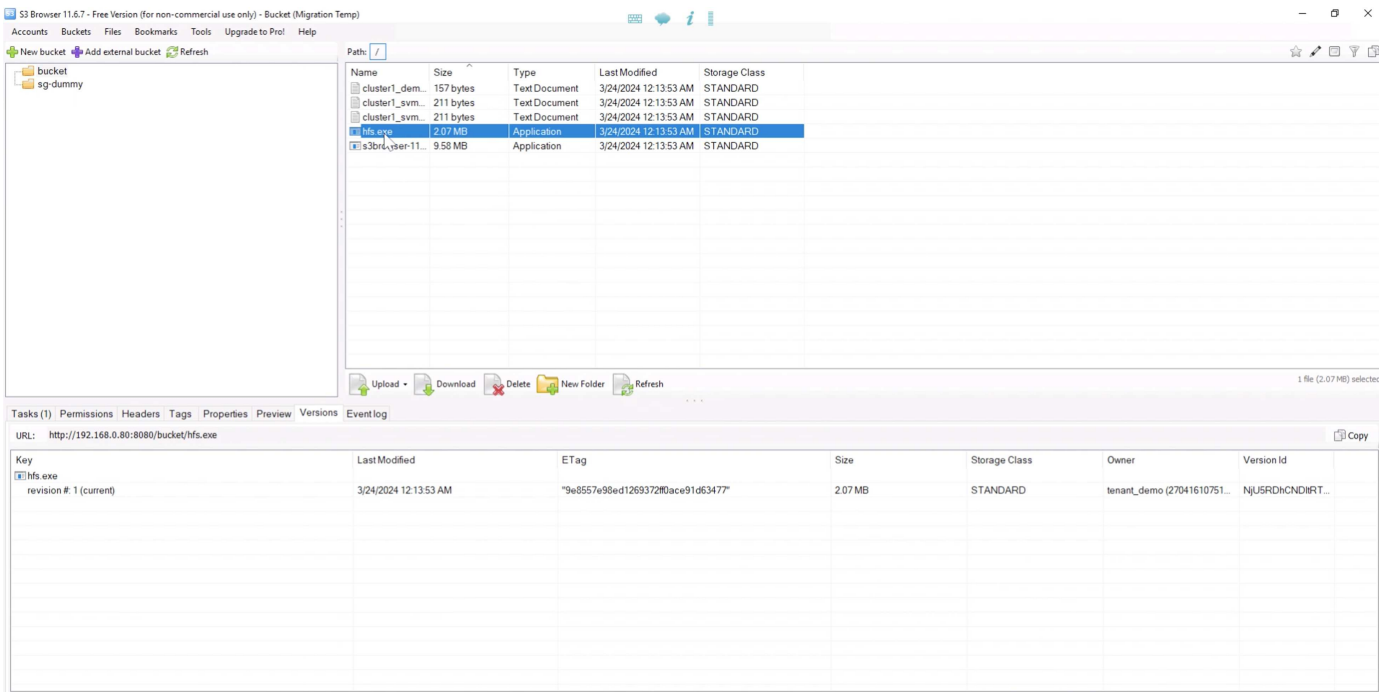
이제 버킷이 보호 중인 버킷 목록에 클라우드 기호를 표시합니다.

버킷을 선택하고 "SnapMirror (ONTAP 또는 Cloud)" 탭으로 이동하면 SnapMirror Repaitionship 상태가 표시됩니다.

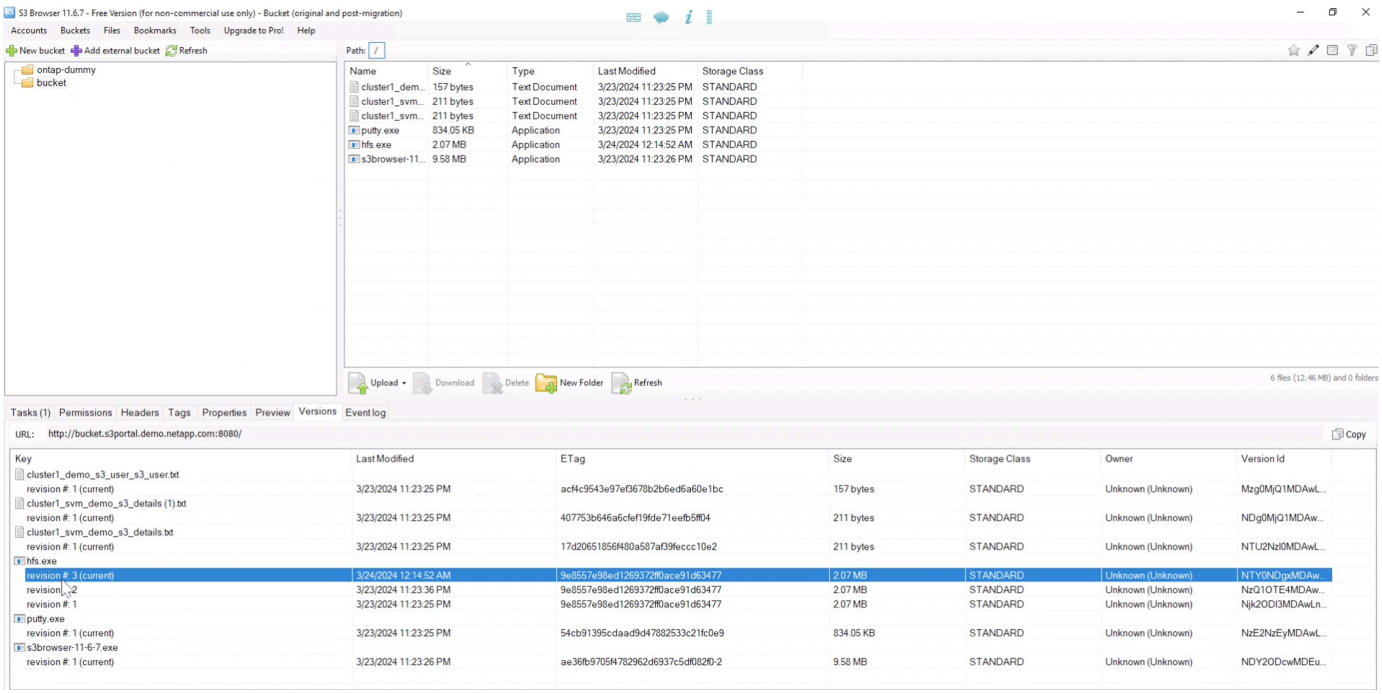


복제 세부 정보입니다

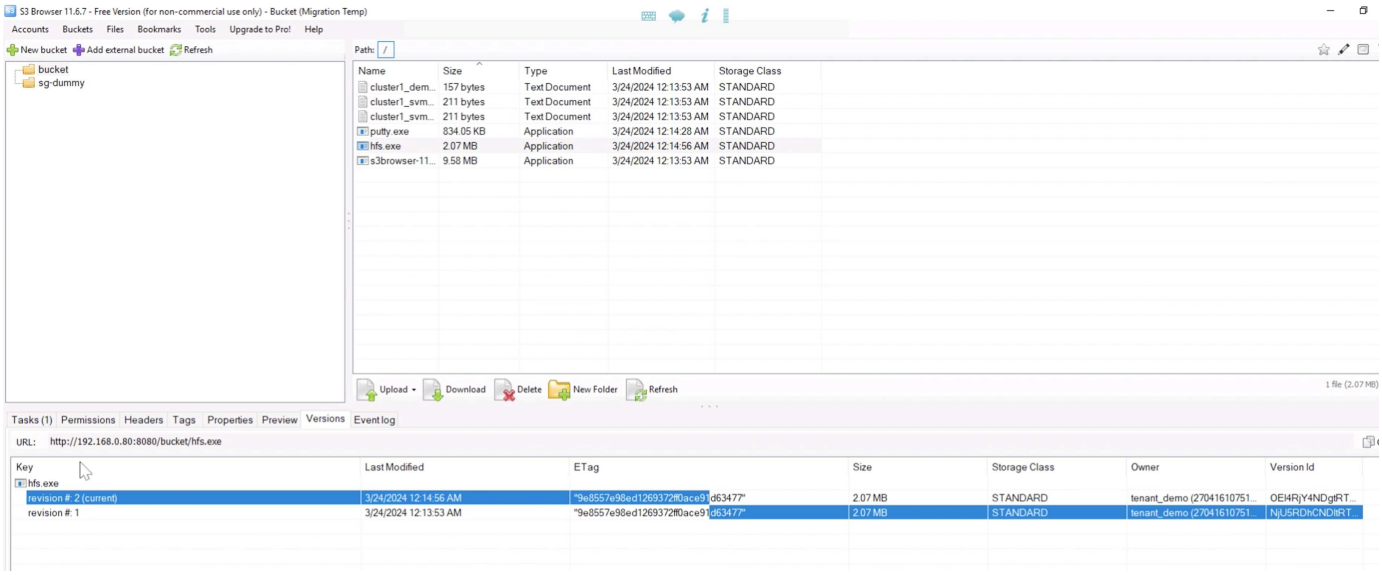
이제 ONTAP에서 StorageGRID로 성공적으로 복제 버킷이 생겼습니다. 그렇다면 실제로 복제되는 것은 무엇일까요? 우리의 소스와 대상은 모두 버전이 지정된 버킷입니다. 이전 버전도 대상으로 복제됩니까? S3Browser로 StorageGRID 버킷을 보면 기존 버전이 복제되지 않았고 삭제된 객체가 존재하지 않으며 해당 객체에 대한 삭제 마커도 없는 것을 알 수 있습니다. 복제된 오브젝트는 StorageGRID 버킷에 1개의 버전만 있습니다.



ONTAP 버킷에서 이전에 사용한 것과 동일한 오브젝트에 새 버전을 추가하고 복제 방법을 보자.



StorageGRID 측면을 보면, 이 버킷에도 새 버전이 생성되었지만 SnapMirror 관계 이전 버전에서 초기 버전이 누락되어 있는 것을 알 수 있습니다.



이는 ONTAP SnapMirror S3 프로세스가 개체의 현재 버전만 복제하기 때문입니다. 그래서 StorageGRID 측에 버전 버킷을 만들어 목적지로 만들었습니다. 이렇게 하면 StorageGRID에서 개체의 버전 기록을 유지할 수 있습니다.

라파엘 게데스, 아론 클라인

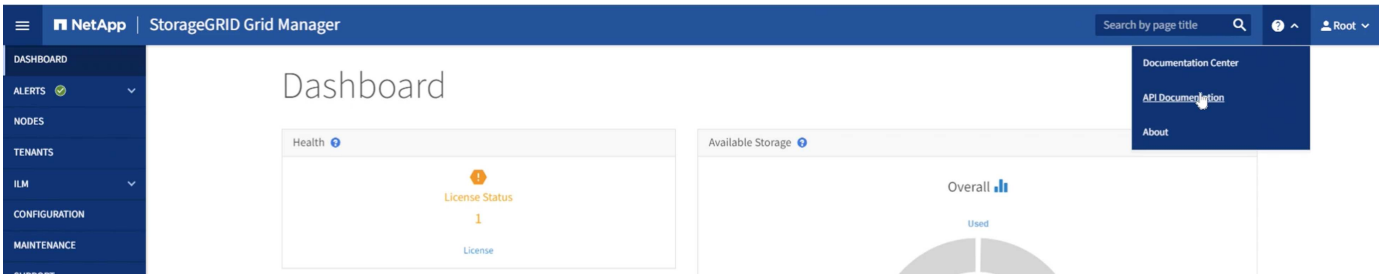
ONTAP S3에서 **StorageGRID**로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 **S3**를 지원합니다

ONTAP S3에서 StorageGRID로 오브젝트 기반 스토리지를 원활하게 마이그레이션하여 엔터프라이즈급 S3를 지원합니다

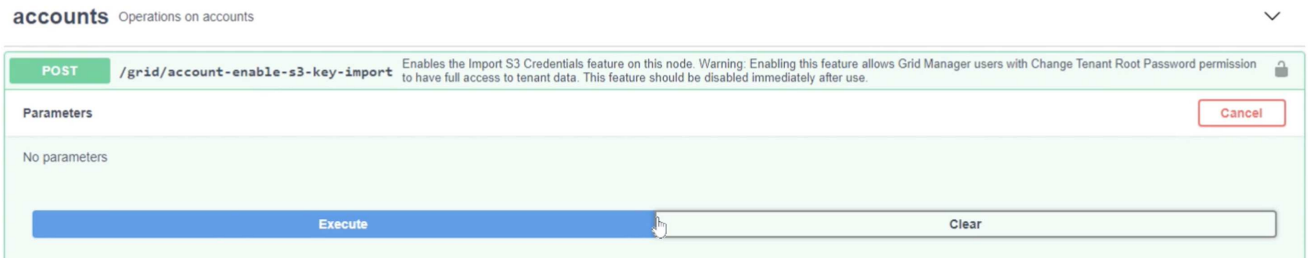
S3 키를 마이그레이션합니다

마이그레이션의 경우 대부분의 경우 대상 측에서 새 자격 증명을 생성하지 않고 사용자의 자격 증명을 마이그레이션합니다. StorageGRID는 사용자에게 S3 키를 가져올 수 있도록 API를 제공합니다.

테넌트 관리자 UI가 아닌 StorageGRID 관리 UI에 로그인하면 API 문서 swagger 페이지가 열립니다.

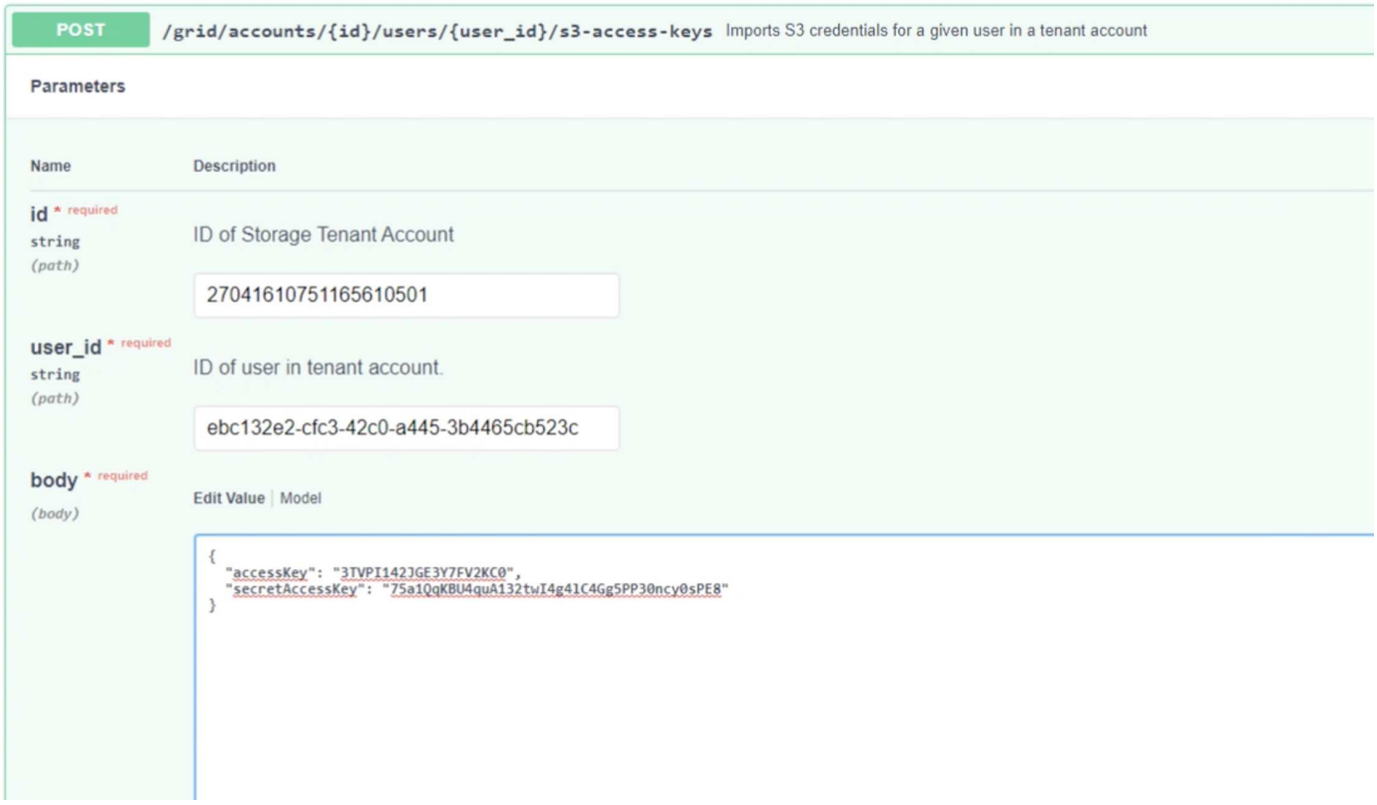


"accounts" 섹션을 확장하고 "POST/grid/account-enable-s3-key-import"를 선택한 후 "try it out" 버튼을 클릭한 다음 실행 버튼을 클릭합니다.

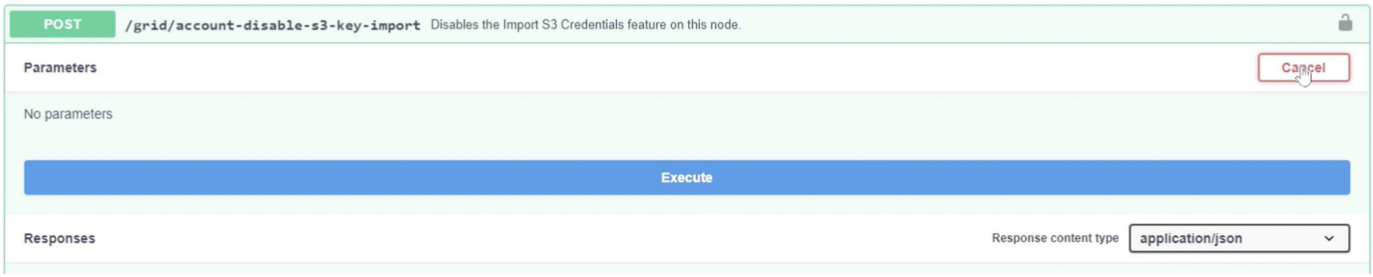


이제 "accounts" 아래에서 아래로 스크롤하여 "POST/grid/accounts/{id}/users/{user_id}/s3-access-keys"로 이동합니다.

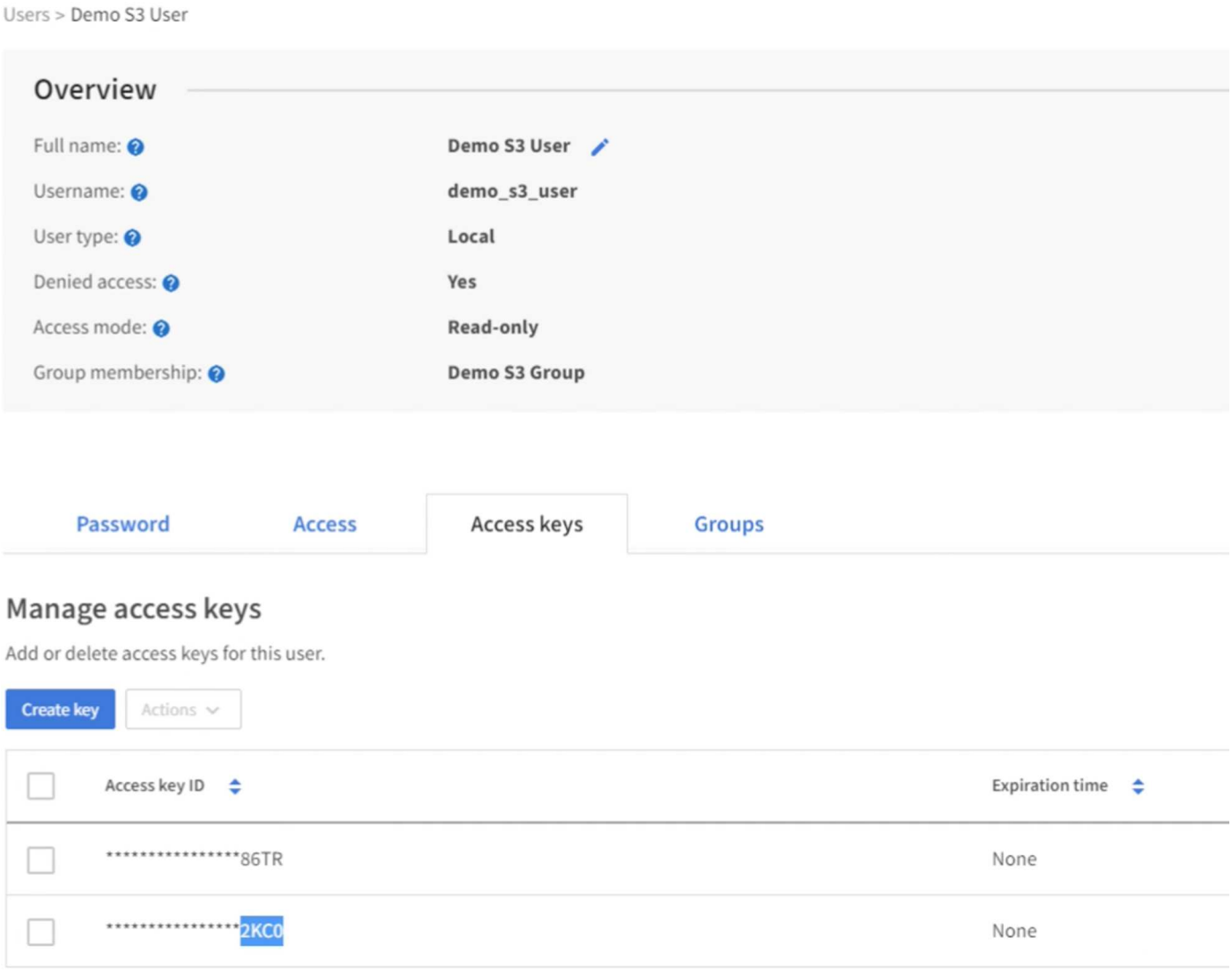
여기서 이전에 수집한 테넌트 ID와 사용자 계정 ID를 입력합니다. json 상자에 ONTAP 사용자의 필드와 키를 입력합니다. 키의 만료를 설정하거나 ","Expires":123456789"를 제거하고 실행을 클릭합니다.



모든 사용자 키 가져오기를 완료하면 "accounts" "POST/grid/account-disable-s3-key-import"에서 키 가져오기 기능을 비활성화해야 합니다.



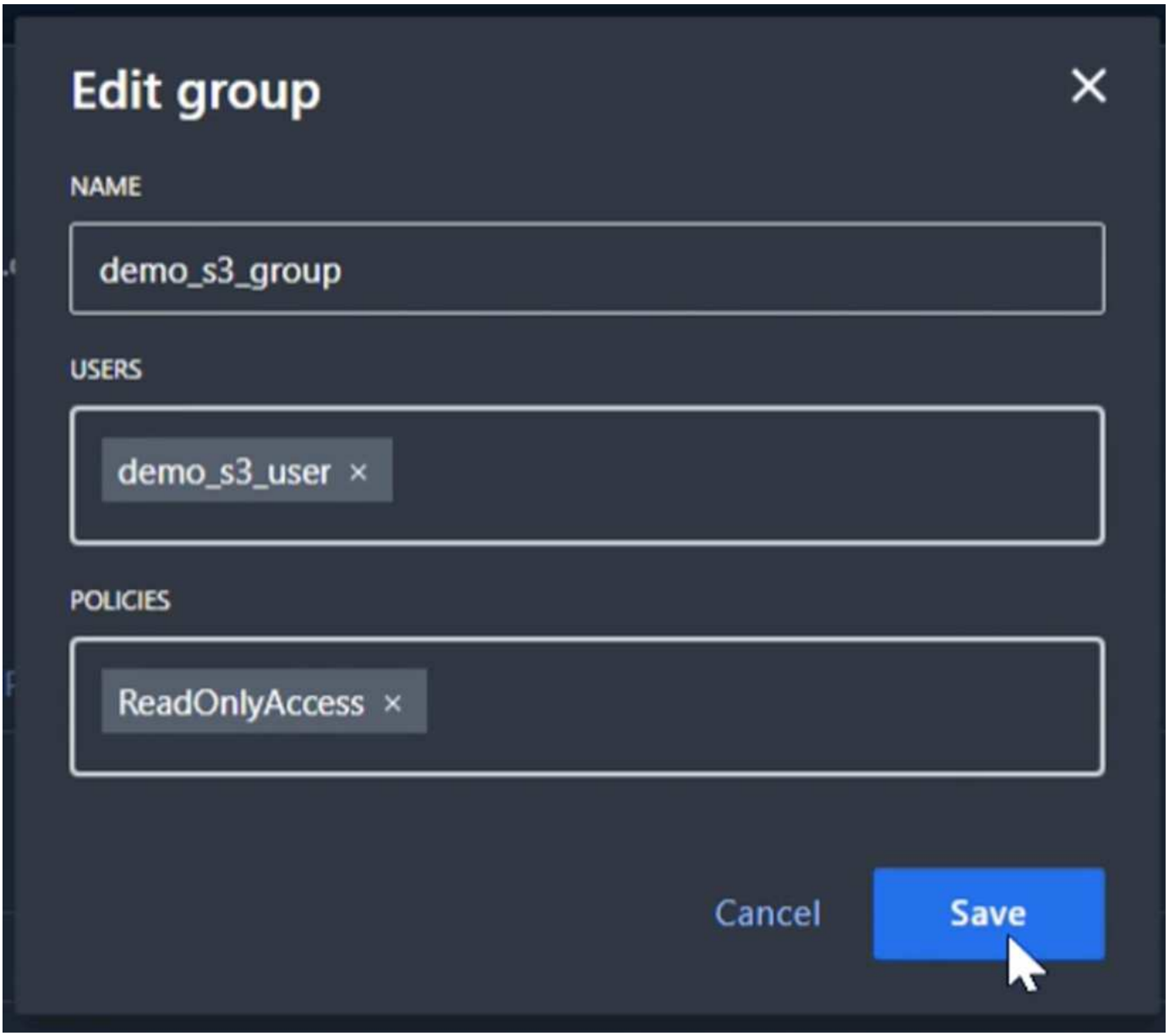
테넌트 관리자 UI에서 사용자 계정을 보면 새 키가 추가된 것을 볼 수 있습니다.



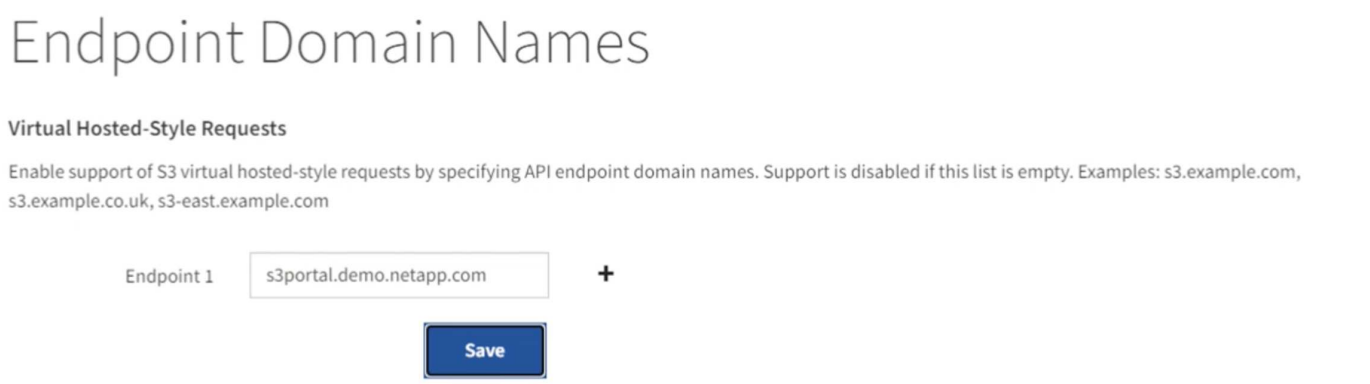
마지막 컷오버입니다

ONTAP에서 StorageGRID로 영구 복제하는 버킷이 의도라면 여기서 끝낼 수 있습니다. ONTAP S3에서 StorageGRID로 마이그레이션하는 경우에는 데이터를 중단하고 컷오버할 때입니다.

ONTAP 시스템 관리자 내에서 S3 그룹을 편집하고 "ReadOnlyAccess"로 설정합니다. 이렇게 하면 사용자가 더 이상 ONTAP S3 버킷에 쓰지 못하게 됩니다.



이제 ONTAP 클러스터에서 StorageGRID 엔드포인트를 가리키도록 DNS를 구성하면 됩니다. 끝점 인증서가 올바른지 확인하고 가상 호스팅 스타일 요청이 필요한 경우 StorageGRID에 끝점 도메인 이름을 추가합니다



클라이언트가 TTL이 만료될 때까지 기다리거나 DNS를 플러시하여 새 시스템으로 확인하면 모든 것이 제대로 작동하는지 테스트할 수 있습니다. 가져온 키가 아니라 StorageGRID 데이터 액세스를 테스트하는 데 사용한 초기 임시 S3 키를 정리하고, SnapMirror 관계를 제거하고, ONTAP 데이터를 제거하기만 하면 됩니다.

라파엘 게데스, 아론 클라인

툴 및 애플리케이션 가이드

StorageGRID와 함께 Cloudera Hadoop S3A 커넥터를 사용하십시오

안젤라 청 _ 에 의해

Hadoop은 한동안 데이터 과학자들이 선호하는 분야입니다. Hadoop을 사용하면 간단한 프로그래밍 프레임워크를 사용하여 컴퓨터 클러스터 전반에 걸쳐 대규모 데이터 세트를 분산 처리할 수 있습니다. Hadoop은 단일 서버에서 수천 개의 시스템으로 스케일업할 수 있도록 설계되었으며, 각 시스템은 로컬 컴퓨팅과 스토리지를 소유합니다.

Hadoop 워크플로우에 S3A를 사용하는 이유는 무엇입니까?

시간이 지나면서 데이터 양이 증가함에 따라 자체 컴퓨팅 및 스토리지로 새 시스템을 추가하는 방식이 비효율적으로 되었습니다. 선형적으로 확장하면 리소스를 효율적으로 사용하고 인프라를 관리하는 데 어려움이 발생합니다.

이러한 과제를 해결하기 위해 Hadoop S3A 클라이언트는 S3 오브젝트 스토리지에 대한 고성능 I/O를 제공합니다. S3A를 사용하여 Hadoop 워크플로우를 구축하면 오브젝트 스토리지를 데이터 저장소로 활용할 수 있으며, 컴퓨팅과 스토리지를 독립적으로 확장할 수 있는 분리된 컴퓨팅 및 스토리지를 사용할 수 있습니다. 또한 컴퓨팅과 스토리지를 분리하여 컴퓨팅 작업에 적절한 양의 리소스를 할당하고 데이터 세트 크기에 따라 용량을 제공할 수 있습니다. 따라서 Hadoop 워크플로우의 전체 TCO를 줄일 수 있습니다.

StorageGRID를 사용하도록 S3A 커넥터를 구성합니다

필수 구성 요소

- StorageGRID S3 엔드포인트 URL, 테넌트 S3 액세스 키 및 Hadoop S3A 연결 테스트를 위한 암호 키입니다.
- Java 패키지를 설치하기 위해 클러스터의 각 호스트에 대한 Cloudera 클러스터 및 루트 또는 sudo 권한입니다.

2022년 4월 현재, Cloudera 7.1.7을 사용한 Java 11.0.14는 StorageGRID 11.5 및 11.6을 대상으로 테스트를 마쳤습니다. 그러나 Java 버전 번호는 새로 설치할 때 다를 수 있습니다.

Java 패키지를 설치합니다

1. 를 확인하십시오 "Cloudera 지원 매트릭스" 지원되는 JDK 버전.
2. 를 다운로드합니다 "Java 11.x 패키지" 이 운영 체제는 Cloudera 클러스터 운영 체제와 일치합니다. 이 패키지를 클러스터의 각 호스트에 복사합니다. 이 예에서는 CentOS에 rpm 패키지가 사용됩니다.
3. 각 호스트에 루트로 로그인하거나 sudo 권한이 있는 계정을 사용합니다. 각 호스트에서 다음 단계를 수행합니다.
   a. 패키지 설치:

```
$ sudo rpm -Uvh jdk-11.0.14_linux-x64_bin.rpm
```

   b. Java가 설치된 위치를 확인합니다. 여러 버전이 설치된 경우 새로 설치된 버전을 기본값으로 설정합니다.

```
alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 +1           /usr/java/jre1.8.0_291-amd64/bin/java
  2           /usr/java/jdk-11.0.14/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

c. 이 줄을 '/etc/profile' 끝에 추가합니다. 경로는 위의 선택 경로와 일치해야 합니다.

```
export JAVA_HOME=/usr/java/jdk-11.0.14
```

d. 프로파일을 적용하려면 다음 명령을 실행합니다.

```
source /etc/profile
```

Cloudera HDFS S3A 구성

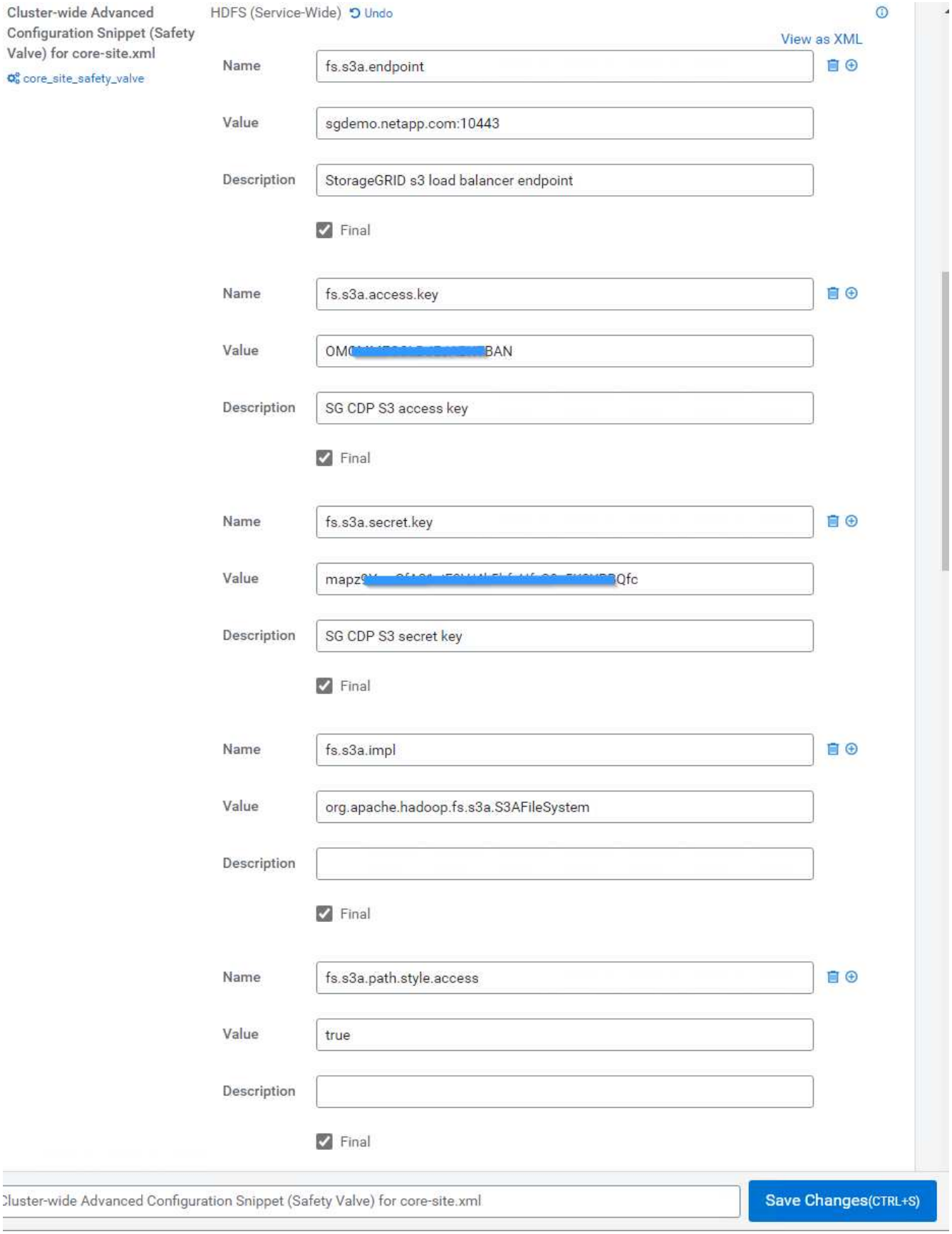
- 단계 *

1. Cloudera Manager GUI에서 클러스터 > HDFS를 선택하고 Configuration을 선택합니다.
2. 범주 아래에서 고급을 선택하고 아래로 스크롤하여 core-site.xml에 대한 클러스터 차원의 고급 구성 조각(안전 밸브)을 찾습니다.
3. (+) 기호를 클릭하고 다음 값 쌍을 추가합니다.

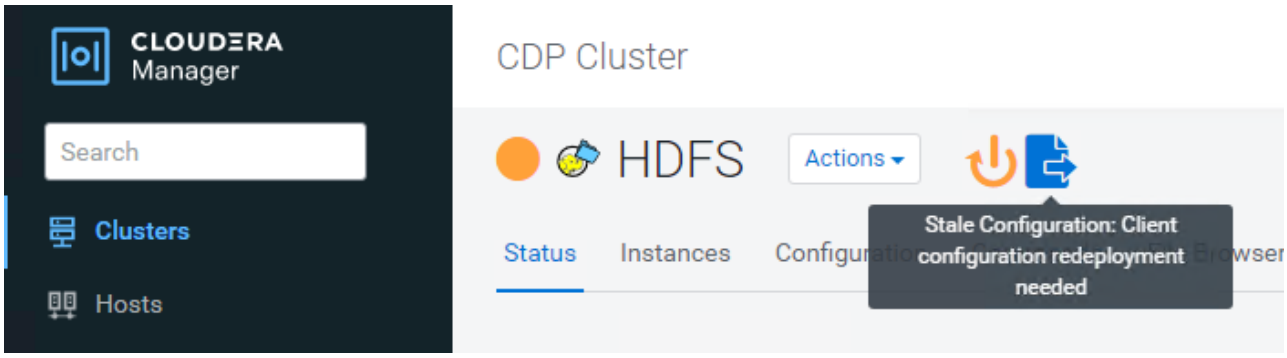
이름	값
fs.s3a.access.key	_<StorageGRID의 테넌트 S3 액세스 키> _
fs.s3a.secret.key	_<StorageGRID의 테넌트 S3 비밀 키> _
FS.s3a.CONNECTION.SSL.ENABLED	[true 또는 false] (이 항목이 누락된 경우 기본값은 https)
FS.s3a.endpoint	_<StorageGRID S3 엔드포인트: port> _
FS.s3a.IMPL	org.apache.하둡.fs.s3a.s3aFileSystem

이름	값
FS.s3a.path.style.access	[TRUE 또는 FALSE](이 항목이 누락된 경우 기본값은 가상 호스트 스타일)

- 샘플 스크린샷 *



1. 변경 내용 저장 단추를 클릭합니다. HDFS 메뉴 표시줄에서 오래된 구성 아이콘을 선택하고 다음 페이지에서 오래된 서비스 다시 시작 을 선택한 다음 지금 다시 시작 을 선택합니다.



StorageGRID에 대한 S3A 연결을 테스트합니다

기본 연결 테스트를 수행합니다

Cloudera 클러스터의 호스트 중 하나에 로그인하고 'Hadoop fs-ls s3a://*<bucket-name>*/'를 입력합니다.

다음 예에서는 경로 syle을 기존 HDFS 테스트 버킷과 테스트 객체와 함께 사용합니다.

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:24:37 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:24:37 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
Found 1 items
-rw-rw-rw-   1 root root       1679 2022-02-14 16:03 s3a://hdfs-test/test
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
```

문제 해결

시나리오 **1**

StorageGRID에 대한 HTTPS 연결을 사용하고 15분 시간 제한 후 "shake_failure" 오류가 발생합니다.

- 이유: * StorageGRID 연결을 위해 오래되었거나 지원되지 않는 TLS 암호 제품군을 사용하는 이전 JRE/JDK 버전.
- 샘플 오류 메시지 *

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:52:34 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:52:35 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/02/15 19:04:51 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
ls: doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
```

- 해상도: * JDK 11.x 이상이 설치되어 있는지 확인하고 Java 라이브러리를 기본값으로 설정합니다. 을 참조하십시오 Java 패키지를 설치합니다 섹션을 참조하십시오.

시나리오 **2:**

"요청한 대상에 대한 유효한 인증 경로를 찾을 수 없습니다."라는 오류 메시지와 함께 StorageGRID에 연결하지 못했습니다.

- 이유: * StorageGRID S3 엔드포인트 서버 인증서가 Java 프로그램에서 신뢰되지 않습니다.

샘플 오류 메시지:

```
[root@hdp6 ~]# hadoop fs -ls s3a://hdfs-test/
22/03/11 20:58:12 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/03/11 20:58:13 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/03/11 21:12:25 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target: Unable to execute HTTP
request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

- 해결 방법: * 알려진 공개 인증서 서명 기관에서 발급한 서버 인증서를 사용하여 인증이 보안되는지 확인하는 것이 좋습니다. 또는 사용자 지정 CA 또는 서버 인증서를 Java 신뢰 저장소에 추가합니다.

StorageGRID 사용자 지정 CA 또는 서버 인증서를 Java 신뢰 저장소에 추가하려면 다음 단계를 수행하십시오.

1. 기존 기본 Java cacerts 파일을 백업합니다.

```
cp -ap $JAVA_HOME/lib/security/cacerts
$JAVA_HOME/lib/security/cacerts.orig
```

2. StorageGRID S3 끝점 인증서를 Java 신뢰 저장소로 가져옵니다.

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts
-storepass changeit -noprompt -alias sg-lb -file <StorageGRID CA or
server cert in pem format>
```

문제 해결 팁

1. 디버깅하려면 Hadoop 로그 수준을 높입니다.

   export hadoop_root_logger=hadoop.root.logger=debug, console

2. 명령을 실행하고 로그 메시지를 error.log로 전달합니다.

   'Hadoop fs-ls s3a://<*bucket-name*>/&> error.log'

안젤라 청 _ 에 의해

S3cmd를 사용하여 StorageGRID에서 S3 액세스를 테스트하고 시연합니다

_ 아론 클라인 _

S3cmd 는 S3 작업을 위한 무료 명령줄 도구 및 클라이언트입니다. s3cmd를 사용하여 StorageGRID에서 S3 액세스를 테스트하고 시연할 수 있습니다.

S3cmd를 설치하고 구성합니다

워크스테이션이나 서버에 S3cmd를 설치하려면 에서 다운로드합니다 "명령줄 S3 클라이언트". s3cmd 는 문제 해결을 지원하기 위한 도구로 각 StorageGRID 노드에 미리 설치되어 있습니다.

초기 구성 단계

1. s3cmd — 구성
2. access_key와 secret_key만 제공하십시오. 나머지는 기본값을 유지합니다.
3. 제공된 자격 증명으로 액세스를 테스트하시겠습니까? [Y/n]:n(실패하므로 테스트 생략)
4. 설정을 저장하시겠습니까? [y/N]y입니다
   a. 구성이 '/root/.s3cfg'에 저장되었습니다.
5. s3cfg에서 "=" 기호 다음에 host_base 및 host_bucket 필드가 비어 있도록 합니다.
   a. host_base=
   b. host_bucket=

4단계에서 host_base 및 host_bucket을 지정하는 경우 CLI에서 -host를 사용하여 엔드포인트를 지정할 필요가 없습니다. 예:

```
host_base = 192.168.1.91:8082
host_bucket = bucketX.192.168.1.91:8082
s3cmd ls s3://bucketX --no-check-certificate
```

기본 명령 예

- * 버킷 생성: *

  S 3cmd MB S3://s3cmdbucket — host=<endpoint>:<port> — no-check-certificate

- * 모든 버킷 나열: *

  S 3cmd ls — host=<endpoint>:<port> — no-check-certificate

- * 모든 버킷과 해당 내용을 나열합니다. *

  S 3cmd la—host=<endpoint>:<port>--no-check-certificate

- * 특정 버킷의 오브젝트 목록: *

  's3cmd ls s3://<bucket>--host=<endpoint>:<port>--no-check-certificate'

- * 버킷 삭제: *

  S 3cmd rb s3://s3cmdbucket — host=<endpoint>:<port> — no-check-certificate

- * 개체 넣기: *

  S 3cmd put <file>S3:/<bucket>--host=<endpoint>:<port>--no-check-certificate

- * 개체 가져오기: *

  's3cmd get s3://<bucket>/<object><file>--host=<endpoint>:<port>--no-check-certificate'

- * 개체 삭제: *

  S 3cmd del S3://<bucket>/<object>--host=<endpoint>:<port>--no-check-certificate

NetApp StorageGRID를 공동 스토리지로 사용하는 Vertica Eon 모드 데이터베이스

안젤라 청 _ 에 의해

이 가이드에서는 NetApp StorageGRID에서 공용 스토리지를 사용하는 Vertica Eon Mode 데이터베이스를 생성하는 절차를 설명합니다.

소개

Vertica는 분석 데이터베이스 관리 소프트웨어입니다. 대량의 데이터를 처리하도록 설계된 columnar 스토리지 플랫폼으로서, 기존의 집약적인 시나리오에서 매우 빠른 쿼리 성능을 지원합니다. Vertica 데이터베이스는 Eon 또는 Enterprise의 두 가지 모드 중 하나로 실행됩니다. 두 모드를 모두 사내 또는 클라우드에 구축할 수 있습니다.

EON 및 엔터프라이즈 모드는 주로 데이터를 저장하는 위치에 따라 다릅니다.

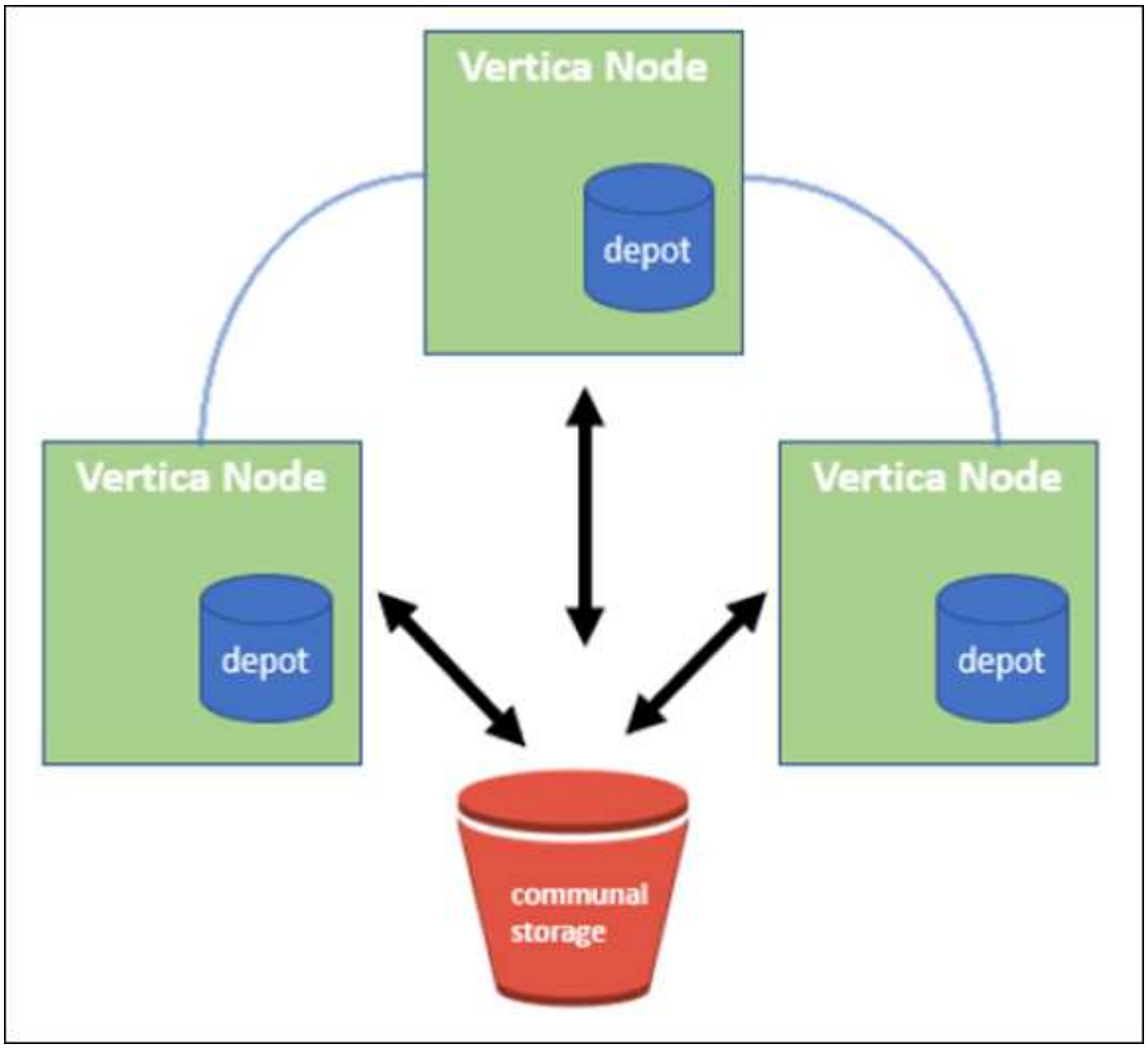
- eon Mode 데이터베이스는 공용 스토리지를 사용하여 데이터를 저장합니다. 이 방법은 Vertica에서 권장합니다.

- 엔터프라이즈 모드 데이터베이스는 데이터베이스를 구성하는 노드의 파일 시스템에 로컬로 데이터를 저장합니다.

EON 모드 아키텍처

eon Mode는 컴퓨팅 리소스를 데이터베이스의 공용 스토리지 계층과 분리하여 컴퓨팅과 스토리지를 별도로 확장할 수 있도록 합니다. Eon Mode의 Vertica는 다양한 워크로드를 처리하고 별도의 컴퓨팅 및 스토리지 리소스를 사용하여 서로 격리하도록 최적화되어 있습니다.

eon Mode는 사내 또는 Amazon S3에 호스팅된 공유 오브젝트 저장소인 S3 버킷에 데이터를 저장합니다.



공용 저장 장치

Eon Mode는 데이터를 로컬에 저장하는 대신 모든 데이터와 카탈로그(메타데이터)에 단일 공동 스토리지 위치를 사용합니다. 공용 스토리지는 데이터베이스 노드 간에 공유되는 데이터베이스의 중앙 집중식 저장소 위치입니다.

공용 스토리지의 속성은 다음과 같습니다.

- 클라우드 또는 온프레미스 오브젝트 스토리지의 공용 스토리지는 개별 시스템의 디스크 스토리지에 비해 스토리지 장애로 인해 데이터 손실이 발생할 가능성이 더 적고 복구 성능이 더 낮습니다.
- 모든 데이터는 동일한 경로를 사용하여 모든 노드에서 읽을 수 있습니다.

- 용량은 노드의 디스크 공간에 의해 제한되지 않습니다.
- 데이터는 적소에 저장되므로 변화하는 요구사항에 따라 클러스터를 탄력적으로 확장할 수 있습니다. 데이터가 노드에 로컬로 저장된 경우 노드를 추가하거나 제거하려면 노드 간에 상당한 양의 데이터를 이동해야 하며, 제거할 노드나 새로 생성된 노드로 이동해야 합니다.

물류창고입니다

공용 스토리지의 한 가지 단점은 속도이다. 공유 클라우드 위치에서 데이터에 액세스하는 것은 로컬 디스크에서 데이터를 읽는 것보다 속도가 느립니다. 또한 많은 노드에서 데이터를 한 번에 읽는 경우에는 공용 스토리지에 대한 연결이 병목 현상을 일으킬 수 있습니다. 데이터 액세스 속도를 높이기 위해 Eon Mode 데이터베이스의 노드는 데이터 센터라는 데이터의 로컬 디스크 캐시를 유지합니다. 쿼리를 실행할 때 노드는 먼저 필요한 데이터가 서비스 센터에 있는지 확인합니다. 이 경우 데이터의 로컬 복사본을 사용하여 쿼리를 완료합니다. 데이터가 서비스 센터에 없는 경우 노드는 공용 스토리지에서 데이터를 가져와 서비스 센터에 복사본을 저장합니다.

NetApp StorageGRID 권장 사항

Vertica는 데이터베이스 데이터를 오브젝트 스토리지에 수천 또는 수백만 개의 압축된 오브젝트(관찰 크기는 오브젝트당 200~500MB임)로 저장합니다. 사용자가 데이터베이스 쿼리를 실행하면 Vertica는 바이트 범위 가져오기 호출을 사용하여 이러한 압축된 개체에서 선택한 데이터 범위를 병렬로 검색합니다. 각 바이트 범위 GET는 약 8KB입니다.

10TB 데이터베이스 서비스 센터에서 사용자 쿼리 테스트를 수행하는 동안 초당 4,000 - 10,000개의 GET(바이트 범위 가져오기) 요청이 그리드에 전송되었습니다. SG6060 어플라이언스를 사용하여 이 테스트를 실행할 때 어플라이언스 노드당 CPU % 활용도가 낮지만(약 20% ~ 30%) CPU 시간의 2/3 이상이 I/O를 기다리고 있습니다 SGF6024에서는 I/O 대기가 0% ~ 0.5%로 매우 적습니다.

지연 시간이 매우 짧은 소규모 IOPS의 높은 수요(평균 0.01초 미만)로 인해 오브젝트 스토리지 서비스에 SFG6024를 사용하는 것이 좋습니다. SG6060이 매우 큰 데이터베이스 크기에 필요한 경우 고객은 적극적으로 쿼리한 데이터 세트를 지원하기 위해 서비스 센터 사이징에 대해 Vertica 계정 팀과 협력해야 합니다.

Admin Node 및 API Gateway Node의 경우 고객은 SG100 또는 SG1000을 사용할 수 있습니다. 병렬 및 데이터베이스 크기의 사용자 쿼리 요청 수에 따라 선택이 달라집니다. 고객이 타사 로드 밸런싱 장치를 사용하려는 경우, 성능 수요가 높은 워크로드를 위한 전용 로드 밸런싱 장치를 사용하는 것이 좋습니다. StorageGRID 사이징의 경우 NetApp 세일즈 팀에 문의하십시오.

기타 StorageGRID 구성 권장 사항은 다음과 같습니다.

- * 그리드 토폴로지 *. SGF6024를 동일한 그리드 사이트에서 다른 스토리지 어플라이언스 모델과 혼합하지 마십시오. 장기간 아카이브 보호를 위해 SG6060을 사용하려는 경우 성능을 향상시키기 위해 활성 데이터베이스의 전용 그리드 로드 밸런서가 있는 SGF6024를 자체 그리드 사이트(물리적 또는 논리적 사이트)에 보관하십시오. 여러 가지 어플라이언스 모델을 동일한 사이트에서 혼합하여 사이트에서의 전반적인 성능을 줄일 수 있습니다.
- * 데이터 보호 *. 보호를 위해 복제 복사본을 사용합니다. 활성 데이터베이스에 대해 삭제 코딩을 사용하지 마십시오. 고객은 비활성 데이터베이스를 장기간 보호하기 위해 삭제 코딩을 사용할 수 있습니다.
- * 그리드 압축 사용 안 함 *. Vertica 개체 저장소에 저장하기 전에 개체를 압축합니다. 그리드 압축을 사용하면 스토리지 사용량이 추가로 절감되지 않고 바이트 범위 가져오기 성능이 크게 저하됩니다.
- * HTTP 대 HTTPS S3 엔드포인트 연결 *. 벤치마크 테스트 중에 Vertica 클러스터에서 StorageGRID 로드 밸런서 엔드포인트로 HTTP S3 연결을 사용할 경우 성능이 약 5% 향상되는 것을 확인했습니다. 이 선택은 고객의 보안 요구 사항을 기반으로 해야 합니다.

Vertica 구성을 위한 권장 사항은 다음과 같습니다.

- * Vertica 데이터베이스 기본 서비스 센터 설정은 읽기 및 쓰기 작업에 대해 활성화(값 = 1)됩니다 *. 성능 향상을

위해 이러한 서비스 센터 설정을 유지할 것을 적극 권장합니다.

- * 스트리밍 제한 비활성화 *. 구성에 대한 자세한 내용은 섹션을 참조하십시오 스트리밍 제한 비활성화.

StorageGRID에서 공용 스토리지를 사용하는 온프레미스 Eon 모드 설치

다음 섹션에서는 StorageGRID에서 공용 스토리지를 사용하여 Eon 모드를 사내에 설치하는 절차에 대해 설명합니다. 사내 S3(Simple Storage Service) 호환 오브젝트 스토리지를 구성하는 절차는 Vertica 가이드의 절차와 유사합니다. "Eon 모드 데이터베이스를 온-프레미스에 설치합니다".

기능 테스트에 사용된 설정은 다음과 같습니다.

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- Vertica 노드용 CentOS 7.x OS가 있는 3개의 가상 시스템(VM)이 클러스터를 구성합니다. 이 설정은 기능 테스트 전용이며, Vertica 운영 데이터베이스 클러스터용이 아닙니다.

이 세 노드는 SSH(Secure Shell) 키로 설정되어 클러스터 내의 노드 간에 암호 없이 SSH를 사용할 수 있습니다.

NetApp StorageGRID에 필요한 정보입니다

StorageGRID에서 공용 스토리지를 사용하는 사내에 Eon 모드를 설치하려면 다음 필수 정보가 있어야 합니다.

- StorageGRID S3 엔드포인트의 IP 주소 또는 FQDN(정규화된 도메인 이름) 및 포트 번호입니다. HTTPS를 사용하는 경우 StorageGRID S3 엔드포인트에 구현된 사용자 지정 인증 기관(CA) 또는 자체 서명된 SSL 인증서를 사용합니다.
- 버킷 이름. 미리 존재해야 하며 비어 있어야 합니다.
- 버킷에 대한 읽기 및 쓰기 액세스를 통해 키 ID 및 비밀 액세스 키에 액세스합니다.

S3 엔드 포인트에 액세스하기 위한 권한 부여 파일 생성

S3 끝점에 액세스하기 위한 권한 부여 파일을 생성할 때는 다음과 같은 사전 요구 사항이 적용됩니다.

- Vertica가 설치되어 있습니다.
- 클러스터가 설정, 구성 및 준비되면 데이터베이스를 생성할 수 있습니다.

S3 끝점에 액세스하기 위한 권한 부여 파일을 생성하려면 다음 단계를 수행하십시오.

1. 'admintools'를 실행하여 Eon Mode 데이터베이스를 생성할 Vertica 노드에 로그인합니다.

   기본 사용자는 Vertica 클러스터 설치 중에 생성된 dbadmin입니다.

2. 텍스트 편집기를 사용하여 '/home/dbadmin' 디렉토리 아래에 파일을 만듭니다. 파일 이름은 'sg_auth.conf'와 같이 원하는 모든 것이 될 수 있습니다.
3. S3 엔드포인트가 표준 HTTP 포트 80 또는 HTTPS 포트 443을 사용하는 경우 포트 번호를 건너뜁니다. HTTPS를 사용하려면 다음 값을 설정합니다.

   - "awsenablehttps=1"을 선택하지 않으면 값을 "0"으로 설정합니다.
   - ``awauth=<S3 access key ID>:<secret access key>'

◦ ``awsendpoint=<StorageGRID S3 endpoint>:<port>'

StorageGRID S3 엔드포인트 HTTPS 연결에 사용자 지정 CA 또는 자체 서명된 SSL 인증서를 사용하려면 인증서의 전체 파일 경로와 파일 이름을 지정합니다. 이 파일은 각 Vertica 노드의 동일한 위치에 있어야 하며 모든 사용자에 대한 읽기 권한이 있어야 합니다. StorageGRID S3 엔드포인트 SSL 인증서가 공개적으로 알려진 CA에 의해 서명된 경우 이 단계를 건너뜁니다.

``awscfile=<filepath/filename>'

예를 들어, 다음 샘플 파일을 참조하십시오.

```
awsauth = MNVU4OYFAY2xyz123:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wANabcxyz
awsendpoint = s3.england.connectlab.io:10443
awsenablehttps = 1
awscafile = /etc/custom-cert/grid.pem
```

+

운영 환경에서 고객은 공개적으로 알려진 CA가 서명한 서버 인증서를 StorageGRID S3 로드 밸런서 끝점에 구현해야 합니다.

모든 **Vertica** 노드에서 서비스 센터 경로를 선택합니다

서비스 센터 스토리지 경로에 대해 각 노드에서 디렉토리를 선택하거나 생성합니다. 서비스 센터 스토리지 경로 매개 변수에 대해 제공한 디렉토리는 다음과 같아야 합니다.

- 클러스터의 모든 노드에서 동일한 경로(예: '/home/dbadmin/depot')
- dbadmin 사용자가 읽고 쓸 수 있습니다
- 충분한 보관

  기본적으로 Vertica는 depot 스토리지에 대한 디렉토리를 포함하는 파일 시스템 공간의 60%를 사용합니다. create_db 명령에서 '--depot-size' 인수를 사용하여 서비스 센터 크기를 제한할 수 있습니다. 을 참조하십시오 "Eon 모드 데이터베이스에 대한 Vertica 클러스터 크기 조정" 일반 Vertica 사이징 지침을 참조하거나 Vertica 어카운트 매니저에게 문의하십시오.

  admintools create_db" 도구는 서비스 센터 경로가 없는 경우 해당 경로를 생성하려고 시도합니다.

Eon 온프레미스 데이터베이스 생성

Eon 온프레미스 데이터베이스를 만들려면 다음 단계를 수행하십시오.

1. 데이터베이스를 생성하려면 admintools create_db 툴을 사용합니다.

   다음 목록에서는 이 예제에 사용된 인수에 대해 간략하게 설명합니다. 필수 인수와 선택적 인수에 대한 자세한 설명은 Vertica 문서를 참조하십시오.

   ◦ 에서 생성된 권한 부여 파일의 -x <경로/파일 이름 “S3 끝점에 액세스하기 위한 권한 부여 파일 생성” 를 누릅니다.

인증 세부 정보는 성공적으로 생성된 후 데이터베이스 내에 저장됩니다. 이 파일을 제거하여 S3 비밀 키가 노출되지 않도록 할 수 있습니다.

- 공용 스토리지 위치 <S3://StorageGrid 버켓 이름>
- -s <이 데이터베이스에 사용할 Vertica 노드의 쉼표로 구분된 목록>
- d <생성할 데이터베이스 이름>
- 이 새 데이터베이스에 대해 설정할 -p <암호>. 예를 들어, 다음 샘플 명령을 참조하십시오.

```
admintools -t create_db -x sg_auth.conf --communal-storage
-location=s3://vertica --depot-path=/home/dbadmin/depot --shard
-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'<password>'
```

새 데이터베이스를 생성하는 데는 데이터베이스의 노드 수에 따라 몇 분 정도 소요됩니다. 데이터베이스를 처음 만들 때 사용권 계약에 동의하라는 메시지가 표시됩니다.

예를 들어 다음 샘플 권한 부여 파일 및 'db 생성' 명령을 참조하십시오.

```
[dbadmin@vertica-vm1 ~]$ cat sg_auth.conf
awsauth = MNVU4OYFAY2CPKVXVxxxx:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wAN+xxxx
awsendpoint = s3.england.connectlab.io:10445
awsenablehttps = 1

[dbadmin@vertica-vm1 ~]$ admintools -t create_db -x sg_auth.conf
--communal-storage-location=s3://vertica --depot-path=/home/dbadmin/depot
--shard-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'xxxxxxxx'
Default depot size in use
Distributing changes to cluster.
    Creating database vmart
    Starting bootstrap node v_vmart_node0007 (10.45.74.19)
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (UP)
    Creating database nodes
    Creating node v_vmart_node0008 (host 10.45.74.29)
    Creating node v_vmart_node0009 (host 10.45.74.39)
    Generating new configuration information
    Stopping single node db before adding additional nodes.
```

```
    Database shutdown complete
    Starting all nodes
Start hosts = ['10.45.74.19', '10.45.74.29', '10.45.74.39']
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
        v_vmart_node0008 (10.45.74.29)
        v_vmart_node0009 (10.45.74.39)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (UP) v_vmart_node0008: (UP)
v_vmart_node0009: (UP)
Creating depot locations for 3 nodes
Communal storage detected: rebalancing shards

Waiting for rebalance shards. We will wait for at most 36000 seconds.
Installing AWS package
    Success: package AWS installed
Installing ComplexTypes package
    Success: package ComplexTypes installed
Installing MachineLearning package
    Success: package MachineLearning installed
Installing ParquetExport package
    Success: package ParquetExport installed
Installing VFunctions package
    Success: package VFunctions installed
Installing approximate package
    Success: package approximate installed
Installing flextable package
    Success: package flextable installed
Installing kafka package
    Success: package kafka installed
Installing logsearch package
    Success: package logsearch installed
Installing place package
    Success: package place installed
Installing txtindex package
    Success: package txtindex installed
Installing voltagesecure package
```

```
    Success: package voltagesecure installed
Syncing catalog on vmart with 2000 attempts.
Database creation SQL tasks completed successfully. Database vmart created
successfully.
```

오브젝트 크기(바이트)	버킷/객체 키 전체 경로
61입니다	S3://vertica/051/026d63a9d4a33237bf0e2c2a794a00a000021a07/026d63a9d4a33237bf0e2cf2a794a00a000021a07_0 DFS
145년	S3://vertica/2c4/026d63a9d4a33237bf0e2c2cf2a794a00a000021a3d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a3d_0 DFS
146	S3://vertica/33c/026d63a9d4a33237bf0e2c2cf2a794a00a000021a1d/026d63a9d4a33237bf0e2c2cf2a794a00a000021a1d_0 DFS
40세	S3://vertica/382/026d63a9d4a33237bf0e2c2a794a00a000021a31/026d63a9d4a33237bf0e2c2a794a00a000021a31_0 DFS
145년	S3://vertica/42F/026d63a9d4a33237bf0e2c2a794a00a000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a21_0 DFS
34세	S3://vertica/472/026d63a9d4a33237bf0e2c2cf2a794a00a000021a25/026d63a9d4a33237bf0e2c2cf2a794a00a000021a25_0 DFS
41세	S3://vertica/476/026d63a9d4a33237bf0e2c2cf2a794a00a000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a2d_0 DFS
61입니다	S3://vertica/52A/026d63a9d4a33237bf0e2c2cf2a794a00a000021a5d/026d63a9d4a33237bf0e2c2cf2a794a00a000021a5d_0 DFS
131입니다	S3://vertica/5d2/026d63a9d4a33237bf0e2c2cf2a794a00a000021a19/026d63a9d4a33237bf0e2c2cf2a794a00a000021a19_0 DFS

오브젝트 크기(바이트)	버킷/객체 키 전체 경로
91세	S3://vertica/5f7/026d63a9d4a33237bf0e2c2cf2a794a00a000021a11/026d63a9d4a33237bf0e2c2cf2a794a00a000021a11_0 DFS
118입니다	S3://vertica/82d/026d63a9d4a33237bf0e2c2cf2a794a00a000021a15/026d63a9d4a33237bf0e2cf2a794a00a0000000021a15_0 DFS
115년	S3://vertica/9a2/026d63a9d4a33237bf0e2c2cf2a794a00a000021a61/026d63a9d4a33237bf0e2c2cf2a794a00a000021a61_0 DFS
33세	S 3://vertica/ACD/026d63a9d4a33237bf0e2c2a794a00a000021a29/026d63a9d4a33237bf0e2c2a794a00a000021a29_0 DFS
133입니다	S3://vertica/b98/026d63a9d4a33237bf0e2c2cf2a794a00a000021a4d/026d63a9d4a33237bf0e2c2cf2a794a00a000021a4d_0 DFS
38세	S 3://vertica/DB3/026d63a9d4a33237bf0e2c2cf2a794a00a000021a49/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a49_0 DFS
38세	S3://vertica/EBA/026d63a9d4a33237bf0e2c2a794a00a000021a59/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59_0 DFS
21521920	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000215e2/026d63a33237bf0e2c2cf2a794a00a0000215e2
6865408	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2a794a00a000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a000021602
204217344	S3://vertica/metadata/VMart/Libraries/026d63a9d4a33237bf0e2c2a794a00a000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a000021610
16109056	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2cf2a794a00a0000217e0/026d63a9d4a33237bf0e2c2a794a00a0000217e0

오브젝트 크기(바이트)	버킷/객체 키 전체 경로
12853248	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2cf2a794a00a000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a000021800 tar
8937984	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00002187a/026d63a33237bf0e2c2cf2a794a00a00002187a.
56260608	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2cf2a794a00a0000218b2/026d63a9d4a33237bf0e2c2a794a00a0000218b2
53947904	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000219ba/026d63a33237bf0e2c2cf2a794a00a0000219ba
44932608	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2cf2a794a00a0000219de/026d63a33237bf0e2c2cf2a794a00a0000219de
256306688	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2cf2a794a00a000021a6e/026d63a33237bf0e2c2a794a00a000021a6e
8062464	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2cf2a794a00a000021e34/026d63a9d4a33237bf0e2c2cf2a794a00a000021e34
20024832	S3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2cf2a794a00a000021e70/026d63a9d4a33237bf0e2c2cf2a794a00a000021e70
10444	S 3://vertica/metadata/VMart/cluster_config.json
823266	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C13/chkpt_1.cat.gz`
254년	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C13/Completed

오브젝트 크기(바이트)	버킷/객체 키 전체 경로
2958	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C2_2/chkpt_1.cat.gz`
231	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C2_2/Completed
822521	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C4_chkpt_1.cat.gz`
231	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C4/Completed
746513	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat`
2596	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz`
821065	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz`
6440	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat`
8518	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat`

오브젝트 크기(바이트)	버킷/객체 키 전체 경로
0	S 3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat`
822922	S 3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C14_7/chkpt_1.cat.gz`
232입니다	S 3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C14_7/Completed
822930	S 3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz`
755033	S 3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat`
0	S 3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat`
822922	S 3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C14_7/chkpt_1.cat.gz`
232입니다	S 3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/C14_7/Completed
822930	S 3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz`

오브젝트 크기(바이트)	버킷/객체 키 전체 경로
755033	S 3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat`
0	S 3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat`

스트리밍 제한 비활성화

이 절차는 다른 온프레미스 오브젝트 스토리지에 대한 Vertica 가이드를 기반으로 하며 StorageGRID에 적용할 수 있어야 합니다.

1. 데이터베이스를 만든 후 AWSStreamingConnectionPercentage 구성 매개 변수를 0으로 설정하여 비활성화합니다. 이 설정은 공용 스토리지가 있는 Eon 모드 온-프레미스 설치에는 필요하지 않습니다. 이 구성 매개 변수는 Vertica가 스트리밍 읽기에 사용하는 개체 저장소에 대한 연결 수를 제어합니다. 클라우드 환경에서 이 설정은 오브젝트 저장소에서 데이터를 스트리밍하는 데 사용 가능한 모든 파일 핸들을 사용하지 않도록 도와줍니다. 이 경우 일부 파일 핸들을 다른 오브젝트 저장소 작업에 사용할 수 있습니다. 온프레미스 오브젝트 저장소의 대기 시간이 짧기 때문에 이 옵션이 필요하지 않습니다.
2. 매개 변수 값을 업데이트하려면 "vsql" 문을 사용합니다. 암호는 “온-프레미스 데이터베이스 만들기”에서 설정한 데이터베이스 암호입니다. 예를 들어, 다음 샘플 출력을 참조하십시오.

```
[dbadmin@vertica-vm1 ~]$ vsql
Password:
Welcome to vsql, the Vertica Analytic Database interactive terminal.
Type:   \h or \? for help with vsql commands
        \g or terminate with semicolon to execute query
        \q to quit
dbadmin=> ALTER DATABASE DEFAULT SET PARAMETER
AWSStreamingConnectionPercentage = 0; ALTER DATABASE
dbadmin=> \q
```

물류창고 설정을 확인하는 중입니다

Vertica 데이터베이스 기본 서비스 센터 설정은 읽기 및 쓰기 작업에 대해 활성화됩니다(값 = 1). 성능 향상을 위해 이러한 서비스 센터 설정을 유지할 것을 적극 권장합니다.

```
vsql -c 'show current all;' | grep -i UseDepot
DATABASE | UseDepotForReads | 1
DATABASE | UseDepotForWrites | 1
```

샘플 데이터 로드(옵션)

이 데이터베이스가 테스트용으로 제거되는 경우 테스트를 위해 이 데이터베이스에 샘플 데이터를 로드할 수 있습니다. Vertica는 각 Vertica 노드의 '/opt/vertica/examples/VMart_Schema/'에 있는 샘플 데이터 세트 VMart와 함께 제공됩니다. 이 샘플 데이터 집합에 대한 자세한 내용을 확인할 수 있습니다 "여기".

다음 단계에 따라 샘플 데이터를 로드합니다.

1. Vertica 노드 중 하나에 dbadmin으로 로그인합니다. cd /opt/vertica/examples/VMart_Schema/
2. 데이터베이스에 예제 데이터를 로드하고 하위 단계 c 및 d에 프롬프트가 표시되면 데이터베이스 암호를 입력합니다.
   a. 'cd/opt/vertica/examples/VMart_Schema'를 선택합니다
   b. './vmart_gen'
   c. "vsql<vmart_define_schema.sql"을 참조하십시오
   d. "vsql <vmart_load_data.sql"을 선택합니다
3. 미리 정의된 SQL 쿼리가 여러 개 있습니다. 일부 쿼리를 실행하여 테스트 데이터가 데이터베이스에 성공적으로 로드되었는지 확인할 수 있습니다. 예: ``vsql<vmart_queries1.sql'

추가 정보를 찾을 수 있는 위치

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

- "NetApp StorageGRID 11.7 제품 문서"
- "StorageGRID 데이터 시트"
- "Vertica 10.1 제품 설명서"

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2021년 9월	최초 릴리스.

안젤라 청 _ 에 의해

ELK 스택을 사용한 StorageGRID 로그 분석

안젤라 청 _ 에 의해

StorageGRID syslog 포워드 기능을 사용하면 StorageGRID 로그 메시지를 수집하고 분석하도록 외부 syslog 서버를 구성할 수 있습니다. 엘크(Elasticsearch, Logstash, Kibana)는 가장 인기 있는 로그 분석 솔루션 중 하나가 되었습니다. 샘플 elk 구성과 이 구성을 사용하여 실패한 S3 요청을 식별하고 해결하는 방법을 보려면 를 "ELK 비디오를 사용한 StorageGRID 로그 분석" 참조하십시오. StorageGRID 11.9에서는 부하 분산 장치 엔드포인트 액세스 로그를 외부 syslog 서버로 내보낼 수 있습니다. 이 새로운 기능에 대해 자세히 알아보려면 여기를 "YouTube 동영상" 참조하십시오. 이 문서에서는 Logstash 구성, Kibana 쿼리, 차트 및 대시보드의 예제 파일을 제공하여 StorageGRID 로그 관리 및 분석을 빠르게 시작할 수 있도록 합니다.

요구 사항

- StorageGRID 11.6.0.2 이상
- 엘크(Elasticsearch, Logstash 및 Kibana) 7.1x 이상 설치 및 작동 중

샘플 파일

- "Logstash 7.x 샘플 파일 패키지를 다운로드합니다" + * MD5 체크섬 * 148c23d0021d9a4b4a6c0287464deab + * SHA256 체크섬 * f51ec9e2e3f842d5a7861566ba561bbbb4373038b4e7b3b3b3d522adf2d6
- "Logstash 8.x 샘플 파일 패키지를 다운로드합니다" + * MD5 체크섬 * e11bae3a662f87c310ef363d0fe06835+ * SHA256 체크섬 * 5c670755742cfdf5a723a596ba087e0153a65baef3934afdb682f61cd278d
- "StorageGRID 11.9용 Logstash 8.x 샘플 파일 패키지를 다운로드합니다" + * MD5 체크섬 * 41272857c4a54600f95995f6ed74800d + * SHA256 체크섬 * 67048e8661052719990851e1ad960d4902fe537a6e135e8600177188da677c9

가정

독자는 StorageGRID 및 ELK 용어와 운영에 대해 잘 알고 있습니다.

지침

두 가지 샘플 버전은 그로크 패턴으로 정의된 이름의 차이로 인해 제공됩니다. 예를 들어, Logstash 구성 파일의 SYSLOGBASE 그로크 패턴은 설치된 Logstash 버전에 따라 필드 이름을 다르게 정의합니다.

```
match => {"message" => '<%{POSINT:syslog_pri}>%{SYSLOGBASE}
%{GREEDYDATA:msg-details}'}
```

- Logstash 7.17 샘플 *

Field	Value
t _id	7C1MaYEBRH8UbfKnIls8
t _index	sgrid2-2022.06.15
# _score	-
t _type	_doc
@timestamp	Jun 15, 2022 @ 17:36:46.038
t host	grid2-site2-s1
t logsource	SITE2-S1
t msg-details	Reloading syslog service
t pid	628
t program	update-sysl
t syslog_pri	37
t timestamp	Jun 15 21:36:46

- Logstash 8.23 샘플 *

Table JSON

Search field names

Actions	Field	Value
▫▫▫	_id	yuhOiIEBVP6KX4EwqcyU
▫▫▫	_index	sglog-2022.06.21
▫▫▫	# _score	-
▫▫▫	@timestamp	Jun 21, 2022 @ 18:07:45.444
▫▫▫	t event.original	<28>Jun 21 22:07:45 SITE2-S3 ADE: syslog messages being dropped
▫▫▫	t host.hostname	SITE2-S3
▫▫▫	t msg-details	syslog messages being dropped
▫▫▫	t process.name	ADE
▫▫▫	t syslog_pri	28
▫▫▫	t timestamp	Jun 21 22:07:45

• 단계 *

1. 설치된 엘크 버전을 기반으로 제공된 샘플의 압축을 풉니다. + 샘플 폴더에는 + * sglog-2-file.conf: * 이 구성 파일은 데이터 변환 없이 Logstash의 파일에 StorageGRID 로그 메시지를 출력합니다. 이 옵션을 사용하여 로그 스타재가 StorageGRID 메시지를 수신하는지 확인하거나 StorageGRID 로그 패턴을 이해하는 데 도움을 줄 수 있습니다. + * sglog-2-es.conf: * 이 구성 파일은 다양한 패턴과 필터를 사용하여 StorageGRID 로그 메시지를 변환합니다. 여기에는 패턴 또는 필터를 기반으로 메시지를 드롭하는 Drop 문 예가 포함되어 있습니다. 인덱싱을 위해 Elasticsearch로 출력이 전송됩니다. + 파일 내의 명령에 따라 선택한 구성 파일을 사용자 지정합니다.
2. 사용자 지정 구성 파일 테스트:

```
/usr/share/logstash/bin/logstash --config.test_and_exit -f <config-
file-path/file>
```

   마지막으로 반환된 줄이 아래 줄과 비슷하면 구성 파일에 구문 오류가 없는 것입니다.

```
[LogStash::Runner] runner - Using config.test_and_exit mode. Config
Validation Result: OK. Exiting Logstash
```

3. /etc/logstash/logstash.yml에서 config.reload.automatic 를 활성화하지 않은 경우 Logstash 서버의 config:/etc/logstash/conf.d+에 사용자 지정된 conf 파일을 복사합니다. 그렇지 않으면 구성 다시 로드 간격이 경과될 때까지 기다립니다.

```
 grep reload /etc/logstash/logstash.yml
# Periodically check if the configuration has changed and reload the
pipeline
config.reload.automatic: true
config.reload.interval: 5s
```

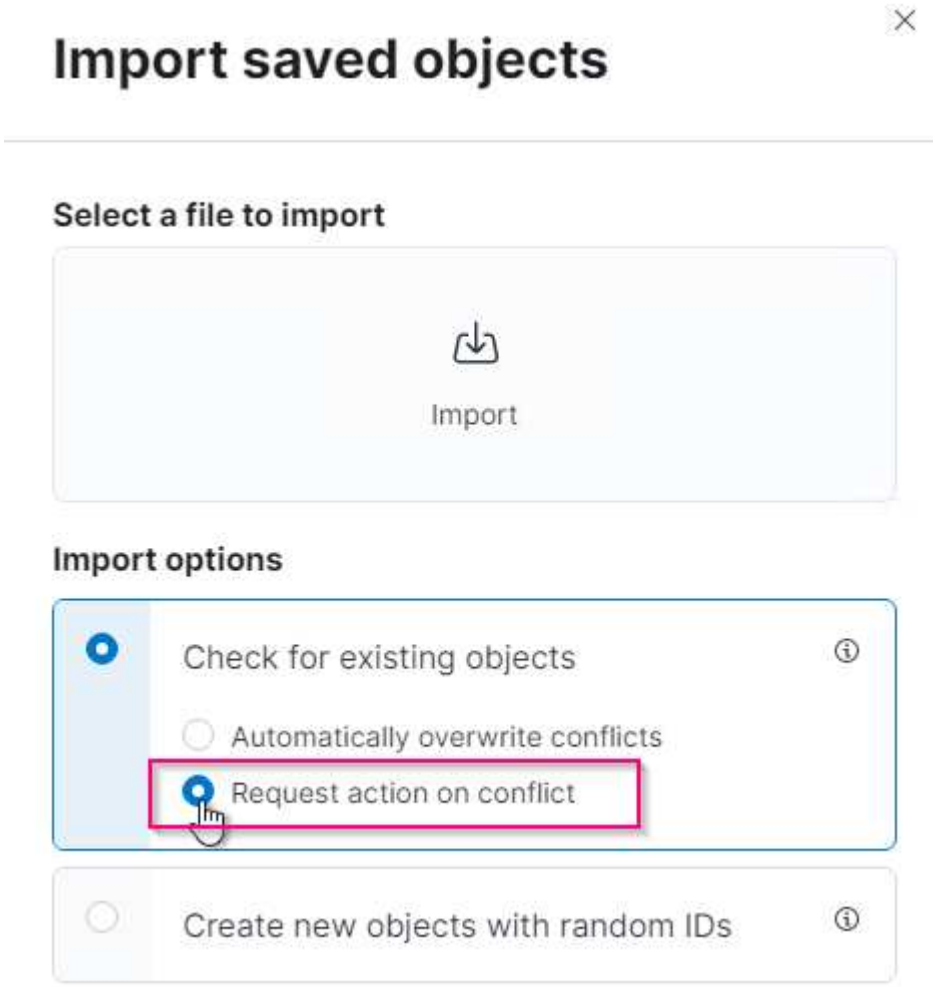
4. /var/log/logstash/logstash-plain.log 를 확인하고 새 구성 파일로 Logstash를 시작하는 데 오류가 없는지 확인합니다.
5. TCP 포트가 시작되고 수신 중인지 확인합니다. + 이 예에서는 TCP 포트 5000이 사용됩니다.

```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

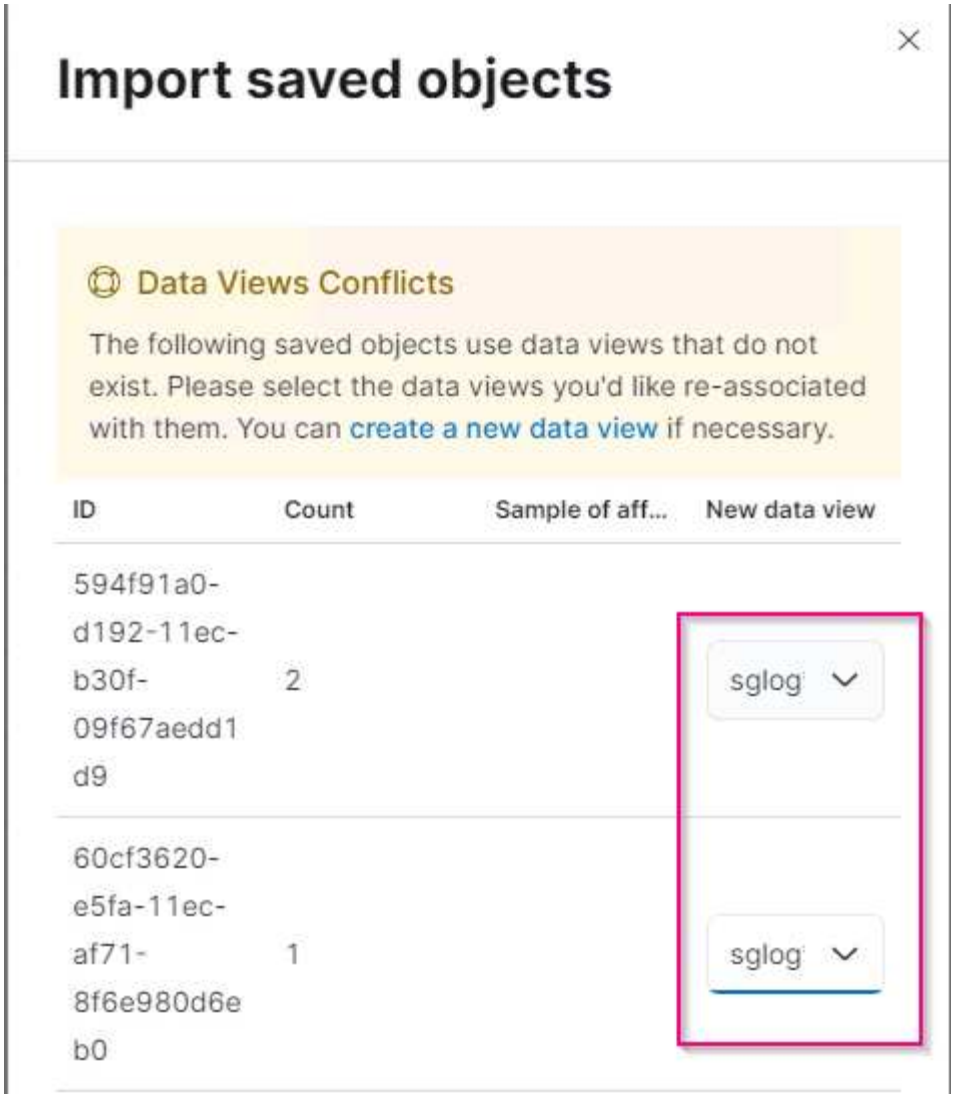
6. StorageGRID 관리자 GUI에서 로그 메시지를 Logstash로 보내도록 외부 syslog 서버를 구성합니다. 자세한 내용은 을 "데모 비디오" 참조하십시오.
7. 정의된 TCP 포트에 대한 StorageGRID 노드 연결을 허용하려면 Logstash 서버에서 방화벽을 구성하거나 비활성화해야 합니다.
8. Kibana GUI에서 관리 → 개발 도구 를 선택합니다. 콘솔 페이지에서 이 가져오기 명령을 실행하여 Elasticsearch에 새 인덱스가 생성되었는지 확인합니다.

```
GET /_cat/indices/*?v=true&s=index
```

9. 키바나 GUI에서 인덱스 패턴(엘크 7.x) 또는 데이터 뷰(엘크 8.x)를 생성합니다.
10. Kibana GUI의 상단 중앙에 있는 검색 상자에 '저장된 개체'를 입력합니다. + 저장된 개체 페이지에서 가져오기를 선택합니다. 불러오기 옵션 아래에서 '충돌 시 작업 요청'을 선택합니다.



ELK <version> -query-chart-sample.ndjson을 가져옵니다. + 충돌을 해결할 것인지 묻는 메시지가 나타나면 8단계에서 만든 색인 패턴이나 데이터 보기를 선택합니다.



다음 Kibana 객체를 가져왔습니다. + * Query * + * audit-msg-s3rq-orlm + * bycast log S3 관련 메시지 + * LogLevel 경고 이상 + * 보안 이벤트 실패 + * nginx-GW 액세스 로그(elk8-sample-for-sg119.zip에서만 사용 가능) + * S3 * audit * * 요청 기반 HTTP 상태 * * * * * bycast.log * 요청 기반 HTTP 요청 시

이제 Kibana를 사용하여 StorageGRID 로그 분석을 수행할 준비가 되었습니다.

추가 리소스

- "syslog101"
- "엘크 스택"
- "Grok 패턴 목록"
- "Logstash:Grok에 대한 초보자용 가이드"
- "Logstash: syslog 심층 탐구 실습 가이드"
- "Kibana 가이드 – 문서 탐색"
- "StorageGRID 감사 로그 메시지 참조"

Prometheus 및 Grafana를 사용하여 메트릭 보존 기간을 연장합니다

_ 아론 클라인 _

본 기술 보고서는 NetApp StorageGRID 외부 Prometheus 및 Grafana 서비스와 연동하는 방법에 대한 자세한 지침을 제공합니다.

소개

StorageGRID는 Prometheus를 사용하여 메트릭을 저장하고 내장된 Grafana 대시보드를 통해 이러한 메트릭의 시각화를 제공합니다. Prometheus 메트릭은 클라이언트 액세스 인증서를 구성하고 지정된 클라이언트에 대한 Prometheus 액세스를 활성화하여 StorageGRID에서 안전하게 액세스할 수 있습니다. 오늘날 이 메트릭 데이터의 보존은 관리 노드의 스토리지 용량에 의해 제한됩니다. 이러한 메트릭의 사용자 지정 시각화를 생성하는 데 더 오랜 시간이 걸릴 뿐만 아니라 사용자 지정 시각화를 만들기 위해 새 Prometheus 및 Grafana 서버를 구축하고, StorageGRID 인스턴스에서 메트릭을 스크레핑하도록 새 서버를 구성하고, 우리에게 중요한 메트릭이 포함된 대시보드를 만들 것입니다. 에서 수집된 Prometheus 메트릭에 대한 자세한 정보를 확인할 수 있습니다 "StorageGRID 설명서".

프로메테우스 연방

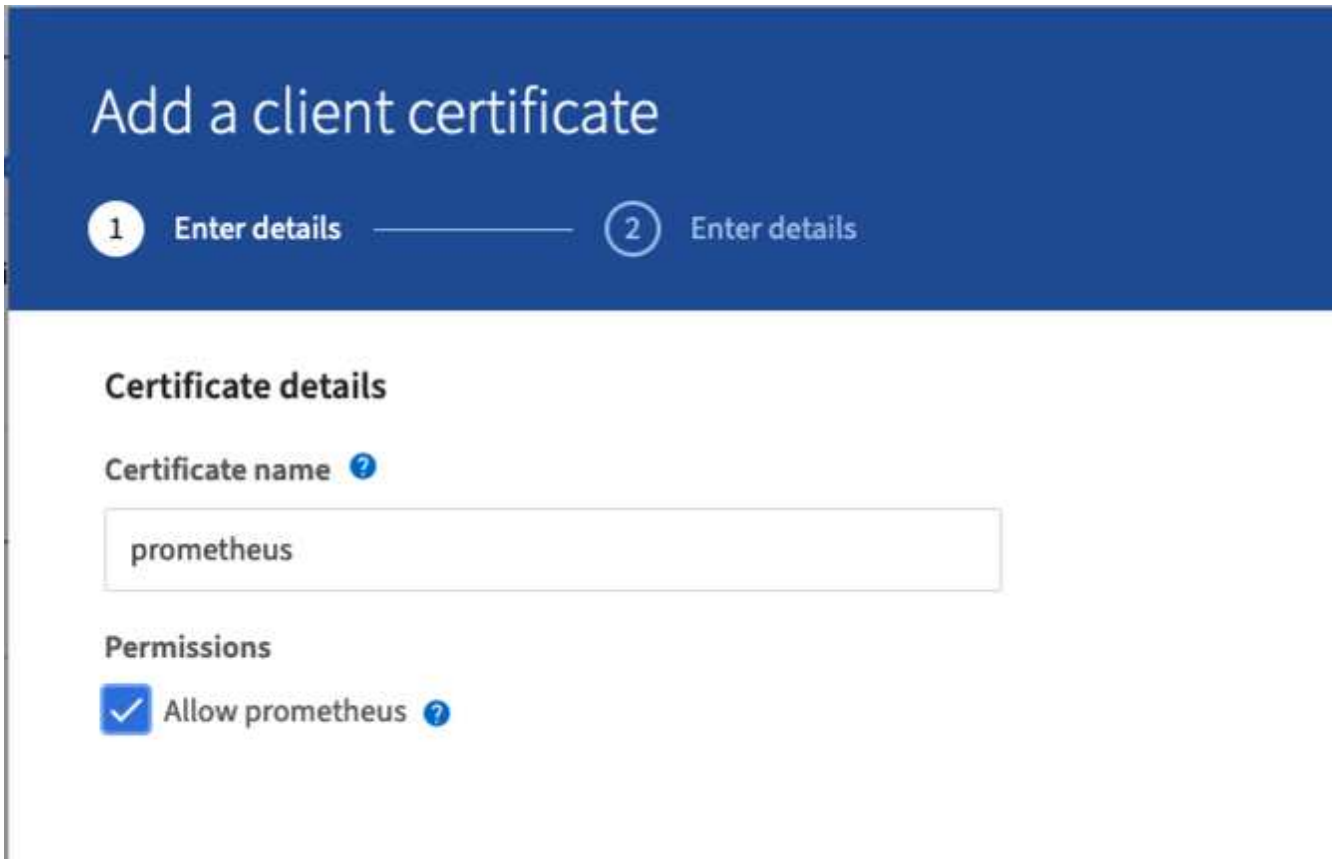
실습 세부 정보

이 예제에서는 StorageGRID 11.6 노드와 Debian 11 서버에 모든 가상 시스템을 사용합니다. StorageGRID 관리 인터페이스는 공개적으로 신뢰할 수 있는 CA 인증서로 구성됩니다. 이 예제에서는 StorageGRID 시스템 또는 Debian Linux 설치의 설치 및 구성을 사용하지 않습니다. Prometheus 및 Grafana에서 지원하기를 원하는 Linux의 맛을 사용할 수 있습니다. Prometheus와 Grafana는 모두 Docker 컨테이너로 설치하거나, 소스에서 구축하거나, 사전 컴파일된 바이너리로 구축할 수 있습니다. 이 예제에서는 Prometheus와 Grafana 바이너리를 동일한 Debian 서버에 직접 설치합니다. 의 기본 설치 지침을 다운로드하여 따릅니다 https://prometheus.io 및 https://grafana.com/grafana/ 각각

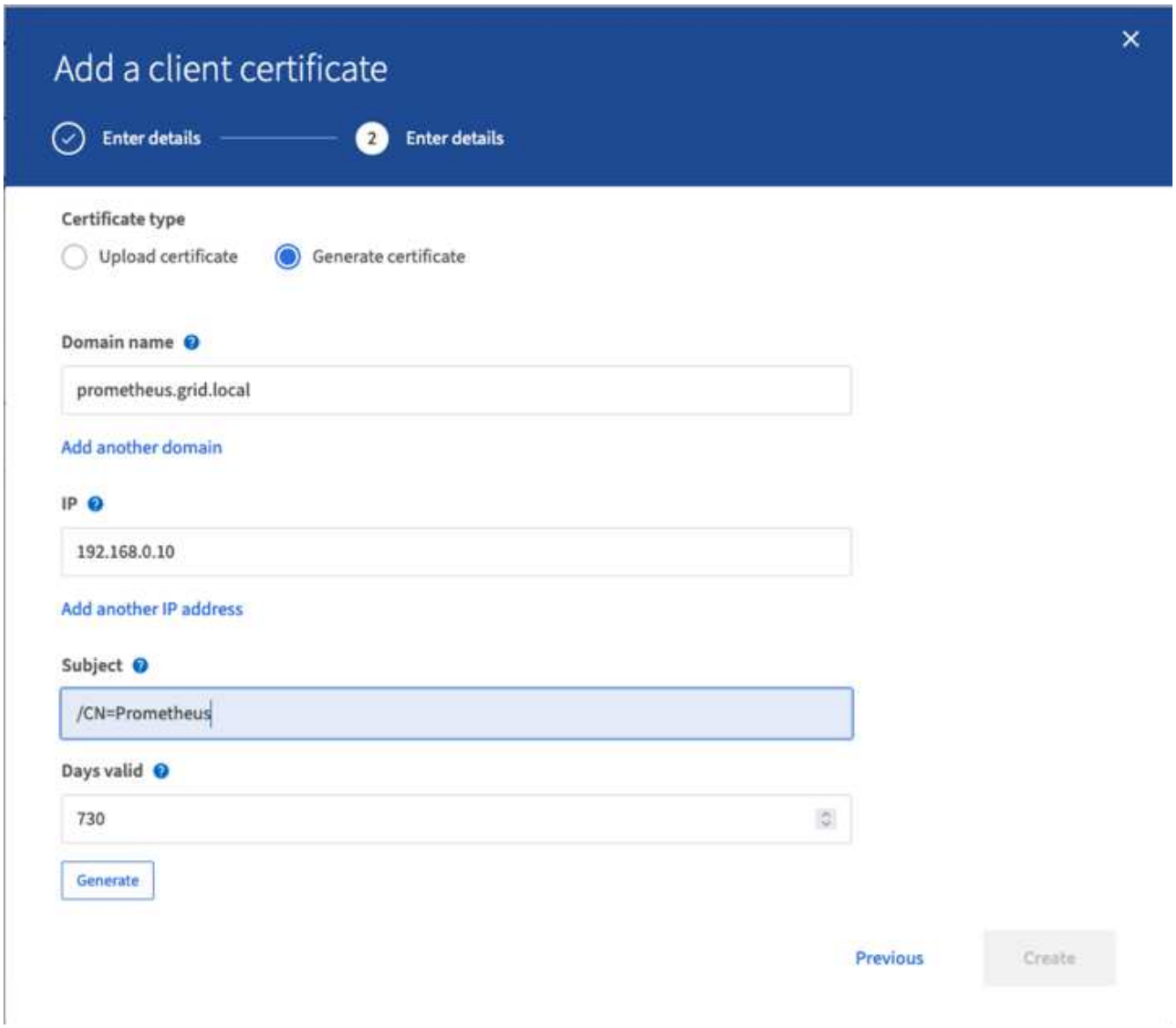
Prometheus 클라이언트 액세스를 위해 StorageGRID를 구성합니다

StorageGRID에 저장된 Prometheus 메트릭에 액세스하려면 개인 키가 있는 클라이언트 인증서를 생성하거나 업로드하고 클라이언트에 대한 권한을 활성화해야 합니다. StorageGRID 관리 인터페이스에는 SSL 인증서가 있어야 합니다. 이 인증서는 신뢰할 수 있는 CA에서 또는 자체 서명된 경우 수동으로 신뢰할 수 있는 Prometheus 서버에 의해 신뢰되어야 합니다. 자세한 내용은 를 참조하십시오 "StorageGRID 설명서".

1. StorageGRID 관리 인터페이스의 왼쪽 아래에서 "구성"을 선택하고 "보안" 아래의 두 번째 열에서 인증서를 클릭합니다.
2. 인증서 페이지에서 "클라이언트" 탭을 선택하고 "추가" 버튼을 클릭합니다.
3. 액세스 권한이 부여된 클라이언트의 이름을 제공하고 이 인증서를 사용합니다. "권한" 아래의 "Prometheus 허용" 앞의 상자를 클릭하고 계속 단추를 클릭합니다.

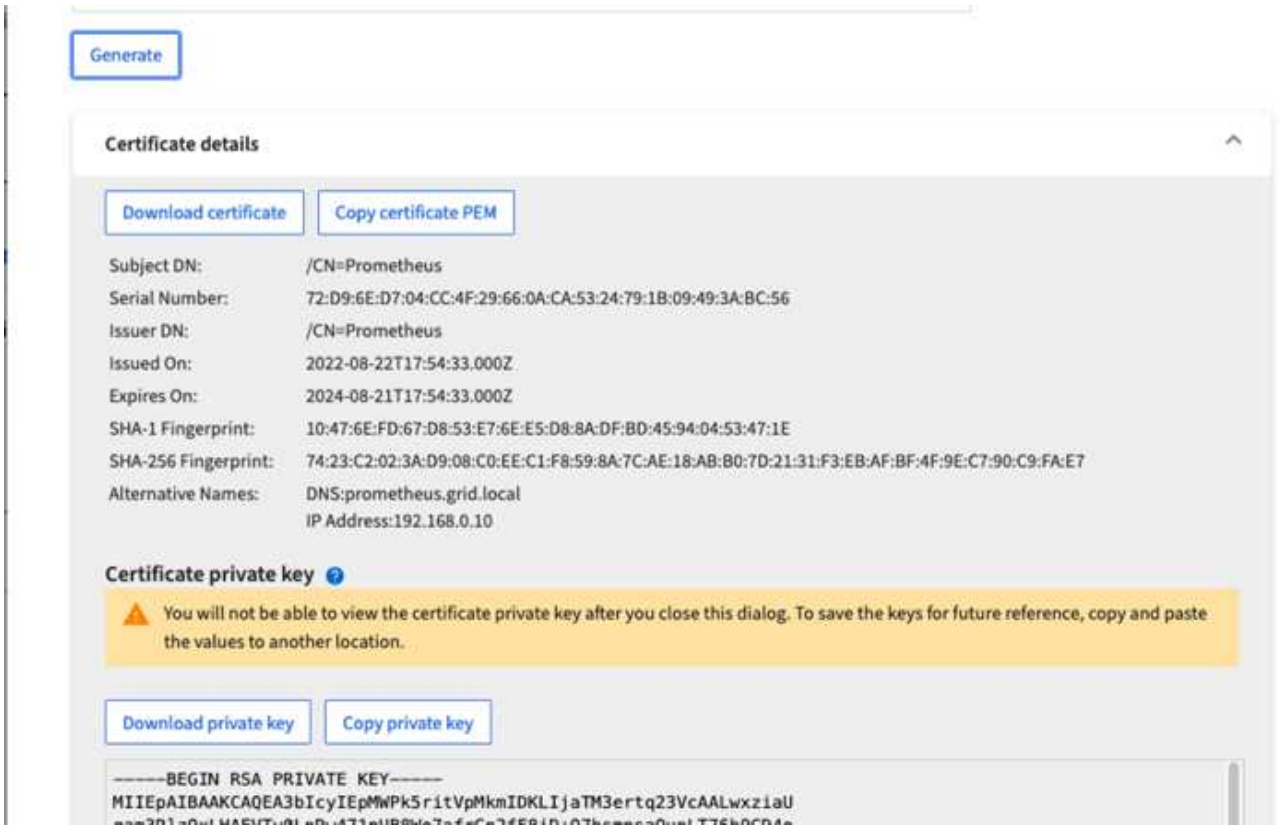


4. CA 서명 인증서가 있는 경우 "인증서 업로드" 라디오 버튼을 선택할 수 있지만, 여기서는 "인증서 생성" 라디오 버튼을 선택하여 StorageGRID가 클라이언트 인증서를 생성하도록 할 것입니다. 필수 필드가 입력되어 표시됩니다. 클라이언트 서버의 FQDN, 서버의 IP, 제목 및 유효한 날짜를 입력합니다. 그런 다음 "생성" 버튼을 클릭합니다.



> Be mindful of the certificate days valid entry as you will need to renew this certificate in both StorageGRID and the Prometheus server before it expires to maintain uninterrupted collection.

1. 인증서 PEM 파일과 개인 키 PEM 파일을 다운로드합니다.



> This is the only time you can download the private key, so make sure you do not skip this step.

Prometheus 설치를 위해 **Linux** 서버를 준비합니다

Prometheus를 설치하기 전에 Prometheus 사용자, 디렉토리 구조를 사용하여 환경을 준비하고 메트릭 스토리지 위치의 용량을 구성하려고 합니다.

1. Prometheus 사용자를 생성합니다.

```
sudo useradd -M -r -s /bin/false Prometheus
```

2. Prometheus, 클라이언트 인증서 및 메트릭 데이터용 디렉토리를 생성합니다.

```
sudo mkdir /etc/Prometheus /etc/Prometheus/cert /var/lib/Prometheus
```

3. ext4 파일 시스템을 사용하여 메트릭 보존을 위해 사용 중인 디스크를 포맷했습니다.

```
mkfs -t ext4 /dev/sdb
```

4. 그런 다음 Prometheus 메트릭 디렉토리에 파일 시스템을 마운트했습니다.

```
sudo mount -t auto /dev/sdb /var/lib/prometheus/
```

5. 메트릭 데이터에 사용 중인 디스크의 uuid를 가져옵니다.

```
sudo ls -al /dev/disk/by-uuid/
   lrwxrwxrwx 1 root root   9 Aug 18 17:02 9af2c5a3-bfc2-4ec1-85d9-
ebab850bb4a1 -> ../../sdb
```

6. /etc/fstab/에 항목을 추가하면 /dev/sdb 의 uuuid 를 사용하여 재부팅 후에도 마운트가 유지됩니다.

```
/etc/fstab
UUID=9af2c5a3-bfc2-4ec1-85d9-ebab850bb4a1 /var/lib/prometheus   ext4
defaults    0   0
```

Prometheus를 설치하고 구성합니다

이제 서버가 준비되었으므로 Prometheus 설치를 시작하고 서비스를 구성할 수 있습니다.

1. Prometheus 설치 패키지의 압축을 풉니다

```
tar xzf prometheus-2.38.0.linux-amd64.tar.gz
```

2. 바이너리를 /usr/local/bin에 복사하고 소유권을 이전에 만든 Prometheus 사용자로 변경합니다

```
sudo cp prometheus-2.38.0.linux-amd64/{prometheus,promtool}
/usr/local/bin
sudo chown prometheus:prometheus /usr/local/bin/{prometheus,promtool}
```

3. 콘솔 및 라이브러리를 /etc/Prometheus에 복사합니다

```
sudo cp -r prometheus-2.38.0.linux-amd64/{consoles,console_libraries}
/etc/prometheus/
```

4. StorageGRID에서 이전에 다운로드한 클라이언트 인증서 및 개인 키 PEM 파일을 /etc/Prometheus/certs로 복사합니다
5. Prometheus 구성 YAML 파일을 생성합니다

```
sudo nano /etc/prometheus/prometheus.yml
```

6. 다음 설정을 삽입합니다. 작업 이름은 원하는 모든 것이 될 수 있습니다. "-targets:['']"를 관리 노드의 FQDN으로 변경하고 인증서 및 개인 키 파일 이름의 이름을 변경한 경우 TLS_config 섹션이 일치하도록 업데이트하십시오. 그런 다음 파일을 저장합니다. 그리드 관리 인터페이스에서 자체 서명된 인증서를 사용하는 경우 인증서를 다운로드하여 고유한 이름의 클라이언트 인증서와 함께 놓고 TLS_config 섹션에서 ca_file:/etc/Prometheus/cert/UCERT.pem을 추가합니다

   a. 이 예에서는 alertmanager, cassandra, node 및 StorageGRID로 시작하는 모든 메트릭을 수집합니다. Prometheus 메트릭에 대한 자세한 내용은 에서 확인할 수 있습니다 "StorageGRID 설명서".

```
# my global config
global:
  scrape_interval: 60s # Set the scrape interval to every 15 seconds.
Default is every 1 minute.

scrape_configs:
  - job_name: 'StorageGRID'
    honor_labels: true
    scheme: https
    metrics_path: /federate
    scrape_interval: 60s
    scrape_timeout: 30s
    tls_config:
      cert_file: /etc/prometheus/cert/certificate.pem
      key_file: /etc/prometheus/cert/private_key.pem
    params:
      match[]:
        -
'{__name__=~"alertmanager_.*|cassandra_.*|node_.*|storagegrid_.*"}'
    static_configs:
    - targets: ['sgdemo-rtp.netapp.com:9091']
```

> 그리드 관리 인터페이스에서 자체 서명된 인증서를 사용하는 경우 인증서를 다운로드하여 고유한 이름의 클라이언트 인증서와 함께 배치합니다. TLS_config 섹션에서 클라이언트 인증서 및 개인 키 줄 위에 인증서를 추가합니다
>
> ```
> ca_file: /etc/prometheus/cert/UIcert.pem
> ```

1. /etc/Prometheus 및 /var/lib/Prometheus에 있는 모든 파일 및 디렉토리의 소유권을 Prometheus 사용자로 변경합니다

```
sudo chown -R prometheus:prometheus /etc/prometheus/
sudo chown -R prometheus:prometheus /var/lib/prometheus/
```

2. /etc/systemd/system에서 Prometheus 서비스 파일을 생성합니다

```
sudo nano /etc/systemd/system/prometheus.service
```

3. 다음 줄을 삽입하고 메트릭 데이터의 보존 기간을 1년으로 설정하는 #- storage.tsdb.retention.time=1y#를 확인합니다. 또는 #- storage.sdb.retention.size=300GiB#를 사용하여 스토리지 제한에 따라 기본 보존을 수행할 수도 있습니다. 메트릭 보존을 설정할 수 있는 유일한 위치입니다.

```
[Unit]
Description=Prometheus Time Series Collection and Processing Server
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
        --config.file /etc/prometheus/prometheus.yml \
        --storage.tsdb.path /var/lib/prometheus/ \
        --storage.tsdb.retention.time=1y \
        --web.console.templates=/etc/prometheus/consoles \
        --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

4. 새 Prometheus 서비스를 등록하려면 시스템 서비스를 다시 로드하십시오. 그런 다음 Prometheus 서비스를 시작하고 활성화합니다.

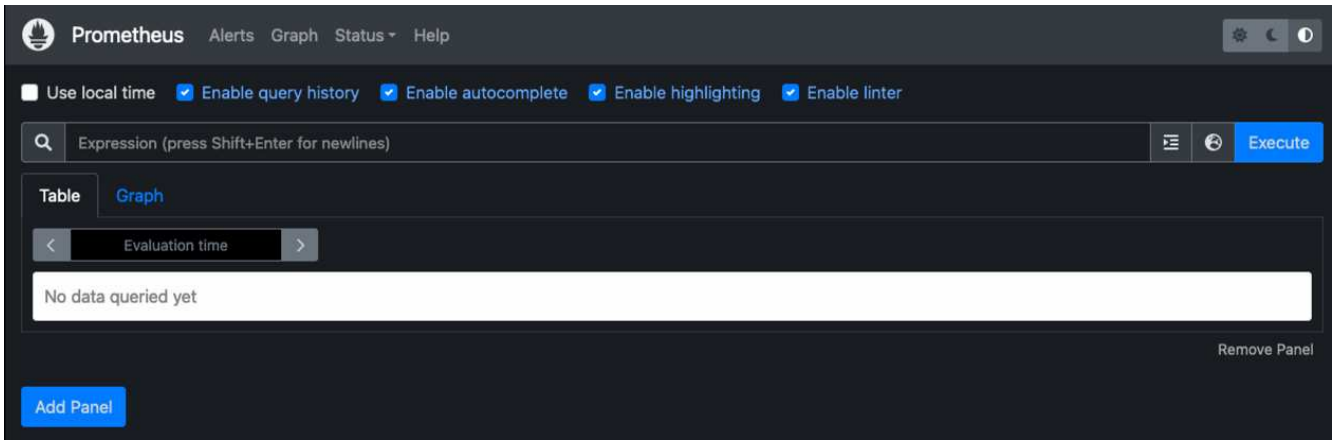
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. 서비스가 올바르게 실행되는지 확인합니다

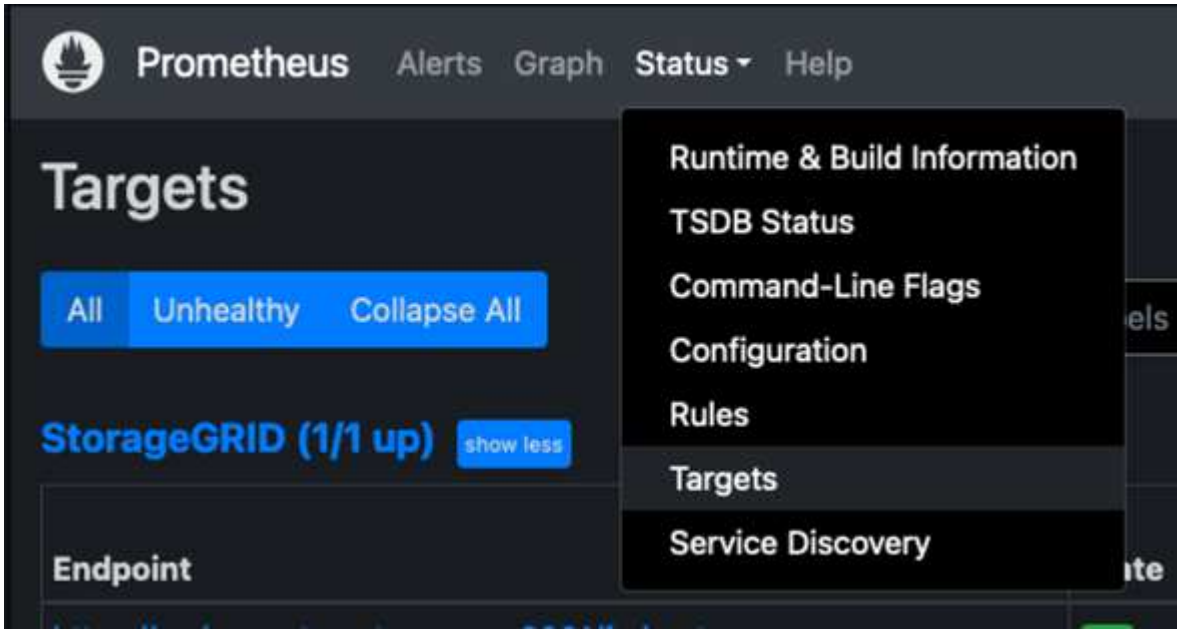
```
sudo systemctl status prometheus
```

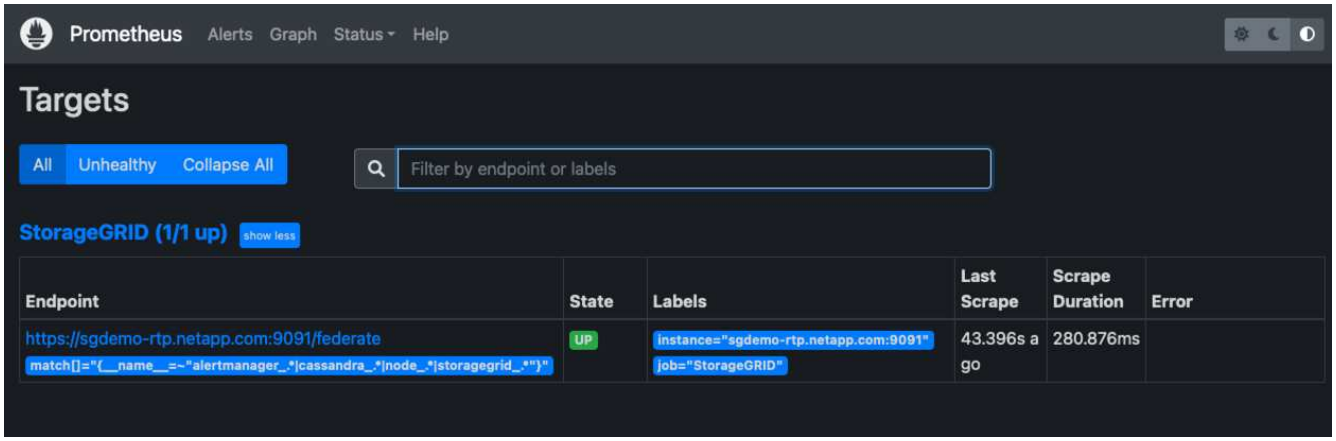
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 28818)
     Memory: 107.7M
        CPU: 1.143s
     CGroup: /system.slice/prometheus.service
             └─6498 /usr/local/bin/prometheus --config.file
/etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
--web.console.templates=/etc/prometheus/consoles --web.con>

Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.510Z caller=head.go:544 level=info component=tsdb
msg="Replaying WAL, this may take a while"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=0 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=1 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:621 level=info component=tsdb msg="WAL
replay completed" checkpoint_replay_duration=55.57µs wal_rep>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:997 level=info fs_type=EXT4_SUPER_MAGIC
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1000 level=info msg="TSDB started"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1181 level=info msg="Loading
configuration file" filename=/etc/prometheus/prometheus.yml
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:1218 level=info msg="Completed loading
of configuration file" filename=/etc/prometheus/prometheus.y>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:961 level=info msg="Server is ready to
receive web requests."
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=manager.go:941 level=info component="rule
manager" msg="Starting rule manager..."
```

6. 이제 Prometheus 서버의 UI로 이동할 수 있습니다 http://Prometheus-server:9090 UI를 참조하십시오

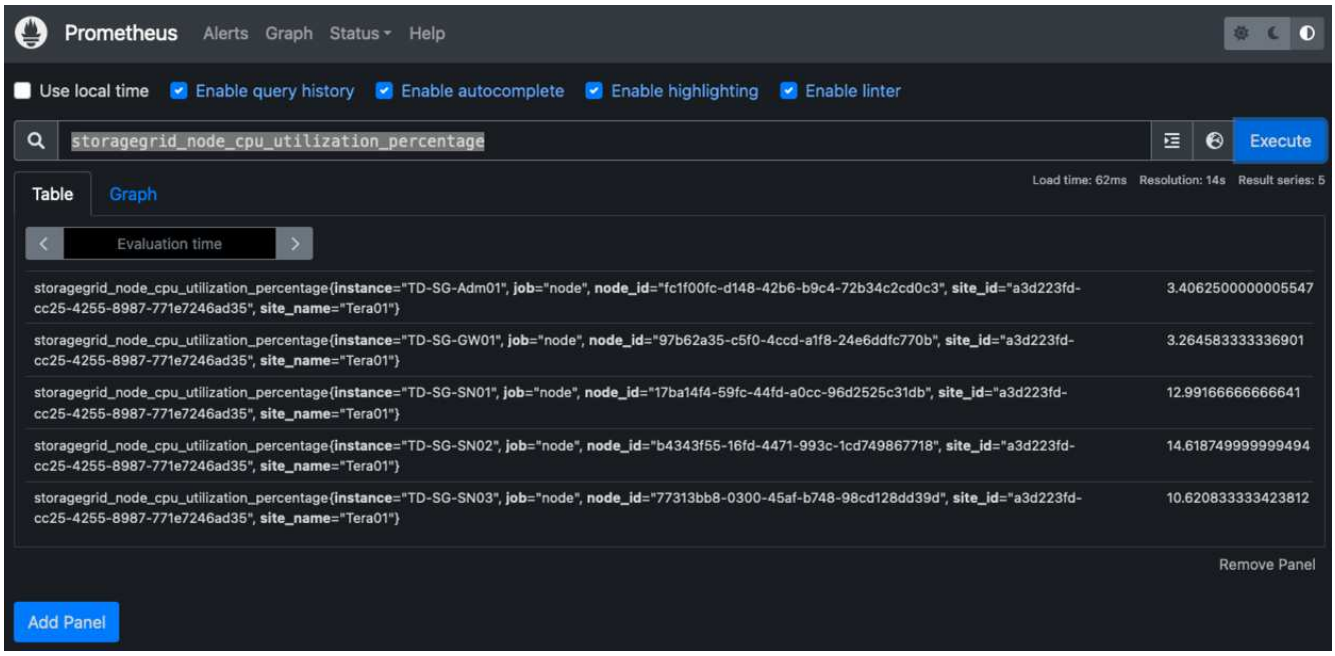


7. "상태" 대상 아래에서 Prometheus.yml에서 구성한 StorageGRID 끝점의 상태를 볼 수 있습니다





8. 그래프 페이지에서 테스트 쿼리를 실행하고 데이터가 스크레핑되었는지 확인할 수 있습니다. 예를 들어 쿼리 표시줄에 "StorageGrid_node_cpu_Utilization_percentage"를 입력하고 실행 단추를 클릭합니다.



Grafana 설치 및 구성

Prometheus가 설치되고 작동되었으므로 Grafana 설치 및 대시보드 구성으로 이동할 수 있습니다

Grafana 인스턴션

1. Grafana의 최신 Enterprise Edition을 설치합니다

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key
https://packages.grafana.com/gpg.key
```

2. 안정적인 릴리스를 위해 이 리포지토리를 추가합니다.

```
echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://packages.grafana.com/enterprise/deb stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
```

3. 리포지토리를 추가한 후

```
sudo apt-get update
sudo apt-get install grafana-enterprise
```

4. 새 이식편 서비스를 등록하려면 시스템 서비스를 다시 로드하십시오. 그런 다음 Grafana 서비스를 시작 및 활성화합니다.

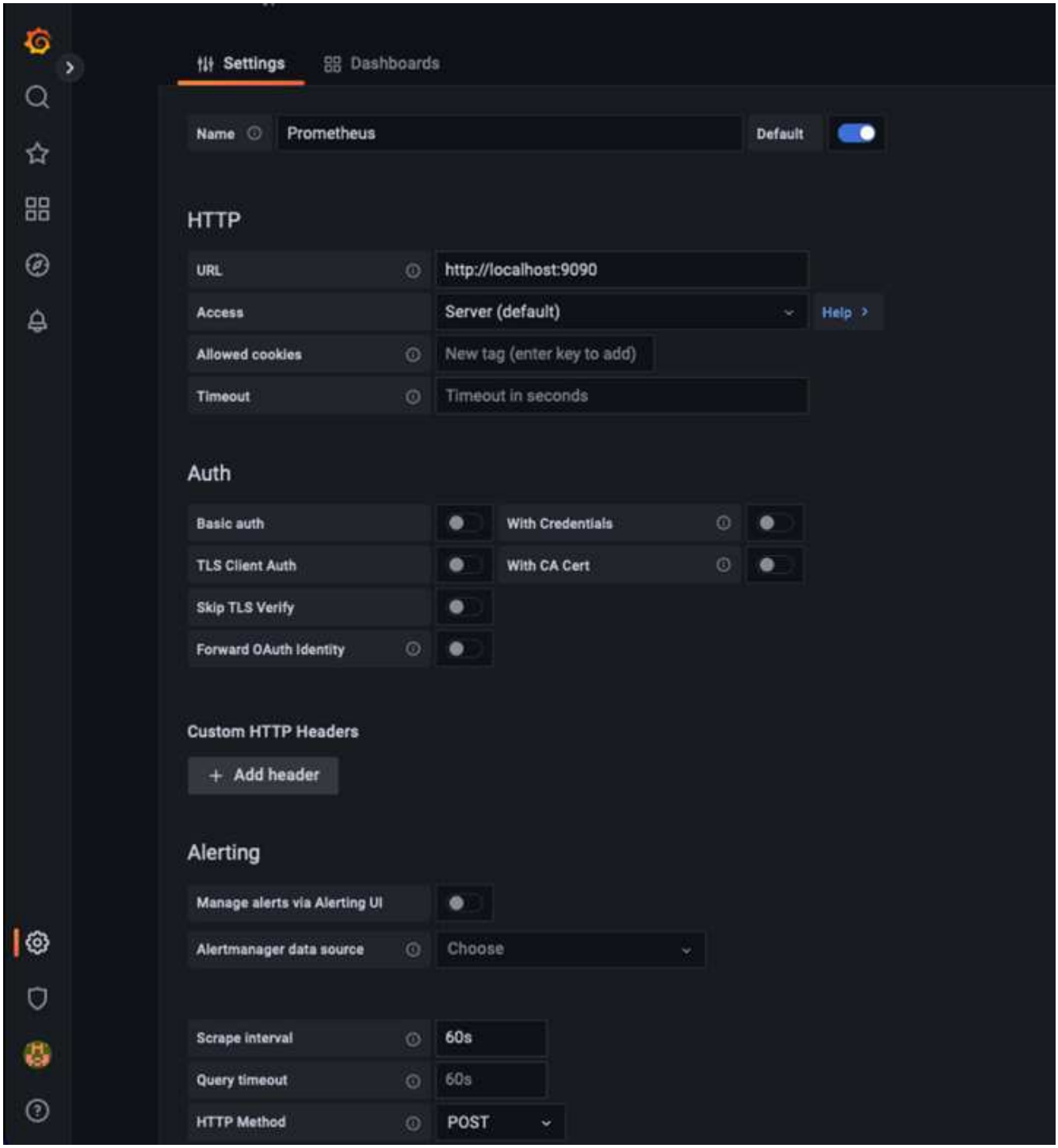
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafana가 이제 설치 및 실행 중입니다. 브라우저를 열고 HTTP://Prometheus-server:3000을 열면 Grafana 로그인 페이지가 표시됩니다.
6. 기본 로그인 자격 증명은 admin/admin이며, 메시지가 표시되면 새 암호를 설정해야 합니다.

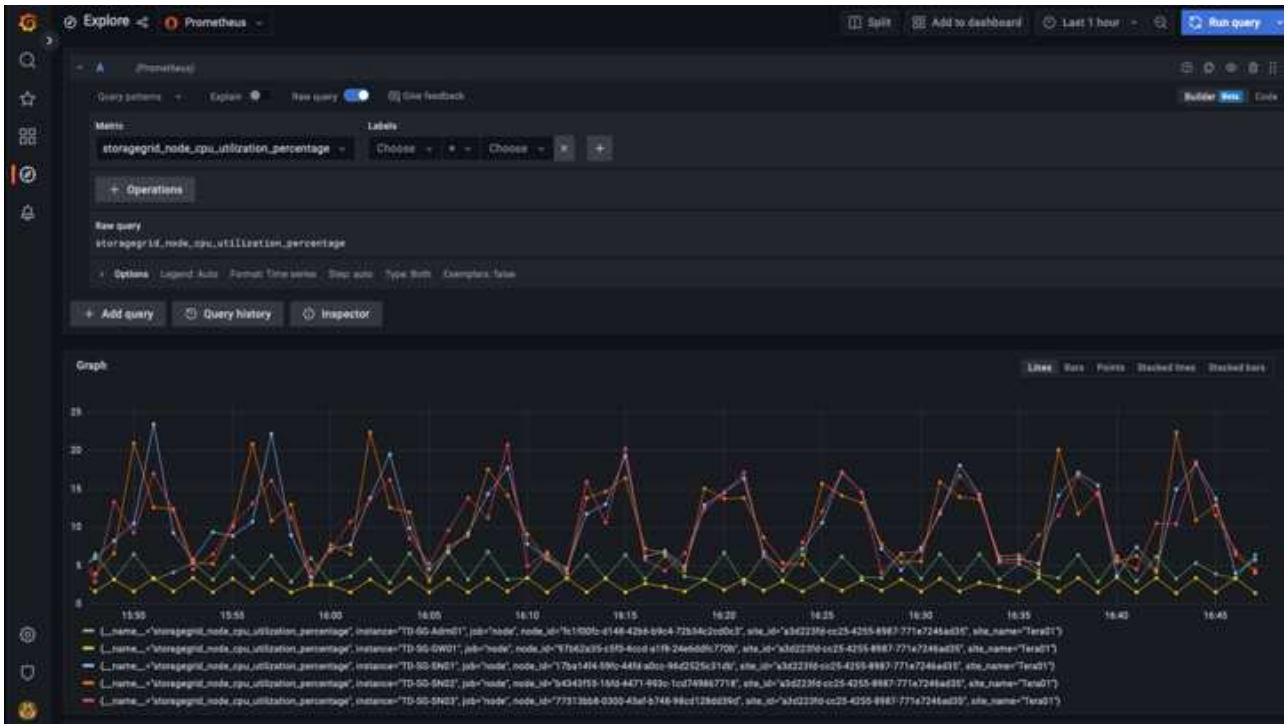
StorageGRID에 대한 **Grafana** 대시보드를 생성합니다

Grafana와 Prometheus가 설치 및 실행되었으므로 이제 데이터 소스를 생성하고 대시보드를 구축하여 두 가지를 연결할 시간입니다

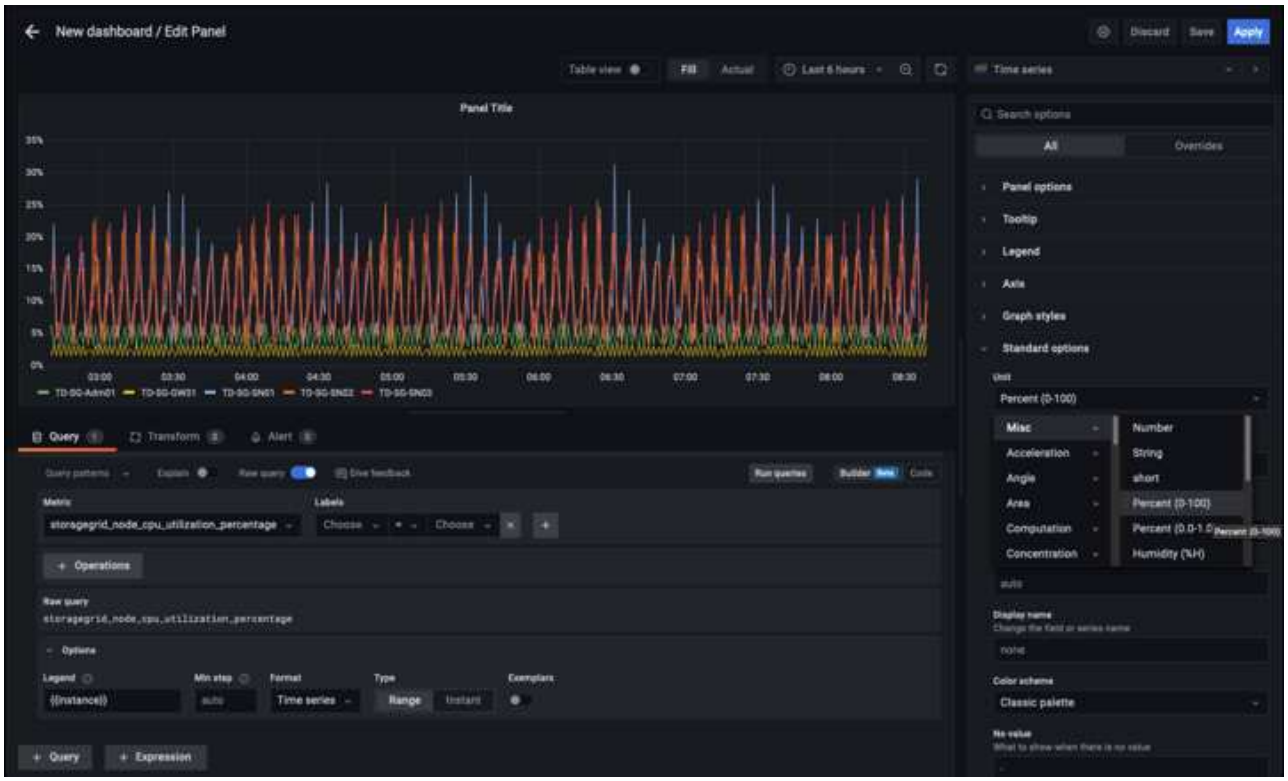
1. 왼쪽 창에서 "구성"을 확장하고 "데이터 소스"를 선택한 다음 "데이터 소스 추가" 버튼을 클릭합니다
2. Prometheus는 최고의 데이터 소스 중 하나가 될 것입니다. 그렇지 않은 경우 검색 표시줄을 사용하여 "Prometheus"를 찾습니다.
3. Prometheus 인스턴스의 URL과 Prometheus 간격에 맞게 스크레핑 간격을 입력하여 Prometheus 소스를 구성합니다. Prometheus에서 경고 관리자를 구성하지 않았기 때문에 알림 섹션도 비활성화했습니다.



4. 원하는 설정을 입력한 후 아래로 스크롤하여 "Save & Test(저장 및 테스트)"를 클릭합니다.
5. 구성 테스트가 완료되면 탐색 버튼을 클릭합니다.
   a. 탐색 창에서 Prometheus를 "StorageGrid_node_cpu_Utilization_percentage"로 테스트한 것과 동일한 메트릭을 사용하고 "쿼리 실행" 단추를 클릭할 수 있습니다



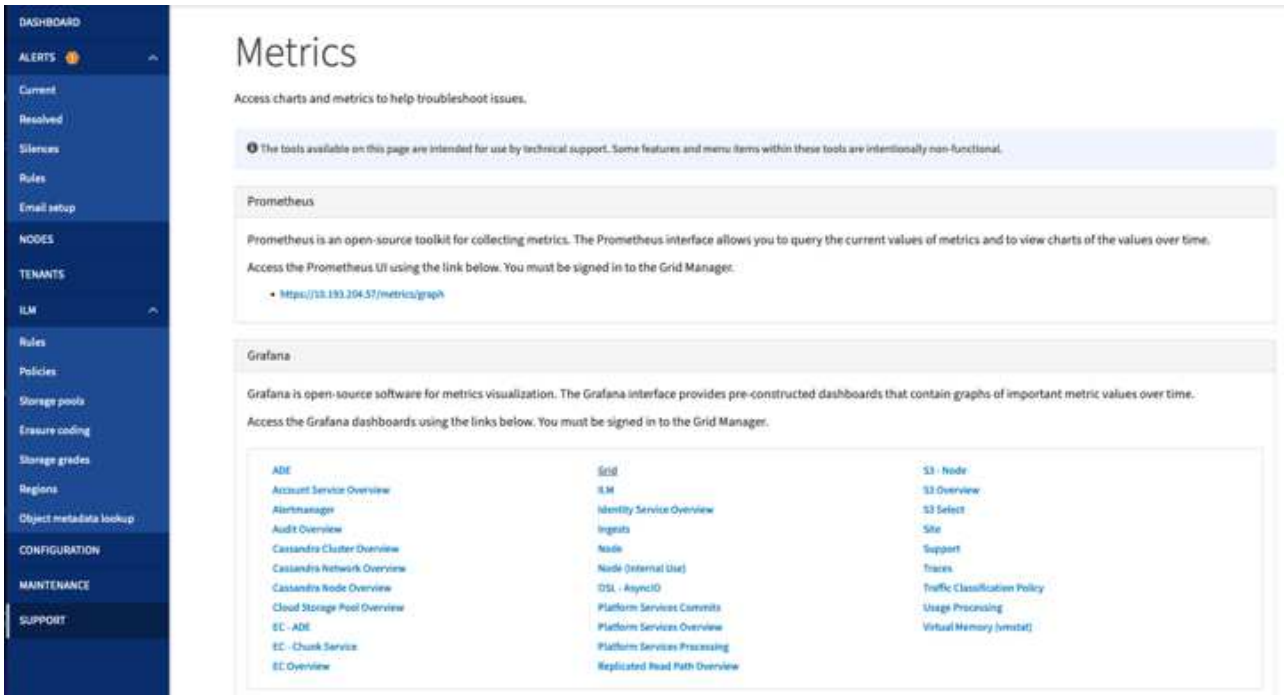
6. 이제 데이터 소스가 구성되었으므로 대시보드를 생성할 수 있습니다.
   a. 왼쪽 창에서 "대시보드"를 확장하고 "+새 대시보드"를 선택합니다.
   b. "Add a new panel(새 패널 추가)"을 선택합니다.
   c. 메트릭을 선택하여 새 패널을 구성합니다. 다시 "StorageGrid_node_cpu_Utilization_percentage"를 사용하고, 패널 제목을 입력하고, 하단에 있는 "Options"를 확장하고, 범례를 사용자 지정으로 변경하려면 "{{instance}}"를 입력하고, 오른쪽 창에 "Standard options"에서 "Unit"을 "Misc/Percent(0-100)"로 설정합니다. 그런 다음 "적용"을 클릭하여 패널을 대시보드에 저장합니다.



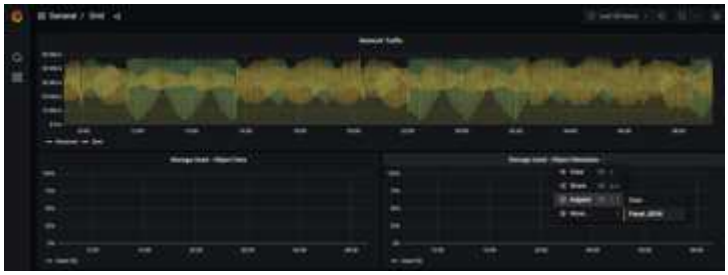
7. 원하는 각 메트릭에 대해 이러한 대시보드를 계속 구축할 수 있지만 다행히 StorageGRID에는 사용자 지정 대시보드에 복사할 수 있는 패널이 포함된 대시보드가 이미 있습니다.

   a. StorageGRID 관리 인터페이스의 왼쪽 창에서 "지원"을 선택하고 "도구" 열 아래쪽에서 "메트릭"을 클릭합니다.

   b. 메트릭스 내에서 중간 열의 맨 위에 있는 "Grid" 링크를 선택하겠습니다.

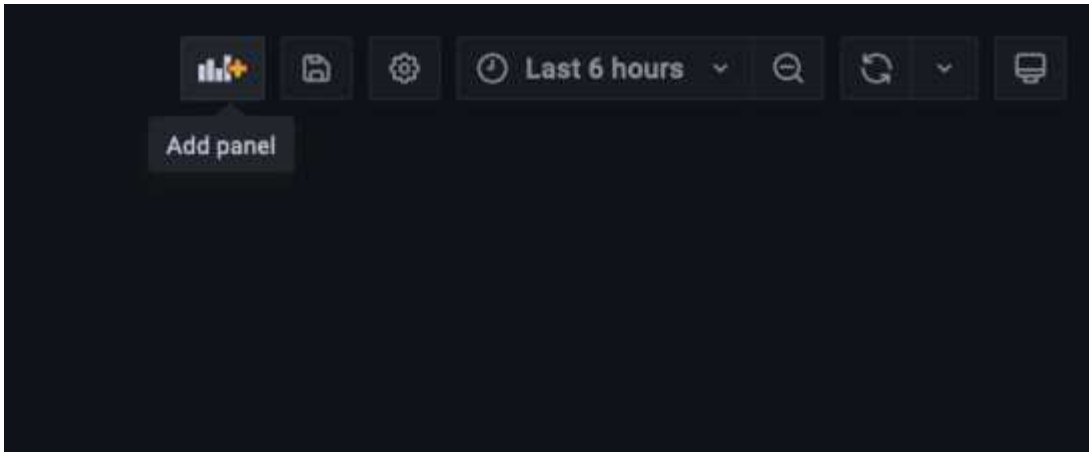


   c. Grid 대시보드에서 "Storage Used - Object Metadata" 패널을 선택합니다. 작은 아래쪽 화살표 및 패널 제목 끝을 클릭하여 메뉴를 드롭다운합니다. 이 메뉴에서 "검사" 및 "패널 JSON"을 선택합니다.



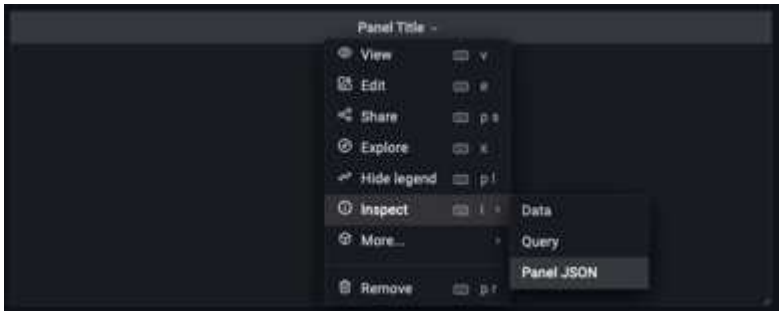
   d. JSON 코드를 복사하고 창을 닫습니다.

e. 새 대시보드에서 아이콘을 클릭하여 새 패널을 추가합니다.

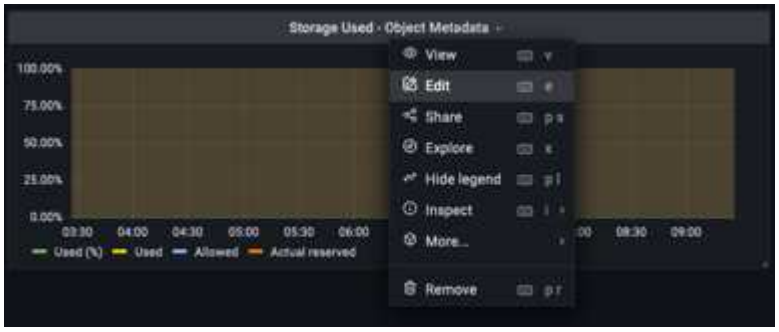


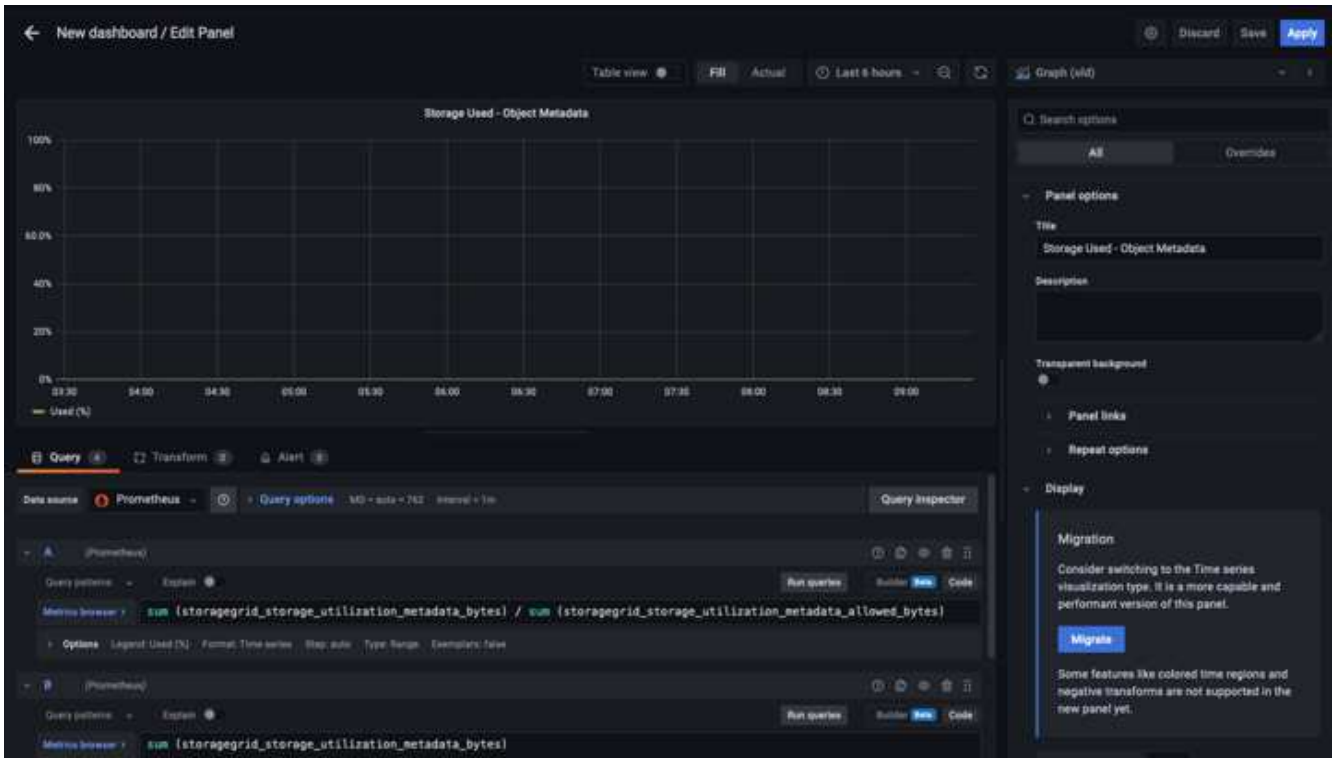
f. 변경하지 않고 새 패널을 적용합니다

g. StorageGRID 패널과 마찬가지로 JSON을 검사하십시오. JSON 코드를 모두 제거하고 StorageGRID 패널에서 복사한 코드로 교체합니다.



h. 새 패널을 편집하면 오른쪽에 "migrate(마이그레이션)" 버튼이 있는 Migration(마이그레이션) 메시지가 표시됩니다. 버튼을 클릭한 다음 "적용" 버튼을 클릭합니다.





8. 모든 패널이 제자리에 있고 원하는 대로 구성되면 오른쪽 위에 있는 디스크 아이콘을 클릭하여 대시보드를 저장하고 대시보드에 이름을 지정합니다.

결론

이제 Prometheus 서버에 맞춤형 데이터 보존 및 스토리지 용량을 추가할 수 있습니다. 이를 통해 운영 관련 메트릭이 포함된 자체 대시보드를 지속적으로 구축할 수 있습니다. 에서 수집된 Prometheus 메트릭에 대한 자세한 정보를 확인할 수 있습니다 "StorageGRID 설명서".

F5 DNS를 사용하여 StorageGRID 전역 로드 밸런싱을 구현하세요.

스티브 고먼(F5) 작성

이 기술 보고서는 NetApp StorageGRID F5 DNS 서비스와 함께 구성하여 글로벌 로드 밸런싱을 구현하는 방법에 대한 자세한 지침을 제공합니다. 이를 통해 여러 사이트 및/또는 HA 그룹에 분산된 스토리지 그리드 환경에서 데이터 가용성 향상, 데이터 일관성 강화, S3 트랜잭션 라우팅 최적화가 가능합니다.

소개

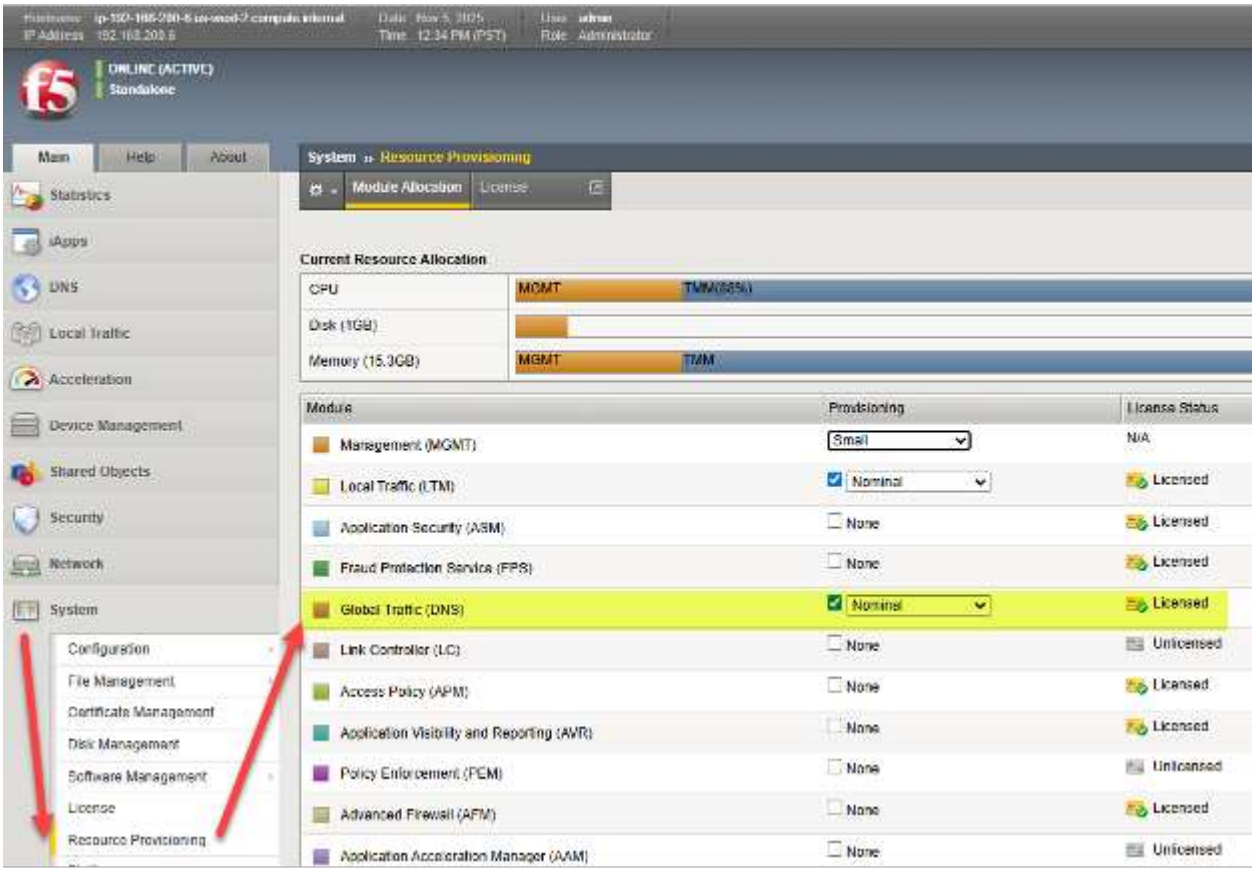
이전에는 BIG-IP GTM(Global Traffic Manager) 또는 GSLB(Global Server Load Balancing)로 불렸던 F5 BIG-IP DNS 솔루션은 여러 액티브-액티브 HA 그룹과 액티브-액티브 멀티사이트 StorageGRID 솔루션 간의 원활한 액세스를 효과적으로 구현할 수 있도록 지원합니다.

F5 BIG-IP 멀티사이트 StorageGRID 구성

지원할 StorageGRID 사이트 수와 관계없이 최소 2개의 BIG-IP 어플라이언스(물리적 또는 가상)에 BIG-IP DNS 모듈이 활성화 및 설정되어 있어야 합니다. DNS 어플라이언스가 많을수록 기업은 더욱 높은 수준의 이중화를 확보할 수 있습니다.

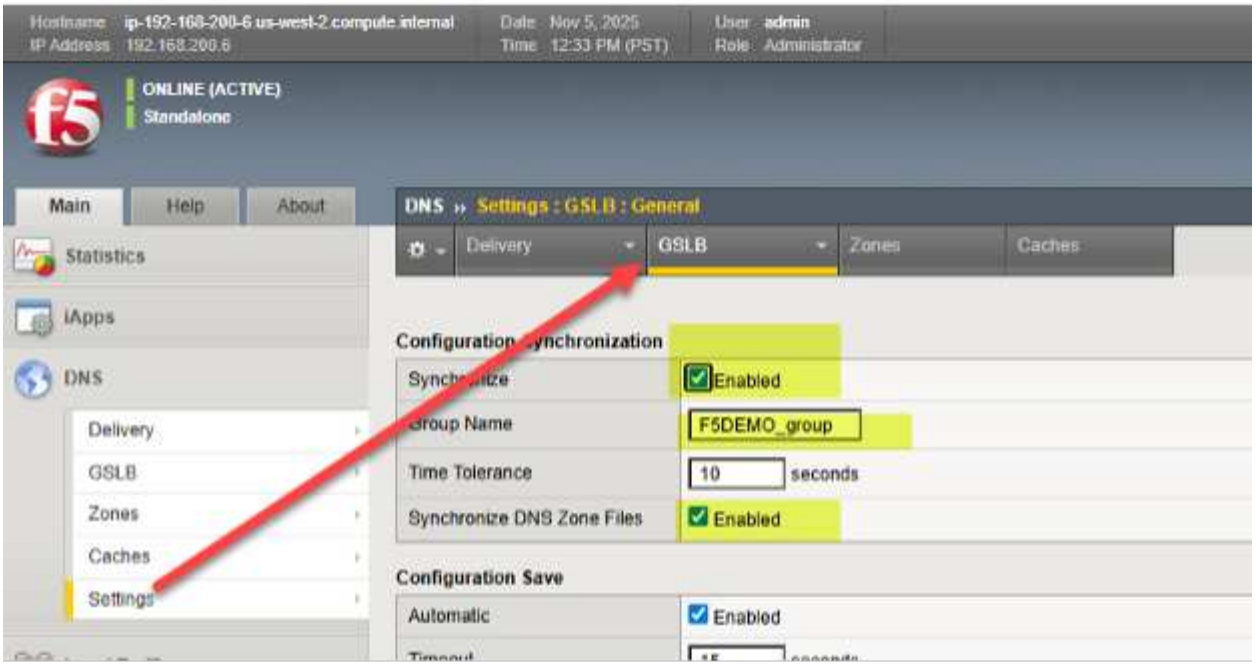
BIG-IP DNS - 초기 설정의 첫 단계

BIG-IP 어플라이언스의 초기 프로비저닝이 완료되면 웹 브라우저를 사용하여 TMUI(BIG-IP GUI) 인터페이스에 로그인하고 시스템 → 리소스 프로비저닝을 선택하십시오. 앞서 강조한 바와 같이, "글로벌 트래픽(DNS)" 모듈에 체크 표시가 되어 있고 라이선스가 부여된 것으로 표시되는지 확인하십시오. 참고로 이미지에서처럼 "로컬 트래픽(LTM)"은 동일한 어플라이언스에 프로비저닝되는 경우가 흔합니다.

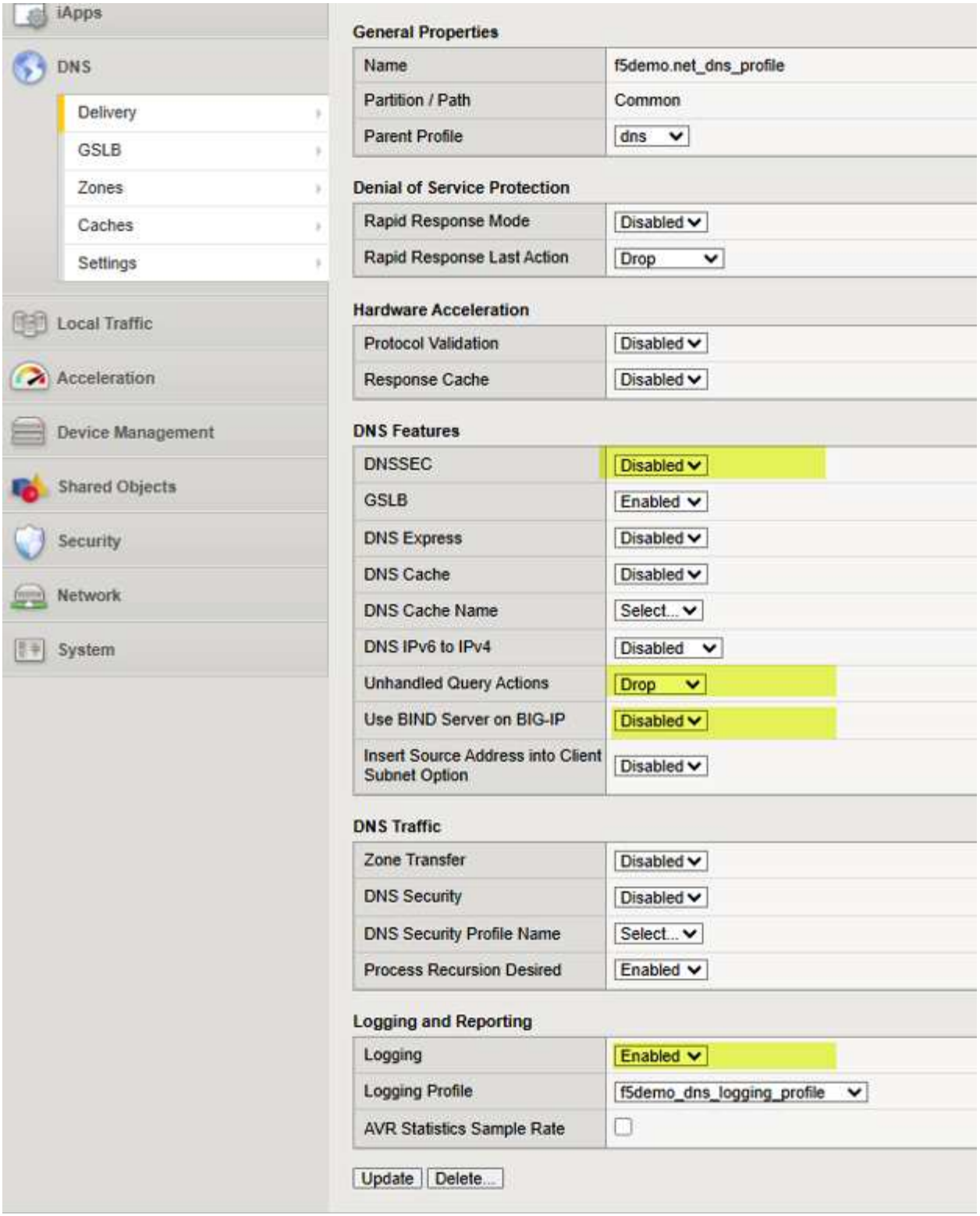


DNS 프로토콜 기본 요소 구성

StorageGRID 사이트의 글로벌 트래픽 관리를 위한 첫 번째 단계는 DNS 탭을 선택하는 것입니다. 여기에서 거의 모든 글로벌 트래픽 스티어링이 구성되며, 설정→GLSB를 선택합니다. 두 가지 동기화 옵션을 활성화하고 참여하는 BIG-IP 어플라이언스 간에 공유될 DNS 그룹 이름을 선택하십시오.



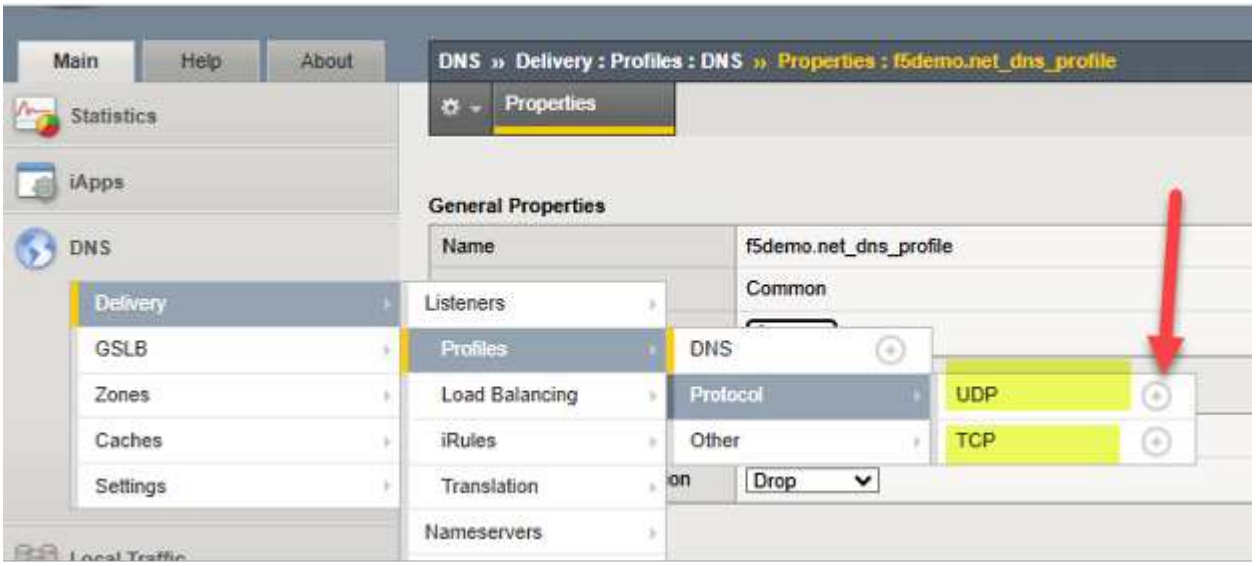
다음으로, DNS > 배달 > 프로필 > DNS: 생성으로 이동하여 활성화 또는 비활성화하려는 DNS 기능을 관리할 프로필을 생성합니다. 특정 DNS 로그 생성에 관심이 있다면 이전 링크의 DNS 교육 가이드를 참조하세요. 다음은 정상적으로 작동하는 DNS 프로필의 예입니다. 중요한 값을 나타내는 네 가지 강조 표시를 확인하십시오. 참고를 위해 각 설정에 대한 설명은 다음 F5 KB(지식 기반) 문서에서 확인할 수 있습니다. "여기".



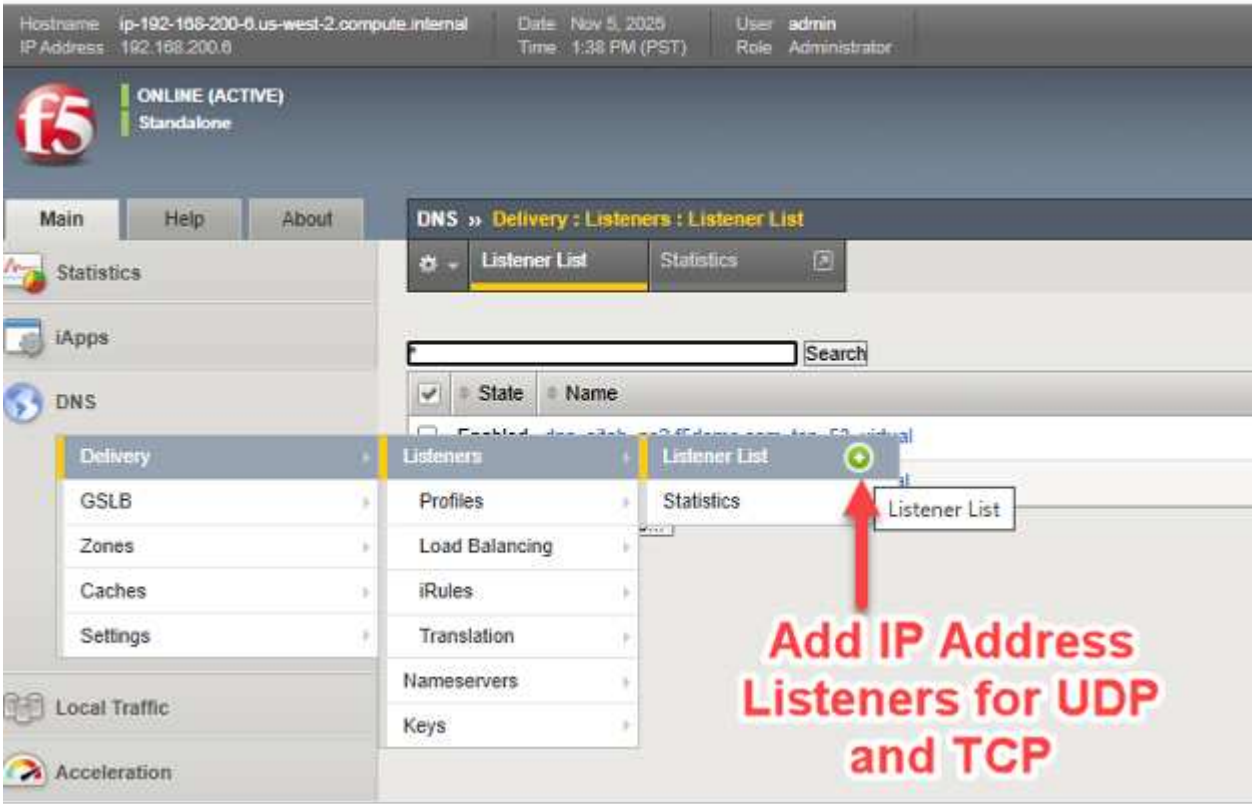
이 단계에서는 생성된 "프로필"을 통해 UDP 및 TCP 프로토콜의 특성을 조정할 수 있으며, 이 두 프로토콜 모두 BIG-IP와 관련된 DNS 트래픽을 처리할 수 있습니다. UDP와 TCP에 대해 각각 새로운 프로필을 하나씩 생성하기만 하면 됩니다. DNS 트래픽이 WAN 링크를 통과할 것이라고 가정할 때, WAN 환경에서 성능이 우수한 것으로 알려진 UDP 및 TCP 특성을 그대로 사용하는 것이 좋은 방법입니다. 각 프로토콜을 추가하려면 각 프로토콜 옆에 있는 "+" 아이콘을 클릭하고 상위 프로필을 다음과 같이 설정하십시오.

UDP → "상위" 프로필 "udp_gtm_dns" 사용

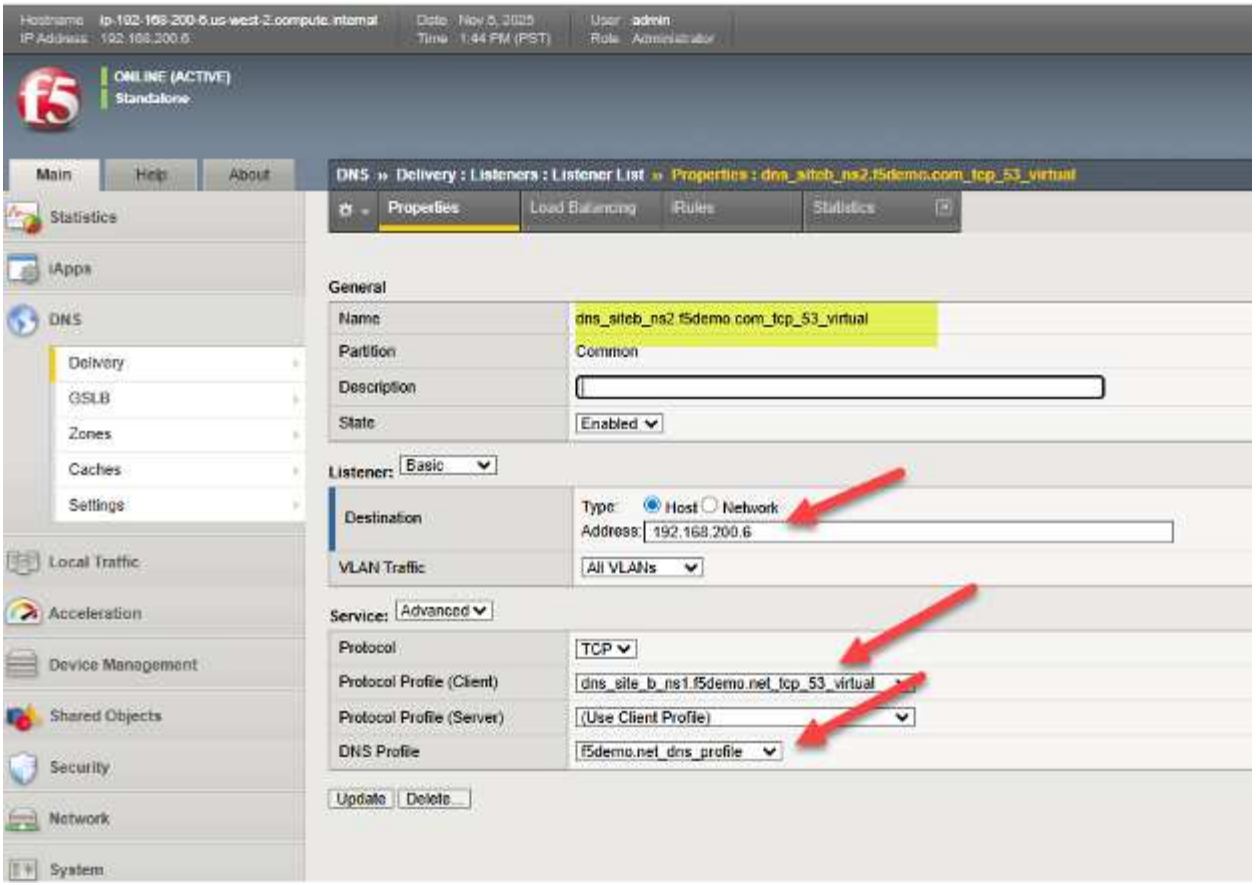
TCP → "상위" 프로필 "f5-tcp-wan" 사용



이제 BIG-IP DNS와 관련된 UDP 및 TCP 트래픽 모두에 IP 주소를 할당하기만 하면 됩니다. BIG-IP LTM에 익숙한 사람이라면 이것이 기본적으로 DNS 가상 서버를 생성하는 것이며, 가상 서버에는 "수신" IP 주소가 필요하다는 것을 알 것입니다. 스크린샷과 같이 화살표를 따라 DNS/UDP 및 DNS/TCP용 리스너/가상 서버를 생성하세요.



다음은 실제 BIG-IP DNS의 예시입니다. 여기에서 TCP 가상 서버 리스너 설정을 볼 수 있으며, 이 설정이 앞서 설명한 여러 단계와 어떻게 연결되는지 확인할 수 있습니다. 여기에는 DNS 프로필 및 프로토콜(TCP) 프로필을 참조하는 것과 DNS에서 사용할 유효한 IP 주소를 구성하는 것이 포함됩니다. BIG-IP로 생성하는 모든 객체와 마찬가지로, 예시로 제시된 dns/siteb/TCP53과 같이 객체가 무엇인지 명확하게 식별할 수 있는 의미 있는 이름을 사용하는 것이 좋습니다.



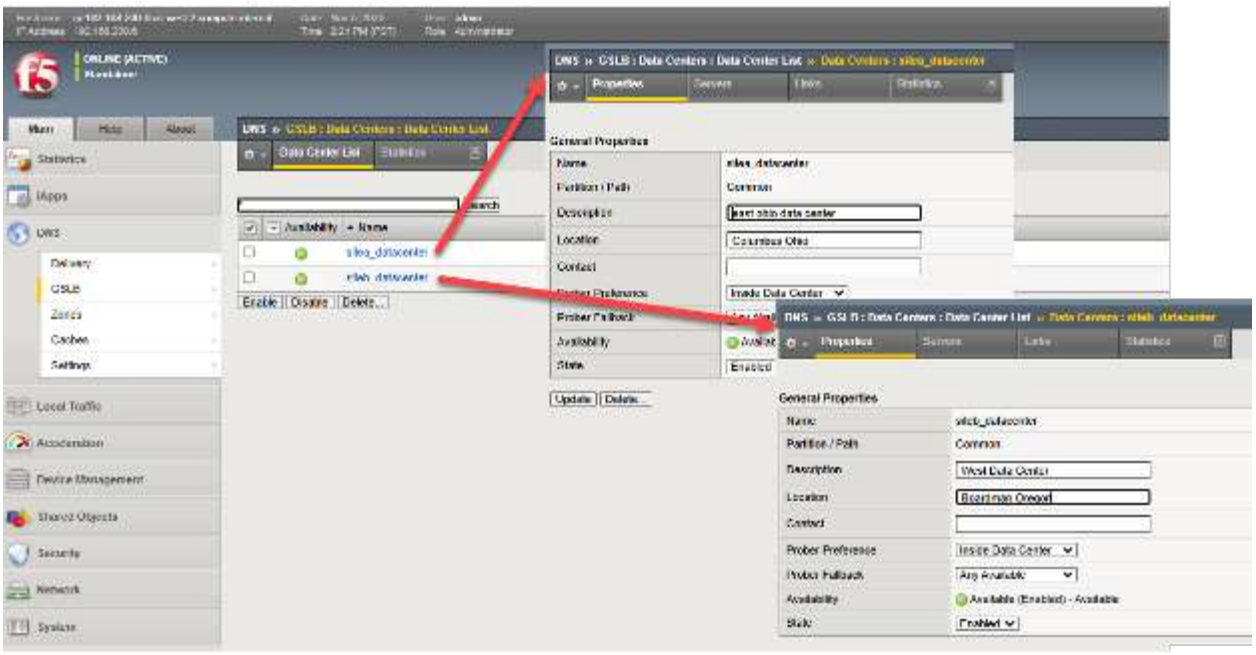
이것으로 DNS 모듈이 활성화된 BIG-IP 어플라이언스의 초기 설정 단계(일반적으로 한 번만 수행)가 완료되었습니다. 이제 저희는 어플라이언스를 사용하여 글로벌 트래픽 관리 솔루션을 설정하는 구체적인 단계로 넘어갈 준비가 되었습니다. 이 솔루션은 물론 StorageGRID 사이트의 특성과 연동될 것입니다.

데이터 센터 사이트 구축 및 **BIG-IP** 간 통신 설정 **4**단계

1단계**:** 데이터 센터 구축

BIG-IP LTM을 통해 로컬 로드 밸런싱을 받을 노드 클러스터를 호스팅할 각 사이트는 BIG-IP DNS에 입력해야 합니다. 이 작업은 하나의 BIG-IP DNS 서버에서만 수행하면 됩니다. 트래픽 관리를 지원하기 위해 DNS 동기화 그룹을 생성할 예정이며, 이 구성은 그룹의 DNS 구성원들 간에 공유됩니다.

TMUI GUI를 통해 DNS > GSLB > 데이터 센터 > 데이터 센터 목록을 선택하고 각 StorageGRID 사이트에 대한 항목을 생성합니다. 그림 1과 같이 네트워크 설정을 사용하는 경우, StorageGRID 사이트가 아닌 다른 사이트에 DNS 어플라이언스가 있다면 스토리지 사이트 외에 해당 사이트에 대한 데이터 센터를 추가하십시오. 이 예시에서는 사이트 a와 b가 오하이오와 오리건에 생성되었으며, BIG-IP는 듀얼 DNS 및 LTM 어플라이언스입니다.



2단계**:** 서버 생성 **(**솔루션에 포함된 모든 **BIG-IP** 어플라이언스 목록**)**

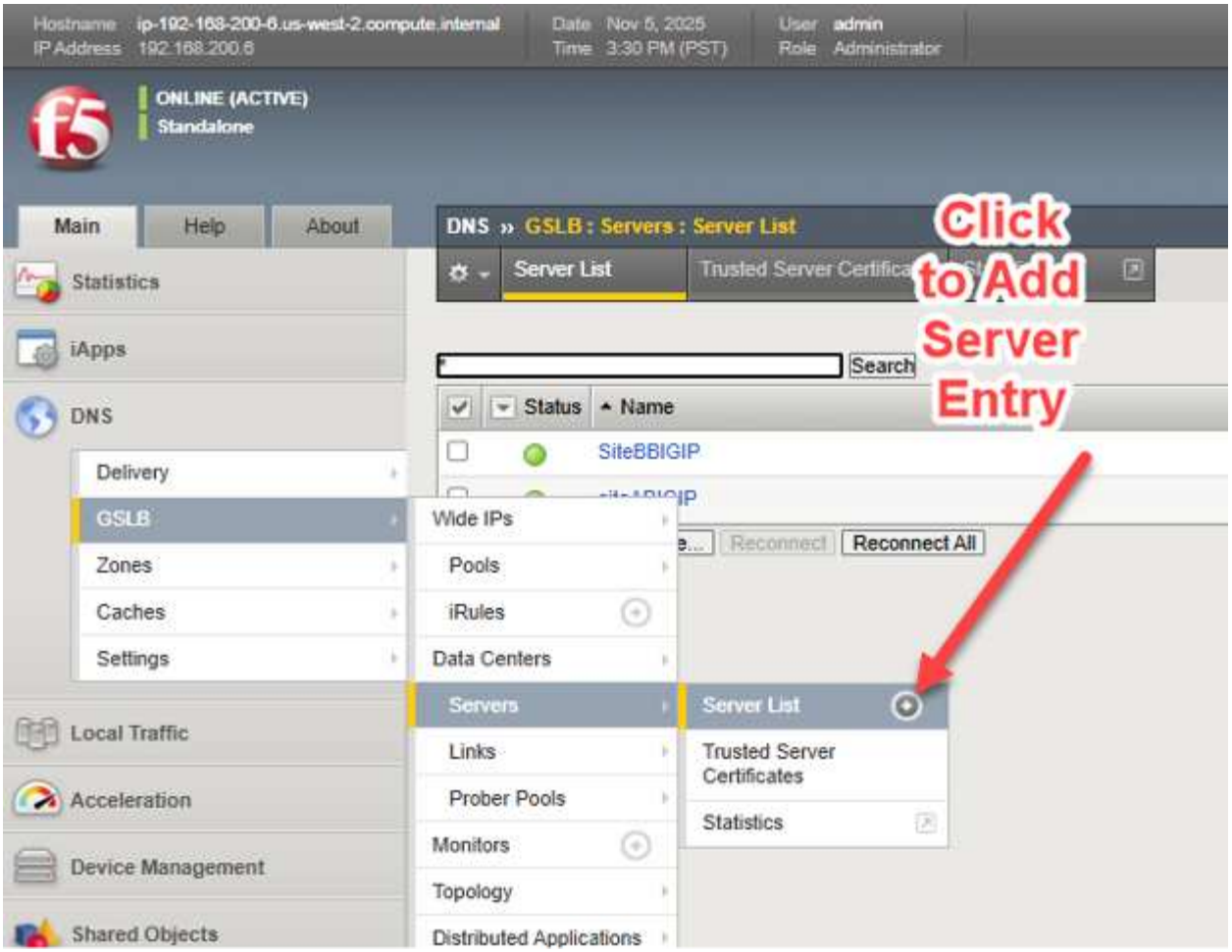
이제 각 StorageGRID 사이트 클러스터를 BIG-IP DNS 설정에 연결할 준비가 되었습니다. 앞서 언급했듯이, 각 사이트의 BIG-IP 어플라이언스는 "프런트엔드"에서 접근 가능한 IP 주소/포트를 "백엔드" IP 주소/포트를 사용하는 스토리지 노드 어플라이언스 "풀" 세트에 연결하는 가상 서버 구성을 통해 S3 트래픽의 실제 로드 밸런싱을 수행합니다.

예를 들어, 풀에 있는 모든 스토리지 노드가 사이트 폐쇄와 같은 관리상의 이유로 또는 예상치 못한 실시간 상태 점검 실패로 인해 오프라인 상태가 될 경우, DNS 쿼리 응답을 변경하여 트래픽을 다른 사이트로 리디렉션합니다.

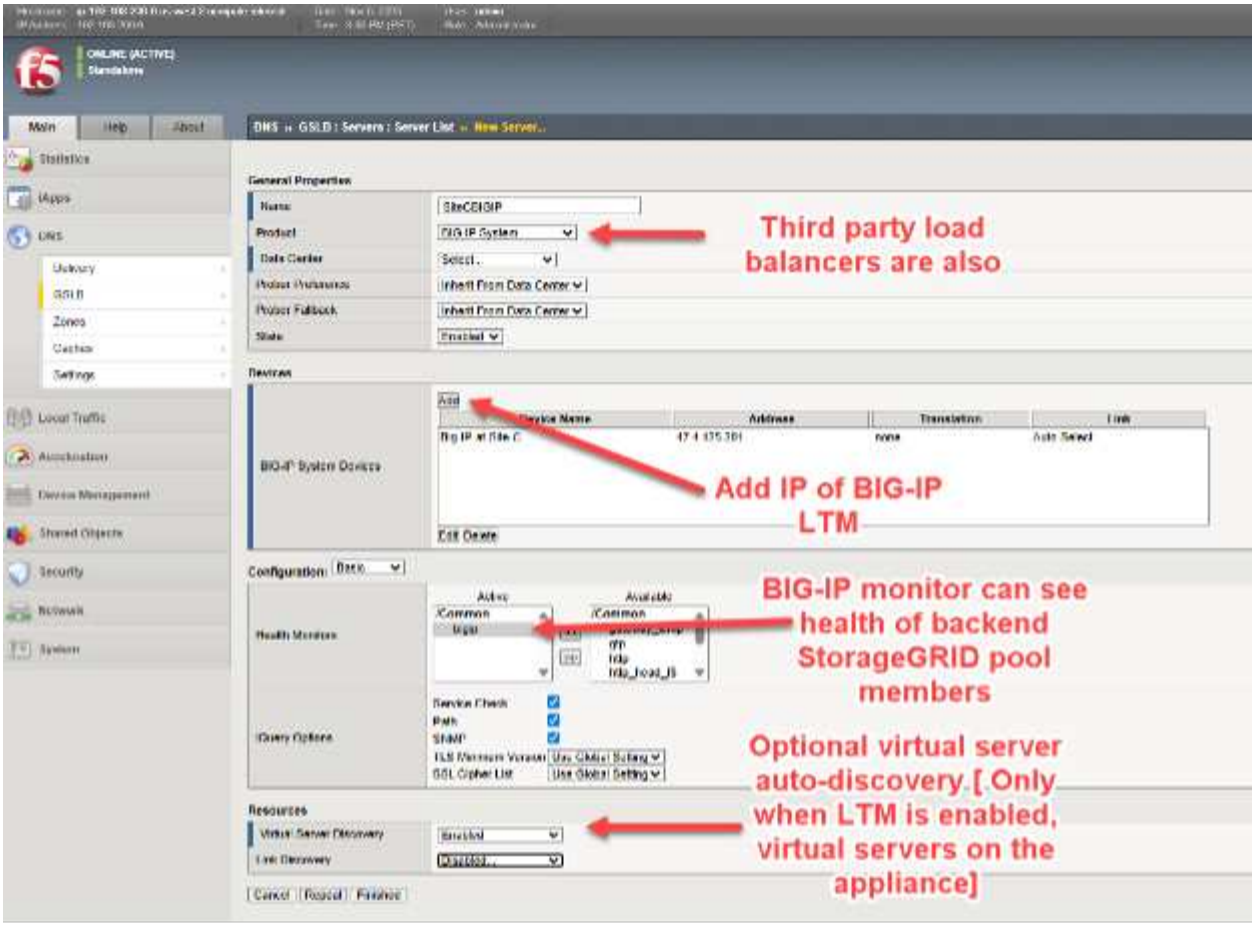
StorageGrid 사이트, 특히 로컬 가상 서버를 각 어플라이언스의 BIG-IP DNS 구성에 연결하려면 설정을 한 번만 수행하면 됩니다. 향후 단계에서 BIG-IP DNS 어플라이언스 전체 그룹의 설정이 동기화될 예정입니다.

간단히 말해, DNS, LTM 또는 DNS와 LTM 모두에 대한 라이선스를 보유한 모든 BIG-IP 어플라이언스의 목록(서버 목록이라고 함)을 생성할 것입니다. 이 마스터 목록은 목록 작성이 완료되면 모든 BIG-IP DNS 어플라이언스와 동기화됩니다.

BIG-IP DNS 라이선스가 있는 어플라이언스에서 DNS > GSLB > 서버 > 서버 목록을 선택하고 추가 버튼(+)을 선택합니다.



각 BIG-IP를 추가할 때 고려해야 할 네 가지 핵심 요소는 다음과 같습니다. * 제품 드롭다운 메뉴에서 BIG-IP를 선택합니다. 다른 로드 밸런서도 사용할 수 있지만, 일반적으로 각 사이트의 백엔드 노드 상태가 악화될 때 실시간 가시성과 대응력이 부족합니다. * BIG-IP DNS 어플라이언스의 IP 주소를 추가하십시오. 일반적으로 BIG-IP DNS 어플라이언스를 처음 추가할 때는 현재 GUI에서 액세스하는 어플라이언스의 주소가 사용되며, 이후에는 솔루션에 포함된 다른 어플라이언스의 주소가 사용됩니다. * 상태 모니터를 선택할 때는 로드 밸런서를 추가할 때 BIG-IP 어플라이언스를 사용하는 경우 백엔드 StorageGRID 노드 상태를 고려하기 위해 항상 "BIG-IP"를 사용하십시오. * 선택적으로, 어플라이언스가 듀얼 DNS/LTM 어플라이언스인 경우 가상 서버 자동 검색을 요청할 수 있습니다.

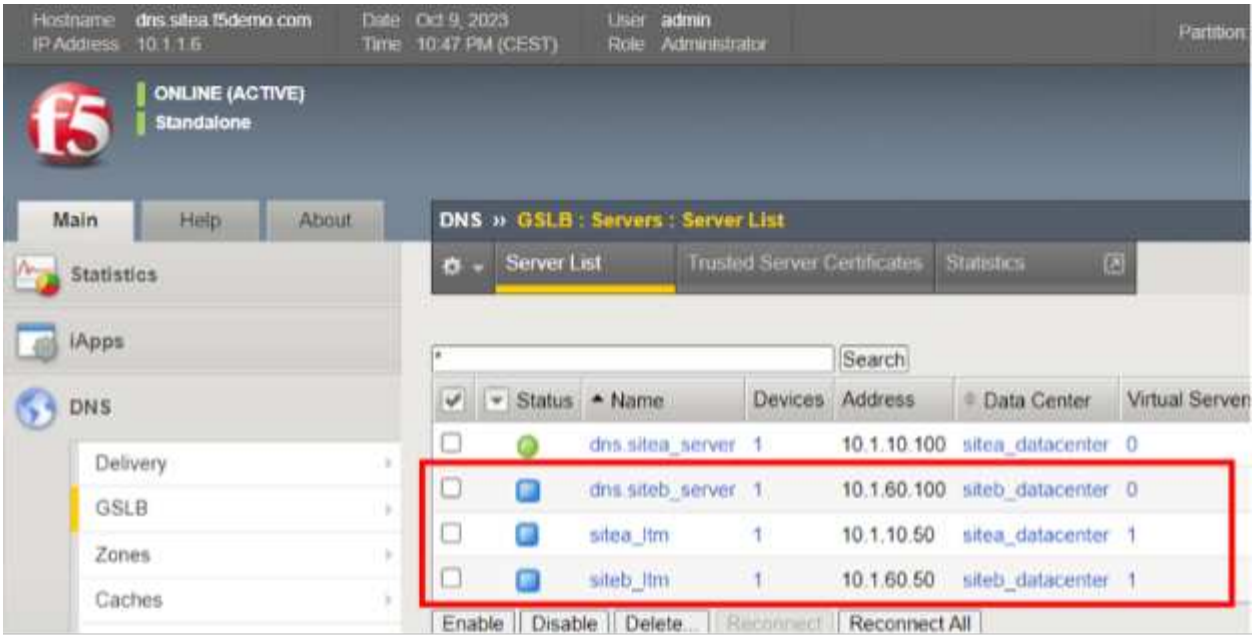


일시적인 네트워크 문제나 네트워크 위치 간 방화벽 ACL 규칙과 같은 일부 상황에서는 이 단계에서 원격 어플라이언스를 추가할 때 가상 서버 검색에서 LTM이 구성된 원격 어플라이언스에 대한 항목이 표시되지 않을 수 있습니다. 이러한 경우, 새 어플라이언스("서버")를 추가한 후 아래와 같이 가상 서버를 수동으로 추가할 수 있습니다. BIG-IP DNS 전용 어플라이언스를 추가하는 경우 해당 장치에서 검색되거나 추가될 가상 서버는 없습니다.

BIG-IP DNS 어플라이언스, BIG-IP LTM 어플라이언스, 그리고 DNS와 LTM 장치 역할을 모두 수행하는 모든 어플라이언스를 포함하여 솔루션의 각 어플라이언스에 대해 모든 사이트에 이러한 서버 항목을 추가해야 합니다.

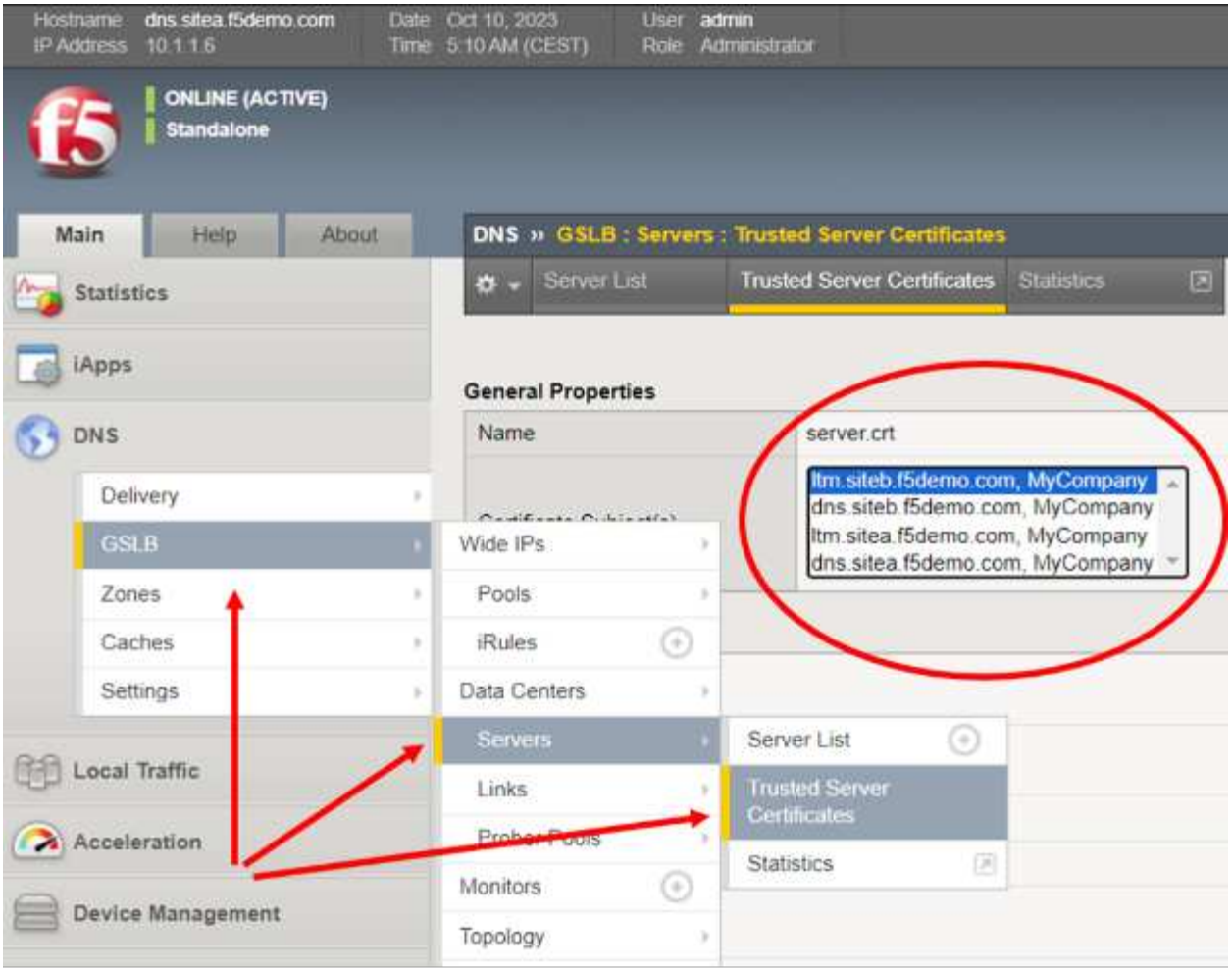
3단계**:** 모든 **BIG-IP** 장비 간의 신뢰 구축

다음 예시에서는 4개의 장비가 서버로 추가되었으며, 이 장비들은 두 개의 사이트에 분산되어 있습니다. 각 사이트에는 전용 BIG-IP DNS와 BIG-IP LTM이 있다는 점에 유의하십시오. 하지만 현재 로그인한 기기를 제외한 모든 기기의 " 상태" 열에 파란색 아이콘이 표시되고 있습니다. 이는 다른 BIG-IP 장비들과 아직 신뢰 관계가 구축되지 않았음을 의미합니다.



신뢰 관계를 추가하려면 방금 GUI를 통해 구성 세부 정보를 입력한 BIG-IP에 SSH로 접속한 다음 "root" 계정을 사용하여 BIG-IP 명령줄 인터페이스에 액세스하십시오. 명령 프롬프트에서 다음 단일 명령을 입력하십시오: *bigip_add*

"bigip_add" 명령은 클러스터 내 GSLB 서버 간 암호화된 "iQuery" 채널 설정에 사용할 관리 인증서를 대상 BIGIP 장치에서 가져옵니다. iQuery는 기본적으로 TCP 포트 4353을 사용하여 실행되며, BOG-IP DNS 구성원이 동기화된 상태를 유지할 수 있도록 하는 하트비트 역할을 합니다. 암호화 채널에서 XML과 gzip을 사용합니다. 옵션 없이 "bigip_add"를 실행하면 현재 사용자 이름을 사용하여 GSLB 서버 목록에 있는 모든 BIGIP 장치에 대해 명령이 실행되고 엔드포인트에 연결됩니다. 성공 여부를 빠르게 확인하려면 BIG-IP GUI로 돌아가서 표시되는 드롭다운 메뉴에 모든 서버의 인증서가 나열되어 있는지 확인하십시오.



4단계**:** 모든 **BIG-IP DNS** 어플라이언스를 **DNS** 그룹과 동기화합니다**.**

마지막 단계에서는 단일 장치의 TMUI GUI를 사용하여 모든 BIG-IP DNS 어플라이언스를 완벽하게 구성할 수 있게 됩니다. 예를 들어 StorageGRID 사이트가 두 개인 경우, 이제 SSH를 사용하여 다른 사이트의 BIG-IP DNS 명령줄에 접속해야 합니다. 루트 권한으로 접속한 후, 방화벽 정책/ACL에서 두 BIG-IP DNS 장치가 TCP 포트 22(SSH), 443(HTTPS) 및 4354(F5 iQuery 프로토콜)에서 통신할 수 있도록 허용했는지 확인하고, 명령 프롬프트에서 다음 명령어를 실행하십시오. *gtm_add* <이전에 모든 *GUI* 단계를 수행했던 첫 번째 사이트 *BIG-IP DNS*의 *IP* 주소>

이 시점부터 모든 추가 DNS 구성 작업은 그룹에 추가된 모든 BIG-IP DNS 어플라이언스에서 수행할 수 있습니다. 위의 명령인 gtm_add는 LTM 전용 어플라이언스 멤버에는 적용할 필요가 없습니다. DNS를 지원하는 장비만 동기화된 DNS 그룹에 포함되기 위해 이 명령이 필요합니다.

데이터 센터 사이트 구축 및 **BIG-IP** 간 통신 설정

이 시점에서 기본 BIG-IP DNS 어플라이언스 그룹을 정상적으로 생성하는 모든 단계가 완료되었습니다. 이제 각 StorageGRID 데이터센터에서 제공되는 분산 웹/S3 서비스를 가리키는 이름(FQDN)을 생성하는 작업을 진행할 수 있습니다.

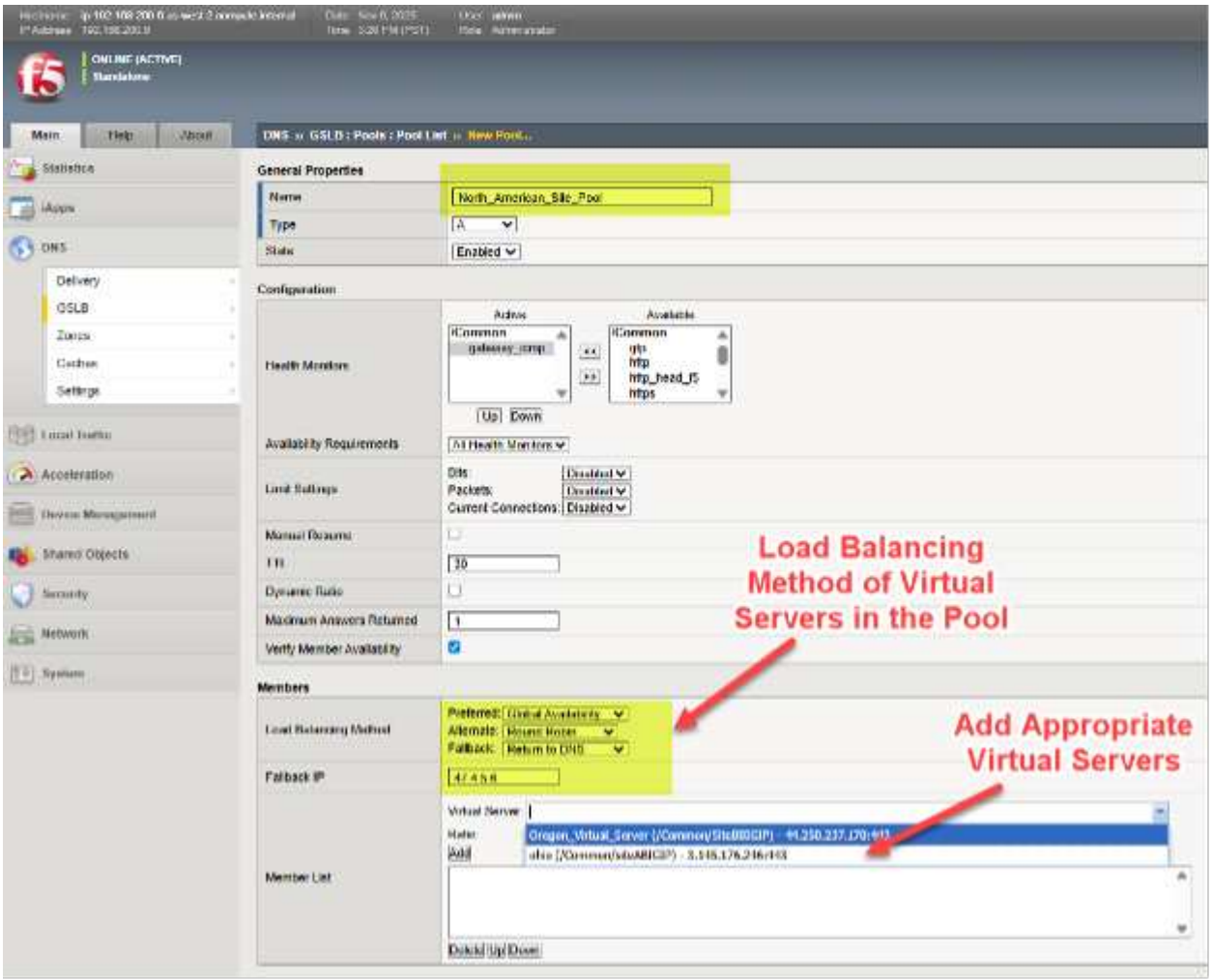
이러한 이름은 "와이드 IP" 또는 줄여서 WIP라고 하며, DNS A 리소스 레코드가 있는 일반 DNS FQDN입니다. 하지만 기존의 A 리소스 레코드처럼 서버를 직접 가리키는 대신, 내부적으로 BIG-IP 가상 서버 풀을 가리킵니다. 각 풀은 개별적으로 하나 이상의 가상 서버 세트로 구성될 수 있습니다. S3 클라이언트가 이름 확인을 위해 IP 주소를 요청하면 정책에 따라 선택된 최적의 StorageGRID 사이트에 있는 S3 가상 서버의 주소를 받게 됩니다.

간단하고 가상의 예를 들자면, *storage.quantumvault.com*이라는 이름에 대한 WIP(작업 진행 중) 프로젝트에서는 BIG-IP DNS 솔루션이 두 개의 잠재적 가상 서버 풀과 연결될 수 있습니다. 첫 번째 그룹은 북미 지역의 4개 사이트로 구성될 수 있고, 두 번째 그룹은 유럽 지역의 3개 사이트로 구성될 수 있습니다.

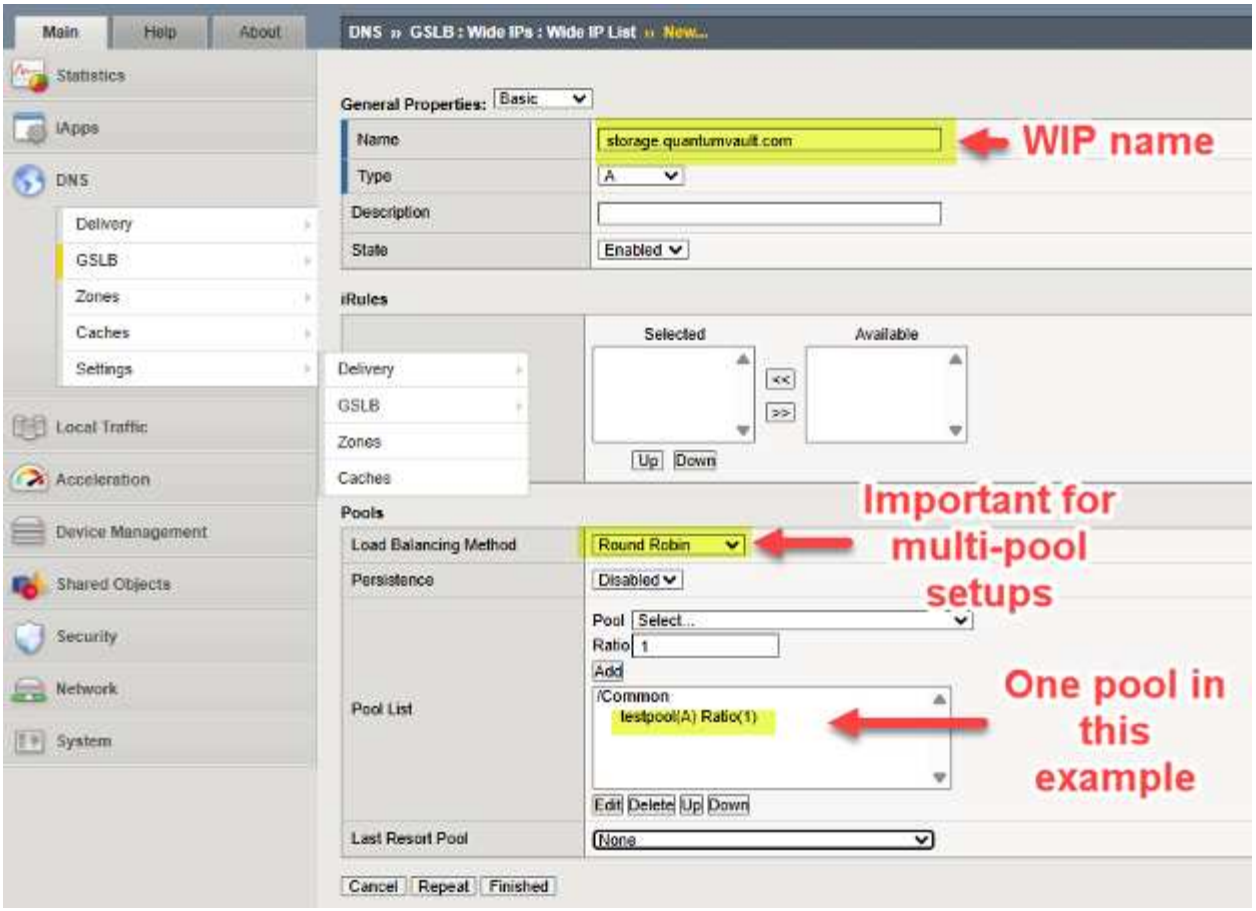
선택된 풀은 다양한 정책적 결정을 통해 도출될 수 있으며, 예를 들어 5:1의 간단한 비율을 사용하여 대부분의 트래픽을 북미 StorageGRID 사이트로 보낼 수 있습니다. 아마도 토폴로지 기반의 선택이 더 가능성이 높을 것입니다. 예를 들어, 유럽에서 발생하는 모든 S3 트래픽은 유럽 사이트로, 나머지 세계의 S3 트래픽은 북미 데이터 센터로 전달되도록 풀을 선택하는 방식입니다.

BIG-IP DNS에서 풀을 찾았다고 가정해 보겠습니다. 북미 풀이 선택되었다고 하면, storage.quantumvault.com을 확인하기 위해 반환되는 실제 DNS A 리소스 레코드는 북미 4개 사이트에 있는 BIG-IP LTM에서 지원하는 4개의 가상 서버 중 하나가 될 수 있습니다. 다시 말해, 어떤 방식을 선택할지는 정책에 따라 결정됩니다. 라운드 로빈과 같은 간단한 "정적" 접근 방식이 있는 반면, 각 사이트의 로컬 DNS 리졸버에서 지연 시간을 측정하는 성능 프로브와 같은 고급 "동적" 선택 방식이 유지 관리되고 사이트 선택 기준으로 사용됩니다.

BIG-IP DNS에서 가상 서버 풀을 설정하려면 **DNS > GSLB >** 풀 **>** 풀 목록 **>** 추가**(+)** 메뉴 경로를 따르십시오. 이 예시에서는 다양한 북미 가상 서버가 풀에 추가되고, 이 풀이 선택될 경우 계층형 로드 밸런싱 방식이 선호되는 것을 볼 수 있습니다.



DNS에서 확인될 서비스 이름인 WIP(Wide IP)를 배포에 추가하려면 DNS > GSLB > Wide IPs > Wide IP List > Create (+) 경로를 따릅니다. 다음 예시에서는 S3 지원 스토리지 서비스의 개발 중인 예시를 제공합니다.



글로벌 트래픽 관리를 지원하도록 **DNS**를 조정합니다**.**

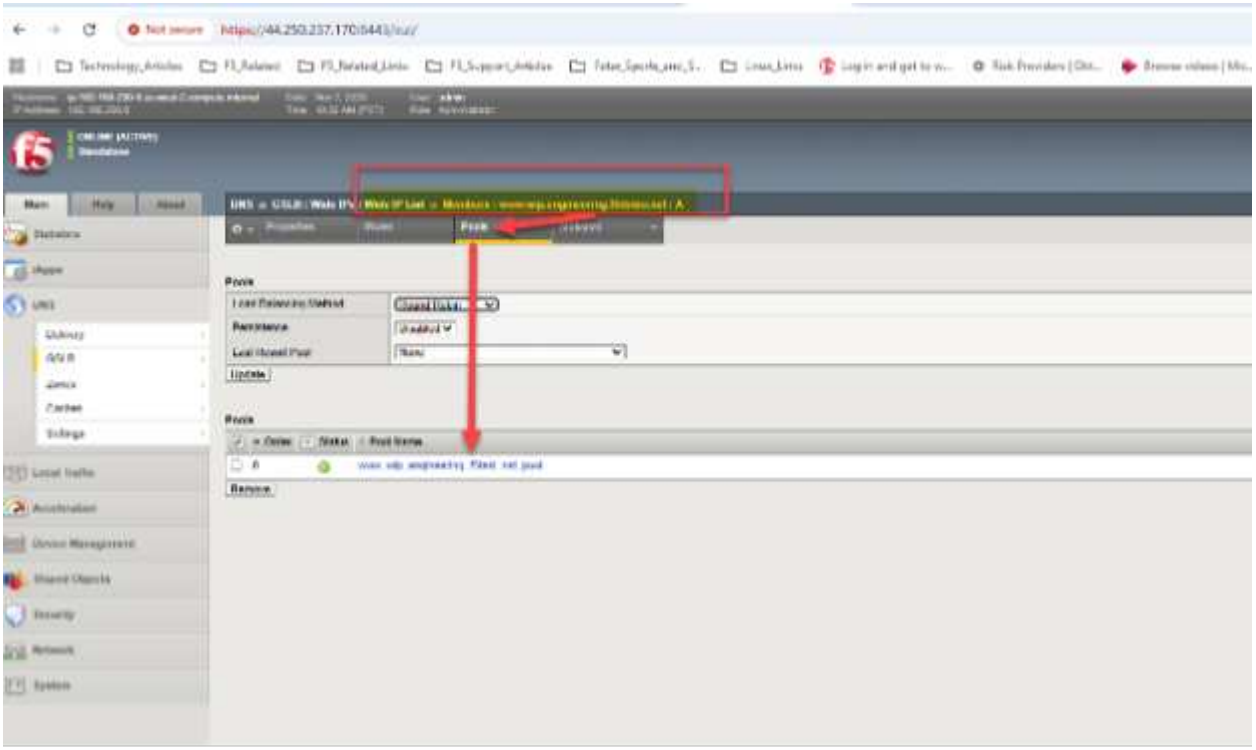
현재 모든 기본 BIG-IP 어플라이언스가 GSLB(글로벌 서버 로드 밸런싱)를 수행할 준비가 되었습니다. 솔루션을 활용하려면 S3 트래픽 흐름에 사용되는 이름을 조정하고 할당하기만 하면 됩니다. 일반적인 접근 방식은 기업의 기존 DNS 도메인 일부를 BIG-IP DNS의 제어에 위임하는 것입니다. 즉, 네임스페이스의 일부, 즉 서브도메인을 "분리"하고 이 서브도메인의 제어권을 BIG-IP DNS 어플라이언스에 위임하는 것입니다. 기술적으로 이는 BIG-IP DNS 어플라이언스가 엔터프라이즈 DNS에 A DNS 리소스 레코드(RR)를 갖도록 한 다음 이러한 이름/주소를 위임된 도메인에 대한 네임 서버(NS) DNS 리소스 레코드로 만듦으로써 수행됩니다.

오늘날 기업들이 DNS를 관리하는 방법은 다양하며, 그중 하나가 완전 호스팅 솔루션입니다. 예를 들어 Windows Server 2025를 통해 DNS를 운영하고 관리하는 것이 이에 해당합니다. 또 다른 접근 방식으로는 기업이 AWS Route53 또는 Squarespace와 같은 클라우드 DNS 제공업체를 활용하는 것이 있습니다.

이해를 돕기 위한 가상의 예시를 들어보겠습니다. 저희는 AWS Route53에서 관리하는 기존 도메인(예시 도메인: f5demo.net)을 통해 S3 프로토콜로 객체 읽기/쓰기를 지원하는 StorageGRID 사용하고 있습니다.

글로벌 트래픽 관리를 위해 engineering.f5demo.net 서브도메인을 BIG-IP DNS 어플라이언스에 할당하고자 합니다. 이를 위해 engineering.f5demo.net에 대한 새로운 NS(네임 서버) 리소스 레코드를 생성하고 해당 레코드를 BIG-IP DNS 어플라이언스 이름 목록으로 지정합니다. 예시에서 우리는 두 대의 BIG-IP DNS 어플라이언스를 보유하고 있으므로, 각각에 대해 두 개의 A 리소스 레코드를 생성합니다.

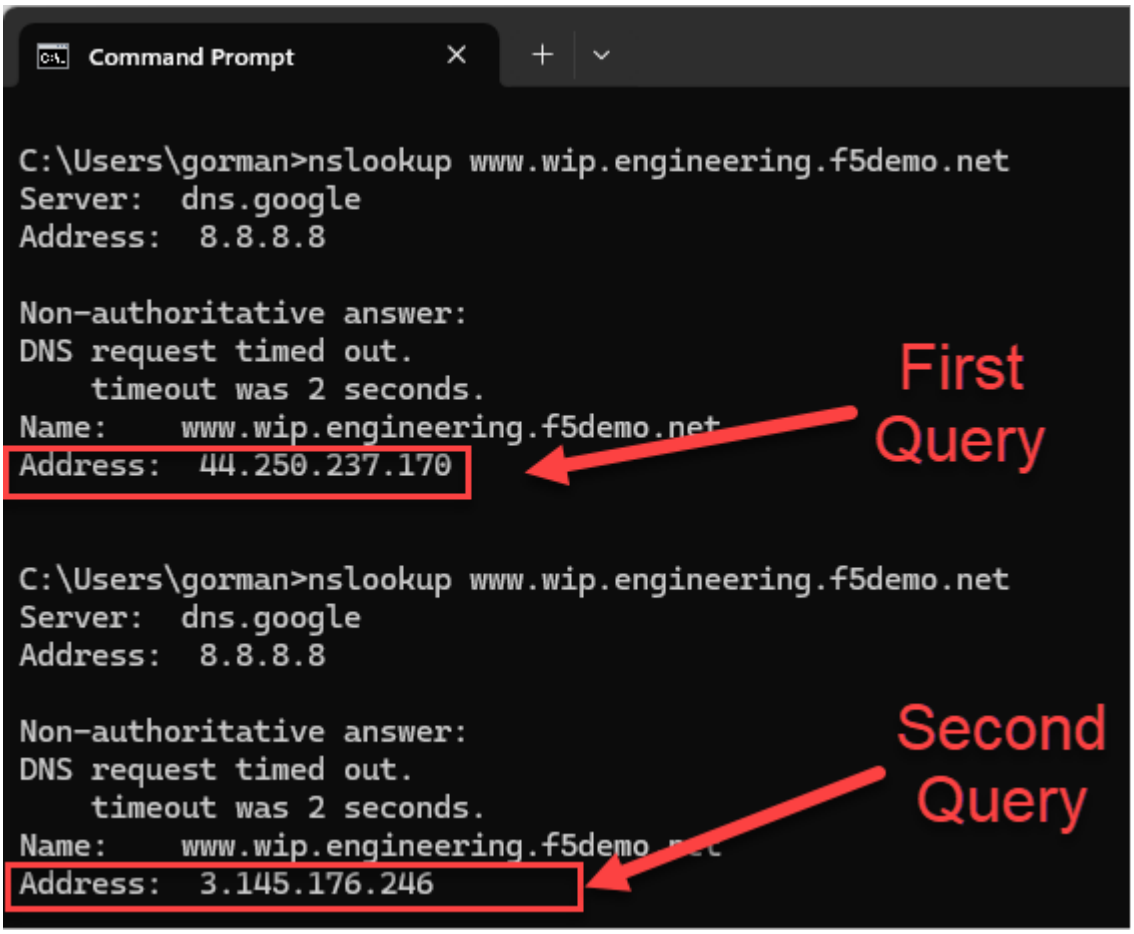
이제 예시로 BIG-IP DNS에 Wide IP(WIP)를 설정해 보겠습니다. DNS는 그룹 동기화를 사용하므로 하나의 어플라이언스 GUI에서만 조정하면 됩니다. BIG-IP DNS GUI에서 *DNS > GSLB > Wide IPs > Wide IP List (+)*로 이동합니다. 기존 DNS FQDN 설정에서는 하나 이상의 IPv4 주소를 입력해야 하지만, 저희의 경우에는 하나 이상의 StorageGRID 가상 서버 풀을 가리키기만 하면 됩니다.



예시에서 우리는 오하이오와 오리건 두 지역에 일반 웹 HTTPS 서버를 두고 있습니다. 간단한 "라운드 로빈" 방식을 사용하면 글로벌 DNS가 두 가상 서버 IP 모두를 사용하여 _www.wip.engineering.f5demo.net_에 대한 A 리소스 레코드 매핑 쿼리에 응답하는 것을 확인할 수 있습니다.

간단한 테스트는 웹 브라우저를 사용하거나, StorageGRID 사용하는 S3의 경우 S3Browser와 같은 그래픽 도구를 사용하여 수행할 수 있습니다. DNS 쿼리가 실행될 때마다, 해당 풀에서 라운드 로빈 방식을 선택했기 때문에 다음 트래픽의 대상으로 사용되는 데이터 센터 사이트가 선택됩니다.

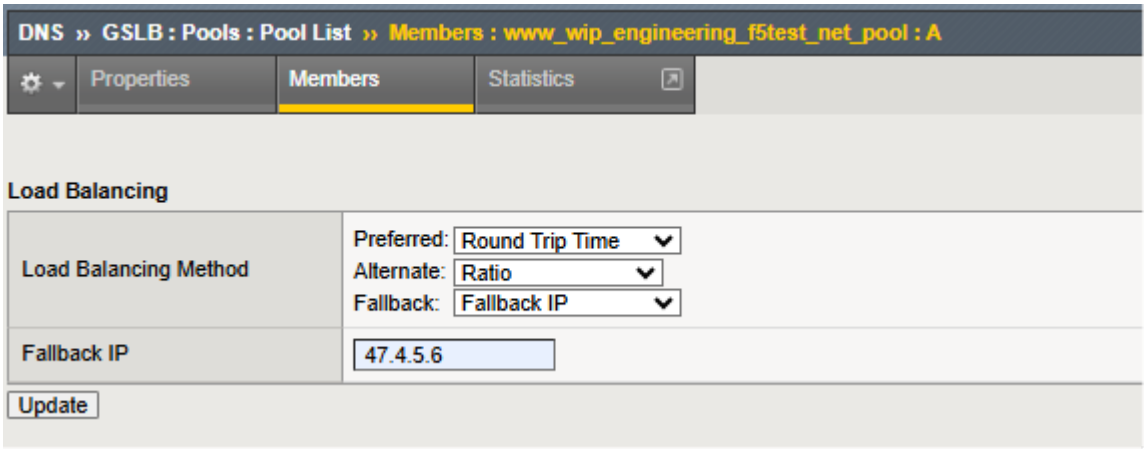
예시 설정에서 dig 또는 nslookup을 사용하여 두 개의 DNS 쿼리를 신속하게 생성하고 BIG-IP DNS가 실제로 라운드 로빈 로드 밸런싱을 수행하여 두 사이트 모두 시간에 따라 트래픽을 수신하는지 확인할 수 있습니다.



보다 고급 기술에 대한 탐색을 제안합니다.

가능한 접근 방식 중 하나는 위에서 제시한 단순한 "라운드 로빈" 예시 대신 "전역 가용성" 모드를 사용하는 것입니다. 글로벌 가용성을 사용하면 풀의 순차적 순서 또는 단일 풀 내의 가상 서버 순서에 따라 트래픽을 해당 풀로 전달할 수 있습니다. 이러한 방식으로 모든 S3 트래픽은 기본적으로 예를 들어 뉴욕시 사이트로 향하도록 설정될 수 있습니다.

상태 점검 결과 해당 사이트의 StorageGRID 노드 가용성에 문제가 있는 것으로 나타나면, 트래픽은 세인트루이스로 우회될 수 있습니다. 세인트루이스에서 건강 관련 문제가 발생할 경우, 프랑크푸르트에 있는 사이트가 S3 읽기 또는 쓰기 트랜잭션을 수신할 수 있습니다. 따라서 글로벌 가용성은 S3 StorageGRID 솔루션 전체의 복원력을 확보하는 한 가지 접근 방식입니다. 또 다른 접근 방식은 계층형 접근 방식을 사용하는 등 다양한 로드 밸런싱 방식을 혼합하여 사용하는 것입니다.



이 예시에서 "동적" 옵션은 구성된 풀에 있는 사이트에 대한 첫 번째 로드 밸런싱 선택 사항입니다. 예시에서 보여지는 것처럼, 로컬 DNS 리졸버 성능에 대한 능동적인 프로빙을 사용하는 지속적인 측정 접근 방식이 유지되며, 이는 사이트 선정의 촉매제가 됩니다. 이러한 접근 방식을 사용할 수 없는 경우, 각 부지에 할당된 비율에 따라 개별 부지를 선택할 수 있습니다. 비율에 따라 규모가 크고 대역폭이 높은 StorageGRID 사이트는 규모가 작은 사이트보다 더 많은 S3 트랜잭션을 처리할 수 있습니다. 마지막으로, 재해 복구 시나리오를 염두에 두고 풀에 있는 모든 사이트가 비정상 상태가 될 경우 지정된 대체 IP가 최후의 수단으로 사용됩니다. BIG-IP DNS의 흥미로운 로드 밸런싱 방법 중 하나는 " 토폴로지"입니다. 이 방법은 DNS 쿼리의 수신 소스인 S3 사용자의 로컬 DNS 확인자를 관찰하고 인터넷 토폴로지 정보를 사용하여 풀에서 가장 "가까운" 사이트를 선택합니다.

마지막으로, 사이트가 전 세계에 걸쳐 있는 경우 F5 BIG-IP DNS 설명서에 자세히 설명된 동적 "프로브" 기술을 사용하는 것을 고려해 볼 만합니다. 프로브를 사용하면 빈번하게 발생하는 DNS 쿼리 소스를 모니터링할 수 있습니다. 예를 들어, 트래픽이 일반적으로 동일한 로컬 DNS 리졸버를 사용하는 기업 간 파트너를 생각해 볼 수 있습니다. BIG-IP DNS 프로브는 전 세계 각 사이트의 BIG-IP LTM에서 실행하여 S3 트랜잭션에 대해 가장 낮은 지연 시간을 제공할 가능성이 높은 사이트를 대략적으로 파악할 수 있습니다. 따라서 아시아 지역의 트래픽은 북미나 유럽에 위치한 StorageGRID 사이트보다 아시아에 위치한 사이트에서 더 효율적으로 처리될 수 있습니다.

결론

F5 BIG-IP와 NetApp StorageGRID 의 통합은 여러 사이트에 걸쳐 데이터 가용성과 일관성을 유지하고 S3 트랜잭션 라우팅을 최적화하는 것과 관련된 기술적 문제를 해결합니다. 이 솔루션을 도입하면 스토리지의 복원력, 성능 및 안정성이 향상되어 강력하고 확장 가능하며 유연한 스토리지 인프라를 구축하고자 하는 기업에 이상적입니다.

더 자세한 내용을 알아보려면 F5의 BIG-IP DNS 공식 문서를 여기에서 확인할 수 있습니다. "링크". 단계별 지침을 제공하는 수업 운영 가이드도 함께 제공됩니다. "여기".

Datadog SNMP 구성

_ 아론 클라인 _

StorageGRID SNMP 메트릭 및 트랩을 수집하도록 데이터 독을 구성합니다.

데이터 독을 구성합니다

Datadog는 메트릭, 시각화 및 알림을 제공하는 모니터링 솔루션입니다. 다음 구성은 Ubuntu 22.04.1 호스트에서 Linux 에이전트 버전 7.43.1을 사용하여 StorageGRID 시스템에 로컬로 배포되었습니다.

StorageGRID MIB 파일에서 생성된 **Datadog** 프로파일 및 트랩 파일입니다

Datadog는 제품 MIB 파일을 SNMP 메시지를 매핑하는 데 필요한 datadog 참조 파일로 변환하는 방법을 제공합니다.

발견된 지침에 따라 생성된 데이터 독그 트랩 해결 매핑에 대한 StorageGRID YAML 파일입니다 "여기". +이 파일을 /etc/datadog-agent/conf.d/snmp.d/trap_db/+에 넣습니다

- "TRAP YAML 파일을 다운로드합니다" 를 누릅니다
  - * MD5 체크섬 * 42e27e4210719945a46172b98c379517+
  - * SHA256 checksum * d0f5c8e6c3c902d054f854b70a85f928cba8b7c76391d356f05d2cf73b6887+

이 StorageGRID 프로필 YAML 파일은 발견된 지침에 따라 생성된 데이터 독그 메트릭 매핑에 대해 생성됩니다 "여기". +이 파일을 /etc/datadog-agent/conf.d/snmp.d/profiles/+에 넣습니다

- "YAML 프로필 파일을 다운로드합니다" 를 누릅니다
  - * MD5 체크섬 * 72bb7784f4801adda4e0c3ea77df19aa+
  - * SHA256 체크섬 * b6b7fadd33063422a8b8e39b3ead8ab38349ee0229926eadc8585f0087b8cee+

메트릭의 **SNMP** 데이터 독이 구성됩니다

메트릭에 대한 SNMP 구성은 두 가지 방법으로 관리할 수 있습니다. StorageGRID 시스템이 포함된 네트워크 주소 범위를 제공하거나 개별 장치의 IP를 정의하여 자동 검색을 구성할 수 있습니다. 구성 위치는 결정에 따라 다릅니다. 자동 검색은 데이터 로그 에이전트 YAML 파일에서 정의됩니다. 명시적 장치 정의는 SNMP 구성 YAML 파일에 구성되어 있습니다. 다음은 동일한 StorageGRID 시스템에 대한 각 의 예입니다.

자동 검색

구성은 /etc/datadog-agent/datadog.YAML에 있습니다

```
listeners:
  - name: snmp
snmp_listener:
  workers: 100  # number of workers used to discover devices concurrently
  discovery_interval: 3600  # interval between each autodiscovery in
seconds
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
  configs:
    - network_address: 10.0.0.0/24  # CIDR subnet
      snmp_version: 2
      port: 161
      community_string: 'st0r@gegrid'  # enclose with single quote
      profile: netapp-storagegrid
```

개별 장치

/etc/datadog-agent/conf.d/snmp.d/conf.yaML

```
init_config:
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
instances:
- ip_address: '10.0.0.1'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'  # enclose with single quote
- ip_address: '10.0.0.2'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
- ip_address: '10.0.0.3'
  profile: netapp-storagegrid
 community_string: 'st0r@gegrid'
- ip_address: '10.0.0.4'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
```

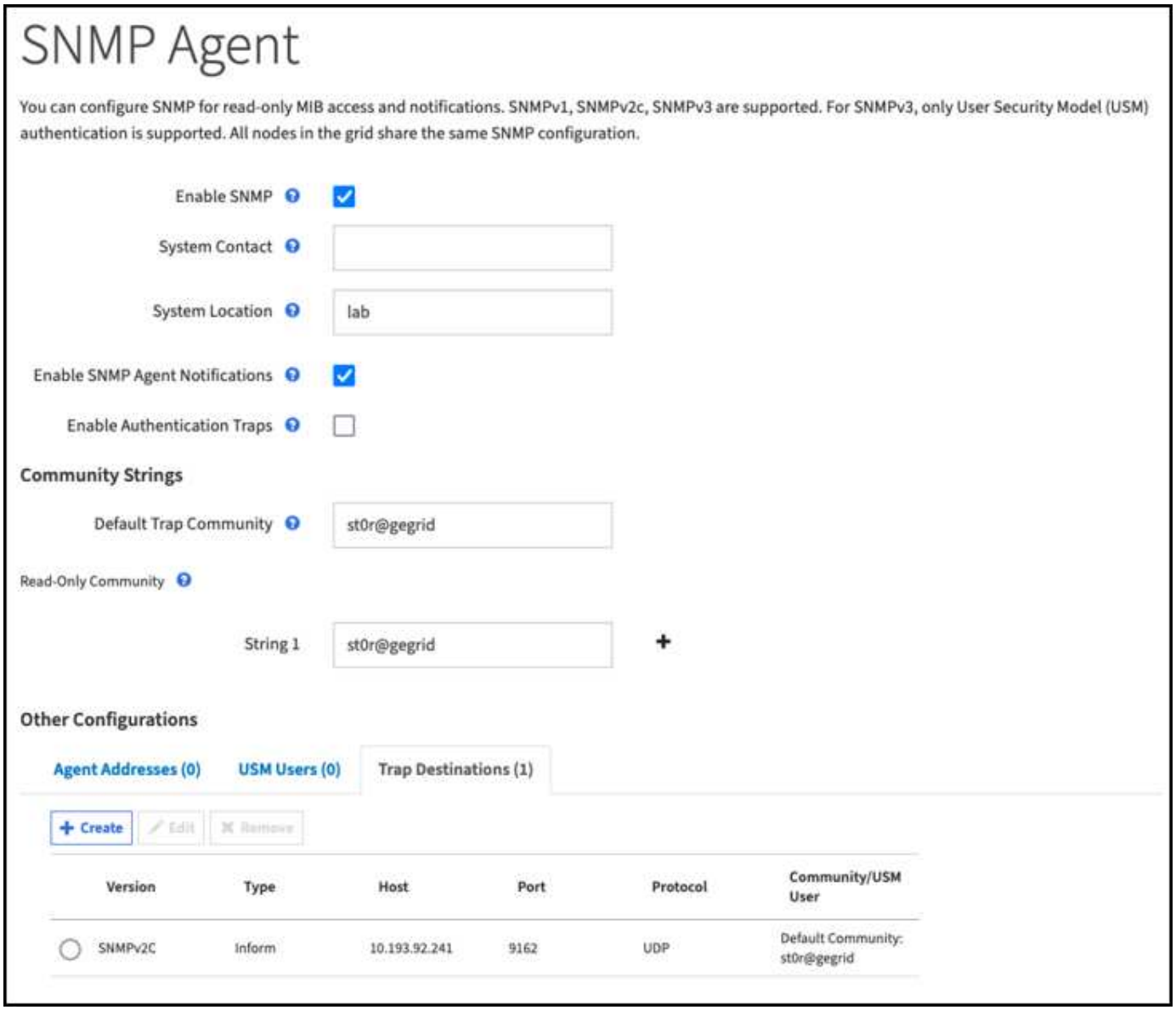
트랩에 대한 **SNMP** 구성

SNMP 트랩에 대한 구성은 datadog 구성 YAML 파일 /etc/datadog-agent/datadog.YAML에서 정의됩니다

```
network_devices:
  namespace:  # optional, defaults to "default".
  snmp_traps:
    enabled: true
    port: 9162 # on which ports to listen for traps
    community_strings: # which community strings to allow for v2 traps
      - st0r@gegrid
```

StorageGRID SNMP 구성의 예

StorageGRID 시스템의 SNMP 에이전트는 구성 탭, 모니터링 열 아래에 있습니다. SNMP를 활성화하고 원하는 정보를 입력합니다. 트랩을 구성하려면 "트랩 대상"을 선택하고 트랩 구성을 포함하는 데이터 독그 에이전트 호스트의 대상을 생성합니다.



rclone을 사용하여 StorageGRID에서 개체를 마이그레이션, 저장 및 삭제합니다

지그프리드 헤프와 아론 클라인 작사

rclone은 S3 작업을 위한 무료 명령줄 도구 및 클라이언트입니다. rclone을 사용하여 StorageGRID에서 오브젝트 데이터를 마이그레이션, 복사, 삭제할 수 있습니다. rclone에는 아래 예와 같이 "퍼지" 기능을 사용하여 비어 있지 않은 경우에도 버킷을 삭제할 수 있는 기능이 포함되어 있습니다.

rclone을 설치하고 구성합니다

워크스테이션 또는 서버에 rclone을 설치하려면 에서 다운로드하십시오 "rclone.org".

초기 구성 단계

1. config 스크립트를 실행하거나 수동으로 파일을 생성하여 rclone 구성 파일을 생성합니다.
2. 이 예에서는 rclone 구성에서 원격 StorageGRID S3 엔드포인트 이름에 sgdemo를 사용합니다.
   a. 구성 파일 ~/.config/rclone/rclone.conf를 생성합니다

```
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com
```

   b. rclone 구성을 실행합니다

rclone config

```
2023/04/13 14:22:45 NOTICE: Config file
"/root/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> sgdemo
```

```
Option Storage.
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Providers including AWS,
Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio,
SeaweedFS, and Tencent COS
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Better checksums for other remotes
   \ "hasher"
 7 / Box
   \ "box"
 8 / Cache a remote
   \ "cache"
 9 / Citrix Sharefile
   \ "sharefile"
10 / Compress a remote
   \ "compress"
11 / Dropbox
   \ "dropbox"
12 / Encrypt/Decrypt a remote
   \ "crypt"
13 / Enterprise File Fabric
   \ "filefabric"
14 / FTP Connection
```

```
   \ "ftp"
15 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
16 / Google Drive
   \ "drive"
17 / Google Photos
   \ "google photos"
18 / Hadoop distributed file system
   \ "hdfs"
19 / Hubic
   \ "hubic"
20 / In memory object storage system.
   \ "memory"
21 / Jottacloud
   \ "jottacloud"
22 / Koofr
   \ "koofr"
23 / Local Disk
   \ "local"
24 / Mail.ru Cloud
   \ "mailru"
25 / Mega
   \ "mega"
26 / Microsoft Azure Blob Storage
   \ "azureblob"
27 / Microsoft OneDrive
   \ "onedrive"
28 / OpenDrive
   \ "opendrive"
29 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore,
OVH)
   \ "swift"
30 / Pcloud
   \ "pcloud"
31 / Put.io
   \ "putio"
32 / QingCloud Object Storage
   \ "qingstor"
33 / SSH/SFTP Connection
   \ "sftp"
34 / Sia Decentralized Cloud
   \ "sia"
35 / Sugarsync
   \ "sugarsync"
36 / Tardigrade Decentralized Cloud Storage
   \ "tardigrade"
```

```
37 / Transparently chunk/split large files
   \ "chunker"
38 / Union merges the contents of several upstream fs
   \ "union"
39 / Uptobox
   \ "uptobox"
40 / Webdav
   \ "webdav"
41 / Yandex Disk
   \ "yandex"
42 / Zoho
   \ "zoho"
43 / http Connection
   \ "http"
44 / premiumize.me
   \ "premiumizeme"
45 / seafile
   \ "seafile"
```

```
Storage> 4
```

```
Option provider.
Choose your S3 provider.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / Amazon Web Services (AWS) S3
   \ "AWS"
 2 / Alibaba Cloud Object Storage System (OSS) formerly Aliyun
   \ "Alibaba"
 3 / Ceph Object Storage
   \ "Ceph"
 4 / Digital Ocean Spaces
   \ "DigitalOcean"
 5 / Dreamhost DreamObjects
   \ "Dreamhost"
 6 / IBM COS S3
   \ "IBMCOS"
 7 / Minio Object Storage
   \ "Minio"
 8 / Netease Object Storage (NOS)
   \ "Netease"
 9 / Scaleway Object Storage
   \ "Scaleway"
10 / SeaweedFS S3
   \ "SeaweedFS"
11 / StackPath Object Storage
   \ "StackPath"
12 / Tencent Cloud Object Storage (COS)
   \ "TencentCOS"
13 / Wasabi Object Storage
   \ "Wasabi"
14 / Any other S3 compatible provider
   \ "Other"
provider> 14
```

```
Option env_auth.
Get AWS credentials from runtime (environment variables or
EC2/ECS meta data if no env vars).
Only applies if access_key_id and secret_access_key is blank.
Enter a boolean value (true or false). Press Enter for the
default ("false").
Choose a number from below, or type in your own value.
 1 / Enter AWS credentials in the next step.
   \ "false"
 2 / Get AWS credentials from the environment (env vars or IAM).
   \ "true"
env_auth> 1
```

```
Option access_key_id.
AWS Access Key ID.
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
access_key_id> ABCDEFGH123456789JKL
```

```
Option secret_access_key.
AWS Secret Access Key (password).
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
secret_access_key> 123456789ABCDEFGHIJKLMN0123456789PQRST+V
```

```
Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a
region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Use this if unsure.
 1 | Will use v4 signatures and an empty region.
   \ ""
   / Use this only if v4 signatures don't work.
 2 | E.g. pre Jewel/v10 CEPH.
   \ "other-v2-signature"
region> 1
```

```
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> sgdemo.netapp.com
```

```
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
location_constraint>
```

```
Option acl.
Canned ACL used when creating buckets and storing or copying
objects.
This ACL is used for creating objects and if bucket_acl isn't
set, for creating buckets too.
For more info visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-
overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as
S3
doesn't copy the ACL from the source but rather writes a fresh
one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Owner gets FULL_CONTROL.
 1 | No one else has access rights (default).
   \ "private"
   / Owner gets FULL_CONTROL.
 2 | The AllUsers group gets READ access.
   \ "public-read"
   / Owner gets FULL_CONTROL.
 3 | The AllUsers group gets READ and WRITE access.
   | Granting this on a bucket is generally not recommended.
   \ "public-read-write"
   / Owner gets FULL_CONTROL.
 4 | The AuthenticatedUsers group gets READ access.
   \ "authenticated-read"
   / Object owner gets FULL_CONTROL.
 5 | Bucket owner gets READ access.
   | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-read"
   / Both the object owner and the bucket owner get FULL_CONTROL
over the object.
 6 | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-full-control"
acl>
```

```
Edit advanced config?
y) Yes
n) No (default)
y/n> n
```

```
--------------------
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com:443
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>
```

```
Current remotes:
```

```
Name                 Type
====                 ====
sgdemo               s3
```

```
e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

기본 명령 예

- * 버킷 생성: *

  `rclone mkdir remote:bucket`

  ```
  rclone mkdir sgdemo:test01
  ```

  SSL 인증서를 무시해야 하는 경우 — 확인 안 함 - 인증서를 사용합니다.

- * 모든 버킷 나열: *

```
rclone lsd remote:
```

rclone LSD sgdemo 수:

- * 특정 버킷의 오브젝트 목록: *

```
rclone ls remote:bucket
```

rclone ls sgdemo: test01

```
    65536 TestObject.0
    65536 TestObject.1
    65536 TestObject.10
    65536 TestObject.12
    65536 TestObject.13
    65536 TestObject.14
    65536 TestObject.15
    65536 TestObject.16
    65536 TestObject.17
    65536 TestObject.18
    65536 TestObject.2
    65536 TestObject.3
    65536 TestObject.5
    65536 TestObject.6
    65536 TestObject.7
    65536 TestObject.8
    65536 TestObject.9
  33554432 bigobj
      102 key.json
       47 locked01.txt
4294967296 sequential-read.0.0
       15 test.txt
      116 version.txt
```

- * 버킷 삭제: *

```
rclone rmdir remote:bucket
```

rclone rmdir sgdemo:test02

- * 개체 넣기: *

```
rclone copy filename remote:bucket
```

rclone copy~/test/testfile.txt sgdemo:test01

- * 개체 가져오기: *

```
rclone copy remote:bucket/objectname filename
```

rclone copy sgdemo:test01/testfile.txt~/test/testfileS3.txt

- * 개체 삭제: *

```
rclone delete remote:bucket/objectname
```

rclone delete sgdemo:test01/testfile.txt

- * 버킷에서 오브젝트 마이그레이션 *

```
rclone sync source:bucket destination:bucket --progress

rclone sync source_directory destination:bucket --progress
```

rclone sync sgdemo: test01 sgdemo: clone01 — 진행률

```
Transferred:        4.032 GiB / 4.032 GiB, 100%, 95.484 KiB/s, ETA
0s
Transferred:           22 / 22, 100%
Elapsed time:       1m4.2s
```

progress(진행) 또는 -P를 사용하여 작업의 진행 상황을 표시합니다. 그렇지 않으면 출력이 없습니다.

- * 버켓과 모든 오브젝트 내용 삭제 *

```
rclone purge remote:bucket --progress
```

rclone purge sgdemo: test01 — 진행률

```
Transferred:              0 B / 0 B, -, 0 B/s, ETA -
Checks:                46 / 46, 100%
Deleted:               23 (files), 1 (dirs)
Elapsed time:         10.2s
```

rclone ls sgdemo: test01

```
2023/04/14 09:40:51 Failed to ls: directory not found
```

Veeam 백업 및 복제를 사용한 구축에 대한 StorageGRID 모범 사례

올리버 헨셀과 아론 클라인 작사

이 가이드에서는 NetApp StorageGRID 구성과 일부 Veeam 백업 및 복제를 중점적으로 다룹니다. 이 문서는 Linux 시스템에 익숙하고 Veeam 백업 및 복제와 함께 NetApp StorageGRID 시스템의 유지 관리 또는 구축을 담당하는 스토리지 및 네트워크 관리자를 위해 작성되었습니다.

개요

스토리지 관리자는 가용성, 빠른 복구 목표, 요구 사항에 맞게 확장 및 장기 데이터 보존을 위한 정책을 자동화하는 솔루션을 사용하여 증가하는 데이터를 관리할 수 있습니다. 이러한 솔루션은 손실 또는 악의적인 공격으로부터 보호되어야 합니다. Veeam과 NetApp은 파트너십을 통해 Veeam 백업 및 복구를 사내 오브젝트 스토리지에 NetApp StorageGRID과 결합하는 데이터 보호 솔루션을 만들었습니다.

Veeam과 NetApp StorageGRID는 전 세계적으로 빠르게 증가하는 데이터 및 늘어나는 규정 요구 사항을 충족하는 사용하기 쉬운 솔루션을 제공합니다. 클라우드 기반 오브젝트 스토리지는 복원력, 확장 기능, 운영 및 비용 효율성으로 인해 백업 대상으로 자연스럽게 선택할 수 있는 것으로 유명합니다. 이 문서는 Veeam 백업 솔루션 및 StorageGRID 시스템 구성에 대한 지침과 권장사항을 제공합니다.

Veeam의 오브젝트 워크로드에는 작은 오브젝트의 여러 동시 배치, 삭제 및 목록 작업이 생성됩니다. 불변성을 설정하면 보존 및 목록 버전을 설정하기 위한 요청 수가 개체 저장소에 추가됩니다. 백업 작업의 프로세스에는 일일 변경 사항에 대한 객체 쓰기가 포함되며 새 쓰기가 완료된 후 작업은 백업의 보존 정책에 따라 모든 객체를 삭제합니다. 백업 작업의 스케줄링은 거의 항상 중복됩니다. 이렇게 겹치면 객체 저장소의 50/50 PUT/DELETE 워크로드로 구성된 백업 윈도우의 상당 부분이 발생합니다. Veeam에서 작업 슬롯 설정을 사용하여 동시 작업 수를 조정하면 백업 작업 블록 크기를 늘리고 다중 개체 삭제 요청의 객체 수를 줄여 객체 크기를 늘릴 수 있습니다. 또한 작업을 완료할 최대 기간을 선택하면 성능 및 비용에 맞게 솔루션을 최적화할 수 있습니다.

제품 설명서를 꼭 읽어보세요. "Veeam 백업 및 복제" 그리고 "StorageGRID" 시작하기 전에. Veeam은 StorageGRID 솔루션의 크기를 조정하기 전에 사용해야 하는 Veeam 인프라 크기와 용량 요구 사항을 파악하는 데 도움이 되는 계산기를 제공합니다. Veeam Ready Program 웹사이트에서 Veeam- NetApp 검증 구성을 항상 확인하세요. "Veeam Ready Object, Object Immutability 및 Repository를 사용할 수 있습니다" .

Veeam 구성

권장 버전

Veeam Backup & Replication 12 또는 12.1 시스템에 최신 핫픽스를 적용하는 것이 좋습니다. 현재는 최소한 Veeam 12 패치 P20230718을 설치할 것을 권장합니다.

S3 저장소 구성

스케일아웃 백업 저장소(SOBR)는 S3 오브젝트 스토리지의 용량 계층입니다. 용량 계층은 기본 저장소의 확장 기능으로, 데이터 보존 기간이 길고 스토리지 솔루션이 저렴합니다. Veeam은 S3 Object Lock API를 통해 불변성을 제공하는 기능을 제공합니다. Veeam 12는 스케일아웃 저장소에서 여러 버킷을 사용할 수 있습니다. StorageGRID은 단일 버킷의 오브젝트 또는 용량에 대한 제한이 없습니다. 여러 버킷을 사용하면 백업 데이터가 오브젝트에서 페타바이트 규모로 증가할 수 있는 대규모 데이터 세트를 백업할 때 성능이 향상될 수 있습니다.

특정 솔루션 및 요구 사항의 사이징에 따라 동시 작업을 제한해야 할 수 있습니다. 기본 설정에서는 각 CPU 코어와 각 작업 슬롯에 대해 하나의 리포지토리 작업 슬롯을 지정하고 동시 작업 슬롯 제한은 64입니다. 예를 들어 서버에 2개의 CPU 코어가 있는 경우 총 128개의 동시 스레드가 개체 저장소에 사용됩니다. 여기에는 PUT, GET, BATCH Delete가 포함됩니다. Veeam 백업이 새로운 백업 및 백업 데이터의 안정적 상태에 도달하고 만료 예정인 경우 시작할 작업 슬롯에 대해 보수적인 제한을 선택하고 이 값을 조정하는 것이 좋습니다. NetApp 어카운트 팀과 협력하여 원하는 시간 및 성능을 만족하도록 StorageGRID 시스템의 크기를 적절하게 조정해 주십시오. 최적의 솔루션을 제공하기 위해 슬롯당 작업 슬롯의 수와 작업 제한을 조정해야 할 수 있습니다.

백업 작업 구성입니다

Veeam 백업 작업은 신중하게 고려해야 하는 다양한 블록 크기 옵션으로 구성할 수 있습니다. 기본 블록 크기는 1MB이며, 압축 및 중복제거를 통해 Veeam이 제공하는 스토리지 효율성을 통해 초기 전체 백업에는 약 500KB의 오브젝트 크기와 증분 작업에 대해서는 100~200kB 오브젝트를 생성합니다. NetApp은 더 큰 백업 블록 크기를 선택하여 성능을 크게 향상시키고 오브젝트 저장소 요구 사항을 축소할 수 있습니다. 블록 크기가 클수록 오브젝트 저장소의 성능이 크게 향상되지만, 스토리지 효율성 성능의 저하로 인해 기본 스토리지 용량 요구사항이 증가할 가능성이 있습니다. 전체 백업에 대해 약 2MB의 객체를 생성하는 4MB 블록 크기로 백업 작업을 구성하고 증가분에 대해 700kB-1MB 객체 크기를 생성하는 것이 좋습니다. 고객은 Veeam 지원의 도움을 받아 8MB 블록 크기를 사용하여 백업 작업을 구성하는 것도 고려할 수 있습니다.

변경 불가능한 백업을 구현하면 오브젝트 저장소에서 S3 오브젝트 잠금을 사용합니다. 불변성 옵션은 객체에 대한 목록 및 보존 업데이트를 위해 객체 저장소에 대한 요청을 더 많이 생성합니다.

백업 보존 기간이 만료되면 백업 작업이 객체 삭제를 처리합니다. Veeam은 요청당 1,000개의 오브젝트가 포함된 다중 오브젝트 삭제 요청의 삭제 요청을 오브젝트 저장소로 전송합니다. 소규모 솔루션의 경우 요청당 객체 수를 줄이기 위해 조정해야 할 수 있습니다. 이 값을 낮추면 삭제 요청을 StorageGRID 시스템의 노드에 고르게 분산시킬 수 있는 이점이 추가됩니다. 다중 개체 삭제 제한을 구성할 때는 아래 표의 값을 시작점으로 사용하는 것이 좋습니다. 표의 값에 선택한 어플라이언스 유형의 노드 수를 곱하여 Veeam의 설정 값을 구합니다. 이 값이 1000보다 크거나 같으면 기본값을 조정할 필요가 없습니다. 이 값을 조정해야 하는 경우, Veeam 지원에 문의하여 변경하십시오.

어플라이언스 모델	노드별 **S3MultiObjectDeleteLimit**
SG5712를 참조하십시오	34
SG5760입니다	75를
SG6060입니다	200

특정 요구 사항에 맞는 권장 구성을 위해 NetApp 세일즈 팀과 협력하십시오. Veeam 구성 권장 사항에는 다음이 포함됩니다.

- 백업 작업 블록 크기 = 4MB
- SOBR 작업 슬롯 제한 = 2-16
- 다중 개체 삭제 제한 = 34-1000

StorageGRID 구성

권장 버전

Veeam 배포에는 최신 핫픽스가 적용된 NetApp StorageGRID 11.9 또는 12.0 버전이 권장됩니다. StorageGRID 시스템에는 항상 최신 핫픽스를 적용하고 최신 상태를 유지하는 것이 좋습니다.

로드 밸런서 및 **S3** 엔드포인트 구성

Veeam을 사용하면 HTTPS를 통해서만 엔드포인트를 연결해야 합니다. 암호화되지 않은 연결은 Veeam에서 지원되지 않습니다. SSL 인증서는 자체 서명된 인증서, 신뢰할 수 있는 개인 인증 기관 또는 신뢰할 수 있는 공용 인증 기관일 수 있습니다. S3 저장소에 대한 지속적인 액세스를 보장하려면 HA 구성에서 로드 밸런서를 2개 이상 사용하는 것이 좋습니다. 로드 밸런서는 모든 관리 노드 및 게이트웨이 노드에 있는 StorageGRID에서 제공하는 통합 로드 밸런서 서비스이거나 F5, Kemp, Hafroxy, Loadbalancer.org 등과 같은 타사 솔루션일 수 있습니다 StorageGRID 로드 밸런서를 사용하면 Veeam 워크로드의 우선순위를 지정할 수 있는 트래픽 분류자(QoS 규칙)를 설정하거나, Veeam을 StorageGRID 시스템에서 우선순위가 높은 워크로드에 영향을 미치지 않도록 제한할 수 있습니다.

S3 버킷

StorageGRID 는 안전한 멀티 테넌트 스토리지 시스템입니다. Veeam 워크로드에 대한 전용 테넌트를 만드는 것이 좋습니다. 저장 용량 할당량은 선택적으로 할당할 수 있습니다. 모범 사례로 "자체 ID 소스 사용"을 활성화하세요. 적절한 비밀번호로 테넌트 루트 관리 사용자를 보호합니다. Veeam Backup 12는 S3 버킷에 대해 강력한 일관성을 요구합니다. StorageGRID 버킷 수준에서 구성된 다양한 일관성 옵션을 제공합니다. Veeam이 여러 위치에서 데이터에 액세스하는 다중 사이트 배포의 경우 "strong-global"을 선택합니다. Veeam 백업 및 복원이 단일 사이트에서만 발생하는 경우 일관성 수준을 "strong-site"로 설정해야 합니다. 버킷 일관성 수준에 대한 자세한 내용은 다음을 검토하십시오. "문서화" . Veeam 불변성 백업에 StorageGRID 사용하려면 버킷 생성 중에 S3 개체 잠금을 전역적으로 활성화하고 버킷에서 구성해야 합니다.

라이프사이클 관리

StorageGRID는 StorageGRID 노드와 사이트에서 오브젝트 레벨의 보호를 위해 복제 및 삭제 코딩을 지원합니다. 삭제 코딩에는 최소 200kB 오브젝트 크기가 필요합니다. Veeam의 1MB에 대한 기본 블록 크기는 Veeam의 스토리지 효율성 후 종종 이 200kB 권장 최소 크기보다 작을 수 있는 오브젝트 크기를 생성합니다. 솔루션의 성능을 위해 사이트 간 연결이 지연 시간을 추가하거나 StorageGRID 시스템의 대역폭을 제한하지 않는 한 여러 사이트에 걸쳐 있는 삭제 코딩 프로필을 사용하지 않는 것이 좋습니다. 다중 사이트 StorageGRID 시스템에서는 각 사이트에 단일 복제본을 저장하도록 ILM 규칙을 구성할 수 있습니다. 내구성을 최대화하기 위해 각 사이트에 삭제 코딩 복사본을 저장하도록 규칙을 구성할 수 있습니다. 이 워크로드를 위해 Veeam Backup 서버에 로컬에 2개의 복제본을 사용하는 것이 가장 좋습니다.

성능 삭제

Veeam은 백업 삭제 프로세스의 삭제 요청 속도 조정 및 스케줄링을 제공합니다. 삭제 성능을 더욱 조정하려면 동기 삭제를 비활성화하고 ILM 스캐너가 개체의 최종 삭제를 관리하도록 할 수 있습니다.

동기 삭제 비활성화 단계

1. StorageGRID 그리드 관리자를 엽니다.
2. 오른쪽 상단 모서리에서 물음표를 선택한 다음 API 문서를 선택하세요.
3. 오른쪽 상단 모서리에서 Private API 문서 페이지 링크를 클릭하세요.
4. ilm-advanced를 확장합니다.
5. GET ilm-advanced를 선택하세요.
6. '시도해보기'를 선택한 다음 '실행'을 선택합니다.
7. 응답 결과를 확인하세요.

    a. 값이 null이면 기본 ilm-advanced 값이 사용 중임을 의미합니다.

    b. 값이 null이 아닌 경우 사용자 정의 ILM 고급 값이 사용 중임을 의미합니다. "data" : 이후의 모든 출력을 { 에서 시작하여 마지막에서 두 번째 }까지 복사합니다.

        i. 텍스트 편집기에 저장하세요.

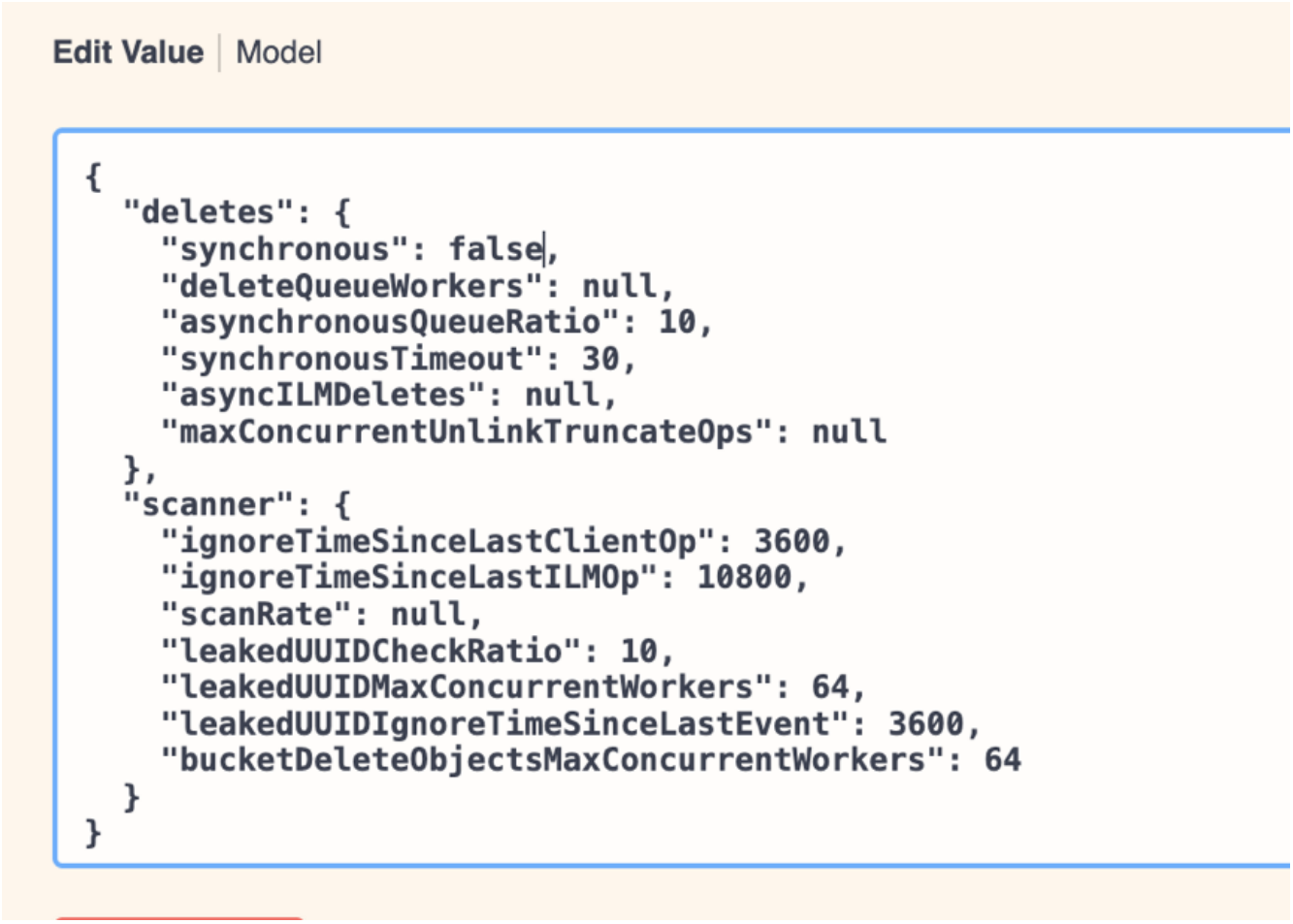
        응답 예시:

Response body


```
{
  "responseTime": "2025-09-19T15:01:28.142Z",
  "status": "success",
  "apiVersion": "4.2",
  "data": {
    "deletes": {
      "synchronous": null,
      "deleteQueueWorkers": null,
      "asynchronousQueueRatio": null,
      "synchronousTimeout": null,
      "asyncILMDeletes": null,
      "maxConcurrentUnlinkTruncateOps": null
    },
    "scanner": {
      "ignoreTimeSinceLastClientOp": null,
      "ignoreTimeSinceLastILMOp": null,
      "scanRate": null,
      "leakedUUIDCheckRatio": null,
      "leakedUUIDMaxConcurrentWorkers": null,
      "leakedUUIDIgnoreTimeSinceLastEvent": null,
      "bucketDeleteObjectsMaxConcurrentWorkers": null
    }
  }
}
```

8. PUT ilm-advanced를 선택합니다.
9. API 본문 편집을 시작하려면 '시도해보기'를 선택하세요.
    a. 기본적으로 API 본문에는 기본값이 포함되며 이전에 구성된 사용자 정의 값은 포함되지 않습니다. 이것이 5~7단계를 실행하는 것이 매우 중요한 이유입니다.
10. 5~7단계에서 기본값이 아닌 값이 발견되면 API 본문을 7단계에서 저장된 출력으로 바꿉니다. . 그렇지 않은 경우 5-7단계에서 값이 null인 경우 API 본문을 그대로 둡니다.
11. API 본문 상자에서 다음 매개변수를 조정하세요.
    a. 동기 값을 false로 설정합니다.

    API 본문 텍스트 예:

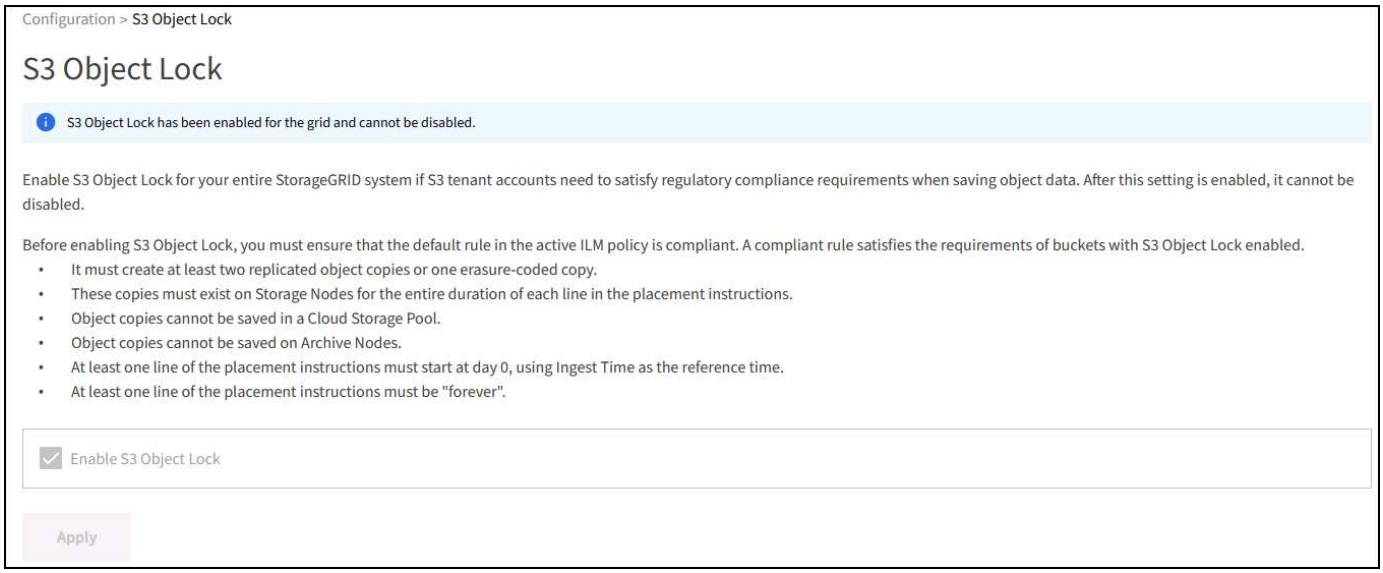


12. 완료되면 실행을 선택하세요

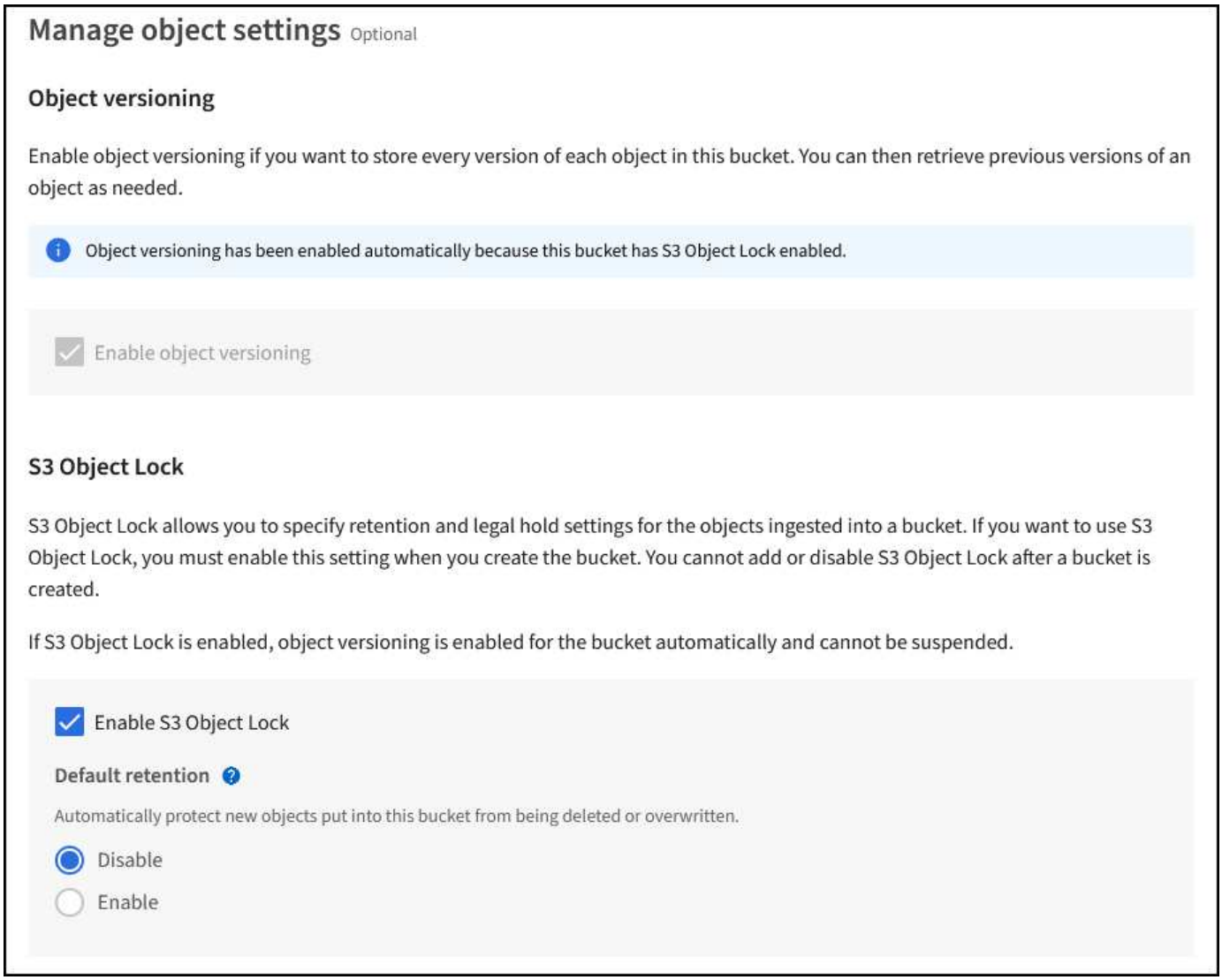
구현 핵심 사항

StorageGRID

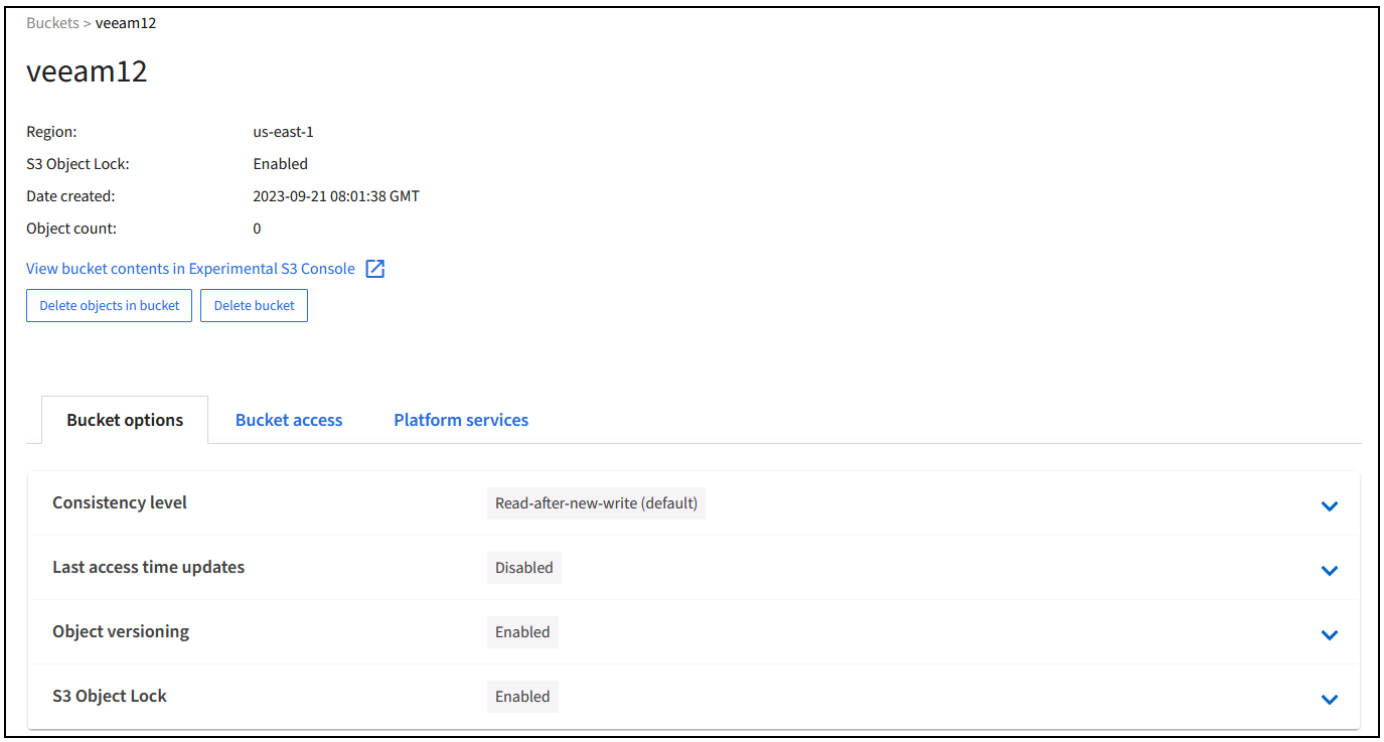
불변성이 필요한 경우 StorageGRID 시스템에서 오브젝트 잠금이 활성화되어 있는지 확인합니다. 관리 UI의 구성/S3 오브젝트 잠금 아래에서 옵션을 찾습니다.



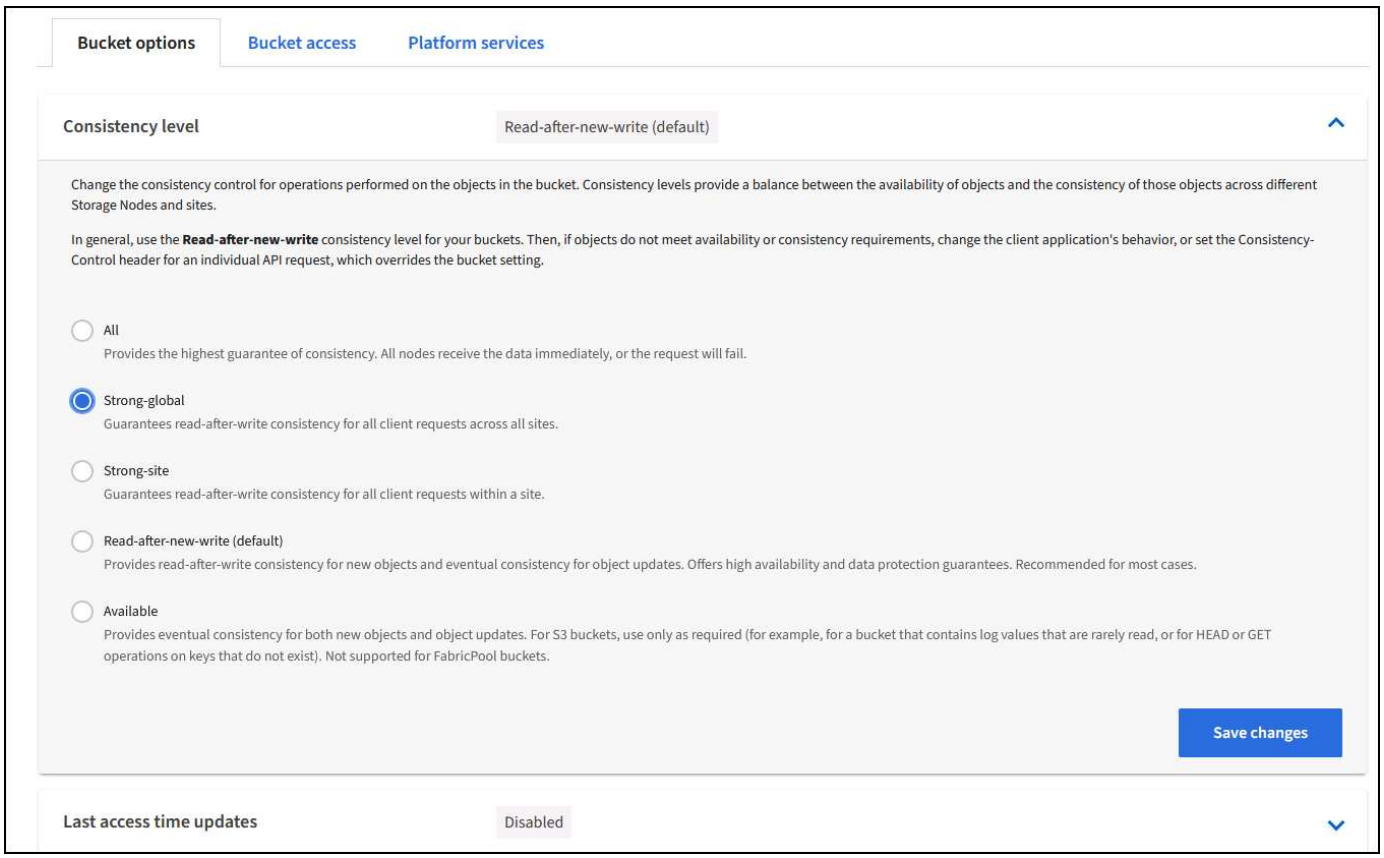
버킷을 생성할 때 불변의 백업에 이 버킷을 사용하려면 "S3 오브젝트 잠금 활성화"를 선택하십시오. 이렇게 하면 버킷 버전 관리가 자동으로 활성화됩니다. Veeam에서 객체 보존을 명시적으로 설정하므로 기본 보존을 사용하지 않도록 설정합니다. Veeam에서 변경 불가능한 백업을 생성하지 않는 경우 버전 관리 및 S3 오브젝트 잠금을 선택하지 않아야 합니다.



버킷이 생성되면 생성된 버킷의 세부 정보 페이지로 이동합니다. 정합성 보장 수준을 선택합니다.

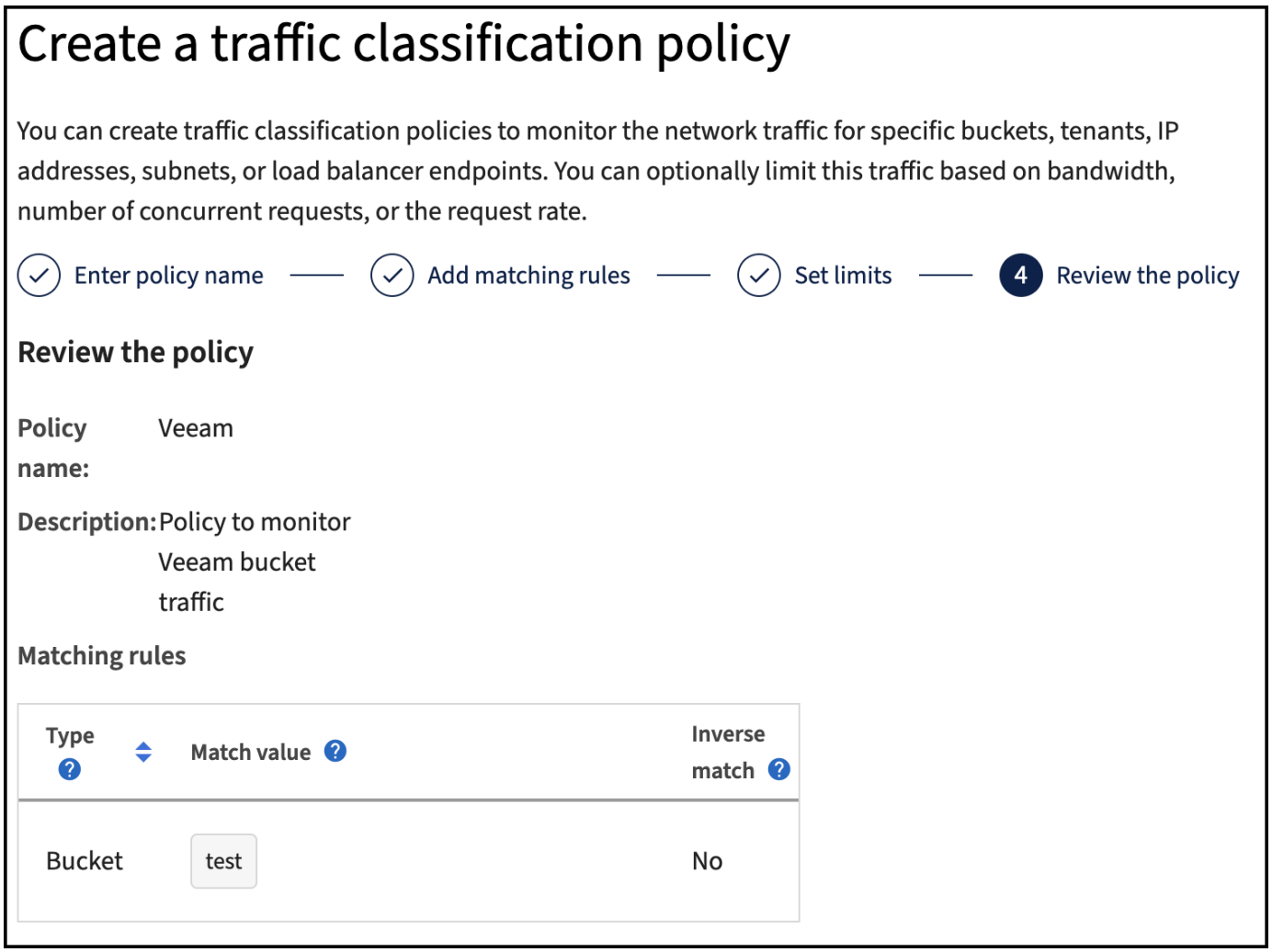


Veeam을 사용하려면 S3 버킷에 대해 강력한 일관성이 필요합니다. 따라서 Veeam을 통해 여러 위치의 데이터에 액세스할 수 있는 멀티 사이트 배포의 경우 "강력한 글로벌"을 선택하십시오. Veeam 백업 및 복원을 단일 사이트에서만 수행할 경우 일관성 수준을 "강력한 사이트"로 설정해야 합니다. 변경 사항을 저장합니다.



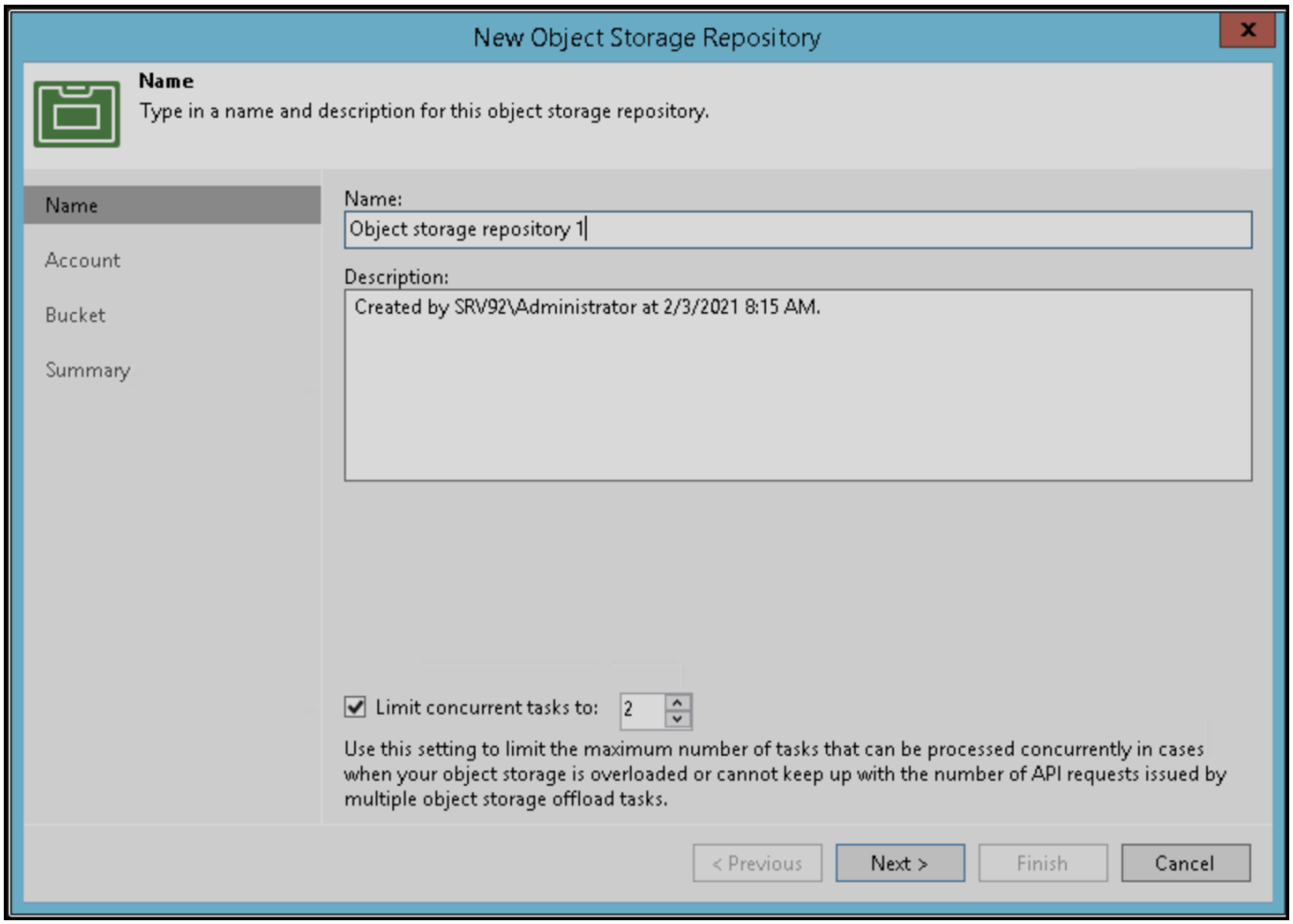
StorageGRID는 모든 관리 노드와 전용 게이트웨이 노드에서 통합 로드 밸런서 서비스를 제공합니다. 이 로드 밸런서를 사용하면 QoS(트래픽 분류 정책)를 구성할 수 있다는 이점이 많습니다. 이러한 기능은 다른 클라이언트 워크로드에 대한 애플리케이션 영향을 제한하거나 다른 워크로드에 대한 우선 순위를 지정하는 데 주로 사용되지만 모니터링에 도움이 되는 추가 메트릭 수집도 제공합니다.

구성 탭에서 "트래픽 분류"를 선택하고 새 정책을 생성합니다. 규칙의 이름을 지정하고 유형으로 버킷 또는 테넌트를 선택합니다. 버킷 또는 테넌트의 이름을 입력하십시오. QoS가 필요한 경우 제한을 설정하지만 대부분의 구현에서는 모니터링 이점을 추가하려고 하므로 제한을 설정하지 마십시오.

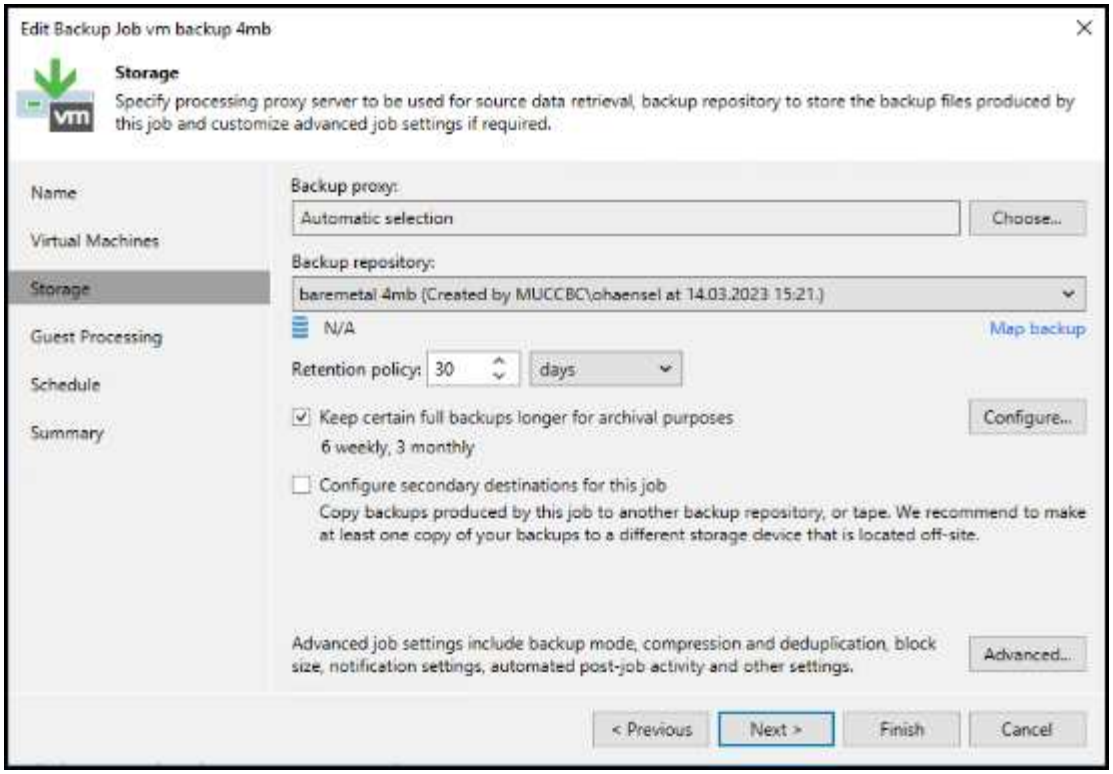


Veeam을 선택합니다

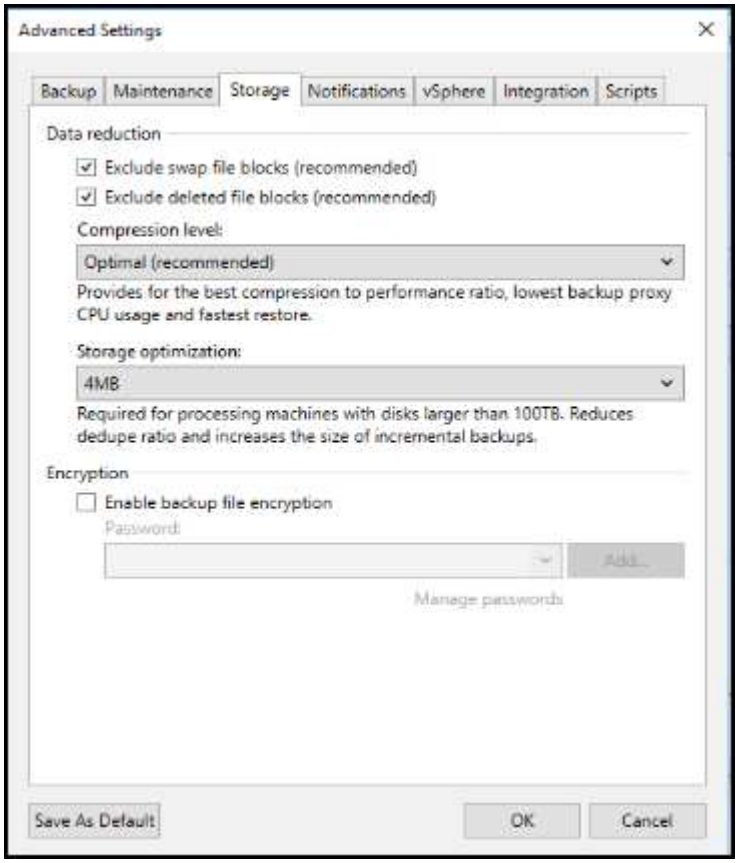
StorageGRID 어플라이언스의 모델 및 수량에 따라 버킷에서 동시 작업 수의 제한을 선택하고 구성해야 할 수 있습니다.



Veeam 콘솔의 백업 작업 구성에 관한 Veeam 설명서를 따라 마법사를 시작합니다. VM을 추가한 후 SOBR 리포지토리를 선택합니다.



고급 설정 을 클릭하고 저장소 최적화 설정을 4MB 이상으로 변경합니다. 압축 및 중복제거가 활성화되어야 합니다. 요구 사항에 따라 게스트 설정을 변경하고 백업 작업 일정을 구성합니다.



StorageGRID 모니터링

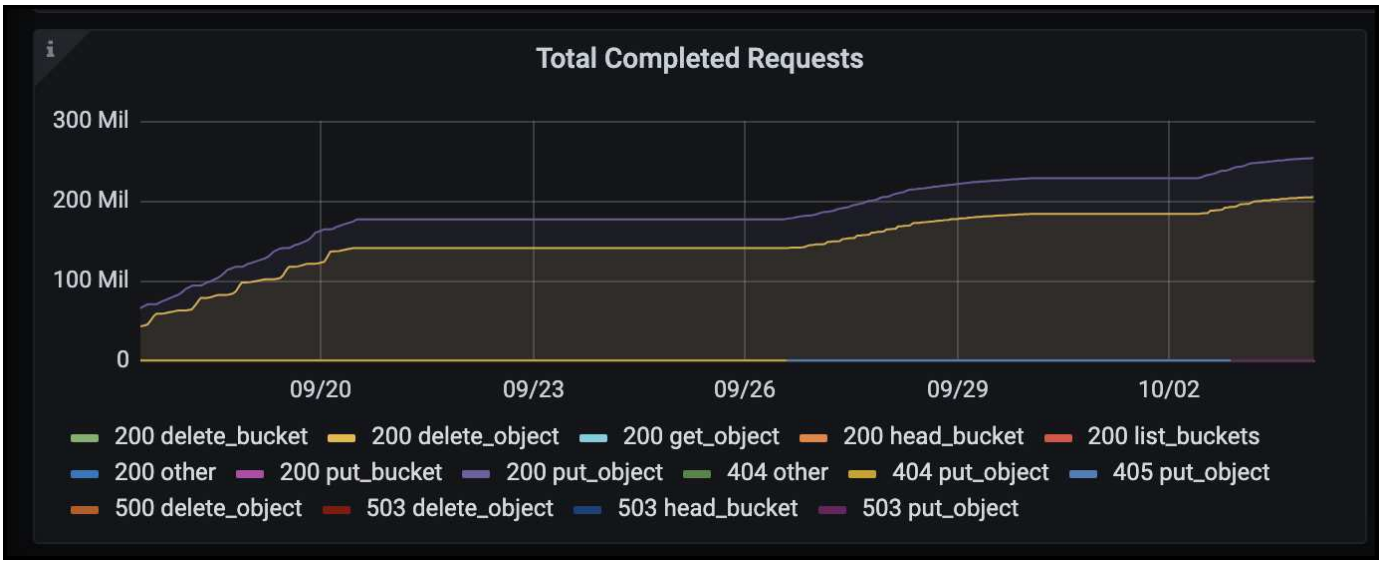
Veeam과 StorageGRID가 함께 작동하는 방식을 자세히 보려면 첫 번째 백업의 보존 시간이 만료될 때까지 기다려야 합니다. 지금까지는 Veeam 워크로드가 주로 PUT 작업으로 구성되며 삭제가 발생하지 않습니다. 백업 데이터가 만료되고 정리가 시작되면 오브젝트 저장소에서 전체 일관된 사용량을 확인하고 필요한 경우 Veeam에서 설정을 조정할 수 있습니다.

StorageGRID는 지원 탭 메트릭 페이지에 있는 시스템 작동을 모니터링하는 편리한 차트를 제공합니다. 주요 대시보드는 정책을 생성한 경우 S3 개요, ILM 및 트래픽 분류 정책입니다. S3 개요 대시보드에서 S3 작업 속도, 지연 시간 및 요청 응답에 대한 정보를 확인할 수 있습니다.

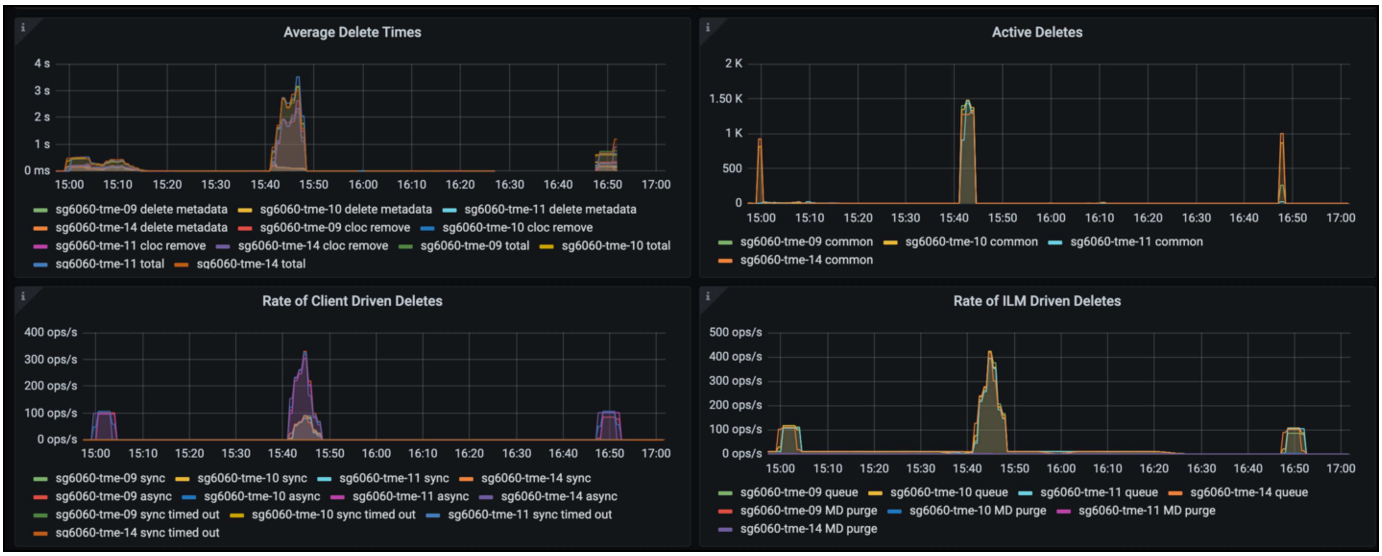
S3 속도 및 활성 요청을 보면 각 노드가 처리 중인 로드의 양과 유형별로 전체 요청 수를 확인할 수 있습니다.

Average Duration(평균 기간) 차트에는 각 노드가 각 요청 유형에 대해 걸리는 평균 시간이 표시됩니다. 이는 요청의 평균 대기 시간이며 추가 튜닝이 필요하거나 StorageGRID 시스템이 더 많은 로드를 처리할 수 있는 공간이 있음을 나타내는 좋은 지표가 될 수 있습니다.

총 완료된 요청 차트에서 유형 및 응답 코드별로 요청을 볼 수 있습니다. 응답에 대해 200(OK)이 아닌 응답이 표시되면 StorageGRID 시스템이 503(느린 속도) 응답을 보내면서 로드가 과중하게 로드되고 있는 것과 같은 문제일 수 있으며 추가적인 튜닝이 필요하거나 로드가 증가하기 위해 시스템을 확장할 시간이 되었을 수 있습니다.



ILM 대시보드에서 StorageGRID 시스템의 삭제 성능을 모니터링할 수 있습니다. StorageGRID는 각 노드에서 동기 및 비동기 삭제를 결합하여 모든 요청의 전반적인 성능을 최적화하고 시도합니다.



트래픽 분류 정책을 사용하면 로드 밸런서에 대한 메트릭을 볼 수 있습니다. 요청 처리량, 속도, 기간, Veeam이 전송 및 수신하는 객체 크기 등을 확인할 수 있습니다.

추가 정보를 찾을 수 있는 위치

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

- "NetApp StorageGRID 제품 설명서"
- "Veeam 백업 및 복제"

StorageGRID를 사용하여 Dremio 데이터 소스를 구성합니다

안젤라 청 _ 에 의해

Dremio는 클라우드 기반 또는 온프레미스 오브젝트 스토리지를 비롯한 다양한 데이터 소스를 지원합니다. StorageGRID를 오브젝트 스토리지 데이터 소스로 사용하도록 Dremio를 구성할 수 있습니다.

Dremio 데이터 소스를 구성합니다

필수 구성 요소

- StorageGRID S3 끝점 URL, 테넌트 S3 액세스 키 ID 및 보안 액세스 키

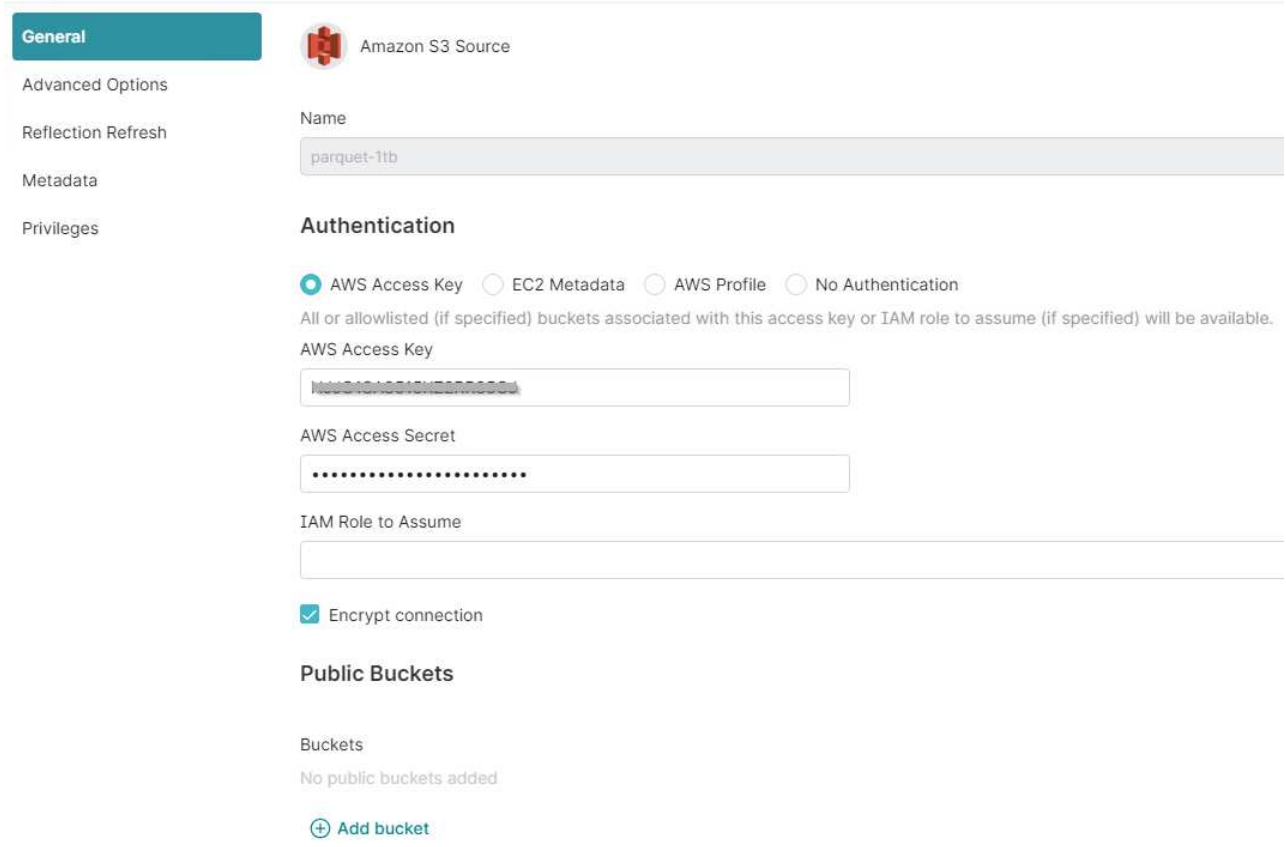
- StorageGRID 구성 권장 사항: 압축을 사용하지 않도록 설정(기본적으로 해제됨) 를 누릅니다
  Dremio는 쿼리 중에 동일한 개체 내에서 다른 바이트 범위를 동시에 가져오기 위해 바이트 범위 GET를 사용합니다. 일반적으로 바이트 범위 요청의 크기는 1MB입니다. 압축된 객체는 바이트 범위 가져오기 성능을 저하시킵니다.

Dremio 가이드

"Amazon S3에 연결 - S3 호환 스토리지 구성".

지침

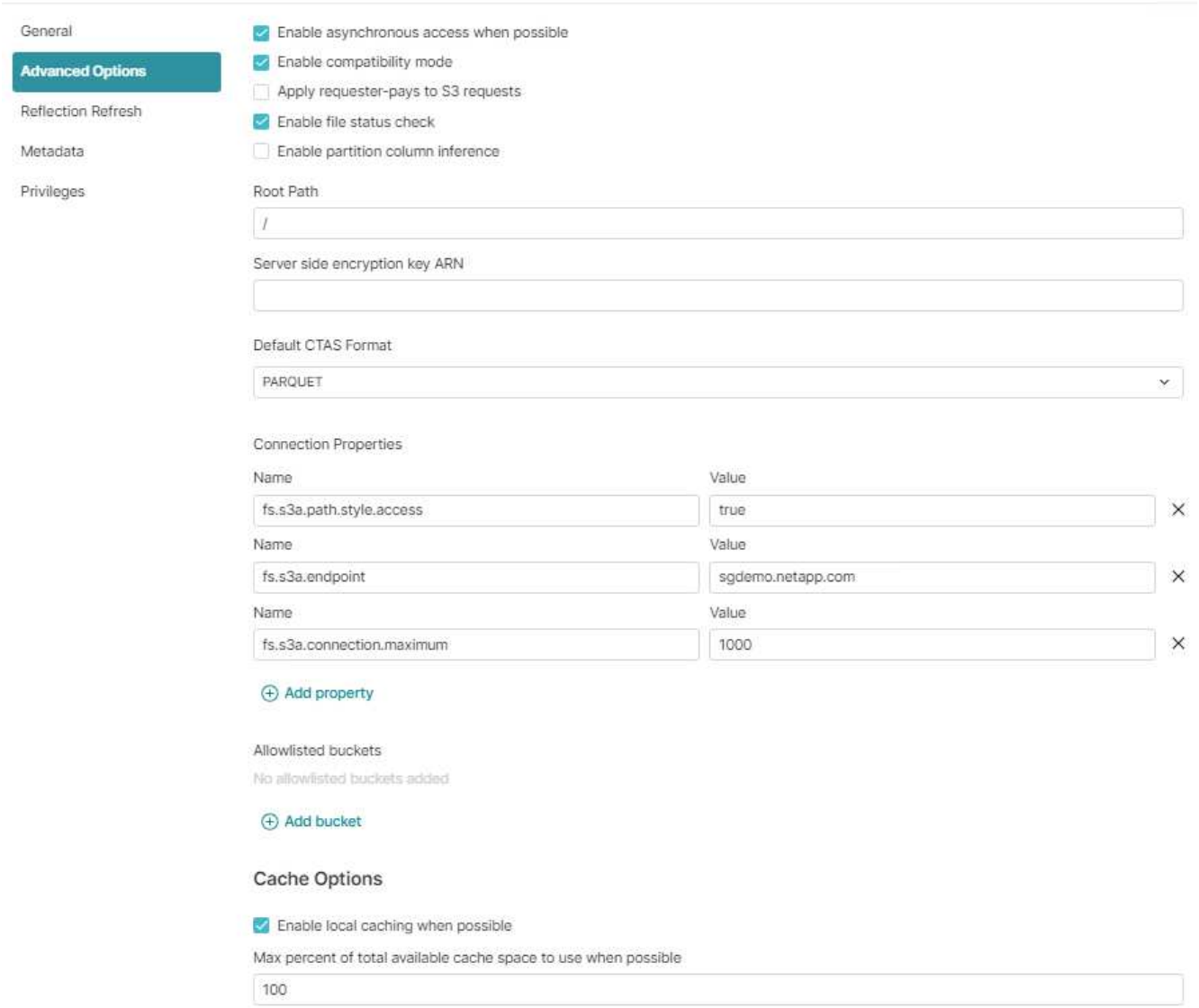
1. Dremio Datasets 페이지에서 + 기호를 클릭하여 소스를 추가하고 'Amazon S3'를 선택합니다.
2. 이 새 데이터 소스의 이름, StorageGRID S3 테넌트 액세스 키 ID 및 비밀 액세스 키를 입력합니다.
3. StorageGRID S3 끝점에 연결하기 위해 https를 사용하는 경우 '연결 암호화' 확인란을 선택합니다. 를 누릅니다
   이 S3 끝점에 대해 자체 서명된 CA 인증서를 사용하는 경우 Dremio 가이드 지침에 따라 이 CA 인증서를 Dremio 서버의 <JAVA_HOME>/JRE/lib/security+에 추가합니다
   - 샘플 스크린샷 *



4. '고급 옵션'을 클릭하고 '호환 모드 사용'을 선택합니다.
5. 연결 속성에서 + 속성 추가를 클릭하고 이러한 s3a 속성을 추가합니다.
6. FS.s3a.connection. 최대 기본값은 100입니다. S3 데이터 세트에 100개 이상의 열이 있는 대형 Parquet 파일이 포함된 경우 에서 100보다 큰 값을 입력해야 합니다. 이 설정은 Dremio 가이드를 참조하십시오.

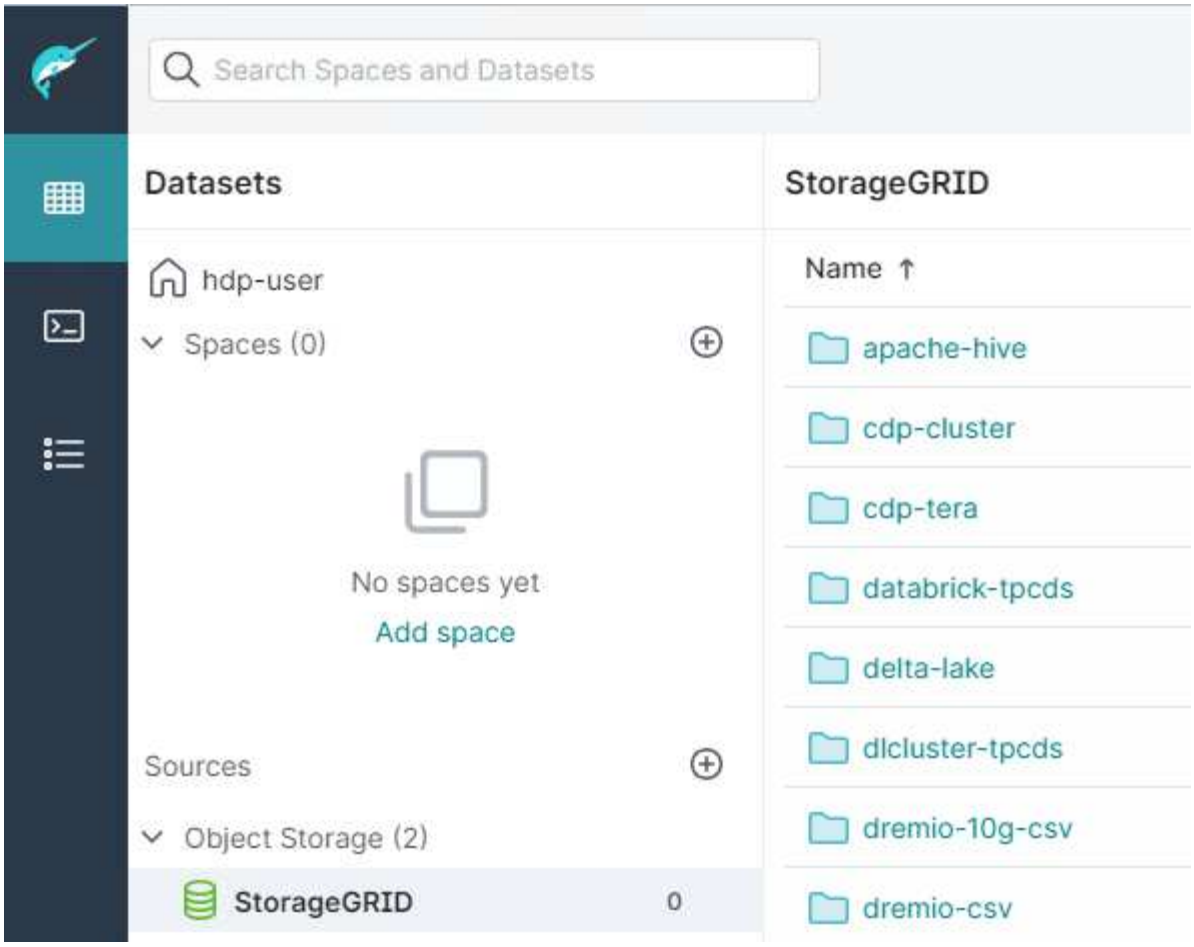
이름	값
FS.s3a.endpoint	_<StorageGRID S3 엔드포인트: port> _
FS.s3a.path.style.access	참
FS.s3a.connection.maximum입니다	_< 100보다 큰 값 > _

◦ 샘플 스크린샷 *



7. 조직 또는 응용 프로그램 요구 사항에 따라 다른 Dremio 옵션을 구성합니다.
8. 이 새 데이터 원본을 만들려면 저장 단추를 클릭합니다.
9. StorageGRID 데이터 소스가 성공적으로 추가되면 버킷 목록이 왼쪽 패널에 표시됩니다. 를 누릅니다

◦ 샘플 스크린샷 *



GitLab을 사용한 NetApp StorageGRID

안젤라 청 _ 에 의해

NetApp은 GitLab에서 StorageGRID를 테스트했습니다. 아래의 GitLab 구성 샘플을 참조하십시오. 을 참조하십시오 "GitLab 객체 스토리지 구성 가이드" 를 참조하십시오.

객체 저장소 연결 예

Linux 패키지 설치의 경우, 이 예제는 의 예입니다 `connection` 통합 양식의 설정입니다. 편집 `/etc/gitlab/gitlab.rb` 원하는 값으로 다음 줄을 추가합니다.

```
# Consolidated object storage configuration
gitlab_rails['object_store']['enabled'] = true
gitlab_rails['object_store']['proxy_download'] = true
gitlab_rails['object_store']['connection'] = {
  'provider' => 'AWS',
  'region' => 'us-east-1',
  'endpoint' => 'https://<storagegrid-s3-endpoint:port>',
  'path_stype' => 'true',
  'aws_access_key_id' => '<AWS_ACCESS_KEY_ID>',
  'aws_secret_access_key' => '<AWS_SECRET_ACCESS_KEY>'
}
# OPTIONAL: The following lines are only needed if server side encryption
is required
gitlab_rails['object_store']['storage_options'] = {
  'server_side_encryption' => 'AES256'
}
gitlab_rails['object_store']['objects']['artifacts']['bucket'] = 'gitlab-
artifacts'
gitlab_rails['object_store']['objects']['external_diffs']['bucket'] =
'gitlab-mr-diffs'
gitlab_rails['object_store']['objects']['lfs']['bucket'] = 'gitlab-lfs'
gitlab_rails['object_store']['objects']['uploads']['bucket'] = 'gitlab-
uploads'
gitlab_rails['object_store']['objects']['packages']['bucket'] = 'gitlab-
packages'
gitlab_rails['object_store']['objects']['dependency_proxy']['bucket'] =
'gitlab-dependency-proxy'
gitlab_rails['object_store']['objects']['terraform_state']['bucket'] =
'gitlab-terraform-state'
gitlab_rails['object_store']['objects']['pages']['bucket'] = 'gitlab-
pages'
```

절차 및 API 예

StorageGRID에서 S3 암호화 옵션 테스트 및 시연

_ 아론 클라인 _

StorageGRID와 S3 API를 사용하면 유휴 데이터를 다양한 방법으로 암호화할 수 있습니다. 자세한 내용은 을 참조하십시오 "StorageGRID 암호화 방법을 검토합니다".

이 가이드에서는 S3 API 암호화 방법을 보여 줍니다.

서버 측 암호화(SSE)

SSE를 사용하면 클라이언트가 개체를 저장하고 StorageGRID에서 관리하는 고유 키로 암호화할 수 있습니다. 개체가 요청되면 StorageGRID 에 저장된 키에 의해 개체가 해독됩니다.

SSE 예

- SSE가 있는 개체를 넣습니다

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- 객체를 확인하여 암호화를 확인합니다

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- 객체를 가져옵니다

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

고객 제공 키(SSE-C)를 사용한 서버측 암호화

SSE를 사용하면 클라이언트가 객체를 저장하고 해당 객체와 함께 제공된 고유 키를 사용하여 해당 객체를 암호화할 수 있습니다. 개체가 요청될 때 개체를 해독하고 반환하려면 동일한 키를 제공해야 합니다.

SSE-C의 예

- 테스트 또는 데모용으로 암호화 키를 만들 수 있습니다
  - 암호화 키를 만듭니다

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- 생성된 키가 있는 개체를 넣습니다

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- 물체를 향하십시오

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
            {
                "AcceptRanges": "bytes",
                "LastModified": "2022-05-02T19:20:02+00:00",
                "ContentLength": 47,
                "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
                "ContentType": "binary/octet-stream",
                "Metadata": {},
                "SSECustomerAlgorithm": "AES256",
                "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
            }
```

암호화 키를 제공하지 않으면 "HeadObject 작업을 호출할 때 오류 발생(404): 찾을 수 없음" 오류가 발생합니다.

- 객체를 가져옵니다

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

암호화 키를 제공하지 않으면 "GetObject 작업을 호출할 때 오류가 발생했습니다(InvalidRequest). 즉, 개체가 서버측 암호화 형식을 사용하여 저장되었습니다."라는 오류가 발생합니다. 객체를 검색하려면 올바른 매개 변수를 제공해야 합니다."

버킷 서버 측 암호화(SSE-S3)

SSE-S3를 사용하면 클라이언트가 버킷에 저장된 모든 오브젝트에 대해 기본 암호화 동작을 정의할 수 있습니다. 개체는 StorageGRID 에서 관리하는 고유 키로 암호화됩니다. 개체가 요청되면 StorageGRID 에 저장된 키에 의해 개체가 해독됩니다.

버킷 **SSE-S3**의 예

- 새 버킷을 생성하고 기본 암호화 정책을 설정합니다
  - 새 버킷을 생성합니다

```
aws s3api create-bucket --bucket <bucket> --region us-east-1
--endpoint-url https://s3.example.com
```

  - 버킷 암호화

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- 물체를 버킷에 넣으십시오

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- 물체를 향하십시오

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- 객체를 가져옵니다

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

StorageGRID에서 S3 오브젝트 잠금을 테스트하고 시연합니다

_ 아론 클라인 _

Object Lock은 개체가 삭제되거나 덮어써지는 것을 방지하는 WORM 모델을 제공합니다. StorageGRID의 객체 잠금 구현은 규제 요구사항을 충족하고, 객체 보존에 대한 법적 보류 및 규정 준수 모드를 지원하고, 기본 버킷 보존 정책을 지원하는 데 도움이 되는 코호트 평가입니다.

이 가이드에서는 S3 오브젝트 잠금 API를 보여 줍니다.

법적 증거 자료 보관

- 개체 잠금 법적 보류는 개체에 적용되는 간단한 켜기/끄기 상태입니다.

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- 가져오기 작업으로 확인합니다.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- 법적 증거 자료 보관 기능을 끕니다

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- 가져오기 작업으로 확인합니다.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

준수 모드

- 개체 보존은 타임스탬프까지 보존하여 수행됩니다.

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- 보존 상태를 확인합니다

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

기본 보존

- 객체 API에 정의된 보존 종료 날짜를 기준으로 보존 기간을 일 및 년 단위로 설정합니다.

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- 보존 상태를 확인합니다

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- 물체를 버킷에 넣으십시오

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- 버킷에 설정된 보존 기간은 객체의 보존 타임 스탬프로 변환됩니다.

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

정의된 보존 개체가 있는 개체 삭제 테스트

오브젝트 잠금은 버전 관리를 기반으로 합니다. 보존은 개체 버전에 정의됩니다. 보존이 정의되어 있고 버전이 지정되지 않은 개체를 삭제하려고 하면 삭제 표식이 개체의 현재 버전으로 만들어집니다.

- 보존이 정의된 개체를 삭제합니다

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- 버킷의 물체를 나열합니다

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

  - 개체가 나열되지 않은 것을 확인합니다.

- 버전 목록을 사용하여 삭제 마커와 원래 잠긴 버전을 확인합니다

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- 객체의 잠긴 버전을 삭제합니다

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

StorageGRID의 정책 및 사용 권한

다음은 StorageGRID S3의 정책 및 사용 권한의 예입니다.

정책의 구조

StorageGRID에서 그룹 정책은 AWS 사용자(IAM) S3 서비스 정책과 동일합니다.

그룹 정책은 StorageGRID에서 필요합니다. S3 액세스 키가 있지만 사용자 그룹에 할당되지 않았거나 일부 사용 권한을 부여하는 정책이 없는 그룹에 할당되어 있는 사용자는 데이터에 액세스할 수 없습니다.

버킷 및 그룹 정책은 대부분의 동일한 요소를 공유합니다. 정책은 json 형식으로 구축되며 를 사용하여 생성할 수 있습니다 "AWS 정책 생성기"

모든 정책은 영향, 작업 및 리소스를 정의합니다. 버킷 정책도 주체를 정의합니다.

효과 * 는 요청을 허용 또는 거부합니다.

Principal *

- 버킷 정책에만 적용됩니다.
- 보안 주체는 권한을 부여하거나 거부하고 있는 계정/사용자입니다.
- 다음과 같이 정의할 수 있습니다.
  - 와일드카드 " * "

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

  - 테넌트의 모든 사용자에 대한 테넌트 ID(AWS 계정과 동일)

```
"Principal": { "AWS": "27233906934684427525" }
```

  - 사용자(버킷이 상주하는 테넌트 내에서 로컬 또는 페더레이션됨 또는 그리드의 다른 테넌트)

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:user/tenant1user1" }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/tenant2user1" }
```

◦ 그룹(버킷이 상주하는 테넌트 내에서 로컬 또는 페더레이션된 그룹 또는 그리드의 다른 테넌트)

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:group/DevOps"  }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

작업 * 은 사용자에게 부여되거나 거부되는 S3 작업 집합입니다.

그룹 정책의 경우 사용자가 S3 작업을 수행하려면 S3:ListBucket 작업이 허용됩니다.

리소스 * 는 작업을 수행할 수 있는 권한을 부여하거나 거부한 주체인 버킷 또는 버킷입니다. 선택적으로 정책 작업이 유효한 경우 * 조건 * 이 있을 수 있습니다.

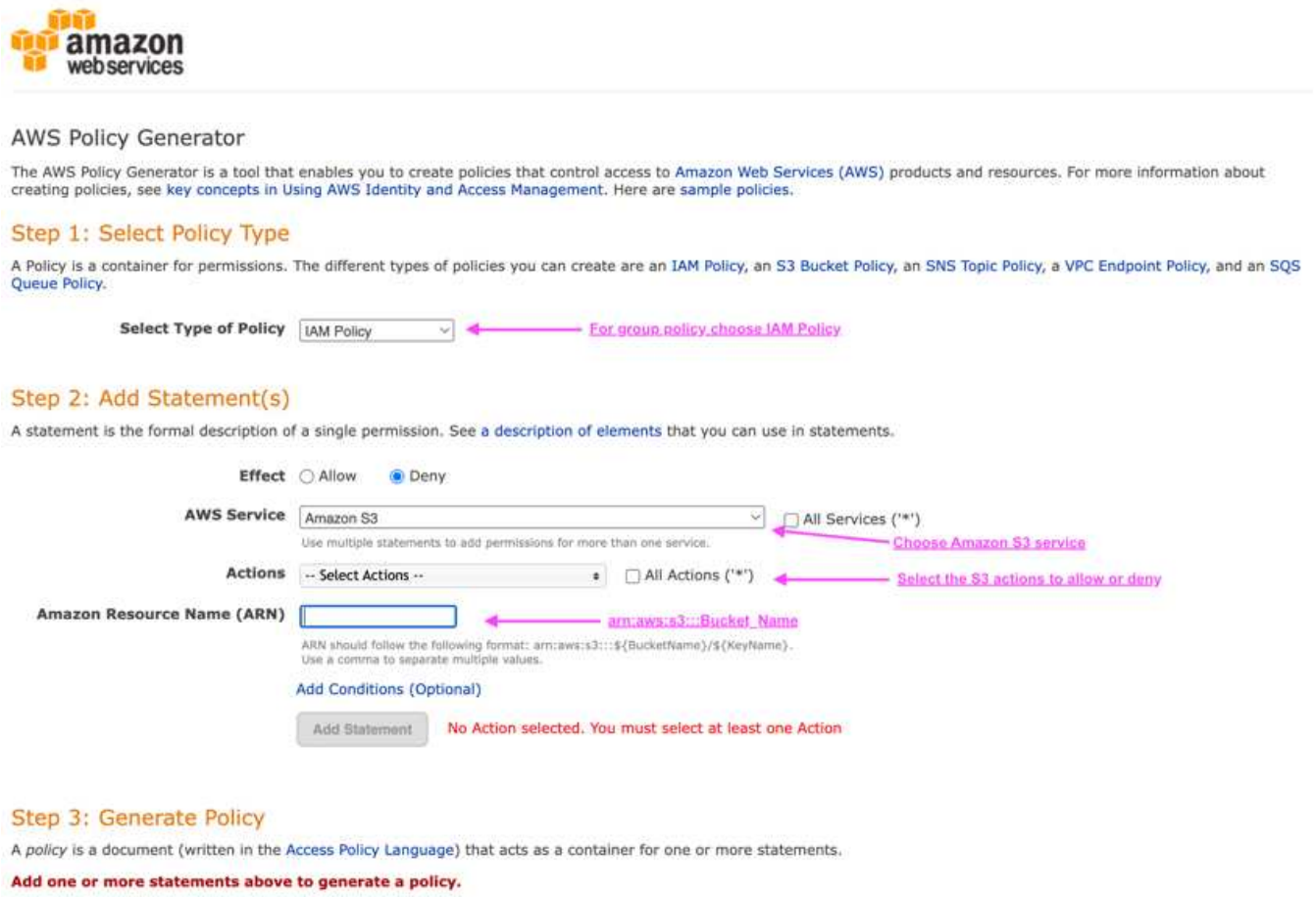
JSON 정책 형식은 다음과 같습니다.

```
{
  "Statement": [
    {
      "Sid": "Custom name for this permission",
      "Effect": "Allow or Deny",
      "Principal": {
        "AWS": [
          "arn:aws:iam::tenant_ID::user/User_Name",
          "arn:aws:iam::tenant_ID::federated-user/User_Name",
          "arn:aws:iam::tenant_ID:group/Group_Name",
          "arn:aws:iam::tenant_ID:federated-group/Group_Name",
          "tenant_ID"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:Other_Action"
      ],
      "Resource": [
        "arn:aws:s3:::Example_Bucket",
        "arn:aws:s3:::Example_Bucket/*"
      ],
    }
  ]
}
```

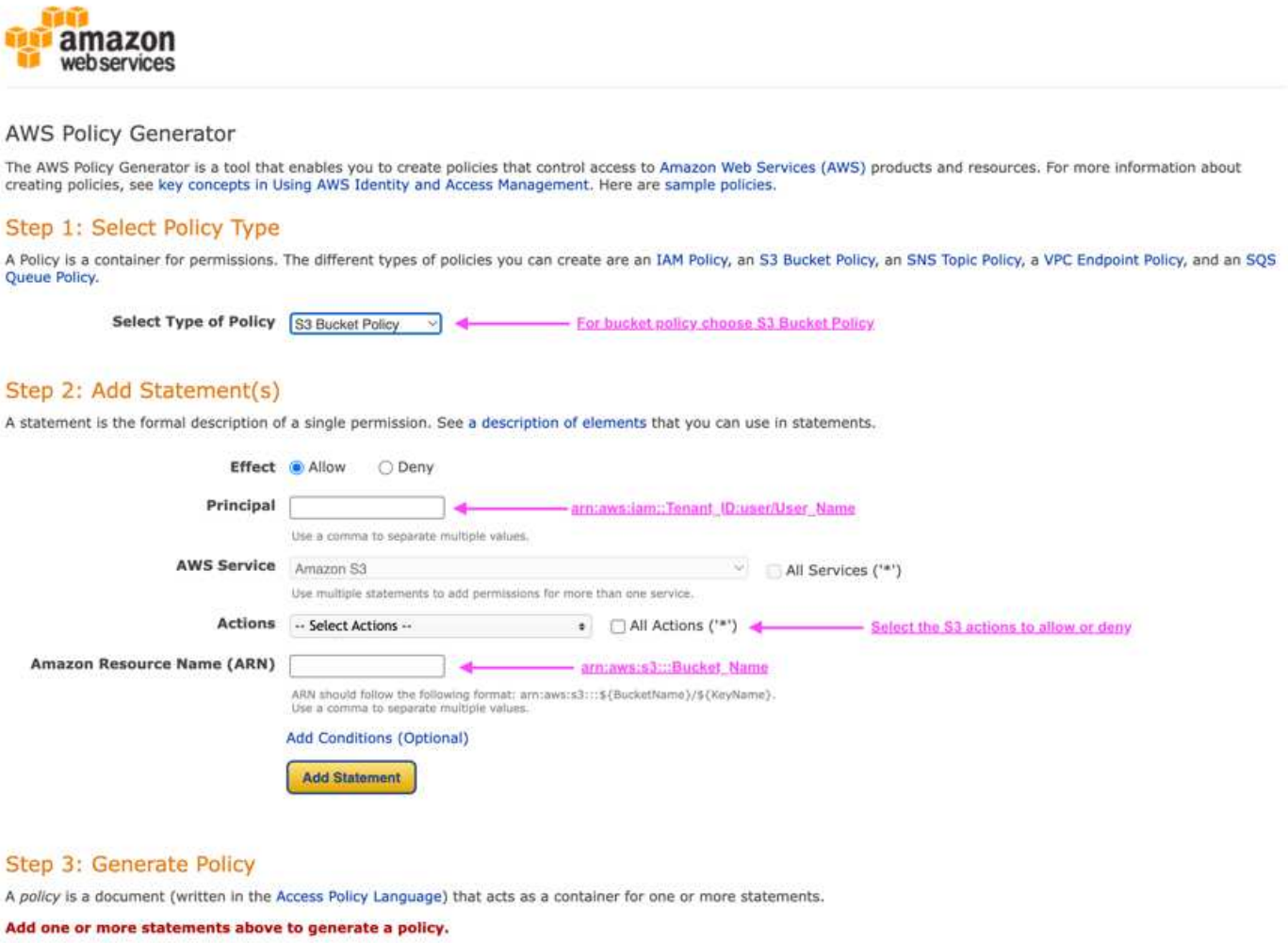
AWS 정책 생성기 사용

AWS 정책 생성기는 json 코드를 올바른 형식과 구현하려는 정보로 가져오는 데 도움이 되는 유용한 도구입니다.

StorageGRID 그룹 정책에 대한 권한을 생성하려면 * 정책 유형에 대한 IAM 정책을 선택하십시오. * 원하는 효과에 대한 버튼을 선택합니다 - 허용 또는 거부. 권한 거부로 정책을 시작한 다음 작업 드롭다운에서 권한 허용 * 을 추가하는 것이 좋습니다. 이 권한에 포함할 S3 작업 중 많은 수의 상자 또는 "모든 작업" 상자 옆에 있는 상자를 클릭합니다. * 아마존 리소스 이름(ARN) 상자에 버킷 경로를 입력합니다. 버킷 이름 앞에 "arn:AWS:S3:::::"를 추가합니다. ex. "arn:AWS:S3:::example_bucket"

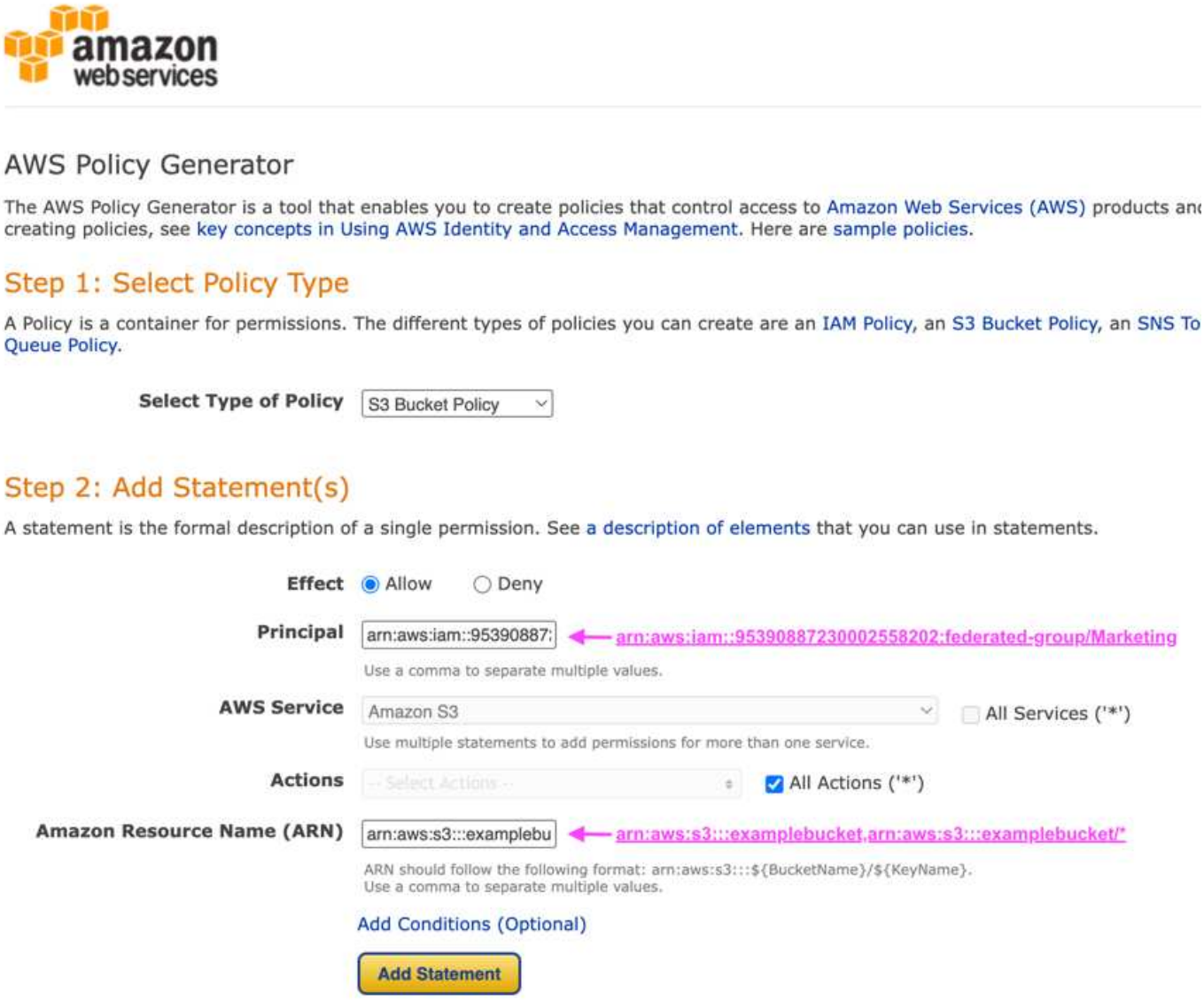


버킷 정책에 대한 권한을 생성하려면 * 정책 유형에 대해 S3 버킷 정책을 선택합니다. * 원하는 효과에 대한 버튼을 선택합니다 - 허용 또는 거부. 거부 권한으로 정책을 시작한 다음 허용 권한 * 을 Principal의 사용자 또는 그룹 정보에 추가하는 것이 좋습니다. * 작업 드롭다운에서 이 권한에 포함할 S3 작업 중 많은 항목 옆에 있는 상자를 클릭하거나 "모든 작업" 상자를 클릭합니다. * 아마존 리소스 이름(ARN) 상자에 버킷 경로를 입력합니다. 버킷 이름 앞에 "arn:AWS:S3:::::"를 추가합니다. ex. "arn:AWS:S3:::example_bucket"



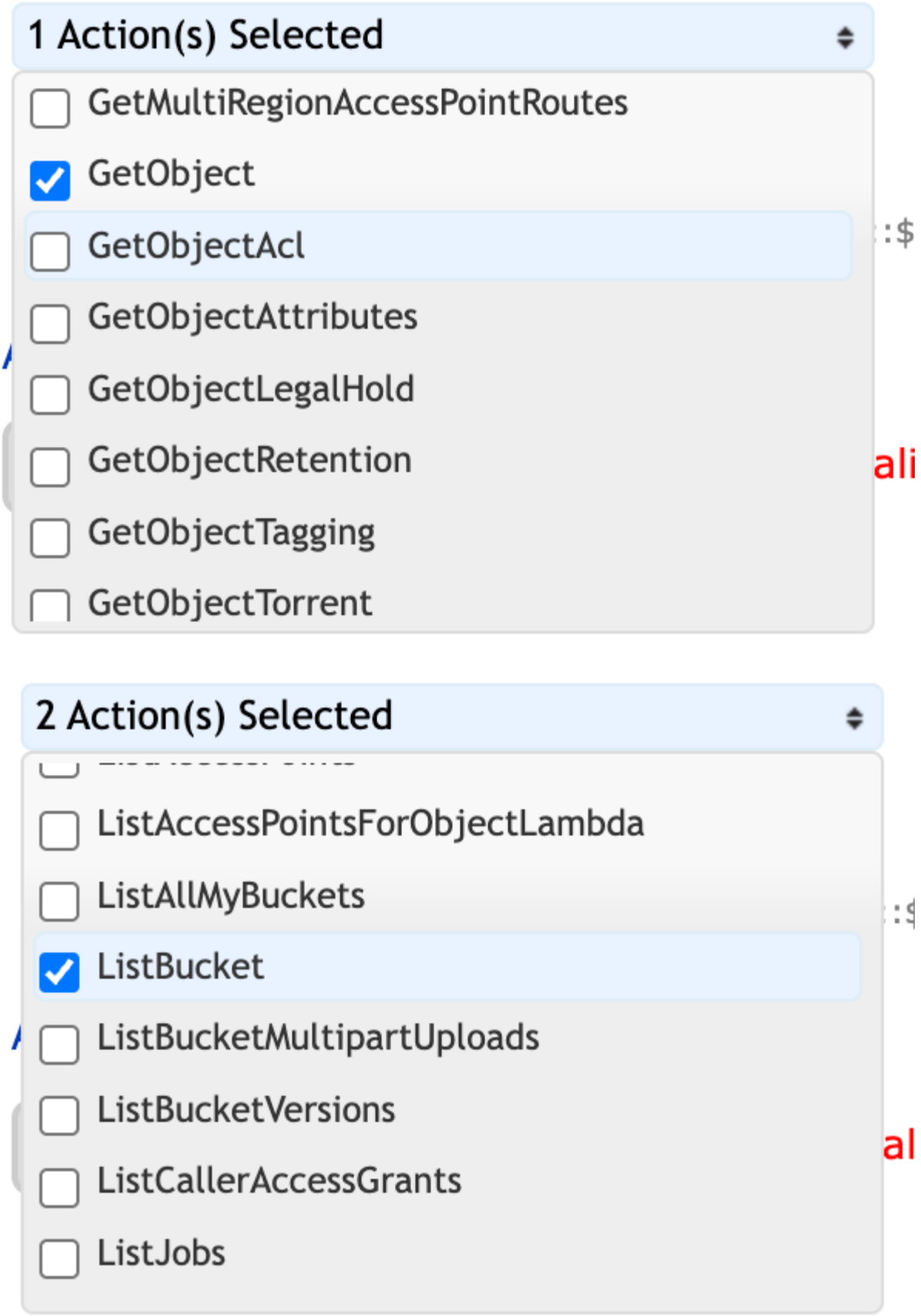
예를 들어, 모든 사용자가 버킷의 모든 오브젝트에 대해 GetObject 작업을 수행할 수 있도록 버킷 정책을 생성하려는 경우 지정된 계정의 "Marketing" 그룹에 속한 사용자만 전체 액세스 권한을 허용합니다.

- 정책 유형으로 S3 Bucket Policy 를 선택합니다.
- 효과 허용 을 선택합니다
- 마케팅 그룹 정보 - arn:AWS:IAM::95390887230002558202:Federated-group/Marketing을 입력합니다
- "모든 작업" 상자를 클릭합니다.
- 버킷 정보 -arn:AWS:S3::example_bucket, arn:AWS:S3::example_bucket/ * 을 입력합니다

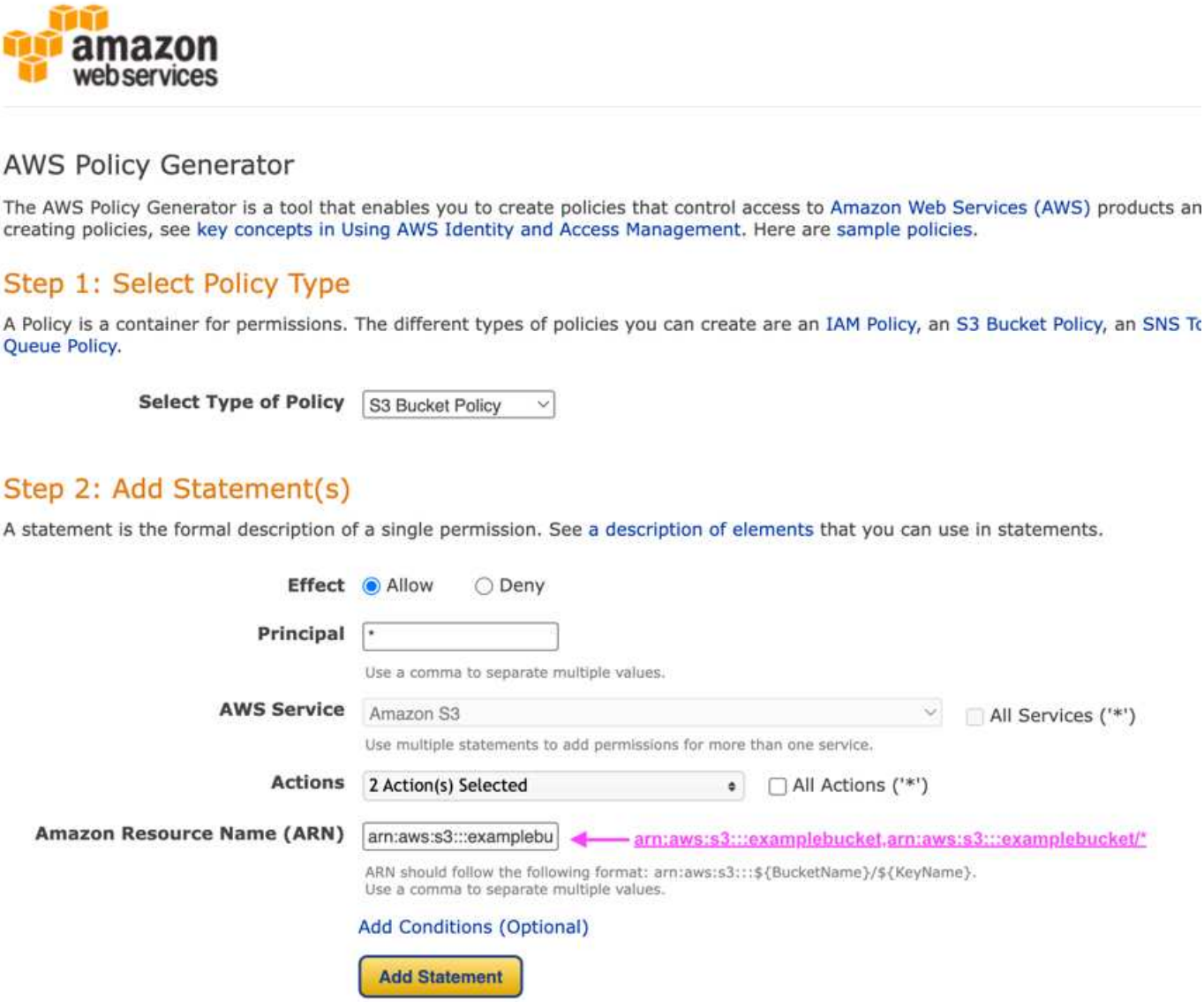


- "문 추가" 버튼을 클릭합니다

- 효과 허용 을 선택합니다
- 모든 사람에 대해 별표 ++ * + 를 입력합니다
- GetObject 및 ListBucket 작업 옆에 있는 상자를 클릭합니다."

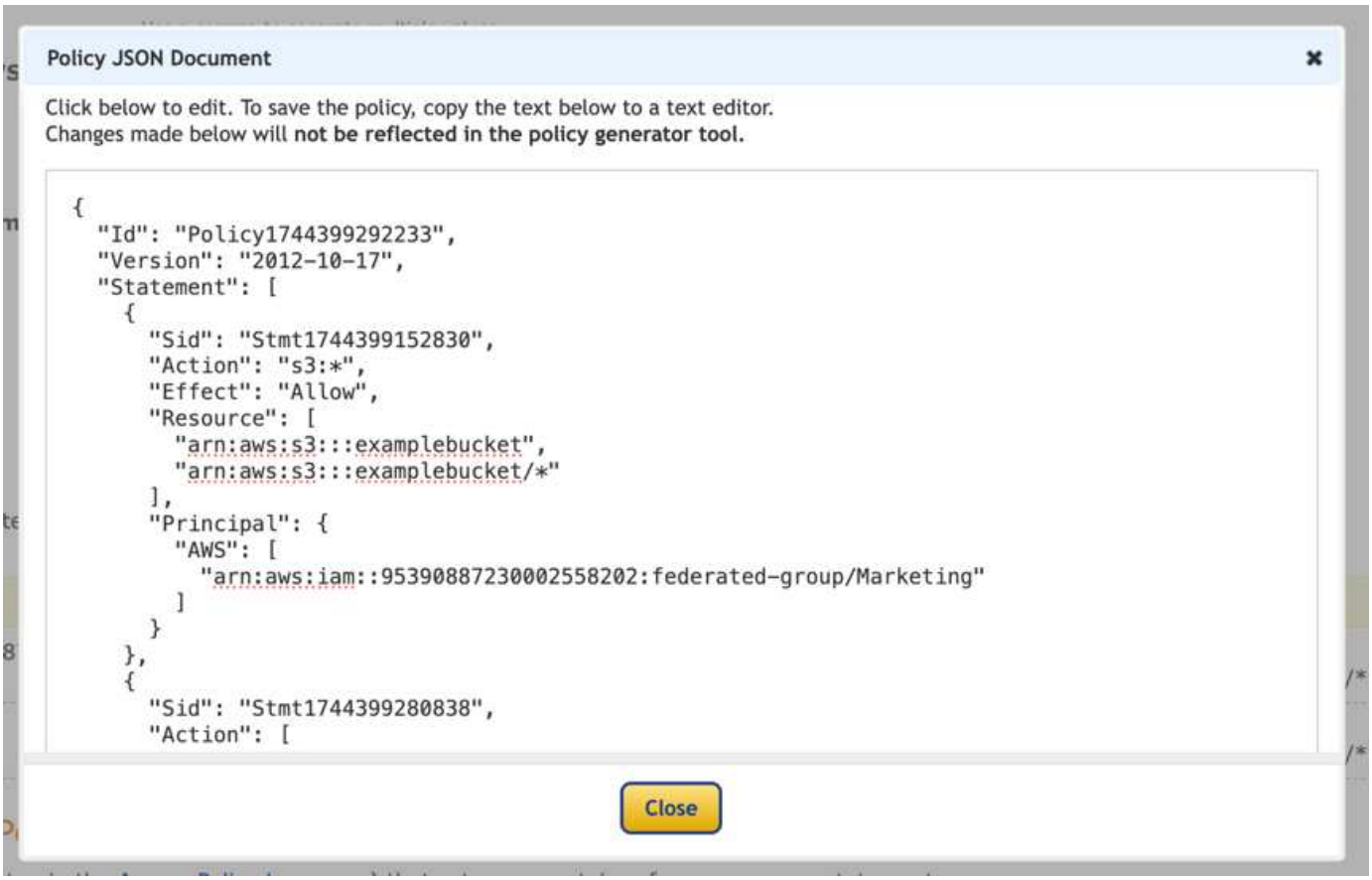


- 버킷 정보 -arn:AWS:S3::example_bucket, arn:AWS:S3::example_bucket/ * 을 입력합니다



- "문 추가" 버튼을 클릭합니다

- "정책 생성" 버튼을 클릭하면 생성된 정책과 함께 팝업 창이 나타납니다.



- 다음과 같은 전체 json 텍스트를 복사합니다.

```
{
  "Id": "Policy1744399292233",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1744399152830",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "Stmt1744399280838",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

이 json은 있는 그대로 사용할 수도 있고 "Statement" 줄 위의 ID 및 버전 줄을 제거할 수도 있으며 각 권한에 대해 보다 의미 있는 제목을 사용하여 SID를 사용자 지정할 수도 있고 이러한 항목을 제거할 수도 있습니다.

예를 들면 다음과 같습니다.

```
{
  "Statement": [
    {
      "Sid": "MarketingAllowFull",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "EveryoneReadOnly",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

그룹 정책(IAM)

홈 디렉토리 스타일 버킷 액세스

이 그룹 정책은 사용자가 사용자 이름이 인 버킷의 객체에 액세스하는 것만 허용합니다.

```
{
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

오브젝트 잠금 버킷 생성을 거부합니다

이 그룹 정책은 사용자가 버킷에 개체 잠금이 설정된 버킷을 생성할 수 없도록 제한합니다.

이 정책은 StorageGRID UI에서 적용되지 않으며 S3 API에서만 적용됩니다.

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

개체 잠금 보존 제한

이 버킷 정책은 객체 잠금 보존 기간을 10일 이하로 제한합니다

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

버전 **ID**를 기준으로 개체를 삭제하지 못하도록 제한합니다

이 그룹 정책은 버전 ID를 기준으로 버전이 지정된 개체를 삭제하지 못하도록 제한합니다

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

그룹을 읽기 전용 권한으로 단일 하위 디렉토리(접두사)로 제한합니다

이 정책을 사용하면 그룹의 구성원이 버킷 내의 하위 디렉터리(접두사)에 읽기 전용 액세스 권한을 가질 수 있습니다. 버킷 이름은 "study"이고 하위 디렉토리는 "study01"입니다.

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
```

```
                "arn:aws:s3::: study"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```

버킷 정책

읽기 전용 액세스 권한이 있는 단일 사용자로 버킷을 제한합니다

이 정책을 사용하면 단일 사용자가 버킷에 대한 읽기 전용 액세스를 가질 수 있고 다른 모든 사용자에 대한 액세스를 명시적으로 부인할 수 있습니다. 정책 맨 위에 있는 Deny 문을 그룹화하는 것은 보다 빠른 평가를 위한 좋은 방법입니다.

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": "arn:aws:iam::349215141330028336 65:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::349215141330028336 65:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

읽기 전용 액세스 권한이 있는 소수의 사용자로 버킷을 제한합니다.

```
{
    "Statement": [
      {
        "Sid": "Deny all S3 actions to employees 002-005",
        "Effect": "deny",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": "*",
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      },
      {
        "Sid": "Allow read-only access for employees 002-005",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion"
        ],
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      }
    ]
}
```

버킷에서 버전 지정된 객체의 사용자 삭제를 제한합니다

이 버킷 정책은 사용자 ID "56622399308951294926"으로 식별된 사용자(versionID로 식별됨)가 버전 ID로 버전이 지정된 객체를 삭제하지 못하도록 제한합니다

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

StorageGRID의 버킷 수명 주기

S3 라이프사이클 구성을 생성하여 StorageGRID 시스템에서 특정 오브젝트 삭제 시기를 제어할 수 있습니다.

라이프사이클 구성이란 무엇입니까?

라이프사이클 구성은 특정 S3 버킷의 오브젝트에 적용되는 규칙 세트입니다. 각 규칙은 영향을 받는 개체와 해당 개체가 만료되는 시기(특정 날짜 또는 특정 일 수 이후)를 지정합니다.

각 오브젝트는 S3 버킷 라이프사이클 또는 ILM 정책의 보존 설정을 따릅니다. S3 버킷 라이프사이클이 구성되면 라이프사이클 만료 작업이 버킷 라이프사이클 필터와 일치하는 오브젝트에 대한 ILM 정책을 재정의합니다. 버킷 수명 주기 필터와 일치하지 않는 객체는 ILM 정책의 보존 설정을 사용합니다. 객체가 버킷 수명 주기 필터와 일치하고 만료 작업이 명시적으로 지정되지 않은 경우 ILM 정책의 보존 설정이 사용되지 않으며 객체 버전이 영구적으로 보존됩니다.

따라서 ILM 규칙의 배치 지침이 개체에 계속 적용되더라도 그리드에서 개체를 제거할 수 있습니다. 또는 객체에 대한 ILM 배치 지침이 만료된 후에도 객체가 그리드에 유지될 수 있습니다.

StorageGRID는 수명 주기 구성에서 최대 1,000개의 수명 주기 규칙을 지원합니다. 각 규칙에는 다음 XML 요소가 포함될 수 있습니다.

- 만료: 지정된 날짜에 도달하거나 지정된 일 수에 도달할 때 개체를 인제스트할 때로부터 개체를 삭제합니다.
- NoncurrentVersionExpiration: 지정된 일 수에 도달할 때 개체가 비전류가 되었을 때부터 개체를 삭제합니다.
- 필터(접두사, 태그)
- 상태 *ID

StorageGRID는 다음 버킷 작업을 사용하여 라이프사이클 구성을 관리합니다.

- DeleteBucketLifecycle
- GetBuckLifecycleConfiguration 을 참조하십시오
- PutBucketLifecycleConfiguration을 참조하십시오

수명 주기 정책의 구조

라이프사이클 구성을 만드는 첫 번째 단계에서는 하나 이상의 규칙이 포함된 JSON 파일을 만듭니다. 예를 들어 이 JSON 파일에는 다음과 같은 세 가지 규칙이 포함되어 있습니다.

1. *규칙 1*은 category1/ 접두사와 일치하고 key2 값이 tag2인 객체에만 적용됩니다. Expiration 매개변수는 필터와 일치하는 객체가 2020년 8월 22일 자정에 만료되도록 지정합니다.
2. *규칙 2*는 category2/ 접두사와 일치하는 객체에만 적용됩니다. 만료 매개변수는 필터와 일치하는 객체가 수집된 후 100일 후에 만료되도록 지정합니다.

   > 일 수를 지정하는 규칙은 오브젝트가 수집된 시점을 기준으로 합니다. 현재 날짜가 수집 날짜와 일 수를 더한 값을 초과하면 라이프사이클 구성이 적용되는 즉시 일부 객체가 버킷에서 제거될 수 있습니다.

3. *규칙 3*은 category3/ 접두사와 일치하는 객체에만 적용됩니다. 만료 매개변수는 일치하는 객체의 모든 비현재 버전이 비현재 버전으로 전환된 후 50일 후에 만료되도록 지정합니다.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

버킷에 라이프사이클 구성을 적용합니다

문서 수정 상태 구성 파일을 만든 후 PutBucketLifecycleConfiguration 요청을 실행하여 버킷에 적용합니다.

이 요청은 예제 파일의 수명주기 구성을 이름이 인 버킷의 객체에 `testbucket` 적용합니다.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

수명 주기 구성이 버킷에 성공적으로 적용되었는지 확인하려면 GetBucketLifecycleConfiguration 요청을 실행합니다. 예를 들면 다음과 같습니다.

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

표준(버전 없음) 버킷에 대한 예시 수명 주기 정책

90일 후에 개체 삭제

사용 사례: 이 정책은 임시 파일, 로그 또는 중간 처리 데이터와 같이 제한된 기간 동안만 관련성이 있는 데이터를 관리하는 데 적합합니다. 이점: 저장 비용을 절감하고 버킷을 깔끔하게 유지할 수 있습니다.

```
{
    "Rules": [
      {
        "ID": "Delete after 90 day rule",
        "Filter": {},
        "Status": "Enabled",
          "Expiration": {
              "Days": 90
        }
      }
    ]
}
```

버전이 지정된 버킷에 대한 수명 주기 정책 예

10일 후 비현재 버전 삭제

사용 사례: 이 정책은 시간이 지남에 따라 누적되어 상당한 공간을 차지할 수 있는 최신 버전이 아닌 객체의 저장소를 관리하는 데 도움이 됩니다. 이점: 최신 버전만 보관하여 저장소 사용량을 최적화합니다.

```
{
    "Rules": [
            {
        "ID": "NoncurrentVersionExpiration 10 day rule",
        "Filter": {},
        "Status": "Enabled",
          "NoncurrentVersionExpiration": {
              "NoncurrentDays": 10
        }
    }
    ]
}
```

5개의 비현재 버전을 유지하세요

사례: 복구 또는 감사 목적으로 제한된 수의 이전 버전을 보관하려는 경우에 유용합니다. 이점: 충분한 기록 및 복구 지점을 보장하기 위해 충분한 수의 최신이 아닌 버전을 보관합니다.

```
{
    "Rules": [
      {
        "ID": "NewerNoncurrentVersions 5 version rule",
        "Filter": {},
        "Status": "Enabled",
        "NoncurrentVersionExpiration": {
            "NewerNoncurrentVersions": 5
        }
    }
    ]
}
```

다른 버전이 없는 경우 삭제 마커를 제거합니다.

사용 사례: 이 정책은 시간이 지남에 따라 누적될 수 있는 모든 비현재 버전을 제거한 후 남은 삭제 마커를 관리하는 데 도움이 됩니다. 이점: 불필요한 잡동사니를 줄입니다.

```
{
    "Rules": [
    {
        "ID": "Delete marker cleanup rule",
        "Filter": {},
        "Status": "Enabled",
        "Expiration": {
        "ExpiredObjectDeleteMarker": true
        }
    }
    ]
}
```

현재 버전은 **30**일 후에 삭제하고, 현재가 아닌 버전은 **60**일 후에 삭제하고, 다른 버전이 없으면 현재 버전 삭제로 생성된 삭제 마커를 제거합니다.

사용 사례: 삭제 마커를 포함하여 현재 버전과 이전 버전에 대한 완전한 수명 주기를 제공합니다. 이점: 스토리지 비용을 절감하고 충분한 복구 지점과 기록을 유지하면서 버킷을 깔끔하게 유지합니다.

```
{
  "Rules": [
    {
      "ID": "Delete current version",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "Days": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 60
      }
    },
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    }
  ]
}
```

다른 버전이 없는 삭제 마커를 제거하고, **"accounts_ prefix"**가 있는 개체의 경우 **4**개의 비현재 버전과 최소 **30**일 분의 기록을 유지하고, 다른 모든 개체 버전의 경우 **2**개의 버전과 최소 **10**일 분의 기록을 유지합니다.

사용 사례: 삭제 마커를 포함하여 현재 버전과 이전 버전의 전체 수명 주기를 관리하기 위해 다른 객체와 함께 특정 객체에 대한 고유한 규칙을 제공합니다. 이점: 스토리지 비용을 절감하고 버킷을 깔끔하게 유지하는 동시에 다양한 클라이언트 요구 사항을 충족할 수 있는 충분한 복구 지점과 기록을 유지합니다.

```
{
  "Rules": [
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    },
    {
      "ID": "accounts version retention",
      "Filter": {"Prefix":"account_"},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 4,
        "NoncurrentDays": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 2,
        "NoncurrentDays": 10
      }
    }
  ]
}
```

결론

- 정기적으로 수명 주기 정책을 검토하고 업데이트하고 이를 ILM 및 데이터 관리 목표에 맞춰 조정합니다.
- 의도한 대로 작동하는지 확인하기 위해 정책을 광범위하게 적용하기 전에 비생산 환경이나 버킷에서 테스트합니다.
- 논리 구조가 복잡해질 수 있으므로 규칙에 대한 설명적 ID를 사용하여 더 직관적으로 만드십시오.
- 버킷 수명 주기 정책이 저장소 사용량과 성능에 미치는 영향을 모니터링하여 필요한 조정을 실시합니다.

기술 보고서

StorageGRID 기술 보고서 소개

NetApp StorageGRID는 퍼블릭, 프라이빗 및 하이브리드 멀티 클라우드 환경에서 다양한 사용 사례를 지원하는 소프트웨어 정의 오브젝트 스토리지 제품군입니다. StorageGRID은 Amazon S3 API를 기본적으로 지원하며 자동화된 라이프사이클 관리와 같은 업계 최고의 혁신 기능을 제공하여 비정형 데이터를 장기적으로 비용 효율적으로 저장, 보호 및 보존합니다.

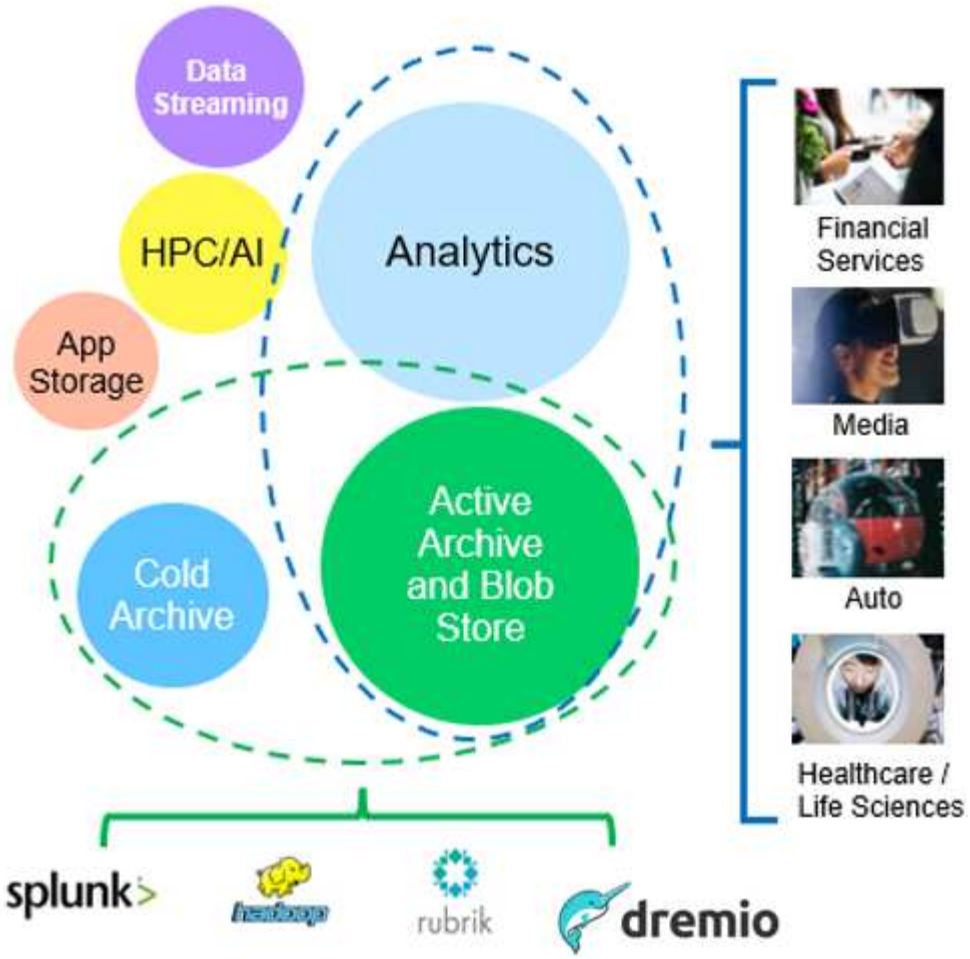
StorageGRID은 여러 StorageGRID 기능 및 통합에 대한 모범 사례와 권장 사항을 설명하는 문서를 제공합니다.

NetApp StorageGRID 및 빅데이터 분석

NetApp StorageGRID 사용 사례

NetApp StorageGRID 오브젝트 스토리지 솔루션은 확장성, 데이터 가용성, 보안 및 고성능을 제공합니다. 모든 규모와 다양한 산업 분야의 조직이 광범위한 사용 사례에 StorageGRID S3를 사용합니다. 몇 가지 일반적인 시나리오를 살펴보겠습니다.

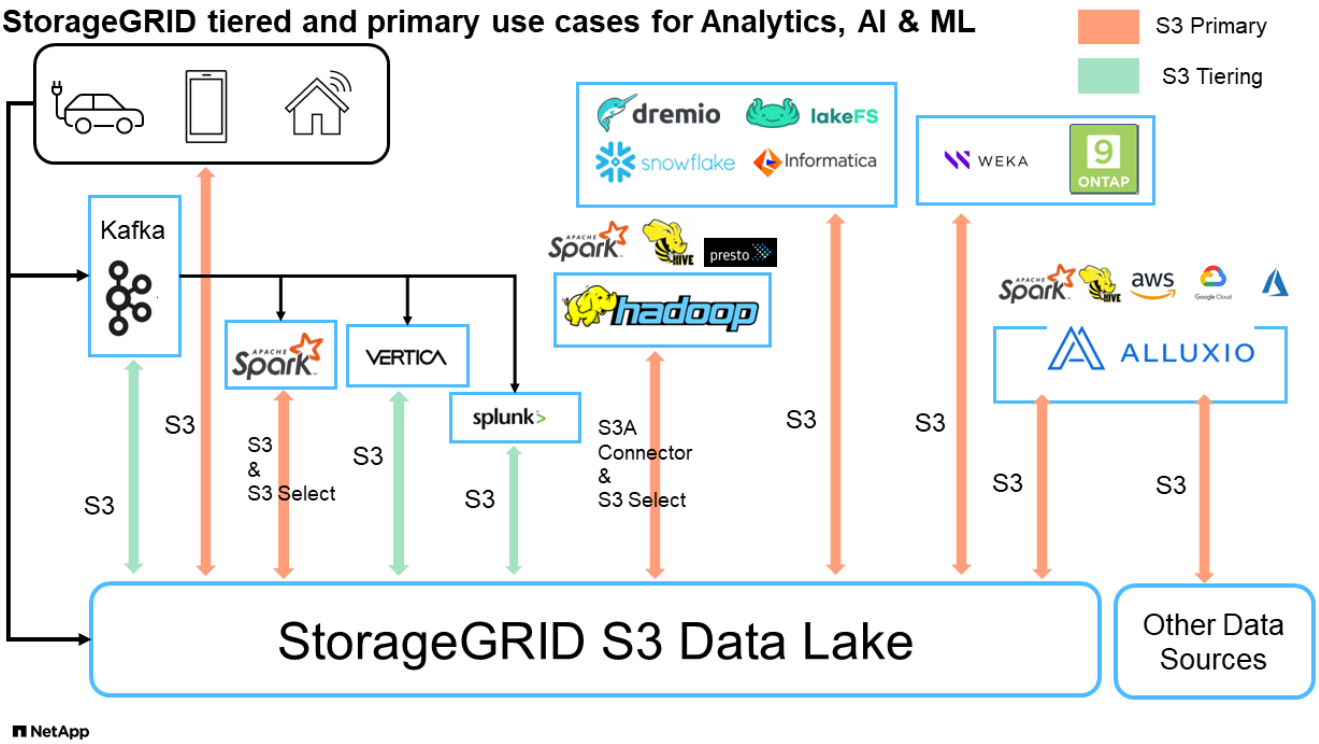
- 빅 데이터 분석: * StorageGRID S3는 기업에서 Apache Spark, Splunk Smartstore 및 Dremio와 같은 도구를 사용하여 분석을 위해 대량의 정형 및 비정형 데이터를 저장하는 데이터 레이크로 자주 사용됩니다.
- 데이터 계층화: * NetApp 고객은 ONTAP의 FabricPool 기능을 사용하여 고성능 로컬 계층 간에 데이터를 자동으로 StorageGRID로 이동합니다. 계층화하면 콜드 데이터를 저렴한 오브젝트 스토리지에서 즉시 사용 가능한 상태로 유지하면서 고가의 플래시 스토리지를 핫 데이터용으로 확보할 수 있습니다. 따라서 성능과 비용 절감 효과가 극대화됩니다.
- 데이터 백업 및 재해 복구: * 기업에서는 StorageGRID S3를 안정적이고 비용 효율적인 솔루션으로 사용하여 중요한 데이터를 백업하고 재해 발생 시 복구할 수 있습니다.
- 응용 프로그램용 데이터 저장: * StorageGRID S3는 응용 프로그램용 스토리지 백엔드로 사용할 수 있으므로 개발자가 파일, 이미지, 비디오 및 기타 유형의 데이터를 쉽게 저장하고 검색할 수 있습니다.
- 콘텐츠 전송: * StorageGRID S3를 사용하여 정적 웹 사이트 콘텐츠, 미디어 파일 및 소프트웨어 다운로드를 전 세계 사용자에게 저장하고 제공할 수 있으며, StorageGRID의 지리적 분산 및 글로벌 네임스페이스를 활용하여 빠르고 안정적인 콘텐츠 전송을 수행할 수 있습니다.
- 데이터 아카이브: * StorageGRID는 다양한 스토리지 유형을 제공하고 공용 장기 저비용 스토리지 옵션에 대한 계층화를 지원하며, 규정 준수 또는 기간별 목적으로 보존해야 하는 데이터의 보관 및 장기 보존에 이상적인 솔루션입니다.
- 오브젝트 스토리지 사용 사례 *



위 중 빅 데이터 분석은 최상위 사용 사례 중 하나이며 사용량이 증가하고 있습니다.

데이터 레이크에 **StorageGRID**를 사용해야 하는 이유

- 협업 증가 - 업계 표준 API 액세스를 지원하는 대규모 공유 멀티 사이트 멀티 테넌시
- 운영 비용 절감 - 자동 복구, 자동화된 단일 스케일아웃 아키텍처를 통해 운영 간소화
- 확장성 - 기존 Hadoop 및 데이터 웨어하우스 솔루션과 달리 StorageGRID S3 오브젝트 스토리지는 스토리지를 컴퓨팅과 데이터와 분리하므로 기업이 필요에 따라 스토리지 요구사항을 확장할 수 있습니다.
- 내구성 및 안정성 - StorageGRID는 99.9999999%의 내구성을 제공하여 저장된 데이터가 데이터 손실에 대한 저항성이 높습니다. 또한 고가용성을 제공하여 데이터에 항상 액세스할 수 있도록 보장합니다.
- 보안-StorageGRID는 암호화, 액세스 제어 정책, 데이터 라이프사이클 관리, 오브젝트 잠금 및 버전 관리와 같은 다양한 보안 기능을 제공하여 S3 버킷에 저장된 데이터를 보호합니다
- StorageGRID S3 데이터 레이크 *



S3 오브젝트 스토리지를 사용한 벤치마킹 데이터 웨어하우스 및 레이크하우스: 비교 연구

이 문서에서는 NetApp StorageGRID를 사용하는 다양한 데이터 웨어하우스 및 레이크하우스 에코시스템에 대한 포괄적인 벤치마크를 제공합니다. S3 오브젝트 스토리지에서 가장 뛰어난 성능을 제공하는 시스템을 결정하는 것이 목표입니다. 데이터와레호스/레이크하우스 아키텍처 및 테이블 형식(Parquet 및 Iceberg)에 대한 자세한 내용은 이 문서를 "아파치 아이스버그: 확실한 가이드"참조하십시오.

- 벤치마크 도구 - TPC-DS - https://www.tpc.org/tpcds/
- 빅 데이터 에코시스템
  - VM 클러스터, 각각 128G RAM 및 24개의 vCPU, 시스템 디스크용 SSD 스토리지
  - Hive 3.1.3 포함 Hadoop 3.3.5(이름 노드 1개 + 데이터 노드 4개)
  - Spark 3.0.0(마스터 1명 + 작업자 4명) 및 Hadoop 3.3.5 지원 델타 레이크
  - Dremio v25.2(코디네이터 1명 + 실행자 5명)
  - Trino v438(코디네이터 1명 + 작업자 5명)
  - Starburst v453(코디네이터 1명 + 작업자 5명)
- 오브젝트 스토리지
  - NetApp ® StorageGRID ® 11.8(SG6060 + SG1000 로드 밸런서 3개 포함
  - 개체 보호 - 복사본 2개(결과는 EC 2+1과 유사함)
- 데이터베이스 크기 1000GB
- Parquet 형식을 사용하여 각 쿼리 테스트에 대한 모든 에코시스템에서 캐시가 비활성화되었습니다. Iceberg 형식의 경우 캐시 사용 안 함 시나리오와 캐시 사용 시나리오 간에 S3 GET 요청 수와 총 쿼리 시간을 비교했습니다.

TPC-DS에는 벤치마킹을 위해 설계된 99개의 복잡한 SQL 쿼리가 포함되어 있습니다. 99개의 쿼리를 실행하는 데 걸린

총 시간을 측정하고 S3 요청의 유형과 수를 조사하여 상세 분석을 수행했습니다. 이 테스트에서는 널리 사용되는 두 가지 테이블 형식인 Parquet과 Iceberg의 효율성을 비교했습니다.

*파케 테이블 형식의 TPC-DS 쿼리 결과 *

에코시스템	하이브	델타 레이크	드리미오	트리노	별 모양
TPCDS 99 쿼리 총 시간(분)	1084[1]	55	36	32	28
S3 요청 분석	가져오기	1,117,184	2,074,610	3,939,690	1,504,212
1,495,039입니다	관찰: 모든 제품군 GET	80% 범위 32MB 객체에서 2KB ~ 2MB, 초당 50 ~ 100회의 요청	73% 범위는 32MB 개체에서 100KB 미만으로, 초당 1000 - 1400개의 요청 수입니다	90% 1M 바이트 범위는 256MB 객체, 초당 2500-3000개 요청에서 가져옵니다	범위 가져오기 크기: 100KB 미만 50%, 1MB 주위 16%, 2MB-9MB 27%, 초당 3500-4000개 요청
범위 가져오기 크기: 100KB 미만 50%, 1MB 주위 16%, 2MB-9MB 27%, 4000-5000 요청/초	개체 나열	312,053입니다	24,158입니다	120	509
512	머리 (존재하지 않는 객체)	156,027	12,103	96	0
0	머리 (존재하는 객체)	982,126	922,732	0	0
0	총 요청 수입니다	2,567,390입니다	3,033,603입니다	3,939.906	1,504,721번

1. 조회 번호 72를 완료할 수 없습니다

    ◦ Iceberg 테이블 형식의 TPC-DS 쿼리 결과 *

에코시스템	드리미오	트리노	별 모양
TPCDS 99 쿼리 + 총 시간(캐시 사용 안 함)	22	28	22
TPCDS 99 쿼리 + 총 2분(캐시 사용)	16	28	21.5입니다

에코시스템	드리미오	트리노	별 모양
S3 요청 분석	가져오기(캐시 사용 안 함)	1,985,922	938,639입니다
931,582를 참조하십시오	가져오기(캐시 사용)	611,347	30,158명
3,281	관찰: 모든 제품군 GET	범위 가져오기 크기: 67% 1MB, 15% 100KB, 10% 500KB, 3500 - 4500개 요청/초	범위 가져오기 크기: 100KB 미만 42%, 1MB 주위 17%, 2MB-9MB 33%, 초당 3500-4000개의 요청
범위 가져오기 크기: 100KB 미만 43%, 1MB 주위 17%, 2MB-9MB 33%, 4000-5000개의 요청/초	개체 나열	1465	0
0	머리 (존재하지 않는 객체)	1464	0
0	머리 (존재하는 객체)	3,702	509
509	총 요청 수(캐시 사용 안 함)	1,992,553	939,148입니다

Trino/Starburst 성능은 컴퓨팅 리소스에 의해 병목 현상이 발생했습니다. 클러스터에 RAM을 추가하면 총 쿼리 시간이 줄어듭니다.

첫 번째 표에서 볼 수 있듯이 Hive는 다른 현대 데이터 레이크하우스 생태계보다 상당히 느립니다. Hive는 많은 수의 S3 목록 오브젝트 요청을 보냈으며, 이는 일반적으로 모든 오브젝트 스토리지 플랫폼에서 느리며, 특히 많은 오브젝트가 포함된 버킷을 처리할 때 매우 느립니다. 이렇게 하면 전체 쿼리 기간이 크게 늘어납니다. 또한 현대적인 레이크하우스 생태계는 Hive의 초당 50-100개 요청에 비해 초당 2,000개에서 5,000개의 요청에 이르는 수많은 GET 요청을 동시에 전송할 수 있습니다. Hive 및 Hadoop S3A의 표준 파일 시스템은 S3 오브젝트 스토리지와 상호 작용할 때 Hive의 느린 속도에 기여합니다.

Hive 또는 Spark와 함께 Hadoop(HDFS 또는 S3 오브젝트 스토리지)을 사용하려면 Hadoop 및 Hive/Spark에 대한 폭넓은 지식이 필요하며, 각 서비스의 설정이 상호 작용하는 방식에 대한 이해가 필요합니다. 모두 1,000개 이상의 설정이 있으며, 그 중 다수는 상호 연관되어 있으며 독립적으로 변경할 수 없습니다. 설정과 값을 최적으로 조합하려면 엄청난 시간과 노력이 필요합니다.

Parquet와 Iceberg 결과를 비교하면 테이블 형식이 중요한 성능 요인이라는 것을 알 수 있습니다. Iceberg 테이블 형식은 S3 요청 수 면에서 Parquet보다 더 효율적이며, Parquet 형식에 비해 요청 수가 35%~50% 적습니다.

Dremio, Trino 또는 Starburst의 성능은 주로 클러스터의 컴퓨팅 능력에 의해 구동됩니다. 이 세 가지 모두 S3 오브젝트 스토리지 연결에 S3A 커넥터를 사용하지만 Hadoop이 필요하지 않으며 Hadoop의 fs.s3a 설정 대부분은 이러한 시스템에서 사용되지 않습니다. 따라서 다양한 Hadoop S3A 설정을 학습하고 테스트할 필요가 없으므로 성능 조정이 간소화됩니다.

이 벤치마크 결과에서 알 수 있듯이, S3 기반 워크로드에 최적화된 빅데이터 분석 시스템이 주요 성능 요소라는 결론을 내릴 수 있습니다. 최신 레이크하우스는 쿼리 실행을 최적화하고 메타데이터를 효율적으로 사용하며 S3 데이터에 대한 원활한 액세스를 제공하므로 S3 스토리지로 작업할 때 Hive보다 성능이 향상됩니다.

StorageGRID를 사용하여 Dremio S3 데이터 소스를 구성하려면 이 항목을 "페이지" 참조하십시오.

아래 링크를 방문하여 StorageGRID와 Dremio가 함께 작동하여 현대적이고 효율적인 데이터 레이크 인프라를 제공하는 방법과 NetApp가 Hive+ HDFS에서 Dremio+ StorageGRID로 마이그레이션하여 빅데이터 분석 효율성을 획기적으로 개선한 방법에 대해 자세히 알아보십시오.

- "NetApp StorageGRID로 빅데이터의 성능을 향상하십시오"
- "StorageGRID 및 Dremio를 사용하는 현대적이고 강력하고 효율적인 데이터 레이크 인프라"
- "NetApp이 제품 분석을 통해 고객 경험을 재정의하는 방법"

Hadoop S3A 튜닝

안젤라 청 _ 에 의해

Hadoop S3A 커넥터는 Hadoop 기반 애플리케이션과 S3 오브젝트 스토리지 간의 원활한 상호 작용을 지원합니다. S3 오브젝트 스토리지로 작업할 때 성능을 최적화하려면 Hadoop S3A Connector를 튜닝해야 합니다. 세부 조정을 시작하기에 앞서, Hadoop과 그 구성 요소에 대한 기본적인 이해를 갖췄습니다.

Hadoop이란?

- Hadoop * 은 대규모 데이터 처리 및 스토리지를 처리하도록 설계된 강력한 오픈 소스 프레임워크입니다. 이를 통해 컴퓨터 클러스터 간에 분산 스토리지 및 병렬 처리가 가능합니다.

Hadoop의 3가지 핵심 구성 요소는 다음과 같습니다.

- * Hadoop HDFS (Hadoop 분산 파일 시스템) * : 스토리지를 처리하고 데이터를 블록으로 분할하여 노드에 분산시킵니다.
- * Hadoop MapReduce *: 작업을 작은 청크로 분할하고 병렬로 실행하여 데이터를 처리합니다.
- * Hadoop YARN (또 다른 리소스 협상 담당자) : * "리소스를 관리하고 작업을 효율적으로 예약합니다"

Hadoop HDFS 및 S3A 커넥터

HDFS는 Hadoop 에코시스템의 핵심 구성 요소로, 효율적인 빅 데이터 처리에 중요한 역할을 합니다. HDFS는 안정적인 스토리지 및 관리를 지원합니다. 병렬 처리 및 최적화된 데이터 스토리지를 보장하여 데이터 액세스 및 분석 속도가 빨라집니다.

빅데이터 처리 시 HDFS는 대규모 데이터 세트를 위한 내결함성 스토리지를 제공하는 데 탁월합니다. 이 점은 데이터 복제를 통해 실현됩니다. 데이터 웨어하우스 환경에서 대량의 정형 데이터와 비정형 데이터를 저장하고 관리할 수 있습니다. 또한 Apache Spark, Hive, Pig 및 Flink와 같은 선도적인 빅 데이터 처리 프레임워크와 원활하게 통합되어 확장 가능하고 효율적인 데이터 처리가 가능합니다. Unix 기반(Linux) 운영 체제와 호환되기 때문에 빅 데이터 처리를 위해 Linux 기반 환경을 사용하는 것을 선호하는 기업에 이상적인 선택입니다.

시간이 지나면서 데이터 볼륨이 증가함에 따라 자체 컴퓨팅 및 스토리지를 사용하여 Hadoop 클러스터에 새 시스템을 추가하는 방식이 비효율적이 되었습니다. 선형적으로 확장하면 리소스를 효율적으로 사용하고 인프라를 관리하는 데 어려움이 발생합니다.

이러한 과제를 해결하기 위해 Hadoop S3A 커넥터는 S3 오브젝트 스토리지에 대한 고성능 I/O를 제공합니다. S3A를 사용하여 Hadoop 워크플로우를 구축하면 오브젝트 스토리지를 데이터 저장소로 활용할 수 있으며, 컴퓨팅과 스토리지를 독립적으로 확장할 수 있는 분리된 컴퓨팅 및 스토리지를 사용할 수 있습니다. 또한 컴퓨팅과 스토리지를 분리하면 컴퓨팅 작업에 적절한 양의 리소스를 투입하고 데이터 세트의 크기에 따라 용량을 제공할 수 있습니다. 따라서 Hadoop 워크플로우의 전체 TCO를 줄일 수 있습니다.

Hadoop S3A 커넥터 튜닝

S3는 HDFS와 다르게 동작하며 파일 시스템의 모양을 유지하려는 일부 시도는 공격적으로 최적화되지 않습니다. S3 리소스를 가장 효율적으로 활용하려면 신중한 튜닝/테스트/실험이 필요합니다.

이 문서의 Hadoop 옵션은 Hadoop 3.3.5를 기반으로 합니다. 을 참조하십시오 "Hadoop 3.3.5 core-site.xml" 사용 가능한 모든 옵션

참고 – 일부 Hadoop fs.s3a 설정의 기본값은 Hadoop 버전마다 다릅니다. 현재 Hadoop 버전과 관련된 기본값을 확인하십시오. 이러한 설정이 Hadoop core-site.xml에 지정되지 않은 경우 기본값이 사용됩니다. Spark 또는 Hive 구성 옵션을 사용하여 런타임에 값을 재정의할 수 있습니다.

이 페이지로 이동해야 합니다 "아파치 하둡 페이지" 각 fs.s3a 옵션을 이해합니다. 가능한 경우 비운영 Hadoop 클러스터에서 테스트하여 최적의 값을 찾습니다.

읽어야 합니다 "S3A 커넥터로 작업할 때 성능을 극대화합니다" 기타 튜닝 권장 사항

몇 가지 주요 고려 사항을 살펴보겠습니다.

- 1. 데이터 압축 *

StorageGRID 압축을 활성화하지 마십시오. 대부분의 빅 데이터 시스템은 전체 객체를 검색하는 대신 바이트 범위 GET를 사용합니다. 압축된 객체와 함께 GET 바이트 범위를 사용하면 GET 성능이 크게 저하됩니다.

- 2. S3A 커밋 *

일반적으로 magic s3a committer가 권장됩니다. 이를 참조하십시오 "일반 S3A 커밋 옵션 페이지" 마법 커밋 및 관련 s3a 설정에 대한 더 나은 이해를 얻기 위해.

매직 커미터:

Magic Committer는 특히 S3Guard에 의존하여 S3 오브젝트 저장소에서 일관된 디렉토리 목록을 제공합니다.

이제 일관된 S3(이 경우)를 통해 Magic Committer를 모든 S3 버킷과 함께 안전하게 사용할 수 있습니다.

선택 및 실험:

사용 사례에 따라 클러스터 HDFS 파일 시스템에 의존하는 스테이징 커밋자와 Magic committer 중에서 선택할 수 있습니다.

두 가지를 모두 실험하여 귀사의 워크로드 및 요구사항에 가장 적합한 솔루션을 결정하십시오.

요약하면, S3A committers는 S3에 대한 일관적이고, 고성능의 안정적인 출력 약속이라는 근본적인 과제에 대한 솔루션을 제공합니다. 내부 설계로 데이터 무결성을 유지하면서 효율적인 데이터 전송을 보장합니다.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable “magic committer” support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

- 3. 스레드, 연결 풀 크기 및 블록 크기 *
- 단일 버킷과 상호 작용하는 각 * S3A * 클라이언트에는 업로드 및 복사 작업을 위한 개방형 HTTP 1.1 연결 전용 풀과 스레드가 있습니다.
- "이러한 풀 크기를 조정하여 성능과 메모리/스레드 사용량 간의 균형을 맞출 수 있습니다".
- S3에 데이터를 업로드하면 블록으로 나뉩니다. 기본 블록 크기는 32MB입니다. fs.s3a.block.size 속성을 설정하여 이 값을 사용자 지정할 수 있습니다.
- 블록 크기가 클수록 업로드 시 다중 파트 관리 오버헤드를 줄여 대용량 데이터 업로드의 성능을 향상시킬 수 있습니다. 대용량 데이터 세트의 권장 값은 256MB 이상입니다.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

- 4. 멀티 파트 업로드 *

s3a committers * 항상 * MPU(멀티 파트 업로드)를 사용하여 데이터를 S3 버킷에 업로드합니다. 작업 실패, 추측에 의한 작업 실행, 커밋 전 작업 중단 등을 허용하기 위해 필요합니다. 다음은 다중 파트 업로드와 관련된 몇 가지 주요 사양입니다.

- 최대 개체 크기: 5TiB(테라바이트)
- 업로드당 최대 부품 수: 10,000.
- 부품 번호: 1 ~ 10,000 범위(포함).
- 부품 크기: 5MiB에서 5GiB 사이. 멀티 파트 업로드의 마지막 부분에 대한 최소 크기 제한은 없습니다.

S3 멀티 파트 업로드에 더 작은 파트 크기를 사용하면 장점과 단점이 모두 있습니다.

- 장점 *:
- 네트워크 문제에서 빠른 복구: 작은 부품을 업로드하면 네트워크 오류로 인해 실패한 업로드를 다시 시작할 때의 영향이 최소화됩니다. 부품에 오류가 발생하면 전체 오브젝트가 아닌 특정 부분만 다시 업로드하면 됩니다.
- 향상된 병렬 처리: 다중 스레딩 또는 동시 연결을 활용하여 더 많은 파트를 병렬로 업로드할 수 있습니다. 이 병렬화는 특히 큰 파일을 처리할 때 성능을 향상시킵니다.

- 단점 *:
- 네트워크 오버헤드: 파트 크기가 작을수록 업로드할 파트가 더 많아지며 각 파트마다 자체 HTTP 요청이 필요합니다. HTTP 요청이 많을수록 개별 요청을 시작 및 완료하는 데 따르는 오버헤드가 증가합니다. 많은 수의 작은 파트를 관리하면 성능에 영향을 줄 수 있습니다.
- 복잡성: 주문 관리, 부품 추적, 성공적인 업로드 보장은 번거로울 수 있습니다. 업로드를 중단해야 하는 경우 이미 업로드한 모든 부품을 추적하고 제거해야 합니다.

Hadoop의 경우 fs.s3a.multipart.size에 256MB 이상의 파트 크기가 권장됩니다. 항상 fs.s3a.mutlipart.threshold 값을 2 x fs.s3a.multipart.size 값으로 설정하십시오. 예를 들어 fs.s3a.multipart.size=256M,fs.s3a.mullipart.threshold는 512M이어야 합니다.

대형 데이터 세트에 더 큰 파트 크기를 사용합니다. 특정 사용 사례와 네트워크 상태에 따라 이러한 요소의 균형을 맞추는 부품 크기를 선택하는 것이 중요합니다.

다중 부분 업로드는 입니다 "3단계 프로세스":

1. 업로드가 시작되면 StorageGRID에서 업로드 ID를 반환합니다.
2. 개체 부분은 upload-id를 사용하여 업로드됩니다.
3. 모든 객체 부분이 업로드되면 는 업로드 ID와 함께 완전한 멀티 파트 업로드 요청을 보냅니다. StorageGRID는 업로드된 부분에서 객체를 생성하며 클라이언트는 객체에 액세스할 수 있습니다.

전체 다중 파트 업로드 요청이 성공적으로 전송되지 않으면 부품은 StorageGRID에 남아 있고 객체를 생성하지 않습니다. 이 문제는 작업이 중단, 실패 또는 중단될 때 발생합니다. 업로드가 시작된 후 15일이 경과하면 멀티 파트 업로드가 완료되거나 중단되거나 StorageGRID가 이러한 부품을 제거할 때까지 파트가 그리드에 남아 있습니다. 버킷에 여러 개의(수억 ~ 수백만) 진행 중인 멀티 파트 업로드가 있는 경우 Hadoop이 'list-multipart-uploads’를 전송할 때(이 요청은 업로드 ID로 필터링되지 않음) 요청을 완료하는 데 시간이 오래 걸리거나 시간이 초과될 수 있습니다. 적절한 fs.s3a.mutlipart.purge를 true로 설정하여 적절한 fs.s3a.multipart.purge.age 값을 설정할 수 있습니다(예: 5-7일, 기본값 86400, 즉 1일을 사용하지 마십시오). 또는 NetApp 지원 팀에 문의하여 상황을 조사하십시오.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

- 5. 메모리의 버퍼 쓰기 데이터 *

성능을 높이기 위해 쓰기 데이터를 S3에 업로드하기 전에 메모리에 버퍼링할 수 있습니다. 이렇게 하면 작은 쓰기 수를 줄이고 효율성을 높일 수 있습니다.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

S3 및 HDFS는 서로 다른 방식으로 작동한다는 점을 기억하십시오. S3 리소스를 가장 효율적으로 활용하려면 신중한

튜닝/테스트/실험이 필요합니다.

TR-4871: Commvault로 백업 및 복구용으로 StorageGRID를 구성합니다

StorageGRID 및 Commvault를 사용하여 데이터를 백업하고 복구합니다

CommVault와 NetApp은 파트너 관계를 통해 Commvault의 전체 백업 및 복구 NetApp 기능을 클라우드 스토리지용 NetApp StorageGRID 소프트웨어와 결합하여 공동 데이터 보호 솔루션을 구축했습니다. CommVault의 완벽한 백업 및 복구 및 NetApp StorageGRID는 전 세계적으로 빠르게 증가하는 데이터 및 늘어나는 규제에 대한 요구 사항을 충족할 수 있도록 지원하는 사용하기 쉬운 고유한 솔루션을 제공합니다.

많은 조직은 스토리지를 클라우드로 마이그레이션하고, 시스템을 확장하고, 데이터의 장기 보존을 위한 정책을 자동화하려고 합니다. 클라우드 기반 오브젝트 스토리지는 복원력, 확장 기능, 운영 및 비용 효율성으로 잘 알려져 있으며, 이를 백업 대상으로 자연스럽게 선택할 수 있습니다. CommVault와 NetApp는 2014년에 통합 솔루션을 공동으로 인증했으며 그 이후 두 솔루션 간의 통합을 더욱 강화했습니다. 전 세계 모든 유형의 고객이 Commvault Complete 백업 및 복구 및 StorageGRID 통합 솔루션을 채택했습니다.

Commvault 및 StorageGRID 정보

CommVault Complete Backup and Recovery 소프트웨어는 처음부터 단일 플랫폼에서 통합된 코드 베이스로 구축된 엔터프라이즈급 통합 데이터 및 정보 관리 솔루션입니다. 모든 기능은 백엔드 기술을 공유하므로 데이터 보호, 관리 및 액세스에 대해 완벽하게 통합된 접근 방식의 탁월한 장점과 이점을 제공합니다. 이 소프트웨어에는 데이터를 보호, 보관, 분석, 복제 및 검색하는 모듈이 포함되어 있습니다. 이 모듈은 서로 원활하게 상호 작용하는 공통 백엔드 서비스와 고급 기능을 공유합니다. 이 솔루션은 기업의 모든 데이터 관리 측면을 해결하는 동시에 무한한 확장성과 데이터 및 정보에 대한 전례 없는 제어를 제공합니다.

Commvault 클라우드 계층인 NetApp StorageGRID는 엔터프라이즈 하이브리드 클라우드 오브젝트 스토리지 솔루션입니다. 이 제품은 특별 제작된 어플라이언스나 소프트웨어 정의 구축을 통해 여러 사이트에 배포할 수 있습니다. StorageGRID을 사용하면 데이터를 저장 및 보호하는 방법을 결정하는 데이터 관리 정책을 설정할 수 있습니다. StorageGRID는 정책을 개발하고 적용하는 데 필요한 정보를 수집합니다. 또한 성능, 내구성, 가용성, 지리적 위치, 운영 효율성 요구사항을 비롯한 다양한 특성과 요구사항을 지속 가능성, 비용. 데이터는 여러 위치 간에 이동하는 동안 또는 데이터가 노후화되는 시기에 완벽하게 관리되고 보호됩니다.

StorageGRID 지능형 정책 엔진을 활용하면 다음 옵션 중 하나를 선택할 수 있습니다.

- 삭제 코딩을 사용하여 복원력을 위해 여러 사이트에서 데이터를 백업합니다.
- 오브젝트를 원격 사이트에 복사하여 WAN 지연 시간 및 비용을 최소화합니다.

StorageGRID에서 오브젝트를 저장할 때 오브젝트는 위치나 복사본의 수에 상관없이 하나의 오브젝트로 액세스합니다. 이 동작은 재해 복구에 매우 중요합니다. 데이터의 백업 복사본 하나가 손상된 경우에도 StorageGRID에서 데이터를 복원할 수 있기 때문입니다.

백업 데이터를 기본 스토리지에 보관하는 것은 비용이 많이 들 수 있습니다. NetApp StorageGRID를 사용하면 비활성 백업 데이터를 StorageGRID로 마이그레이션하여 기본 스토리지의 공간을 늘릴 수 있고 StorageGRID의 다양한 기능을 활용할 수 있습니다. 시간이 지나면 백업 데이터의 가치가 변경되고 백업 데이터를 저장하는 비용도 변경됩니다. StorageGRID를 사용하면 운영 스토리지의 비용을 최소화하면서 데이터의 내구성을 높일 수 있습니다.

주요 기능

Commvault 소프트웨어 플랫폼의 주요 기능은 다음과 같습니다.

- 가상 및 물리적 서버, NAS 시스템, 클라우드 기반 인프라 및 모바일 장치에서 모든 주요 운영 체제, 애플리케이션 및 데이터베이스를 지원하는 완벽한 데이터 보호 솔루션입니다.
- 단일 콘솔을 통한 간편한 관리: 기업 전체의 모든 기능과 모든 데이터 및 정보를 보고 관리하고 액세스할 수 있습니다.
- 데이터 백업 및 아카이빙, 스냅샷 관리, 데이터 복제, e-discovery용 콘텐츠 인덱싱 등 다양한 보호 방법
- 디스크 및 클라우드 스토리지에 대한 중복 제거 기능을 사용하여 스토리지를 효율적으로 관리
- AFF, FAS, NetApp HCI, E-Series 어레이 및 NetApp SolidFire ® 스케일아웃 스토리지 시스템과 같은 NetApp 스토리지 시스템과의 통합 또한 NetApp Cloud Volumes ONTAP 소프트웨어와 통합하여 NetApp 스토리지 포트폴리오 전반에서 인덱싱된 애플리케이션 인식 NetApp Snapshot ™ 복사본 생성을 자동화합니다.
- 업계 최고의 온프레미스 가상 하이퍼바이저 및 퍼블릭 클라우드 하이퍼스케일러 플랫폼을 지원하는 완벽한 가상 인프라 관리
- 고급 보안 기능으로 중요한 데이터에 대한 액세스를 제한하고, 세분화된 관리 기능을 제공하며, Active Directory 사용자에게 SSO(Single Sign-On) 액세스를 제공합니다.
- 정책 기반 데이터 관리: 물리적 위치가 아닌 비즈니스 요구사항에 따라 데이터를 관리할 수 있도록 지원합니다.
- 사용자가 데이터를 보호, 검색 및 복구할 수 있는 최첨단 최종 사용자 환경을 제공합니다.
- API 기반 자동화를 통해 vRealize Automation 또는 Service Now와 같은 타사 툴을 사용하여 데이터 보호 및 복구 작업을 관리할 수 있습니다.

지원되는 워크로드에 대한 자세한 내용은 를 "CommVault의 지원 기술"참조하십시오.

백업 옵션

Commvault Complete 백업 및 복구 소프트웨어와 클라우드 스토리지를 구축한 경우 두 가지 백업 옵션이 있습니다.

- 운영 디스크 타겟에 백업하고 클라우드 스토리지에 보조 복사본을 백업합니다.
- 1차 타겟으로 클라우드 스토리지에 백업

과거에는 클라우드 또는 오브젝트 스토리지 성능이 운영 백업에 너무 낮은 것으로 간주되었습니다. 기본 디스크 타겟을 사용하면 백업 및 복원 프로세스가 더 빨라졌으며, 클라우드에 보조 복사본을 콜드 백업으로 유지할 수 있었습니다. StorageGRID은 차세대 오브젝트 스토리지를 나타냅니다. StorageGRID는 다른 오브젝트 스토리지 공급업체보다 뛰어난 성능과 높은 처리량뿐만 아니라 성능 및 유연성을 제공할 수 있습니다.

다음 표에는 StorageGRID의 각 백업 옵션의 이점이 나와 있습니다.

	디스크에 대한 기본 백업 및 **StorageGRID**에 대한 보조 복사	**StorageGRID**에 기본 백업
성능	라이브 마운트 또는 라이브 복구를 사용하는 가장 빠른 복구 시간: 계층 0/계층 1 워크로드에 가장 적합합니다.	라이브 마운트 또는 라이브 복구 작업에 사용할 수 없습니다. 스트리밍 복원 작업 및 장기 보존에 적합합니다.

	디스크에 대한 기본 백업 및 **StorageGRID**에 대한 보조 복사	**StorageGRID**에 기본 백업
구축 아키텍처	첫 번째 백업 랜딩 계층으로 All-Flash 또는 회전식 디스크를 사용합니다. StorageGRID는 보조 계층으로 사용됩니다.	StorageGRID를 포괄적인 백업 타겟으로 사용하여 구축을 단순화합니다.
고급 기능(실시간 복원)	지원	지원되지 않습니다

추가 정보를 찾을 수 있는 위치

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

- StorageGRID 11.9 설명서 센터+ https://docs.netapp.com/us-en/storagegrid-119/
- NetApp 제품 설명서 https://docs.netapp.com
- Commvault 설명서 https://documentation.commvault.com/2024/essential/index.html

테스트된 솔루션 개요

테스트를 거친 솔루션은 Commvault 및 NetApp 솔루션을 결합하여 강력한 공동 솔루션을 제공합니다.

솔루션 설정

랩 설정에서 StorageGRID 환경은 4개의 NetApp StorageGRID SG5712 어플라이언스, 1개의 가상 기본 관리 노드 및 1개의 가상 게이트웨이 노드로 구성되었습니다. SG5712 어플라이언스는 엔트리 레벨 옵션으로서 기본 구성입니다. NetApp StorageGRID SG5760 또는 SG6060과 같은 고성능 어플라이언스 옵션을 선택하면 큰 성능 이점을 얻을 수 있습니다. 사이징 지원은 NetApp StorageGRID 솔루션 설계자에게 문의하십시오.

StorageGRID는 데이터 보호 정책을 위해 통합 라이프사이클 관리(ILM) 정책을 사용하여 데이터를 관리하고 보호합니다. ILM 규칙은 위에서 아래로 정책에서 평가됩니다. 다음 표에 나와 있는 ILM 정책을 구현했습니다.

ILM 규칙	한정자	수집 동작
삭제 코딩 2+1	200KB를 넘는 오브젝트	균형
2 복사	모든 개체	이중 커밋

ILM 2 Copy 규칙이 기본 규칙입니다. 이 테스트에서는 삭제 코딩 2+1 규칙이 200KB 이상의 객체에 적용되었습니다. 200KB보다 작은 개체에 기본 규칙이 적용되었습니다. 이러한 방식으로 규칙을 적용하는 것이 StorageGRID 모범 사례입니다.

이 테스트 환경에 대한 자세한 기술 정보는 의 솔루션 설계 및 모범 사례 섹션을 참조하십시오 "Commvault 및 NetApp 스케일아웃 데이터 보호" 기술 보고서:

StorageGRID 하드웨어 사양

다음 표에서는 이 테스트에 사용된 NetApp StorageGRID 하드웨어를 설명합니다. 10Gbps 네트워킹을 지원하는 StorageGRID SG5712 어플라이언스는 엔트리 레벨 옵션으로 기본 구성을 나타냅니다. 선택적으로 SG5712를 25Gbps 네트워킹용으로 구성할 수 있습니다.

하드웨어	수량	디스크	가용 용량	네트워크
StorageGRID SG5712 어플라이언스	4	48 x 4TB(니어라인 SAS HDD)	136TB	10Gbps

NetApp StorageGRID SG5760, SG6060 또는 All-Flash SGF6112 어플라이언스와 같은 고성능 어플라이언스 옵션을 선택하면 중요한 성능 이점을 제공할 수 있습니다. 사이징 지원은 NetApp StorageGRID 솔루션 설계자에게 문의하십시오.

Commvault 및 **StorageGRID** 소프트웨어 요구사항

다음 표에는 테스트를 위해 VMware 소프트웨어에 설치된 Commvault 및 NetApp StorageGRID 소프트웨어에 대한 소프트웨어 요구 사항이 나와 있습니다. MediaAgent 데이터 전송 관리자 4개와 CommServe 서버 1개가 설치되었습니다. 이 테스트에서는 VMware 인프라에 10Gbps 네트워킹이 구현되었습니다. 다음 표를 참조하십시오

다음 표에는 Commvault 소프트웨어의 전체 시스템 요구사항이 나와 있습니다.

구성 요소	수량	데이터 저장소	크기	합계	필요한 총 **IOPS**입니다
CommServe 서버	1	OS	500GB	500GB	해당 없음
		SQL	500GB	500GB	해당 없음
MediaAgent를 선택합니다	4	가상 CPU(vCPU)	16	64	해당 없음
		RAM	128GB	512	해당 없음
		OS	500GB	2TB	해당 없음
		인덱스 캐시	2TB	8TB	200 이상
		DDB입니다	2TB	8TB	200-80,000K입니다

테스트 환경에서는 NetApp E-Series E2812 스토리지 어레이의 VMware에 기본 관리 노드 1개와 가상 게이트웨이 노드 1개가 구축되었습니다. 각 노드는 다음 표에 설명된 최소 운영 환경 요구 사항을 갖춘 별도의 서버에 있었습니다.

다음 표에는 StorageGRID 가상 관리자 노드 및 게이트웨이 노드에 대한 요구 사항이 나와 있습니다.

노드 유형입니다	수량	**vCPU**	**RAM**	스토리지
게이트웨이 노드	1	8	24GB	OS용 100GB LUN
관리자 노드	1	8	24GB	OS용 100GB LUN 관리자 노드 테이블용 200GB LUN 관리자 노드 감사 로그용 200GB LUN

StorageGRID 사이징 가이드

귀사 환경의 특정 사이징에 대해서는 NetApp 데이터 보호 전문가에게 문의하십시오. NetApp 데이터 보호 전문가는 Commvault Total Backup Storage Calculator 툴을 사용하여 백업 인프라스트럭처 요구 사항을 추정할 수 있습니다. 이 도구를 사용하려면 Commvault Partner Portal에 액세스해야 합니다. 필요한 경우 액세스를 위해 등록합니다.

Commvault 크기 조정 입력

다음 작업을 사용하여 데이터 보호 솔루션의 크기 조정을 위한 검색을 수행할 수 있습니다.

- 보호해야 하는 시스템 또는 애플리케이션/데이터베이스 워크로드와 프런트 엔드 용량(테라바이트[TB])을 식별합니다.
- 보호해야 하는 VM/파일 워크로드 및 이와 유사한 프런트엔드 용량(TB)을 식별합니다.
- 단기 및 장기 보존 요구 사항 파악
- 식별된 데이터 세트/작업 부하에 대한 일별 변경률 확인
- 향후 12개월, 24개월 및 36개월간 예상되는 데이터 증가율을 식별합니다.
- 비즈니스 요구사항에 따라 데이터 보호/복구를 위한 RTO 및 RPO 정의

이 정보를 사용할 수 있게 되면 백업 인프라스트럭처 사이징을 수행하여 필요한 스토리지 용량을 분석할 수 있습니다.

StorageGRID 사이징 가이드

NetApp StorageGRID 사이징을 수행하기 전에 워크로드의 다음 측면을 고려하십시오.

- 사용 가능한 용량
- WORM 모드
- 평균 개체 크기입니다
- 성능 요구사항
- ILM 정책이 적용되었습니다

사용 가능한 용량은 StorageGRID로 계층화한 백업 워크로드의 크기 및 보존 일정에 맞게 조정되어야 합니다.

WORM 모드가 활성화되거나 비활성화됩니까? Commvault에서 WORM을 활성화하면 StorageGRID에서 오브젝트 잠금이 구성됩니다. 이렇게 하면 필요한 오브젝트 스토리지 용량이 증가합니다. 필요한 용량은 보존 기간 및 각 백업에서 변경된 객체 수에 따라 달라집니다.

평균 개체 크기는 StorageGRID 환경의 성능을 사이징하는 데 도움이 되는 입력 매개 변수입니다. Commvault 워크로드에 사용되는 평균 개체 크기는 백업 유형에 따라 다릅니다.

다음 표에는 백업 유형별로 평균 개체 크기가 나열되어 있으며 복원 프로세스에서 개체 저장소에서 읽는 내용이 설명되어 있습니다.

백업 유형	평균 개체 크기	복원 동작
StorageGRID에서 보조 복사본을 만듭니다	32MB	32MB 객체의 전체 읽기
백업을 StorageGRID로 전송(중복 제거 사용)	8MB	1MB 랜덤 범위 읽기
백업을 StorageGRID로 전송(중복 제거 사용 안 함)	32MB	32MB 객체의 전체 읽기

또한 전체 백업 및 증분 백업에 대한 성능 요구 사항을 이해하면 StorageGRID 스토리지 노드의 크기를 결정하는 데 도움이 됩니다. StorageGRID ILM(정보 라이프사이클 관리) 정책 데이터 보호 방법은 Commvault 백업을 저장하는 데 필요한 용량을 결정하고 그리드 사이징에 영향을 줍니다.

StorageGRID ILM 복제는 StorageGRID에서 오브젝트 데이터를 저장하는 데 사용하는 두 가지 메커니즘 중 하나입니다. StorageGRID에서 데이터를 복제하는 ILM 규칙에 개체를 할당하면 시스템은 오브젝트 데이터의 정확한 복사본을 생성하고 이 복사본을 스토리지 노드에 저장합니다.

삭제 코딩은 StorageGRID에서 오브젝트 데이터를 저장하는 데 사용하는 두 번째 방법입니다. StorageGRID에서 삭제 코딩 복사본을 생성하도록 구성된 ILM 규칙에 오브젝트를 할당하면 오브젝트 데이터를 데이터 조각으로 분할합니다. 그런 다음 추가 패리티 조각을 계산하고 각 조각을 서로 다른 스토리지 노드에 저장합니다. 개체에 액세스하면 저장된 조각을 사용하여 다시 조립됩니다. 패리티 조각이 손상되거나 손실된 경우 삭제 코딩 알고리즘을 통해 남은 데이터 및 패리티 조각의 일부를 사용하여 해당 조각을 다시 생성할 수 있습니다.

이 두 메커니즘에는 다음과 같은 예가 보여 주는 것처럼 서로 다른 양의 스토리지가 필요합니다.

- 복제된 복사본 2개를 저장하면 스토리지 오버헤드가 두 배로 증가합니다.
- 2+1 삭제 코딩 복사본을 저장할 경우 스토리지 오버헤드가 1.5배 증가합니다.

테스트 대상인 솔루션의 경우, 단일 사이트에 엔트리 레벨의 StorageGRID 배포를 사용했습니다.

- 관리 노드: VMware 가상 머신(VM)
- 로드 밸런서: VMware VM
- 스토리지 노드: 4TB 드라이브 장착 시 SG5712 4개
- 기본 관리자 노드 및 게이트웨이 노드: 운영 워크로드 요구 사항이 최소인 VMware VM

StorageGRID는 또한 타사 로드 밸런서를 지원합니다.

StorageGRID는 일반적으로 데이터를 복제하는 데이터 보호 정책을 사용하여 노드 및 사이트 수준 장애로부터 데이터를 보호하는 두 개 이상의 사이트에 구축됩니다. 데이터를 StorageGRID에 백업하면 알고리즘을 통해 안정적으로 데이터를 분리 및 재조립하는 삭제 코딩이나 여러 복사본을 사용해 데이터를 보호할 수 있습니다.

사이징 툴을 사용할 수 있으며 "Fusion" 그리드의 크기를 조정합니다.

확장

스토리지 노드에 스토리지를 추가하거나, 기존 사이트에 새 그리드 노드를 추가하거나, 새 데이터 센터 사이트를 추가하여 NetApp StorageGRID 시스템을 확장할 수 있습니다. 현재 시스템의 운영을 중단하지 않고도 확장을 수행할 수 있습니다.
StorageGRID는 스토리지 노드에 고성능 노드를 사용하거나 로드 밸런서와 관리 노드를 실행하는 물리적 어플라이언스에 사용하거나 노드를 추가하기만 하면 성능을 확장할 수 있습니다.

StorageGRID 시스템 확장에 대한 자세한 내용은 를 "StorageGRID 11.9 확장 가이드"참조하십시오.

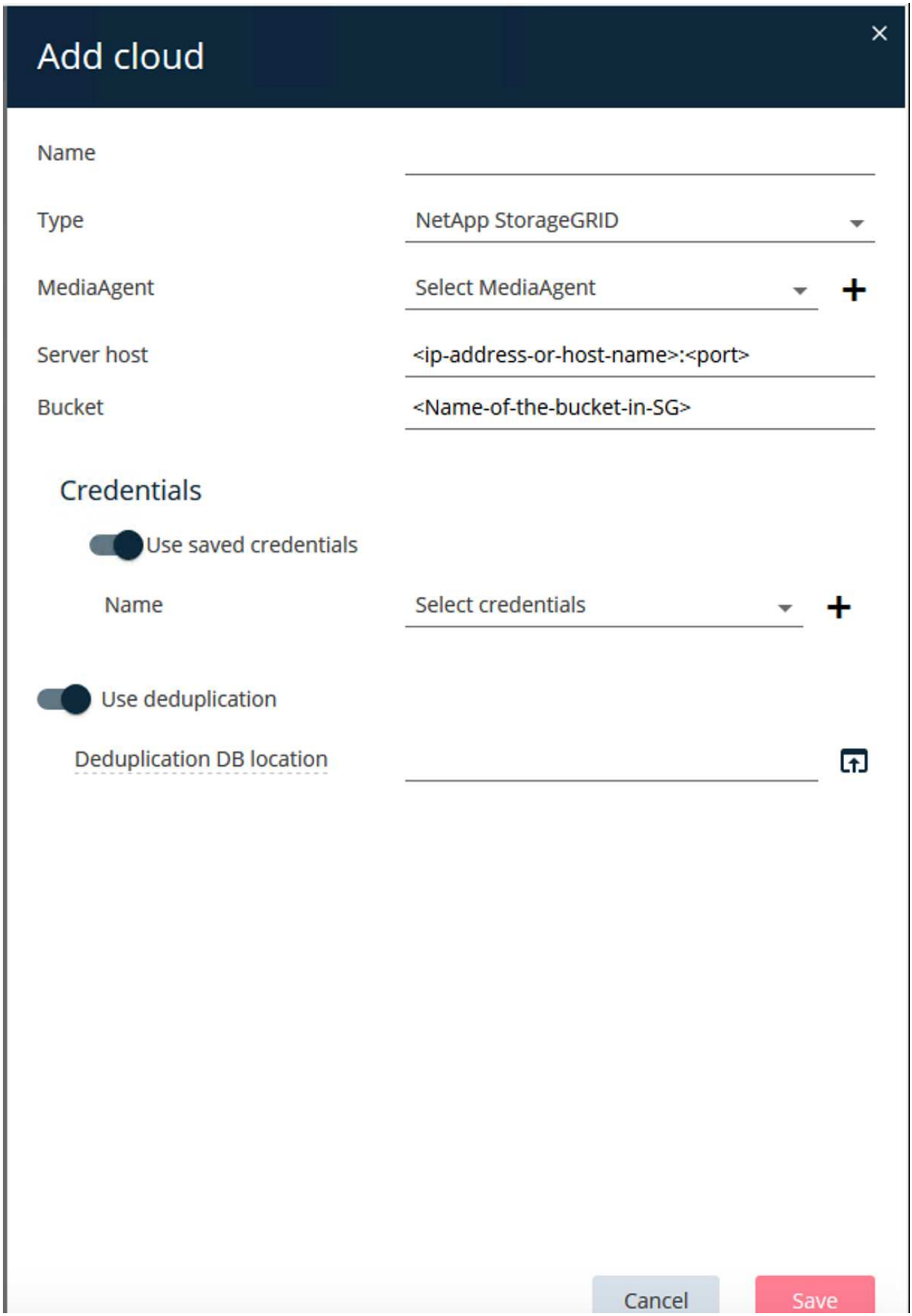
데이터 보호 작업을 실행합니다

Commvault Complete NetApp 백업 및 복구를 사용하여 StorageGRID를 구성하기 위해 다음 단계를 수행하여 Commvault 소프트웨어 내에서 StorageGRID를 클라우드 라이브러리로 추가했습니다.

1단계**: StorageGRID**로 **Commvault** 구성

단계

1. Commvault Command Center에 로그인합니다. 왼쪽 패널에서 스토리지 > 클라우드 > 추가 를 클릭하여 클라우드 추가 대화 상자를 확인하고 이에 대응하십시오.


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. 유형으로 NetApp StorageGRID를 선택합니다.
3. MediaAgent의 경우 클라우드 라이브러리와 연결된 모든 항목을 선택합니다.
4. 서버 호스트의 경우 StorageGRID 끝점의 IP 주소 또는 호스트 이름과 포트 번호를 입력합니다.

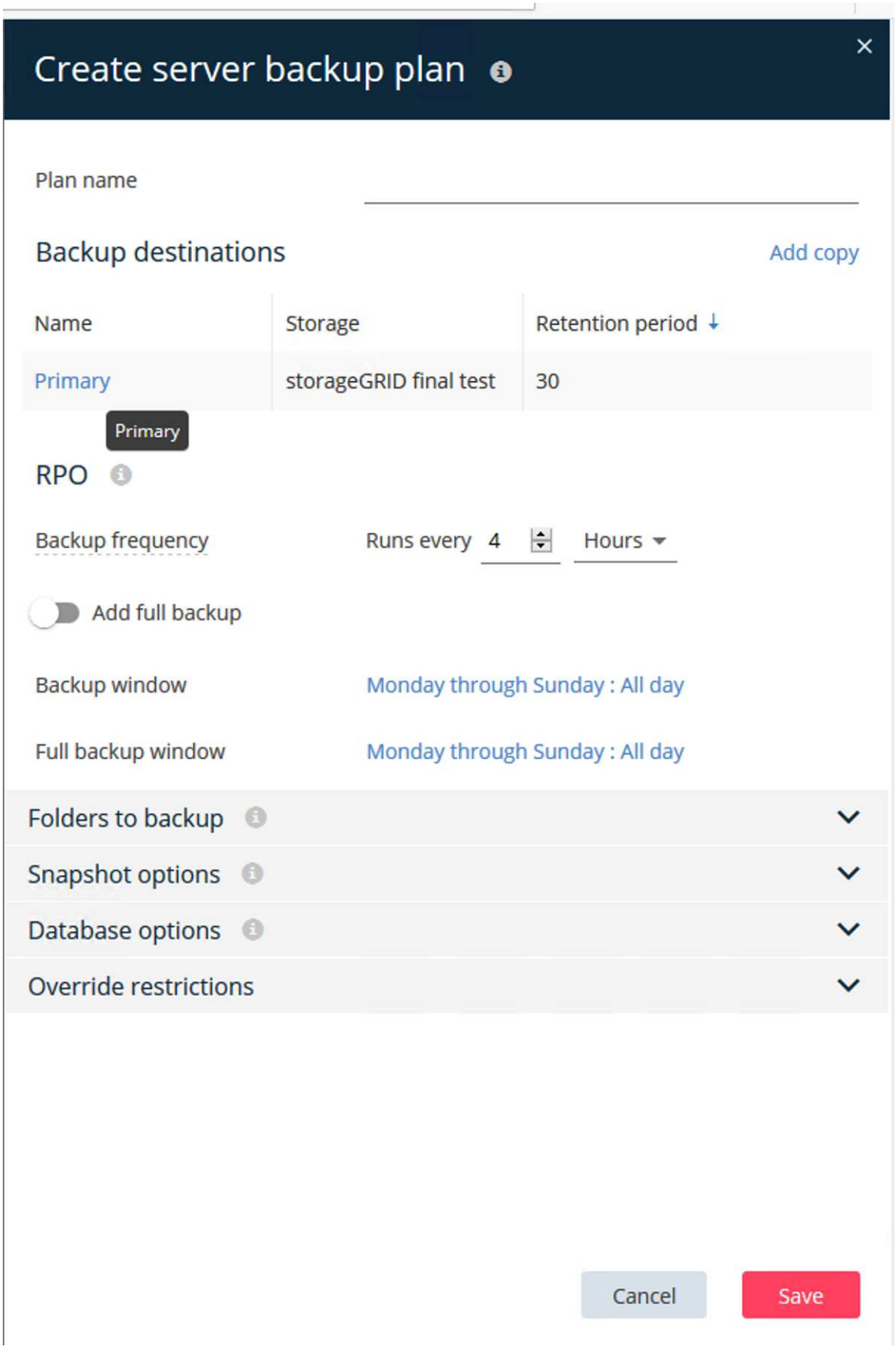
   의 StorageGRID 설명서에 나와 있는 단계를 따릅니다 "로드 밸런서 엔드포인트(포트)를 구성하는 방법". 자체 서명된 인증서가 있는 HTTPS 포트와 StorageGRID 끝점의 IP 주소 또는 도메인 이름이 있는지 확인합니다.

5. 중복 제거를 사용하려면 이 옵션을 설정하고 중복 제거 데이터베이스 위치에 대한 경로를 제공합니다.
6. 저장 을 클릭합니다.

2단계**: StorageGRID**를 기본 타겟으로 사용하여 백업 계획을 생성합니다

단계

1. 왼쪽 패널에서 관리 > 계획을 선택하여 서버 백업 계획 생성 대화 상자를 보고 이에 응답합니다.

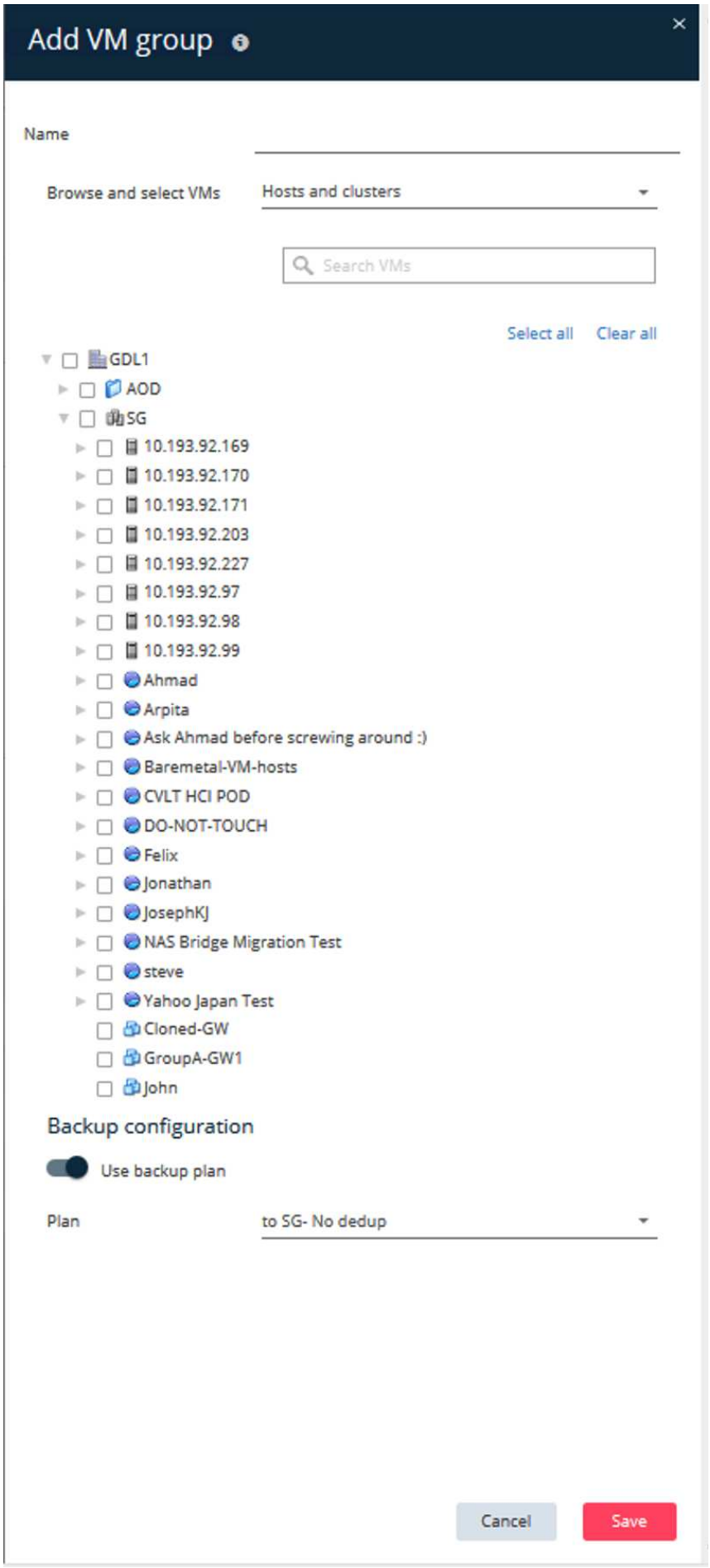

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. 계획 이름을 입력합니다.
3. 이전에 생성한 StorageGRID S3(Simple Storage Service) 스토리지 백업 대상을 선택합니다.
4. 원하는 백업 보존 기간 및 복구 지점 목표(RPO)를 입력합니다.
5. 저장 을 클릭합니다.

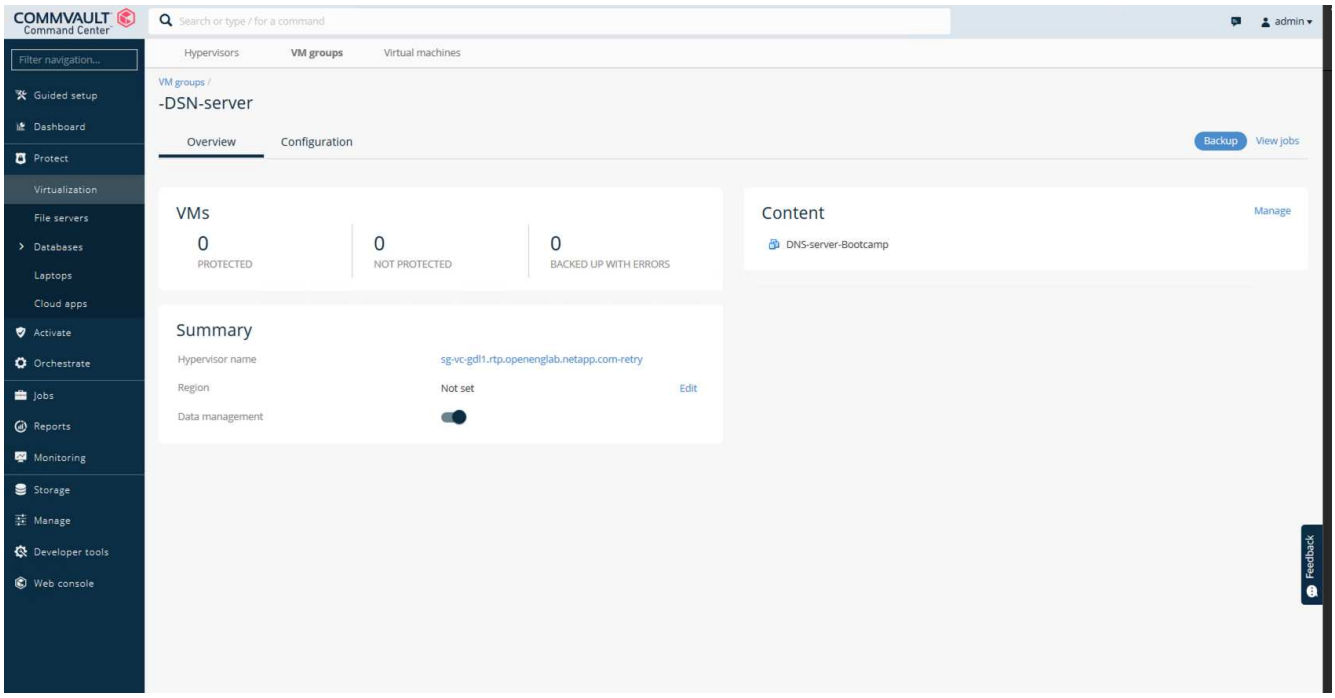
3단계**:** 워크로드를 보호하기 위한 백업 작업을 시작합니다

단계

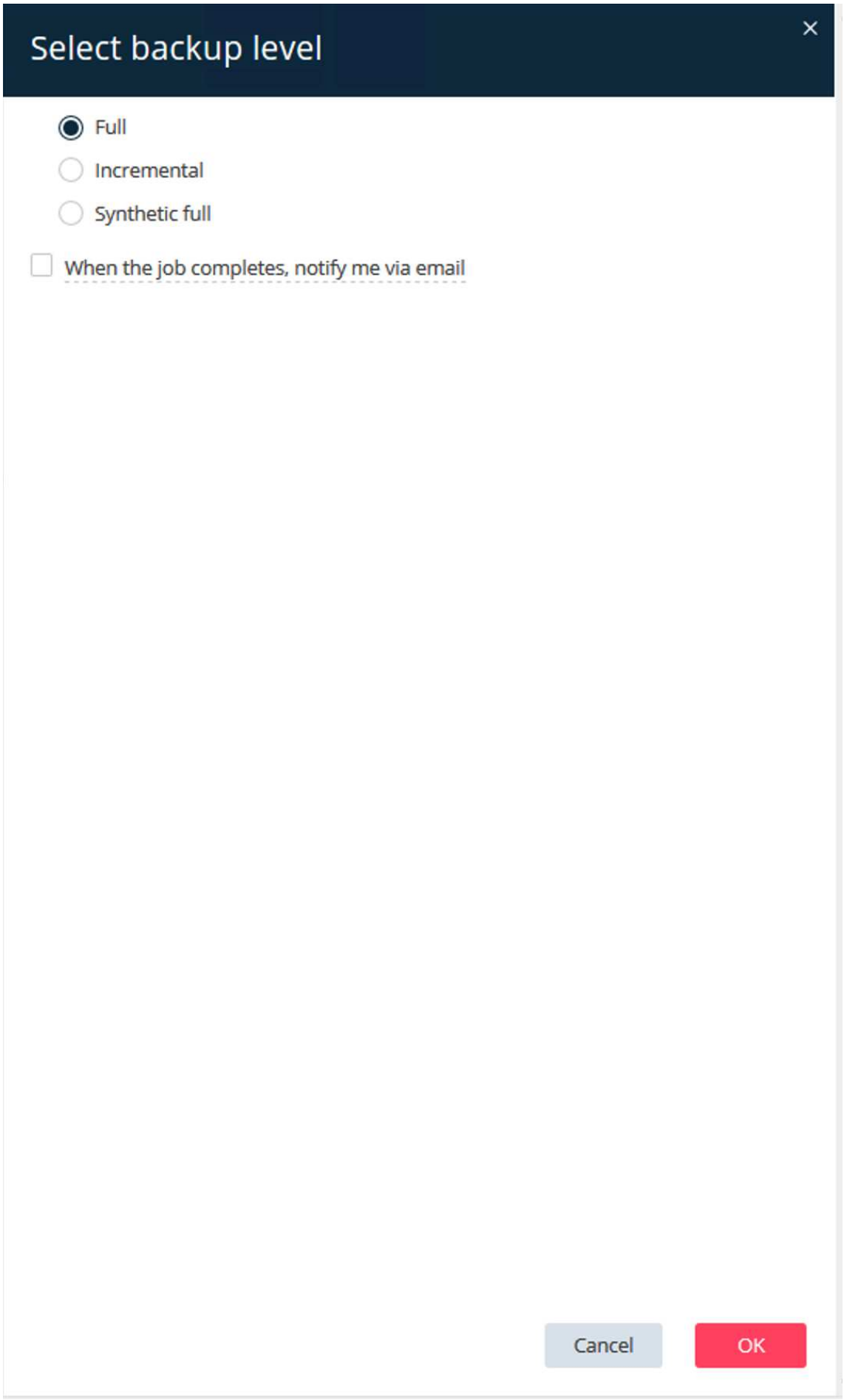
1. Commvault Command Center에서 보호 > 가상화 로 이동합니다.
2. VMware vCenter Server 하이퍼바이저를 추가합니다.
3. 방금 추가한 하이퍼바이저를 클릭합니다.
4. Add VM group(VM 그룹 추가) 을 클릭하여 보호할 vCenter 환경을 볼 수 있도록 Add VM Group(VM 그룹 추가) 대화 상자에 응답합니다.


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

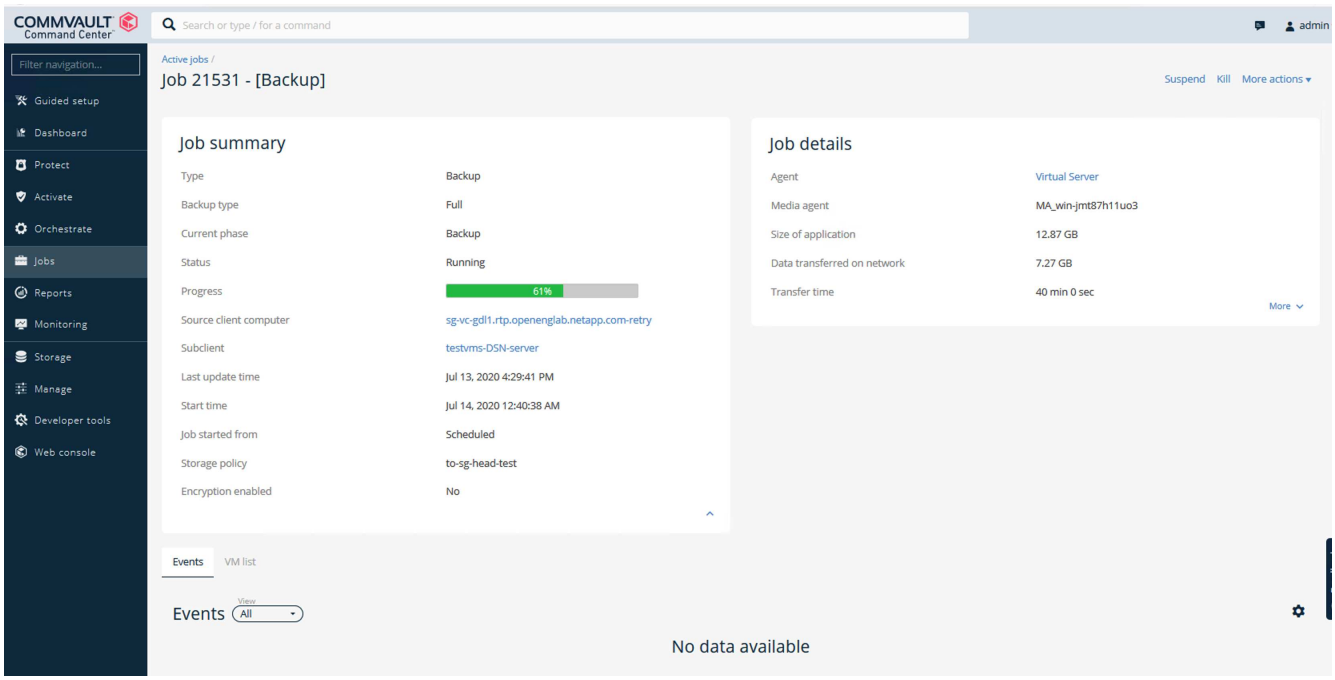
5. 데이터 저장소, VM 또는 VM 컬렉션을 선택하고 이름을 입력합니다.
6. 이전 작업에서 생성한 백업 계획을 선택합니다.
7. Save를 클릭하여 생성한 VM 그룹을 확인합니다.
8. VM group 창의 오른쪽 위 모서리에서 Backup:



9. 백업 레벨로 Full을 선택하고, 백업이 완료되면 e-메일을 요청한 후 OK를 클릭하여 백업 작업을 시작합니다.


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. 작업 요약 페이지로 이동하여 작업 메트릭을 확인합니다.



기준 성능 테스트를 검토합니다

보조 복사 작업에서 4개의 Commvault MediaAgent가 NetApp AFF A300 시스템에 데이터를 백업하고 NetApp StorageGRID에 보조 복사본이 생성되었습니다. 테스트 설정 환경에 대한 자세한 내용은 기술 보고서의 솔루션 설계 및 모범 사례 섹션을 참조하십시오 "Commvault 및 NetApp 스케일아웃 데이터 보호" .

테스트는 VM 100개와 VM 1000개로 수행되었으며, 둘 다 Windows와 CentOS VM의 50/50혼합 구성에서 수행되었습니다. 다음 표에는 기본 성능 테스트의 결과가 나와 있습니다.

작동	백업 속도	복원 속도
보조 복사	2TB/시간	1.27TB/시간
오브젝트와 주고받는 직접 연결(중복제거 켜짐)	2.2TB/시간	1.22TB/시간

시간 종료 성능을 테스트하기 위해 250만 개의 오브젝트를 삭제했습니다. 그림 2 및 3에서 볼 수 있듯이 삭제 실행은 3시간 이내에 완료되었으며 80TB 이상의 공간을 확보했습니다. 삭제 실행이 오전 10시 30분에 시작되었습니다.

그림 **1: 250**만 개**(80TB)** 개체를 **3**시간 이내에 삭제

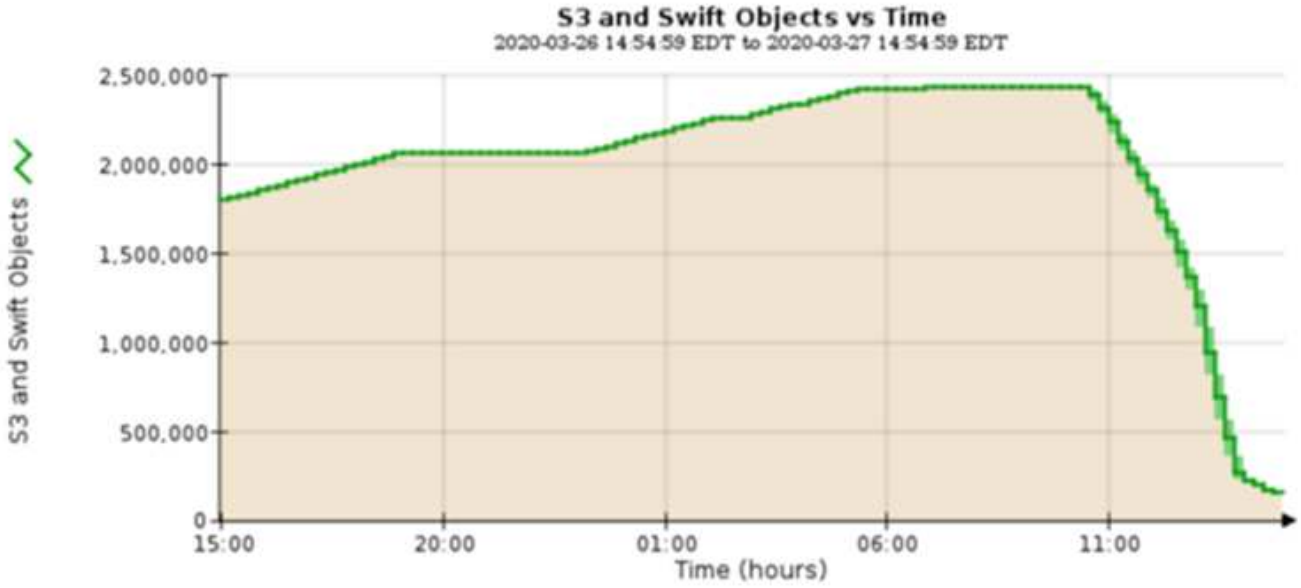
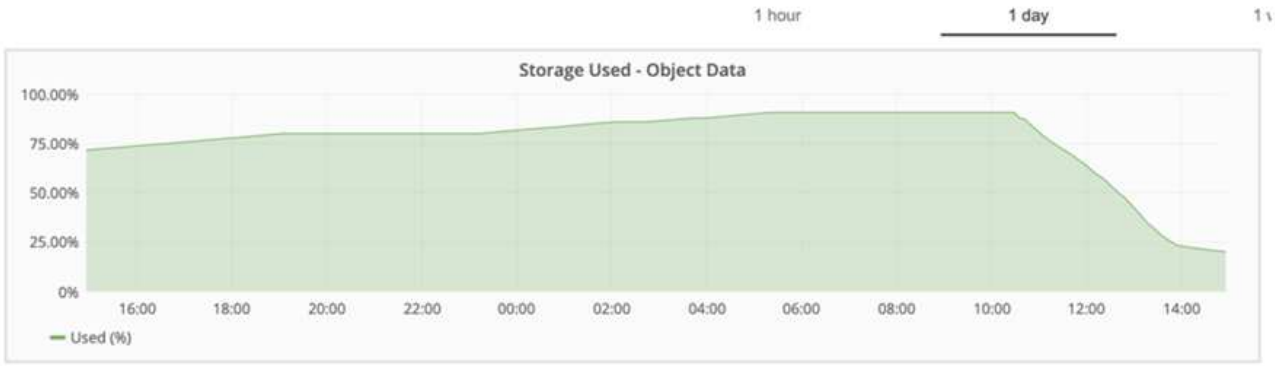


그림 **2: 3**시간 이내에 **80TB**의 스토리지 용량 확보



버킷 일관성 수준 권장 사항

NetApp StorageGRID를 사용하면 최종 사용자가 S3(Simple Storage Service) 버킷의 오브젝트에 대해 수행하는 작업에 대한 일관성 수준을 선택할 수 있습니다.

CommVault MediaAgent는 Commvault 환경의 Data Mover입니다. 대부분의 경우 MediaAgent는 운영 StorageGRID 사이트에 로컬로 기록하도록 구성됩니다. 따라서 로컬 운영 사이트 내에서 높은 수준의 정합성 보장 수준을 사용하는 것이 좋습니다. StorageGRID에서 생성된 Commvault 버킷의 일관성 수준을 설정할 때 다음 지침을 사용합니다.

Commvault 버전이 11.0.0 - 서비스 팩 16 이전 버전인 경우 Commvault를 최신 버전으로 업그레이드하는 것을 고려해 보십시오. 옵션이 아닌 경우 사용 중인 버전에 대한 지침을 따르십시오.

- CommVault 11.0.0 이전 버전 - 서비스 팩 16.* 11.0.0 이전 버전에서 Commvault는 복원 및 정리 프로세스의 일부로 존재하지 않는 개체에 대해 S3 헤드 및 GET 작업을 수행합니다. 버킷 일관성 수준을 강력한 사이트로 설정하여 Commvault로 StorageGRID 백업을 위한 최적의 일관성 수준을 달성합니다.
- CommVault 버전 11.0.0 - 서비스 팩 16 이상.* 버전 11.0.0 - 서비스 팩 16 이상에서는 존재하지 않는 개체에 대해 수행되는 S3 헤드 및 GET 작업의 수가 최소화됩니다. Commvault 및 StorageGRID 환경에서 높은 일관성 수준을 보장하기 위해 기본 버킷 정합성 보장 수준을 새 쓰기 후 읽기 로 설정합니다.

TR-4626: 로드 밸런서

StorageGRID과 함께 타사 로드 밸런서를 사용하십시오

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

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

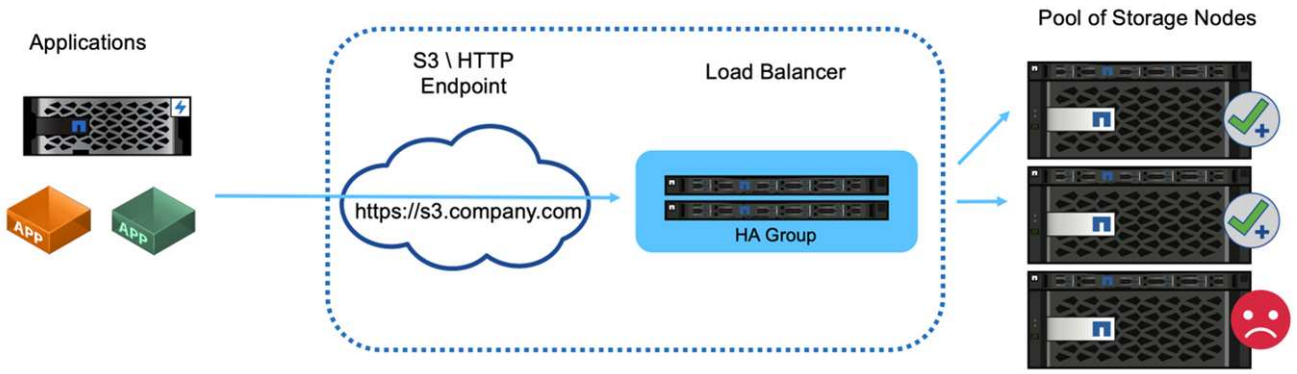
오브젝트 스토리지는 클라우드 스토리지라는 용어와 동의하며, 클라우드 스토리지를 활용하는 애플리케이션은 URL을 통해 해당 스토리지를 처리합니다. 단순한 URL 뒤단에 있는 StorageGRID는 단일 사이트 또는 지리적으로 분산된 사이트에서 용량, 성능 및 내구성을 확장할 수 있습니다. 이러한 단순성을 가능하게 하는 구성 요소는 로드 밸런서입니다.

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

로드 밸런서 기본 사항

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

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



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

로컬 및 글로벌 로드 밸런서

로드 밸런서에는 두 가지 유형이 있습니다.

- * 로컬 트래픽 관리자(LTM) *. 단일 사이트의 노드 풀에 연결을 분산합니다.

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

추가 정보를 찾을 수 있는 위치

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

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

StorageGRID 로드 밸런서 사용

StorageGRID Gateway Node 로드 밸런서의 역할에 대해 알아보세요.

NetApp® StorageGRID® 게이트웨이 노드를 구현하기 위한 일반 지침입니다.

StorageGRID 게이트웨이 노드 로드 밸런서 대 타사 로드 밸런서

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

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

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

StorageGRID 로드 밸런서는 다음과 같은 이점을 제공합니다.

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

StorageGRID 의 통합 노드로서 로컬 트래픽 관리자는 고급 상태 검사를 사용하여 스토리지 노드 상태, 부하 및 리소스 가용성에 따라 요청을 분산할 수 있습니다. 또한 StorageGRID 링크 비용이 사이트 간에 "0"으로 설정된 경우 여러 사이트에 부하를 분산하는 기능도 있습니다. 스토리지 노드를 사용할 수 없지만 게이트웨이 노드를 사이트에서 사용할 수 있는 경우, 부하가 자동으로 그리드의 다른 사이트로 전달됩니다.

게이트웨이 노드의 로드 밸런서 캐싱 기능은 데이터 처리의 일환으로 데이터 세트를 여러 번 다시 읽는 특정 작업 부하(예: AI 학습)에 대해 상당한 성능 향상을 제공하기 위한 것입니다. 캐싱 게이트웨이 노드는 그리드의 나머지 부분과 물리적으로 떨어진 곳에 배치하여 일부 작업 부하에서 더 나은 성능을 제공하고 WAN 네트워크 활용도를 낮출 수도 있습니다. 캐시는 쓰기가 캐시되지 않고 캐시 상태를 수정하지 않는 읽기 모드에서 작동합니다. 각 캐싱 게이트웨이 노드는 다른 캐싱 게이트웨이 노드와 독립적으로 작동합니다.

StorageGRID Gateway 노드 배포에 대한 자세한 내용은 다음을 참조하세요. "StorageGRID 설명서" .

StorageGRID에서 HTTPS용 SSL 인증서를 구현하는 방법에 대해 알아봅니다

StorageGRID에서 SSL 인증서를 구현하는 것의 중요성과 단계를 이해합니다.

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

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

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

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

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

StorageGRID에서 신뢰할 수 있는 타사 로드 밸런서를 구성합니다

StorageGRID에서 신뢰할 수 있는 타사 로드 밸런서를 구성하는 방법을 알아보십시오.

하나 이상의 외부 계층 7 로드 밸런서와 IP 기반의 S3 버킷 또는 그룹 정책을 사용 중인 경우 StorageGRID는 실제 보낸 사람의 IP 주소를 결정해야 합니다. 로드 밸런서에 의해 요청에 삽입된 X-Forwarded-For(XFF) 헤더를 보면 이 작업을 수행할 수 있습니다. XFF 헤더는 스토리지 노드로 직접 전송된 요청에서 쉽게 스푸핑될 수 있으므로 StorageGRID는 각 요청이 신뢰할 수 있는 계층 7 로드 밸런서에 의해 라우팅되고 있는지 확인해야 합니다. StorageGRID에서 요청의 소스를 신뢰할 수 없는 경우 XFF 헤더를 무시합니다. 신뢰할 수 있는 외부 레이어 7 로드 밸런서 목록을 구성할 수 있는 그리드 관리 API가 있습니다. 이 새로운 API는 비공개이며 향후 StorageGRID 릴리스에서 변경될 수 있습니다. 최신 정보는 KB 문서, 를 참조하십시오 "타사 레이어 7 로드 밸런서와 함께 작동하도록 StorageGRID를 구성하는 방법".

로컬 트래픽 매니저 로드 밸런서에 대해 알아보십시오

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

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

스토리지 노드의 리소스 그룹을 생성합니다

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

- S3 HTTPS: 18082
- S3 HTTP: 18084

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

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

상태 점검

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

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

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

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

S3 상태 점검의 예

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

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

파일 또는 콘텐츠 기반의 상태 점검

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

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

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

세션 지속성

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

가상 호스팅 방식의 주소 지정

이제 가상 호스팅 방식이 AWS S3의 기본 방법이며 StorageGRID와 많은 애플리케이션이 경로 스타일을 지원하는

반면, 호스팅된 가상 지원을 구축하는 것이 모범 사례입니다. 가상 호스팅 방식의 요청에는 호스트 이름의 일부분으로 버켓이 있습니다.

가상 호스팅 스타일을 지원하려면 다음을 수행합니다.

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

SSL 종료

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

지원되는 구성은 세 가지입니다.

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

패스스루 구성

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

소스 클라이언트 **IP** 가시성

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

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

단계

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

로드 밸런싱 전략

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

- * 라운드 로빈. * 보편적인 적합하지만 소수의 노드와 대규모 전송으로 인해 단일 노드가 어려움을 겪고 있습니다.
- * 최소 연결. * 소형 및 혼합 오브젝트 워크로드에 적합하며, 모든 노드에 대한 연결의 균등한 분산을 제공합니다.

알고리즘 선택은 선택할 스토리지 노드의 수가 늘어날수록 더 중요해집니다.

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

연결 배포를 확인하는 중입니다

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

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

StorageGRID 구성의 몇 가지 사용 사례에 대해 알아보십시오

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

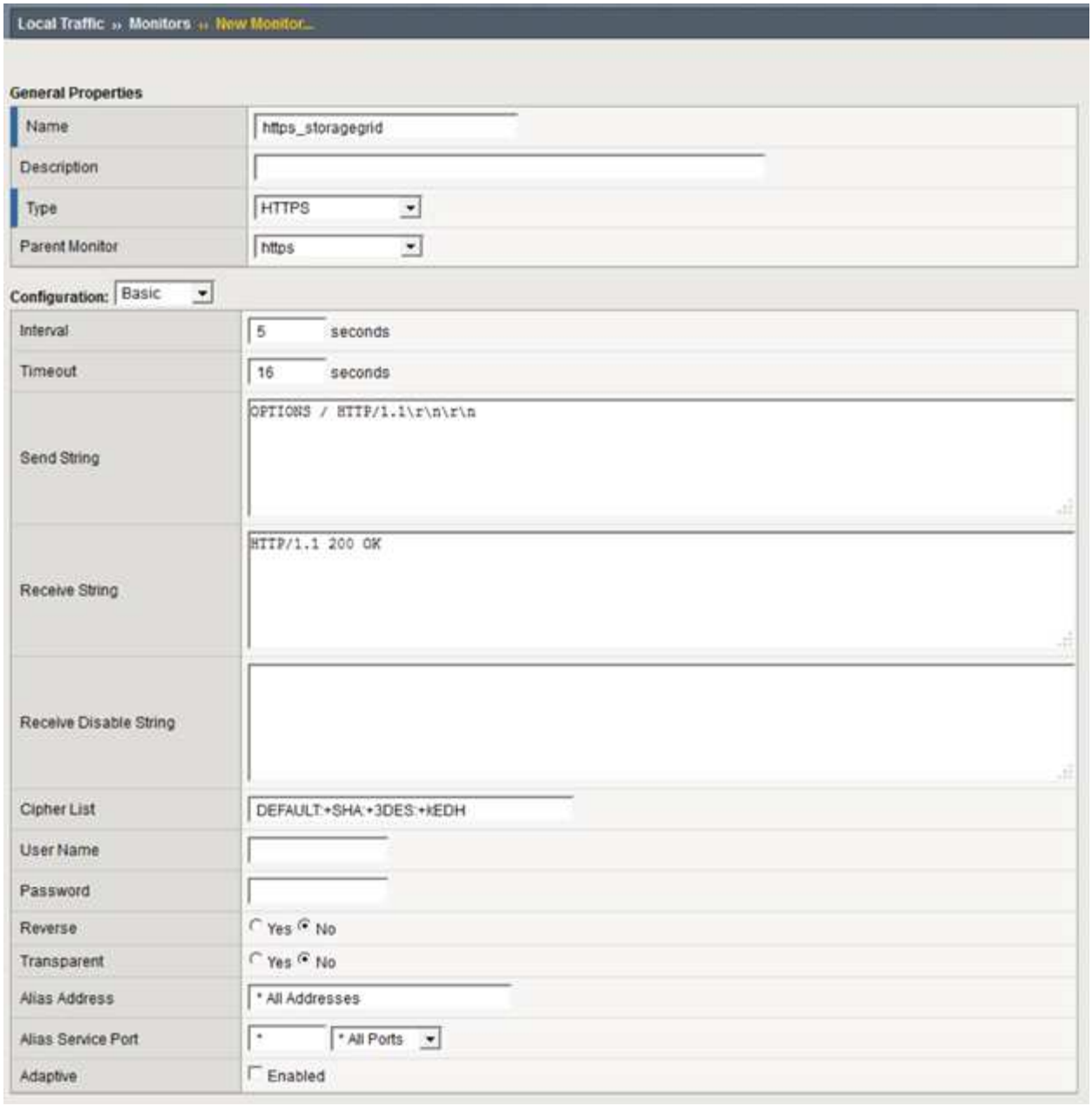
다음 예에서는 NetApp IT를 포함하여 StorageGRID 고객이 구현한 구성을 보여 줍니다.

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

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

단계

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



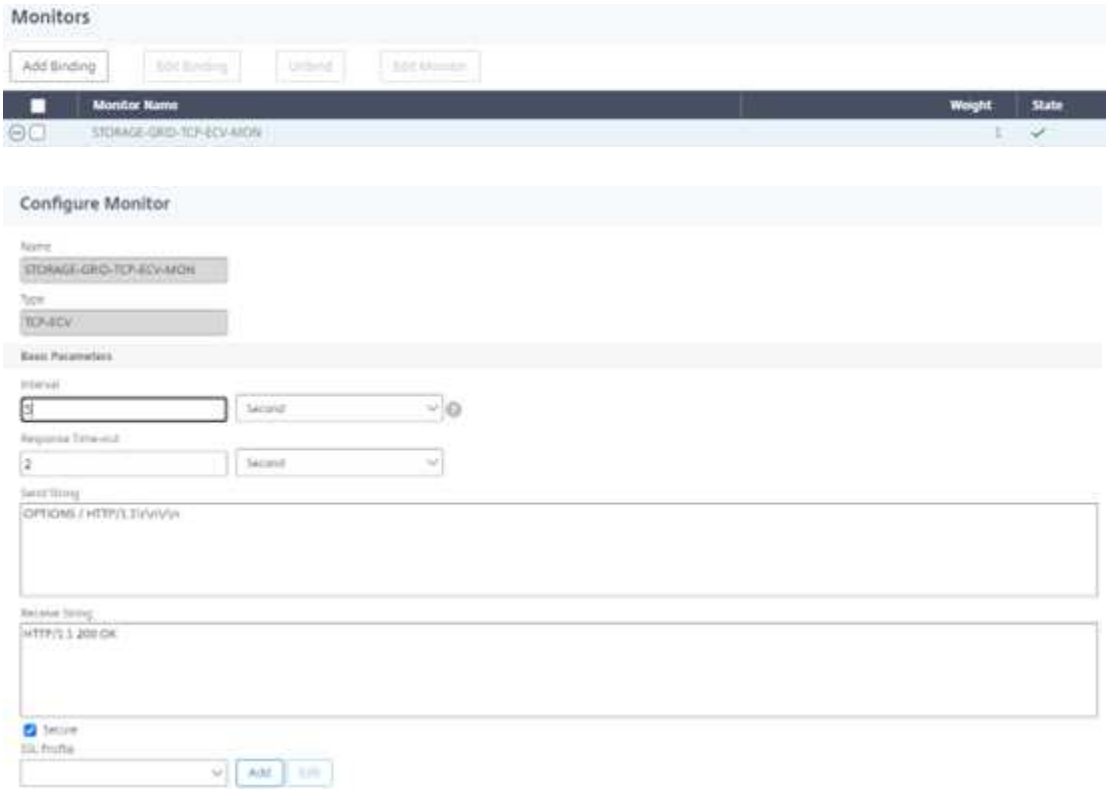
2. Create Pool에서 필요한 각 포트에 대해 하나의 풀을 생성합니다.
   a. 이전 단계에서 만든 상태 모니터를 할당합니다.
   b. 부하 분산 방법을 선택합니다.
   c. 서비스 포트 18082(S3)를 선택합니다.
   d. 노드 추가

Citrix NetScaler를 선택합니다

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

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

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



Loadbalancer.org

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

케이이엠피주식회사

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

HAProxy

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

다음은 HAProxy에서 SSL 종료의 예입니다.

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

다음은 SSL pass-through의 예입니다.

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

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

StorageGRID에서 SSL 연결을 검증합니다

StorageGRID에서 SSL 연결의 유효성을 검사하는 방법에 대해 알아봅니다.

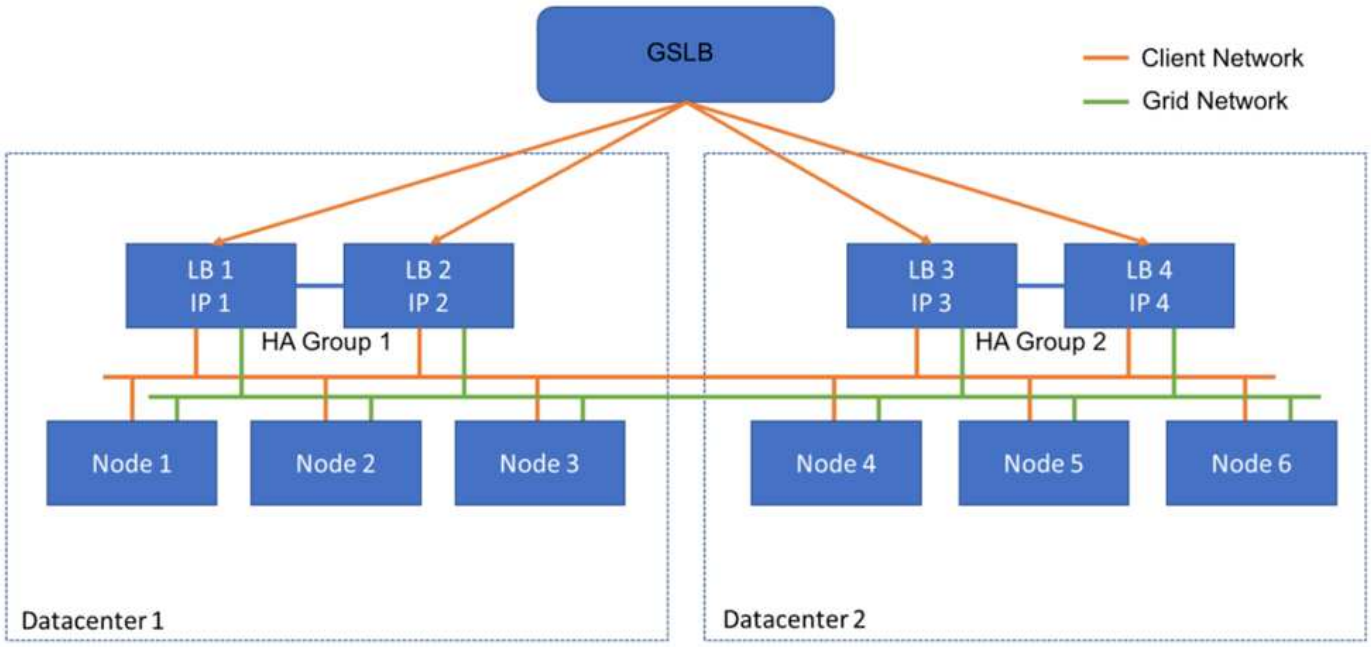
로드 밸런서를 구성한 후에는 OpenSSL 및 AWS CLI와 같은 툴을 사용하여 연결의 유효성을 확인해야 합니다. S3 브라우저와 같은 다른 응용 프로그램은 SSL 구성 오류를 무시할 수 있습니다.

StorageGRID의 글로벌 로드 밸런싱 요구 사항을 이해합니다

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

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

로컬 로드 밸런싱을 제공하는 StorageGRID의 조합 또는 타사 조합 또는 앞에서 논의된 많은 타사가 GSLB와 사이트 로컬 로드 밸런싱을 모두 제공할 수 있습니다.



TR-4645: 보안 기능

오브젝트 저장소에서 **StorageGRID** 데이터와 메타데이터의 보안 유지

StorageGRID 오브젝트 스토리지 솔루션의 핵심 보안 기능에 대해 알아보십시오.

이는 NetApp® StorageGRID®의 다양한 보안 기능에 대한 개요로, 데이터 액세스, 개체 및 메타데이터, 관리 액세스, 플랫폼 보안 등을 다룹니다. StorageGRID 12.0에서 출시된 최신 기능을 포함하도록 업데이트되었습니다.

보안은 NetApp StorageGRID 오브젝트 스토리지 솔루션의 핵심 부분입니다. 오브젝트 스토리지에 적합한 다양한 유형의 다양한 콘텐츠 데이터 또한 본질적으로 민감하고 규정 및 규정 준수를 충족해야 하기 때문에 보안은 특히 중요합니다. StorageGRID의 기능이 계속해서 발전함에 따라 소프트웨어는 조직의 보안 입지를 보호하고 조직이 업계 모범 사례를 준수하도록 지원하는 데 매우 중요한 여러 보안 기능을 사용할 수 있습니다.

이 논문은 StorageGRID 12.0의 다양한 보안 기능에 대한 개요를 5가지 범주로 나누어 설명합니다.

- 데이터 액세스 보안 기능
- 오브젝트 및 메타데이터 보안 기능
- 관리 보안 기능
- 플랫폼 보안 기능
- 클라우드 통합

본 문서는 보안 데이터시트로 작성되었으며, 기본적으로 구성되지 않은 보안 기능을 지원하도록 시스템을 구성하는 방법에 대한 자세한 설명은 제공하지 않습니다. 그만큼 "StorageGRID 강화 가이드 를 참조하십시오" 공식에서 사용 가능합니다 "StorageGRID 설명서" 페이지.

이 보고서에 설명된 기능 외에도 StorageGRID는 를 "NetApp 제품 보안 취약성 대응 및 알림 정책"따릅니다. 보고된

취약성은 제품 보안 사고 대응 프로세스에 따라 확인 및 대응됩니다.

NetApp StorageGRID는 매우 까다로운 엔터프라이즈 오브젝트 스토리지 사용 사례를 위한 고급 보안 기능을 제공합니다.

추가 정보를 찾을 수 있는 위치

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

- NetApp StorageGRID: SEC 17a-4(f), FINRA 4511(c) 및 CFTC 1.31(c)-(d) 준수 평가 https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- NetApp StorageGRID NIST FIPS 140-3 커널 암호화 인증 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- NetApp StorageGRID NIST SP 800-90B 엔트로피 인증 https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- NetApp StorageGRID 캐나다 사이버 보안 센터 공통 기준 인증 https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- StorageGRID 문서 페이지https://docs.netapp.com/us-en/storagegrid/[]
- NetApp 제품 설명서 https://www.netapp.com/support-and-training/documentation/

용어 및 약어

이 섹션에서는 문서에 사용된 용어에 대한 정의를 제공합니다.

용어 또는 약어	정의
S3를 참조하십시오	간단한 스토리지 서비스.
클라이언트	데이터 액세스를 위한 S3 프로토콜 또는 관리를 위한 HTTP 프로토콜을 통해 StorageGRID와 인터페이스할 수 있는 애플리케이션.
테넌트 관리자	StorageGRID 테넌트 계정의 관리자입니다
테넌트 사용자입니다	StorageGRID 테넌트 계정 내의 사용자입니다
TLS	전송 계층 보안
ILM을 참조하십시오	정보 수명 주기 관리
LAN을 선택합니다	LAN(Local Area Network)을 선택합니다
그리드 관리자	StorageGRID 시스템의 관리자입니다
그리드	StorageGRID 시스템
버킷	S3에 저장된 오브젝트의 컨테이너입니다
LDAP를 지원합니다	Lightweight Directory Access Protocol의 약어입니다
초	증권거래위원회; 교환원, 중개인 또는 딜러를 규제합니다
FINRA/핀라	금융 업계 규제 당국. SEC Rule 17a-4(f)의 형식 및 미디어 요구 사항을 준수합니다.
CFTC의 약어입니다	상품 선물 거래 위원회; 상품 선물 거래를 규제합니다

용어 또는 약어	정의
NIST	미국 표준 기술 연구소

데이터 액세스 보안 기능

StorageGRID의 데이터 액세스 보안 기능에 대해 알아보십시오.

피처	기능	영향	규정 준수
구성 가능한 TLS(Transport Layer Security)	TLS는 클라이언트와 StorageGRID 게이트웨이 노드, 스토리지 노드 또는 로드 밸런서 끝점 간의 통신을 위한 핸드셰이크 프로토콜을 설정합니다. StorageGRID는 TLS에 대해 다음 암호화 제품군을 지원합니다. • TLS_AES_256_GCM_SHA384를 참조하십시오 • TLS_AES_128_GCM_SHA256를 참조하십시오 • ECDHE-ECDSA-AES256-GCM-SHA384를 참조하십시오 • ECDHE-RSA-AES256-GCM-SHA384를 참조하십시오 • ECDHE-ECDSA-AES128-GCM-SHA256를 참조하십시오 • ECDHE-RSA-AES128-GCM-SHA256를 참조하십시오 • TLS_AES_256_GCM_SHA384를 참조하십시오 • DHE-RSA-AES128-GCM-SHA256를 참조하십시오 • DHE-RSA-AES256-GCM-SHA384를 참조하십시오 • AES256-GCM-SHA384를 참조하십시오 • AES128-GCM-SHA256를 참조하십시오 • TLS_CHACHA20_POLY1305_SHA256를 참조하십시오 • ECDHE-ECDSA-CHACHA20-POLY1305를 참조하십시오 • ECDHE-RSA-CHACHA20-POLY1305를 참조하십시오 TLS v1.2 및 1.3이 지원됩니다. SSLv3, TLS v1.1 및 이전 버전은 지원되지 않습니다.	클라이언트와 StorageGRID가 서로를 식별 및 인증하고 기밀성 및 데이터 무결성을 유지할 수 있도록 합니다. 최신 TLS 버전 사용을 보장합니다. 이제 구성 /보안 설정에서 암호를 구성할 수 있습니다	—

피처	기능	영향	규정 준수
구성 가능한 서버 인증서(로드 밸런서 끝점)	그리드 관리자는 서버 인증서를 생성하거나 사용하도록 부하 분산 엔드포인트를 구성할 수 있습니다.	표준 CA(신뢰할 수 있는 인증 기관)에서 서명한 디지털 인증서를 사용하여 로드 밸런서 엔드포인트별 그리드와 클라이언트 간 개체 API 작업을 인증할 수 있습니다.	—
구성 가능한 서버 인증서(API 끝점)	그리드 관리자는 조직의 신뢰할 수 있는 CA에서 서명한 서버 인증서를 사용하도록 모든 StorageGRID API 끝점을 중앙에서 구성할 수 있습니다.	신뢰할 수 있는 표준 CA에서 서명한 디지털 인증서를 사용하여 클라이언트와 그리드 간의 개체 API 작업을 인증할 수 있습니다.	—
멀티 테넌시	StorageGRID는 그리드당 여러 테넌트를 지원하며 각 테넌트에는 자체 네임스페이스가 있습니다. 테넌트는 S3 프로토콜을 제공합니다. 기본적으로 버킷/컨테이너 및 오브젝트에 대한 액세스가 계정 내의 사용자로 제한됩니다. 테넌트는 한 명의 사용자(예: 각 사용자가 자신의 계정을 가지고 있는 엔터프라이즈 배포) 또는 여러 사용자(예: 각 계정이 회사 및 서비스 공급자의 고객인 서비스 공급자 구축)를 가질 수 있습니다. 사용자는 로컬 또는 페더레이션될 수 있으며 페더레이션 사용자는 Active Directory 또는 LDAP(Lightweight Directory Access Protocol)로 정의됩니다. StorageGRID는 사용자가 로컬 또는 페더레이션 계정 자격 증명을 사용하여 로그인할 수 있는 테넌트별 대시보드를 제공합니다. 사용자는 데이터 및 버킷에 의해 저장된 개체의 사용 정보를 포함하여 그리드 관리자가 할당한 할당량에 대해 테넌트 사용량에 대한 시각화 보고서에 액세스할 수 있습니다. 관리 권한이 있는 사용자는 사용자, 그룹 및 액세스 키 관리와 같은 테넌트 수준 시스템 관리 작업을 수행할 수 있습니다.	StorageGRID 관리자는 테넌트 액세스를 격리하면서 여러 테넌트의 데이터를 호스팅할 수 있으며, Active Directory 또는 LDAP와 같은 외부 ID 공급자와 사용자를 연합하여 사용자 ID를 설정할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
액세스 자격 증명 거부 안 함	모든 S3 작업은 고유한 테넌트 계정, 사용자 및 액세스 키로 식별되고 기록됩니다.	그리드 관리자가 어떤 API 작업이 어떤 개인에 의해 수행되는지 설정할 수 있습니다.	—

피처	기능	영향	규정 준수
익명 액세스를 사용할 수 없습니다	기본적으로 S3 계정에 대해서는 익명 액세스가 비활성화됩니다. 요청자는 테넌트 계정의 유효한 사용자에 대한 유효한 액세스 자격 증명이 있어야 계정 내의 버킷, 컨테이너 또는 개체에 액세스할 수 있습니다. 명시적 IAM 정책을 통해 S3 버킷 또는 오브젝트에 대한 익명 액세스를 활성화할 수 있습니다.	그리드 관리자가 버킷/컨테이너 및 객체에 대한 익명 액세스를 비활성화하거나 제어할 수 있습니다.	—
규정 준수 WORM	SEC Rule 17a-4(f)의 요구 사항을 충족하도록 설계되었으며 Cohasset에 의해 검증되었습니다. 고객은 버킷 수준의 규정 준수를 지원할 수 있습니다. 보존은 연장할 수 있지만 줄일 수는 없습니다. 정보 수명 주기 관리(ILM) 규칙은 최소 데이터 보호 수준을 적용합니다.	규정 데이터 보존 요구사항이 있는 테넌트에서 저장된 오브젝트 및 오브젝트 메타데이터에 대해 WORM 보호를 지원할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
웜	그리드 관리자는 클라이언트 수정 비활성화 옵션을 활성화하여 그리드 전체에서 WORM을 설정할 수 있습니다. 이렇게 하면 클라이언트가 모든 테넌트 계정에서 객체 또는 객체 메타데이터를 덮어쓰거나 삭제하지 못하게 됩니다. S3 테넌트 관리자는 IAM 정책을 지정하여 오브젝트 및 메타데이터 덮어쓰기에 대한 사용자 지정 S3:PutOverwriteObject 권한이 포함된 테넌트, 버킷 또는 오브젝트 접두사로 WORM을 활성화할 수도 있습니다.	그리드 관리자 및 테넌트 관리자가 저장된 오브젝트 및 오브젝트 메타데이터에 대한 WORM 보호를 제어할 수 있도록 합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)

피처	기능	영향	규정 준수
KMS 호스트 서버 암호화 키 관리	그리드 관리자는 그리드 관리자에서 하나 이상의 외부 키 관리 서버(KMS)를 구성하여 StorageGRID 서비스 및 스토리지 어플라이언스에 암호화 키를 제공할 수 있습니다. 각 KMS 호스트 서버 또는 KMS 호스트 서버 클러스터는 KMIP(Key Management Interoperability Protocol)를 사용하여 관련 StorageGRID 사이트의 어플라이언스 노드에 암호화 키를 제공합니다.	유휴 데이터 암호화를 달성합니다. 어플라이언스 볼륨이 암호화된 후에는 노드가 KMS 호스트 서버와 통신할 수 없는 한 어플라이언스의 모든 데이터에 액세스할 수 없습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
구현할 수 있습니다	StorageGRID는 내장 이중화 및 자동 페일오버 기능을 제공합니다. 디스크 또는 노드에서 전체 사이트에 이르기까지 여러 번의 장애가 발생하더라도 테넌트 계정, 버킷 및 오브젝트에 계속 액세스할 수 있습니다. StorageGRID는 리소스를 인식하며 요청을 가용 노드 및 데이터 위치로 자동으로 리디렉션합니다. StorageGRID 사이트는 island 모드에서도 작동할 수 있습니다. WAN 중단 시 사이트의 나머지 시스템 연결이 끊어지면 로컬 리소스를 사용하여 읽기 및 쓰기를 계속할 수 있으며 WAN이 복구될 때 복제가 자동으로 재개됩니다.	그리드 관리자는 가동 시간, SLA 및 기타 계약상의 의무를 해결하고 비즈니스 연속성 계획을 구현할 수 있습니다.	—
• S3 전용 데이터 액세스 보안 기능 *	AWS 서명 버전 2 및 버전 4	API 요청 서명은 S3 API 작업에 대한 인증을 제공합니다. 아마존은 두 가지 버전의 서명 버전 2와 버전 4를 지원합니다. 서명 프로세스는 요청자의 신원을 확인하고 전송 중인 데이터를 보호하며 잠재적인 재생 공격을 방지합니다.	Signature Version 4에 대한 AWS 권장 사항과 일치하며 Signature Version 2의 이전 버전과의 호환성을 지원합니다.
—	S3 오브젝트 잠금	StorageGRID의 S3 오브젝트 잠금 기능은 Amazon S3의 S3 오브젝트 잠금에 상응하는 오브젝트 보호 솔루션입니다.	테넌트가 S3 오브젝트 잠금이 설정된 상태에서 버킷을 생성하여 특정 오브젝트를 일정 시간 동안 또는 무기한으로 보존해야 하는 규정을 준수할 수 있습니다.

피처	기능	영향	규정 준수
SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)	S3 자격 증명의 안전한 스토리지	S3 액세스 키는 SHA-2(암호 해싱 기능)로 보호되는 형식으로 저장됩니다.	키 길이(10도 31의 임의 생성 번호)와 암호 해시 알고리즘을 조합하여 액세스 키를 안전하게 저장할 수 있습니다.
—	시간이 제한된 S3 액세스 키	사용자에 대한 S3 액세스 키를 생성할 때 고객은 액세스 키에서 만료 날짜 및 시간을 설정할 수 있습니다.	그리드 관리자가 임시 S3 액세스 키를 프로비저닝할 수 있는 옵션을 제공합니다.
—	사용자 계정당 여러 개의 액세스 키	StorageGRID를 사용하면 사용자 계정에 대해 여러 개의 액세스 키를 생성하고 동시에 활성화할 수 있습니다. 각 API 작업은 테넌트 사용자 계정 및 액세스 키로 기록되므로 여러 키가 활성 상태에서도 거부 안 됨(Nonrepudiation)이 유지됩니다.	클라이언트가 액세스 키를 중단 없이 회전할 수 있도록 하며 각 클라이언트가 자체 키를 가질 수 있도록 하여 클라이언트 간에 키를 공유하지 않도록 합니다.
—	S3 IAM 액세스 정책	StorageGRID는 S3 IAM 정책을 지원하므로 그리드 관리자가 테넌트, 버킷 또는 오브젝트 접두사를 기준으로 세분화된 액세스 제어를 지정할 수 있습니다. 또한 StorageGRID는 IAM 정책 조건 및 변수를 지원하여 보다 동적인 액세스 제어 정책을 지원합니다.	그리드 관리자가 전체 테넌트에 대해 사용자 그룹별로 액세스 제어를 지정할 수 있도록 허용하며, 테넌트 사용자가 자신의 버킷 및 객체에 대한 액세스 제어를 지정할 수도 있습니다.
—	S3 보안 토큰 서비스 API AssumeRole	StorageGRID S3 STS API AssumeRole을 지원하여 축소된 권한과 제한된 기간으로 임시 보안 자격 증명(액세스 키 ID, 비밀 액세스 키, 세션 토큰)을 제공합니다. AssumeRole API의 일부로 세션 중에 권한을 추가로 제한하는 인라인 세션 정책이 지원됩니다.	테넌트 관리자가 개체 데이터에 대한 안전한 임시 액세스를 제공할 수 있습니다.

피처	기능	영향	규정 준수
—	간단한 알림 서비스	StorageGRID 객체 액세스에 대한 알림 전송을 지원합니다. 다음과 같은 이벤트 유형이 지원됩니다. • s3:객체 생성됨: • s3:ObjectCreated:Put • s3:ObjectCreated:게시물 • s3:객체 생성:복사 • s3:ObjectCreated:CompleteMultipartUpload • s3:객체 제거됨: • s3:ObjectRemoved:삭제 • s3:ObjectRemoved:DeleteMarkerCreated • s3:객체 복원:게시	테넌트 관리자가 개체에 대한 액세스를 모니터링할 수 있습니다.
—	StorageGRID에서 관리하는 키(SSE)를 사용한 서버측 암호화	StorageGRID는 SSE를 지원하므로 StorageGRID에서 관리하는 암호화 키로 유휴 데이터의 멀티 테넌트 보호가 가능합니다.	테넌트가 오브젝트를 암호화할 수 있도록 합니다. 이러한 개체를 쓰고 검색하려면 암호화 키가 필요합니다.
SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)	고객이 제공한 암호화 키(SSE-C)를 사용한 서버측 암호화	StorageGRID는 SSE-C를 지원하여 클라이언트가 관리하는 암호화 키를 사용하여 저장된 데이터를 멀티 테넌트(Multi-tenant) 보호할 수 있습니다. StorageGRID가 모든 개체 암호화 및 암호 해독 작업을 관리하지만 SSE-C를 사용하여 클라이언트는 암호화 키 자체를 관리해야 합니다.	클라이언트가 제어하는 키를 사용하여 개체를 암호화할 수 있습니다. 이러한 개체를 쓰고 검색하려면 암호화 키가 필요합니다.

오브젝트 및 메타데이터 보안

StorageGRID의 개체 및 메타데이터 보안 기능을 살펴봅니다.

피처	기능	영향	규정 준수
AES(Advanced Encryption Standard) 서버측 개체 암호화	StorageGRID는 AES 128 및 AES 256 기반의 서버측 오브젝트 암호화를 제공합니다. 그리드 관리자는 암호화를 전역 기본 설정으로 활성화할 수 있습니다. 또한 StorageGRID는 S3 x-amz-server-side 암호화 헤더를 지원하여 오브젝트별로 암호화를 활성화하거나 비활성화할 수 있습니다. 이 기능을 활성화하면 저장 또는 그리드 노드 간에 전송 중인 객체가 암호화됩니다.	기본 스토리지 하드웨어에 관계없이 안전하게 개체를 저장하고 전송할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
내장된 키 관리	암호화가 활성화되면 각 오브젝트가 무작위로 생성된 고유 대칭 키로 암호화되며 외부 액세스 없이 StorageGRID 내에 저장됩니다.	외부 키 관리 없이도 개체 암호화 가능	
FIPS(Federal Information Processing Standard) 140-2 준수 암호화 디스크	SG5812, SG5860, SG6160 및 SGF6024 StorageGRID 어플라이언스는 FIPS 140-2 준수 암호화 디스크의 옵션을 제공합니다. 선택적으로 외부 KMIP 서버를 통해 디스크의 암호화 키를 관리할 수 있습니다.	시스템 데이터, 메타데이터 및 오브젝트의 안전한 스토리지 지원 또한 StorageGRID 소프트웨어 기반 오브젝트 암호화를 제공하여 오브젝트의 저장 및 전송을 보호합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
노드에 대한 연방 정보 처리 표준(FIPS) 140-3 호환 암호화	SG5812, SG5860, SG6160, SGF6112, SG1100 및 SG110 StorageGRID 어플라이언스는 FIPS 140-3 호환 노드 암호화 옵션을 제공합니다. 노드의 암호화 키는 외부 KMIP 서버에서 관리합니다.	시스템 데이터, 메타데이터 및 오브젝트의 안전한 스토리지 지원 또한 StorageGRID 소프트웨어 기반 오브젝트 암호화를 제공하여 오브젝트의 저장 및 전송을 보호합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
백그라운드 무결성 검사 및 자가 복구	StorageGRID는 오브젝트 및 하위 오브젝트 수준에서 해시, 체크섬, 순환 중복 검사(CRC)의 인터잠금 메커니즘을 사용하여 오브젝트가 스토리지에 있을 때와 전송 중일 때 데이터 비일관성, 변조 또는 수정으로부터 보호합니다. StorageGRID는 손상되거나 무단 변경된 오브젝트를 자동으로 감지하여 교체하는 한편, 변경된 데이터를 격리하고 관리자에게 경고합니다.	그리드 관리자는 데이터 내구성과 관련된 SLA, 규정 및 기타 의무를 충족할 수 있습니다. 고객이 데이터를 암호화, 변조 또는 수정하려는 랜섬웨어 또는 바이러스를 감지하는 데 도움이 됩니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)

피처	기능	영향	규정 준수
정책 기반 오브젝트 배치 및 보존	StorageGRID를 통해 그리드 관리자는 객체 보존, 배치, 보호, 전환 및 만료가 지정된 ILM 규칙을 구성할 수 있습니다. 그리드 관리자는 StorageGRID 메타데이터로 오브젝트를 필터링하고 그리드 전체, 테넌트, 버킷, 키 접두사, 및 사용자 정의 메타데이터 키-값 쌍 StorageGRID는 클라이언트에서 명시적으로 삭제하지 않는 한, 라이프사이클 전반에서 ILM 규칙에 따라 오브젝트를 저장할 수 있도록 도와줍니다.	데이터 배치, 보호 및 보존을 적용할 수 있도록 지원 고객이 내구성, 가용성, 성능에 대한 SLA를 달성할 수 있도록 지원합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
백그라운드 메타데이터 검사	StorageGRID은 주기적으로 백그라운드에서 오브젝트 메타데이터를 검사하여 ILM에서 지정한 대로 오브젝트 데이터 배치 또는 보호 변경 사항을 적용합니다.	손상된 개체를 찾는 데 도움이 됩니다.	
일관성 조정 가능	테넌트는 버킷 수준의 일관성 수준을 선택하여 다중 사이트 연결과 같은 리소스를 사용할 수 있도록 할 수 있습니다.	필요한 수의 사이트 또는 리소스를 사용할 수 있는 경우에만 그리드에 쓰기를 커밋하는 옵션을 제공합니다.	

관리 보안 기능

StorageGRID의 관리 보안 기능에 대해 알아봅니다.

피처	기능	영향	규정 준수
서버 인증서(그리드 관리 인터페이스)	그리드 관리자는 조직의 신뢰할 수 있는 CA에서 서명한 서버 인증서를 사용하도록 그리드 관리 인터페이스를 구성할 수 있습니다.	신뢰할 수 있는 표준 CA에서 서명한 디지털 인증서를 사용하여 관리 클라이언트와 그리드 간의 관리 UI 및 API 액세스를 인증할 수 있습니다.	—
관리 사용자 인증	관리 사용자는 사용자 이름과 암호를 사용하여 인증됩니다. 관리 사용자 및 그룹은 로컬 또는 페더레이션될 수 있으며 고객의 Active Directory 또는 LDAP에서 가져올 수 있습니다. 로컬 계정 암호는 bcrypt로 보호되는 형식으로 저장되고 명령줄 암호는 SHA-2로 보호되는 형식으로 저장됩니다.	관리 UI 및 API에 대한 관리 액세스를 인증합니다.	—

피처	기능	영향	규정 준수
SAML 지원	StorageGRID는 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하는 SSO(Single Sign-On)를 지원합니다. SSO가 활성화된 경우 모든 사용자는 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스하기 전에 외부 ID 공급자에 의해 인증되어야 합니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.	SSO 및 다단계 인증(MFA)과 같은 그리드 및 테넌트 관리자를 위한 추가 보안 수준 지원	NIST SP800-63 를 참조하십시오
세분화된 권한 제어	그리드 관리자는 역할에 권한을 할당하고 관리 사용자 그룹에 역할을 할당할 수 있습니다. 그러면 관리 UI와 API를 모두 사용하여 관리 클라이언트가 수행할 수 있는 작업이 적용됩니다.	그리드 관리자가 관리자 및 그룹에 대한 액세스 제어를 관리할 수 있습니다.	—

피처	기능	영향	규정 준수
분산 감사 로깅	StorageGRID는 최대 16개 사이트에서 수백 개의 노드로 확장할 수 있는 분산형 감사 로깅 인프라를 내장하고 있습니다. StorageGRID 소프트웨어 노드는 중복 감사 릴레이 시스템을 통해 전송되어 하나 이상의 감사 로그 저장소에 캡처되는 감사 메시지를 생성합니다. 감사 메시지는 클라이언트 실행형 S3 API 작업, ILM을 통한 오브젝트 라이프사이클 이벤트, 백그라운드 오브젝트 상태 점검, 관리 UI 또는 API를 통한 구성 변경 등과 같이 오브젝트 레벨에서 세분화된 이벤트를 캡처합니다. 감사 로그는 syslog를 통해 내보내질 수 있으며, 이를 통해 Splunk 및 ELK와 같은 도구를 사용하여 감사 메시지를 마이닝할 수 있습니다. 감사 메시지에는 네 가지 유형이 있습니다. • 시스템 감사 메시지 • 오브젝트 스토리지 감사 메시지 • HTTP 프로토콜 감사 메시지 • 관리 감사 메시지 감사 로그는 장기 보관 및 애플리케이션 액세스를 위해 S3 버킷에 저장할 수 있습니다.	그리드 관리자는 검증되고 확장 가능한 감사 서비스를 제공하며 다양한 목표에 대한 감사 데이터를 마이닝할 수 있습니다. 이러한 목표에는 문제 해결, SLA 성능 감사, 클라이언트 데이터 액세스 API 작업, 관리 구성 변경 등이 포함됩니다.	—
시스템 감사	시스템 감사 메시지는 그리드 노드 상태, 손상된 개체 감지, ILM 규칙에 따라 지정된 모든 위치에 커밋된 개체, 시스템 차원의 유지 관리 작업(그리드 작업)의 진행률과 같은 시스템 관련 이벤트를 캡처합니다.	고객이 시스템 문제를 해결하도록 지원하고 SLA에 따라 개체가 저장된다는 증거를 제공합니다. SLA는 StorageGRID ILM 규칙을 통해 구현되며 무결성이 보호됩니다.	—

피처	기능	영향	규정 준수
오브젝트 스토리지 감사	오브젝트 스토리지 감사 메시지는 오브젝트 API 트랜잭션 및 라이프사이클 관련 이벤트를 캡처합니다. 이러한 이벤트에는 오브젝트 스토리지 및 검색, 그리드 노드에서 그리드 노드로 전송 및 검증이 포함됩니다.	고객이 시스템을 통해 데이터의 진행 상황과 StorageGRID ILM으로 지정된 SLA 제공 여부를 감사하는 데 도움이 됩니다.	—
HTTP 프로토콜 감사	HTTP 프로토콜 감사 메시지는 클라이언트 응용 프로그램 및 StorageGRID 노드와 관련된 HTTP 프로토콜 상호 작용을 캡처합니다. 또한 고객은 특정 HTTP 요청 헤더(예: X-Forwarded-For 및 사용자 메타데이터[x-amz-meta- *])를 감사에 캡처할 수 있습니다.	고객이 클라이언트와 StorageGRID 간의 데이터 액세스 API 작업을 감사하고 개별 사용자 계정 및 액세스 키에 대한 작업을 추적할 수 있도록 도와줍니다. 또한 고객은 사용자 메타데이터를 감사에 로그인하고 Splunk 또는 elk와 같은 로그 마이닝 툴을 사용하여 오브젝트 메타데이터를 검색할 수 있습니다.	—
관리 감사	관리 감사 메시지는 관리 UI(그리드 관리 인터페이스) 또는 API에 관리자 사용자 요청을 기록합니다. API에 대한 GET 또는 HEAD 요청이 아닌 모든 요청은 API에 대한 사용자 이름, IP 및 요청 유형을 사용하여 응답을 기록합니다.	그리드 관리자가 소스 IP와 대상 IP를 어느 시점에 어느 사용자가 변경했는지에 대한 시스템 구성 변경 기록을 설정할 수 있도록 도와줍니다.	—
관리 UI 및 API 액세스를 위한 TLS 1.3 지원	TLS는 관리 클라이언트와 StorageGRID 관리 노드 간의 통신을 위한 핸드셰이크 프로토콜을 설정합니다.	관리 클라이언트와 StorageGRID가 서로 식별 및 인증하고 기밀성 및 데이터 무결성을 유지할 수 있도록 합니다.	—
StorageGRID 모니터링용 SNMPv3	SNMPv3는 개인 정보 보호를 위해 강력한 인증 및 데이터 암호화를 제공하여 보안을 제공합니다. v3에서는 암호화 프로토콜에 CBC-DES를 사용하여 프로토콜 데이터 유닛이 암호화됩니다. 프로토콜 데이터 단위를 보낸 사람의 사용자 인증은 HMAC-SHA 또는 HMAC-MD5 인증 프로토콜을 통해 제공됩니다. SNMPv2 및 v1은 계속 지원됩니다.	그리드 관리자가 관리자 노드에서 SNMP 에이전트를 활성화하여 StorageGRID 시스템을 모니터링할 수 있도록 합니다.	—

피처	기능	영향	규정 준수
Prometheus 메트릭스 내보내기용 클라이언트 인증서	그리드 관리자는 StorageGRID Prometheus 데이터베이스에 대한 안전하고 인증된 액세스를 제공하는 데 사용할 수 있는 클라이언트 인증서를 업로드하거나 생성할 수 있습니다.	그리드 관리자는 클라이언트 인증서를 사용하여 Grafana와 같은 애플리케이션을 사용하여 외부에서 StorageGRID를 모니터링할 수 있습니다.	—

플랫폼 보안 기능

StorageGRID의 플랫폼 보안 기능에 대해 알아봅니다.

피처	기능	영향	규정 준수
내부 PKI(공개 키 인프라), 노드 인증서 및 TLS	StorageGRID는 내부 PKI 및 노드 인증서를 사용하여 노드 간 통신을 인증하고 암호화합니다. 노드 간 통신은 TLS에 의해 보호됩니다.	LAN 또는 WAN을 통한 시스템 트래픽 보안, 특히 다중 사이트 구축 시 유용합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
노드 방화벽	StorageGRID는 IP 테이블 및 방화벽 규칙을 자동으로 구성하여 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 제어하고 사용되지 않는 포트를 닫습니다.	StorageGRID 시스템, 데이터 및 메타데이터를 원치 않는 네트워크 트래픽으로부터 보호합니다.	—
OS 강화	StorageGRID 물리적 어플라이언스 및 가상 노드의 기본 운영 체제가 강화되며 관련 없는 소프트웨어 패키지가 제거됩니다.	잠재적인 공격 대상을 최소화합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
주기적인 플랫폼 및 소프트웨어 업데이트	StorageGRID는 운영 체제, 응용 프로그램 바이너리 및 소프트웨어 업데이트를 포함하는 정기적인 소프트웨어 릴리즈를 제공합니다.	StorageGRID 시스템을 최신 소프트웨어 및 응용 프로그램 바이너리로 업데이트하는 데 도움이 됩니다.	—
SSH(Secure Shell)를 통한 루트 로그인 비활성화	모든 StorageGRID 노드에서 SSH를 통한 루트 로그인이 비활성화됩니다. SSH 액세스에서는 인증서 인증을 사용합니다.	고객이 루트 로그인의 잠재적인 원격 암호 크래킹으로부터 보호할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)

피처	기능	영향	규정 준수
자동 시간 동기화	StorageGRID는 여러 외부 시간 네트워크 시간 프로토콜(NTP) 서버에 대해 각 노드의 시스템 클록을 자동으로 동기화합니다. Stratum 3 이상의 NTP 서버가 4개 이상 필요합니다.	모든 노드에서 동일한 시간 참조를 보장합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
클라이언트, 관리자 및 내부 그리드 트래픽을 위한 별도의 네트워크	StorageGRID 소프트웨어 노드 및 하드웨어 어플라이언스는 여러 가상 및 물리적 네트워크 인터페이스를 지원하므로 고객이 여러 네트워크에서 클라이언트, 관리 및 내부 그리드 트래픽을 분리할 수 있습니다.	그리드 관리자는 내부 및 외부 네트워크 트래픽을 분리하고 서로 다른 SLA를 가진 네트워크를 통해 트래픽을 전달할 수 있습니다.	—
다중 VLAN(Virtual LAN) 인터페이스	StorageGRID는 StorageGRID 클라이언트 및 그리드 네트워크에서 VLAN 인터페이스 구성을 지원합니다.	그리드 관리자는 보안, 유연성 및 성능을 위해 애플리케이션 트래픽을 분할하고 격리할 수 있습니다.	
신뢰할 수 없는 클라이언트 네트워크	신뢰할 수 없는 클라이언트 네트워크 인터페이스는 로드 밸런서 끝점으로 명시적으로 구성된 포트에 대해서만 인바운드 연결을 허용합니다.	신뢰할 수 없는 네트워크에 노출된 인터페이스의 보안을 보장합니다.	—
구성 가능한 방화벽	관리, 그리드 및 클라이언트 네트워크에 대한 열린 포트 및 닫힌 포트를 관리합니다.	그리드 관리자가 포트에 대한 액세스를 제어하고 포트에 대한 승인된 장치 액세스를 관리할 수 있습니다.	
향상된 SSH 동작	설치 전에 기본적으로 SSH를 비활성화합니다. 기본 상태에서는 SSH 액세스는 링크 로컬 관리 포트 주소에서만 활성화됩니다. 관리자 및 루트 사용자 비밀번호는 어플라이언스 컴퓨팅 컨트롤러 일련 번호로 설정됩니다. 로그인은 직렬 콘솔과 그래픽 콘솔(BMC KVM)에서만 허용됩니다. 모든 네트워크 포트에서 SSH가 비활성화되었습니다.	네트워크 접근 보호를 강화합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
노드 암호화	새로운 KMS 호스트 서버 암호화 기능의 일부로 새로운 노드 암호화 설정이 StorageGRID 어플라이언스 설치 프로그램에 추가됩니다.	이 설정은 어플라이언스 설치의 하드웨어 구성 단계에서 활성화해야 합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)

클라우드 통합

StorageGRID를 클라우드 서비스와 통합하는 방식 이해

피처	기능	영향
알림 기반 바이러스 검사	StorageGRID 플랫폼 서비스는 이벤트 알림을 지원합니다. 이벤트 알림을 외부 클라우드 컴퓨팅 서비스와 함께 사용하여 데이터에 대한 바이러스 검사 워크플로우를 트리거할 수 있습니다.	테넌트 관리자가 외부 클라우드 컴퓨팅 서비스를 사용하여 데이터의 바이러스 검사를 트리거할 수 있습니다.

TR-4921: 랜섬웨어 방어

랜섬웨어로부터 StorageGRID S3 오브젝트 보호

StorageGRID 보안 모범 사례로 랜섬웨어 공격과 데이터를 보호하는 방법에 대해 알아보십시오.

랜섬웨어 공격이 증가하고 있습니다. 이 문서에서는 StorageGRID에서 개체 데이터를 보호하는 방법에 대한 몇 가지 권장 사항을 제공합니다.

오늘날의 랜섬웨어는 데이터 센터에 있어서 항상 존재하는 위험입니다. 랜섬웨어는 데이터를 암호화하여 사용하는 사용자 및 애플리케이션이 사용할 수 없도록 설계되었습니다. 보안은 강화된 네트워킹과 견고한 사용자 보안 관행의 일반적인 방어부터 시작하며, 데이터 액세스 보안 관행에 따라야 합니다.

랜섬웨어는 오늘날 가장 큰 보안 위협 중 하나입니다. NetApp StorageGRID 팀은 이러한 위협에 대비하기 위해 고객과 협력하고 있습니다. 개체 잠금 및 버전 관리를 사용하면 원치 않는 변경을 방지하고 악의적인 공격으로부터 복구할 수 있습니다. 데이터 보안은 오브젝트 스토리지가 데이터 센터의 한 부분에 불과합니다.

StorageGRID 모범 사례

StorageGRID의 경우 보안 모범 사례에는 관리 및 개체 액세스를 위해 서명된 인증서와 함께 HTTPS를 사용하는 것이 포함되어야 합니다. 애플리케이션 및 개인에 대한 전용 사용자 계정을 생성하고 애플리케이션 액세스 또는 사용자 데이터 액세스에 테넌트 루트 계정을 사용하지 마십시오. 즉, 최소 권한 원칙을 따릅니다. IAM(Identity and Access Management) 정책이 정의된 보안 그룹을 사용하여 사용자 권한을 관리하고 응용 프로그램 및 사용자에 고유한 계정에 액세스합니다. 적절한 조치를 취하는 동안에도 데이터를 보호해야 합니다. S3(Simple Storage Service)의 경우 오브젝트를 암호화하도록 수정하면 원래 오브젝트를 덮어쓰면 수행됩니다.

방어방법

S3 API의 기본 랜섬웨어 보호 메커니즘은 오브젝트 잠금을 구현하는 것입니다. 모든 애플리케이션이 오브젝트 잠금과 호환되지 않으므로 이 보고서에서 설명하는 오브젝트를 보호하기 위한 다른 두 가지 옵션, 즉 버전 관리가 활성화된 다른 버킷으로의 복제 및 IAM 정책을 통한 버전 관리가 있습니다.

추가 정보를 찾을 수 있는 위치

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

- NetApp StorageGRID 문서 센터https://docs.netapp.com/us-en/storagegrid/[]
- NetApp StorageGRID 지원 https://docs.netapp.com/us-en/storagegrid-enable/

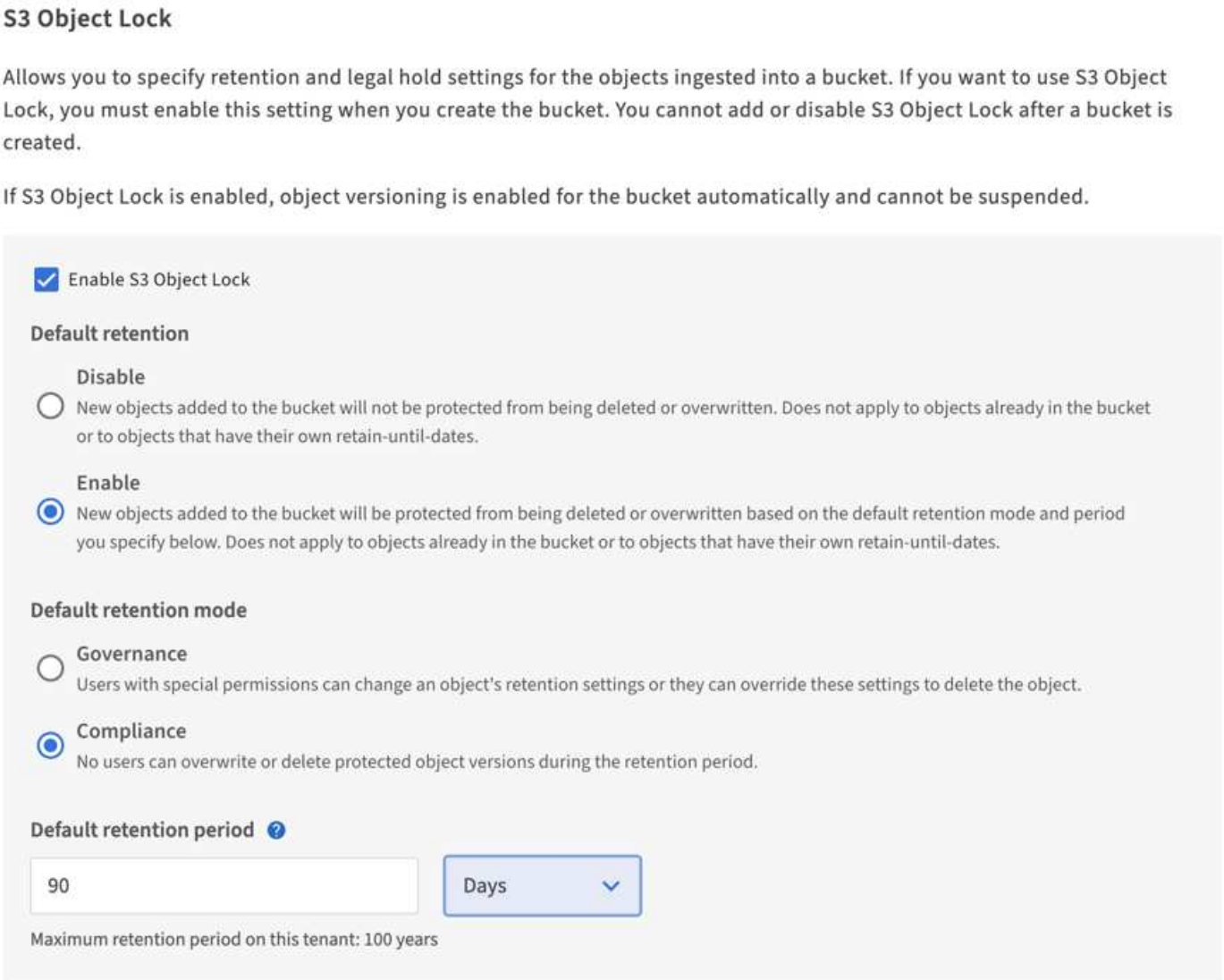
- NetApp 제품 설명서 https://www.netapp.com/support-and-training/documentation/

오브젝트 잠금을 사용한 랜섬웨어 방어

StorageGRID의 오브젝트 잠금이 WORM 모델을 제공하여 데이터 삭제 또는 덮어쓰기를 방지하는 방법과 규정 요구사항을 충족하는 방법에 대해 알아보십시오.

오브젝트 잠금은 WORM 모델을 제공하여 오브젝트를 삭제하거나 덮어쓰지 못하도록 합니다. StorageGRID은 오브젝트 잠금 구축을 "Cohasset 평가됨" 통해 규정 요구사항을 충족하고, 오브젝트 보존에 대한 법적 증거 자료 보관, 규정 준수 모드, 거버넌스 모드와 기본 버킷 보존 정책을 지원합니다. 버킷 생성 및 버전 관리에서 오브젝트 잠금을 활성화해야 합니다. 개체의 특정 버전이 잠겨 있으며 버전 ID가 정의되지 않은 경우 현재 버전의 개체에 보존이 배치됩니다. 현재 버전에 보존이 구성되어 있고 개체를 삭제, 수정 또는 덮어쓰려고 하면 삭제 표식 또는 개체의 새 수정본을 현재 버전으로 사용하여 새 버전이 만들어집니다. 잠긴 버전은 현재 버전이 아닌 버전으로 유지됩니다. 아직 호환되지 않는 애플리케이션의 경우 오브젝트 잠금과 버킷에 배치된 기본 보존 구성을 계속 사용할 수 있습니다. 구성이 정의된 후 버킷에 삽입되는 각 새 오브젝트에 오브젝트 보존을 적용합니다. 보존 시간이 경과하기 전에 응용 프로그램이 개체를 삭제하거나 덮어쓰지 않도록 구성된 한 이 기능은 작동합니다.

테넌트 관리 UI에서 버킷을 생성할 때 객체 잠금을 활성화하고 기본 보존 모드와 보존 기간을 구성할 수 있습니다. 이 옵션을 구성하면 해당 버킷에 수집된 모든 객체에 대한 최소 객체 잠금 보존 기간이 설정됩니다.



다음은 Object Lock API를 사용하는 몇 가지 예입니다.

오브젝트 잠금 법적 보관은 오브젝트에 적용되는 간단한 켜기/끄기 상태입니다.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

법적 증거 자료 보관 상태를 설정해도 성공하면 어떤 값도 반환되지 않으므로 가져오기 작업으로 확인할 수 있습니다.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

법적 보류를 해제하려면 끄기 상태를 적용합니다.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

객체 보존 설정은 Retain until timestamp로 설정됩니다.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

다시 한 번 말씀드리지만 성공 시 반환된 값이 없으므로 GET 호출과 마찬가지로 보존 상태를 확인할 수 있습니다.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

객체 잠금이 활성화된 버킷에 기본 보존을 설정하면 보존 기간이 일 및 년 단위로 사용됩니다.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

대부분의 작업과 마찬가지로 성공 시 응답이 반환되지 않으므로 확인할 구성에 대해 GET를 수행할 수 있습니다.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

다음으로, 보존 구성이 적용된 상태로 버켓에 객체를 넣을 수 있습니다.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

Put 작업이 응답을 반환합니다.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

보존 개체에서 이전 예제에서 버킷에 설정된 보존 기간은 개체의 보존 타임스탬프로 변환됩니다.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

버전 관리와 함께 복제된 버킷을 사용하는 랜섬웨어 방어

StorageGRID CloudMirror를 사용하여 오브젝트를 보조 버킷으로 복제하는 방법에 대해 알아보십시오.

모든 애플리케이션과 워크로드가 오브젝트 잠금과 호환되지 않습니다. 또 다른 옵션은 오브젝트를 동일한 그리드(액세스가 제한된 다른 테넌트 권장) 또는 StorageGRID 플랫폼 서비스를 사용하는 기타 S3 엔드포인트인 CloudMirror에 복제하는 것입니다.

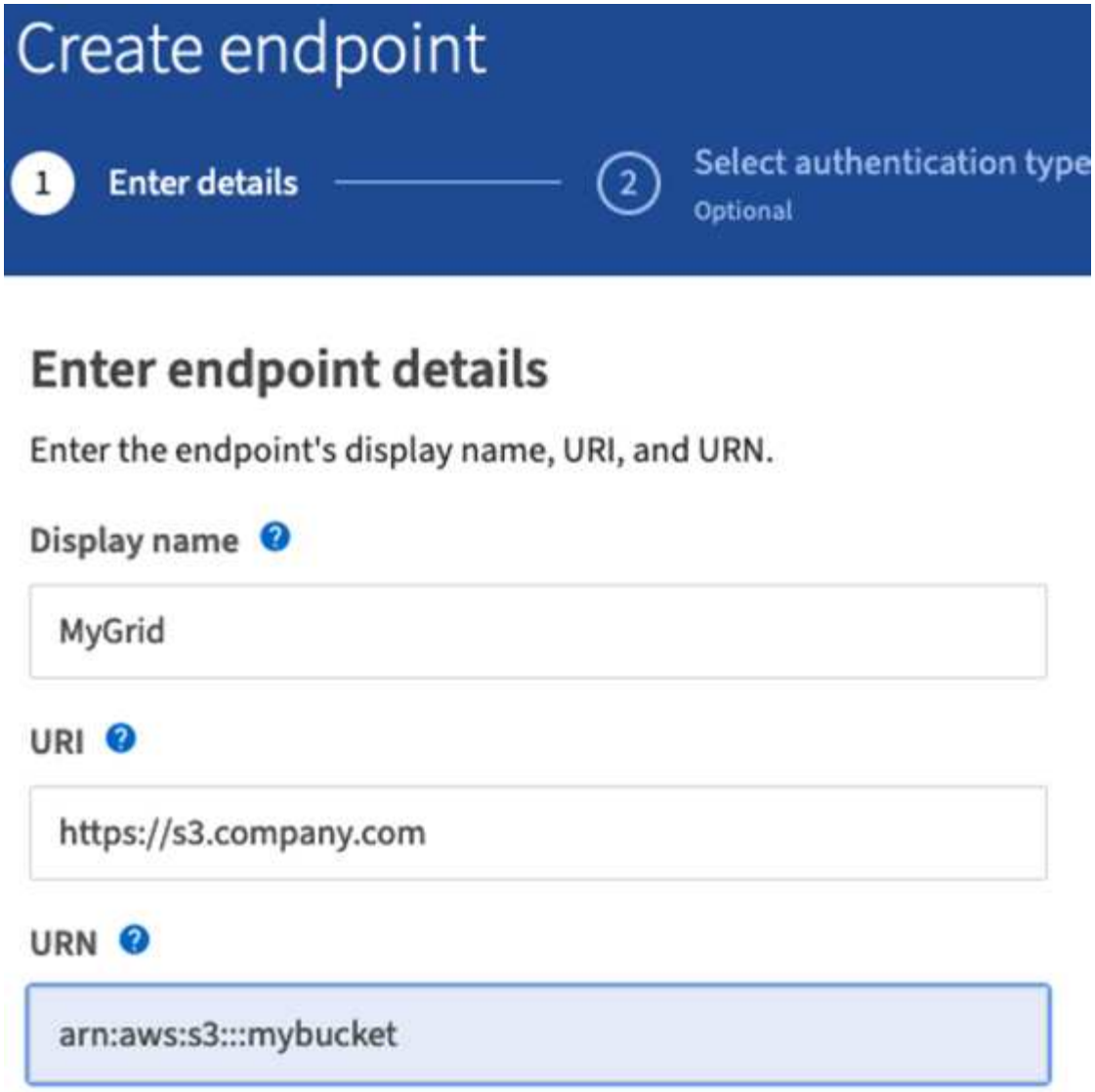
StorageGRID CloudMirror는 StorageGRID의 구성 요소로, 버킷의 오브젝트를 소스 버킷에 수집될 때 정의된 대상에 복제하도록 구성할 수 있으며 삭제를 복제하지 않는다. CloudMirror는 StorageGRID의 통합 구성 요소이므로 S3 API 기반 공격에 의해 해제하거나 조작할 수 없습니다. 버전 관리를 사용하도록 설정한 상태에서 이 복제된 버킷을 구성할 수 있습니다. 이 시나리오에서는 폐기해도 안전한 복제된 버킷의 이전 버전을 자동으로 정리해야 합니다. 이를 위해 StorageGRID ILM 정책 엔진을 사용할 수 있습니다. 공격을 식별하고 복구하기에 충분한 며칠간 현재 시간을 기준으로 개체 배치를 관리하는 규칙을 만듭니다.

이 접근 방식의 한 가지 단점은 버킷의 완전한 두 번째 복사본과 일정 시간 동안 유지되는 오브젝트의 여러 버전을 확보함으로써 더 많은 스토리지를 소비한다는 것입니다. 또한 기본 버킷에서 의도적으로 삭제된 객체를 복제된 버킷에서 수동으로 제거해야 합니다. NetApp CloudSync와 같은 제품 이외의 다른 복제 옵션으로는 비슷한 솔루션에 대해 삭제 작업을 복제할 수 있습니다. 버전 관리가 활성화되고 객체 잠금이 설정되지 않은 보조 버킷의 또 다른 단점은 보조 위치에 손상을 일으키는 데 사용할 수 있는 권한이 있는 계정이 많다는 것입니다. 장점은 해당 엔드포인트 또는 테넌트 버킷에 대한 고유한 계정이어야 하며, 주 위치의 계정에 대한 액세스 권한이 포함되지 않거나 그 반대의 경우도 마찬가지입니다.

소스 및 대상 버킷을 생성하고 대상이 버전 관리로 구성된 후에는 다음과 같이 복제를 구성하고 설정할 수 있습니다.

단계

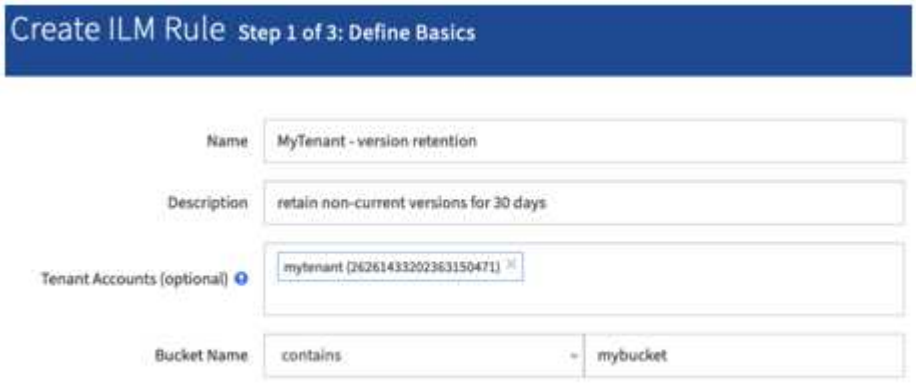
1. CloudMirror를 구성하려면 S3 대상에 대한 플랫폼 서비스 엔드포인트를 생성합니다.

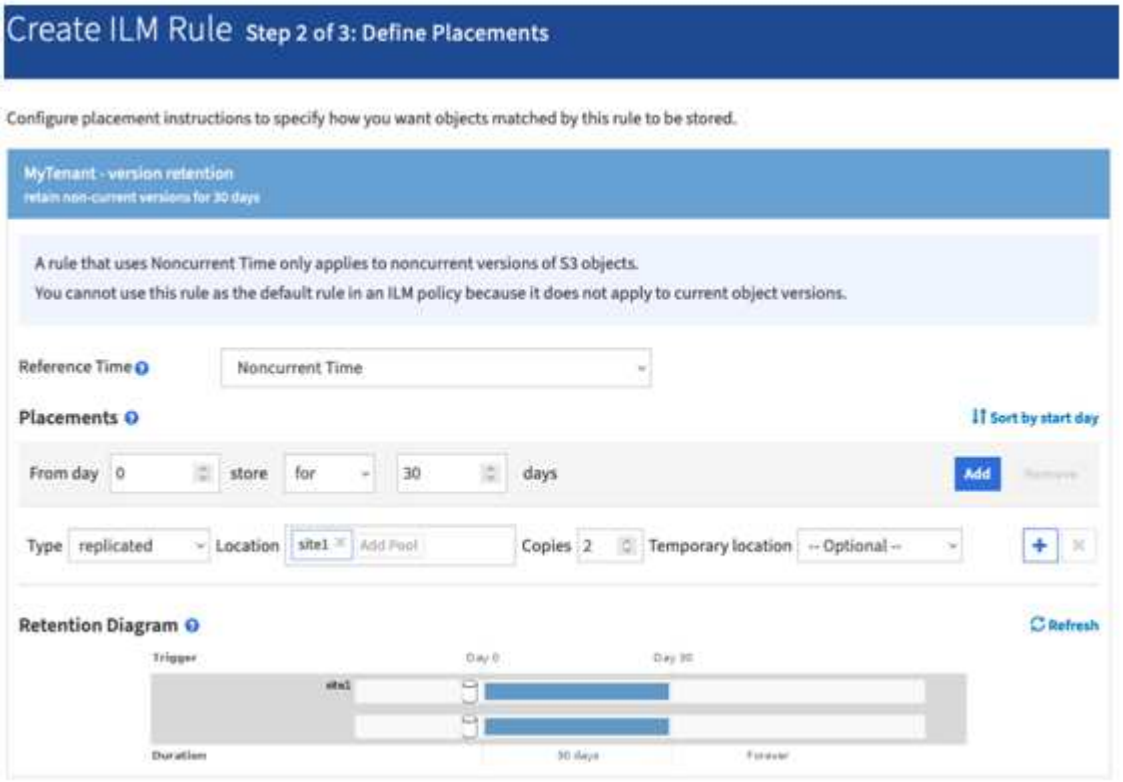


2. 소스 버킷에서 구성된 엔드포인트를 사용하도록 복제를 구성합니다.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. 스토리지 배치 및 버전 스토리지 기간 관리를 관리하는 ILM 규칙을 생성합니다. 이 예에서는 저장할 객체의 최신 버전이 아닌 버전이 구성되어 있습니다.





30일 동안 사이트 1에 2개의 복사본이 있습니다. 또한 소스 버킷 스토리지 기간과 일치하도록 ILM 규칙에서 수집 시간을 참조 시간으로 사용하는 것을 기반으로 오브젝트의 현재 버전에 대한 규칙을 구성합니다. 오브젝트 버전에 대한 스토리지 배치는 삭제 코딩 또는 복제할 수 있습니다.

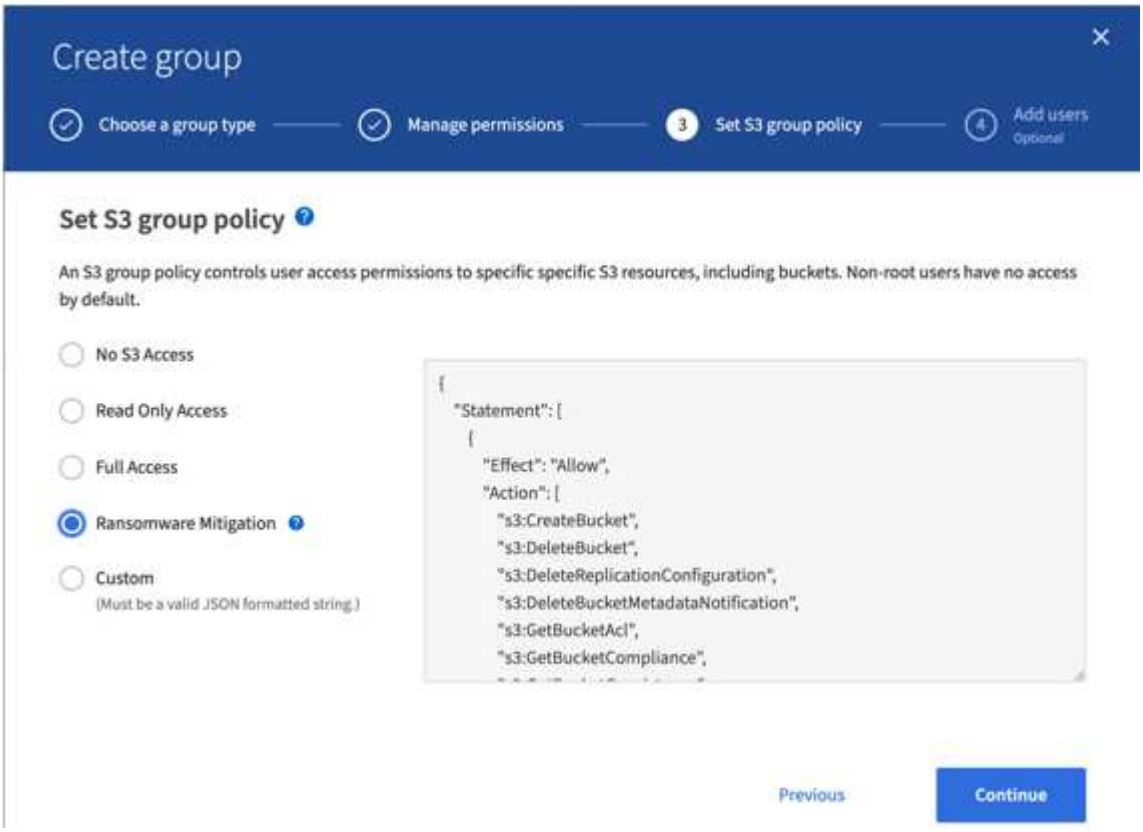
보호 **IAM** 정책을 통한 버전 관리를 사용한 랜섬웨어 방어

버킷에서 버전 관리를 활성화하고 StorageGRID의 사용자 보안 그룹에 IAM 정책을 구현하여 데이터를 보호하는 방법에 대해 알아보십시오.

오브젝트 잠금 또는 복제를 사용하지 않고 데이터를 보호하는 방법은 버킷에서 버전 관리를 활성화하고 사용자 보안 그룹에 IAM 정책을 구현하여 사용자의 오브젝트 버전 관리 기능을 제한하는 것입니다. 공격이 발생할 경우 데이터의 잘못된 새 버전이 현재 버전으로 만들어지고 최신 버전이 아닌 최신 버전이 안전한 클린 데이터입니다. 데이터에 대한 액세스를 얻기 위해 손상된 계정에는 나중에 복원 작업을 위해 데이터를 보호하는 최신 버전이 아닌 버전을 삭제하거나 변경할 수 있는 액세스 권한이 없습니다. 이전 시나리오와 마찬가지로 ILM 규칙은 사용자가 선택한 기간 동안 비최신

버전의 보존을 관리합니다. 단점은 공격자 공격에 대한 권한이 있는 계정이 존재할 가능성이 여전히 존재하지만 모든 응용 프로그램 서비스 계정과 사용자는 보다 제한적인 액세스를 사용하여 구성해야 한다는 것입니다. 제한 그룹 정책은 사용자 또는 응용 프로그램에서 수행할 수 있는 각 작업을 명시적으로 허용해야 하며, 사용자가 수행할 수 없도록 하려는 모든 작업은 명시적으로 거부해야 합니다. 앞으로 새 작업이 도입될 수 있으므로 와일드카드 ALLOW를 사용하지 않는 것이 좋습니다. 이 경우 허용할지 거부할지 여부를 제어할 수 있습니다 NetApp. 이 솔루션의 경우 거부 목록에는 사용자 또는 프로그래밍 방식의 변경으로부터 버킷 및 개체 버전의 버전 관리를 보호하기 위해 DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration 및 PutBucketVersioning이 포함되어야 합니다.

StorageGRID 에서 S3 그룹 정책 옵션인 "랜섬웨어 완화"를 사용하면 이 솔루션을 더 쉽게 구현할 수 있습니다. 테넌트에서 사용자 그룹을 생성할 때 그룹 권한을 선택하면 이 선택적 정책을 볼 수 있습니다.



다음은 명시적으로 허용되는 대부분의 사용 가능한 작업과 필요한 최소 거부 작업이 포함된 그룹 정책의 내용입니다.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
```

```
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
```

```
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

랜섬웨어 조사 및 해결

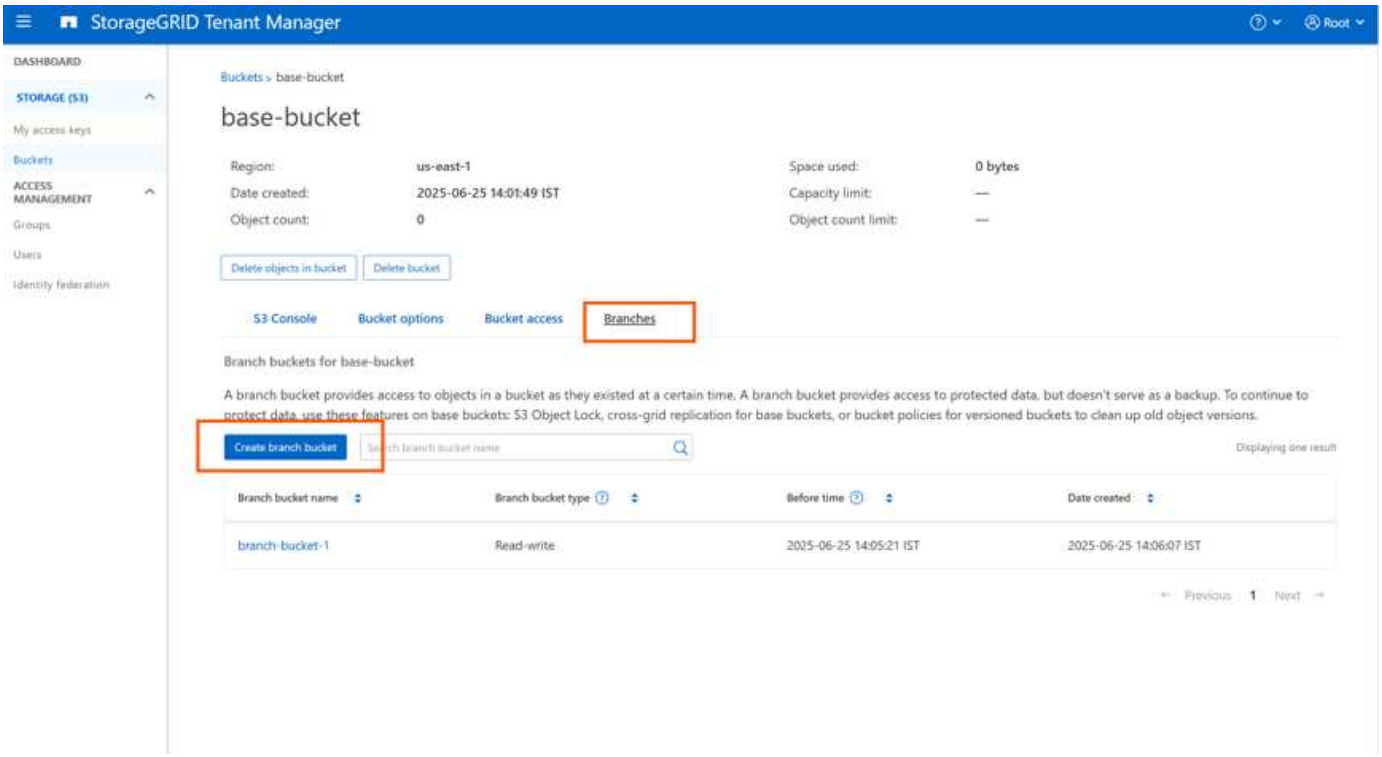
StorageGRID 사용하여 랜섬웨어 공격이 발생한 후 버킷을 조사하고 해결하는 방법을 알아보세요.

StorageGRID 12.0에서는 랜섬웨어 방어를 위한 버전 관리의 유용성을 확장하기 위해 새로운 브랜치 버킷 기능이 추가되었습니다. 분기 버킷은 버킷에 있는 객체에 대한 액세스를 특정 시점에 존재했던 그대로 제공하며, 해당 객체가 버킷에 계속 존재하는 경우에 한합니다. 버전 관리가 활성화된 기본 버킷에 대해서만 브랜치 버킷을 생성할 수 있습니다.

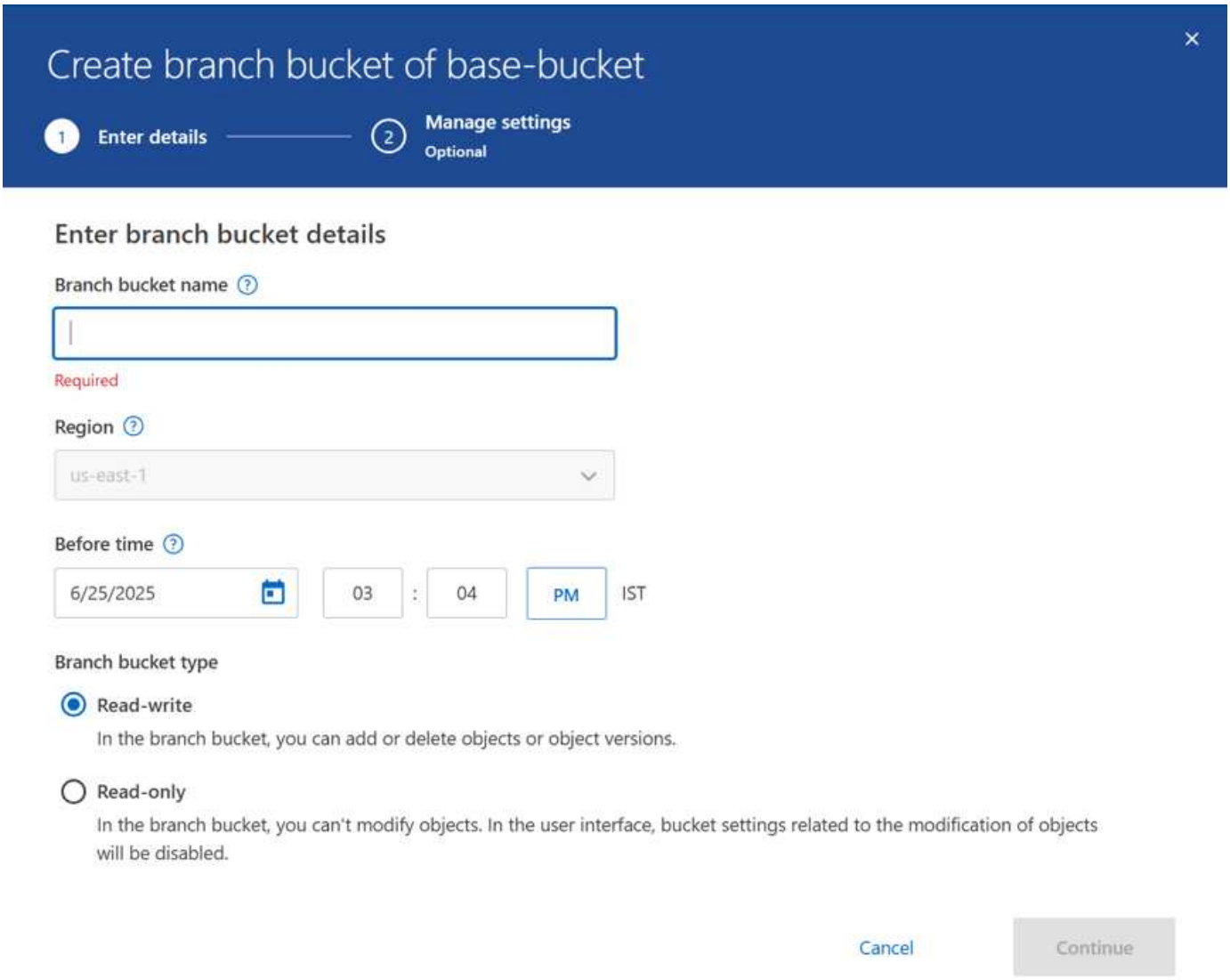
즉, 랜섬웨어 공격이 발생했다고 의심되는 경우 초기 공격 시간 이전에 존재했던 모든 개체와 버전을 포함하는 읽기/쓰기 또는 읽기 전용 분기 버킷을 만들 수 있습니다. 이 분기 버킷을 사용하면 기본 버킷 내용과 비교하여 어떤 객체가 변경되었는지, 그리고 변경 사항이 공격의 일부인지 여부를 파악할 수 있습니다. 공격을 조사하는 동안 클린 브랜치를 사용하여 클라이언트 작업을 계속하기 위해 브랜치 버킷을 사용할 수도 있습니다.

지점 버킷 만들기

- 기본 버킷 세부 정보 페이지와 지점 탭으로 이동하여 지점 버킷을 만듭니다.



- 지점 버킷 만들기 버튼을 클릭하면 기본 버킷과 연관된 지역의 세부 정보가 미리 입력된 팝업이 열립니다.
- 시간 전에 브랜치 버킷 이름을 제공하고, 어떤 유형의 브랜치 버킷을 생성할지 선택합니다.



TR-4765: StorageGRID 모니터링

StorageGRID 모니터링 소개

Splunk와 같은 외부 애플리케이션을 사용하여 StorageGRID 시스템을 모니터링하는 방법에 대해 알아보십시오.

NetApp StorageGRID 오브젝트 기반 스토리지를 효과적으로 모니터링하여 관리자는 긴급한 문제에 빠르게 대응하고 인력을 사전에 추가하여 증가하는 워크로드를 처리할 수 있습니다. 이 보고서에서는 주요 지표를 모니터링하는 방법과 외부 모니터링 애플리케이션을 활용하는 방법에 대한 일반적인 지침을 제공합니다. 기존의 모니터링 및 문제 해결 가이드를 보완하기 위한 것입니다.

NetApp StorageGRID 구축은 일반적으로 여러 사이트와 다수의 노드로 구성되며 내결함성이 있는 분산 오브젝트 스토리지 시스템을 구축하는 데 필요한 다수의 노드로 구성됩니다. StorageGRID와 같은 분산 및 복구 기능이 있는 스토리지 시스템에서는 그리드가 계속 정상적으로 작동하는 동안 오류 상태가 발생하는 것이 정상입니다. 관리자의 과제는 오류 조건(예: 노드 다운)이 문제를 즉시 해결해야 하는 임계값과 분석해야 하는 정보를 파악하는 것입니다. StorageGRID에서 제공하는 데이터를 분석하면 워크로드를 이해하고 리소스를 더 추가해야 하는 경우와 같은 정보에 입각한 의사 결정을 내릴 수 있습니다.

StorageGRID는 모니터링의 주제를 자세히 살펴보는 훌륭한 문서를 제공합니다. 이 보고서에서는 사용자가 StorageGRID에 대해 잘 알고 있고 해당 문서에 대한 문서를 검토한 것으로 가정합니다. NetApp은 이 정보를 반복하는 대신 이 가이드 전체에서 제품 설명서를 참조합니다. StorageGRID 제품 설명서는 온라인에서 PDF 형식으로 제공됩니다.

이 문서의 목표는 제품 설명서를 보완하고 Splunk와 같은 외부 애플리케이션을 사용하여 StorageGRID 시스템을 모니터링하는 방법에 대해 논의하는 것입니다.

데이터 소스

NetApp StorageGRID를 성공적으로 모니터링하려면 StorageGRID 시스템의 상태 및 운영에 대한 데이터를 수집할 위치를 파악하는 것이 중요합니다.

- * 웹 UI 및 대시보드. * StorageGRID 그리드 관리자는 관리자가 논리적 프레젠테이션에서 확인해야 하는 정보의 최상위 보기를 제공합니다. 관리자는 문제 해결 및 로그 수집을 위한 서비스 수준 정보를 더욱 자세히 살펴볼 수도 있습니다.
- * 감사 로그. * StorageGRID는 PUT, GET, 삭제와 같은 테넌트 작업의 세부적인 감사 로그를 유지합니다. 또한 수집부터 데이터 관리 규칙의 애플리케이션에 이르기까지 오브젝트의 라이프사이클을 추적할 수 있습니다.
- * 메트릭 API. * StorageGRID GMI의 기반이 되는 API는 API 기반이므로 개방형 API입니다. 이 접근 방식을 사용하면 외부 모니터링 및 분석 툴을 사용하여 데이터를 추출할 수 있습니다.

추가 정보를 찾을 수 있는 위치

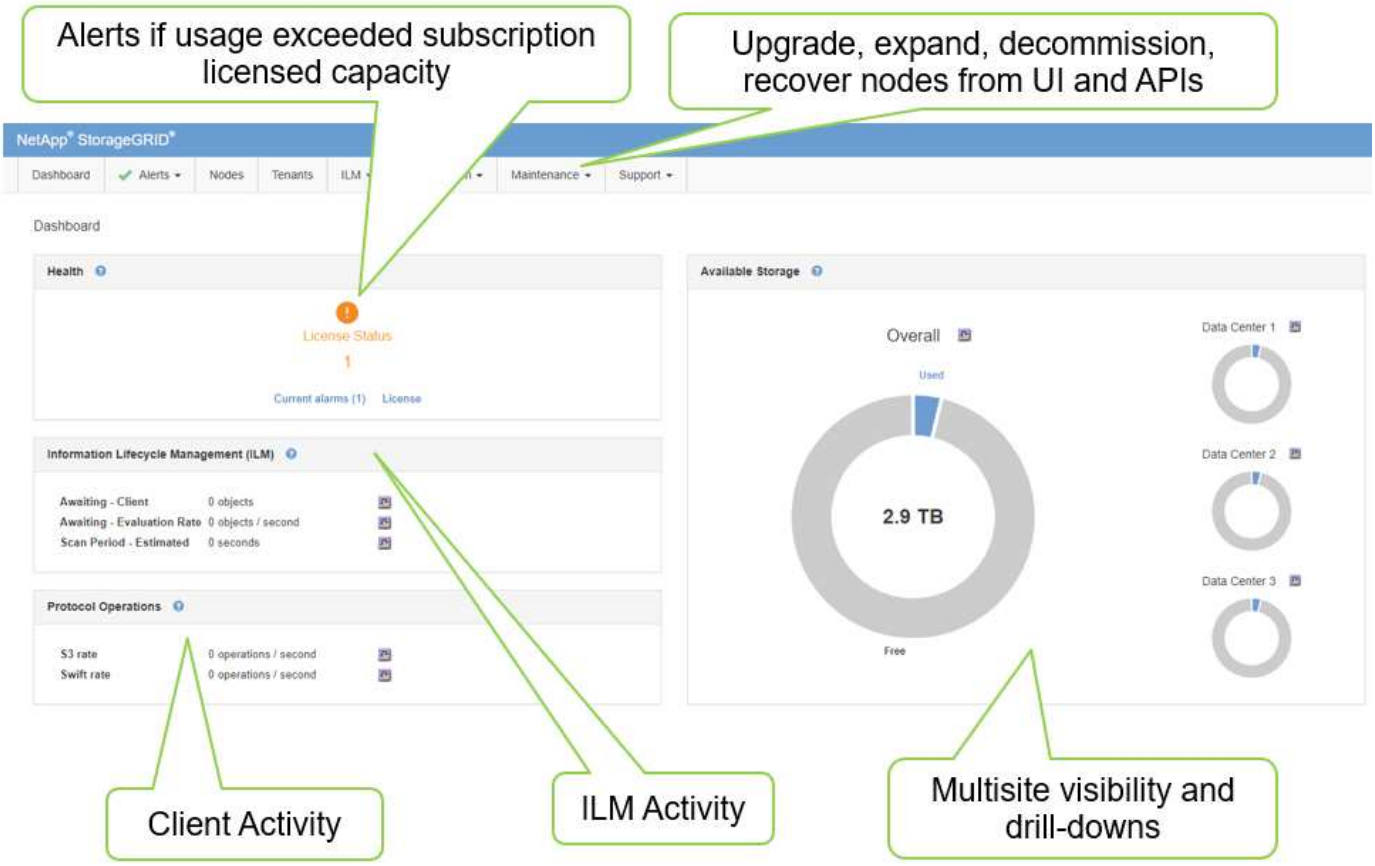
이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- NetApp StorageGRID 문서 센터 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 지원 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp 제품 설명서 https://www.netapp.com/support-and-training/documentation/
- Splunk를 위한 NetApp StorageGRID 앱 https://splunkbase.splunk.com/app/3898/#/details

GMI 대시보드를 사용하여 **StorageGRID**를 모니터링합니다

StorageGRID 그리드 관리 인터페이스(GMI) 대시보드를 통해 StorageGRID 인프라를 중앙 집중식으로 볼 수 있으므로 전체 그리드의 상태, 성능 및 용량을 모니터링할 수 있습니다.

GMI 대시보드를 사용하여 그리드의 각 핵심 구성 요소를 검사합니다.



정기적으로 모니터링해야 하는 정보입니다

이 기술 보고서의 이전 버전에는 주기적으로 확인해야 할 메트릭과 트렌드가 나열되어 있습니다. 이제 해당 정보가 에 "모니터링 및 문제 해결 설명서"포함됩니다.

스토리지 모니터링

이 기술 보고서의 이전 버전에는 객체 스토리지 공간, 메타데이터 공간, 네트워크 리소스 등과 같은 중요한 메트릭의 모니터링 위치가 나열되어 있습니다. 이제 해당 정보가 에 "모니터링 및 문제 해결 설명서"포함됩니다.

경고를 사용하여 **StorageGRID** 모니터링

StorageGRID의 알림 시스템을 사용하여 문제를 모니터링하고, 사용자 지정 경고를 관리하고, SNMP 또는 이메일을 사용하여 알림 알림을 확장하는 방법에 대해 알아봅니다.

경고는 StorageGRID 시스템 내의 다양한 이벤트와 조건을 모니터링할 수 있도록 중요한 정보를 제공합니다.

경고 시스템은 StorageGRID 시스템에서 발생할 수 있는 문제를 모니터링하는 기본 도구로 설계되었습니다. 경고 시스템은 시스템에서 실행 가능한 문제에 초점을 맞추고 사용이 간편한 인터페이스를 제공합니다.

Dell은 시스템 모니터링 및 문제 해결에 도움이 되는 다양한 기본 경고 규칙을 제공합니다. 사용자 지정 알림을 만들고, 기본 알림을 편집 또는 비활성화하고, 알림 알림을 해제하여 알림을 추가로 관리할 수 있습니다.

알림은 SNMP 또는 e-메일 알림을 통해 확장할 수도 있습니다.

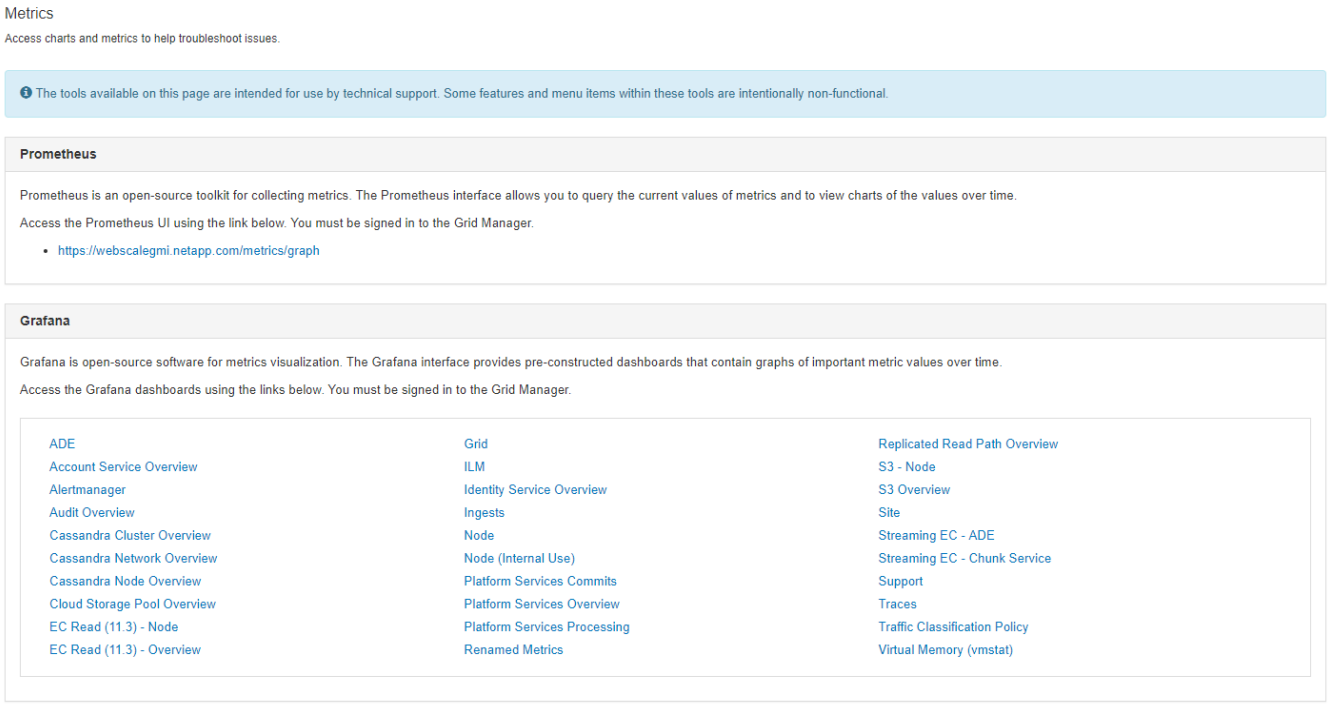
경고에 대한 자세한 내용은 온라인 및 PDF 형식으로 제공되는 를 "제품 설명서" 참조하십시오.

StorageGRID의 고급 모니터링 기능

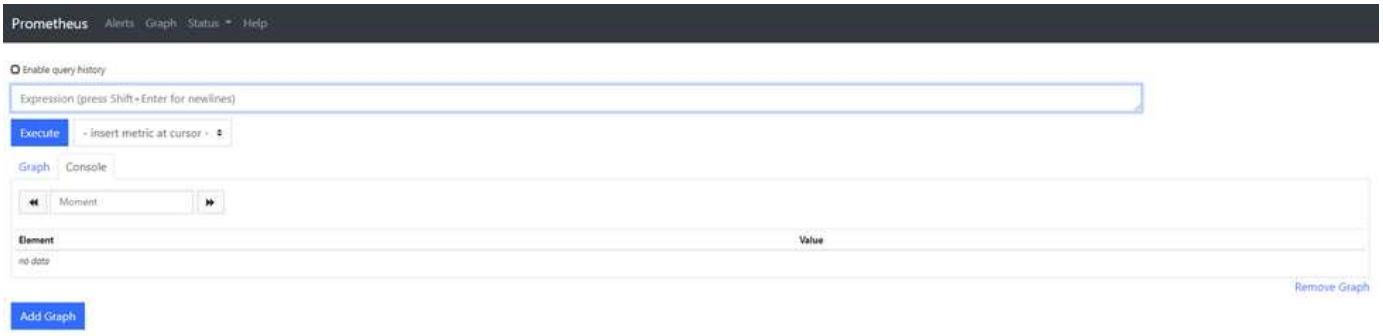
문제 해결에 도움이 되는 메트릭에 액세스하고 내보내는 방법에 대해 알아봅니다.

Prometheus 쿼리를 통해 메트릭 API를 봅니다

Prometheus는 메트릭을 수집하는 오픈 소스 소프트웨어입니다. GMI를 통해 StorageGRID의 임베디드 Prometheus에 액세스하려면 지원 [메트릭] 메뉴로 이동하십시오.



또는 링크로 직접 이동할 수 있습니다.

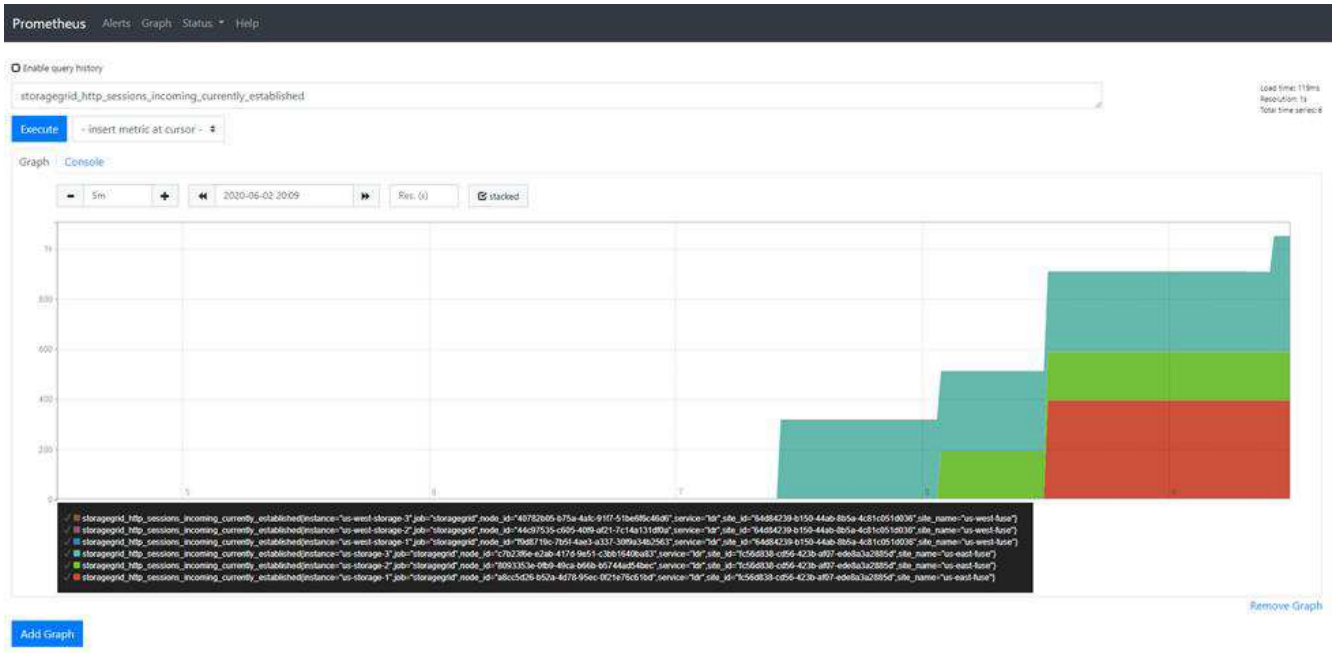


이 보기를 사용하여 Prometheus 인터페이스에 액세스할 수 있습니다. 여기에서 사용 가능한 메트릭을 검색하고 쿼리를 실험해 볼 수도 있습니다.

Prometheus URL 쿼리를 만들려면 다음 단계를 수행합니다.

단계

1. 쿼리 텍스트 상자에 입력을 시작합니다. 입력하면 메트릭이 나열됩니다. 목적상 StorageGRID 및 노드로 시작하는 메트릭만 중요합니다.
2. 각 노드의 HTTP 세션 수를 보려면 `storagegrid_http` 를 입력하고 를 선택합니다 `storagegrid_http_sessions_incoming_currently_established`. Execute(실행) 를 클릭하여 정보를 그래프 또는 콘솔 형식으로 표시합니다.



이 URL을 통해 작성하는 쿼리와 차트는 유지되지 않습니다. 복잡한 쿼리는 관리 노드의 리소스를 소비합니다. NetApp은 이 보기를 사용하여 사용 가능한 메트릭을 탐색할 것을 권장합니다.

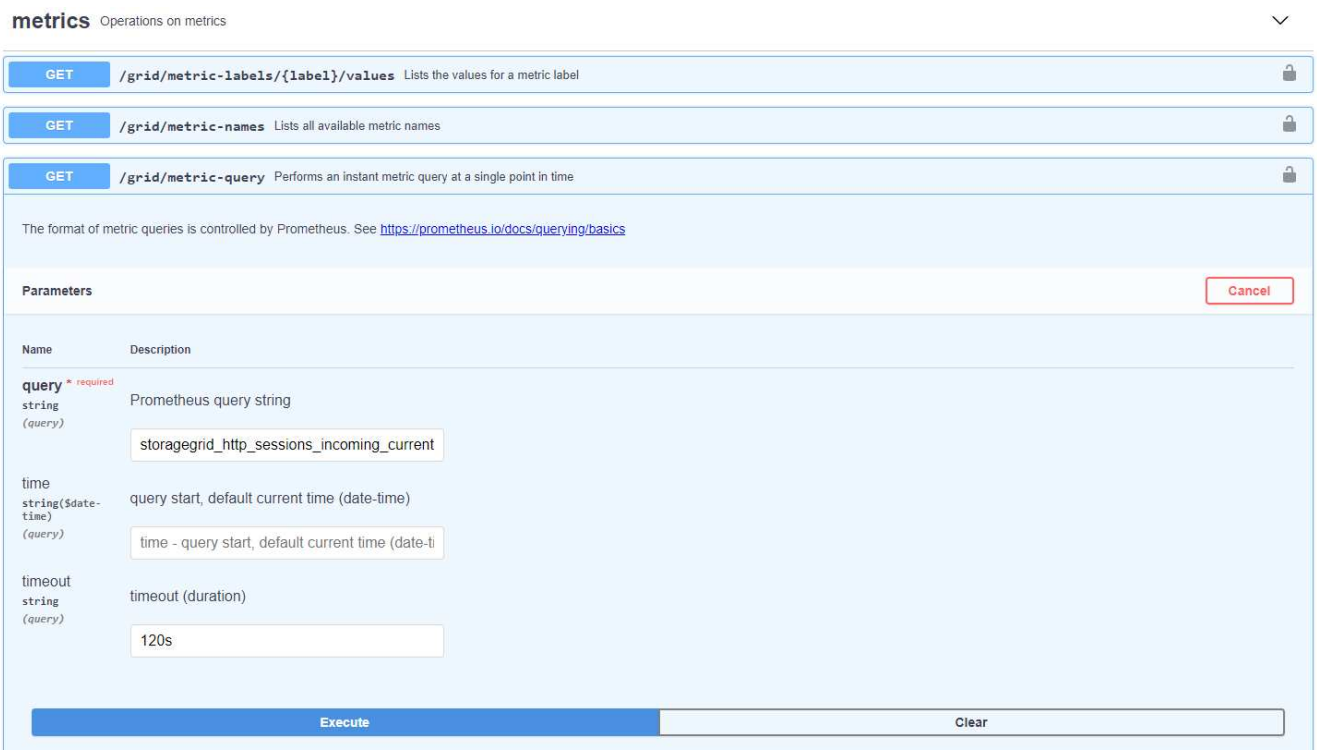
추가 포트를 열어야 하므로 Prometheus 인스턴스에 직접 접속하지 않는 것이 좋습니다. API를 통한 메트릭 액세스는 권장되고 안전한 방법입니다.

API를 통해 메트릭을 내보냅니다

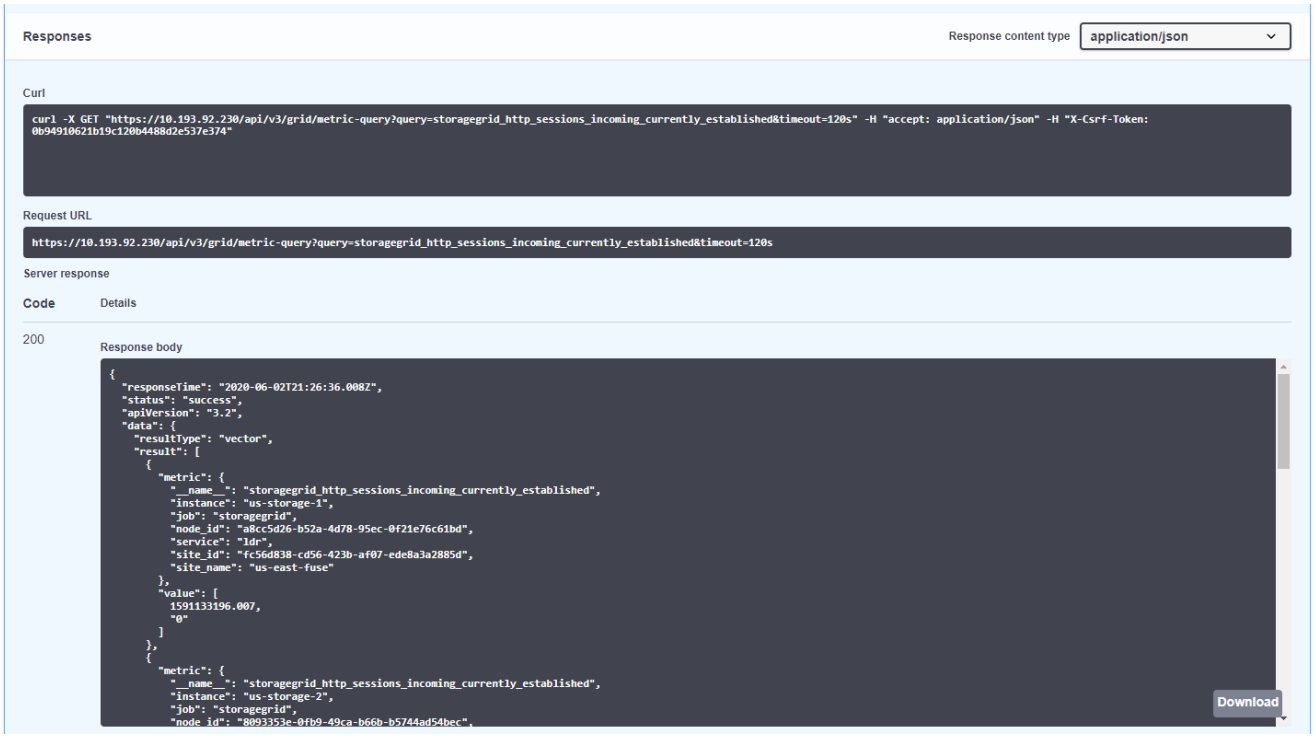
StorageGRID 관리 API를 통해 동일한 데이터에 액세스할 수도 있습니다.

API를 통해 메트릭을 내보내려면 다음 단계를 수행하십시오.

1. GMI에서 도움말 [API Documentation] 메뉴를 선택합니다.
2. 메트릭까지 아래로 스크롤하여 Get/grid/metric-query를 선택합니다.



응답에는 Prometheus URL 쿼리를 통해 얻을 수 있는 것과 동일한 정보가 포함됩니다. 각 스토리지 노드에 현재 설정된 HTTP 세션 수를 다시 볼 수 있습니다. 읽기 쉽도록 JSON 형식으로 응답을 다운로드할 수도 있습니다. 다음 그림에서는 Prometheus 쿼리 응답의 예를 보여 줍니다.



API를 사용하면 인증된 쿼리를 수행할 수 있다는 이점이 있습니다

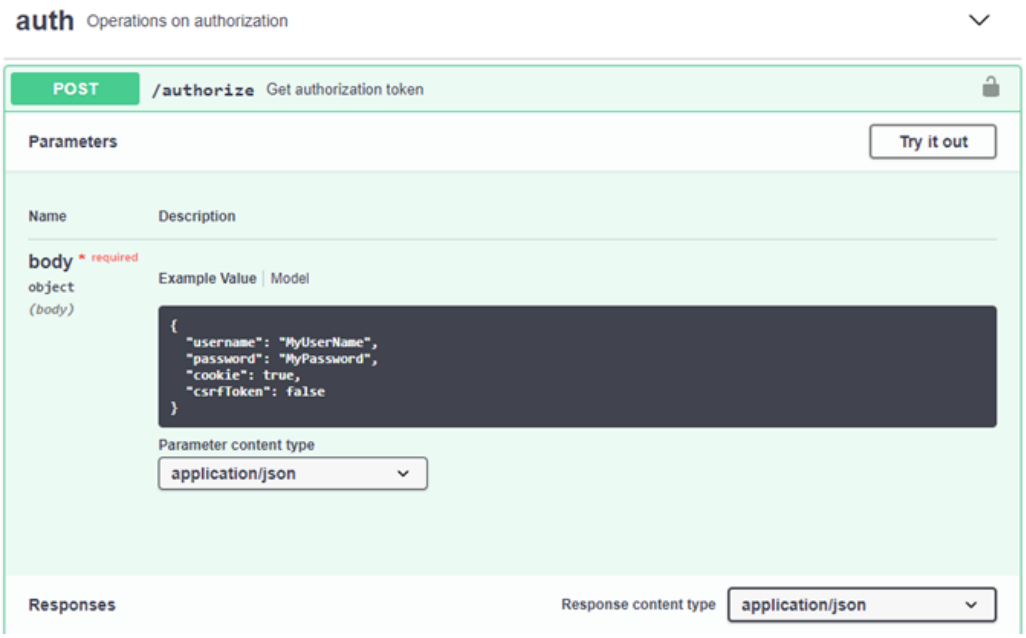
StorageGRID에서 curl을 사용하여 메트릭에 액세스할 수 있습니다

curl을 사용하여 CLI를 통해 메트릭에 액세스하는 방법을 알아보십시오.

이 작업을 수행하려면 먼저 인증 토큰을 얻어야 합니다. 토큰을 요청하려면 다음 단계를 따르십시오.

단계

1. GMI에서 도움말 [API Documentation] 메뉴를 선택합니다.
2. 인증까지 아래로 스크롤하여 승인에 대한 작업을 찾습니다. 다음 스크린샷은 POST 메서드의 매개 변수를 보여 줍니다.



3. 시험해보기 를 클릭하고 GMI 사용자 이름과 암호로 본문을 편집합니다.
4. 실행 을 클릭합니다.
5. curl 섹션에 제공된 curl 명령을 복사하여 터미널 창에 붙여 넣습니다. 명령은 다음과 같습니다.

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

> GMI 암호에 특수 문자가 포함된 경우 특수 문자를 이스케이프 처리하려면 \ 를 사용해야 합니다. 예를 들어, replace! 포함\!

6. 앞의 curl 명령을 실행하면 다음 예제와 같은 인증 토큰이 출력에 제공됩니다.

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

이제 인증 토큰 문자열을 사용하여 curl을 통해 메트릭에 액세스할 수 있습니다. 메트릭 액세스 프로세스는 섹션의 단계와 유사합니다 "StorageGRID의 고급 모니터링 기능". 그러나 데모 목적으로 메트릭 범주에서 Get/grid/metric-labels/{label}/ 값을 선택한 예를 보여 줍니다.

7. 예를 들어, 앞의 인증 토큰을 사용하여 다음 curl 명령을 실행하면 StorageGRID의 사이트 이름이 나열됩니다.

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

curl 명령은 다음 출력을 생성합니다.

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

StorageGRID에서 Grafana 대시보드를 사용하여 메트릭을 봅니다

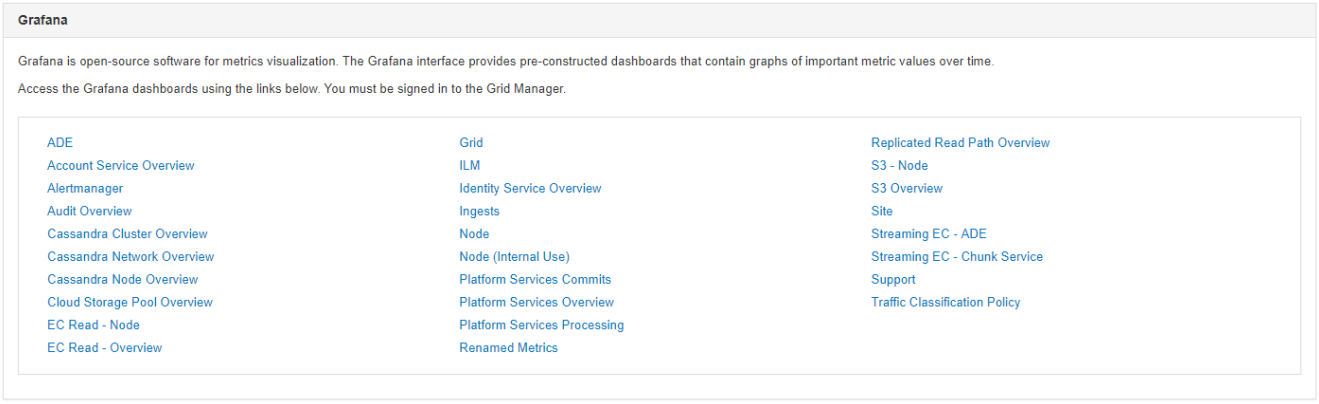
Grafana 인터페이스를 사용하여 StorageGRID 데이터를 시각화하고 모니터링하는 방법에 대해 알아보십시오.

Grafana는 메트릭 시각화를 위한 오픈 소스 소프트웨어입니다. 기본적으로 NetApp은 StorageGRID 시스템에 관한 유용하고 강력한 정보를 제공하는 사전 구성된 대시보드를 보유하고 있습니다.

이러한 사전 구성된 대시보드는 모니터링뿐만 아니라 문제 해결에도 유용합니다. 일부 제품은 기술 지원 부서에서 사용할 수 있습니다. 예를 들어 스토리지 노드의 메트릭을 보려면 다음 단계를 수행합니다.

단계

1. GMI에서 Support [Metrics](지원 [메트릭]) 메뉴를 선택합니다.
2. Grafana 섹션에서 Node 대시보드를 선택합니다.



3. Grafana에서 메트릭을 보려는 노드로 호스트를 설정합니다. 이 경우 스토리지 노드가 선택됩니다. 다음 스크린샷 캡처보다 더 많은 정보가 제공됩니다.

StorageGRID에서 트래픽 분류 정책을 사용합니다

StorageGRID에서 네트워크 트래픽을 관리하고 최적화하기 위해 트래픽 분류 정책을 설정하고 구성하는 방법에 대해 알아봅니다.

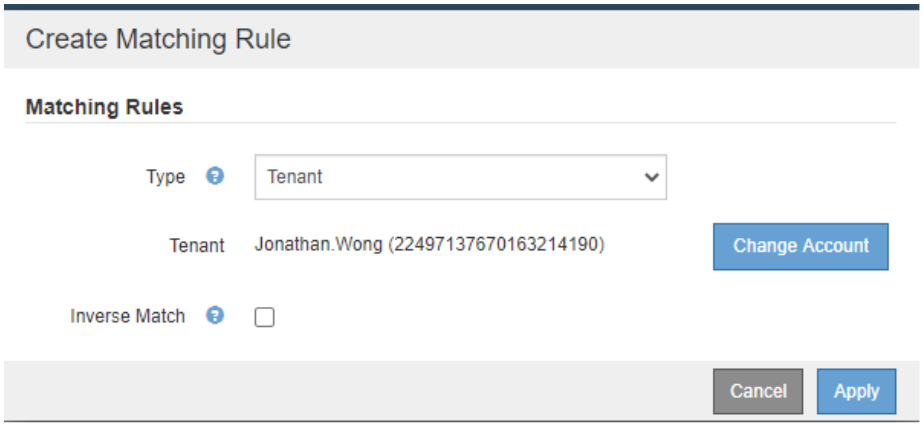
트래픽 분류 정책은 특정 테넌트, 버킷, IP 서브넷 또는 로드 밸런서 끝점을 기준으로 트래픽을 모니터링 및/또는 제한하는 방법을 제공합니다. 네트워크 연결 및 대역폭은 StorageGRID에서 특히 중요한 메트릭입니다.

트래픽 분류 정책을 구성하려면 다음 단계를 수행하십시오.

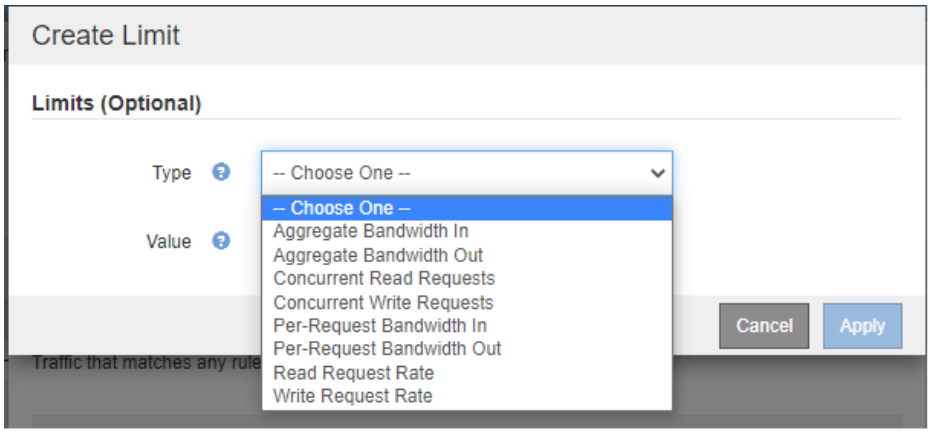
단계

1. GMI에서 구성 [시스템 설정 > 교통 분류] 메뉴로 이동합니다.
2. Create+를 클릭합니다
3. 정책의 이름과 설명을 입력합니다.

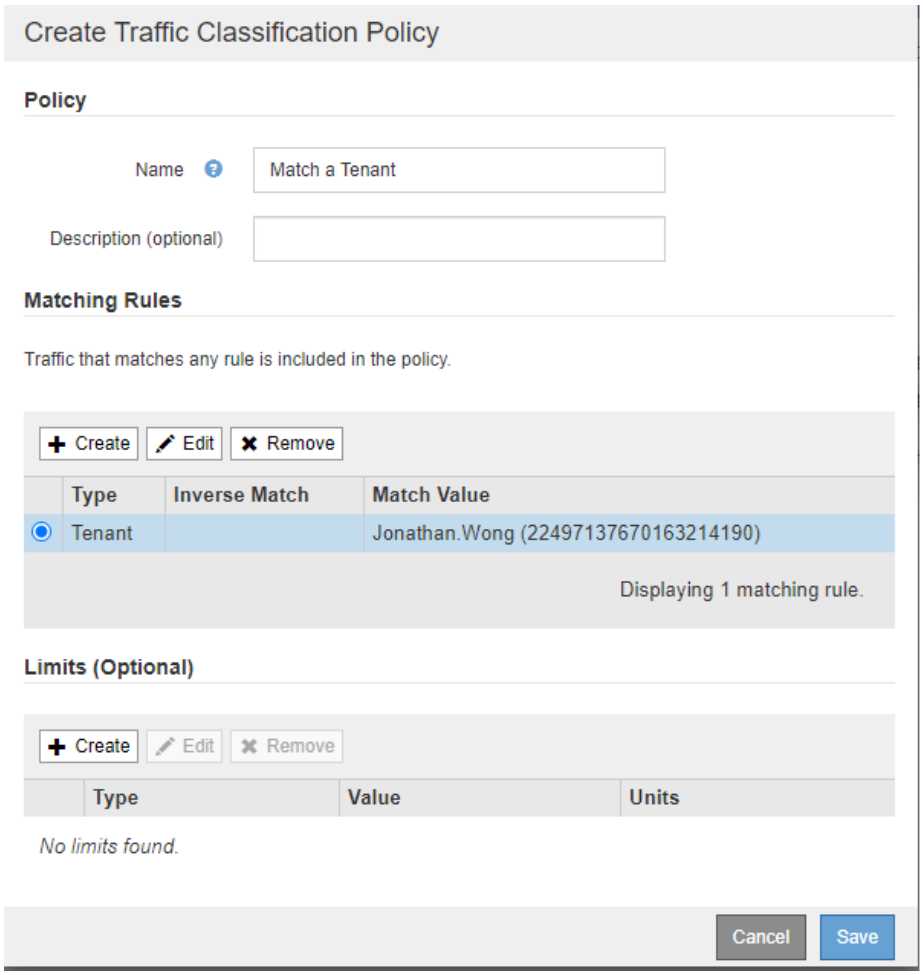
4. 일치하는 규칙을 만듭니다.



5. 제한을 설정합니다(선택 사항).



6. 정책을 저장합니다



트래픽 분류 정책과 관련된 메트릭을 보려면 정책을 선택하고 메트릭을 클릭합니다. 부하 분산 요청 트래픽 및 평균 요청 기간 등의 정보를 표시하는 Grafana 대시보드가 생성됩니다.

감사 로그를 사용하여 **StorageGRID**를 모니터링합니다

StorageGRID 감사 로그를 사용하여 테넌트 및 그리드 활동에 대한 자세한 인사이트를 얻고 Splunk와 같은 툴을 로그 분석에 활용하는 방법에 대해 알아보십시오.

StorageGRID 감사 로그를 사용하면 테넌트 및 그리드 활동에 대한 세부 정보를 수집할 수 있습니다. 감사 로그는 NFS를 통해 분석에 사용할 수 있습니다. 감사 로그를 내보내는 방법에 대한 자세한 지침은 관리자 안내서 를 참조하십시오.

감사를 내보낸 후 Splunk 또는 Logstash + Elasticsearch와 같은 로그 분석 툴을 사용하여 테넌트 활동을 이해하거나 자세한 청구 및 비용 청구 보고서를 생성할 수 있습니다.

감사 메시지에 대한 자세한 내용은 StorageGRID 설명서에 포함되어 있습니다. 을 "감사 메시지"참조하십시오.

Splunk용 **StorageGRID** 앱을 사용하십시오

Splunk 플랫폼 내에서 StorageGRID 환경을 모니터링하고 분석할 수 있는 Splunk용 NetApp StorageGRID 앱에 대해 알아보십시오.

Splunk는 머신 데이터를 가져오고 인덱싱하여 강력한 검색 및 분석 기능을 제공하는 소프트웨어 플랫폼입니다. NetApp StorageGRID 앱은 StorageGRID에서 활용하는 데이터를 가져오고 강화하는 Splunk용 애드온 앱입니다.

StorageGRID 추가 기능을 설치, 업그레이드 및 구성하는 방법에 대한 지침은 다음 웹 사이트에서 확인할 수 있습니다. https://splunkbase.splunk.com/app/3895/#/details

TR-4882: StorageGRID 베어 메탈 그리드를 설치합니다

StorageGRID 설치 소개

베어 메탈 호스트에 StorageGRID를 설치하는 방법을 알아보십시오.

TR-4882는 NetApp StorageGRID 작업 설치를 생성하는 실용적인 단계별 지침을 제공합니다. 설치 작업은 베어 메탈 또는 Red Hat Enterprise Linux(RHEL)에서 실행되는 가상 머신(VM)에 있을 수 있습니다. 제안된 레이아웃 및 스토리지 구성에서 3개의 물리적(또는 가상) 시스템에 6개의 StorageGRID 컨테이너식 서비스를 "제한적" 설치합니다. 일부 고객은 이 TR에 나온 구현 예제를 따르면 구현 프로세스를 더 쉽게 이해할 수 있습니다.

StorageGRID 및 설치 프로세스에 대한 자세한 내용은 제품 설명서의 [설치, 업그레이드 및 핫픽스 StorageGRID]를 참조하십시오 https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html .

구축을 시작하기 전에 NetApp StorageGRID 소프트웨어의 컴퓨팅, 스토리지 및 네트워킹 요구사항을 살펴보겠습니다. StorageGRID는 Podman 또는 Docker 내에서 컨테이너식 서비스로 실행됩니다. 이 모델에서 일부 요구사항은 호스트 운영 체제(StorageGRID 소프트웨어를 실행하는 Docker를 호스팅하는 OS)를 의미합니다. 또한 일부 리소스는 각 호스트 내에서 실행되는 Docker 컨테이너에 직접 할당됩니다. 이 배포에서는 하드웨어 사용을 극대화하기 위해 물리적 호스트당 두 개의 서비스를 구축하고 있습니다. 자세한 내용은 다음 섹션을 계속 "StorageGRID를 설치하기 위한 사전 요구 사항"진행하십시오.

이 TR에 요약된 단계를 수행하면 6개의 베어 메탈 호스트에 StorageGRID가 설치됩니다. 이제 대부분의 테스트 시나리오에서 유용한 작업 그리드 및 클라이언트 네트워크를 사용할 수 있습니다.

추가 정보를 찾을 수 있는 위치

본 TR에서 설명한 정보에 대해 자세히 알아보려면 다음 문서 리소스를 검토하십시오.

- NetApp StorageGRID 문서 센터 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 지원 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp 제품 설명서 https://www.netapp.com/support-and-training/documentation/

StorageGRID를 설치하기 위한 사전 요구 사항

StorageGRID을 구축하기 위한 컴퓨팅, 스토리지, 네트워크, Docker 및 노드 요구사항에 대해 알아보십시오.

컴퓨팅 요구사항

아래 표에는 각 StorageGRID 노드 유형에 대해 지원되는 최소 리소스 요구사항이 나와 있습니다. StorageGRID 노드에 필요한 최소 리소스입니다.

노드 유형입니다	**CPU** 코어	**RAM**
관리자	8	24GB
스토리지	8	24GB
게이트웨이	8	24GB

또한 각 물리적 Docker 호스트가 제대로 작동하려면 최소 16GB의 RAM을 할당해야 합니다. 따라서 예를 들어, 표에 설명된 서비스 중 두 개를 물리적 Docker 호스트 하나에서 함께 호스팅하려면 다음 계산을 수행합니다.

24+24+16=64GB RAM 및 8+8=16코어

최신 서버가 이러한 요구 사항을 초과하기 때문에 6개의 서비스(StorageGRID 컨테이너)를 3개의 물리적 서버에 결합합니다.

네트워킹 요구 사항

StorageGRID 트래픽의 3가지 유형은 다음과 같습니다.

- * 그리드 트래픽 (필수). * 그리드의 모든 노드 사이를 이동하는 내부 StorageGRID 트래픽입니다.
- * Admin traffic (선택 사항). * 시스템 관리 및 유지 보수에 사용되는 트래픽입니다.
- * 클라이언트 트래픽(선택 사항). * S3 및 Swift 클라이언트의 모든 오브젝트 스토리지 요청을 포함하여 외부 클라이언트 애플리케이션과 그리드 간에 이동하는 트래픽입니다.

StorageGRID 시스템에서 사용할 네트워크를 최대 3개까지 구성할 수 있습니다. 각 네트워크 유형은 겹치지 않는 별도의 서브넷에 있어야 합니다. 모든 노드가 동일한 서브넷에 있는 경우에는 게이트웨이 주소가 필요하지 않습니다.

이 평가를 위해 그리드 및 클라이언트 트래픽이 포함된 두 개의 네트워크에 배포됩니다. 나중에 관리자 네트워크를 추가하여 추가 기능을 제공할 수 있습니다.

모든 호스트의 인터페이스에 네트워크를 일관되게 매핑하는 것이 매우 중요합니다. 예를 들어, 각 노드에 ens192 및 ens224라는 두 개의 인터페이스가 있는 경우 모든 호스트의 동일한 네트워크 또는 VLAN에 모두 매핑되어야 합니다. 이

설치에서는 루프백이 컨테이너 내부의 if1이므로 설치 프로그램이 Docker 컨테이너에 eth0@if2 및 eth2@if3으로 매핑하므로 일관된 모델이 매우 중요합니다.

Docker 네트워킹에 대한 참고 사항

StorageGRID는 일부 Docker 컨테이너 구현과 다른 방식으로 네트워킹을 사용합니다. Docker(또는 Kubernetes 또는 Swarm) 제공 네트워킹을 사용하지 않습니다. 대신 StorageGRID는 실제로 컨테이너를 -net=none으로 생성하므로 Docker가 컨테이너를 네트워크에 연결하는 데 아무런 작업도 수행하지 않습니다. StorageGRID 서비스에 의해 컨테이너가 생성된 후 노드 구성 파일에 정의된 인터페이스에서 새 macvlan 디바이스가 생성됩니다. 이 장치는 새 MAC 주소를 가지며 물리적 인터페이스에서 패킷을 수신할 수 있는 별도의 네트워크 장치 역할을 합니다. 그런 다음 macvlan 디바이스가 컨테이너 네임스페이스로 이동되고 컨테이너 내부의 eth0, eth1 또는 eth2 중 하나로 이름이 변경됩니다. 이 시점에서 네트워크 장치가 더 이상 호스트 OS에 표시되지 않습니다. 이 예에서 그리드 네트워크 디바이스는 Docker 컨테이너 내부의 eth0이고 클라이언트 네트워크는 eth2입니다. 관리자 네트워크가 있는 경우 디바이스는 컨테이너에 eth1이 됩니다.

> ⓘ 컨테이너 네트워크 장치의 새 MAC 주소는 일부 네트워크 및 가상 환경에서 무차별 모드를 활성화해야 할 수 있습니다. 이 모드를 사용하면 물리적 장치가 알려진 물리적 MAC 주소와 다른 MAC 주소에 대한 패킷을 수신 및 전송할 수 있습니다. VMware vSphere에서 실행되는 경우 RHEL을 실행할 때 StorageGRID 트래픽을 처리할 포트 그룹에서 무차별 모드, MAC 주소 변경 및 위조 전송을 수락해야 합니다. Ubuntu 또는 Debian은 대부분의 상황에서 이러한 변경 없이 작동합니다. +

구축하는 것이었습니다

각 노드에는 다음 표에 나와 있는 크기의 SAN 기반 또는 로컬 디스크 디바이스가 필요합니다.

> ⓘ 표의 숫자는 전체 그리드 또는 각 물리적 호스트에 대한 숫자가 아니라 각 StorageGRID 서비스 유형에 대한 것입니다. 구축 선택 사항에 따라 이 문서의 뒷부분에 나오는 에서 각 물리적 호스트의 수를 "물리적 호스트 레이아웃 및 요구 사항"계산합니다. + 별표로 표시된 경로 또는 파일 시스템은 설치 관리자에 의해 StorageGRID 컨테이너 자체에 만들어집니다. 관리자가 수동으로 구성하거나 파일 시스템을 생성할 필요는 없지만 이러한 요구 사항을 충족하기 위해서는 호스트에 블록 디바이스가 필요합니다. 즉, 블록 디바이스는 명령을 사용하여 나타나지만 `lsblk` 호스트 OS 내에서 포맷하거나 마운트되지는 않습니다. +

노드 유형입니다	**LUN** 사용 목적	**LUN** 수입니다	**LUN**의 최소 크기입니다	수동 파일 시스템이 필요합니다	제안된 노드 구성 항목입니다
모두	관리자 노드 시스템 공간 `/var/local` (SSD가 여기에 유용함)	관리자 노드당 1개	90GB	아니요	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`
모든 노드	에서 Docker 스토리지 풀 `/var/lib/docker for container pool`	각 호스트(물리적 또는 VM)에 1개	컨테이너당 100GB	예 – etx4	NA – 호스트 파일 시스템으로 포맷 및 마운트(컨테이너에 매핑되지 않음)

노드 유형입니다	**LUN** 사용 목적	**LUN** 수입니다	**LUN**의 최소 크기입니다	수동 파일 시스템이 필요합니다	제안된 노드 구성 항목입니다
관리자	관리자 노드 감사 로그(관리자 컨테이너의 시스템 데이터) `/var/local/audit/export`	관리자 노드당 1개	200GB	아니요	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
관리자	관리자 노드 테이블(관리자 컨테이너의 시스템 데이터) `/var/local/mysql_ibdata`	관리자 노드당 1개	200GB	아니요	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
스토리지 노드	오브젝트 스토리지(블록 장치) `/var/local/rangedb0` (SSD가 여기에 유용함) `/var/local/rangedb1` `/var/local/rangedb2`	각 저장소 컨테이너마다 3개	4000GB	아니요	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

이 예에서는 컨테이너 유형별로 다음 표에 나와 있는 디스크 크기가 필요합니다. 물리적 호스트별 요구 사항은 이 문서의 뒷부분에 설명되어 "물리적 호스트 레이아웃 및 요구 사항"있습니다.

컨테이너 유형별 디스크 크기입니다

관리 컨테이너

이름	크기**(GiB)**
Docker-Store 를 참조하십시오	100(컨테이너당)
ADM-OS입니다	90
ADM - 감사	200
ADM - MySQL입니다	200

스토리지 컨테이너

이름	크기**(GiB)**
Docker-Store 를 참조하십시오	100(컨테이너당)
SN-OS입니다	90
Rangedb-0	4096

이름	크기**(GiB)**
범위-1	4096
범위 b-2	4096

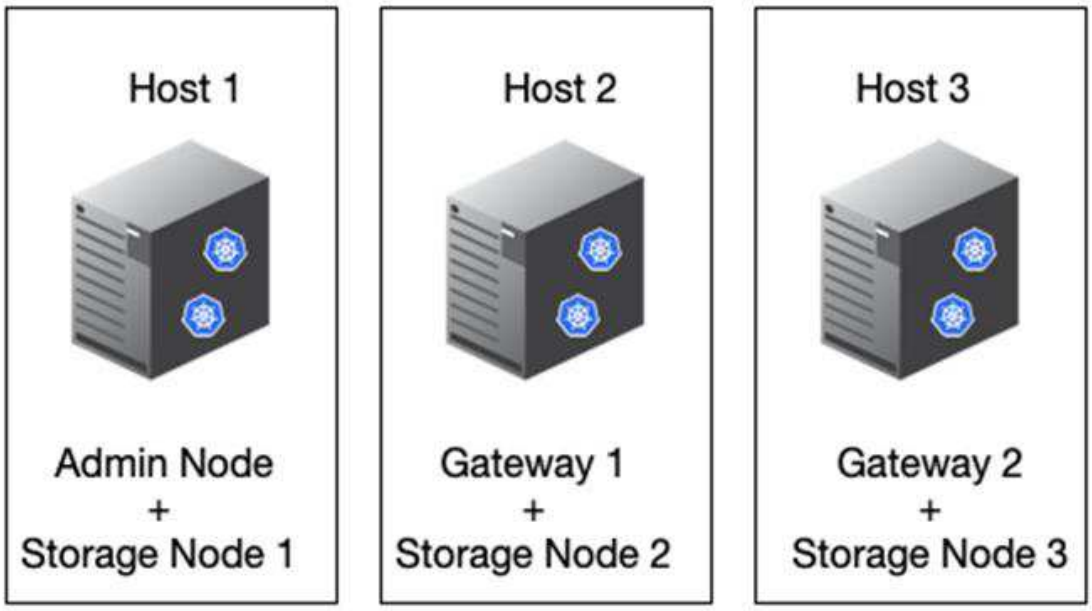
게이트웨이 컨테이너

이름	크기**(GiB)**
Docker-Store 를 참조하십시오	100(컨테이너당)
/var/local 을 선택합니다	90

물리적 호스트 레이아웃 및 요구 사항

위 표에 나와 있는 컴퓨팅 및 네트워크 요구 사항을 결합하면 16코어, 64GB RAM 및 2개의 네트워크 인터페이스를 갖춘 물리적 서버(또는 가상) 3대를 설치하는 데 필요한 기본 하드웨어 세트를 확보할 수 있습니다. 더 높은 처리량을 원할 경우 그리드 또는 클라이언트 네트워크에서 두 개 이상의 인터페이스를 연결하고 노드 구성 파일에서 bond0.520과 같은 VLAN 태그가 지정된 인터페이스를 사용할 수 있습니다. 작업 부하가 더 강할 경우 호스트와 컨테이너 모두에 더 많은 메모리가 더 적합합니다.

다음 그림과 같이 이들 서버는 호스트당 2개의 Docker 컨테이너를 호스팅합니다. RAM은 컨테이너당 24GB, 호스트 OS 자체에 16GB를 제공하여 계산합니다.



물리적 호스트(또는 VM)당 필요한 총 RAM은 24 x 2 + 16 = 64GB입니다. 다음 표에는 호스트 1, 2 및 3에 필요한 디스크 스토리지가 나와 있습니다.

호스트 **1**	크기**(GiB)**
• Docker 스토어 *	`/var/lib/docker` (파일 시스템)
200(100 x 2)	• 관리 컨테이너 *
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
• 보관 컨테이너 *	SN- `/var/local` OS(장치)
90	Rangedb-0(장치)
4096	Rangedb-1(장치)
4096	Rangedb-2(장치)

호스트 **2**	크기**(GiB)**
• Docker 스토어 *	`/var/lib/docker` (공유)
200(100 x 2)	• 게이트웨이 컨테이너 *
GW-OS입니다 *`/var/local`	100
• 보관 컨테이너 *	*`/var/local`
100	Rangedb-0
4096	범위-1
4096	범위 b-2

호스트 **3**	크기**(GiB)**
• Docker 스토어 *	`/var/lib/docker` (공유)
200(100 x 2)	• 게이트웨이 컨테이너 *
*`/var/local`	100
• 보관 컨테이너 *	*`/var/local`
100	Rangedb-0
4096	범위-1
4096	범위 b-2

Docker 저장소는 /var/local(컨테이너당)당 100GB x 2개의 컨테이너 = 200GB를 허용하여 계산되었습니다.

노드 준비

StorageGRID의 초기 설치를 준비하려면 먼저 RHEL 버전 9.2를 설치하고 SSH를 활성화하십시오. 모범 사례에 따라 네트워크 인터페이스, NTP(Network Time Protocol), DNS 및 호스트 이름을 설정합니다. 그리드 네트워크에는 적어도 하나의 활성화된 네트워크 인터페이스가 필요하고 클라이언트 네트워크에는 다른 인터페이스가 필요합니다. VLAN 태그가 지정된 인터페이스를 사용하는 경우 아래 예에 따라 구성하십시오. 그렇지 않으면 단순한 표준 네트워크 인터페이스 구성으로 충분합니다.

그리드 네트워크 인터페이스에서 VLAN 태그를 사용해야 하는 경우 구성에 다음 형식의 두 파일이 있어야 합니다 `/etc/sysconfig/network-scripts/` .

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

이 예에서는 그리드 네트워크의 물리적 네트워크 장치가 enp67s0이라고 가정합니다. Bond0과 같은 연결된 장치일 수도 있습니다. 본딩을 사용하든 표준 네트워크 인터페이스를 사용하든 네트워크 포트에 기본 VLAN이 없거나 기본 VLAN이 그리드 네트워크와 연결되어 있지 않은 경우 노드 구성 파일에서 VLAN 태그가 지정된 인터페이스를 사용해야 합니다. StorageGRID 컨테이너 자체는 이더넷 프레임의 태그를 해제하지 않으므로 상위 OS에서 처리해야 합니다.

iSCSI를 사용한 저장소 설정(옵션

iSCSI 스토리지를 사용하지 않는 경우 host1, host2 및 host3에 요구 사항을 충족하기에 충분한 크기의 블록 디바이스가 포함되어 있는지 확인해야 합니다. host1, host2 및 host3 스토리지 요구 사항은 을 "컨테이너 유형별 디스크 크기입니다" 참조하십시오.

iSCSI를 사용하여 스토리지를 설정하려면 다음 단계를 완료하십시오.

단계

1. NetApp E-Series 또는 NetApp ONTAP ® 데이터 관리 소프트웨어와 같은 외부 iSCSI 스토리지를 사용하는 경우 다음 패키지를 설치합니다.

```
sudo yum install iscsi-initiator-utils
sudo yum install device-mapper-multipath
```

2. 각 호스트에서 이니시에이터 ID를 찾습니다.

```
# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2006-04.com.example.node1
```

3. 2단계의 이니시에이터 이름을 사용하여 스토리지 디바이스의 LUN(표에 표시된 숫자 및 크기 "구축하는 것이었습니다")을 각 스토리지 노드에 매핑합니다.
4. 을 사용하여 새로 생성된 LUN을 `iscsiadm` 검색하고 로그인합니다.

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

자세한 내용은 "iSCSI 초기자 생성" Red Hat 고객 포털 을 참조하십시오.

5. 다중 경로 디바이스 및 관련 LUN WWID를 표시하려면 다음 명령을 실행합니다.

```
# multipath -ll
```

다중 경로 장치와 함께 iSCSI를 사용하지 않는 경우 장치 변경 및 재부팅이 동일하게 유지되는 고유한 경로 이름으로 장치를 마운트하기만 하면 됩니다.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

장비 이름만 사용하면 `/dev/sdx` 나중에 장비를 제거하거나 추가할 경우 문제가 발생할 수 있습니다. + 다중 경로 장치를 사용하는 경우 `/etc/multipath.conf` 다음과 같이 별칭을 사용하도록 파일을 수정합니다. +

이러한 장치는 레이아웃에 따라 일부 노드에 있을 수도 있고 없을 수도 있습니다.

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

호스트 OS에 Docker를 설치하기 전에 LUN 또는 디스크 백업을 포맷하고 마운트합니다. `/var/lib/docker` 다른 LUN은 노드 구성 파일에 정의되어 있으며, StorageGRID 컨테이너에서 직접 사용됩니다. 즉, 호스트 OS에 표시되지 않고 컨테이너 자체에 나타나며 해당 파일 시스템은 설치 관리자가 처리합니다.

iSCSI 지원 LUN을 사용하는 경우 fstab 파일에 다음 줄과 유사한 내용을 배치합니다. 참고로, 다른 LUN은 호스트 OS에 마운트할 필요가 없지만 사용 가능한 블록 디바이스로 표시되어야 합니다.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Docker 설치를 준비하는 중입니다

Docker 설치를 준비하려면 다음 단계를 완료하십시오.

단계

1. 세 호스트 모두에서 Docker 스토리지 볼륨에 파일 시스템을 생성합니다.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   다중 경로와 함께 iSCSI 장치를 사용하는 경우 를 `/dev/mapper/Docker-Store`사용합니다.

2. Docker 스토리지 볼륨 마운트 지점을 생성합니다.

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. docker-storage-volume-device에 대한 유사한 항목을 에 추가합니다 `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   다음 `_netdev` 옵션은 iSCSI 장치를 사용하는 경우에만 권장됩니다. 로컬 블록 디바이스를 사용하는 경우에는 `_netdev` 필요하지 않으며 `defaults` 사용하는 것이 좋습니다.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. 새 파일 시스템을 마운트하고 디스크 사용량을 확인합니다.

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. 스왑을 끄고 성능상의 이유로 사용하지 않도록 설정합니다.

   ```
   $ sudo swapoff --all
   ```

6. 설정을 유지하려면 /etc/fstab에서 다음과 같은 스왑 항목을 모두 제거하십시오.

```
/dev/mapper/rhel-swap swap defaults 0 0
```

스왑을 완전히 사용하지 않도록 설정하면 성능이 크게 저하될 수 있습니다.

7. 노드의 테스트 재부팅을 수행하여 `/var/lib/docker` 볼륨이 지속적이고 모든 디스크 디바이스가 반환되는지 확인합니다.

StorageGRID용 Docker를 설치합니다

StorageGRID용 Docker를 설치하는 방법을 알아보십시오.

Docker를 설치하려면 다음 단계를 완료하십시오.

단계

1. Docker용 yum repo를 구성합니다.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. 필요한 패키지를 설치합니다.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Docker를 시작합니다.

```
sudo systemctl start docker
```

4. Docker를 테스트합니다

```
sudo docker run hello-world
```

5. Docker가 시스템 시작 시 실행되는지 확인합니다.

```
sudo systemctl enable docker
```

StorageGRID에 대한 노드 구성 파일을 준비합니다

StorageGRID용 노드 구성 파일을 준비하는 방법에 대해 알아봅니다.

상위 레벨에서 노드 구성 프로세스에는 다음 단계가 포함됩니다.

단계

1. `/etc/storagegrid/nodes`모든 호스트에 디렉토리를 생성합니다.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. 컨테이너/노드 유형 레이아웃과 일치하도록 물리적 호스트별로 필요한 파일을 생성합니다. 이 예에서는 각 호스트 시스템에서 물리적 호스트당 두 개의 파일을 생성했습니다.

> 파일 이름은 설치를 위한 실제 노드 이름을 정의합니다. 예를 들어, 은 `dc1-adm1.conf` 이라는 노드가 `dc1-adm1`됩니다.

— 호스트1:
```
dc1-adm1.conf
dc1-sn1.conf
```

— 호스트2:
```
dc1-gw1.conf
dc1-sn2.conf
```

— 호스트3:
```
dc1-gw2.conf
dc1-sn3.conf
```

노드 구성 파일 준비

다음 예제에서는 `/dev/disk/by-path` 형식을 사용합니다. 다음 명령을 실행하여 올바른 경로를 확인할 수 있습니다.

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

및 이러한 명령은 다음과 같습니다.

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

기본 관리자 노드의 예

파일 이름 예:

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

파일 내용의 예:

> 디스크 경로는 아래 예를 따르거나 스타일 이름을 사용할 수 `/dev/mapper/alias` 있습니다. 같은 블록 장치 이름은 재부팅 시 변경되어 그리드에 큰 손상을 줄 수 있으므로 사용하지 `/dev/sdb` 마십시오.

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

스토리지 노드의 예

파일 이름 예:

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

파일 내용의 예:

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

게이트웨이 노드의 예

파일 이름 예:

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

파일 내용의 예:

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

StorageGRID 종속성 및 패키지를 설치합니다

StorageGRID 종속성 및 패키지를 설치하는 방법에 대해 알아봅니다.

StorageGRID 종속성 및 패키지를 설치하려면 다음 명령을 실행합니다.

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

StorageGRID 구성 파일의 유효성을 검사합니다

StorageGRID에 대한 구성 파일의 내용을 확인하는 방법에 대해 알아봅니다.

각 StorageGRID 노드에 대해 에서 구성 파일을 만든 후에는 `/etc/storagegrid/nodes` 해당 파일의 내용을 확인해야 합니다.

구성 파일의 내용을 확인하려면 각 호스트에서 다음 명령을 실행합니다.

```
sudo storagegrid node validate all
```

파일이 올바르면 출력이 각 구성 파일에 대해 Passed(통과) 로 표시됩니다.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

구성 파일이 올바르지 않으면 문제가 경고 및 오류로 표시됩니다. 구성 오류가 발견되면 설치를 계속하기 전에 오류를 수정해야 합니다.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

StorageGRID 호스트 서비스를 시작합니다

StorageGRID 호스트 서비스를 시작하는 방법에 대해 알아봅니다.

StorageGRID 노드를 시작하고 호스트를 재부팅한 후 다시 시작되도록 하려면 StorageGRID 호스트 서비스를 설정하고 시작해야 합니다.

StorageGRID 호스트 서비스를 시작하려면 다음 단계를 완료하십시오.

단계

1. 각 호스트에서 다음 명령을 실행합니다.

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

시작 프로세스는 초기 실행 시 시간이 걸릴 수 있습니다.

2. 다음 명령을 실행하여 구축이 진행되고 있는지 확인합니다.

```
sudo storagegrid node status node-name
```

3. 또는 상태를 반환하는 모든 노드에 대해 `Not-Running` `Stopped`다음 명령을 실행합니다.

```
sudo storagegrid node start node-name
```

예를 들어, 다음 출력을 고려할 때 노드를 시작할 수 `dc1-adm1` 있습니다.

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. 이전에 StorageGRID 호스트 서비스를 사용하도록 설정하고 시작한 경우(또는 서비스가 사용 및 시작되었는지 여부를 잘 모르는 경우) 다음 명령도 실행합니다.

```
sudo systemctl reload-or-restart storagegrid
```

StorageGRID에서 그리드 관리자를 구성합니다

기본 관리 노드에서 StorageGRID의 그리드 관리자를 구성하는 방법에 대해 알아봅니다.

기본 관리자 노드의 그리드 관리자 사용자 인터페이스에서 StorageGRID 시스템을 구성하여 설치를 완료합니다.

높은 수준의 단계

그리드를 구성하고 설치를 완료하려면 다음 작업이 필요합니다.

단계

1. Grid Manager(그리드 관리자)로 이동합니다
2. "StorageGRID 라이센스 정보를 지정합니다"
3. "StorageGRID에 사이트를 추가합니다"
4. "그리드 네트워크 서브넷을 지정합니다"
5. "보류 중인 그리드 노드를 승인합니다"
6. "NTP 서버 정보를 지정합니다"
7. "도메인 이름 시스템 서버 정보를 지정합니다"
8. "StorageGRID 시스템 암호를 지정합니다"
9. "구성을 검토하고 설치를 완료합니다"

Grid Manager(그리드 관리자**)**로 이동합니다

그리드 관리자를 사용하여 StorageGRID 시스템을 구성하는 데 필요한 모든 정보를 정의합니다.

시작하기 전에 기본 관리자 노드를 구축하고 초기 시작 순서를 완료해야 합니다.

그리드 관리자를 사용하여 정보를 정의하려면 다음 단계를 완료하십시오.

단계

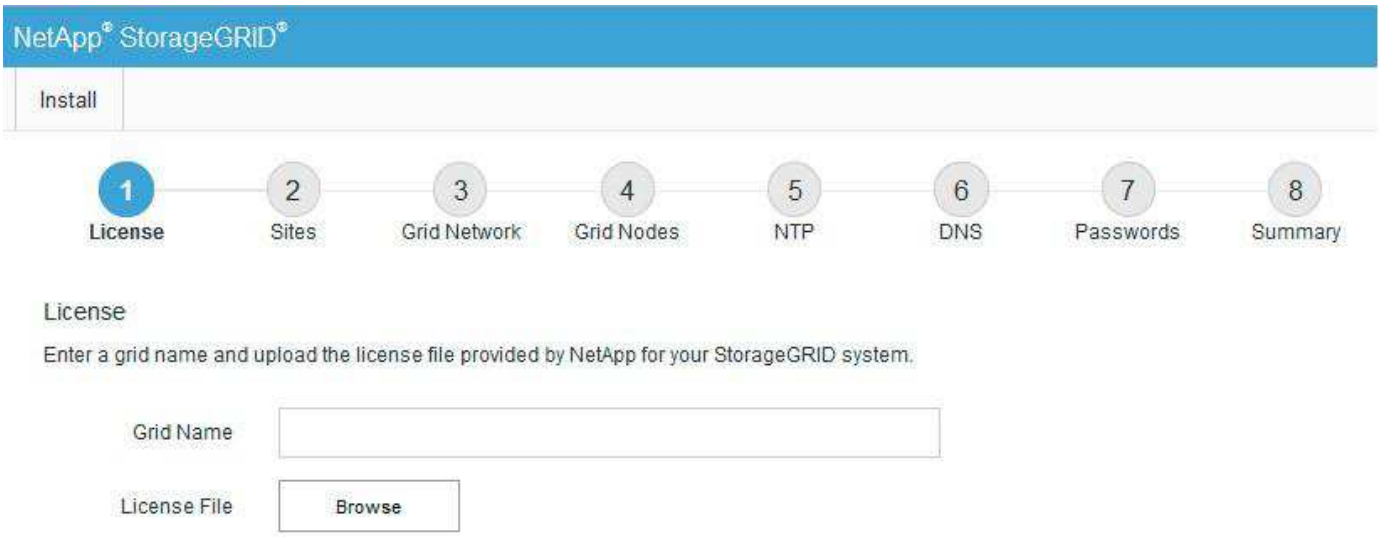
1. 다음 주소에서 Grid Manager에 액세스합니다.

   ```
   https://primary_admin_node_grid_ip
   ```

   또는 포트 8443에서 Grid Manager에 액세스할 수 있습니다.

   ```
   https://primary_admin_node_ip:8443
   ```

2. StorageGRID 시스템 설치 를 클릭합니다. StorageGRID 그리드를 구성하는 데 사용되는 페이지가 표시됩니다.



StorageGRID 라이센스 세부 정보를 추가합니다

StorageGRID 라이센스 파일을 업로드하는 방법에 대해 알아봅니다.

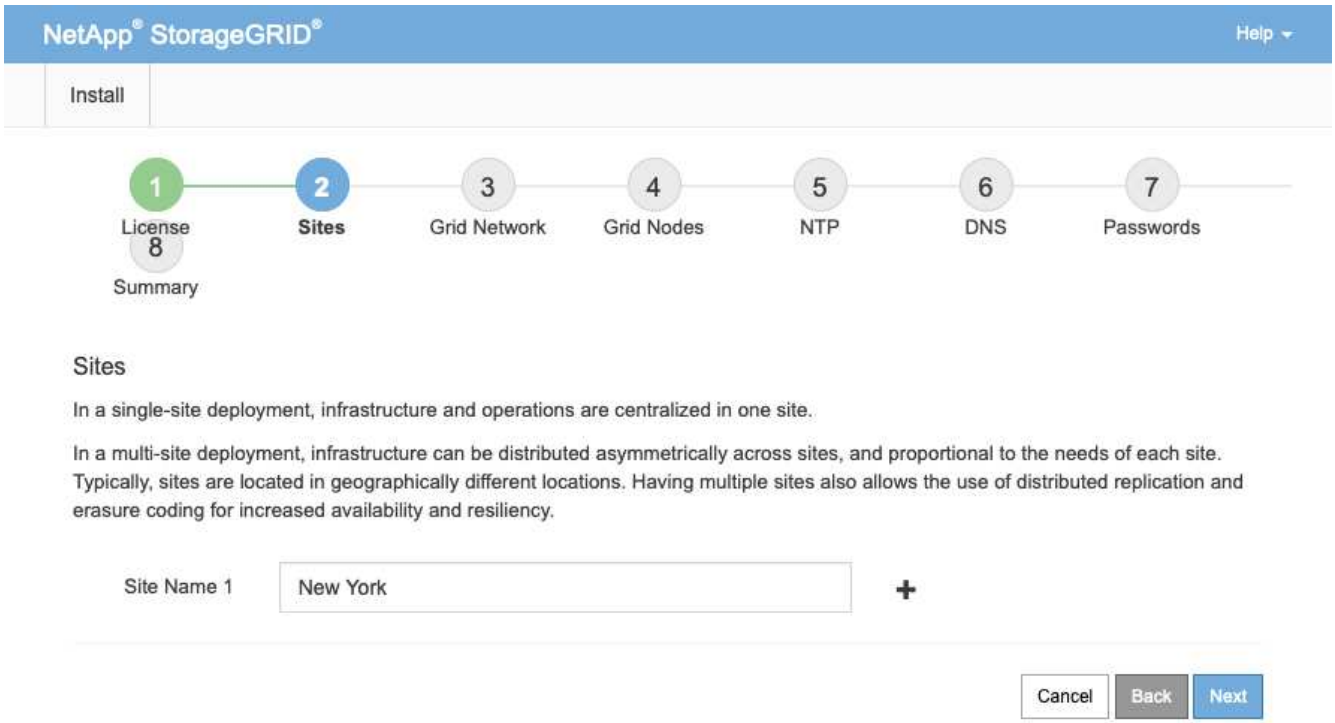
StorageGRID 시스템의 이름을 지정하고 NetApp에서 제공하는 라이센스 파일을 업로드해야 합니다.

StorageGRID 라이센스 정보를 지정하려면 다음 단계를 완료합니다.

단계

1. 라이센스 페이지의 그리드 이름 필드에 StorageGRID 시스템의 이름을 입력합니다. 설치 후 이름이 그리드 토폴로지 트리에서 최상위 수준으로 표시됩니다.
2. 찾아보기 를 클릭하고 NetApp 사용권 파일을 찾은 (`NLF-*unique-id*.txt`다음 열기 를 클릭합니다. 라이센스 파일의 유효성이 검사되고 일련 번호와 라이센스가 있는 스토리지 용량이 표시됩니다.

> StorageGRID 설치 아카이브에는 제품에 대한 지원 권한이 없는 무료 라이센스가 포함되어 있습니다. 설치 후 지원을 제공하는 라이센스로 업데이트할 수 있습니다.



3. 다음 을 클릭합니다.

StorageGRID에 사이트를 추가합니다

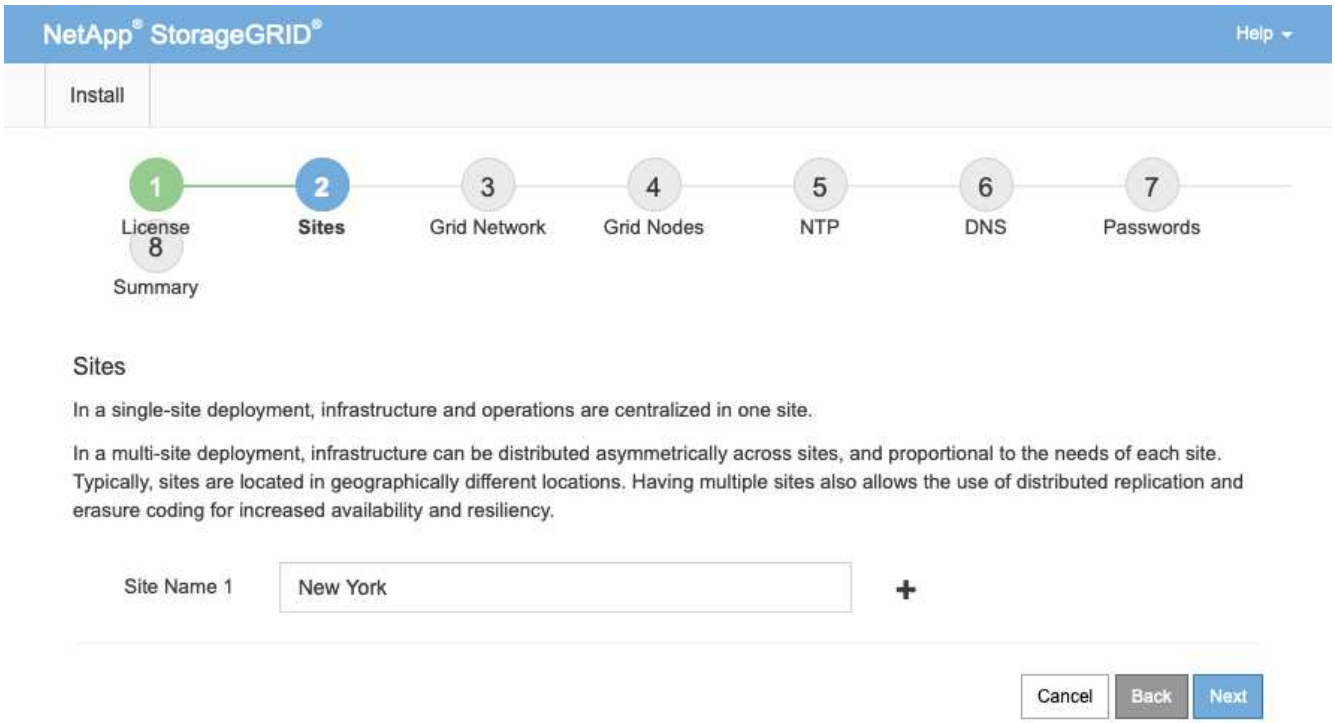
StorageGRID에 사이트를 추가하여 안정성과 스토리지 용량을 높이는 방법에 대해 알아보십시오.

StorageGRID를 설치할 때는 사이트를 하나 이상 만들어야 합니다. StorageGRID 시스템의 안정성과 스토리지 용량을 늘리기 위해 사이트를 추가로 생성할 수 있습니다.

사이트를 추가하려면 다음 단계를 완료합니다.

단계

1. 사이트 페이지에서 사이트 이름을 입력합니다.
2. 사이트를 추가하려면 마지막 사이트 항목 옆에 있는 더하기 기호를 클릭하고 새 사이트 이름 텍스트 상자에 이름을 입력합니다. 그리드 토폴로지에 필요한 만큼 사이트를 추가합니다. 최대 16개의 사이트를 추가할 수 있습니다.



3. 다음 을 클릭합니다.

StorageGRID에 대한 그리드 네트워크 서브넷을 지정합니다

StorageGRID에 대한 그리드 네트워크 서브넷을 구성하는 방법에 대해 알아봅니다.

그리드 네트워크에서 사용되는 서브넷을 지정해야 합니다.

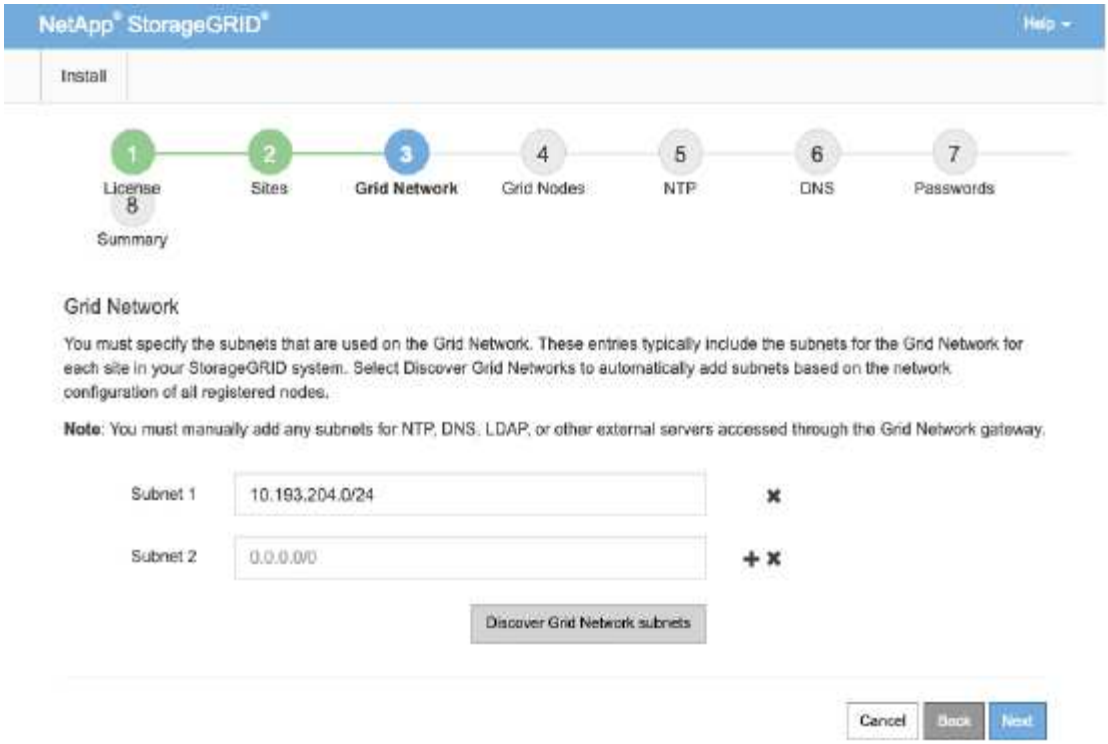
서브넷 항목에는 그리드 네트워크를 통해 연결할 수 있어야 하는 서브넷(예: NTP 서버를 호스팅하는 서브넷)과 더불어 StorageGRID 시스템의 각 사이트에 대한 그리드 네트워크의 서브넷이 포함됩니다.

여러 그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다.

그리드 네트워크 서브넷을 지정하려면 다음 단계를 완료합니다.

단계

1. 서브넷 1 텍스트 상자에서 하나 이상의 그리드 네트워크에 대한 CIDR 네트워크 주소를 지정합니다.
2. 마지막 항목 옆에 있는 더하기 기호를 클릭하여 추가 네트워크 항목을 추가합니다. 노드를 이미 하나 이상 배포한 경우 그리드 네트워크 서브넷 검색 을 클릭하여 그리드 네트워크 서브넷 목록을 그리드 관리자에 등록된 그리드 노드에서 보고하는 서브넷으로 자동으로 채웁니다.



3. 다음 을 클릭합니다.

StorageGRID에 대한 그리드 노드를 승인합니다

StorageGRID 시스템에 연결된 보류 중인 그리드 노드를 검토하고 승인하는 방법에 대해 알아봅니다.

각 그리드 노드가 StorageGRID 시스템에 합류하기 전에 승인해야 합니다.

시작하기 전에 모든 가상 및 StorageGRID 어플라이언스 그리드 노드를 구축해야 합니다.

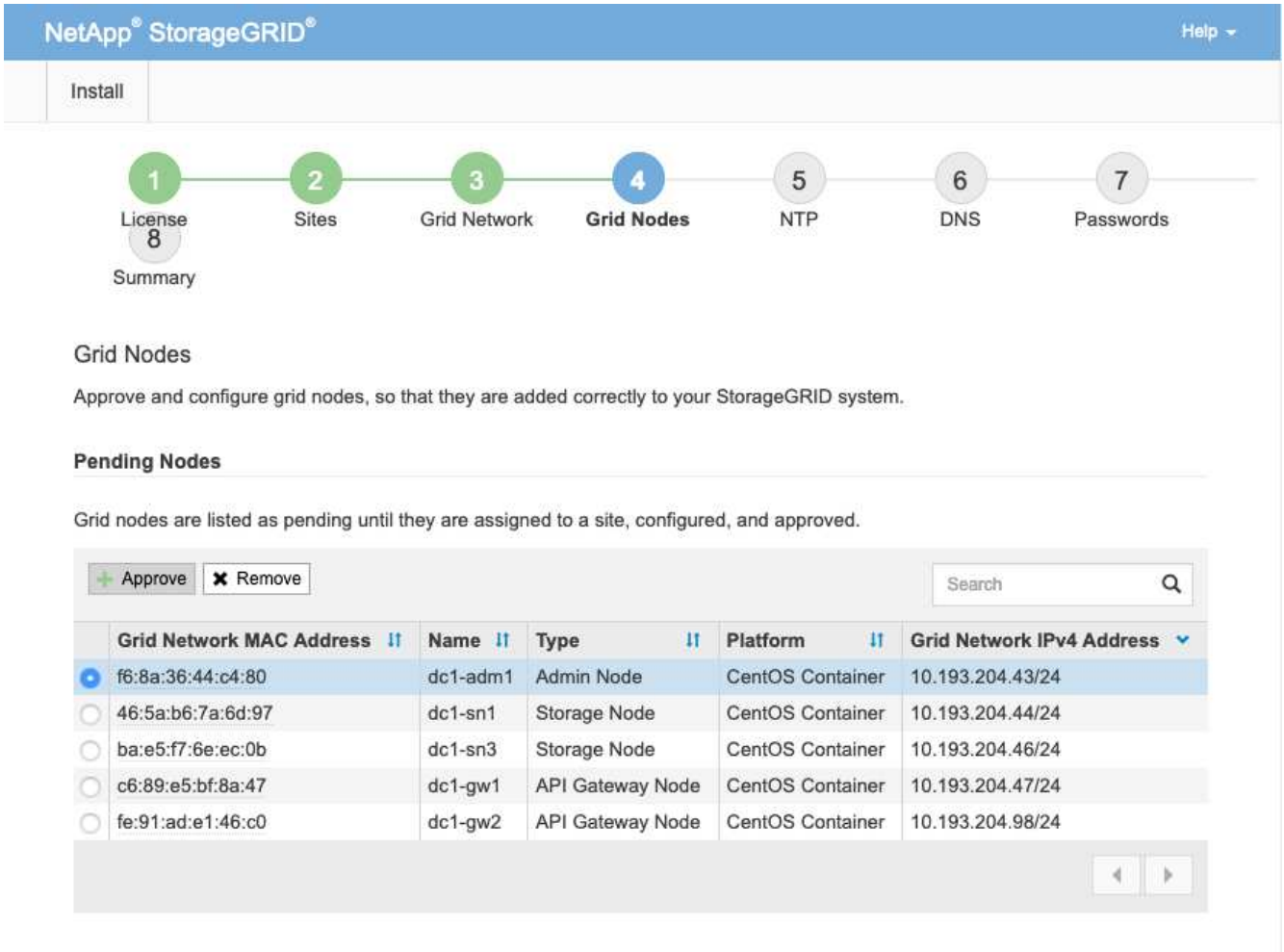
보류 중인 그리드 노드를 승인하려면 다음 단계를 수행하십시오.

단계

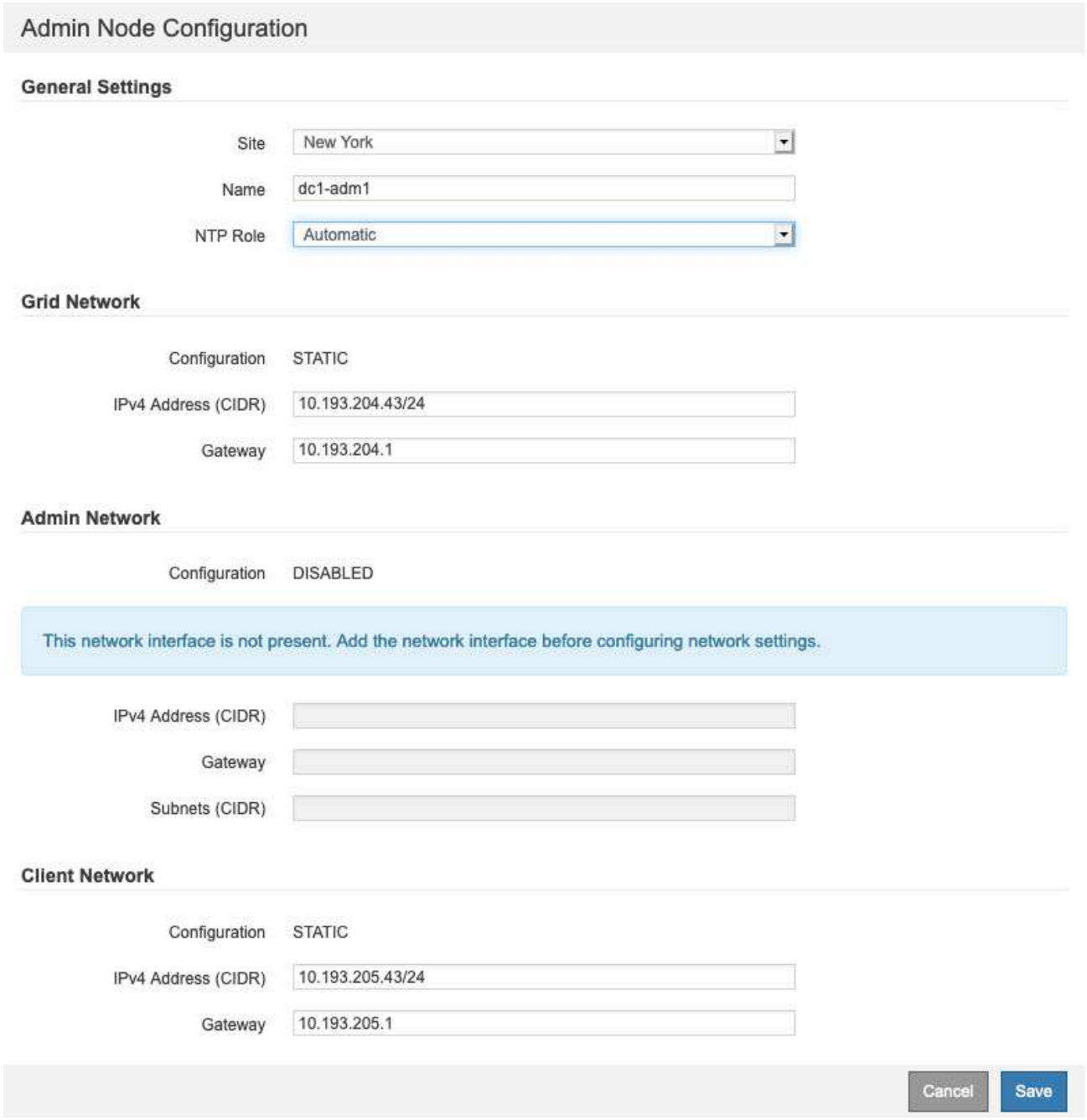
1. Pending Nodes 목록을 검토하고 배포된 모든 그리드 노드가 표시되는지 확인합니다.

   그리드 노드가 누락된 경우 성공적으로 배포되었는지 확인합니다.

2. 승인할 보류 중인 노드 옆에 있는 라디오 단추를 클릭합니다.



3. 승인을 클릭합니다.
4. 일반 설정에서 필요에 따라 다음 속성의 설정을 수정합니다.



--* Site*: 이 그리드 노드에 대한 사이트의 시스템 이름입니다.

—* Name *: 노드에 할당될 호스트 이름 및 Grid Manager에 표시될 이름입니다. 이름은 노드 배포 중에 지정한 이름의 기본값으로 사용되지만 필요에 따라 변경할 수 있습니다.

—* NTP 역할 *: 그리드 노드의 NTP 역할입니다. 옵션은 자동, 기본 및 클라이언트입니다. 자동 옵션을 선택하면 관리 노드, 관리 도메인 컨트롤러(ADC) 서비스가 있는 스토리지 노드, 게이트웨이 노드 및 비정적 IP 주소가 있는 모든 그리드 노드에 기본 역할이 할당됩니다. 다른 모든 그리드 노드는 클라이언트 역할이 할당됩니다.

각 사이트에서 최소 2개의 노드가 4개 이상의 외부 NTP 소스에 액세스할 수 있는지 확인합니다. 사이트에서 하나의 노드만 NTP 소스에 연결할 수 있는 경우 해당 노드가 중단되면 타이밍 문제가 발생합니다. 또한 사이트당 두 노드를 기본 NTP 소스로 지정하면 사이트가 나머지 그리드에서 격리될 경우 정확한 시간을 보장할 수 있습니다.

--* ADC 서비스(스토리지 노드만 해당)*: 자동 을 선택하여 시스템에서 노드에 ADC 서비스가 필요한지 여부를 결정하도록 합니다. ADC 서비스는 그리드 서비스의 위치 및 가용성을 추적합니다. 각 사이트에 최소 3개의 저장소 노드가 ADC 서비스를 포함해야 합니다. ADC 서비스를 배포한 후에는 노드에 추가할 수 없습니다.

5. 그리드 네트워크에서 필요에 따라 다음 속성의 설정을 수정합니다.

   --* IPv4 주소(CIDR)*: 그리드 네트워크 인터페이스의 CIDR 네트워크 주소(컨테이너 내부의 eth0). `192.168.1.234/24`예를 들어,

   --* 게이트웨이*: 그리드 네트워크 게이트웨이. `192.168.0.1`예를 들어,

   > ⓘ 그리드 서브넷이 여러 개 있는 경우 게이트웨이가 필요합니다.

   > ⓘ 그리드 네트워크 구성을 위해 DHCP를 선택하고 여기서 값을 변경하면 새로운 값이 노드에서 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀에 있지 않은지 확인합니다.

6. 그리드 노드에 대한 관리 네트워크를 구성하려면 필요에 따라 관리 네트워크 섹션에서 설정을 추가하거나 업데이트합니다.

   서브넷(CIDR) 텍스트 상자에 이 인터페이스의 경로 대상 서브넷을 입력합니다. 여러 개의 관리자 서브넷이 있는 경우 관리자 게이트웨이가 필요합니다.

   > ⓘ 관리자 네트워크 구성을 위해 DHCP를 선택하고 여기서 값을 변경하면 새로운 값이 노드에서 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀에 있지 않은지 확인합니다.

   - 어플라이언스 *: StorageGRID 어플라이언스의 경우 StorageGRID 어플라이언스 설치 프로그램을 사용하여 초기 설치 중에 관리자 네트워크가 구성되지 않은 경우 이 그리드 관리자 대화 상자에서 구성할 수 없습니다. 대신 다음 단계를 수행해야 합니다.

     a. 어플라이언스를 재부팅합니다. 어플라이언스 설치 프로그램에서 **Advanced › reboot** 를 선택합니다. 재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

     b. 네트워킹 구성 [링크 구성] 메뉴를 선택하고 해당 네트워크를 활성화합니다.

     c. 메뉴: Configure Networking [IP Configuration](네트워킹 구성 [IP 구성])을 선택하고 활성화된 네트워크를 구성합니다.

     d. 홈 페이지로 돌아가서 설치 시작 을 클릭합니다.

     e. Grid Manager(그리드 관리자)에서 노드가 Approved Nodes(승인 노드) 테이블에 나열되면 노드를 재설정합니다.

     f. Pending Nodes 테이블에서 노드를 제거합니다.

     g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

     h. 적절한 네트워크를 구성할 수 있는지 확인합니다. IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다. 자세한 내용은 해당 어플라이언스 모델의 설치 및 유지 관리 지침을 참조하십시오.

7. 그리드 노드에 대한 클라이언트 네트워크를 구성하려면 클라이언트 네트워크 섹션에서 필요에 따라 설정을 추가하거나 업데이트합니다. 클라이언트 네트워크가 구성된 경우 게이트웨이가 필요하며 설치 후 해당 게이트웨이가 노드의 기본 게이트웨이가 됩니다.

   - 어플라이언스 *: StorageGRID 어플라이언스의 경우 StorageGRID 어플라이언스 설치 프로그램을 사용하여 초기 설치 중에 클라이언트 네트워크가 구성되지 않은 경우 이 그리드 관리자 대화 상자에서 구성할 수 없습니다. 대신 다음 단계를 수행해야 합니다.

a. 어플라이언스를 재부팅합니다. 어플라이언스 설치 프로그램에서 **Advanced › reboot** 를 선택합니다. 재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

b. 네트워킹 구성 [링크 구성] 메뉴를 선택하고 해당 네트워크를 활성화합니다.

c. 메뉴: Configure Networking [IP Configuration](네트워킹 구성 [IP 구성])을 선택하고 활성화된 네트워크를 구성합니다.

d. 홈 페이지로 돌아가서 설치 시작 을 클릭합니다.

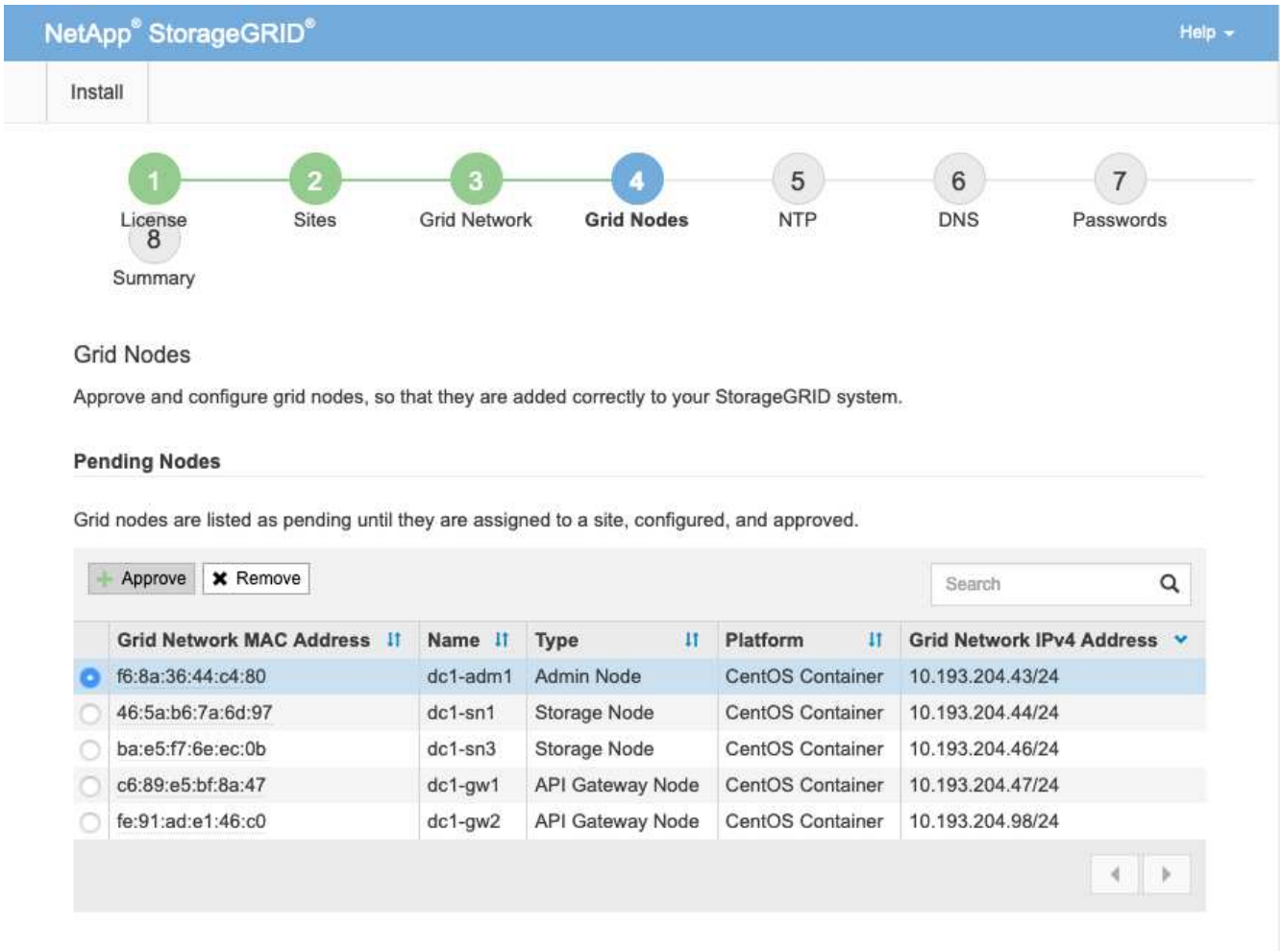
e. Grid Manager(그리드 관리자)에서 노드가 Approved Nodes(승인 노드) 테이블에 나열되면 노드를 재설정합니다.

f. Pending Nodes 테이블에서 노드를 제거합니다.

g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

h. 적절한 네트워크를 구성할 수 있는지 확인합니다. IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

8. 저장 을 클릭합니다. 그리드 노드 항목이 승인된 노드 목록으로 이동합니다.



9. 승인할 각 보류 중인 그리드 노드에 대해 1-8단계를 반복합니다.

   그리드에서 원하는 모든 노드를 승인해야 합니다. 그러나 요약 페이지에서 설치를 클릭하기 전에 언제든지 이 페이지로 돌아갈 수 있습니다. 승인된 그리드 노드의 속성을 수정하려면 해당 라디오 단추를 클릭한 다음 편집을 클릭합니다.

10. 그리드 노드 승인이 완료되면 다음 을 클릭합니다.

StorageGRID에 대한 NTP 서버 세부 정보를 지정합니다

별도의 서버에서 수행되는 작업을 동기화 상태로 유지할 수 있도록 StorageGRID 시스템의 NTP 구성 정보를 지정하는 방법에 대해 알아봅니다.

시간 변동 문제를 방지하려면 Stratum 3 이상의 외부 NTP 서버 참조 4개를 지정해야 합니다.

> 프로덕션 수준 StorageGRID 설치에 외부 NTP 소스를 지정할 때 Windows Server 2016 이전 버전의 Windows에서는 Windows 시간(W32Time) 서비스를 사용하지 마십시오. 이전 버전의 Windows에서 사용한 시간 서비스는 충분히 정확하지 않으며 StorageGRID와 같은 까다로운 환경에서 사용할 수 있도록 Microsoft에서 지원하지 않습니다.

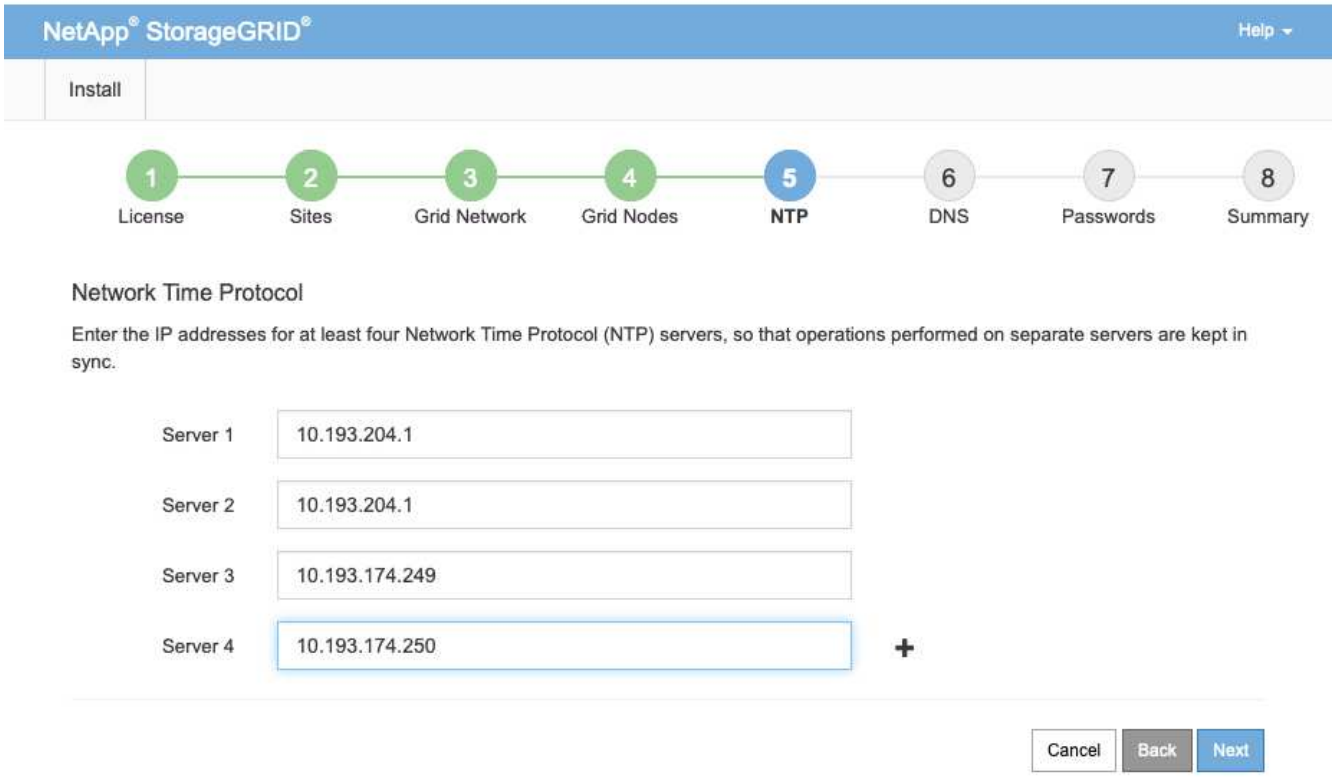
외부 NTP 서버는 이전에 기본 NTP 역할을 할당한 노드에서 사용됩니다.

> 클라이언트 네트워크가 NTP 서버의 유일한 소스가 될 수 있을 만큼 설치 프로세스 초기에 활성화되지 않았습니다. 그리드 네트워크 또는 관리 네트워크를 통해 NTP 서버를 하나 이상 연결할 수 있는지 확인합니다.

NTP 서버 정보를 지정하려면 다음 단계를 완료하십시오.

단계

1. 서버 1 - 서버 4 텍스트 상자에 4개 이상의 NTP 서버에 대한 IP 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 클릭하여 더 많은 서버 항목을 추가합니다.



3. 다음 을 클릭합니다.

StorageGRID에 대한 DNS 서버 세부 정보를 지정합니다

StorageGRID용 DNS 서버를 구성하는 방법에 대해 알아봅니다.

IP 주소 대신 호스트 이름을 사용하여 외부 서버에 액세스할 수 있도록 StorageGRID 시스템의 DNS 정보를 지정해야 합니다.

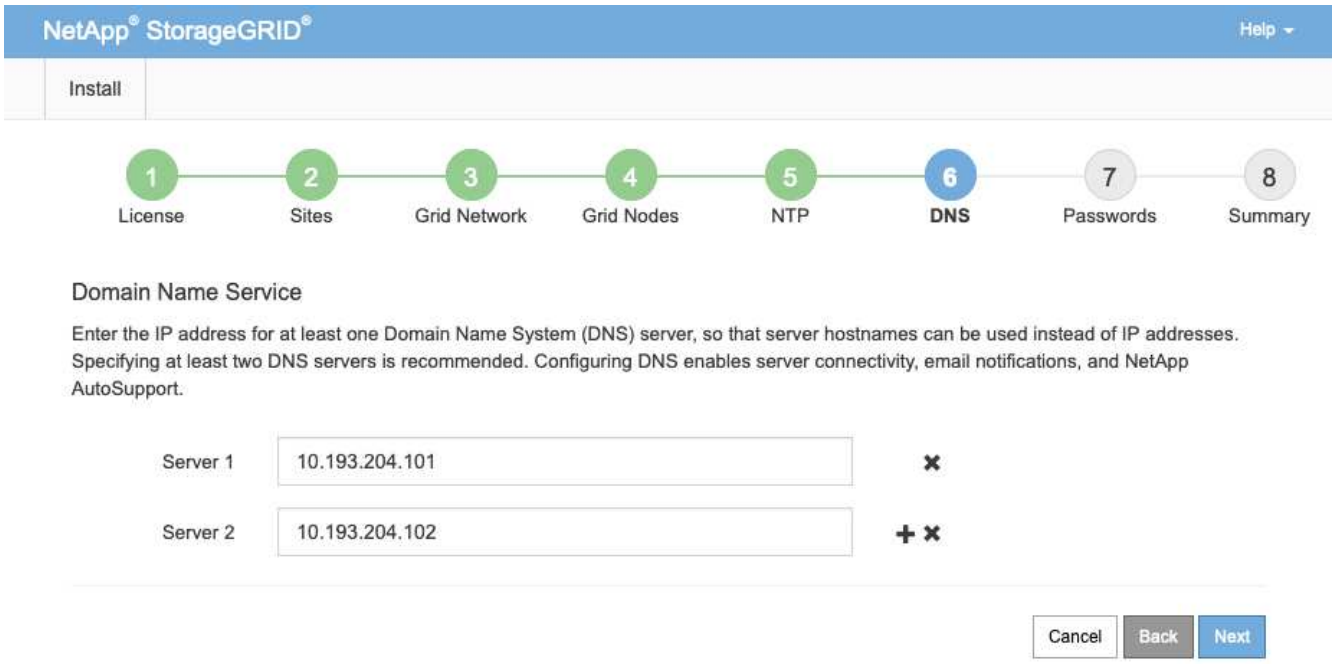
DNS 서버 정보를 지정하면 이메일 알림 및 NetApp AutoSupport ® 메시지에 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다. NetApp에서는 DNS 서버를 두 개 이상 지정할 것을 권장합니다.

네트워크 연결 시 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 선택해야 합니다.

DNS 서버 정보를 지정하려면 다음 단계를 완료하십시오.

단계

1. 서버 1 텍스트 상자에서 DNS 서버의 IP 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 클릭하여 서버를 더 추가합니다.



3. 다음 을 클릭합니다.

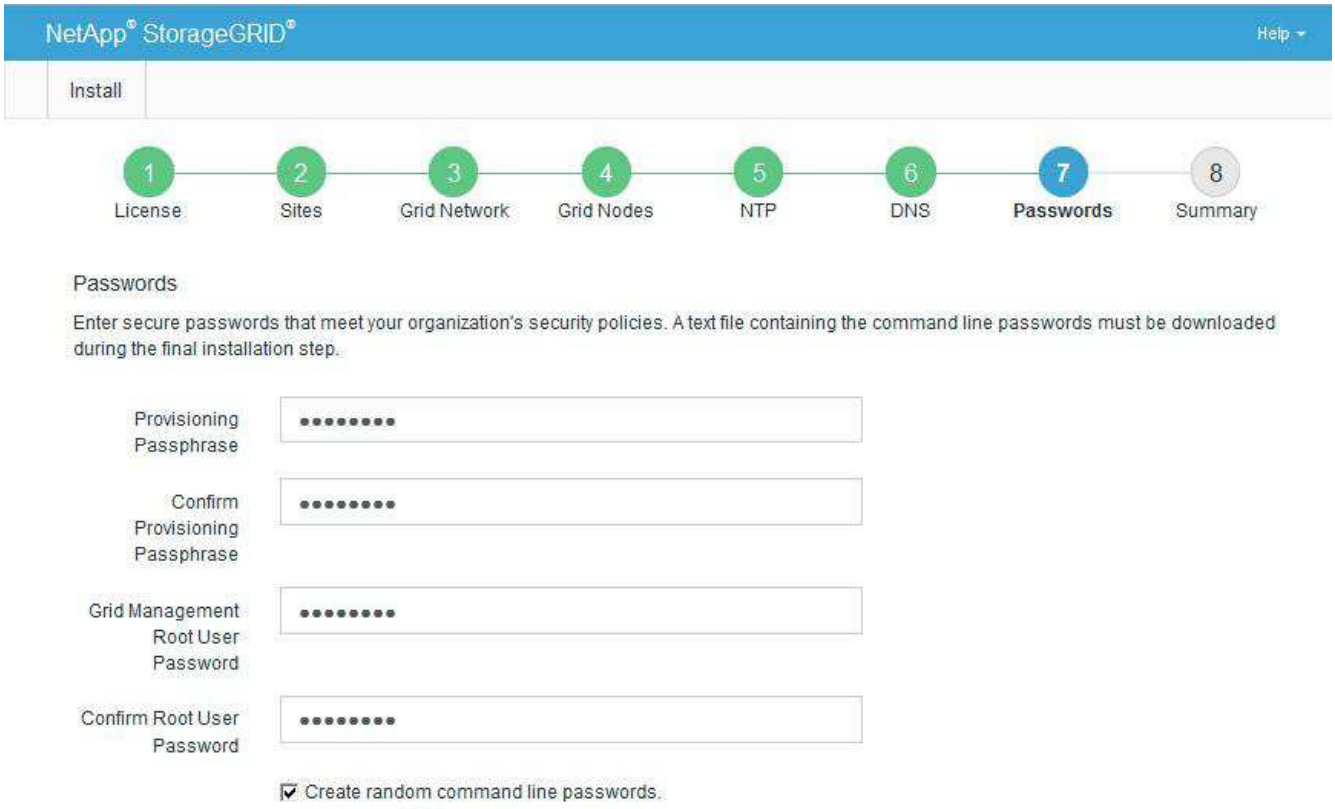
StorageGRID에 대한 시스템 암호를 지정합니다

프로비저닝 암호 및 그리드 관리 루트 사용자 암호를 설정하여 StorageGRID 시스템을 보호하는 방법에 대해 알아봅니다.

StorageGRID 시스템을 보호하는 데 사용할 암호를 입력하려면 다음 단계를 수행하십시오.

단계

1. Provisioning Passphrase에 StorageGRID 시스템의 그리드 토폴로지를 변경하는 데 필요한 프로비저닝 암호를 입력합니다. 이 암호는 안전한 곳에 기록해야 합니다.
2. Provisioning Passphrase 확인 에 Provisioning 암호를 다시 입력합니다.
3. Grid Management Root User Password(그리드 관리 루트 사용자 암호)에서 그리드 관리자에 루트 사용자로 액세스하는 데 사용할 암호를 입력합니다.
4. Confirm Root User Password(루트 사용자 암호 확인)에 Grid Manager 암호를 다시 입력합니다.



5. 개념 증명 또는 데모 목적으로 그리드를 설치하는 경우 무작위 명령줄 암호 만들기 옵션을 선택 취소합니다.

   프로덕션 배포의 경우 보안을 위해 항상 무작위 암호를 사용해야 합니다. 루트 또는 관리자 계정을 사용하여 명령줄에서 그리드 노드에 액세스하기 위해 기본 암호를 사용하려면 데모 그리드에 대해서만 무작위 명령줄 암호 만들기 옵션을 선택 취소합니다.

   > 요약 페이지에서 설치를 클릭하면 복구 패키지 파일을 다운로드하라는 메시지가 (`sgws-recovery-packageid-revision.zip`표시됩니다.) 설치를 완료하려면 이 파일을 다운로드해야 합니다. 시스템에 액세스하기 위한 암호는 `Passwords.txt` 복구 패키지 파일에 포함된 파일에 저장됩니다.

6. 다음 을 클릭합니다.

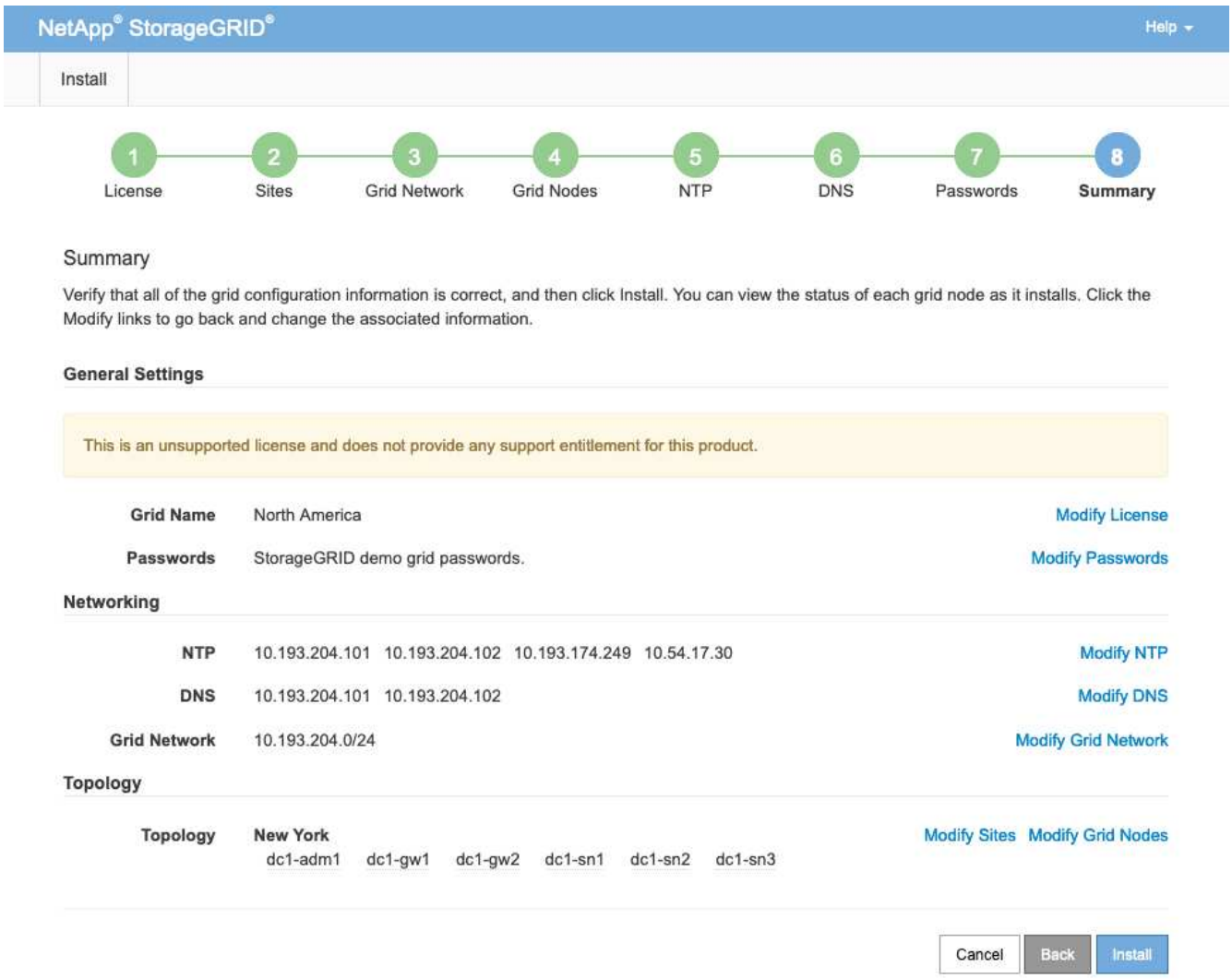
구성을 검토하고 **StorageGRID** 설치를 완료합니다

그리드 구성 정보를 검증하고 StorageGRID 설치 프로세스를 완료하는 방법에 대해 알아봅니다.

설치가 성공적으로 완료되도록 하려면 입력한 구성 정보를 주의 깊게 검토하십시오. 다음 단계를 수행합니다.

단계

1. 요약 페이지를 봅니다.



2. 모든 그리드 구성 정보가 올바른지 확인합니다. 뒤로 돌아가 오류를 수정하려면 요약 페이지의 수정 링크를 사용합니다.
3. 설치 를 클릭합니다.

> 노드가 클라이언트 네트워크를 사용하도록 구성된 경우 설치 를 클릭하면 해당 노드의 기본 게이트웨이가 그리드 네트워크에서 클라이언트 네트워크로 전환됩니다. 연결이 끊긴 경우 액세스 가능한 서브넷을 통해 기본 관리자 노드에 액세스하고 있는지 확인합니다. 자세한 내용은 "네트워크 설치 및 구축"을 참조하십시오.

4. 복구 패키지 다운로드 를 클릭합니다.

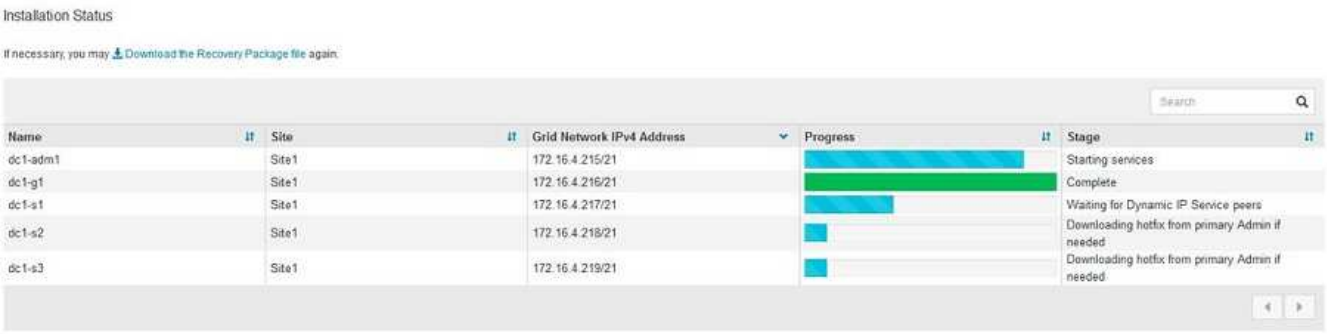
   그리드 토폴로지가 정의된 지점으로 설치가 진행되면 복구 패키지 파일을 다운로드하라는 메시지가 (`.zip`표시됩니다.) 이 파일의 내용에 액세스할 수 있는지 확인합니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 다운로드해야 합니다.

   파일의 내용을 추출한 다음 안전하고 별도의 두 위치에 저장할 수 있는지 확인합니다 `.zip` .

복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

5. I have successfully download and Verified the Recovery Package File 옵션을 선택하고 Next를 클릭합니다.

설치가 여전히 진행 중인 경우 설치 상태 페이지가 열립니다. 이 페이지에는 각 그리드 노드의 설치 진행률이 표시됩니다.



모든 그리드 노드의 전체 단계에 도달하면 그리드 관리자의 로그인 페이지가 열립니다.

6. 설치 중에 지정한 암호를 사용하여 루트 사용자로 Grid Manager에 로그인합니다.

StorageGRID에서 베어 메탈 노드를 업그레이드합니다

StorageGRID의 베어 메탈 노드의 업그레이드 프로세스에 대해 알아보십시오.

베어 메탈 노드의 업그레이드 프로세스는 어플라이언스 또는 VMware 노드의 업그레이드 프로세스와 다릅니다. 베어 메탈 노드의 업그레이드를 수행하기 전에 먼저 GUI를 통해 업그레이드를 실행하기 전에 모든 호스트에서 RPM 파일을 업그레이드해야 합니다.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

이제 GUI를 통해 소프트웨어 업그레이드를 진행할 수 있습니다.

TR-4907: Veritas Enterprise Vault로 StorageGRID를 구성합니다

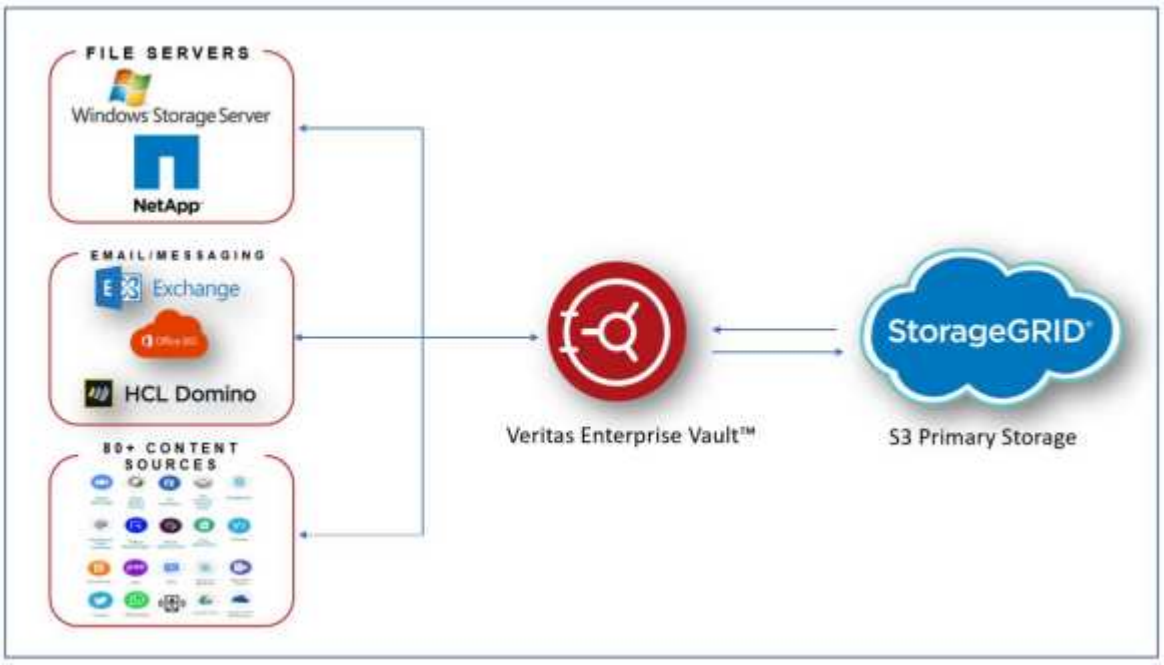
사이트 페일오버를 위한 **StorageGRID** 구성 소개

Veritas Enterprise Vault에서 StorageGRID를 재해 복구를 위한 운영 스토리지 타겟으로 사용하는 방법에 대해 알아보십시오.

이 구성 가이드에서는 NetApp ® StorageGRID ® 를 Veritas Enterprise Vault를 사용하는 운영 스토리지 타겟으로 구성하는 단계를 제공합니다. 또한 DR(재해 복구) 시나리오에서 사이트 페일오버를 위해 StorageGRID를 구성하는 방법에 대해 설명합니다.

명확히 설명하십시오

StorageGRID는 Veritas Enterprise Vault를 위한 사내 S3 호환 클라우드 백업 타겟을 제공합니다. 다음 그림에서는 Veritas Enterprise Vault 및 StorageGRID 아키텍처를 보여 줍니다.



추가 정보를 찾을 수 있는 위치

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

- NetApp StorageGRID 문서 센터 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 지원 https://docs.netapp.com/us-en/storagegrid-enable/

- NetApp 제품 설명서 https://www.netapp.com/support-and-training/documentation/

StorageGRID 및 Veritas Enterprise Vault를 구성합니다

StorageGRID 11.5 이상 및 Veritas Enterprise Vault 14.1 이상에 대한 기본 구성을 구현하는 방법에 대해 알아봅니다.

이 구성 가이드는 StorageGRID 11.5 및 Enterprise Vault 14.1을 기반으로 합니다. 한 번 쓰기의 경우 S3 오브젝트 잠금, StorageGRID 11.6 및 Enterprise Vault 14.2.2를 사용하는 WORM(Read Many) 모드 스토리지가 사용되었습니다. 이 지침에 대한 자세한 내용은 "StorageGRID 설명서" 페이지를 참조하거나 StorageGRID 전문가에게 문의하십시오.

StorageGRID 및 Veritas Enterprise Vault를 구성하기 위한 필수 구성 요소

- Veritas Enterprise Vault를 사용하여 StorageGRID를 구성하기 전에 다음 사전 요구 사항을 확인하십시오.

> WORM 스토리지(오브젝트 잠금)의 경우 StorageGRID 11.6 이상이 필요합니다.

- Veritas Enterprise Vault 14.1 이상이 설치되어 있습니다.

> WORM 스토리지(Object Lock)의 경우 Enterprise Vault 버전 14.2.2 이상이 필요합니다.

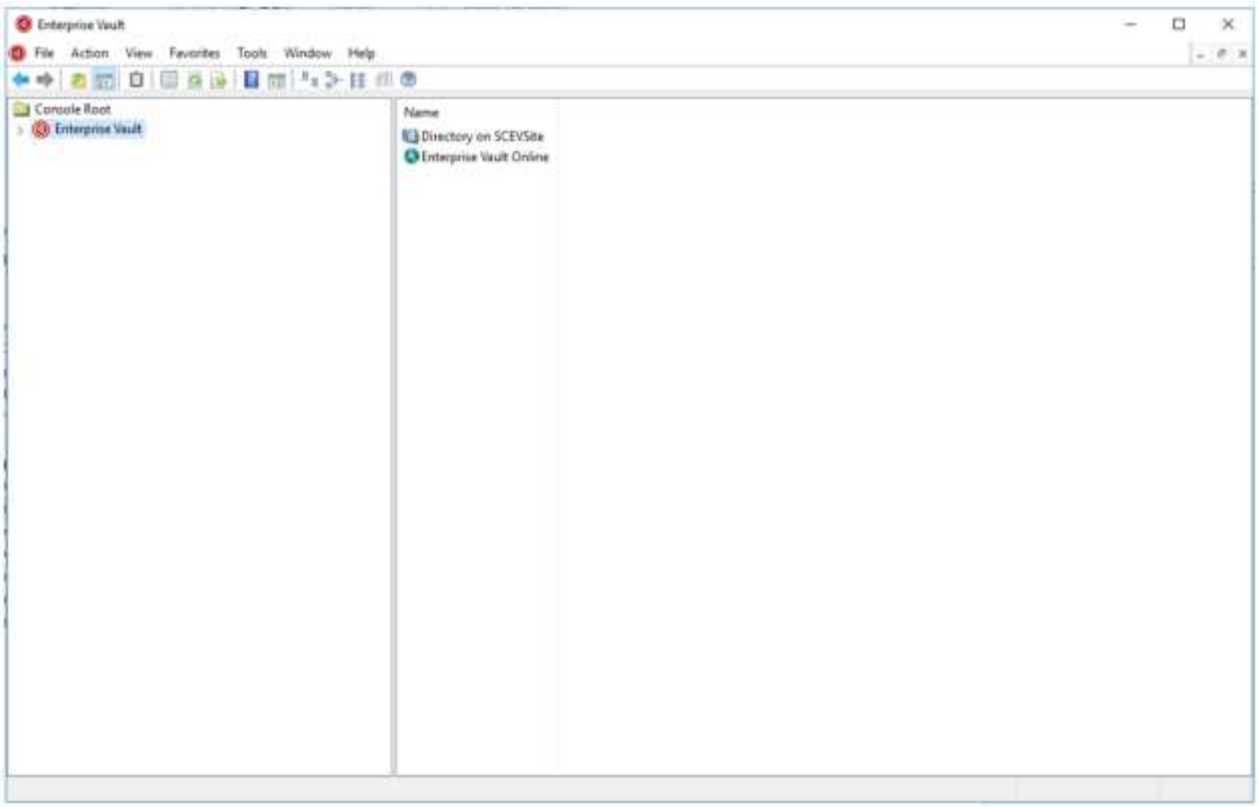
- 볼트 저장소 그룹과 볼트 저장소가 생성되었습니다. 자세한 내용은 Veritas Enterprise Vault 관리 가이드 를 참조하십시오.
- StorageGRID 테넌트, 액세스 키, 비밀 키 및 버킷이 생성되었습니다.
- StorageGRID 로드 밸런서 끝점이 생성되었습니다(HTTP 또는 HTTPS).
- 자체 서명된 인증서를 사용하는 경우 StorageGRID 자체 서명된 CA 인증서를 Enterprise Vault Server에 추가합니다. 자세한 내용은 여기를 참조하십시오 "Veritas 기술 자료 문서".
- 최신 Enterprise Vault 구성 파일을 업데이트하고 적용하여 NetApp StorageGRID와 같은 지원되는 스토리지 솔루션을 활성화합니다. 자세한 내용은 여기를 참조하십시오 "Veritas 기술 자료 문서".

Veritas Enterprise Vault를 사용하여 StorageGRID를 구성합니다

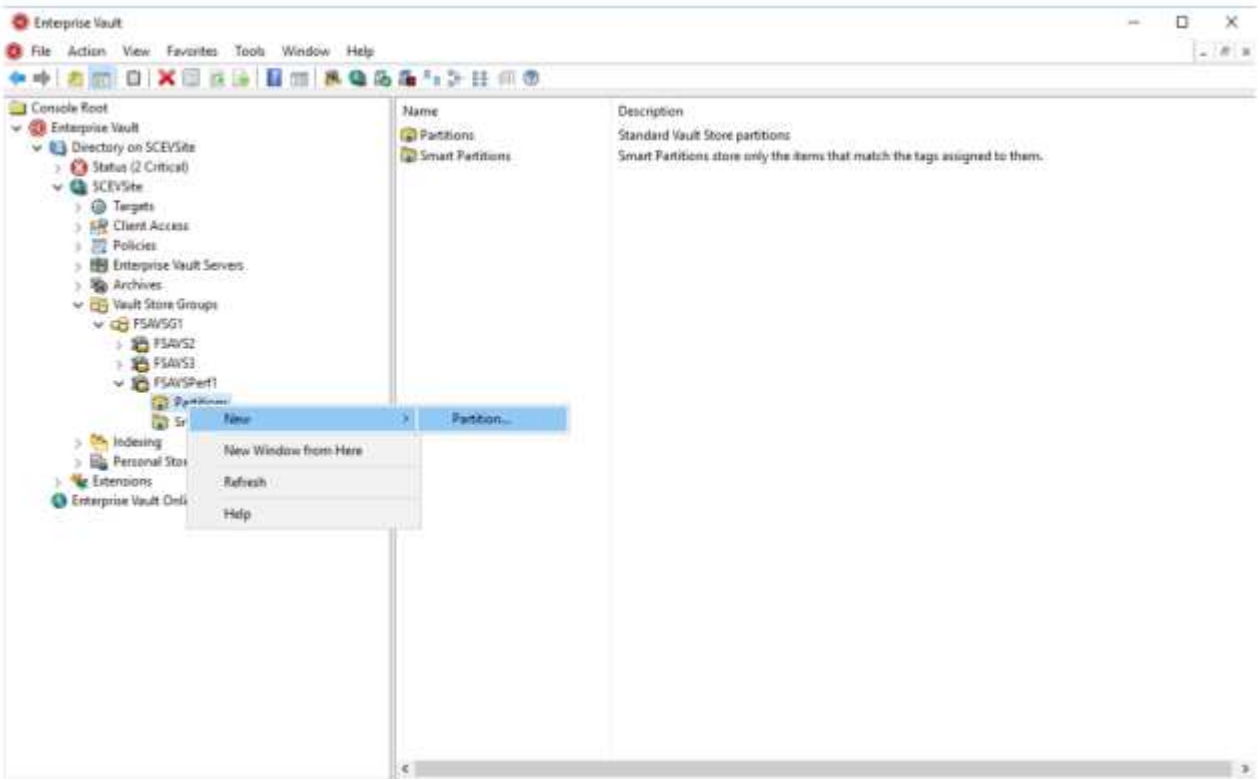
Veritas Enterprise Vault를 사용하여 StorageGRID를 구성하려면 다음 단계를 완료하십시오.

단계

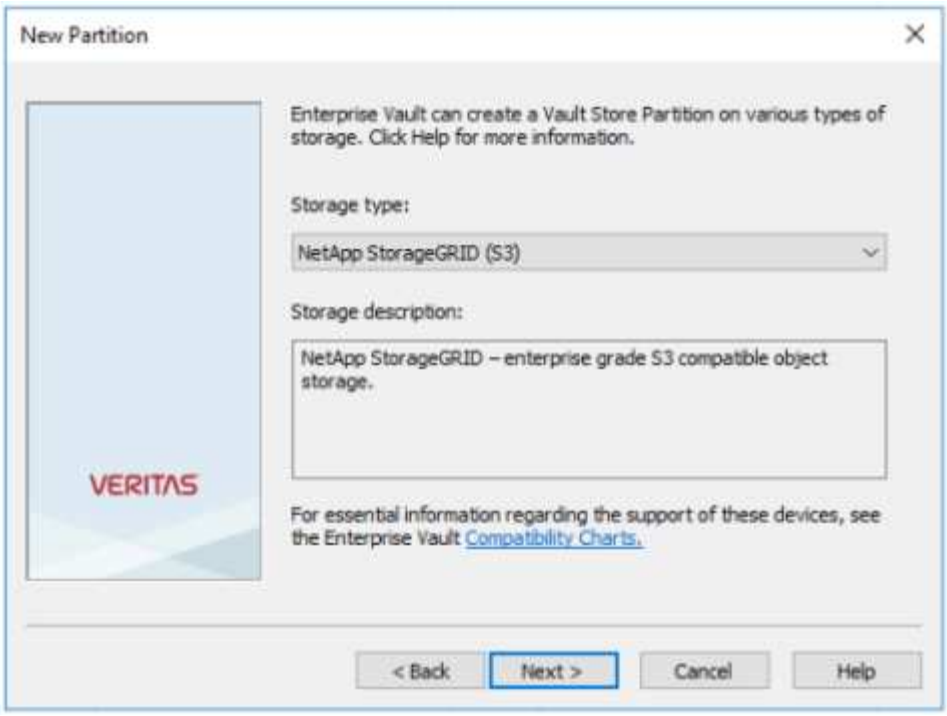
1. Enterprise Vault 관리 콘솔을 시작합니다.



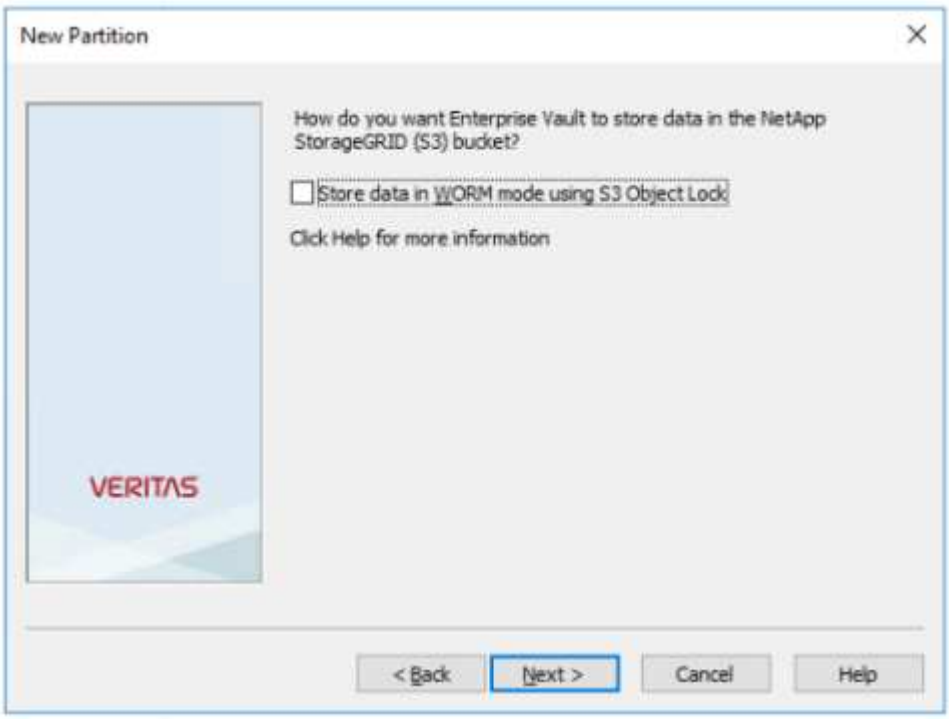
2. 적절한 볼트 저장소에 새 볼트 저장소 파티션을 작성합니다. 볼트 저장소 그룹 폴더를 확장한 다음 적절한 볼트 저장소를 확장합니다. 파티션 을 마우스 오른쪽 단추로 클릭하고 메뉴: 새로 만들기 [파티션] 를 선택합니다.



3. 새 파티션 생성 마법사를 따릅니다. 스토리지 유형 드롭다운 메뉴에서 NetApp StorageGRID (S3) 를 선택합니다. 다음 을 클릭합니다.

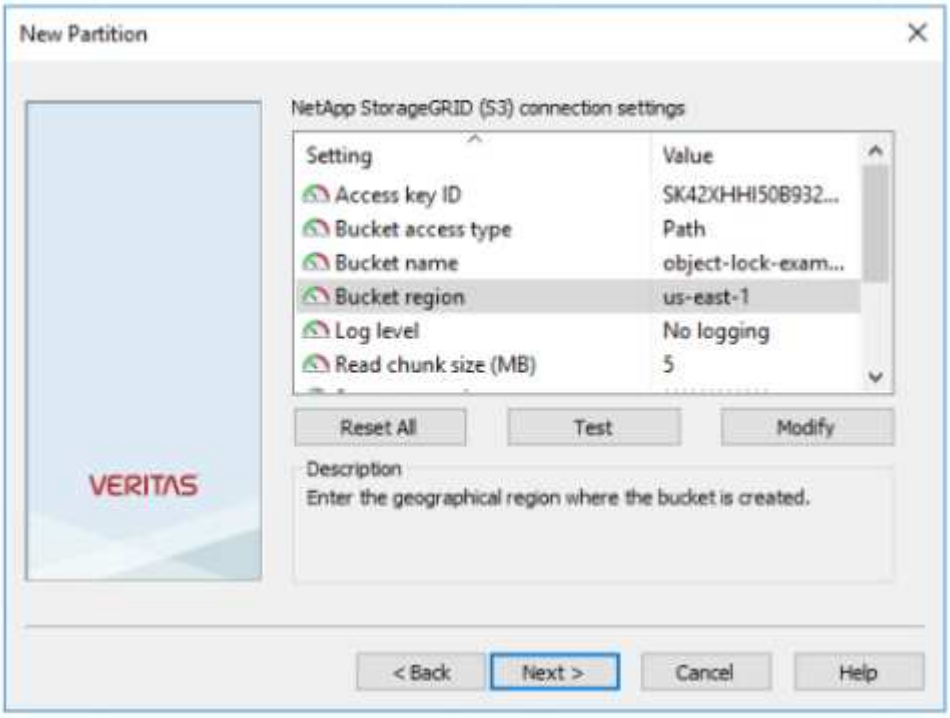


4. S3 오브젝트 잠금을 사용하여 WORM 모드로 데이터 저장 옵션을 선택하지 않은 상태로 둡니다. 다음 을 클릭합니다.

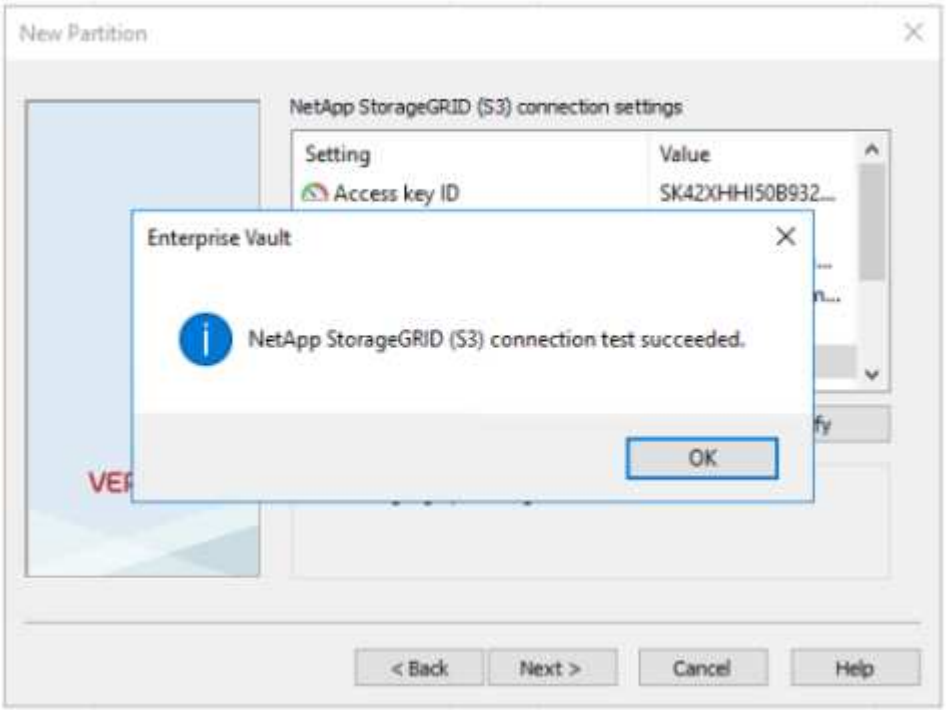


5. 연결 설정 페이지에서 다음 정보를 제공합니다.
   - 액세스 키 ID입니다
   - 비밀 액세스 키
   - 서비스 호스트 이름: StorageGRID(예: https://<hostname>:<LBE_port>)에 구성된 로드 밸런서 엔드포인트(LBE) 포트를 포함해야 합니다.

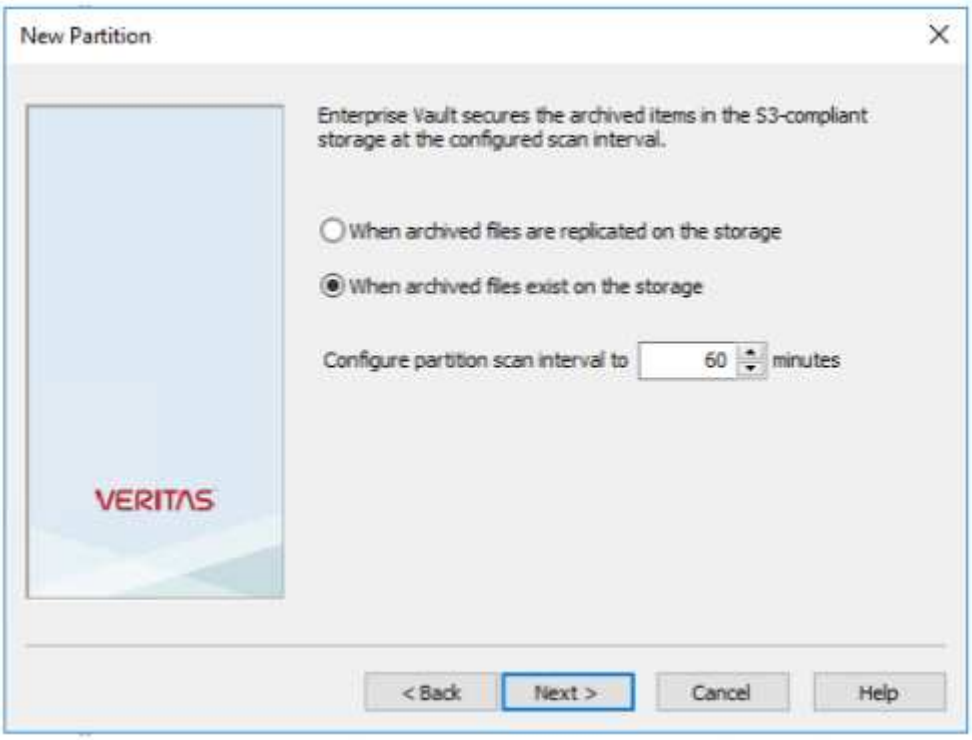
- 버킷 이름: 사전 생성된 타겟 버킷의 이름입니다. Veritas Enterprise Vault는 버킷을 생성하지 않습니다.
- 버킷 영역: `us-east-1` 이(가) 기본값입니다.



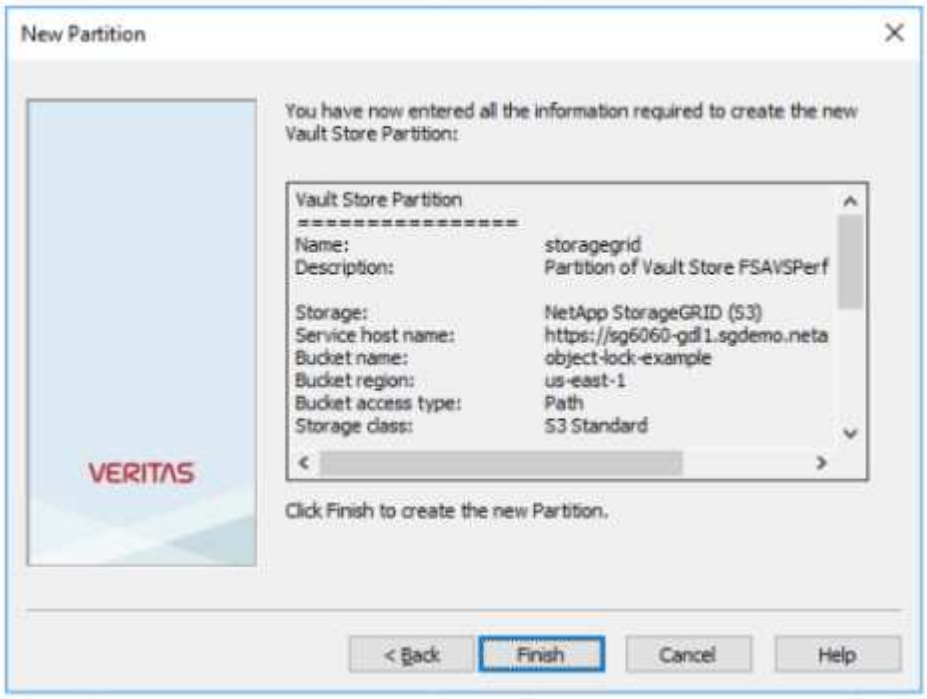
6. StorageGRID 버킷에 대한 연결을 확인하려면 테스트 를 클릭합니다. 연결 테스트가 성공했는지 확인합니다. 확인을 클릭한 후 다음을 클릭합니다.



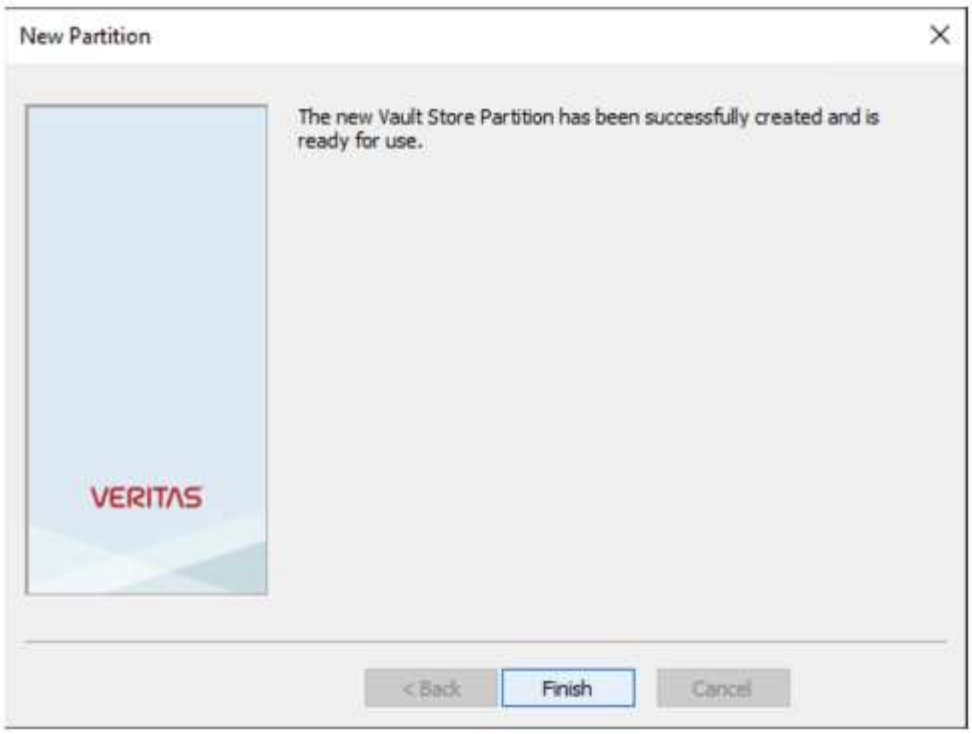
7. StorageGRID는 S3 복제 매개 변수를 지원하지 않습니다. 오브젝트를 보호하기 위해 StorageGRID은 ILM(정보 라이프사이클 관리) 규칙을 사용하여 여러 복사본 또는 삭제 코딩 등 데이터 보호 체계를 지정합니다. When Archived Files exist on the Storage 옵션을 선택하고 Next를 클릭합니다.



8. 요약 페이지에서 정보를 확인하고 마침 을 클릭합니다.



9. 새 볼트 저장소 파티션이 생성되면 StorageGRID를 기본 저장소로 사용하여 Enterprise Vault에서 데이터를 보관, 복원 및 검색할 수 있습니다.



WORM 스토리지에 대한 StorageGRID S3 오브젝트 잠금을 구성합니다

S3 오브젝트 잠금을 사용하여 WORM 스토리지에 StorageGRID를 구성하는 방법에 대해 알아보십시오.

WORM 스토리지를 위해 StorageGRID를 구성하기 위한 사전 요구 사항

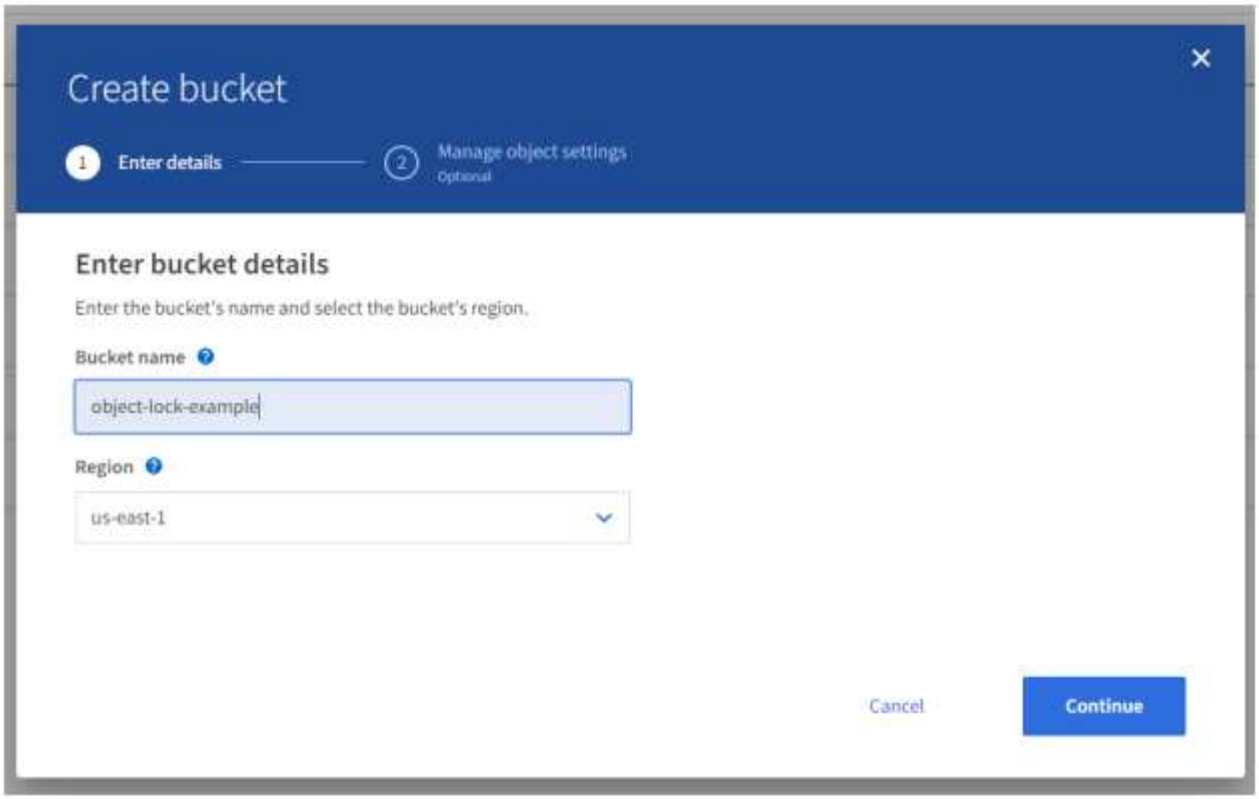
WORM 스토리지의 경우 StorageGRID은 S3 오브젝트 잠금을 사용하여 규정 준수를 위해 오브젝트를 유지합니다. 이를 위해서는 S3 오브젝트 잠금 기본 버킷 보존이 도입된 StorageGRID 11.6 이상이 필요합니다. Enterprise Vault에는 버전 14.2.2 이상이 필요합니다.

StorageGRID S3 오브젝트 잠금 기본 버킷 보존을 구성합니다

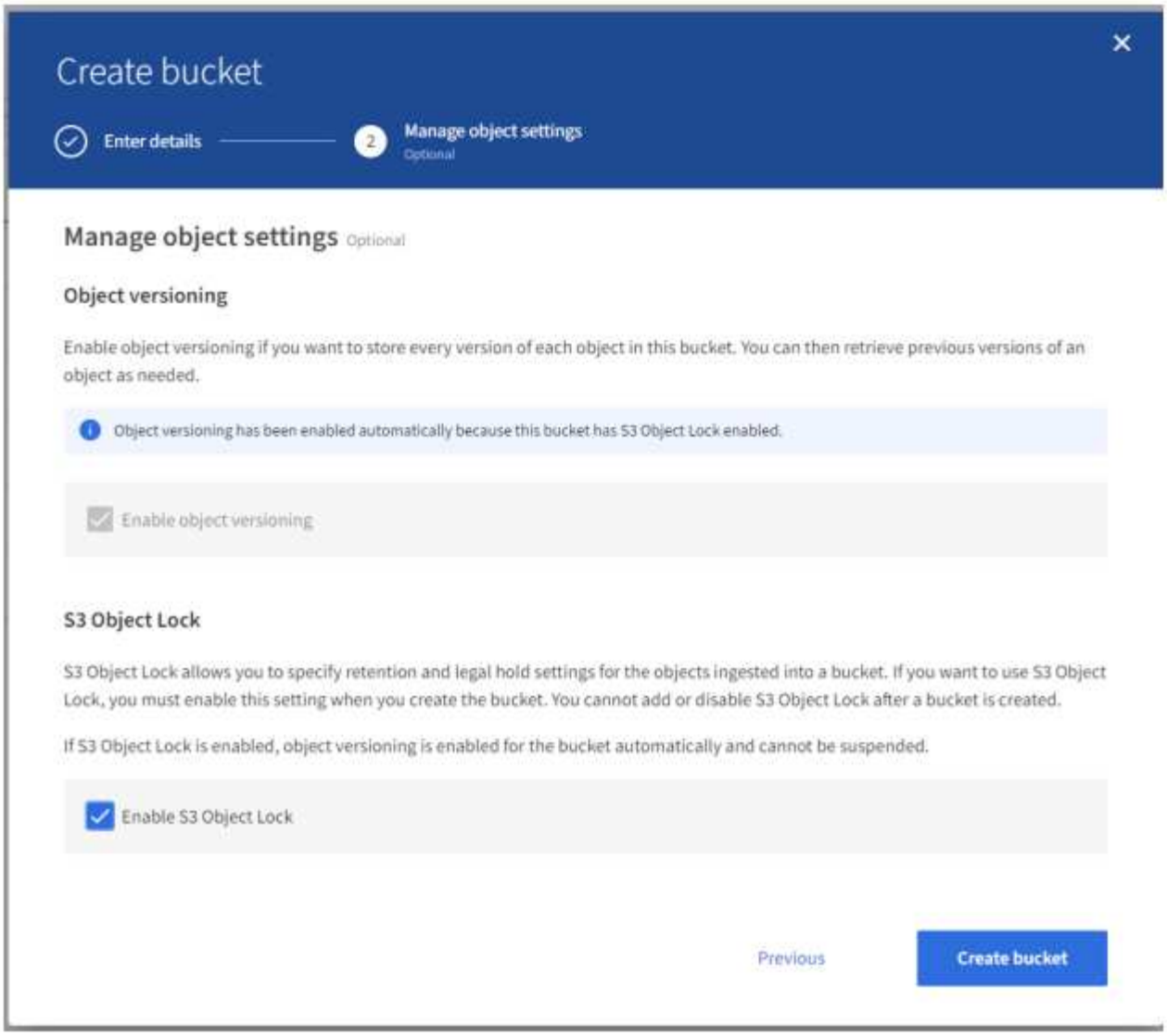
StorageGRID S3 오브젝트 잠금 기본 버킷 보존을 구성하려면 다음 단계를 완료하십시오.

단계

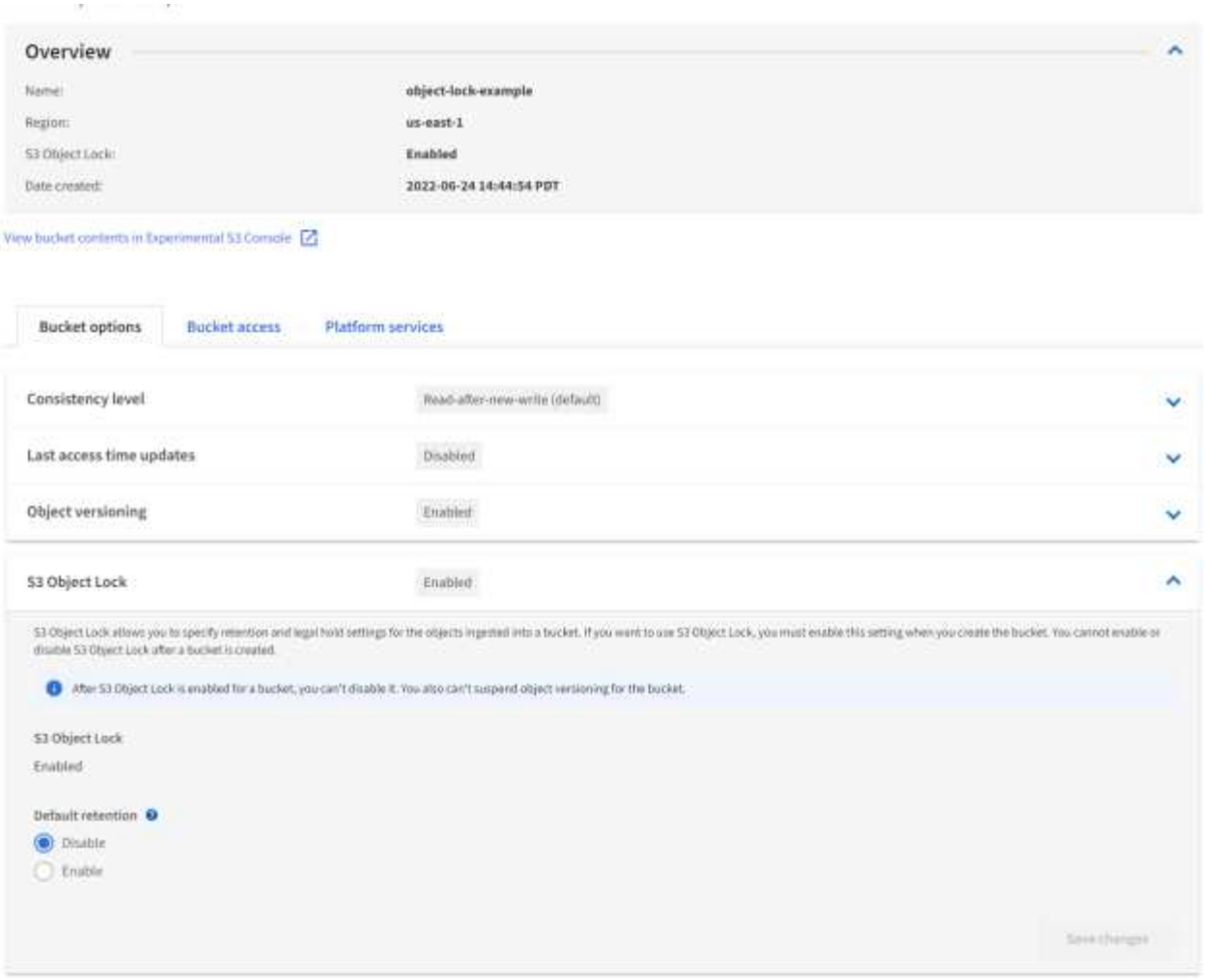
1. StorageGRID 테넌트 관리자에서 버킷을 생성하고 계속을 클릭합니다



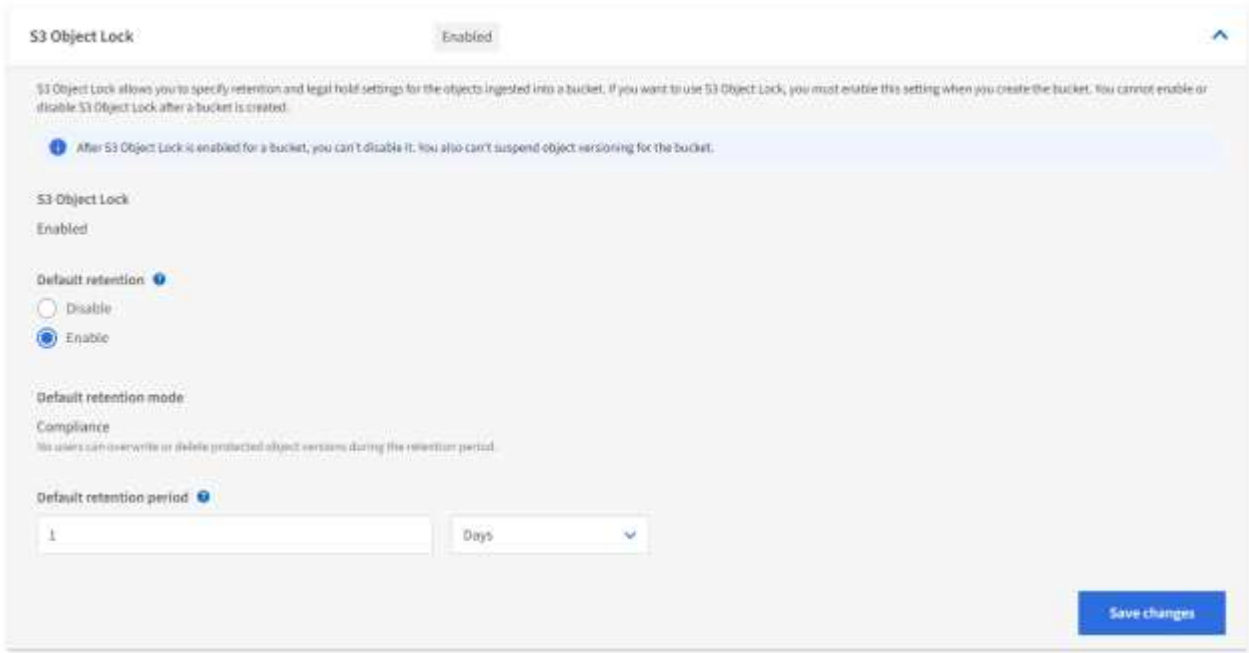
2. Enable S3 Object Lock 옵션을 선택하고 Create Bucket 을 클릭합니다.



3. 버킷을 생성한 후 버킷을 선택하여 버킷 옵션을 봅니다. S3 오브젝트 잠금 드롭다운 옵션을 확장합니다.



4. 기본 보존에서 사용을 선택하고 기본 보존 기간을 1일로 설정합니다. 변경 내용 저장 을 클릭합니다.



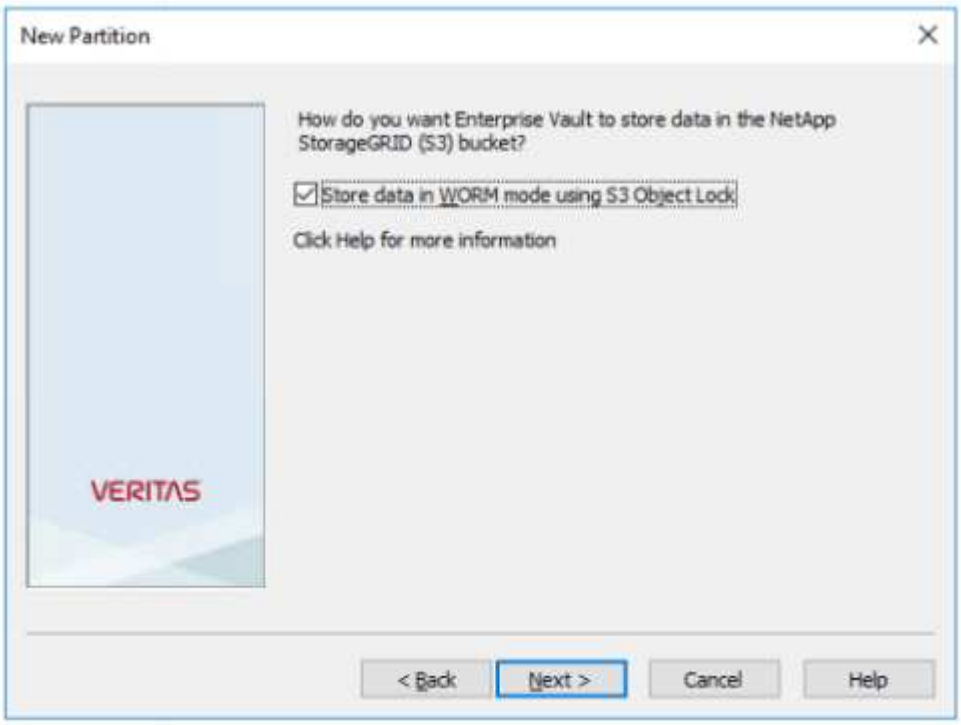
이제 Enterprise Vault에서 WORM 데이터를 저장할 준비가 되었습니다.

Enterprise Vault 설정

Enterprise Vault를 구성하려면 다음 단계를 완료하십시오.

단계

1. 섹션에서 1-3단계를 반복하되 "기본 구성" 이번에는 S3 오브젝트 잠금을 사용하여 WORM 모드에 데이터 저장 옵션을 선택합니다. 다음 을 클릭합니다.



2. S3 Bucket 연결 설정을 입력할 때 S3 오브젝트 잠금 기본 보존이 활성화된 S3 버킷 이름을 입력해야 합니다.
3. 연결을 테스트하여 설정을 확인합니다.

재해 복구를 위한 StorageGRID 사이트 장애 조치 구성

재해 복구 시나리오에서 StorageGRID 사이트 장애 조치를 구성하는 방법에 대해 알아보십시오.

StorageGRID 아키텍처 구축이 멀티사이트인 것이 일반적입니다. 사이트는 DR을 위한 액티브-액티브 또는 액티브-패시브일 수 있습니다. DR 시나리오에서 Veritas Enterprise Vault가 운영 스토리지(StorageGRID)에 대한 연결을 유지하고 사이트 장애 시에도 데이터를 계속 수집 및 검색할 수 있는지 확인합니다. 이 섹션에서는 2개 사이트, 액티브-패시브 구축을 위한 고급 구성 지침을 제공합니다. 이러한 지침에 대한 자세한 내용은 "StorageGRID 설명서" 페이지를 참조하거나 StorageGRID 전문가에게 문의하십시오.

Veritas Enterprise Vault를 사용하여 StorageGRID를 구성하기 위한 사전 요구 사항

StorageGRID 사이트 페일오버를 구성하기 전에 다음과 같은 사전 사항을 확인하십시오.

- 사이트 1과 사이트 2개와 같은 두 개의 StorageGRID 배포가 있습니다.

- 각 사이트에서 로드 밸런싱을 위해 로드 밸런서 서비스 또는 게이트웨이 노드를 실행하는 관리자 노드가 생성되었습니다.
- StorageGRID 로드 밸런서 끝점이 생성되었습니다.

StorageGRID 사이트 페일오버 구성

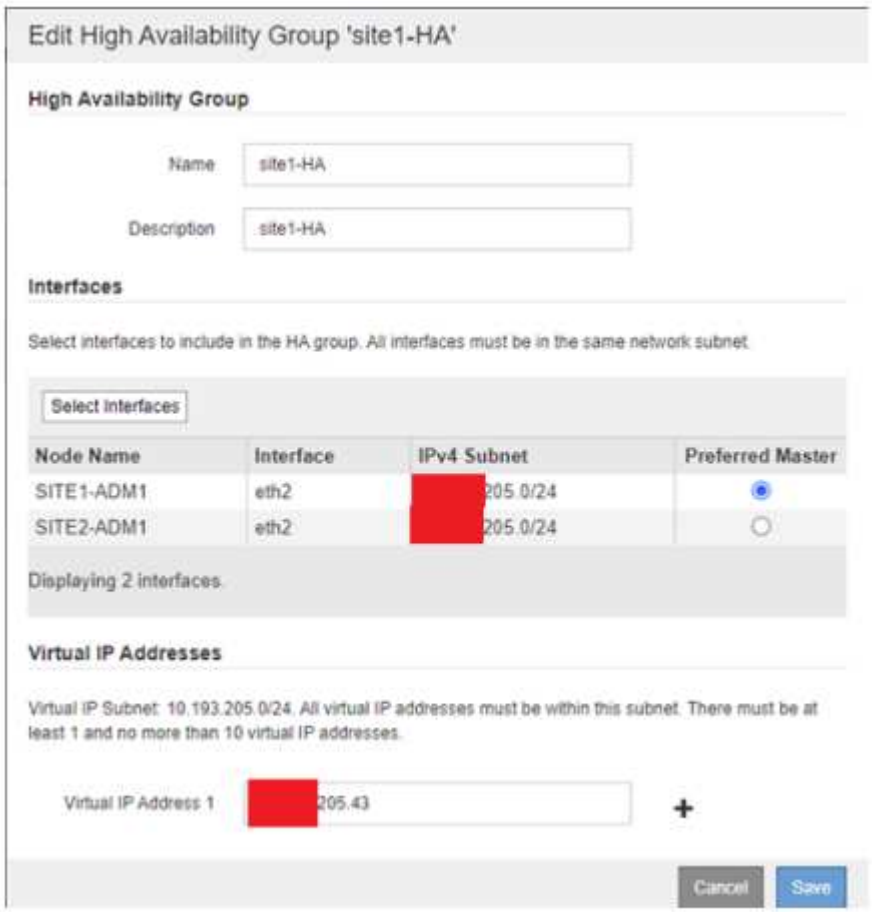
StorageGRID 사이트 장애 조치를 구성하려면 다음 단계를 완료하십시오.

단계

1. 사이트 장애 시 StorageGRID에 대한 연결을 보장하려면 고가용성(HA) 그룹을 구성합니다. StorageGRID 그리드 관리자 인터페이스(GMI)에서 구성, 고가용성 그룹 및 + 생성을 클릭합니다.

   [Vertias/Veritas - 생성 - 고가용성 - 그룹]

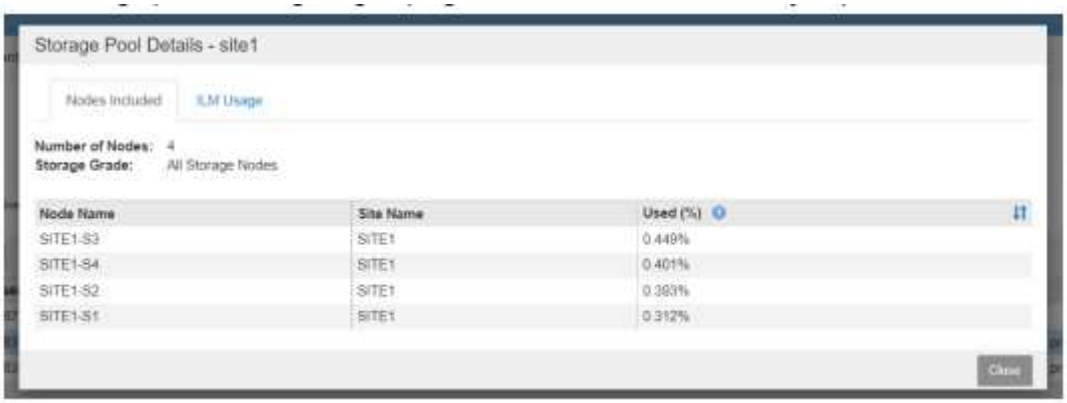
2. 필요한 정보를 입력합니다. Select Interfaces를 클릭하고 site1과 site2의 네트워크 인터페이스를 모두 포함합니다. 여기서 site1(운영 사이트)이 기본 마스터입니다. 동일한 서브넷 내에서 가상 IP 주소를 할당합니다. 저장 을 클릭합니다.

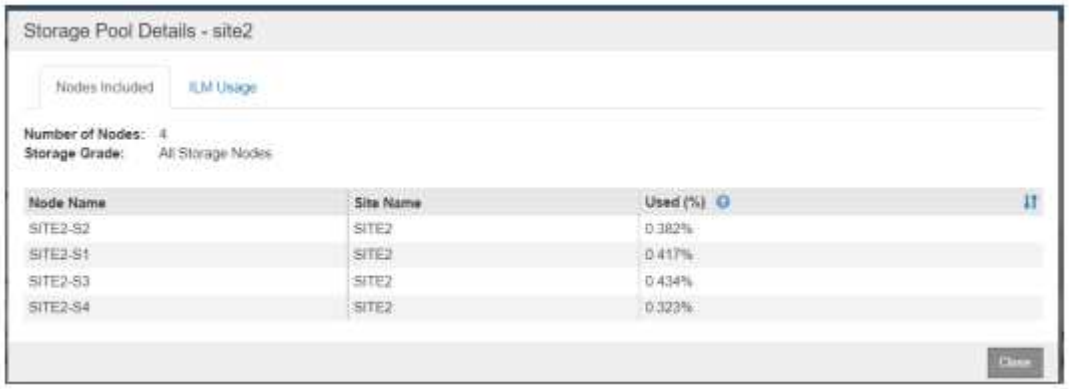


3. 이 가상 IP(VIP) 주소는 Veritas Enterprise Vault의 파티션 구성 중에 사용되는 S3 호스트 이름과 연결되어야 합니다. VIP 주소는 트래픽을 사이트1로 해결하고, 사이트1에 장애가 발생하면 VIP 주소는 트래픽을 사이트2로 투명하게 다시 라우팅합니다.
4. 데이터가 site1과 site2에 모두 복제되었는지 확인합니다. 이렇게 하면 site1이 실패해도 site2에서 개체 데이터를 계속 사용할 수 있습니다. 이 작업은 먼저 스토리지 풀을 구성하여 수행합니다.

StorageGRID GMI에서 ILM, 스토리지 풀, + 생성을 차례로 클릭합니다. 마법사를 따라 site1에 대해 하나씩, site2에 대해 두 개의 스토리지 풀을 생성합니다.

스토리지 풀은 오브젝트 배치를 정의하는 데 사용되는 노드의 논리적 그룹입니다





5. StorageGRID GMI에서 ILM, 규칙을 클릭한 다음 + 만들기를 클릭합니다. 마법사에 따라 수집 동작이 Balanced인 사이트당 저장할 복제본 하나를 지정하는 ILM 규칙을 생성합니다.

6. ILM 규칙을 ILM 정책에 추가하고 정책을 활성화합니다.

이렇게 구성하면 다음과 같은 결과가 나타납니다.

- site1이 운영 엔드포인트이고 site2가 보조 엔드포인트입니다. site1에 장애가 발생하면 VIP가 site2로 페일오버됩니다.
- 아카이빙된 데이터가 Veritas Enterprise Vault에서 전송되면 StorageGRID는 복제본 한 개가 사이트1에 저장되고 다른 DR 복제본이 사이트2에 저장되도록 보장합니다. site1에 장애가 발생하면 Enterprise Vault는 사이트2에서

계속 수집 및 검색합니다.

이 두 구성은 모두 Veritas Enterprise Vault에 영향을 미치지 않습니다. S3 끝점, 버킷 이름, 액세스 키 등은 동일합니다. Veritas Enterprise Vault 파티션에서 S3 연결 설정을 재구성할 필요가 없습니다.

StorageGRID 평가판 소프트웨어에 액세스하는 단계

이 지침은 NetApp과 협력하는 NetApp 세일즈, 파트너 및 잠재 고객을 위한 것입니다.

계정을 등록하십시오

1. 회사 이메일을 사용하여 에 계정을 "NetApp Support 사이트" 등록합니다.
   a. 새로 생성된 계정으로 로그인하지 않았는지 확인합니다.
   b. 이미 계정이 있는 경우 로그인되어 있지 않은지 확인하고 다음 단계를 진행합니다.
2. 비기술적 지원 케이스를 생성하여 액세스 수준을 "잠재 고객"으로 높입니다. 이렇게 하려면 ""문제를 보고하십시오 "웹 사이트의 바닥글에서 " 링크를 클릭하십시오.
3. 피드백 범주로 "등록 문제"를 선택합니다.
4. 설명 섹션에 "내 계정 이메일 주소는 _ 귀하의 - 이메일 - 주소 _ 입니다. 잠재 고객이 StorageGRID 평가판 소프트웨어를 다운로드할 수 있도록 액세스하려고 합니다."
   a. 잠재 고객 액세스 요청을 제안한 NetApp 내부 담당자의 이름을 언급하십시오.

StorageGRID를 다운로드합니다

1. 지원 케이스를 검토 및 승인하면 NetApp 지원 팀에서 이메일을 통해 귀하의 계정에 잠재 고객 액세스 권한이 부여되었음을 알려드립니다.
2. 를 "StorageGRID 평가판 소프트웨어"다운로드하십시오.

평가판 라이센스 파일은 zip 파일 내에 있습니다. 일단 압축이 풀리면 StorageGRID-Webscale-<version>\vSphere\NLF000000.txt 입니다.

소프트웨어 다운로드는 법적 요구 사항을 준수하기 위한 무역 규정 준수 조치와 관련된 프로세스입니다. 규정 준수를 보장하기 위해 사용자는 액세스 권한을 얻기 전에 계정을 생성하고 지원 케이스를 개설해야 합니다. 이 프로세스를 통해 잠재 고객에게 필요한 즉시 운영 가능한 소프트웨어를 제공하는 동시에 적절한 제어 및 문서화를 유지할 수 있습니다.

StorageGRID는 오픈 소스 또는 대체 버전이 아닌 "프로덕션 준비" 버전을 제공합니다. 잠재 고객이 프로덕션 라이센스로 업그레이드하지 않는 한 * 지원은 제공되지 않습니다 *.

위 단계에 문제가 있는 경우 StorageGRID.Feedback@netapp.com 으로 문의하십시오.

NetApp StorageGRID 블로그

여기에서 몇 가지 훌륭한 NetApp StorageGRID 블로그를 찾을 수 있습니다.

- 2024년 2월 16일: "StorageGRID 11.8 소개: 향상된 보안, 단순성 및 사용자 환경"
- 2024년 2월 16일: "StorageGRID 11.8 소개"
- 2024년 2월 2일: "StorageGRID+ lakeFS 솔루션 요약 발표"
- 2023년 12월 12일: "StorageGRID에 대한 빅 데이터 분석: Dremio는 Apache Hive보다 23배 빠른 성능을 제공합니다"
- 2023년 11월 7일: "StorageGRID를 이용한 온프레미스 글레이셔 스펙트럼 로직"
- 2023년 10월 17일: "하둡을 통한 전환: Dremio 및 StorageGRID로 데이터 분석 현대화"
- 2023년 9월 1일: "Cloud Insights를 활용하여 Fluent Bit을 사용하여 로그를 모니터링하고 수집합니다"
- 2023년 8월 30일: "Amazon S3 파일 시스템의 마운트 지점이 이제 GA로 변경되었습니다"
- 2023년 5월 16일: "StorageGRID 11.7 및 새로운 All-Flash 오브젝트 스토리지 어플라이언스 SGF6112를 소개합니다"
- 2023년 5월 16일: "StorageGRID 오브젝트 스토리지 제품군의 새로운 기능"
- 2023년 3월 30일: "StorageGRID를 사용한 Amazon S3 알파 릴리스 마운트 지점"
- 2023년 3월 30일: "BlueXP를 사용하여 3:2:1 호환 백업 정책으로 Epic EHR을 보호합니다"
- 2023년 3월 14일: "3:2:1 호환 아키텍처에서 하나의 명령으로 Epic Systems EHR 데이터베이스를 백업하는 방법"
- 2023년 2월 14일: "초콜릿, 스키, 시계, 메인프레임의 공통점은 무엇입니까?"
- 2023년 1월 18일: "StorageGRID S3 오브젝트 잠금은 Veritas NetBackup에서 검증되었습니다"
- 2023년 1월 16일: "StorageGRID는 NF203 및 ISO/IEC 25051 준수 인증을 갱신합니다"
- 2022년 12월 6일: "StorageGRID는 KPMG 규정 준수 인증을 획득했습니다"
- 2022년 11월 23일: "NetApp과 Modzy가 제공하는 MLOps를 통한 설명 가능한 AI"
- 2022년 11월 7일: "StorageGRID 및 ONTAP S3 지원: 차이점, 유사점 및 통합"
- 2022년 10월 5일: "NetApp Cloud Insights에는 StorageGRID 갤러리 대시보드가 추가되었습니다"
- 2022년 10월 5일: "스노우플레이크(Snowflake)용 StorageGRID에서 데이터를 해동하십시오"
- 2022년 9월 26일: "서비스 공급자를 위한 NetApp StorageGRID"
- 2022년 9월 19일: "StorageGRID용 DataLock 및 랜섬웨어 보호 지원"
- 2022년 9월 1일: "다음 메트릭을 사용하여 그래프로 표시합니다"
- 2022년 8월 23일: "StorageGRID에서 데이터 레이크를 구축합니다"
- 2022년 8월 17일: "이 모든 것은 개체 잠금에서 시작됩니다… 중요 백업 애플리케이션을 위한 S3 스토리지 에코시스템 구축"
- 2022년 8월 16일: "StorageGRID를 오픈 소스 엘크 스택과 통합하여 고객 경험을 개선합니다"
- 2022년 8월 5일: "NetApp StorageGRID는 일반 조건 보안 인증을 획득했습니다"
- 2022년 7월 26일: "StorageGRID의 검증된 파트너 솔루션 목록 을 확인하십시오"

- 2022년 6월 9일: "StorageGRID와 함께 Cloudera Hadoop S3A 커넥터를 사용하십시오"
- 2022년 5월 26일: "StorageGRID: 사내 백업 및 복제 데이터 저장 및 관리"
- 2022년 5월 24일: "NetApp과 Alluxio로 분석 워크로드를 현대화하십시오"
- 2022년 5월 10일: "Lab on Demand는 StorageGRID를 위한 최고의 영업 툴입니다"

NetApp StorageGRID 문서

각 NetApp StorageGRID 릴리스에 대한 전체 설명서는 여기에서 확인할 수 있습니다.

- "StorageGRID 어플라이언스"
- "StorageGRID 소프트웨어 11.5 - 12.0"

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인 정보 보호 정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

https://library.netapp.com/ecm/ecm_download_file/2879263

https://library.netapp.com/ecm/ecm_download_file/2881511